Symbolic Logic

An Accessible Introduction to Serious Mathematical Logic

Volume II

Tony Roy

version 7.3

January 19, 2017

Preface

There is, I think, a gap between what many students learn in their first course in formal logic, and what they are expected to know for their second. While courses in mathematical logic with metalogical components often cast only the barest glance at mathematical induction or even the very idea of reasoning from definitions, a first course may also leave these untreated, and fail explicitly to lay down the definitions upon which the second course is based. The aim of this text is to integrate material from these courses and, in particular, to make serious mathematical logic accessible to students I teach. The first parts introduce classical symbolic logic as appropriate for beginning students; the last parts build to Gödel's adequacy and incompleteness results. A distinctive feature of the last section is a complete development of Gödel's second incompleteness theorem.

Accessibility, in this case, includes components which serve to locate this text among others: First, assumptions about background knowledge are minimal. I do not assume particular content about computer science, or about mathematics much beyond high school algebra. Officially, everything is introduced from the ground up. No doubt, the material requires a certain sophistication — which one might acquire from other courses in critical reasoning, mathematics or computer science. But the requirement does not extend to particular contents from any of these areas.

Second, I aim to build skills, and to keep conceptual distance for different applications of 'so' relatively short. Authors of books that are completely correct and precise may assume skills and require readers to recognize connections not fully explicit. It may be that this accounts for some of the reputed difficulty of the material. The results are often elegant. But this can exclude a class of students capable of grasping and benefiting from the material, if only it is adequately explained. Thus I attempt explanations and examples to put the student at every stage in a position to understand the next. In some cases, I attempt this by introducing relatively concrete methods for reasoning. The methods are, no doubt, tedious or unnecessary for the experienced logician. However, I have found that they are valued by students, insofar as students are presented with an occasion for success. These methods are not meant to wash over or substitute for understanding details, but rather to expose and clarify them. Clarity, beauty and power come, I think, by getting at details, rather than burying or ignoring them.

Third, the discussion is ruthlessly directed at core results. Results may be rendered inaccessible to students, who have many constraints on their time and schedules, simply because the results would come up in, say, a second course rather than a first. My idea is to exclude side topics and problems, and to go directly after (what I see as) the core. One manifestation is the way definitions and results from earlier sections feed into ones that follow. Thus simple integration is a benefit. Another is the way predicate logic with identity is introduced as a whole in Part I. Though it is possible to isolate sentential logic from the first parts of chapter 2 through chapter 7, and so to use the text for separate treatments of sentential and predicate logic, the guiding idea is to avoid repetition that would be associated with independent treatments for sentential logic, or perhaps monadic predicate logic, the full predicate logic, and predicate logic with identity.

Also (though it may suggest I am not so ruthless about extraneous material as I would like to think), I try to offer some perspective about what is accomplished along the way. In addition, this text may be of particular interest to those who have, or desire, an exposure to natural deduction in formal logic. In this case, accessibility arises from the nature of the system, and association with what has come before. In the first part, I introduce both axiomatic and natural derivation systems; and in Part III, show how they are related.

There are different ways to organize a course around this text. For students who are likely to complete the whole, the ideal is to proceed sequentially through the text from beginning to end (but postponing chapter 3 until after chapter 6). Taken as wholes, Part II depends on Part I; Parts III and IV on Parts I and II. Part IV is mostly independent of Part III. I am currently working within a sequence that isolates sentential logic from quantificational logic, treating them in separate quarters, together covering all of chapters 1 - 7 (except 3). A third course picks up leftover chapters from the first two parts (3 and 8) with Part III; and a fourth the leftover chapters from the first parts with Part IV. Perhaps not the most efficient arrangement, but the best I have been able to do with shifting student populations. Other organizations are possible!

A remark about chapter 7 especially for the instructor: By a formal system for reasoning with semantic definitions, chapter 7 aims to leverage derivation skills from earlier chapters to informal reasoning with definitions. I have had a difficult time convincing instructors to try this material — and even been told flatly that these skills "cannot be taught." In my experience, this is false (and when I have been able to convince others to try the chapter, they have quickly seen its value). Perhaps the difficulty is that it is "weird" — none of us had anything like this when we learned logic. Of course, if one is presented with students whose mathematical sophistication is sufficient for advanced work, the material is not necessary. But if, as is often the case especially for students in philosophy, one obtains one's mathematical sophistication *from* courses in logic, this chapter is an important part of the bridge from earlier material to later. Additionally, the chapter is an important "take-away" even for students who will not continue to later material. The chapter closes an open question from chapter 4 — how it is possible to demonstrate quantificational validity. But further, the ability to reason closely with definitions is a skill from which students in (sentential or) predicate logic, even though they never go on to formalize another sentence or do another derivation, will benefit both in philosophy and more generally.

Another remark about the (long) sections 13.3, 13.4 and 13.5. These develop in PA the "derivability conditions" for Gödel's second theorem. They are perhaps for enthusiasts. Still, in my experience many students are enthusiasts and, especially from an introduction, benefit by seeing how the conditions are derived. There are different ways to treat the sections. One might work through them in some detail. One might wave at results individually. And even for the short shrift often accorded the derivability conditions, there is an advantage having a sort of panorama at which one can point and say "thus it is accomplished!"

Naturally, results in this book are not innovative. If there is anything original, it is in presentation. Even here, I am greatly indebted to others, especially perhaps Bergmann, Moor and Nelson, *The Logic Book*, Mendelson, *Introduction to Mathematical Logic*, and Smith, *An Introduction to Gödel's Theorems*. I thank my first logic teacher, G.J. Mattey, who communicated to me his love for the material. And I thank especially my colleagues John Mumma and Darcy Otto for many helpful comments. Hannah Baehr and Catlin Andrade made comments and produced answers to exercises for certain parts. In addition I have received helpful feedback from Steve Johnson, along with students in different logic classes at CSUSB. I welcome comments, and expect that your sufferings will make it better still.

This text evolved over a number of years starting modestly from notes originally provided as a supplement to other texts. It is now long (!) and perhaps best conceived in separate volumes for Parts I and II and then Parts III and IV. With the addition of Part IV it is complete for the first time in this version. (But chapter 11, which I rarely get to in teaching, remains a stub that could be developed in different directions.) Most of the text is reasonably stable, though I shall be surprised if I have not introduced errors in the last part both substantive and otherwise.

I think this is fascinating material, and consider it great reward when students respond “cool!” as they sometimes do. I hope you will have that response more than once along the way.

T.R.
Winter 2017

Contents

Preface **i**

Contents **v**

Named Definitions **ix**

Quick Reference Guides **xvii**

I The Elements: Four Notions of Validity **1**

1 Logical Validity and Soundness **5**
- 1.1 Consistent Stories 6
- 1.2 The Definitions 12
- 1.3 Some Consequences 24

2 Formal Languages **32**
- 2.1 Introductory 32
- 2.2 Sentential Languages 34
- 2.3 Quantificational Languages 48

3 Axiomatic Deduction **69**
- 3.1 General 70
- 3.2 Sentential 74
- 3.3 Quantificational 82

4 Semantics **98**
- 4.1 Sentential 98
- 4.2 Quantificational 115

5 Translation **140**
5.1 General 140
5.2 Sentential 142
5.3 Quantificational 173

6 Natural Deduction **210**
6.1 General 210
6.2 Sentential 220
6.3 Quantificational 273
6.4 The system *ND+* 321

II Transition: Reasoning About Logic **332**

7 Direct Semantic Reasoning **334**
7.1 General 335
7.2 Sentential 338
7.3 Quantificational 354

8 Mathematical Induction **381**
8.1 General Characterization 381
8.2 Preliminary Examples 387
8.3 Further Examples (for Part III) 401
8.4 Additional Examples (for Part IV) 411

III Classical Metalogic: Soundness and Adequacy **426**

9 Preliminary Results **429**
9.1 Semantic Validity Implies Logical Validity 429
9.2 Validity in *AD* Implies Validity in *ND* 434
9.3 Validity in *ND* Implies Validity in *AD* 441
9.4 Extending to *ND+* 462

10 Main Results **467**
10.1 Soundness 468
10.2 Sentential Adequacy 475
10.3 Quantificational Adequacy: Basic Version 486
10.4 Quantificational Adequacy: Full Version 501

11 More Main Results **517**
11.1 Expressive Completeness 517
11.2 Unique Readability 522
11.3 Independence 525
11.4 Isomorphic Models 529
11.5 Compactness and Isomorphism 539
11.6 Submodels and Löwenheim-Skolem 541

IV Logic and Arithmetic: Incompleteness and Computability **546**

12 Recursive Functions and Q **550**
12.1 Recursive Functions 552
12.2 Expressing Recursive Functions 559
12.3 Capturing Recursive Functions 569
12.4 More Recursive Functions 587
12.5 Essential Results 607

13 Gödel's Theorems **618**
13.1 Gödel's First Theorem 618
13.2 Gödel's Second Theorem: Overview 626
13.3 The Derivability Conditions: Background 631
13.4 The Second Condition: $\Box(\mathscr{P} \to \mathscr{Q}) \to (\Box\mathscr{P} \to \Box\mathscr{Q})$ 670
13.5 The Third Condition: $\Box\mathscr{P} \to \Box\Box\mathscr{P}$ 700
13.6 Reflections on the theorem 722

14 Logic and Computability **732**
14.1 Turing Computable Functions 732
14.2 Essential Results 746
14.3 Church's Thesis 752

Concluding Remarks **772**

Answers to Selected Exercises **775**
Chapter Nine 776
Chapter Ten 789
Chapter Eleven 794
Chapter Twelve 795
Chapter Thirteen 802

Chapter Fourteen 910

Bibliography **911**

Index **915**

Named Definitions

chapter 1

AR	Argument	5
LV	Logical Validity	12
LS	Logical Soundness	12
IT	Invalidity Test	13
VT	Validity Test	17

chapter 2

VC	Vocabulary (sentential)	34
FR	Formulas (sentential)	38
SB	Subformulas	40
IS	Immediate Subformula	40
AS	Atomic Subformula	40
MO	Main Operator (formal)	40
AB	Abbreviation (sentential)	42
FR′	Abbreviated Formulas (sentential)	43
VC	Vocabulary	49
TR	Terms	53
FR	Formulas	55
AB	Abbreviation	60
FR′	Abbreviated Formulas	61

chapter 3

MP	Modus Ponens	70
AV	Axiomatic Consequence	71
AS	*AD* Sentential	74
AU	*AD* Quantificational	83
AE	*AD* Equality	86
AD	*AD* Axioms (summary)	89

PA	Peano Axioms	90
	chapter 4	
ST	Satisfaction as Truth (Sentential)	99
T(∼)	Characteristic Table (∼)	99
T(→)	Characteristic Table (→)	99
SV	Sentential Validity	107
T(∨)	Characteristic Table (∨)	111
T(∧)	Characteristic Table (∧)	111
T(↔)	Characteristic Table (↔)	112
ST′	Truth for Abbreviations (Sentential)	114
QI	Quantificational Interpretations	116
TA	Term Assignment	120
SF	Satisfaction	123
B(s)	Branch Condition (s)	124
B(r)	Branch Condition (r)	124
B(∼)	Branch Condition (∼)	124
B(→)	Branch Condition (→)	124
B(∀)	Branch Condition (∀)	125
TI	Truth on an Interpretation	127
QV	Quantificational Validity	130
B(∧)	Branch Condition (∧)	135
B(∨)	Branch Condition (∨)	135
B(↔)	Branch Condition (↔)	135
B(∃)	Branch Condition (∃)	135
SF′	Satisfaction for Abbreviations	138
	chapter 5	
CG	Criterion of Goodness for Translation	141
DC	Declarative Sentences	147
SO	Sentential Operator	147
CS	Compound and Simple	147
MO	Main Operator (informal)	147
TF	Truth Functional Operator	147
TP	Translation Procedure	150
	chapter 6	
$N1$	Natural Derivation One	211
SD	Subderivation	219
FA	Accessible Formula	219

SA	Accessible Subderivation	219
R	*ND* Reiteration	219
→E	*ND* → Exploitation	221
→I	*ND* → Introduction	222
∧E	*ND* ∧ Exploitation	225
∧I	*ND* ∧ Introduction	225
∼I	*ND* ∼ Introduction	230
∼E	*ND* ∼ Exploitation	230
⊥I	*ND* ⊥ Introduction	231
∼I	*ND* ∼ Introduction	232
∼E	*ND* ∼ Exploitation	232
∨I	*ND* ∨ Introduction	233
∨E	*ND* ∨ Exploitation	233
↔E	*ND* ↔ Exploitation	239
↔I	*ND* ↔ Introduction	239
SG	Strategies for a Goal (Sentential)	247
SC	Strategies for a Contradiction (Sentential)	260
∀E	*ND* ∀ Exploitation	274
∃I	*ND* ∃ Introduction	276
∀I	*ND* ∀ Introduction	280
∃E	*ND* ∃ Exploitation	283
SG	Strategies for a Goal	290
SC	Strategies for a Contradiction	290
=I	*ND* = Introduction	301
=E	*ND* = Exploitation	302
(∀E)	(∀) Exploitation	306
(∃I)	(∃) Introduction	306
(∀I)	(∀) Introduction	306
(∃E)	(∃) Exploitation	306
Q	Robinson Arithmetic Axioms	306
IN	Mathematical Induction	312
PA7	Peano Induction Axiom	318
MT	*ND*+ Modus Tollens	321
NB	*ND*+ Negated Biconditional	321
DS	*ND*+ Disjunctive Syllogism	322
HS	*ND*+ Hypothetical Syllogism	322
DN	*ND*+ Double Negation	323
Com	*ND*+ Commutation	324

Assoc	*ND*+ Association	324
Idem	*ND*+ Idempotence	324
Impl	*ND*+ Implication	324
Trans	*ND*+ Transposition	324
DeM	*ND*+ DeMorgan	325
Exp	*ND*+ Exportation	325
Equiv	*ND*+ Equivalence	325
Dist	*ND*+ Distribution	325
QN	*ND*+ Quantifier Negation	325
BQN	*ND*+ Bounded Quantifier Negation	325

chapter 7

ST(|)	Satisfaction for Stroke	337
T(|)	Characteristic Table (|)	338
ST	Sentential Truth (formalized)	339
com	Commutation (metalinguistic)	339
idm	Idempotence (metalinguistic)	339
dem	DeMorgan (metalinguistic)	339
cnj	Conjunctive rules (metalinguistic)	339
dsj	Disjunctive rules (metalinguistic)	339
neg	Negation Rules (metalinguistic)	339
bot	Bottom Introduction (metalinguistic)	339
SV	Sentential Validity (formalized)	342
exs	Existential rules (metalinguistic)	342
ins	Inspection	343
cnd	Conditional rules (metalinguistic)	347
bcnd	Biconditional rules (metalinguistic)	347
abv	Abbreviation (metalinguistic)	347
ST′	Abbreviations for Sentential Truth (formalized)	347
dst	Distribution (metalinguistic)	349
SF	Satisfaction (formalized)	354
SF′	Abbreviations for Satisfaction (formalized)	354
TI	Truth on an Interpretation (formalized)	356
QV	Quantificational Validity (formalized)	356
unv	Universal rules (metalinguistic)	356
qn	Quantifier negation (metalinguistic)	357
TA	Term Assignment (formalized)	359
eq	Equality rules (metalinguistic)	359

SF(R)	Satisfaction for relation symbols (formalized)	360
SF(∀)	Satisfaction for ∀ (formalized)	364
SF′(∃)	Satisfaction for ∃ (formalized)	364
def	Definition (metalinguistic)	370
	chapter 8	
AI	Term Assignment on an Interpretation	414
	chapter 9	
	chapter 10	
Con	Consistency	476
(∗)	Core Thesis (sentential)	477
Max	Maximality	481
(⋆)	Core Thesis (preliminary)	489
Scgt	Scapegoat Set	493
(⋆⋆)	Core Thesis (quantificational)	501
	chapter 11	
A1(∼)	Table for Independence (∼)	526
A1(→)	Table for Independence (→)	526
A2(∼)	Table for Independence (∼)	529
A2(→)	Table for Independence (→)	529
IS	Isomorphism	530
EE	Elementary Equivalence	532
ST	Satisfiability	539
SM	Submodel	541
ES	Elementary Submodel	541
	chapter 12	
suc(x)	successor	553
zero(x)	zero	553
idnt^j_k	identity	553
CM	Composition	553
RC	Recursion	554
plus(x, y)	plus	554
times(x, y)	times	554
fact(y)	factorial	555
RT	Recursion Theorem	556
RM	regular minimization	557
RF	Recursive Functions	557

PR	primitive recursive	558
power(x, y)	power	558
EXr	Expressionr	559
EXf	Expressionf	560
CP	Capture	570
Δ_0	Delta Formulas	571
pred(y)	predecessor	587
subc(x, y)	subtraction with cutoff	587
absval(x - y)	absolute value	588
sg(y)	sign	588
csg(y)	converse sign	588
CF	characteristic function	588
$\text{EQ}(s(\vec{x}), t(\vec{y}))$	equality	589
$\text{LEQ}(s(\vec{x}), t(\vec{y}))$	less than or equal	590
$\text{LESS}(s(\vec{x}), t(\vec{y}))$	less than	590
$\text{NEG}(P(\vec{x}))$	negation	590
$\text{DSJ}(P(\vec{x}), Q(\vec{y}))$	disjunction	590
$\text{IMP}(P(\vec{x}), Q(\vec{y}))$	implication	590
$(\exists y \leq z)P(\vec{x}, z, y)$	exists less than or equal to	590
$(\exists y < z)P(\vec{x}, z, y)$	exists less than	591
$(\forall z \leq y)P(\vec{x}, z)$	all less than or equal to	591
$(\forall z < y)P(\vec{x}, z)$	all less than	591
$(\mu y \leq z)P(\vec{x}, z, y)$	bounded minimization	591
$f(\vec{x})/C_0 \ldots C_k$	definition by cases	592
$\text{FCTR}(m, n)$	factor	592
$\text{PRIME}(n)$	prime	593
pi(n)	prime sequence	593
exp(n, i)	prime exponent	593
len(n)	prime length	594
rm(m, n)	remainder	595
qt(m, n)	quotient	595
cncat(m, n)	concatenation	597
$\text{VAR}(n)$	variable	598
$\text{TERMSEQ}(m, n)$	term sequence	598
$\text{TERM}(n)$	term	599
$\text{ATOMIC}(n)$	atomic formula	599
$\text{WFF}(n)$	well-formed formula	599
$\text{FORMSEQ}(m, n)$	formula sequence	599

PRFADS(m, n)	sentential proof	600
AXIOMADS(n)	sentential axiom	600
cnd(n, o)	conditional	600
neg(n)	negation	600
unv(v, n)	universal	600
MP(m, n, o)	recursive modus ponens	600
TSUBSEQ(m, n, t, v, s, u)	substitution sequence for terms	602
TERMSUB(t, v, s, u)	substitution in terms	602
ATOMSUB(p, v, s, q)	substitution in atomics	603
FSUBSEQ(m, n, p, v, s, q)	substitution sequence for formulas	603
FORMSUB(p, v, s, q)	substitution in formulas	603
formusb(p, v, s)	formsub (function)	603
FREEt(t, v)	free in term	604
FREEf(p, v)	free in formula	604
SENT(n)	sentence	604
FREEFOR(s, v, u)	free for	604
FFSEQ(m, s, v, u)	free for sequence	604
AXIOMAD4(n)	axiom 4	605
AXIOMAD5(n)	axiom 5	605
GEN(m, n)	gen rule	605
AXIOMAD6(n)	axiom 6	605
AXIOMAD7(n)	axiom 7	605
ICON(m, n, o)	immediate consequence	606
AXIOMPA7(n)	PA axiom 7	606
AXIOMAD(n)	axiom of AD	606
PRFAD(m, n)	proof in AD	606
AXIOMQ(n)	axiom of Q	606
PRFQ(m, n)	proof in Q	606
AXIOMQP(n)	axiom of Q less Q7	606
AXIOMPA(n)	axiom of PA	606
PRFPA(m, n)	proof in PA	606
num(n)	number of numeral for value of n	610
	chapter 13	
$f(\vec{x}, \vec{y}, \vec{z})$	composition	640
$\mu v \mathcal{Q}(\vec{x}, v)$	minimization	641
$(\mu y \leq z)\mathcal{Q}(\vec{x}, z, y)$	*bounded minimization*	641
rm	remainder	644

qt	quotient	645
β	beta function	645
$\mathit{suc}(x)$	defined successor	646
$\mathit{zero}(x)$	defined zero	646
$\mathit{idnt}_k^j(x_1 \ldots x_j)$	defined identity function	646
$\dot{-}$	dot minus	653
$\mid$	Factor	654
Pr	*Prime*	656
Rp	*Rprime*	656
G	*Good*	656
d	least good	656
lcm	*lcm*	659
plm	*plm*	659
maxp	*maxp*	662
maxs	*maxs*	662
$h(i)$	$h(i)$	664
CF	coordinate functions	671
CR	coordinate relations	672
pred	*pred*	674
sg	*sg*	674
csg	*csg*	674
ex	*ex*	682
$exc(m, n, i)$	exc	684
$val(n, i)$	val	685
$val^*(m, n, i)$	val*	685
gvar(n)	number of variable *n*	704
$numseq(n)$	numseq	704
$\Sigma^\star$	Sigma Star Formulas	707
LR	Löb Rule	728
	chapter 14	
CT	Church's thesis	753
LR	Language for recursion	759
IR	Interpretation of recursive language	759
AC	Algorithmic computability	764
MKU	MKU Machine	765

Quick Reference Guides

Negation and Quantity 21
Countability 36
Parts of a Formula 40
More on Countability 50
Grammar Quick Reference 64
AD Quick Reference 89
Peano Arithmetic (AD) 97
Semantics Quick Reference (Sentential) 114
Basic Notions of Set Theory 117
Semantics Quick Reference (quantificational) 138
Definitions for Translation 147
Cause and Conditional 167
Definitions for Auxiliary Assumptions 219
ND Quick Reference (Sentential) 241
ND Quick Reference (Quantificational) 303
$\mathscr{L}_{NT}$ reference 307
Robinson and Peano Arithmetic (ND) 318
ND+ Quick Reference 327
Metalinguistic Quick Reference (sentential) 350
Metalinguistic Quick Reference (quantificational) 372
Theorems of Chapter 7 378
Induction Schemes 388
First Theorems of Chapter 8 410
Final Theorems of Chapter 8 425
Theorems of Chapter 9 465
Some Arithmetic Relevant to Gödel Numbering 480
More Arithmetic Relevant to Gödel Numbering 492
Theorems of Chapter 10 516

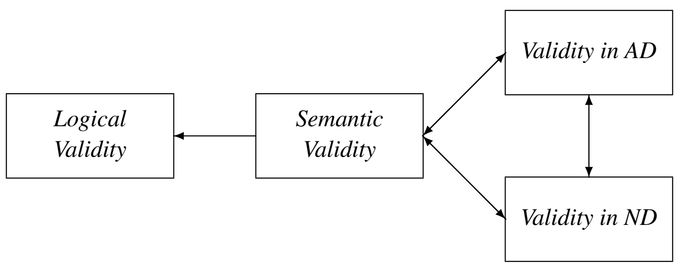
The Recursion Theorem 556
Arithmetic for the *Beta* Function 567
First Results of Chapter 12 608
Final Results of Chapter 12 617
Additional Theorems of PA 632
First theorems of chapter 13 650
Font conventions 669
Second theorems of chapter 13 701
Final theorems of chapter 13 731
Simple Time Dilation 757
Theorems of chapter 14 770

Part III

Classical Metalogic: Soundness and Adequacy

Introductory

In Part I we introduced four notions of validity. In this part, we set out to show that they are interrelated as follows.



An argument is semantically valid iff it is valid in the derivation systems. So the three formal notions apply to exactly the same arguments. And if an argument is semantically valid, then it is logically valid. So any of the formal notions imply logical validity for a corresponding ordinary argument.

More carefully, in Part I, we introduced four main notions of validity. There are logical validity from chapter 1, semantic validity from chapter 4, and syntactic validity in the derivation systems *AD*, from chapter 3 and *ND* from chapter 6. We turn in this part to the task of thinking *about* these notions, and especially about how they are related. The primary result is that $\Gamma \vDash \mathscr{P}$ iff $\Gamma \vdash_{AD} \mathscr{P}$ iff $\Gamma \vdash_{ND} \mathscr{P}$ (iff $\Gamma \vdash_{ND+} \mathscr{P}$). Thus our different formal notions of validity are met by just the same arguments, and the derivation systems — themselves defined in terms of *form* are "faithful" to the semantic notion: what is derivable is neither more nor less than what is semantically valid. And this is just right: If what is derivable were more than what is semantically valid, derivations could lead us from true premises to false conclusions; if it were less, not all semantically valid arguments could be identified as such by derivations. That the derivable is no *more* than what is semantically valid, is known as *soundness* of a derivation system; that it is no *less* is *adequacy*. In addition, we show that if an argument is semantically valid, then a corresponding ordinary argument is *logically valid*. Given the equivalence between the formal notions of validity, it follows that if an argument is valid in any of the formal senses, then it is logically valid. This connects the formal machinery to the notion of validity with which we began.[2]

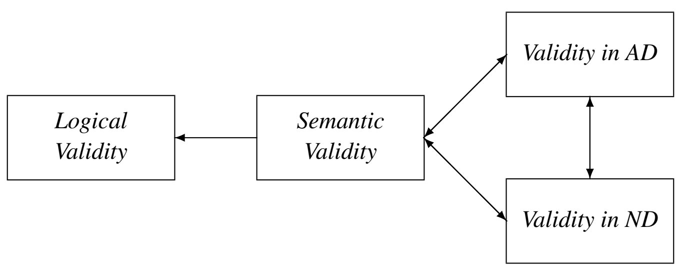
We begin in chapter 9 showing that just the same arguments are valid in the derivation systems *ND* and *AD*. This puts us in a position to demonstrate in chapter 10 the core result that the derivation systems are both sound and adequate. Chapter chapter 11 fills out this core picture in different directions.

[2]*Adequacy* is commonly described as *completeness*. However, this only invites confusion with theory completeness as described in Part IV.

Chapter 9

Preliminary Results

We have said that the aim of this part is to establish the following relations: An argument is semantically valid iff it is valid in *AD*; iff it is valid in *ND*; and if an argument is semantically valid, then it is logically valid.



In this chapter, we begin to develop these relations, taking up some of the simpler cases. We consider the leftmost horizontal arrow, and the rightmost vertical ones. Thus we show that quantificational (semantic) validity implies logical validity, that validity in *AD* implies validity in *ND*, and that validity in *ND* implies validity in *AD* (and similarly for *ND*+). Implications between semantic validity and the syntactical notions will wait for chapter 10.

9.1 Semantic Validity Implies Logical Validity

Logical validity is defined for arguments in ordinary language. From LV, an argument is logically valid iff there is no consistent *story* in which all the premises are true and the conclusion is false. Quantificational validity is defined for arguments in a formal language. From QV, an argument is quantificationally valid iff there is no *interpretation* on which all the premises are true and the conclusion is not. So our task is to show how facts about formal expressions and interpretations connect with ordinary expressions and stories. In particular, where $\mathcal{P}_1 \dots \mathcal{P}_n / \mathcal{Q}$ is an ordinary-language argument, and $\mathcal{P}'_1 \dots \mathcal{P}'_n$, $\mathcal{Q}'$ are the formulas of a good translation, we show that if $\mathcal{P}'_1 \dots \mathcal{P}'_n \vDash \mathcal{Q}'_1$, then the ordinary argument $\mathcal{P}_1 \dots \mathcal{P}_n / \mathcal{Q}$ is logically valid. The reasoning itself is straightforward. We will spend a bit more time discussing the result.

Recall our criterion of goodness for translation CG from chapter 5 (p. 141). When we identify an interpretation function II (sentential or quantificational), we thereby identify an *intended interpretation* II_ω corresponding to any way ω that the world can be. For example, corresponding to the interpretation function,

II B: Bill is happy
H: Hill is happy

$\mathsf{II}_\omega[B] = \mathsf{T}$ just in case Bill is happy at ω, and similarly for H. Given this, a formal translation $\mathcal{A}'$ of some ordinary $\mathcal{A}$ is *good* only if at any ω, $\mathsf{II}_\omega[\mathcal{A}']$ has the same truth value as $\mathcal{A}$ at ω. Given this, we can show,

T9.1. For any ordinary argument $\mathcal{P}_1 \dots \mathcal{P}_n / \mathcal{Q}$, with good translation consisting of II and $\mathcal{P}'_1 \dots \mathcal{P}'_n$, $\mathcal{Q}'$, if $\mathcal{P}'_1 \dots \mathcal{P}'_n \vDash \mathcal{Q}'$, then $\mathcal{P}_1 \dots \mathcal{P}_n / \mathcal{Q}$ is logically valid.

Suppose $\mathcal{P}'_1 \dots \mathcal{P}'_n \vDash \mathcal{Q}'$ but $\mathcal{P}_1 \dots \mathcal{P}_n / \mathcal{Q}$ is not logically valid. From the latter, by LV, there is some consistent story where each of $\mathcal{P}_1 \dots \mathcal{P}_n$ is true but $\mathcal{Q}$ is false. Since $\mathcal{P}_1 \dots \mathcal{P}_n$ are true at ω, by CG, $\mathsf{II}_\omega[\mathcal{P}'_1] = \mathsf{T}$, and ... and $\mathsf{II}_\omega[\mathcal{P}'_n] = \mathsf{T}$. And since ω is consistent with $\mathcal{Q}$ false at ω, $\mathcal{Q}$ is not both true and false at ω; so $\mathcal{Q}$ is not true at ω; so by by CG, $\mathsf{II}_\omega[\mathcal{Q}'_1] \neq \mathsf{T}$. So there is an I that that makes each of $\mathsf{I}[\mathcal{P}'_1] = \mathsf{T}$, and ... and $\mathsf{I}[\mathcal{P}'_n] = \mathsf{T}$ and $\mathsf{I}[\mathcal{Q}'] \neq \mathsf{T}$; so by QV, $\mathcal{P}'_1 \dots \mathcal{P}'_n \nvDash \mathcal{Q}'$. This is impossible; reject the assumption: if $\mathcal{P}'_1 \dots \mathcal{P}'_n \vDash \mathcal{Q}'$ then $\mathcal{P}_1 \dots \mathcal{P}_n / \mathcal{Q}$ is logically valid.

It is that easy. If there is no interpretation where $\mathcal{P}'_1 \dots \mathcal{P}'_n$ are true but $\mathcal{Q}'$ is not, then there is no *intended* interpretation where $\mathcal{P}'_1 \dots \mathcal{P}'_n$ are true but $\mathcal{Q}'$ is not; so, by CG, there is no consistent story where the premises are true and the conclusion is not; so $\mathcal{P}_1 \dots \mathcal{P}_n / \mathcal{Q}$, is logically valid. So if $\mathcal{P}'_1 \dots \mathcal{P}'_n \vDash \mathcal{Q}'$ then $\mathcal{P}_1 \dots \mathcal{P}_n / \mathcal{Q}$ is logically valid.

Let us make a couple of observations: First, CG is stronger than is actually required for our application of semantic to logical validity. CG requires a biconditional for good translation.

$$\omega \quad \rightleftarrows \quad \mathsf{I}_\omega$$

$\mathcal{A}$ is true at ω iff $\mathsf{I}_\omega[\mathcal{A}'] = \mathsf{T}$. But our reasoning applies to premises just the left-to-right portion of this condition: if $\mathcal{P}$ is true at ω then $\mathsf{I}_\omega[\mathcal{P}'] = \mathsf{T}$. And for the conclusion, the reasoning goes in the opposite direction: if $\mathsf{I}_\omega[\mathcal{Q}'] = \mathsf{T}$ then $\mathcal{Q}$ is true at ω (so that if the consequent fails at ω, then the antecedent fails at I_ω). The biconditional from CG guarantees both. But, strictly, for premises, all we need is that truth of an ordinary expression at a story guarantees truth for the corresponding formal one at the intended interpretation. And for a conclusion, all we need is that truth of the formal expression on the intended interpretation guarantees truth of the corresponding ordinary expression at the story.

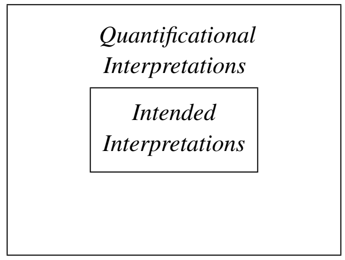
Thus we might use our methods to identify logical validity even where translations are less than completely good. Consider, for example, the following argument.

(A) Bob took a shower and got dressed
―――――
Bob took a shower

As discussed in chapter 5 (p. 160), where I gives S the same value as "Bob took a shower" and D the same as "Bob got dressed," we might agree that there are cases where $\mathsf{I}_\omega[S \wedge D] = \mathsf{T}$ but "Bob took a shower and got dressed" is false. So we might agree that the right-to-left conditional is false, and the translation is not good.

However, even if this is so, given our interpretation function, there is no situation where "Bob took a shower and got dressed" is true but $S \wedge D$ is F at the corresponding intended interpretation. So the left-to-right conditional is sustained. So, even if the translation is not good by CG, it remains possible to use our methods to demonstrate logical validity. Since it remains that if the ordinary premise is true at a story, then the formal expression is true at the corresponding intended interpretation, semantic validity implies logical validity. A similar point applies to conclusions. Of course, we already knew that this argument is logically valid. But the point applies to more complex arguments as well.

Second, observe that our reasoning does not work in reverse. It might be that $\mathcal{P}_1 \dots \mathcal{P}_n / \mathcal{Q}$ is logically valid, even though $\mathcal{P}'_1 \dots \mathcal{P}'_n \not\models \mathcal{Q}'$. Finding a quantificational interpretation where $\mathcal{P}'_1 \dots \mathcal{P}'_n$ are true and $\mathcal{Q}'$ is not shows that $\mathcal{P}'_1 \dots \mathcal{P}'_n \not\models \mathcal{Q}'$. However it does not show that $\mathcal{P}_1 \dots \mathcal{P}_n / \mathcal{Q}$ is not logically valid. Here is why: There may be quantificational interpretations which do not correspond to any consistent story. The situation is like this:



Intended interpretations correspond to stories. If no interpretation whatsoever has the premises true and the conclusion not, then no intended interpretation has the premises true and conclusion not, so no consistent story makes the premises true and the conclusion not. But it may be that some (unintended) interpretation makes the premises true and conclusion false, even though no intended interpretation is that way. Thus, if we were to attempt to run the above reasoning in reverse, a move from the assumption that $\mathcal{P}'_1 \dots \mathcal{P}'_n \not\models \mathcal{Q}'$, to the conclusion that there is a consistent story where $\mathcal{P}_1 \dots \mathcal{P}_n$ are true but $\mathcal{Q}$ is not, would fail.

It is easy to see why there might be unintended interpretations. Consider, first, this standard argument.

(B)
All humans are mortal
Socrates is human
———
Socrates is mortal

It is logically valid. But consider what happens when we translate into a *sentential* language. We might try an interpretation function as follows.

A: All humans are mortal

H: Socrates is human

M: Socrates is mortal

with translation, A, H / M. But, of course, there is a row of the truth table on which A and H are T and M is F. So the argument is not sententially valid. This interpretation is unintended in the sense that it corresponds to no consistent story whatsoever. Sentential languages are sufficient to identify validity when validity results from truth functional structure; but this argument is not valid because of truth functional structure.

We are in a position to expose its validity only in the quantificational case. Thus we might have,

s: Socrates

H^1: {o | o is human}

M^1: {o | o is mortal}

with translation $\forall x(Hx \to Mx)$, Hs/Ms. The argument is quantificationally valid. And, as above, it follows that the ordinary one is logically valid.

But related problems may arise even for quantificational languages. Thus, consider,

(C) Socrates is necessarily human
Socrates is human

Again, the argument is logically valid. But now we end up with something like an additional relation symbol N^1 for {o | o is necessarily human}, and translation Ns/Hs. And this is not quantificationally valid. Consider, for example, an interpretation with $\mathsf{U} = \{1\}$, $\mathsf{I}[s] = 1$, $\mathsf{I}[N] = \{1\}$, and $\mathsf{I}[H] = \{\}$. Then the premise is true, but the conclusion is not. Again, the interpretation corresponds to no consistent story. And, again, the argument includes structure that our quantificational language fails to capture. As it turns out, *modal* logic is precisely an attempt to work with structure introduced by notions of possibility and necessity. Where '$\Box$' represents necessity, this argument, with translation $\Box Hs/Hs$ is valid on standard modal systems.

The upshot of this discussion is that our methods are adequate when they work to identify validity. When an argument is semantically valid, we can be sure that it is logically valid. But we are not in a position to identify all the arguments that are logically valid. Thus quantificational invalidity does not imply logical invalidity. We should not be discouraged by this or somehow put off the logical project. Rather, we have a rationale for *expanding* the logical project! In Part I, we set up formal logic as a "tool" or "machine" to identify logical validity. Beginning with the notion of logical validity, we introduce our formal languages, learn to translate into them, and to manipulate arguments by semantical and syntactical methods. The sentential notions have some utility. But when it turns out that sentential languages miss important structure, we expand the language to include quantificational structure, developing the semantical and syntactical methods to match. And similarly, if our quantificational languages should turn out to miss important structure, we expand the language to capture that structure, and further develop the semantical and syntactical methods. As it happens, the classical quantificational logic we have so far seen is sufficient to identify validity in a wide variety of contexts — and, in particular, for arguments in mathematics. Also, controversy may be introduced as one expands beyond the classical quantificational level. So the logical project is a live one. But let us return to the kinds of validity we have already seen.

E9.1. (i) Recast the above reasoning to show directly a corollary to T9.1: If $\vDash \mathcal{Q}'$, then $\mathcal{Q}$ is necessarily true (that is, true in any consistent story). (ii) Suppose $\nvDash \mathcal{Q}'$; does it follow that $\mathcal{Q}$ is not necessary (that is, not true in some consistent story)? Explain.

9.2 Validity in *AD* Implies Validity in *ND*

It is easy to see that if $\Gamma \vdash_{AD} \mathcal{P}$, then $\Gamma \vdash_{ND} \mathcal{P}$. Roughly, anything we can accomplish in *AD*, we can accomplish in *ND* as well. If a premise appears in an *AD* derivation, that same premise can be used in *ND*. If an axiom appears in an *AD* derivation, that axiom can be derived in *ND*. And if a line is justified by MP or Gen in *AD*, that same line may be justified by rules of *ND*. So anything that can be derived in *AD* can be derived in *ND*. Officially, this reasoning is by induction on the line numbers of an *AD* derivation, and it is appropriate to work out the details more formally. The argument by mathematical induction is longer than anything we have seen so far, but the reasoning is straightforward.

T9.2. If $\Gamma \vdash_{AD} \mathcal{P}$, then $\Gamma \vdash_{ND} \mathcal{P}$.

Suppose $\Gamma \vdash_{AD} \mathcal{P}$. Then there is an *AD* derivation $A = \langle \mathcal{Q}_1 \dots \mathcal{Q}_n \rangle$ of $\mathcal{P}$ from premises in Γ, with $\mathcal{Q}_n = \mathcal{P}$. We show that there is a corresponding *ND* derivation N, such that if $\mathcal{Q}_i$ appears on line i of A, then $\mathcal{Q}_i$ appears, under the scope of the premises alone, on the line numbered 'i' of N. It follows that $\Gamma \vdash_{ND} \mathcal{P}$. For any *premises* $\mathcal{Q}_a$, $\mathcal{Q}_b$,... $\mathcal{Q}_j$ in A, let N begin,

0.a	$\mathcal{Q}_a$	P
0.b	$\mathcal{Q}_b$	P
⋮		
0.j	$\mathcal{Q}_j$	P

Now we reason by induction on the line numbers in A. The general plan is to *construct* a derivation N which accomplishes just what is accomplished in A. Fractional line numbers, as above, maintain the parallel between the two derivations.

Basis: $\mathcal{Q}_1$ in A is a premise or an instance of A1, A2, A3, A4, A5, A6, A7 or A8.

(prem) If $\mathcal{Q}_1$ is a premise $\mathcal{Q}_i$, continue N as follows,

0.a	$\mathcal{Q}_a$	P
0.b	$\mathcal{Q}_b$	P
$\vdots$		
0.j	$\mathcal{Q}_j$	P
1	$\mathcal{Q}_i$	0.i R

So $\mathcal{Q}_1$ appears, under the scope of the premises alone, on the line numbered '1' of N.

(A1) If $\mathcal{Q}_1$ is an instance of A1, then it is of the form, $\mathcal{B} \to (\mathcal{C} \to \mathcal{B})$, and we continue N as follows,

0.a	$\mathcal{Q}_a$	P
0.b	$\mathcal{Q}_b$	P
$\vdots$		
0.j	$\mathcal{Q}_j$	P
1.1	$\quad \mathcal{B}$	A (g, $\to$I)
1.2	$\qquad \mathcal{C}$	A (g, $\to$I)
1.3	$\qquad \mathcal{B}$	1.1 R
1.4	$\quad \mathcal{C} \to \mathcal{B}$	1.2-1.3 $\to$I
1	$\mathcal{B} \to (\mathcal{C} \to \mathcal{B})$	1.1-1.4 $\to$I

So $\mathcal{Q}_1$ appears, under the scope of the premises alone, on the line numbered '1' of N.

(A2) If $\mathcal{Q}_1$ is an instance of A2, then it is of the form, $(\mathcal{B} \to (\mathcal{C} \to \mathcal{D})) \to ((\mathcal{B} \to \mathcal{C}) \to (\mathcal{B} \to \mathcal{D}))$ and we continue N as follows,

0.a	$\mathcal{Q}_a$	P
0.b	$\mathcal{Q}_b$	P
⋮		
0.j	$\mathcal{Q}_j$	P
1.1	$\mathcal{B} \to (\mathcal{C} \to \mathcal{D})$	A (g, →I)
1.2	$\mathcal{B} \to \mathcal{C}$	A (g, →I)
1.3	$\mathcal{B}$	A (g, →I)
1.4	$\mathcal{C}$	1.2,1.3 →E
1.5	$\mathcal{C} \to \mathcal{D}$	1.1,1.3 →E
1.6	$\mathcal{D}$	1.5,1.4 →E
1.7	$\mathcal{B} \to \mathcal{D}$	1.3-1.6 →I
1.8	$(\mathcal{B} \to \mathcal{C}) \to (\mathcal{B} \to \mathcal{D})$	1.2-1.7 →I
1	$(\mathcal{B} \to (\mathcal{C} \to \mathcal{D})) \to ((\mathcal{B} \to \mathcal{C}) \to (\mathcal{B} \to \mathcal{D}))$	1.1-1.8 →I

So $\mathcal{Q}_1$ appears, under the scope of the premises alone, on the line numbered '1' of N.

(A3) Homework.

(A4) If $\mathcal{Q}_1$ is an instance of A4, then it is of the form $\forall x\mathcal{B} \to B^x_t$ for some variable x and term t that is free for x in $\mathcal{B}$, and we continue N as follows,

0.a	$\mathcal{Q}_a$	P
0.b	$\mathcal{Q}_b$	P
⋮		
0.j	$\mathcal{Q}_j$	P
1.1	$\forall x\mathcal{B}$	A (g, →I)
1.2	$\mathcal{B}^x_t$	1.1 ∀E
1	$\forall x\mathcal{B} \to \mathcal{B}^x_t$	1.1-1.2 →I

Since we are given that t is free for x in $\mathcal{B}$, the parallel requirement on ∀E is met at line 1.2. So $\mathcal{Q}_1$ appears, under the scope of the premises alone, on the line numbered '1' of N.

(A5) Homework.

(A6) Homework.

(A7) If $\mathcal{Q}_1$ is an instance of A7, then it is of the form $(x_i = y) \to (h^n x_1 \ldots x_i \ldots x_n = h^n x_1 \ldots y \ldots x_n)$ for some variables $x_1 \ldots x_n$ and y and function symbol h^n; and we continue N as follows,

$$
\begin{array}{r|l l}
0.\text{a} & \mathcal{Q}_a & \text{P} \\
0.\text{b} & \mathcal{Q}_b & \text{P} \\
\vdots & & \\
0.\text{j} & \mathcal{Q}_j & \text{P} \\
1.1 & \quad x_i = y & \text{A } (g, \to\text{I}) \\
1.2 & \quad h^n x_1 \ldots x_i \ldots x_n = h^n x_1 \ldots x_i \ldots x_n & =\text{I} \\
1.3 & \quad h^n x_1 \ldots x_i \ldots x_n = h^n x_1 \ldots y \ldots x_n & 1.2,1.1 \; =\text{E} \\
1 & (x_i = y) \to (h^n x_1 \ldots x_i \ldots x_n = h^n x_1 \ldots y \ldots x_n) & 1.1\text{-}1.3 \; \to\text{I}
\end{array}
$$

So $\mathcal{Q}_1$ appears, under the scope of the premises alone, on the line numbered '1' of N.

(A8) Homework.

Assp: For any i, $1 \leq i < k$, if $\mathcal{Q}_i$ appears on line i of A, then $\mathcal{Q}_i$ appears, under the scope of the premises alone, on the line numbered 'i' of N.

Show: If $\mathcal{Q}_k$ appears on line k of A, then $\mathcal{Q}_k$ appears, under the scope of the premises alone, on the line numbered 'k' of N.

$\mathcal{Q}_k$ in A is a premise, an axiom, or arises from previous lines by MP or Gen. If $\mathcal{Q}_k$ is a premise or an axiom then, by reasoning as in the basis (with line numbers adjusted to $k.n$) if $\mathcal{Q}_k$ appears on line k of A, then $\mathcal{Q}_k$ appears, under the scope of the premises alone, on the line numbered 'k' of A. So suppose $\mathcal{Q}_k$ arises by MP or Gen.

(MP) If $\mathcal{Q}_k$ arises from previous lines by MP, then A is as follows,

$$
\begin{array}{r l l}
i & \mathcal{B} & \\
 & \vdots & \\
j & \mathcal{B} \to \mathcal{C} & \\
 & \vdots & \\
k & \mathcal{C} & i, j \text{ MP}
\end{array}
$$

where $i, j < k$ and $\mathcal{Q}_k$ is $\mathcal{C}$. By assumption, then, there are lines in N,

$$
\begin{array}{r|l}
i & \mathcal{B} \\
 & \vdots \\
j & \mathcal{B} \to \mathcal{C}
\end{array}
$$

So we simply continue derivation N,

$$\begin{array}{l|ll} i & \mathcal{B} & \\ & \vdots & \\ j & \mathcal{B} \to \mathcal{C} & \\ & \vdots & \\ k & \mathcal{C} & i, j \to\text{E} \end{array}$$

So $\mathcal{Q}_k$ appears under the scope of the premises alone, on the line numbered 'k' of N.

(Gen) If $\mathcal{Q}_k$ arises from previous lines by Gen, then A is as follows,

$$\begin{array}{lll} i & \mathcal{B} & \\ & \vdots & \\ k & \forall x\mathcal{B} & i \text{ Gen} \end{array}$$

where $i < k$, and $\mathcal{Q}_k$ is $\forall x\mathcal{B}$. By assumption N has a line i,

$$\begin{array}{l|l} & \vdots \\ i & \mathcal{B} \\ & \vdots \end{array}$$

under the scope of the premises alone. So we continue N as follows,

$$\begin{array}{l|ll} i & \mathcal{B} & \\ & \vdots & \\ k & \forall x\mathcal{B} & i\ \forall\text{I} \end{array}$$

Since i is under the scope of the premises alone, x is not free in an undischarged assumption. Further, since there is no change of variables, we can be sure that x is free for every free instance of x in $\mathcal{B}$, and that x is not free in $\forall x\mathcal{B}$. So the restrictions are met on ∀I. So $\mathcal{Q}_k$ appears under the scope of the premises alone, on the line numbered 'k' of N.

In any case then, $\mathcal{Q}_k$ appears under the scope of the premises alone, on the line numbered 'k' of N.

Indct: For any line j of A, $\mathcal{Q}_j$ appears under the scope of the premises alone, on the line numbered 'j' of N.

So $\Gamma \vdash_{ND} \mathcal{Q}_n$, where this is just to say $\Gamma \vdash_{ND} \mathcal{P}$. So T9.2, if $\Gamma \vdash_{AD} \mathcal{P}$, then $\Gamma \vdash_{ND} \mathcal{P}$. Notice the way we use line numbers, $i.1, i.2, \ldots i.n, i$ in N to make good on the claim that for each $\mathcal{Q}_i$ in A, $\mathcal{Q}_i$ appears on the line numbered 'i' of N — where the line numbered 'i' may or may not be the ith line of N. We need this parallel between the line numbers when it comes to cases for MP and Gen. With the parallel, we are in a position to make use of line numbers from justifications in derivation A, directly in the specification of derivation N.

Given an *AD* derivation, what we have done shows that there exists an *ND* derivation, by showing how to construct it. We can see into how this works, by considering an application. Thus, for example, consider the derivation of T3.2 on p. 75.

(D)

1.	$\mathcal{B} \to \mathcal{C}$	prem
2.	$(\mathcal{B} \to \mathcal{C}) \to [\mathcal{A} \to (\mathcal{B} \to \mathcal{C})]$	A1
3.	$\mathcal{A} \to (\mathcal{B} \to \mathcal{C})$	1,2 MP
4.	$[\mathcal{A} \to (\mathcal{B} \to \mathcal{C})] \to [(\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to \mathcal{C})]$	A2
5.	$(\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to \mathcal{C})$	3,4 MP
6.	$\mathcal{A} \to \mathcal{B}$	prem
7.	$\mathcal{A} \to \mathcal{C}$	5,6 MP

Let this be derivation A; we will follow the method of our induction to construct a corresponding *ND* derivation N. The first step is to list the premises.

0.1	$\mathcal{B} \to \mathcal{C}$	P
0.2	$\mathcal{A} \to \mathcal{B}$	P

Now to the induction itself. The first line of A is a premise. Looking back to the basis case of the induction, we see that we are instructed to produce the line numbered '1' by reiteration. So that is what we do.

0.1	$\mathcal{B} \to \mathcal{C}$	P
0.2	$\mathcal{A} \to \mathcal{B}$	P
1	$\mathcal{B} \to \mathcal{C}$	0.1 R

This may strike you as somewhat pointless! But, again, we need $\mathcal{B} \to \mathcal{C}$ on the line numbered '1' in order to maintain the parallel between the derivations. So our recipe requires this simple step.

Line 2 of A is an instance of A1, and the induction therefore tells us to get it "by reasoning as in the basis." Looking then to the case for A1 in the basis, we continue on that pattern as follows,

0.1	$\mathcal{B} \to \mathcal{C}$	P
0.2	$\mathcal{A} \to \mathcal{B}$	P
1	$\mathcal{B} \to \mathcal{C}$	0.1 R
2.1	| $\mathcal{B} \to \mathcal{C}$	A (g, $\to$I)
2.2	| | $\mathcal{A}$	A (g, $\to$I)
2.3	| | $\mathcal{B} \to \mathcal{C}$	2.1 R
2.4	| $\mathcal{A} \to (\mathcal{B} \to \mathcal{C})$	2.2-2.3 $\to$I
2	$(\mathcal{B} \to \mathcal{C}) \to (\mathcal{A} \to (\mathcal{B} \to \mathcal{C}))$	2.1-2.4 $\to$I

Notice that this reasoning for the show step now applies to line 2, so that the line numbers are 2.1, 2.2, 2.3, 2.4, 2 instead of 1.1, 1.2, 1.3, 1.4, 1 as for the basis. Also, what we have added follows *exactly* the pattern from the recipe in the induction, given the relevant instance of A1.

Line 3 is justified by 1,2 MP. Again, by the recipe from the induction, we continue,

0.1	$\mathcal{B} \to \mathcal{C}$	P
0.2	$\mathcal{A} \to \mathcal{B}$	P
1	$\mathcal{B} \to \mathcal{C}$	0.1 R
2.1	$\quad\mid \mathcal{B} \to \mathcal{C}$	A (g, →I)
2.2	$\quad\mid\quad\mid \mathcal{A}$	A (g, →I)
2.3	$\quad\mid\quad\mid \mathcal{B} \to \mathcal{C}$	2.1 R
2.4	$\quad\mid \mathcal{A} \to (\mathcal{B} \to \mathcal{C})$	2.2-2.3 →I
2	$(\mathcal{B} \to \mathcal{C}) \to (\mathcal{A} \to (\mathcal{B} \to \mathcal{C}))$	2.1-2.4 →I
3	$\mathcal{A} \to (\mathcal{B} \to \mathcal{C})$	1,2 →E

Notice that the line numbers of the justification are identical to those in the justification from A. And similarly, we are in a position to generate each line in A. Thus, for example, line 4 of A is an instance of A2. So we would continue with lines 4.1-4.8 and 4 to generate the appropriate instance of A2. And so forth. As it turns out, the resultant *ND* derivation is not very efficient! But it is a derivation, and our point is merely to show that some *ND* derivation of the same result exists. So if $\Gamma \vdash_{AD} \mathcal{P}$, then $\Gamma \vdash_{ND} \mathcal{P}$.

*E9.2. Set up the above induction for T9.2, and complete the unfinished cases to show that if $\Gamma \vdash_{AD} \mathcal{P}$, then $\Gamma \vdash_{ND} \mathcal{P}$. For cases completed in the text, you may simply refer to the text, as the text refers cases to homework.

E9.3. (i) Where A is the derivation for T3.2, complete the process of finding the corresponding derivation N. Hint: if you follow the recipe correctly, the result should have exactly 21 lines. (ii) This derivation N is not very efficient! See if you can find an *ND* derivation to show $\mathcal{A} \to \mathcal{B}, \mathcal{B} \to \mathcal{C} \vdash_{ND} \mathcal{A} \to \mathcal{C}$ that takes fewer than 10 lines.

E9.4. Consider the axiomatic system *A3* as described for E8.12 on p. 398, and produce a complete demonstration that if $\Gamma \vdash_{A3} \mathcal{P}$, then $\Gamma \vdash_{ND} \mathcal{P}$.

9.3 Validity in *ND* Implies Validity in *AD*

Perhaps the result we have just attained is obvious: if $\Gamma \vdash_{AD} \mathcal{P}$, then of course $\Gamma \vdash_{ND} \mathcal{P}$. But the other direction may be less obvious. Insofar as *AD* may seem to have fewer resources than *ND*, one might wonder whether it is the case that if $\Gamma \vdash_{ND} \mathcal{P}$, then $\Gamma \vdash_{AD} \mathcal{P}$. But, in fact, it is possible to do in *AD* whatever can be done in *ND*. To show this, we need a couple of preliminary results. I begin with an important result known as the *deduction theorem*, turn to some substitution theorems, and finally to the intended result that whatever is provable in *ND* is provable in *AD*.

9.3.1 Deduction Theorem

According to the deduction theorem — subject to an important restriction — if there is an *AD* derivation of $\mathcal{Q}$ from the members of some set of sentences Δ plus $\mathcal{P}$, then there is an *AD* derivation of $\mathcal{P} \rightarrow \mathcal{Q}$ from the members of Δ alone: if $\Delta \cup \{\mathcal{P}\} \vdash_{AD} \mathcal{Q}$ then $\Delta \vdash_{AD} \mathcal{P} \rightarrow \mathcal{Q}$. In practice, this lets us reason just as we do with $\rightarrow$I.

(E)

	members of Δ	
a.	$\mathcal{P}$	
b.	$\mathcal{Q}$	
c.	$\mathcal{P} \rightarrow \mathcal{Q}$	a-b deduction theorem

At (b), there is a derivation of $\mathcal{Q}$ from the mbembers of Δ plus $\mathcal{P}$. At (c), the assumption is discharged to indicate a derivation of $\mathcal{P} \rightarrow \mathcal{Q}$ from the members of Δ alone. By the deduction theorem, if there is a derivation of $\mathcal{Q}$ from Δ plus $\mathcal{P}$, then there is a derivation of $\mathcal{P} \rightarrow \mathcal{Q}$ from Δ alone. Here is the restriction: The discharge of an auxiliary assumption $\mathcal{P}$ is legitimate just in case no application of Gen under its scope generalizes on a variable free in $\mathcal{P}$. The effect is like that of the *ND* restriction on $\forall$I — here, though, the restriction is not on Gen, but rather on the discharge of auxiliary assumptions. In the one case, an assumption available for discharge is one such that no application of Gen under its scope is to a variable free in the assumption; in the other, we cannot apply $\forall$I to a variable free in an undischarged assumption (so that, effectively, every assumption is always available for discharge).

Again, our strategy is to show that given one derivation, it is possible to construct another. In this case, we begin with an *AD* derivation (A) as below, with premises $\Delta \cup \{\mathcal{P}\}$. Treating $\mathcal{P}$ as an auxiliary premise, with scope as indicated in (B), we set out to show that there is an *AD* derivation (C), with premises in Δ alone, and lines numbered '1', '2', . . . corresponding to 1, 2, . . . in (A).

(F)

(A)		(B)		(C)	
1.	$\mathscr{Q}_1$	1.	$\mathscr{Q}_1$	1.	$\mathscr{P} \to \mathscr{Q}_1$
2.	$\mathscr{Q}_2$	2.	$\mathscr{Q}_2$	2.	$\mathscr{P} \to \mathscr{Q}_2$
	$\vdots$		$\vdots$		$\vdots$
	$\mathscr{P}$		$\mid \underline{\mathscr{P}}$		$\mathscr{P} \to \mathscr{P}$
	$\vdots$		$\mid \vdots$		$\vdots$
n.	$\mathscr{Q}_n$	n.	$\mid \mathscr{Q}_n$	n.	$\mathscr{P} \to \mathscr{Q}_n$

That is, we construct a derivation with premises in Δ such that for any formula $\mathscr{A}$ on line i of the first derivation, $\mathscr{P} \to \mathscr{A}$ appears on the line numbered 'i' of the constructed derivation. The last line n of the resultant derivation is the desired result, $\Delta \vdash_{AD} \mathscr{P} \to \mathscr{Q}$.

T9.3. (*Deduction Theorem*) If $\Delta \cup \{\mathscr{P}\} \vdash_{AD} \mathscr{Q}$, and no application of Gen under the scope of $\mathscr{P}$ is to a variable free in $\mathscr{P}$, then $\Delta \vdash_{AD} \mathscr{P} \to \mathscr{Q}$.

Suppose $A = \langle \mathscr{Q}_1, \mathscr{Q}_2, \ldots \mathscr{Q}_n \rangle$ is an *AD* derivation of $\mathscr{Q}$ from $\Delta \cup \{\mathscr{P}\}$, where $\mathscr{Q}$ is $\mathscr{Q}_n$ and no application of Gen under the scope of $\mathscr{P}$ is to a variable free in $\mathscr{P}$. By induction on the line numbers in derivation A, we show there is a derivation C with premises only in Δ, such that for any line i of A, $\mathscr{P} \to \mathscr{Q}_i$ appears on the line numbered 'i' of C. The case when $i = n$ gives the desired result, that $\Delta \vdash_{AD} \mathscr{P} \to \mathscr{Q}$.

Basis: $\mathscr{Q}_1$ of A is an axiom, a member of Δ, or $\mathscr{P}$ itself.

(i) If $\mathscr{Q}_1$ is an axiom or a member of Δ, then begin C as follows,

1.1	$\mathscr{Q}_1$	axiom / premise
1.2	$\mathscr{Q}_1 \to (\mathscr{P} \to \mathscr{Q}_1)$	A1
1	$\mathscr{P} \to \mathscr{Q}_1$	1.1, 1.2 MP

(ii) $\mathscr{Q}_1$ is $\mathscr{P}$ itself. By T3.1, $\vdash_{AD} \mathscr{P} \to \mathscr{P}$; which is to say $\mathscr{P} \to \mathscr{Q}_1$; so begin derivation C,

1	$\mathscr{P} \to \mathscr{P}$	T3.1

In either case, $\mathscr{P} \to \mathscr{Q}_1$ appears on the line numberd '1' of C with premises in Δ alone.

Assp: For any i, $1 \le i < k$, $\mathscr{P} \to \mathscr{Q}_i$ appears on the line numbered 'i' of C, with premises in Δ alone.

Show: $\mathscr{P} \to \mathscr{Q}_k$ appears on the line numbered 'k' of C, with premises in Δ alone.

$\mathcal{Q}_k$ of A is a member of Δ, an axiom, $\mathcal{P}$ itself, or arises from previous lines by MP or Gen. If $\mathcal{Q}_k$ is a member of Δ, an axiom or $\mathcal{P}$ itself then, by reasoning as in the basis, $\mathcal{P} \to \mathcal{Q}_k$ appears on the line numbered 'k' of C from premises in Δ alone. So two cases remain.

(MP) If $\mathcal{Q}_k$ arises from previous lines by MP, then there are lines in derivation A of the sort,

i	$\mathcal{B}$	
	$\vdots$	
j	$\mathcal{B} \to \mathcal{C}$	
	$\vdots$	
k	$\mathcal{C}$	i,j MP

where $\text{i}, \text{j} < k$ and $\mathcal{Q}_k$ is $\mathcal{C}$. By assumption, there are lines in C,

i	$\mathcal{P} \to \mathcal{B}$
	$\vdots$
j	$\mathcal{P} \to (\mathcal{B} \to \mathcal{C})$

So continue derivation C as follows,

i	$\mathcal{P} \to \mathcal{B}$	
	$\vdots$	
j	$\mathcal{P} \to (\mathcal{B} \to \mathcal{C})$	
	$\vdots$	
k.1	$[\mathcal{P} \to (\mathcal{B} \to \mathcal{C})] \to [(\mathcal{P} \to \mathcal{B}) \to (\mathcal{P} \to \mathcal{C})]$	A2
k.2	$(\mathcal{P} \to \mathcal{B}) \to (\mathcal{P} \to \mathcal{C})$	j, k.1 MP
k	$\mathcal{P} \to \mathcal{C}$	i, k.2 MP

So $\mathcal{P} \to \mathcal{Q}_k$ appears on the line numbered 'k' of C, with premises in Δ alone.

(Gen) If $\mathcal{Q}_k$ arises from a previous line by Gen, then there are lines in derivation A of the sort,

i	$\mathcal{B}$
	$\vdots$
k	$\forall x \mathcal{B}$

where $\text{i} < \text{k}$ and $\mathcal{Q}_k$ is $\forall x \mathcal{B}$. Either line k is under the scope of $\mathcal{P}$ in derivation A or not.

(i) If line k is not under the scope of $\mathcal{P}$, then $\forall x \mathcal{B}$ in A follows from Δ alone. So continue C as follows,

k.1	$\mathcal{Q}_1$	exactly as in A but with prefix
k.2	$\mathcal{Q}_2$	'k.' for numeric references
	$\vdots$	
k.k	$\forall x \mathcal{B}$	
k.k+1	$\forall x \mathcal{B} \to (\mathcal{P} \to \forall x \mathcal{B})$	A1
k	$\mathcal{P} \to \forall x \mathcal{B}$	k.k+1, k.k MP

Since each of the lines in A up to k is derived from Δ alone, we have $\mathcal{P} \to \mathcal{Q}_k$ on the line numbered 'k' of C, from premises in Δ alone.

(ii) If line k is under the scope of $\mathcal{P}$, we depend on the assumption, and continue C as follows,

i	$\mathcal{P} \to \mathcal{B}$	(by inductive assumption)
	$\vdots$	
k	$\mathcal{P} \to \forall x \mathcal{B}$	i T3.28

If line k is under the scope of $\mathcal{P}$ then, since no application of Gen under the scope of $\mathcal{P}$ is to a variable free in $\mathcal{P}$, x is not free in $\mathcal{P}$; so k meets the restriction on T3.28. So we have $\mathcal{P} \to \mathcal{Q}_k$ on the line numbered 'k' of C, from premises in Δ alone.

Indct: For for any i, $\mathcal{P} \to \mathcal{Q}_k$ appears on the line numbered 'i' of C, from premises in Δ alone.

So given an *AD* derivation of $\mathcal{Q}$ from $\Delta \cup \{\mathcal{P}\}$, where no application of Gen under the scope of assumption $\mathcal{P}$ is to a variable free in $\mathcal{P}$, there is sure to be an *AD* derivation of $\mathcal{P} \to \mathcal{Q}$ from Δ alone. Notice that T3.28 and T3.30 abbreviate sequences which include applications of Gen. So the restriction on Gen for the deduction theorem applies to applications of these results as well.

As a sample application of the deduction theorem (DT), let us consider another derivation of T3.2. In tis case, $\Delta = \{\mathcal{A} \to \mathcal{B}, \mathcal{B} \to \mathcal{C}\}$, and we argue as follows,

(G)

1.	$\mathcal{A} \to \mathcal{B}$	prem
2.	$\mathcal{B} \to \mathcal{C}$	prem
3.	$\quad\mid \mathcal{A}$	assp (g, DT)
4.	$\quad\mid \mathcal{B}$	1,3 MP
5.	$\quad\mid \mathcal{C}$	2,4 MP
6.	$\mathcal{A} \to \mathcal{C}$	3-5 DT

At line (5) we have established that $\Delta \cup \{\mathcal{A}\} \vdash_{AD} \mathcal{C}$; it follows from the deduction theorem that $\Delta \vdash_{AD} \mathcal{A} \to \mathcal{C}$. But we should be careful: this is not an *AD* derivation of $\mathcal{A} \to \mathcal{C}$ from $\mathcal{A} \to \mathcal{B}$ and $\mathcal{B} \to \mathcal{C}$. And it is not an abbreviation in the sense that we have seen so far — we do not appeal to a result whose derivation could be inserted at that very stage. Rather, what we have is a demonstration, via the deduction theorem, that there *exists* an *AD* derivation of $\mathcal{A} \to \mathcal{C}$ from the premises. If there is any abbreviating, the entire derivation abbreviates, or indicates the existence of, another. Our proof of the deduction theorem shows us that, given a derivation of $\Delta \cup \{\mathcal{P}\} \vdash_{AD} \mathcal{Q}$, it is possible to *construct* a derivation for $\Delta \vdash_{AD} \mathcal{P} \to \mathcal{Q}$.

Let us see how this works in the example. Lines 1-5 become our derivation A, with $\Delta = \{\mathcal{A} \to \mathcal{B}, \mathcal{B} \to \mathcal{C}\}$. For each $\mathcal{Q}_i$ in derivation A, the induction tells us how to derive $\mathcal{A} \to \mathcal{Q}_i$ from Δ alone. Thus $\mathcal{Q}_i$ on the first line is a member of Δ: reasoning from the basis tells us to use A1 as follows,

1.1	$\mathcal{A} \to \mathcal{B}$	prem
1.2	$(\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to (\mathcal{A} \to \mathcal{B}))$	A1
1	$\mathcal{A} \to (\mathcal{A} \to \mathcal{B})$	1.2,1.1 MP

to get $\mathcal{A}$ arrow the form on line 1 of A. Notice that we are again using fractional line numbers to make lines in derivation A correspond to lines in the constructed derivation. One may wonder why we bother getting $\mathcal{A} \to \mathcal{Q}_1$. And again, the answer is that our "recipe" calls for this ingredient at stages connected to MP and Gen. Similarly, we can use A1 to get $\mathcal{A}$ arrow the form on line (2).

1.1	$\mathcal{A} \to \mathcal{B}$	prem
1.2	$(\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to (\mathcal{A} \to \mathcal{B}))$	A1
1	$\mathcal{A} \to (\mathcal{A} \to \mathcal{B})$	1.2,1.1 MP
2.1	$\mathcal{B} \to \mathcal{C}$	prem
2.2	$(\mathcal{B} \to \mathcal{C}) \to (\mathcal{A} \to (\mathcal{B} \to \mathcal{C}))$	A1
2	$\mathcal{A} \to (\mathcal{B} \to \mathcal{C})$	2.2,2.1 MP

The form on line (3) is $\mathcal{A}$ itself. If we wanted a derivation in the primitive system, we could repeat the steps in our derivation of T3.1. But we will simply continue, as in the induction,

1.1	$\mathcal{A} \to \mathcal{B}$	prem
1.2	$(\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to (\mathcal{A} \to \mathcal{B}))$	A1
1	$\mathcal{A} \to (\mathcal{A} \to \mathcal{B}$	1.2,1.2 MP
2.1	$\mathcal{B} \to \mathcal{C})$	prem
2.2	$(\mathcal{B} \to \mathcal{C}) \to (\mathcal{A} \to (\mathcal{B} \to \mathcal{C}))$	A1
2	$\mathcal{A} \to (\mathcal{B} \to \mathcal{C})$	2.2,2.1 MP
3	$\mathcal{A} \to \mathcal{A}$	T3.1

to get $\mathcal{A}$ arrow the form on line (3) of A. The form on line (4) arises from lines (1) and (3) by MP; reasoning in our show step tells us to continue,

1.1	$\mathcal{A} \to \mathcal{B}$	prem
1.2	$(\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to (\mathcal{A} \to \mathcal{B}))$	A1
1	$\mathcal{A} \to (\mathcal{A} \to \mathcal{B})$	1.2,1.1 MP
2.1	$\mathcal{B} \to \mathcal{C}$	prem
2.2	$(\mathcal{B} \to \mathcal{C}) \to (\mathcal{A} \to (\mathcal{B} \to \mathcal{C}))$	A1
2	$\mathcal{A} \to (\mathcal{B} \to \mathcal{C})$	2.2,2.1 MP
3	$\mathcal{A} \to \mathcal{A}$	T3.1
4.1	$(\mathcal{A} \to (\mathcal{A} \to \mathcal{B})) \to ((\mathcal{A} \to \mathcal{A}) \to (\mathcal{A} \to \mathcal{B}))$	A2
4.2	$(\mathcal{A} \to \mathcal{A}) \to (\mathcal{A} \to \mathcal{B})$	4.1,1 MP
4	$\mathcal{A} \to \mathcal{B}$	4.2,3 MP

using A2 to get $\mathcal{A} \to \mathcal{B}$. Notice that the original justification from lines (1) and (3) dictates the appeal to (1) at line (4.2) and to (3) at line (4). The form on line (5) arises from lines (2) and (4) by MP; so, finally, we continue,

1.1	$\mathcal{A} \to \mathcal{B}$	prem
1.2	$(\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to (\mathcal{A} \to \mathcal{B}))$	A1
1	$\mathcal{A} \to (\mathcal{A} \to \mathcal{B})$	1.2,1.1 MP
2.1	$\mathcal{B} \to \mathcal{C}$	prem
2.2	$(\mathcal{B} \to \mathcal{C}) \to (\mathcal{A} \to (\mathcal{B} \to \mathcal{C}))$	A1
2	$\mathcal{A} \to (\mathcal{B} \to \mathcal{C})$	2.2,2.1 MP
3	$\mathcal{A} \to \mathcal{A}$	T3.1
4.1	$(\mathcal{A} \to (\mathcal{A} \to \mathcal{B})) \to ((\mathcal{A} \to \mathcal{A}) \to (\mathcal{A} \to \mathcal{B}))$	A2
4.2	$(\mathcal{A} \to \mathcal{A}) \to (\mathcal{A} \to \mathcal{B})$	4.1,1 MP
4	$\mathcal{A} \to \mathcal{B}$	4.2,3 MP
5.1	$(\mathcal{A} \to (\mathcal{B} \to \mathcal{C})) \to ((\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to \mathcal{C}))$	A2
5.2	$(\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to \mathcal{C})$	5.1,2 MP
5	$\mathcal{A} \to \mathcal{C}$	5.2,4 MP

And we have the *AD* derivation which our proof of the deduction theorem told us there would be. Notice that this derivation is not very efficient! We did it in seven lines (without appeal to T3.1) in chapter 3. What our proof of the deduction theorem tells us is that there is sure to be some derivation — where there is no expectation that the guaranteed derivation is particularly elegant or efficient.

Here is a last example which makes use of the deduction theorem. First, an alternate derivation of T3.3.

(H)

1.	$\mathcal{A} \to (\mathcal{B} \to \mathcal{C})$	prem
2.	$\quad\vert\ \mathcal{B}$	assp (g, DT)
3.	$\quad\vert\ \vert\ \mathcal{A}$	assp (g, DT)
4.	$\quad\vert\ \vert\ \mathcal{B} \to \mathcal{C}$	1,3 MP
5.	$\quad\vert\ \vert\ \mathcal{C}$	4,2 MP
6.	$\quad\vert\ \mathcal{A} \to \mathcal{C}$	3-5 DT
7.	$\mathcal{B} \to (\mathcal{A} \to \mathcal{C})$	2-6 DT

In chapter 3 we proved T3.3 in five lines (with an appeal to T3.2). But perhaps this version is relatively intuitive, coinciding as it does, with strategies from *ND*. In this case, there are two applications of DT, and reasoning from the induction therefore applies twice. First, at line (5), there is an *AD* derivation of $\mathcal{C}$ from $\{\mathcal{A} \to (\mathcal{B} \to \mathcal{C}), \mathcal{B}\} \cup \{\mathcal{A}\}$. By reasoning from the induction, then, there is an *AD* derivation from just $\{\mathcal{A} \to (\mathcal{B} \to \mathcal{C}), \mathcal{B}\}$ with $\mathcal{A}$ arrow each of the forms on lines 1-5. So there is a derivation of $\mathcal{A} \to \mathcal{C}$ from $\{\mathcal{A} \to (\mathcal{B} \to \mathcal{C}), \mathcal{B}\}$. But then reasoning from the induction applies again. By reasoning from the induction applied to this *new* derivation, there is a derivation from just $\mathcal{A} \to (\mathcal{B} \to \mathcal{C})$ with $\mathcal{B}$ arrow each of the forms in it. So there is a derivation of $\mathcal{B} \to (\mathcal{A} \to \mathcal{C})$ from just $\mathcal{A} \to (\mathcal{B} \to \mathcal{C})$. So the first derivation, lines 1-5 above, is replaced by another, by the reasoning from DT. Then *it* is replaced by another, again given the reasoning from DT. The result is an *AD* derivation of the desired result.

Here are a couple more cases, where the latter at least, may inspire a certain affection for the deduction theorem.

T9.4. $\vdash_{AD} \mathcal{A} \to (\mathcal{B} \to (\mathcal{A} \wedge \mathcal{B}))$

T9.5. $\vdash_{AD} (\mathcal{A} \to \mathcal{C}) \to [(\mathcal{B} \to \mathcal{C}) \to ((\mathcal{A} \vee \mathcal{B}) \to \mathcal{C})]$

E9.5. Making use of the deduction theorem, prove T9.4 and T9.5. Having done so, see if you can prove them in the style of chapter 3, without any appeal to DT.

E9.6. By the method of our proof of the deduction theorem, convert the above derivation (H) for T3.3 into an official *AD* derivation. Hint: As described above, the method of the induction applies twice: first to lines 1-5, and then to the new derivation. The result should be derivations with 13, and then 37 lines.

E9.7. Consider the axiomatic system *A2* from E3.4 on p. 81, and produce a demonstration of the deduction theorem for it. That is, show that if $\Delta \cup \{\mathcal{P}\} \vdash_{A2} \mathcal{Q}$, then $\Delta \vdash_{A2} \mathcal{P} \rightarrow \mathcal{Q}$. You may appeal to any of the *A2* theorems listed on 81.

9.3.2 Substitution Theorems

Recall what we are after. Our goal is to show that if $\Gamma \vdash_{ND} \mathcal{P}$, then $\Gamma \vdash_{AD} \mathcal{P}$. Toward this end, the deduction theorem lets AD mimic rules in ND which require subderivations. For equality, we turn to some substitution results. Say a complex term r is *free* in an expression $\mathcal{P}$ just in case no variable in r is bound. Then where $\mathcal{T}$ is any term or formula, let $\mathcal{T}^{r}/\!\!/_{s}$ be $\mathcal{T}$ where at most one free instance of r is replaced by term s. Having shown in T3.37, that $\vdash_{AD} (q_i = s) \rightarrow (\mathcal{R}^n q_1 \ldots q_i \ldots q_n \rightarrow \mathcal{R}^n q_1 \ldots s \ldots q_n)$, one might think we have proved that $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{r}/\!\!/_{s})$ for any atomic formula $\mathcal{A}$ and any terms r and s. But *this is not so*. Similarly, having proved in T3.36 that $\vdash_{AD} (q_i = s) \rightarrow (h^n q_1 \ldots q_i \ldots q_n = h^n q_1 \ldots s \ldots q_n)$, one might think we have proved that $\vdash_{AD} (r = s) \rightarrow (t \rightarrow t^{r}/\!\!/_{s})$ for any terms r, s and t. But this is not so. In each case, the difficulty is that the replaced term r might be a *component* of the other terms $q_1 \ldots q_n$, and so might not be any of $q_1 \ldots q_n$. What we have shown is only that it is possible to replace any of the whole terms, $q_1 \ldots q_n$. Thus, $(x = y) \rightarrow (f^1 g^1 x = f^1 g^1 y)$ is not an instance of T3.36 because we do not replace $g^1 x$ but rather a component of it.

However, as one might expect, it is possible to replace terms in basic parts; use the result to make replacements in terms of which *they* are parts; and so forth, all the way up to wholes. Both $(x = y) \rightarrow (g^1 x = g^1 y)$ and $(g^1 x = g^1 y) \rightarrow (f^1 g^1 x = f^1 g^1 y)$ are instances of T3.36. (Be clear about these examples in your mind.) From these, with T3.2 it follows that $(x = y) \rightarrow (f^1 g^1 x = f^1 g^1 y)$. This example suggests a method for obtaining the more general results: Using T3.36, we work from equalities at the level of the parts, to equalities at the level of the whole. For the case of terms, the proof is by induction on the number of function symbols in an arbitrary term t.

T9.6. For arbitrary terms r, s and t, $\vdash_{AD} (r = s) \rightarrow (t = t^{r}/\!\!/_{s})$.

Basis: If t has no function symbols, then t is a variable or a constant. In this case, either (i) $r \neq t$ and $t^{r}/\!\!/_{s} = t$ (nothing is replaced) or (ii) $r = t$ and $t^{r}/\!\!/_{s} = s$ (all of t is replaced). (i) In this case, by T3.32, $\vdash_{AD} t = t$; which is to say, $\vdash_{AD} (t = t^{r}/\!\!/_{s})$; so with A1, $\vdash_{AD} (r = s) \rightarrow (t = t^{r}/\!\!/_{s})$. (ii) In this case, $(r = s) \rightarrow (t = t^{r}/\!\!/_{s})$ is the same as $(r = s) \rightarrow (r = s)$; so by T3.1, $\vdash_{AD} (r = s) \rightarrow (t = t^{r}/\!\!/_{s})$.

Assp: For any i, $0 \leq i < k$, if t has i function symbols, then $\vdash_{AD} (r = s) \to (t = t^{r}/\!\!/_{s})$.

Show: If t has k function symbols, then $\vdash_{AD} (r = s) \to (t = t^{r}/\!\!/_{s})$.

If t has k function symbols, then t is of the form $h^n q_1 \dots q_n$ for terms $q_1 \dots q_n$ with $< k$ function symbols. If all of t is replaced, or no part of t is replaced, then reason as in the basis. So suppose r is some subcomponent of t; then for some q_i, $t^{r}/\!\!/_{s}$ is $h^n q_1 \dots q_i{}^{r}/\!\!/_{s} \dots q_n$. By assumption, $\vdash_{AD} (r = s) \to (q_i = q_i{}^{r}/\!\!/_{s})$; and by T3.36, $\vdash_{AD} (q_i = q_i{}^{r}/\!\!/_{s}) \to (h^n q_1 \dots q_i \dots q_n = h^n q_1 \dots q_i{}^{r}/\!\!/_{s} \dots q_n)$; so by T3.2, $\vdash_{AD} (r = s) \to (h^n q_1 \dots q_i \dots q_n = h^n q_1 \dots q_i{}^{r}/\!\!/_{s} \dots q_n)$; but this is to say, $\vdash_{AD} (r = s) \to (t = t^{r}/\!\!/_{s})$.

Indct: For any terms r, s and t, $\vdash_{AD} (r = s) \to (t = t^{r}/\!\!/_{s})$.

We might think of this result as a further strengthened or generalized version of the *AD* axiom A7. Where A7 lets us replace just variables in terms of the sort $h^n x_1 \dots x_n$, we are now in a position to replace in arbitrary terms with arbitrary terms.

Now we can go after a similarly strengthened version of A8. We show that for any formula $\mathcal{A}$, if s is free for the replaced instance of r in $\mathcal{A}^{r}/\!\!/_{s}$, then $\vdash_{AD} (r = s) \to (\mathcal{A} \to \mathcal{A}^{r}/\!\!/_{s})$. The argument is by induction on the number of operators in $\mathcal{A}$.

T9.7. For any formula $\mathcal{A}$ and terms r and s, if s is free for the replaced instance of r in $\mathcal{A}$, then $\vdash_{AD} (r = s) \to (\mathcal{A} \to \mathcal{A}^{r}/\!\!/_{s})$.

Consider an arbitrary r, s and $\mathcal{A}$, and suppose s is free for the replaced instance of r in $\mathcal{A}^{r}/\!\!/_{s}$.

Basis: If $\mathcal{A}$ is atomic then (i) $\mathcal{A}^{r}/\!\!/_{s} = \mathcal{A}$ (nothing is replaced) or (ii) $\mathcal{A}$ is an atomic of the form $\mathcal{R}^n t_1 \dots t_i \dots t_n$ and $\mathcal{A}^{r}/\!\!/_{s}$ is $\mathcal{R}^n t_1 \dots t_i{}^{r}/\!\!/_{s} \dots t_n$. (i) In this case, by T3.1, $\vdash_{AD} \mathcal{A} \to \mathcal{A}$, which is to say $\vdash_{AD} \mathcal{A} \to \mathcal{A}^{r}/\!\!/_{s}$; so with A1, $\vdash_{AD} r = s \to (\mathcal{A} \to \mathcal{A}^{r}/\!\!/_{s})$. (ii) In this case, by T9.6, $\vdash_{AD} (r = s) \to (t_i = t_i{}^{r}/\!\!/_{s})$; and by T3.37, $\vdash_{AD} (t_i = t_i{}^{r}/\!\!/_{s}) \to (\mathcal{R}^n t_1 \dots t_i \dots t_n \to \mathcal{R}^n t_1 \dots t_i{}^{r}/\!\!/_{s} \dots t_n)$; so by T3.2, $\vdash_{AD} (r = s) \to (\mathcal{R}^n t_1 \dots t_i \dots t_n \to \mathcal{R}^n t_1 \dots t_i{}^{r}/\!\!/_{s} \dots t_n)$; and this is just to say, $\vdash_{AD} (r = s) \to (\mathcal{A} \to \mathcal{A}^{r}/\!\!/_{s})$.

Assp: For any i, $0 \leq i < k$, if $\mathcal{A}$ has i operator symbols and s is free for the replaced instance of r in $\mathcal{A}$, then $\vdash_{AD} (r = s) \to (\mathcal{A} \to \mathcal{A}^{r}/\!\!/_{s})$.

Corollary to the assumption. If $\mathcal{A}$ has $< k$ operators, then $\mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}}$ has $< k$ operators; and since $\mathscr{s}$ replaces only a free instance of $\mathscr{r}$ in $\mathcal{A}$, $\mathscr{r}$ is free for the replacing instance of $\mathscr{s}$ in $\mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}}$; so where the outer substitution is made to sustain $[\mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}}]^{\mathscr{s}}/\!\!/_{\mathscr{r}} = \mathcal{A}$, we have $\vdash_{AD} (\mathscr{s} = \mathscr{r}) \rightarrow (\mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow [\mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}}]^{\mathscr{s}}/\!\!/_{\mathscr{r}})$ as an instance of the inductive assumption, which is just, $\vdash_{AD} (\mathscr{s} = \mathscr{r}) \rightarrow (\mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow \mathcal{A})$. And by T3.33, $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathscr{s} = \mathscr{r})$; so with T3.2, $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow \mathcal{A})$.

Show: If $\mathcal{A}$ has k operator symbols and $\mathscr{s}$ is free for the replaced instance of $\mathscr{r}$ in $\mathcal{A}$, then $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$.

If $\mathcal{A}$ has k operator symbols, then $\mathcal{A}$ is of the form, $\sim\mathcal{P}$, $\mathcal{P} \rightarrow \mathcal{Q}$ or $\forall x\mathcal{P}$ for variable x and formulas $\mathcal{P}$ and $\mathcal{Q}$ with $< k$ operator symbols. Suppose $\mathscr{s}$ is free for any replaced instance of $\mathscr{r}$ in $\mathcal{A}$.

($\sim$) Suppose $\mathcal{A}$ is $\sim\mathcal{P}$. Then $\mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}}$ is $[\sim\mathcal{P}]^{\mathscr{r}}/\!\!/_{\mathscr{s}}$ which is the same as $\sim[\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}}]$. Since $\mathscr{s}$ is free for a replaced instance of $\mathscr{r}$ in $\mathcal{A}$, it is free for that instance of $\mathscr{r}$ in $\mathcal{P}$; so by the corollary to the assumption, $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow \mathcal{P})$. But by T3.13, $\vdash_{AD} (\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow \mathcal{P}) \rightarrow (\sim\mathcal{P} \rightarrow \sim[\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}}])$; so by T3.2, $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\sim\mathcal{P} \rightarrow \sim[\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}}])$; which is to say, $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$.

($\rightarrow$) Suppose $\mathcal{A}$ is $\mathcal{P} \rightarrow \mathcal{Q}$. Then $\mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}}$ is $\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow \mathcal{Q}$ or $\mathcal{P} \rightarrow \mathcal{Q}^{\mathscr{r}}/\!\!/_{\mathscr{s}}$. (i) In the former case, since $\mathscr{s}$ is free for a replaced instance of $\mathscr{r}$ in $\mathcal{A}$, it is free for that instance of $\mathscr{r}$ in $\mathcal{P}$; so by the corollary to the assumption, $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow \mathcal{P})$; so we may reason as follows,

1.	$(\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow \mathcal{P})$	prem
2.	$\mathscr{r} = \mathscr{s}$	assp (g, DT)
3.	$\mathcal{P} \rightarrow \mathcal{Q}$	assp (g, DT)
4.	$\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}}$	assp (g, DT)
5.	$\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow \mathcal{P}$	1,2 MP
6.	$\mathcal{P}$	5,4 MP
7.	$\mathcal{Q}$	3,6 MP
8.	$\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow \mathcal{Q}$	4-7 DT
9.	$(\mathcal{P} \rightarrow \mathcal{Q}) \rightarrow (\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow \mathcal{Q})$	3-8 DT
10.	$(\mathscr{r} = \mathscr{s}) \rightarrow [(\mathcal{P} \rightarrow \mathcal{Q}) \rightarrow (\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow \mathcal{Q})]$	2-9 DT

So $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow [(\mathcal{P} \rightarrow \mathcal{Q}) \rightarrow (\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow \mathcal{Q})]$; which is to say, $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$. (ii) And similarly in the other case [by homework], $\vdash_{AD} (r = s) \rightarrow [(\mathcal{P} \rightarrow \mathcal{Q}) \rightarrow (\mathcal{P} \rightarrow \mathcal{Q}^{r}/\!/_{s})]$. So in either case, $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{r}/\!/_{s})$.

($\forall$) Suppose $\mathcal{A}$ is $\forall x\mathcal{P}$. Then a free instance of r in $\mathcal{A}$ remains free in $\mathcal{P}$ and $\mathcal{A}^{r}/\!/_{s}$ is $\forall x[\mathcal{P}^{r}/\!/_{s}]$. Since s is free for r in $\mathcal{A}$, s is free for r in $\mathcal{P}$; so by assumption, $\vdash_{AD} (r = s) \rightarrow (\mathcal{P} \rightarrow \mathcal{P}^{r}/\!/_{s})$; so we may reason as follows,

1.	$(r = s) \rightarrow (\mathcal{P} \rightarrow \mathcal{P}^{r}/\!/_{s})$	prem
2.	$\quad r = s$	assp (g, DT)
3.	$\quad \forall x\mathcal{P} \rightarrow \mathcal{P}$	A4
4.	$\quad \mathcal{P} \rightarrow \mathcal{P}^{r}/\!/_{s}$	1,2 MP
5.	$\quad \forall x\mathcal{P} \rightarrow \mathcal{P}^{r}/\!/_{s}$	3,4 T3.2
6.	$\quad \forall x\mathcal{P} \rightarrow \forall x\mathcal{P}^{r}/\!/_{s}$	5 T3.28
7.	$(r = s) \rightarrow (\forall x\mathcal{P} \rightarrow \forall x\mathcal{P}^{r}/\!/_{s})$	2-6 DT

Notice that x is sure to be free for itself in $\mathcal{P}$, so that (3) is an instance of A4. And x is bound in $\forall x\mathcal{P}$, so (6) is an instance of T3.28. And because r is free in $\mathcal{A}$, and s is free for r in $\mathcal{A}$, x cannot be a variable in r or s; so the restriction on DT is met at (7). So $\vdash_{AD} (r = s) \rightarrow (\forall x\mathcal{P} \rightarrow \forall x\mathcal{P}^{r}/\!/_{s})$; which is to say, $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{r}/\!/_{s})$.

So for any $\mathcal{A}$ with k operator symbols, $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{r}/\!/_{s})$.

Indct: For any $\mathcal{A}$, $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{r}/\!/_{s})$.

So T9.7, for any formula $\mathcal{A}$, and terms r and s, if s is free for a replaced instance of r in $\mathcal{A}$, then $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{r}/\!/_{s})$.

It is a short step from T9.7, which allows substitution of just a single term, to T9.8 which allows substitution of arbitrarily many. Where, as in chapter 6, $\mathcal{P}^{t}/_{s}$ is $\mathcal{P}$ with some, but not necessarily all, free instances of term t replaced by term s,

T9.8. For any formula $\mathcal{A}$ and terms r and s, if s is free for the replaced instances of r in $\mathcal{A}$, then $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{r}/_{s})$.

By induction on the number of instances of r that are replaced by s in $\mathcal{A}$. Say $\mathcal{A}_i$ is $\mathcal{A}$ with i free instances of r replaced by s. Suppose s is free for the replaced instances of r in $\mathcal{A}$. We show that for any i, $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}_i)$.

Basis: If no instances of r are replaced by s then $\mathcal{A}_0 = \mathcal{A}$. But by T3.1, $\vdash_{AD} \mathcal{A} \rightarrow \mathcal{A}$, and by A1, $\vdash_{AD} (\mathcal{A} \rightarrow \mathcal{A}) \rightarrow [(r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A})]$;

so by MP, $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A})$; which is to say, $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}_0)$.

Assp: For any i, $0 \leq i < k$, $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}_i)$.

Show: $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}_k)$.

$\mathcal{A}_k$ is of the sort $\mathcal{A}_i{}^{r}/\!\!/_{s}$ for $i < k$. By assumption, then, $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}_i)$, and by T9.7, $\vdash_{AD} (r = s) \rightarrow (\mathcal{A}_i \rightarrow \mathcal{A}_i{}^{r}/\!\!/_{s})$, which is the same as $\vdash_{AD} (r = s) \rightarrow (\mathcal{A}_i \rightarrow \mathcal{A}_k)$. So reason as follows,

1.	$(r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}_i)$	by assumption
2.	$(r = s) \rightarrow (\mathcal{A}_i \rightarrow \mathcal{A}_k)$	T9.7
3.		$r = s$	assp (g, DT)
4.		$\mathcal{A} \rightarrow \mathcal{A}_i$	1,3 MP
5.		$\mathcal{A}_i \rightarrow \mathcal{A}_k$	2,3 MP
6.		$\mathcal{A} \rightarrow \mathcal{A}_k$	4,5 T3.2
7.	$(r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}_k)$	3-6 DT

Since s is free for the replaced instances of r in $\mathcal{A}$, (2) is an instance of T9.7. So $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}_k)$.

Indct: For any i, $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}_i)$.

In effect, the result is by multiple applications of T9.7. No matter how many instances of r have been replaced by s, we may use T9.7 to replace another!

Some final substitution results allow substitution of *formulas* rather than terms. We have the result in syntactic and semantic forms. Where $\mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$ is $\mathcal{A}$ with exactly one instance of a subformula $\mathcal{B}$ replaced by formula $\mathcal{C}$,

T9.9. For any formulas $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$, if $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{C}$, then $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$.

The proof is by induction on the number of operators in $\mathcal{A}$. If you have understood the previous two inductions, this one should be straightforward. Observe that, in the basis, when $\mathcal{A}$ is atomic, $\mathcal{B}$ can only be all of $\mathcal{A}$, and $\mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$ is $\mathcal{C}$. For the show, either $\mathcal{B}$ is all of $\mathcal{A}$ or it is not. If it is, then the result holds by reasoning as in the basis. If $\mathcal{B}$ is a proper part of $\mathcal{A}$, then the assumption applies.

T9.10. For any formulas $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$, if for any d, $\mathsf{I_d}[\mathcal{B}] = \mathsf{S}$ iff $\mathsf{I_d}[\mathcal{C}] = \mathsf{S}$, then $\mathsf{I_d}[\mathcal{A}] = \mathsf{S}$ iff $\mathsf{I_d}[\mathcal{A}^{\mathcal{B}}_{\mathcal{C}}] = \mathsf{S}$.

*E9.8. Set up the above demonstration for T9.7 and complete the unfinished case to provide a complete demonstration that for any formula $\mathcal{A}$, and terms r and s, if s is free for the replaced instance of r in $\mathcal{A}$, then $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{r}/\!\!/_{s})$.

E9.9. Suppose our primitive operators are $\sim$, $\wedge$ and $\exists$ rather than $\sim$, $\rightarrow$ and $\forall$. Modify your argument for T9.7 to show that for any formula $\mathcal{A}$, and terms r and s, if s is free for the replaced instance of r in $\mathcal{A}$, then $\vdash_{AD} (r = s) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{r}/\!\!/_{s})$. Hint: Do not forget that you may appeal to T9.4.

*E9.10. Prove T9.9, to show that for any formulas $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$, if $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{C}$, then $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$. Hint: Where $\mathcal{P} \leftrightarrow \mathcal{Q}$ abbreviates $(\mathcal{P} \rightarrow \mathcal{Q}) \wedge (\mathcal{Q} \rightarrow \mathcal{P})$, you can use (abv) along with T3.19, T3.20 and T9.4 to manipulate formulas of the sort $\mathcal{P} \leftrightarrow \mathcal{Q}$.

E9.11. Where $\mathcal{A}^{\mathcal{B}}/_{\mathcal{C}}$ replaces some, but not necessarily all, instances of formula $\mathcal{B}$ with formula $\mathcal{C}$, use your result from E9.10 to show that if $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{C}$, then $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/_{\mathcal{C}}$.

9.3.3 Intended Result

We are finally ready to show that if $\Gamma \vdash_{ND} \mathcal{P}$ then $\Gamma \vdash_{AD} \mathcal{P}$. As usual, the idea is that the existence of one derivation guarantees the existence of another. In this case, we begin with a derivation in *ND*, and move to the existence of one in *AD*. Suppose $\Gamma \vdash_{ND} \mathcal{P}$. Then there is an *ND* derivation N of $\mathcal{P}$ from premises in Γ, with lines $\langle \mathcal{Q}_1 \ldots \mathcal{Q}_n \rangle$ and $\mathcal{Q}_n = \mathcal{P}$. We show that there is an *AD* derivation A of the same result (with possible appeal to DT). Say derivation A *matches* N iff any $\mathcal{Q}_i$ from N appears at the same scope on the line numbered 'i' of A; and say derivation A is *good* iff it has no application of Gen to a variable free in an undischarged auxiliary assumption. Then, given derivation N, we show that there is a good derivation A that matches N. The reason for the restriction on free variables is to be sure that DT is available at any stage in derivation A. The argument is by induction on the line number of N, where we show that for any i, there is a good derivation A_i that matches N through line i. The case when $i = n$ is an *AD* derivation of $\mathcal{P}$ under the scope of the premises alone, and so a demonstration of the desired result.

T9.11. If $\Gamma \vdash_{ND} \mathcal{P}$, then $\Gamma \vdash_{AD} \mathcal{P}$.

Suppose $\Gamma \vdash_{ND} \mathcal{P}$; then there is an *ND* derivation N of $\mathcal{P}$ from premises in Γ. We show that for any i, there is a good *AD* derivation A_i that matches N through line i.

Basis: The first line of N is a premise or an assumption. Let A_1 be the same. Then A_1 matches N; and since there is no application of Gen, A_1 is good.

Assp: For any i, $1 \leq i < k$, there is a good derivation A_i that matches N through line i.

Show: There is a good derivation A_k that matches N through line k.

Either $\mathcal{Q}_k$ is a premise or assumption, or arises from previous lines by R, ∧E, ∧I, →E, →I, ∼E, ∼I, ∨E, ∨I, ↔E, ↔I, ∀E, ∀I, ∃E, ∃I, =E or =I.

(p/a) If $\mathcal{Q}_k$ is a premise or an assumption, let A_k continue in the same way. Then, by reasoning as in the basis, A_k matches N and is good.

(R) If $\mathcal{Q}_k$ arises from previous lines by R, then N looks something like this,

i	$\mathcal{B}$	
k	$\mathcal{B}$	i R

where $i < k$, $\mathcal{B}$ is accessible at line k, and $\mathcal{Q}_k = \mathcal{B}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\mathcal{B}$ appears at the same scope on the line numbered 'i' of A_{k-1} and is accessible in A_{k-1}. So let A_k continue as follows,

i	$\mathcal{B}$	
	⋮	
$k.1$	$\mathcal{B} \rightarrow \mathcal{B}$	T3.1
k	$\mathcal{B}$	$k.1$,i MP

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good.

(∧E) If $\mathcal{Q}_k$ arises by ∧E, then N is something like this,

i	$\mathcal{B} \wedge \mathcal{C}$			i	$\mathcal{B} \wedge \mathcal{C}$	
			or			
k	$\mathcal{B}$	i ∧E		k	$\mathcal{C}$	i ∧E

where $i < k$ and $\mathcal{B} \wedge \mathcal{C}$ is accessible at line k. In the first case, $\mathcal{Q}_k = \mathcal{B}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\mathcal{B} \wedge \mathcal{C}$ appears at the same scope on the line numbered 'i' of A_{k-1} and is accessible in A_{k-1}. So let A_k continue as follows,

$$\begin{array}{r|ll} i & \mathcal{B} \wedge \mathcal{C} & \\ & & \\ k.1 & (\mathcal{B} \wedge \mathcal{C}) \to \mathcal{B} & \text{T3.20} \\ k & \mathcal{B} & k.1,i \text{ MP} \end{array}$$

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good. And similarly in the other case, by application of T3.19.

($\wedge$I) If $\mathcal{Q}_k$ arises from previous lines by $\wedge$I, then N is something like this,

$$\begin{array}{r|ll} i & \mathcal{B} & \\ j & \mathcal{C} & \\ & & \\ k & \mathcal{B} \wedge \mathcal{C} & i,j \ \wedge\text{I} \end{array}$$

where $i, j < k$, $\mathcal{B}$ and $\mathcal{C}$ are accessible at line k, and $\mathcal{Q}_k = \mathcal{B} \wedge \mathcal{C}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\mathcal{B}$ and $\mathcal{C}$ appear at the same scope on the lines numbered 'i' and 'j' of A_{k-1} and are accessible in A_{k-1}. So let A_k continue as follows,

$$\begin{array}{r|ll} i & \mathcal{B} & \\ j & \mathcal{C} & \\ & & \\ k.1 & \mathcal{B} \to (\mathcal{C} \to (\mathcal{B} \wedge \mathcal{C})) & \text{T9.4} \\ k.2 & \mathcal{C} \to (\mathcal{B} \wedge \mathcal{C}) & k.1,i \text{ MP} \\ k & \mathcal{B} \wedge \mathcal{C} & k.2,j \text{ MP} \end{array}$$

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good.

($\to$E) If $\mathcal{Q}_k$ arises from previous lines by $\to$E, then N is something like this,

$$\begin{array}{r|ll} i & \mathcal{B} \to \mathcal{C} & \\ j & \mathcal{B} & \\ & & \\ k & \mathcal{C} & i,j \ \to\text{E} \end{array}$$

where $i, j < k$, $\mathcal{B} \to \mathcal{C}$ and $\mathcal{B}$ are accessible at line k, and $\mathcal{Q}_k = \mathcal{C}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So

$\mathcal{B} \to \mathcal{C}$ and $\mathcal{B}$ appear at the same scope on the lines numbered 'i' and 'j' of A_{k-1} and are accessible in A_{k-1}. So let A_k continue as follows,

$$\begin{array}{r|ll} i & \mathcal{B} \to \mathcal{C} & \\ j & \mathcal{B} & \\ & & \\ k & \mathcal{C} & i,j \text{ MP} \end{array}$$

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good.

(→I) If $\mathcal{Q}_k$ arises by →I, then N is something like this,

$$\begin{array}{r|l|ll} i & & \underline{\mathcal{B}} & \\ & & & \\ j & & \mathcal{C} & \\ k & \multicolumn{2}{l}{\mathcal{B} \to \mathcal{C}} & i\text{-}j \to\text{I} \end{array}$$

where $i, j < k$, the subderivation is accessible at line k and $\mathcal{Q}_k = \mathcal{B} \to \mathcal{C}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\mathcal{B}$ and $\mathcal{C}$ appear at the same scope on the lines numbered 'i' and 'j' of A_{k-1}; since they appear at the same scope, the parallel subderivation is accessible in A_{k-1}; since A_{k-1} is good, no application of Gen under the scope of $\mathcal{B}$ is to a variable free in $\mathcal{B}$. So let A_k continue as follows,

$$\begin{array}{r|l|ll} i & & \underline{\mathcal{B}} & \\ & & & \\ j & & \mathcal{C} & \\ k & \multicolumn{2}{l}{\mathcal{B} \to \mathcal{C}} & i\text{-}j \text{ DT} \end{array}$$

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good.

(∼E) If $\mathcal{Q}_k$ arises by ∼E , then N is something like this (reverting to the unabbreviated form),

$$\begin{array}{r|l|ll} i & & \underline{\sim\mathcal{B}} & \\ & & & \\ j & & \mathcal{C} \wedge \sim\mathcal{C} & \\ k & \multicolumn{2}{l}{\mathcal{B}} & i\text{-}j \sim\text{E} \end{array}$$

where $i, j < k$, the subderivation is accessible at line k, and $\mathcal{Q}_k = \mathcal{B}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\sim\mathcal{B}$ and $\mathcal{C} \wedge \sim\mathcal{C}$ appear at the same scope on the lines numbered 'i' and 'j' of A_{k-1}; since they appear at the same scope, the parallel subderivation is accessible in A_{k-1}; since A_{k-1} is good, no application of Gen under the scope of $\sim\mathcal{B}$ is to a variable free in $\sim\mathcal{B}$. So let A_k continue as follows,

i	$\quad\sim\mathcal{B}$	
j	$\quad\mathcal{C} \wedge \sim\mathcal{C}$	
$k.1$	$\sim\mathcal{B} \to (\mathcal{C} \wedge \sim\mathcal{C})$	i-j DT
$k.2$	$(\mathcal{C} \wedge \sim\mathcal{C}) \to \mathcal{C}$	T3.20
$k.3$	$(\mathcal{C} \wedge \sim\mathcal{C}) \to \sim\mathcal{C}$	T3.19
$k.4$	$\sim\mathcal{B} \to \mathcal{C}$	$k.1,k.2$ T3.2
$k.5$	$\sim\mathcal{B} \to \sim\mathcal{C}$	$k.1,k.3$ T3.2
$k.6$	$(\sim\mathcal{B} \to \sim\mathcal{C}) \to ((\sim\mathcal{B} \to \mathcal{C}) \to \mathcal{B})$	A3
$k.7$	$(\sim\mathcal{B} \to \mathcal{C}) \to \mathcal{B}$	$k.6,k.5$ MP
k	$\mathcal{B}$	$k.7,k.4$ MP

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good.

($\sim$I) Homework.

($\vee$E) If $\mathcal{Q}_k$ arises by $\vee$E, then N is something like this,

f	$\mathcal{B} \vee \mathcal{C}$	
g	$\quad\mathcal{B}$	
h	$\quad\mathcal{D}$	
i	$\quad\mathcal{C}$	
j	$\quad\mathcal{D}$	
k	$\mathcal{D}$	f,g-h,i-j $\vee$E

where $f, g, h, i, j < k$, $\mathcal{B} \vee \mathcal{C}$ and the two subderivations are accessible at line k and $\mathcal{Q}_k = \mathcal{D}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So the formulas at lines f, g, h, i, j appear at the same scope on corresponding lines in A_{k-1}; since they appear at the same scope, $\mathcal{B} \vee \mathcal{C}$ and corresponding subderivations are accessible in A_{k-1}; since A_{k-1} is good, no application of Gen under the scope of $\mathcal{B}$ is to a variable free in $\mathcal{B}$, and no application of Gen under the scope of $\mathcal{C}$ is to a variable free in $\mathcal{C}$. So let A_k continue as follows,

f	$\mathcal{B} \vee \mathcal{C}$	
g	$\quad \mathcal{B}$	
h	$\quad \mathcal{D}$	
i	$\quad \mathcal{C}$	
j	$\quad \mathcal{D}$	
$k.1$	$\mathcal{B} \to \mathcal{D}$	g-h DT
$k.2$	$\mathcal{C} \to \mathcal{D}$	i-j DT
$k.3$	$(\mathcal{B} \to \mathcal{D}) \to [(\mathcal{C} \to \mathcal{D}) \to ((\mathcal{B} \vee \mathcal{C}) \to \mathcal{D})]$	T9.5
$k.4$	$(\mathcal{C} \to \mathcal{D}) \to ((\mathcal{B} \vee \mathcal{C}) \to \mathcal{D})$	$k.3$,$k.1$ MP
$k.5$	$(\mathcal{B} \vee \mathcal{C}) \to \mathcal{D}$	$k.4$,$k.2$ MP
k	$\mathcal{D}$	$k.5$,f MP

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good.

($\vee$I) Homework.

($\leftrightarrow$E) Homework.

($\leftrightarrow$I) Homework.

($\forall$E) Homework.

($\forall$I) If $\mathcal{Q}_k$ arises by $\forall$I, then N looks something like this,

i	$\mathcal{B}^x_v$	
k	$\forall x \mathcal{B}$	i $\forall$I

where $i < k$, $\mathcal{B}^x_v$ is accessible at line k, and $\mathcal{Q}_k = \forall x \mathcal{B}$; further the *ND* restrictions on $\forall$I are met: (i) v is free for x in $\mathcal{B}$, (ii) v is not free in any undischarged auxiliary assumption, and (iii) v is not free in $\forall x \mathcal{B}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\mathcal{B}^x_v$ appears at the same scope on the line numbered 'i' of A_{k-1} and is accessible in A_{k-1}. So let A_k continue as follows,

i	$\mathcal{B}^x_v$	
$k.1$	$\forall v \mathcal{B}^x_v$	i Gen
$k.2$	$\forall v \mathcal{B}^x_v \to \forall x \mathcal{B}$	T3.27
k	$\forall x \mathcal{B}$	$k.1$,$k.2$ MP

If v is x, we have the desired result already at $k.1$. So suppose $x \neq v$. On its face, $k.2$ does not look like T3.27 according to which $\forall x \mathcal{A} \to \forall y \mathcal{A}^x_y$ with y free for x in $\mathcal{A}$ but not free in $\forall x \mathcal{A}$. To see that we have it right, consider first, $\forall v \mathcal{B}^x_v \to \forall x [\mathcal{B}^x_v]^v_x$; this is an instance of T3.27 so long as x is not free in $\forall v \mathcal{B}^x_v$ but free for v in $\mathcal{B}^x_v$. First, since $\mathcal{B}^x_v$ has all its free instances of x replaced by v, x is not free in $\forall v \mathcal{B}^x_v$. Second, since $v \neq x$, with the constraint (iii), that v is not free in $\forall x \mathcal{B}$, v is not free in $\mathcal{B}$; so every free instance of v in $\mathcal{B}^x_v$ replaces a free instance of x; so x is free for v in $\mathcal{B}^x_v$. So $\forall v \mathcal{B}^x_v \to \forall x [\mathcal{B}^x_v]^v_x$ is an instance of T3.27. But since v is not free in $\mathcal{B}$, and by constraint (i), v is free for x in $\mathcal{B}$, by T8.2, $[\mathcal{B}^x_v]^v_x = \mathcal{B}$. So $k.2$ is a version of T3.27.

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. This time, there is an application of Gen at $k.1$. But A_{k-1} is good and since A_k matches N and, by (ii), v is free in no undischarged auxiliary assumption of N, v is not free in any undischarged auxiliary assumption of A_k; so A_k is good. (Notice that, in this reasoning, we appeal to each of the restrictions that apply to $\forall$I in N).

($\exists$E) If $\mathcal{Q}_k$ arises by $\exists$E, then N looks something like this,

h	$\exists x \mathcal{B}$	
i		$\mathcal{B}^x_v$	
j		$\mathcal{C}$	
k	$\mathcal{C}$	h,i-j $\exists$E

where $h, i, j < k$, $\exists x \mathcal{B}$ and the subderivation are accessible at line k, and $\mathcal{Q}_k = \mathcal{C}$; further, the *ND* restrictions on $\exists$E are met: (i) v is free for x in $\mathcal{B}$, (ii) v is not free in any undischarged auxiliary assumption, and (iii) v is not free in $\exists x \mathcal{B}$ or in $\mathcal{C}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So the formulas at lines h, i and j appear at the same scope on corresponding lines in A_{k-1}; since they appear at the same scope, $\exists x \mathcal{B}$ and the corresponding subderivation are accessible in A_{k-1}. Since A_{k-1} is good, no application of Gen under the scope of $\mathcal{B}^x_v$ is to a variable free in $\mathcal{B}^x_v$. So let A_k continue as follows,

h	$\exists x\mathcal{B}$	
i	$\quad\mid\ \mathcal{B}^x_v$	
j	$\quad\mid\ \mathcal{C}$	
$k.1$	$\mathcal{B}^x_v \to \mathcal{C}$	i-j DT
$k.2$	$\exists v\mathcal{B}^x_v \to \mathcal{C}$	$k.1$ T3.31
$k.3$	$\forall v{\sim}\mathcal{B}^x_v \to \forall x{\sim}\mathcal{B}$	T3.27
$k.4$	$(\forall v{\sim}\mathcal{B}^x_v \to \forall x{\sim}\mathcal{B}) \to ({\sim}\forall x{\sim}\mathcal{B} \to {\sim}\forall v{\sim}\mathcal{B}^x_v)$	T3.13
$k.5$	${\sim}\forall x{\sim}\mathcal{B} \to {\sim}\forall v{\sim}\mathcal{B}^x_v$	$k.4$,$k.3$ MP
$k.6$	$\exists x\mathcal{B} \to \exists v\mathcal{B}^x_v$	$k.5$ abv
$k.7$	$\exists v\mathcal{B}^x_v$	h,$k.6$ MP
k	$\mathcal{C}$	$k.2$,$k.7$ MP

From constraint (iii), that v is not free in $\mathcal{C}$, $k.2$ meets the restriction on T3.31. If $v = x$ we can go directly from h and $k.2$ to k. So suppose $v \neq x$. Then by [homework] $\forall v{\sim}\mathcal{B}^x_v \to \forall x{\sim}\mathcal{B}$ at $k.3$ is an instance of T3.27. So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. There is an application of Gen in T3.31 at $k.2$. But A_{k-1} is good and since A_k matches N and, by (ii), v is free in no undischarged auxiliary assumption of N, v is not free in any undischarged auxiliary assumption of A_k; so A_k is good. (Notice again that we appeal to each of the restrictions that apply to ∃E in N).

(∃I) Homework.

(=E) Homework.

(=I) Homework.

In any case, A_k matches N through line k and is good.

Indct: Derivation A matches N and is good.

So if there is an *ND* derivation to show $\Gamma \vdash_{ND} \mathcal{P}$, then there is a matching *AD* derivation to show the same; so T9.11, if $\Gamma \vdash_{ND} \mathcal{P}$, then $\Gamma \vdash_{AD} \mathcal{P}$. So with T9.2, *AD* and *ND* are equivalent; that is, $\Gamma \vdash_{ND} \mathcal{P}$ iff $\Gamma \vdash_{AD} \mathcal{P}$. Given this, we will often ignore the difference between *AD* and *ND* and simply write $\Gamma \vdash \mathcal{P}$ when there is a(n *AD* or *ND*) derivation of $\mathcal{P}$ from premises in Γ. Also given the equivalence between the systems, we are in a position to *transfer* results from one system to the other without demonstrating them directly for both. We will come to appreciate this, and especially the relative simplicity of *AD*, as time goes by.

As before, given any *ND* derivation, we can use the method of our induction to find a corresponding *AD* derivation. For a simple example, consider the following demonstration that ${\sim}A \to (A \wedge B) \vdash_{ND} A$.

	1.	$\sim A \to (A \wedge B)$	P
	2.	$\quad \sim A$	A (c, $\sim$E)
(I)	3.	$\quad A \wedge B$	1,2 $\to$E
	4.	$\quad A$	3 $\wedge$E
	5.	$\quad A \wedge \sim A$	4,2 $\wedge$I
	6.	A	2-4 $\sim$E

Given relevant cases from the induction, the corresponding *AD* derivation is as follows,

1	$\sim A \to (A \wedge B)$	prem
2	$\quad \sim A$	assp
3	$\quad A \wedge B$	1,2 MP
4.1	$\quad (A \wedge B) \to A$	T3.20
4	$\quad A$	4.1,3 MP
5.1	$\quad A \to (\sim A \to (A \wedge \sim A))$	T9.4
5.2	$\quad \sim A \to (A \wedge \sim A)$	4,5.1 MP
5	$\quad A \wedge \sim A$	5.2,2 MP
6.1	$\sim A \to (A \wedge \sim A)$	2-5 DT
6.2	$(A \wedge \sim A) \to A$	T3.20
6.3	$(A \wedge \sim A) \to \sim A$	T3.19
6.4	$\sim A \to A$	6.1,6.2 T3.2
6.5	$\sim A \to \sim A$	6.1,6.3 T3.2
6.6	$(\sim A \to \sim A) \to ((\sim A \to A) \to A)$	A3
6.7	$(\sim A \to A) \to A$	6.6,6.5 MP
6	A	6.7,6.4 MP

For the first two lines, we simply take over the premise and assumption from the *ND* derivation. For (3), the induction uses MP in *AD* where $\to$E appears in *ND*; so that is what we do. For (4), our induction shows that we can get the effect of $\wedge$E by appeal to T3.20 with MP. (5) in the *ND* derivation is by $\wedge$I, and, as above, we get the same effect by T9.4 with MP. (6) in the *ND* derivation is by $\sim$E. Following the strategy from the induction, we set up for application of A3 by getting the conditional by DT. As usual, the constructed derivation is not very efficient! You should be able to get the same result in just five lines by appeal to T3.20, T3.2 and then T3.7 (try it). But, again, the point is just to show that there always *is* a corresponding derivation.

*E9.12. Set up the above induction for T9.11 and complete the unfinished cases (including the case for $\exists$E) to show that if $\Gamma \vdash_{ND} \mathscr{P}$, then $\Gamma \vdash_{AD} \mathscr{P}$. For cases completed in the text, you may simply refer to the text, as the text refers cases to homework.

E9.13. Consider a system *N2* which is like *ND* except that its only rules are $\wedge$E, $\wedge$I, $\sim$E and $\sim$I, along with the system *A2* from E3.4 on p. 81. Produce a complete demonstration that if $\Gamma \vdash_{N2} \mathcal{P}$, then $\Gamma \vdash_{A2} \mathcal{P}$. You may use any of the theorems for *A2* from E3.4, along with DT from E9.7.

E9.14. Consider the following *ND* derivation and, using the method from the induction, construct a derivation to show $\exists x(C \wedge Bx) \vdash_{AD} C$.

1.	$\exists x(C \wedge Bx)$	P
2.	$\quad C \wedge By$	A (g, 1$\exists$E)
3.	$\quad C$	2 $\wedge$E
4.	C	1,2-3 $\exists$E

Hint: your derivation should have 12 lines.

9.4 Extending to *ND+*

ND+ adds sixteen rules to *ND*: the four inference rules, MT, HS, DS and NB and the twelve replacement rules, DN, Com, Assoc, Idem, Impl, Trans, DeM, Exp, Equiv, Dist, QN and BQN — where some of these have multiple forms. It might seem tedious to go through all the cases but, as it happens, we have already done most of the work. First, it is easy to see that,

T9.12. If $\Gamma \vdash_{ND} \mathcal{P}$ then $\Gamma \vdash_{ND+} \mathcal{P}$.

Suppose $\Gamma \vdash_{ND} \mathcal{P}$. Then there is an *ND* derivation N of $\mathcal{P}$ from premises in Γ. But since every rule of *ND* is a rule of *ND+*, N is a derivation in *ND+* as well. So $\Gamma \vdash_{ND+} \mathcal{P}$.

From T9.2 and T9.12, then, the situation is as follows,

$$\Gamma \vdash_{AD} \mathcal{P} \xrightarrow{9.2} \Gamma \vdash_{ND} \mathcal{P} \xrightarrow{9.12} \Gamma \vdash_{ND+} \mathcal{P}$$

If an argument is valid in *AD*, it is valid in *ND*, and in *ND+*. From T9.11, the leftmost arrow is a biconditional. Again, however, one might think that *ND+* has more resources than *ND*, so that more could be derived in *ND+* than *ND*. But this is not so. To see this, we might begin with the closer systems *ND* and *ND+*, and attempt to show that anything derivable in *ND+* is derivable in *ND*. Alternatively, we choose simply to expand the induction of the previous section to include cases for all the rules of *ND*+. The result is a demonstration that if $\Gamma \vdash_{ND+} \mathcal{P}$, then $\Gamma \vdash_{AD} \mathcal{P}$. Given this, the three systems are connected in a "loop" — so that if there is a derivation in any one of the systems, there is a derivation in the others as well.

T9.13. If $\Gamma \vdash_{ND+} \mathcal{P}$, then $\Gamma \vdash_{AD} \mathcal{P}$.

Suppose $\Gamma \vdash_{ND+} \mathcal{P}$; then there is an *ND*+ derivation N of $\mathcal{P}$ from premises in Γ. We show that for any i, there is a good *AD* derivation A_i that matches N through line i.

Basis: The first line of N is a premise or an assumption. Let A_1 be the same. Then A_1 matches N; and since there is no application of Gen, A_1 is good.

Assp: For any i, $0 \leq i < k$, there is a good derivation A_i that matches N through line i.

Show: There is a good derivation of A_k that matches N through line k.

Either $\mathcal{Q}_k$ is a premise or assumption, arises by a rule of *ND*, or by the *ND*+ derivation rules, MT, HS, DS, NB or replacement rules, DN, Com, Assoc, Idem, Impl, Trans, DeM, Exp, Equiv, Dist, QN or BQN. If $\mathcal{Q}_k$ is a premise or assumption or arises by a rule of *ND*, then by reasoning as for T9.11, there is a good derivation A_k that matches N through line k. So suppose $\mathcal{Q}_k$ arises by one of the *ND*+ rules.

(MT) If $\mathcal{Q}_k$ arises from previous lines by MT, then N is something like this,

i	$\mathcal{B} \to \mathcal{C}$	
j	$\sim\mathcal{C}$	
k	$\sim\mathcal{B}$	i,j MT

where $i, j < k$, $\mathcal{B} \to \mathcal{C}$ and $\sim\mathcal{C}$ are accessible at line k, and $\mathcal{Q}_k = \sim\mathcal{B}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\mathcal{B} \to \mathcal{C}$ and $\sim\mathcal{C}$ appear at the same scope on the lines numbered 'i' and 'j' of A_{k-1} and are accessible in A_{k-1}. So let A_k continue as follows,

i	$\mathcal{B} \to \mathcal{C}$	
j	$\sim\mathcal{C}$	
$k.1$	$(\mathcal{B} \to \mathcal{C}) \to (\sim\mathcal{C} \to \sim\mathcal{B})$	T3.13
$k.2$	$\sim\mathcal{C} \to \sim\mathcal{B}$	$k.1,i$ MP
k	$\sim\mathcal{B}$	$k.2,j$ MP

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good.

(HS) Homework.

(DS) Homework.

(NB) Homework.

(rep) If If $\mathcal{Q}_k$ arises from a replacement rule *rep* of the form $\mathcal{C} \;\lhd\rhd\; \mathcal{D}$, then N is something like this,

i	$\mathcal{B}$		or	i	$\mathcal{B}$	
k	$\mathcal{B}^{\mathcal{C}}/\!/_{\mathcal{D}}$	i *rep*		k	$\mathcal{B}^{\mathcal{D}}/\!/_{\mathcal{C}}$	i *rep*

where $i < k$, $\mathcal{B}$ is accessible at line k and, in the first case, $\mathcal{Q}_k = \mathcal{B}^{\mathcal{C}}/\!/_{\mathcal{D}}$. By assumption A_{k-1} matches N through line $k-1$ and is good. But by T6.11 - T6.28, T6.31, T6.32, and T6.70, $\vdash_{ND} \mathcal{C} \leftrightarrow \mathcal{D}$; so with T9.11, $\vdash_{AD} \mathcal{C} \leftrightarrow \mathcal{D}$; so by T9.9, $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{B}^{\mathcal{C}}/\!/_{\mathcal{D}}$. Call an arbitrary particular result of this sort, *Tx*, and augment A_k as follows,

$0.k$	$\mathcal{B} \leftrightarrow \mathcal{B}^{\mathcal{C}}/\!/_{\mathcal{D}}$	*Tx*
i	$\mathcal{B}$	
$k.1$	$(\mathcal{B} \to \mathcal{B}^{\mathcal{C}}/\!/_{\mathcal{D}}) \wedge (\mathcal{B}^{\mathcal{C}}/\!/_{\mathcal{D}} \to \mathcal{B})$	$0.k$ abv
$k.2$	$[(\mathcal{B} \to \mathcal{B}^{\mathcal{C}}/\!/_{\mathcal{D}}) \wedge (\mathcal{B}^{\mathcal{C}}/\!/_{\mathcal{D}} \to \mathcal{B})] \to (\mathcal{B} \to \mathcal{B}^{\mathcal{C}}/\!/_{\mathcal{D}})$	T3.20
$k.3$	$\mathcal{B} \to \mathcal{B}^{\mathcal{C}}/\!/_{\mathcal{D}}$	$k.2$,$k.1$ MP
k	$\mathcal{B}^{\mathcal{C}}/\!/_{\mathcal{D}}$	$k.3$,i MP

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. There may be applications of Gen in the derivation of *Tx*; but that derivation is under the scope of no undischarged assumption. And under the scope of any undischarged assumptions, there is no new application of Gen. So A_k is good. And similarly in the other case, with some work to flip the biconditional $\vdash_{AD} \mathcal{C} \leftrightarrow \mathcal{D}$ to $\vdash_{AD} \mathcal{D} \leftrightarrow \mathcal{C}$.

In any case, A_k matches N through line k and is good.

Indct: Derivation A matches N and is good.

That is it! The key is that work we have already done collapses cases for all the replacement rules into one. So each of the derivation systems, *AD*, *ND*, and *ND+* is

Theorems of Chapter 9

T9.1 For any ordinary argument $\mathscr{P}_1 \ldots \mathscr{P}_n/\mathscr{Q}$, with good translation consisting of II and $\mathscr{P}'_1 \ldots \mathscr{P}'_n$, $\mathscr{Q}'$, if $\mathscr{P}'_1 \ldots \mathscr{P}'_n \vDash \mathscr{Q}'$, then $\mathscr{P}_1 \ldots \mathscr{P}_n/\mathscr{Q}$ is logically valid.

T9.2 If $\Gamma \vdash_{AD} \mathscr{P}$, then $\Gamma \vdash_{ND} \mathscr{P}$.

T9.3 (*Deduction Theorem*) If $\Delta \cup \{\mathscr{P}\} \vdash_{AD} \mathscr{Q}$, and no application of Gen under the scope of $\mathscr{P}$ is to a variable free in $\mathscr{P}$, then $\Delta \vdash_{AD} \mathscr{P} \rightarrow \mathscr{Q}$.

T9.4 $\vdash_{AD} \mathscr{A} \rightarrow (\mathscr{B} \rightarrow (\mathscr{A} \wedge \mathscr{B}))$

T9.5 $\vdash_{AD} (\mathscr{A} \rightarrow \mathscr{C}) \rightarrow [(\mathscr{B} \rightarrow \mathscr{C}) \rightarrow ((\mathscr{A} \vee \mathscr{B}) \rightarrow \mathscr{C})]$

T9.6 For arbitrary terms r, s and t, $\vdash_{AD} (r = s) \rightarrow (t = t^{r}/\!\!/_{s})$.

T9.7 For any formula $\mathscr{A}$ and terms r and s, if s is free for the replaced instance of r in $\mathscr{A}$, then $\vdash_{AD} (r = s) \rightarrow (\mathscr{A} \rightarrow \mathscr{A}^{r}/\!\!/_{s})$.

T9.8 For any formula $\mathscr{A}$ and terms r and s, if s is free for the replaced instances of r in $\mathscr{A}$, then $\vdash_{AD} (r = s) \rightarrow (\mathscr{A} \rightarrow \mathscr{A}^{r}/_{s})$.

T9.9 For any formulas $\mathscr{A}$, $\mathscr{B}$ and $\mathscr{C}$, if $\vdash_{AD} \mathscr{B} \leftrightarrow \mathscr{C}$, then $\vdash_{AD} \mathscr{A} \leftrightarrow \mathscr{A}^{\mathscr{B}}/\!\!/_{\mathscr{C}}$.

T9.11 If $\Gamma \vdash_{ND} \mathscr{P}$, then $\Gamma \vdash_{AD} \mathscr{P}$.

T9.12 If $\Gamma \vdash_{ND} \mathscr{P}$ then $\Gamma \vdash_{ND+} \mathscr{P}$.

T9.13 If $\Gamma \vdash_{ND+} \mathscr{P}$, then $\Gamma \vdash_{AD} \mathscr{P}$.

equivalent to the others. That is, $\Gamma \vdash_{AD} \mathscr{P}$ iff $\Gamma \vdash_{ND} \mathscr{P}$ iff $\Gamma \vdash_{ND+} \mathscr{P}$. And that is what we set out to show.

*E9.15. Set up the above induction and complete the unfinished cases to show that if $\Gamma \vdash_{ND+} \mathscr{P}$, then $\Gamma \vdash_{AD} \mathscr{P}$. For cases completed in the text, you may simply refer to the text, as the text refers cases to homework.

E9.16. Consider a sentential language with $\sim$ and $\wedge$ primitive, along with systems *N2* with rules $\wedge$E, $\wedge$I, $\sim$E and $\sim$I from E9.13, and *A2* from E3.4 on p. 81. Suppose *N2* is augmented to a system *N2+* that includes rules MT and Com (for $\wedge$). Augment your argument from E9.13 to produce a complete demonstration that if $\Gamma \vdash_{N2+} \mathscr{P}$ then $\Gamma \vdash_{A2} \mathscr{P}$. Hint: You will have to prove some

A2 results parallel to ones for which we have merely appealed to theorems above. Do not forget that you have DT from E9.7.

E9.17. For each of the following concepts, explain in an essay of about two pages, so that (college freshman) Hannah could understand. In your essay, you should (i) identify the objects to which the concept applies, (ii) give and explain the definition, and give and explicate examples (iii) where the concept applies, and (iv) where it does not. Your essay should exhibit an understanding of methods from the text.

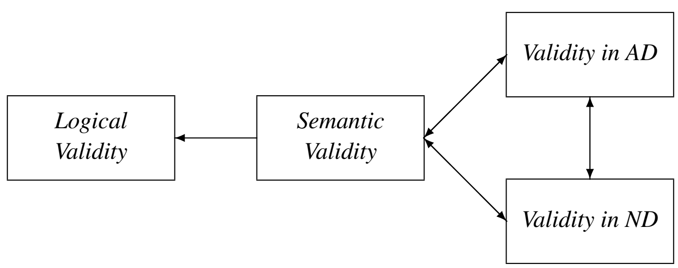
a. The reason semantic validity implies logical validity, but not the other way around.

b. The notion of a *constructive* proof by mathematical induction.

Chapter 10

Main Results

We have introduced four notions of validity, and started to think about their interrelations. In chapter 9, we showed that if an argument is semantically valid, then it is logically valid, and that an argument is valid in *AD* iff it is valid in *ND*. We turn now to the relation between these derivation systems and semantic validity. This completes the project of demonstrating that the different notions of validity are related as follows.



Since *AD* and *ND* are equivalent, it is not necessary separately to establish the relations between *AD* and semantic validity, and between *ND* and semantic validity. Because it is relatively easy to reason about *AD*, we mostly reason about a system like *AD* to establish that an argument is valid in *AD* iff it is semantically valid. From the equivalence between *AD* and *ND* it then follows that an argument is valid in *ND* iff it is semantically valid.

The project divides into two parts. First, we take up the arrows from right to left, and show that if an argument is valid in *AD*, then it is semantically valid: if $\Gamma \vdash_{AD} \mathscr{P}$, then $\Gamma \vDash \mathscr{P}$. Thus our derivation system is *sound*. If a derivation system is sound, it never leads from premises that are true on an interpretation, to a conclusion that is not. Second, moving in the other direction, we show that if an argument is semantically valid, then it is valid in *AD*: if $\Gamma \vDash \mathcal{P}$, then $\Gamma \vdash_{AD} \mathcal{P}$. Thus our derivation system is *adequate*. If a derivation system is adequate, there is a derivation from the premises to the conclusion for every argument that is semantically valid.

10.1 Soundness

It is easy to construct derivation systems that are not sound. Thus, for example, consider a derivation system like *AD* but without the restriction on A4 that the substituted term t be free for the variable x in formula $\mathcal{P}$. Given this, we might reason as follows,

(A)

1.	$\forall x \exists y \sim(x = y)$	prem
2.	$\forall x \exists y \sim(x = y) \rightarrow \exists y \sim(y = y)$	"A4"
3.	$\exists y \sim(y = y)$	1,2 MP

y is not free for x in $\exists y \sim(x = y)$; so line (2) is not an instance of A4. And it is a good thing: Consider any interpretation with at least two elements in U. Then it is true that for every x there is some y not identical to it. So the premise is true. But there is no y in U that is not identical to itself. So the conclusion is not true. So the true premise leads to a conclusion that is not true. So the derivation system is not sound.

We would like to show that *AD* is sound — that there is no sequence of moves, no matter how complex or clever, that would lead from premises that are true to a conclusion that is not true. The argument itself is straightforward: suppose $\Gamma \vdash_{AD} \mathcal{P}$; then there is an *AD* derivation $A = \langle \mathcal{Q}_1 \ldots \mathcal{Q}_n \rangle$ of $\mathcal{P}$ with $\mathcal{Q}_n = \mathcal{P}$. By induction on line numbers in A, we show that for any i, $\Gamma \vDash \mathcal{Q}_i$. The case when $i = n$ is the desired result. So if $\Gamma \vdash_{AD} \mathcal{P}$, then $\Gamma \vDash \mathcal{P}$. This general strategy should by now be familiar. However, for the case involving A4, it will be helpful to obtain a pair of preliminary results.

10.1.1 Switching Theorems

In this section, we develop a couple theorems which link substitutions into formulas and terms with substitutions in variable assignments. As we have seen before, the results are a matched pair, with a first result for terms, that feeds into the basis clause for a result about formulas. Perhaps the hardest part is not so much the proofs of the theorems, as understanding what the theorems say. So let us turn to the first.

Suppose we have some terms t and r with interpretation I and variable assignment d. Say $\mathsf{I_d}[r] = \mathsf{o}$. Then the first proposition is this: term t is assigned the same object on $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}$, as t^x_r is assigned on I_d. Intuitively, this is because the same object is fed into the x-place of the term in each case. With t and $\mathsf{d}(x|\mathsf{o})$,

$$\text{(B)}\qquad \begin{array}{rl} t: & h^n \ldots x \ldots \\ & \qquad\quad | \\ \mathsf{d}(x|\mathsf{o}): & \quad\ \ldots \mathsf{o} \ldots \end{array}$$

object o is the input to the "slot" occupied by x. But we are given that $\mathsf{I}_\mathsf{d}[r] = \mathsf{o}$. So with t^x_r and d,

$$\text{(C)}\qquad \begin{array}{rl} t^x_r: & h^n \ldots r \ldots \\ & \qquad\quad | \\ \mathsf{d}: & \quad\ \ldots \mathsf{o} \ldots \end{array}$$

object o is the input into the "slot" that was occupied by x. So if $\mathsf{I}_\mathsf{d}[r] = \mathsf{o}$, then $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t] = \mathsf{I}_\mathsf{d}[t^x_r]$. In the one case, we guarantee that object o goes into the x-place by meddling with the variable assignment. In the other, we get the same result by meddling with the term. Be sure you are clear about this in your own mind. This will be our first result.

T10.1. For any interpretation I, variable assignment d, with terms t and r, if $\mathsf{I}_\mathsf{d}[r] = \mathsf{o}$, then $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t] = \mathsf{I}_\mathsf{d}[t^x_r]$.

For arbitrary terms t and r, with interpretation I and variable assignment d, suppose $\mathsf{I}_\mathsf{d}[r] = \mathsf{o}$. By induction on the number of function symbols in t, $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t] = \mathsf{I}_\mathsf{d}[t^x_r]$.

Basis: If t has no function symbols, then it is a constant or a variable. Either t is the variable x or it is not. (i) Suppose t is a constant or variable other than x; then $t^x_r = t$ (no replacement is made); but d and $\mathsf{d}(x|\mathsf{o})$ assign just the same things to variables other than x; so they assign just the same things to any variable in t; so by T8.3, $\mathsf{I}_\mathsf{d}[t] = \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t]$. So $\mathsf{I}_\mathsf{d}[t^x_r] = \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t]$. (ii) If t is x, then t^x_r is r (all of t is replaced by r); so $\mathsf{I}_\mathsf{d}[t^x_r] = \mathsf{I}_\mathsf{d}[r] = \mathsf{o}$. But t is x; so $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t] = \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[x]$; and by TA(v), $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[x] = \mathsf{d}(x|\mathsf{o})[x] = \mathsf{o}$. So $\mathsf{I}_\mathsf{d}[t^x_r] = \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t]$.

Assp: For any i, $0 \le i < k$, for t with i function symbols, $\mathsf{I}_\mathsf{d}[t^x_r] = \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t]$.

Show: If t has k function symbols, then $\mathsf{I}_\mathsf{d}[t^x_r] = \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t]$.

If t has k function symbols, then it is of the form, $h^n s_1 \ldots s_n$ where $s_1 \ldots s_n$ have $< k$ function symbols. In this case, $t^x_r = [h^n s_1 \ldots s_n]^x_r = h^n s_1{}^x_r \ldots s_n{}^x_r$. So $\mathsf{I}_\mathsf{d}[t^x_r] = \mathsf{I}_\mathsf{d}[h^n s_1{}^x_r \ldots s_n{}^x_r]$; by TA(f), this is $\mathsf{I}[h^n]\langle \mathsf{I}_\mathsf{d}[s_1{}^x_r] \ldots \mathsf{I}_\mathsf{d}[s_n{}^x_r]\rangle$. Similarly, $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t] = \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[h^n s_1 \ldots s_n]$; and by TA(f), this is $\mathsf{I}[h^n]\langle \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[s_1] \ldots \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[s_n]\rangle$. But by assumption, $\mathsf{I}_\mathsf{d}[s_1{}^x_r] = \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[s_1]$, and ... and $\mathsf{I}_\mathsf{d}[s_n{}^x_r] = \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[s_n]$; so

$\langle \mathsf{I_d}[s_1{}^{x}_{r}] \ldots \mathsf{I_d}[s_n{}^{x}_{r}] \rangle = \langle \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[s_1] \ldots \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[s_n] \rangle$; so $\mathsf{I}[h^n]\langle \mathsf{I_d}[s_1{}^{x}_{r}] \ldots \mathsf{I_d}[s_n{}^{x}_{r}] \rangle = \mathsf{I}[h^n]\langle \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[s_1] \ldots \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[s_n] \rangle$; so $\mathsf{I_d}[t^x_r] = \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t]$.

Indct: For any t, $\mathsf{I_d}[t^x_r] = \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t]$.

Since the "switching" leaves assignments to the parts the same, assignments to the whole remains the same as well.

Similarly, suppose we have we have term r with interpretation I and variable assignment d, where $\mathsf{I_d}[r] = \mathsf{o}$ as before. Suppose r is free for variable x in formula $\mathcal{Q}$. Then the second proposition is that a formula $\mathcal{Q}$ is satisfied on $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}$ iff $\mathcal{Q}^x_r$ is satisfied on $\mathsf{I_d}$. Again, intuitively, this is because the same object is fed into the x-place of the formula in each case. With $\mathcal{Q}$ and $\mathsf{d}(x|\mathsf{o})$,

(D)
$$\begin{array}{rl} \mathcal{Q}: & \mathcal{Q} \ldots x \ldots \\ & \quad\;\;\; | \\ \mathsf{d}(x|\mathsf{o}): & \quad \ldots \mathsf{o} \ldots \end{array}$$

object o is the input to the "slot" occupied by x. But $\mathsf{I_d}[r] = \mathsf{o}$. So with $\mathcal{Q}^x_r$ and d,

(E)
$$\begin{array}{rl} \mathcal{Q}^x_r: & \mathcal{Q} \ldots r \ldots \\ & \quad\;\;\; | \\ \mathsf{d}: & \quad \ldots \mathsf{o} \ldots \end{array}$$

object o is the input into the "slot" that was occupied by x. So if $\mathsf{I_d}[r] = \mathsf{o}$ (and r is free for x in $\mathcal{Q}$), then $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{Q}] = \mathsf{S}$ iff $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$. In the one case, we guarantee that object o goes into the x-place by meddling with the variable assignment. In the other, we get the same result by meddling with the formula. This is our second result, which draws directly upon the first.

T10.2. For any interpretation I, variable assignment d, term r, and formula $\mathcal{Q}$, if $\mathsf{I_d}[r] = \mathsf{o}$, and r is free for x in $\mathcal{Q}$, then $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{Q}] = \mathsf{S}$.

For arbitrary formula $\mathcal{Q}$, term r and interpretation I, suppose r is free for x in $\mathcal{Q}$. By induction on the number of operator symbols in $\mathcal{Q}$,

Basis: Suppose $\mathsf{I_d}[r] = \mathsf{o}$. If $\mathcal{Q}$ has no operator symbols, then it is a sentence letter $\mathcal{S}$ or an atomic of the form $\mathcal{R}^n t_1 \ldots t_n$. In the first case, $\mathcal{Q}^x_r = \mathcal{S}^x_r = \mathcal{S}$. So $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I_d}[\mathcal{S}] = \mathsf{S}$; by SF(s), iff $\mathsf{I}[\mathcal{S}] = \mathsf{T}$; by SF(s) again, iff $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{S}] = \mathsf{S}$; iff $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{Q}] = \mathsf{S}$. In the second case, $\mathcal{Q}^x_r = [\mathcal{R}^n t_1 \ldots t_n]^x_r = \mathcal{R}^n t_1{}^x_r \ldots t_n{}^x_r$. So $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I_d}[\mathcal{R}^n t_1{}^x_r \ldots t_n{}^x_r] = \mathsf{S}$; by SF(r), iff $\langle \mathsf{I_d}[t_1{}^x_r] \ldots \mathsf{I_d}[t_n{}^x_r] \rangle \in \mathsf{I}[\mathcal{R}^n]$; since $\mathsf{I_d}[r] = \mathsf{o}$, by T10.1, iff $\langle \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t_1] \ldots \mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[t_n] \rangle \in \mathsf{I}[\mathcal{R}^n]$; by SF(r), iff $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{R}^n t_1 \ldots t_n] = \mathsf{S}$; iff $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{Q}] = \mathsf{S}$.

Assp: For any i, $0 \leq i < k$, if $\mathcal{Q}$ has i operator symbols, r is free for x in $\mathcal{Q}$ and $\mathsf{I_d}[r] = \mathsf{o}$, then $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$.

Show: If $\mathcal{Q}$ has k operator symbols, r is free for x in $\mathcal{Q}$ and $\mathsf{I_d}[r] = \mathsf{o}$, then $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$.

Suppose $\mathsf{I_d}[r] = \mathsf{o}$. If $\mathcal{Q}$ has k operator symbols, then $\mathcal{Q}$ is of the form $\sim\mathcal{B}$, $\mathcal{B} \to \mathcal{C}$, or $\forall v\mathcal{B}$ for variable v and formulas $\mathcal{B}$ and $\mathcal{C}$ with $< k$ operator symbols.

($\sim$) Suppose $\mathcal{Q}$ is $\sim\mathcal{B}$. Then $\mathcal{Q}^x_r = [\sim\mathcal{B}]^x_r = \sim[\mathcal{B}^x_r]$. Since r is free for x in $\mathcal{Q}$, r is free for x in $\mathcal{B}$; so the assumption applies to $\mathcal{B}$. $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I_d}[\sim\mathcal{B}^x_r] = \mathsf{S}$; by SF($\sim$), iff $\mathsf{I_d}[\mathcal{B}^x_r] \neq \mathsf{S}$; by assumption iff $\mathsf{I_{d(x|o)}}[\mathcal{B}] \neq \mathsf{S}$; by SF($\sim$), iff $\mathsf{I_{d(x|o)}}[\sim\mathcal{B}] = \mathsf{S}$; iff $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$.

($\to$) Homework.

($\forall$) Suppose $\mathcal{Q}$ is $\forall v\mathcal{B}$. Either there are free occurrences of x in $\mathcal{Q}$ or not.

(i) Suppose there are no free occurrences of x in $\mathcal{Q}$. Then $\mathcal{Q}^x_r$ is just $\mathcal{Q}$ (no replacement is made). But since d and $\mathsf{d}(x|\mathsf{o})$ make just the same assignments to variables other than x, they make just the same assignments to all the variables free in $\mathcal{Q}$; so by T8.4, $\mathsf{I_d}[\mathcal{Q}] = \mathsf{S}$ iff $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$. So $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$.

(ii) Suppose there are free occurrences of x in $\mathcal{Q}$. Then x is some variable other than v, and $\mathcal{Q}^x_r = [\forall v\mathcal{B}]^x_r = \forall v[\mathcal{B}^x_r]$.

First, since r is free for x in $\mathcal{Q}$, r is free for x in $\mathcal{B}$, and v is not a variable in r; from this, for any $\mathsf{m} \in \mathsf{U}$, the variable assignments d and $\mathsf{d}(v|\mathsf{m})$ agree on assignments to variables in r; so by T8.3, $\mathsf{I_d}[r] = \mathsf{I_{d(v|m)}}[r]$; so $\mathsf{I_{d(v|m)}}[r] = \mathsf{o}$; so the requirement of the assumption is met for the assignment $\mathsf{d}(v|\mathsf{m})$ and, as an instance of the assumption, for any $\mathsf{m} \in \mathsf{U}$, we have, $\mathsf{I_{d(v|m)}}[\mathcal{B}^x_r] = \mathsf{S}$ iff $\mathsf{I_{d(v|m,x|o)}}[\mathcal{B}] = \mathsf{S}$.

Now suppose $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$ but $\mathsf{I_d}[\mathcal{Q}^x_r] \neq \mathsf{S}$; then $\mathsf{I_{d(x|o)}}[\forall v\mathcal{B}] = \mathsf{S}$ but $\mathsf{I_d}[\forall v\mathcal{B}^x_r] \neq \mathsf{S}$. From the latter, by SF($\forall$), there is some $\mathsf{m} \in \mathsf{U}$ such that $\mathsf{I_{d(v|m)}}[\mathcal{B}^x_r] \neq \mathsf{S}$; so by the above result, $\mathsf{I_{d(v|m,x|o)}}[\mathcal{B}] \neq \mathsf{S}$; so by SF($\forall$), $\mathsf{I_{d(x|o)}}[\forall v\mathcal{B}] \neq \mathsf{S}$; this is impossible. And similarly [by homework] in the other direction. So $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$ iff $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$.

If $\mathcal{Q}$ has k operator symbols, if r is free for x in $\mathcal{Q}$ and $\mathsf{I_d}[r] = \mathsf{o}$, then $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$.

Indct: For any $\mathcal{Q}$, if r is free for x in $\mathcal{Q}$ and $\mathsf{I_d}[r] = \mathsf{o}$, then $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$.

Perhaps the quantifier case looks more difficult than it is. The key point is that since $\mathscr{r}$ is free for x in $\mathcal{Q}$, changes in the assignment to $\mathscr{v}$ do not affect the assignment to $\mathscr{r}$. Thus the assumption applies to $\mathcal{B}$ for variable assignments that differ in their assignments to $\mathscr{v}$. This lets us "take the quantifier off," apply the assumption, and then "put the quantifier back on" in the usual way. Another way to make this point is to see how the argument fails when $\mathscr{r}$ is not free for x in $\mathcal{Q}$. If $\mathscr{r}$ is not free for x in $\mathcal{Q}$, then a change in the assignment to $\mathscr{v}$ may affect the assignment to $\mathscr{r}$. In this case, although $\mathsf{I_d}[\mathscr{r}] = \mathsf{o}$, $\mathsf{I_{d(\mathscr{v}|m)}}[\mathscr{r}]$ might be something else. So there is no reason to think that substituting $\mathscr{r}$ for x will have the same effect as assigning x to o. As we shall see, this restriction corresponds directly to the one on axiom A4. An example of failure for the axiom is the one (A) with which we began the chapter.

*E10.1. Complete the cases for ($\rightarrow$) and ($\forall$) to complete the demonstration of T10.2. You should set up the complete demonstration, but for cases completed in the text, you may simply refer to the text, as the text refers cases to homework.

10.1.2 Soundness

We are now ready for our main proof of soundness for *AD*. Actually, all the parts are already on the table. It is simply a matter of pulling them together into a complete demonstration.

T10.3. If $\Gamma \vdash_{AD} \mathcal{P}$, then $\Gamma \vDash \mathcal{P}$. (*Soundness*)

Suppose $\Gamma \vdash_{AD} \mathcal{P}$. Then there is an *AD* derivation $A = \langle \mathcal{Q}_1 \ldots \mathcal{Q}_n \rangle$ of $\mathcal{P}$ from premises in Γ, with $\mathcal{Q}_n = \mathcal{P}$. By induction on the line numbers in A, we show that for any i, $\Gamma \vDash \mathcal{Q}_i$. The case when $i = n$ is the desired result.

Basis: The first line of A is a premise or an axiom. So $\mathcal{Q}_1$ is either a member of Γ or an instance of A1, A2, A3, A4, A5, A6 A7 or A8. The cases for A1, A2, A3, A5, A6, A7 and A8 are parallel.

(prem) If $\mathcal{Q}_1$ is a member of Γ, then there is no interpretation where all the members of Γ are true and $\mathcal{Q}_1$ is not; so by QV, $\Gamma \vDash \mathcal{Q}_1$.

(Ax) Suppose $\mathcal{Q}_1$ is an instance of A1, A2, A3, A5, A6, A7 or A8 and $\Gamma \nvDash \mathcal{Q}_1$. Then by QV, there is some I such that $\mathsf{I}[\Gamma] = \mathsf{T}$ but $\mathsf{I}[\mathcal{Q}_1] \neq \mathsf{T}$. But by T7.2, T7.3, T7.4, T7.6, T7.8, T7.9, and T7.10, $\vDash \mathcal{Q}_1$; so by QV, $\mathsf{I}[\mathcal{Q}_1] = \mathsf{T}$. This is impossible, reject the assumption: $\Gamma \vDash \mathcal{Q}_1$.

(A4) If $\mathcal{Q}_1$ is an instance of A4, then it is of the form $\forall x \mathcal{B} \rightarrow \mathcal{B}^x_{\mathscr{r}}$ where term $\mathscr{r}$ is free for variable x in formula $\mathcal{B}$. Suppose $\Gamma \nvDash \mathcal{Q}_1$. Then by

QV, there is an I such that $\mathsf{I}[\Gamma] = \mathsf{T}$, but $\mathsf{I}[\forall x \mathcal{B} \to \mathcal{B}^x_r] \neq \mathsf{T}$. From the latter, by TI, there is some d such that $\mathsf{I_d}[\forall x \mathcal{B} \to \mathcal{B}^x_r] \neq \mathsf{S}$; so by SF($\to$), $\mathsf{I_d}[\forall x \mathcal{B}] = \mathsf{S}$ but $\mathsf{I_d}[\mathcal{B}^x_r] \neq \mathsf{S}$; from the first of these, by SF($\forall$), for any $\mathsf{m} \in \mathsf{U}$, $\mathsf{I_{d(x|m)}}[\mathcal{B}] = \mathsf{S}$; in particular, where for some object o, $\mathsf{I_d}[r] = \mathsf{o}$, $\mathsf{I_{d(x|o)}}[\mathcal{B}] = \mathsf{S}$; so, with r free for x in formula $\mathcal{B}$, by T10.2, $\mathsf{I_d}[\mathcal{B}^x_r] = \mathsf{S}$. This is impossible; reject the assumption: $\Gamma \vDash \mathcal{Q}_1$.

Assp: For any i, $1 \leq i < k$, $\Gamma \vDash \mathcal{Q}_i$.

Show: $\Gamma \vDash \mathcal{Q}_k$.

$\mathcal{Q}_k$ is either a premise, an axiom, or arises from previous lines by MP or Gen. If $\mathcal{Q}_k$ is a premise or an axiom then, as in the basis, $\Gamma \vDash \mathcal{Q}_k$. So suppose $\mathcal{Q}_k$ arises by MP or Gen.

(MP) Homework.

(Gen) If $\mathcal{Q}_k$ arises by Gen, then *A* is something like this,

i	$\mathcal{B}$	
	$\vdots$	
k	$\forall x \mathcal{B}$	i Gen

where $i < k$ and $\mathcal{Q}_k = \forall x \mathcal{B}$. Suppose $\Gamma \nvDash \mathcal{Q}_k$; then $\Gamma \nvDash \forall x \mathcal{B}$; so by QV, there is some I such that $\mathsf{I}[\Gamma] = \mathsf{T}$ but $\mathsf{I}[\forall x \mathcal{B}] \neq \mathsf{T}$; from the latter, by TI, there is a d such that $\mathsf{I_d}[\forall x \mathcal{B}] \neq \mathsf{S}$; so by SF($\forall$), there is some $\mathsf{o} \in \mathsf{U}$, such that $\mathsf{I_{d(x|o)}}[\mathcal{B}] \neq \mathsf{S}$. But $\mathsf{I}[\Gamma] = \mathsf{T}$, and by assumption, $\Gamma \vDash \mathcal{B}$; so by QV, $\mathsf{I}[\mathcal{B}] = \mathsf{T}$; so by TI, for any variable assignment h, $\mathsf{I_h}[\mathcal{B}] = \mathsf{S}$; in particular, then, $\mathsf{I_{d(x|o)}}[\mathcal{B}] = \mathsf{S}$. This is impossible; reject the assumption: $\Gamma \vDash \mathcal{Q}_k$.

$\Gamma \vDash \mathcal{Q}_k$.

Indct: For any n, $\Gamma \vDash \mathcal{Q}_n$.

So if $\Gamma \vdash_{AD} \mathcal{P}$, then $\Gamma \vDash \mathcal{P}$. So *AD* is sound. And since *AD* is sound, with theorems T9.2, T9.12 and T9.13 it follows that *ND* and *ND+* are sound as well.

*E10.2. Complete the case for (MP) to round out the demonstration that *AD* is sound. You should set up the complete demonstration, but for cases completed in the text, you may simply refer to the text, as the text refers cases to homework.

E10.3. Consider a derivation system *A4* which has axioms and rules, *A4* A1. Any sentential form $\mathscr{P}$ such that $\vDash \mathscr{P}$.

A2. $\vdash \mathscr{P}^x_t \to \exists x \mathscr{P}$ — where t is free for x in $\mathscr{P}$

MP. $\mathscr{Q}$ follows from $\mathscr{P} \to \mathscr{Q}$ and $\mathscr{P}$

∃E. $\exists x P \to Q$ follows from $\mathscr{P} \to \mathscr{Q}$ — where x is not free in $\mathscr{Q}$

Provide a complete demonstration that *A4* is sound. You may appeal to substitution results from the text as appropriate. Hint: By the soundness of *AD*, if $\mathscr{P}$ is a sentential form and $\vdash_{AD} \mathscr{P}$ then $\mathscr{P}$ is among axioms of the sort (A1).

10.1.3 Consistency

The proof of soundness is the main result we set out to achieve in this section. But before we go on, it is worth pausing to make an application to *consistency*. Say a set Σ (Sigma) of formulas is *consistent* iff there is no formula $\mathscr{A}$ such that $\Sigma \vdash \mathscr{A}$ and $\Sigma \vdash \sim\mathscr{A}$. Consistency is thus defined in terms of *derivations* rather than semantic notions. But we show,

T10.4. If there is an interpretation M such that $\mathsf{M}[\Gamma] = \mathsf{T}$ (a *model* for Γ), then Γ is consistent.

Suppose there is an interpretation M such that $\mathsf{M}[\Gamma] = \mathsf{T}$ but Γ is inconsistent. From the latter, there is a formula $\mathscr{A}$ such that $\Gamma \vdash \mathscr{A}$ and $\Gamma \vdash \sim\mathscr{A}$; so by T10.3, $\Gamma \vDash \mathscr{A}$ and $\Gamma \vDash \sim\mathscr{A}$. But $\mathsf{M}[\Gamma] = \mathsf{T}$; so by QV, $\mathsf{M}[\mathscr{A}] = \mathsf{T}$ and $\mathsf{M}[\sim\mathscr{A}] = \mathsf{T}$; so by TI, for any d, $\mathsf{M_d}[\mathscr{A}] = \mathsf{S}$ and $\mathsf{M_d}[\sim\mathscr{A}] = \mathsf{S}$; from the second of these, by SF($\sim$), $\mathsf{M_d}[\mathscr{A}] \neq \mathsf{S}$. This is impossible; reject the assumption: if there is an interpretation M such that $\mathsf{M}[\Gamma] = \mathsf{T}$, then Γ is consistent.

This is an interesting and important theorem. Suppose we want to show that some set of formulas is inconsistent. For this, it is enough to *derive* a contradiction from the set. But suppose we want to show that there is no way to derive a contradiction. Merely failing to find a derivation does not show that there is not one! But, with soundness, we can demonstrate that there is no such derivation by finding a model for the set.

Similarly, if we want to show that $\Gamma \vdash \mathscr{A}$, it is enough to *produce* the derivation. But suppose we want to show that $\Gamma \nvdash \mathscr{A}$. Merely failing to find a derivation does not show that there is not one! Still, as above, given soundness, we can demonstrate that there is no derivation by finding a model on which the premises are true, with the negation of the conclusion.

T10.5. If there is an interpretation M such that $\mathsf{M}[\Gamma \cup \{\sim\mathcal{A}\}] = \mathsf{T}$, then $\Gamma \nvdash \mathcal{A}$.

The reasoning is left for homework. But the idea is very much as above. With soundness, it is impossible to have both $\mathsf{M}[\Gamma \cup \{\sim\mathcal{A}\}] = \mathsf{T}$ and $\Gamma \vdash \mathcal{A}$.

Again, the result is useful. Suppose, for example, we want to show that $\sim\forall x Ax \nvdash \sim Aa$. You may be unable to find a derivation, and be able to point out flaws in a friend's attempt. But we show that there is no derivation by finding a model on which both $\sim\forall x Ax$ and $\sim\sim Aa$ are true. And this is easy. Let $\mathsf{U} = \{1, 2\}$ with $\mathsf{M}[a] = 1$ and $\mathsf{M}[A] = \{1\}$.

(i) Suppose $\mathsf{M}[\sim\forall x Ax] \neq \mathsf{T}$; then by TI, there is some d such that $\mathsf{M_d}[\sim\forall x Ax] \neq \mathsf{S}$; so by SF($\sim$), $\mathsf{M_d}[\forall x Ax] = \mathsf{S}$; so by SF($\forall$), for any $\mathsf{o} \in \mathsf{U}$, $\mathsf{M}_{\mathsf{d}(x|\mathsf{o})}[Ax] = \mathsf{S}$; so $\mathsf{M}_{\mathsf{d}(x|2)}[Ax] = \mathsf{S}$. But $\mathsf{d}(x|2)[x] = 2$; so by TA(v), $\mathsf{M}_{\mathsf{d}(x|2)}[x] = 2$; so by SF(r), $2 \in \mathsf{M}[A]$; but $2 \notin \mathsf{M}[A]$. This is impossible; reject the assumption: $\mathsf{M}[\sim\forall x Ax] = \mathsf{T}$.
(ii) Suppose $\mathsf{M}[\sim\sim Aa] \neq \mathsf{T}$; then by TI, there is some d such that $\mathsf{M_d}[\sim\sim Aa] \neq \mathsf{S}$; so by SF($\sim$), $\mathsf{M_d}[\sim Aa] = \mathsf{S}$; and by SF($\sim$) again, $\mathsf{M_d}[Aa] \neq \mathsf{S}$. But $\mathsf{M}[a] = 1$; so by TA(c), $\mathsf{M_d}[a] = 1$; so by SF(r), $1 \notin \mathsf{M}[A]$; but $1 \in \mathsf{M}[A]$. This is impossible; reject the assumption: $\mathsf{M}[\sim\sim Aa] = \mathsf{T}$. So $\mathsf{M}[\sim\forall x Ax] = \mathsf{T}$ and $\mathsf{M}[\sim\sim Aa] = \mathsf{T}$. So by T10.5, $\sim\forall x Ax \nvdash \sim Aa$.

If there is a model on which all the members of Γ are true and $\sim\mathcal{A}$ is true, then it is not the case that every model with Γ true has $\mathcal{A}$ true. So, with soundness, there cannot be a derivation of $\mathcal{A}$ from Γ.

*E10.4. Provide an argument to show T10.5. Hint: The reasoning is very much as for T10.4.

E10.5. (a) Show that $\{\exists x Ax, \sim Aa\}$ is consistent. (b) Show that $\forall x(Ax \to Bx), \sim Ba \nvdash \sim\exists x Ax$.

10.2 Sentential Adequacy

The proof of soundness is straightforward given methods we have used before. But the proof of adequacy was revolutionary when Gödel first produced it in 1930. It is easy to construct derivation systems that are *not* adequate. Thus, for example, consider a system like the sentential part of *AD* but without A1. It is easy to see that such a system is sound, and so that derivations without A1 do not go astray. (All we have to do is leave the case for A1 out of the proof for soundness.) But, by our discussion of independence from section 11.3 (see also E8.14), there is no derivation of A1 from A2 and A3 alone. So there are sentential expressions $\mathcal{P}$ such that $\vDash \mathcal{P}$, but for which there is no derivation. So the resultant derivation system would not be adequate. We turn now to showing that our derivation systems are in fact adequate: if $\Gamma \vDash \mathcal{P}$, then $\Gamma \vdash \mathcal{P}$. Given this, with soundness, we have $\Gamma \vDash \mathcal{P}$ iff $\Gamma \vdash \mathcal{P}$, so that our derivation systems deliver just the results they are supposed to.

Adequacy for a system like *AD* was first proved by Kurt Gödel in his 1930 doctoral dissertation. The version of the proof that we will consider is the standard one, essentially due to L. Henkin.[1] An interesting feature of these proofs is that they are not constructive. So far, in proving the equivalence of deductive systems, we have been able to show that there are certain derivations, by showing how to *construct* them. In this case, we show that there are derivations, but without showing how to construct them. As we shall see in Part IV, a constructive proof of adequacy for our full predicate logic is impossible. So this is the only way to go.

The proof of adequacy is more involved than any we have encountered so far. Each of the parts is comparable to what has gone before, and all the parts are straightforward. But there are enough parts that it is possible to lose the forest for the trees. I thus propose to do the proof three times. In this section, we will prove sentential adequacy — that for expressions in a sentential language, if $\Gamma \vDash \mathcal{P}$, then $\Gamma \vdash \mathcal{P}$. This should enable us to grasp the overall shape of the argument without interference from too many details. We will then consider a basic version of the quantificational argument and, after addressing a few complications, put it all together for the full version. Notation and theorem numbers are organized to preserve parallels between the cases.

10.2.1 Basic Idea

The basic idea is straightforward: Let us restrict ourselves to an arbitrary sentential language $\mathcal{L}_s$ and to sentential semantic rules. Derivations are automatically restricted to sentential rules by the restricted language. So derivations and semantics are particularly simple. For formulas in this language, our goal is to show that if $\Gamma \vDash_s \mathcal{P}$, then $\Gamma \vdash \mathcal{P}$. We can see how this works with just a couple of preliminaries.

We begin with a definition and a theorem. As before, let us say,

Con A set Σ of formulas is *consistent* iff there is no formula $\mathcal{A}$ such that $\Sigma \vdash \mathcal{A}$ and $\Sigma \vdash \sim\mathcal{A}$.

[1] Henkin, "Completeness of the First-Order Calculus." Kurt Gödel, "Die Vollständigkeit der Axiome des Logischen Funktionenkalküls." English translation in *From Frege to Gödel*, reprint in *Gödel's Collected Works*.

So consistency is a syntactical notion. A set of formulas is consistent just in case there is no way to derive a contradiction from it. Now for the theorem,

T10.6$_s$. For any set of formulas Σ and sentence $\mathcal{P}$, if $\Sigma \nvdash \sim\mathcal{P}$, then $\Sigma \cup \{\mathcal{P}\}$ is consistent.

> Suppose $\Sigma \nvdash \sim\mathcal{P}$, but $\Sigma \cup \{\mathcal{P}\}$ is not consistent. From the latter, there is some $\mathcal{A}$ such that $\Sigma \cup \{\mathcal{P}\} \vdash \mathcal{A}$ and $\Sigma \cup \{\mathcal{P}\} \vdash \sim\mathcal{A}$. So by DT, $\Sigma \vdash \mathcal{P} \rightarrow \mathcal{A}$ and $\Sigma \vdash \mathcal{P} \rightarrow \sim\mathcal{A}$; by T3.10, $\vdash \sim\sim\mathcal{P} \rightarrow \mathcal{P}$; so by T3.2, $\Sigma \vdash \sim\sim\mathcal{P} \rightarrow \mathcal{A}$, and $\Sigma \vdash \sim\sim\mathcal{P} \rightarrow \sim\mathcal{A}$; but by A3, $\vdash (\sim\sim\mathcal{P} \rightarrow \sim\mathcal{A}) \rightarrow [(\sim\sim\mathcal{P} \rightarrow \mathcal{A}) \rightarrow \sim\mathcal{P}]$; so by two instances of MP, $\Sigma \vdash \sim\mathcal{P}$. But this is impossible; reject the assumption: if $\Sigma \nvdash \sim\mathcal{P}$, then $\Sigma \cup \{\mathcal{P}\}$ is consistent.

The idea is simple: if $\Gamma \cup \{\mathcal{P}\}$ is inconsistent, then by reasoning as for $\sim$I in *ND*, $\sim\mathcal{P}$ follows from Γ alone; so if $\sim\mathcal{P}$ cannot be derived from Γ alone, then $\Gamma \cup \{\mathcal{P}\}$ is consistent. Notice that, insofar as the language is sentential, the derivation does not include any applications of Gen, so the applications of DT are sure to meet the restriction on Gen.

In the last section, we saw that any set with a model is consistent. Now suppose we knew the converse, that any consistent set has a model.

($*$) For any consistent set of formulas Σ', there is an interpretation M' such that $\mathsf{M}'[\Sigma'] = \mathsf{T}$.

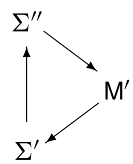
This sets up the key connection between syntactic and semantic notions, between consistency on the one hand, and truth on the other, that we will need for adequacy. Schematically, then, with ($*$) we have the following,

1.	$\Gamma \cup \{\sim\mathcal{P}\}$ has a model	$\Longrightarrow$	$\Gamma \nvDash_s \mathcal{P}$	
2.	$\Gamma \cup \{\sim\mathcal{P}\}$ is consistent	$\Longrightarrow$	$\Gamma \cup \{\sim\mathcal{P}\}$ has a model	($*$)
3.	$\Gamma \cup \{\sim\mathcal{P}\}$ is not consistent	$\Longrightarrow$	$\Gamma \vdash \mathcal{P}$	

(2) is just ($*$). (1) is by simple semantic reasoning: Suppose $\Gamma \cup \{\sim\mathcal{P}\}$ has a model; then there is some M such that $\mathsf{M}[\Gamma \cup \{\sim\mathcal{P}\}] = \mathsf{T}$; so $\mathsf{M}[\Gamma] = \mathsf{T}$ and $\mathsf{M}[\sim\mathcal{P}] = \mathsf{T}$; from the latter, by ST($\sim$), $\mathsf{M}[\mathcal{P}] \neq \mathsf{T}$; so $\mathsf{M}[\Gamma] = \mathsf{T}$ and $\mathsf{M}[\mathcal{P}] \neq \mathsf{T}$; so by SV, $\Gamma \nvDash_s \mathcal{P}$. (3) is by straightforward syntactic reasoning: Suppose $\Gamma \cup \{\sim\mathcal{P}\}$ is not consistent; then by an application of T10.6$_s$, $\Gamma \vdash \sim\sim\mathcal{P}$; but by T3.10, $\vdash \sim\sim\mathcal{P} \rightarrow \mathcal{P}$; so by MP, $\Gamma \vdash \mathcal{P}$. Now suppose $\Gamma \vDash_s \mathcal{P}$; then by (1), reading from right to left, $\Gamma \cup \{\sim\mathcal{P}\}$ does not have a model; so by (2), again from right to left, $\Gamma \cup \{\sim\mathcal{P}\}$ is not consistent;

so by (3), $\Gamma \vdash \mathscr{P}$. So if $\Gamma \models_s \mathscr{P}$, then $\Gamma \vdash \mathscr{P}$, which was to be shown. Of course, knowing that there is some way to derive $\mathscr{P}$ is not the same as knowing what that way is. All the same, $(*)$ tells us that there must exist a model of a certain sort, from which it follows that there must exist a derivation. And the work of our demonstration of adequacy reduces to a demonstration of $(*)$.

So we need to show that every consistent set of formulas Σ' has an interpretation M' such that $\mathsf{M}'[\Sigma'] = \mathsf{T}$. Here is the basic idea: We show that any consistent Σ' is a subset of a corresponding "big" set Σ'' specified in such a way that it must have a model M' — which in turn is a model for the smaller Σ'. Following the arrows,



Given a consistent Σ', we show that there is the big set Σ''. From this we show that there must be an M' that is a model not only for Σ'' but for Σ' as well. So if Σ' is consistent, then it has a model. We proceed through a series of theorems to show that this can be done.

10.2.2 Gödel Numbering

In constructing our big sets, we will want to consider formulas, for inclusion or exclusion, serially — one after another. For this, we need to "line them up" for consideration. Thus, in this section we show,

T10.7$_s$. There is an enumeration $\mathcal{Q}_1, \mathcal{Q}_2 \ldots$ of all formulas in $\mathcal{L}_s$.

> The proof is by construction. We develop a method by which the formulas can be lined up. The method is interesting in its own right, and foreshadows methods from Gödel's Incompleteness Theorem for arithmetic.

In subsection 2.2.1, we required that any sentential language $\mathcal{L}_s$ has countably many sentence letters, which can be ordered into a series, $\mathcal{S}_0$, $\mathcal{S}_1 \ldots$. Assume some such series. We want to show that the *formulas* of $\mathcal{L}_s$ can be so ordered as well. Begin by assigning to each symbol α (alpha) in the language an integer $g[\alpha]$, called its *Gödel Number*.

a. $g[(] = 3$

b. $g[)] = 5$

c. $g[\sim] = 7$

d. $g[\rightarrow] = 9$

e. $g[\mathcal{S}_n] = 11 + 2n$

So, for example, $g[\mathcal{S}_0] = 11$ and $g[\mathcal{S}_4] = 11+2\times 4 = 19$. Clearly each symbol gets a unique Gödel number, and Gödel numbers for individual symbols are odd positive integers.

Now we are in a position to assign a Gödel number to each formula as follows: Where $\alpha_0, \alpha_1 \ldots \alpha_n$ are the symbols, in order from left to right, in some expression $\mathcal{Q}$,

$$g[\mathcal{Q}] = 2^{g[\alpha_0]} \times 3^{g[\alpha_1]} \times 5^{g[\alpha_2]} \times \ldots \times \pi_n{}^{g[\alpha_n]}$$

where 2, 3, $5\ldots\pi_n$ are the first n prime numbers. So, for example, $g[\sim\sim\mathcal{S}_0] = 2^7 \times 3^7 \times 5^{11}$; similarly, $g[\sim(\mathcal{S}_0 \rightarrow \mathcal{S}_4)] = 2^7 \times 3^3 \times 5^{11} \times 7^9 \times 11^{19} \times 13^5 = 15463, 36193, 79608, 90364, 71042, 41201, 87066, 87500, 00000$ — a very big integer! All the same, it is an integer, and it is clear that every expression is assigned to some integer.

Further, different expressions get different Gödel numbers. It is a theorem of arithmetic that every integer is uniquely factored into primes (see the arithmetic for Gödel numbering and more arithmetic for Gödel numbering references). So a given integer can correspond to at most one formula: Given a Gödel number, we can find its unique prime factorization; then if there are seven 2s in the factorization, the first symbol is $\sim$; if there are seven 3s, the second symbol is $\sim$; if there are eleven 5s, the third symbol is $\mathcal{S}_0$; and so forth. Notice that numbers for individual *symbols* are odd, where numbers for *expressions* are even (where the number for an atomic comes out odd when it is thought of as a symbol, but then even when it is thought of as a formula).

The point is not that this is a practical, or a fun, procedure. Rather, the point is that we have integers associated with each expression of the language. Given this, we can take the set of all formulas, and *order* its members according to their Gödel numbers — so that there is an enumeration $\mathcal{Q}_1$, $\mathcal{Q}_2\ldots$ of all formulas. And this is what was to be shown.

E10.6. Find Gödel numbers for the following sentences (for the last, you need not do the calculation).

$\mathcal{S}_7 \qquad \sim\mathcal{S}_0 \qquad \mathcal{S}_0 \rightarrow \sim(\mathcal{S}_1 \rightarrow \sim\mathcal{S}_0)$

Some Arithmetic Relevant to Gödel Numbering

Say an integer i has a "representation as a product of primes" if there are some primes $p_a, p_b \dots p_j$ such that $p_a \times p_b \times \dots \times p_j = i$. We understand a single prime p to be its own representation.

G1. Every integer > 1 has at least one representation as a product of primes.

Basis: 2 is prime and so is its own representation; so the first integer > 1 has a representation as a product of primes.

Assp: For any i, $1 < i < k$, i has a representation as a product of primes.

Show: k has a representation as a product of primes.

If k is prime, the result is immediate; so suppose there are some $i, j < k$ such that $k = i \times j$; by assumption i has a representation as a product of primes $p_a \times \dots \times p_b$ and j has a representation as a product of primes $q_a \times \dots \times q_b$; so $k = i \times j = p_a \times \dots \times p_b \times q_a \times \dots \times q_b$ has a representation as a product of primes.

Indct: Any $i > 1$ has a representation as a product of primes.

Corollary: any integer > 1 is divided by at least one prime.

G2. There are infinitely many prime numbers.

Suppose the number of primes is finite; then there is some list $p_1, p_2 \dots p_n$ of all the primes; consider $q = p_1 \times p_2 \times \dots \times p_n + 1$; no p_i in the list $p_1 \dots p_n$ divides q evenly, since each leaves remainder 1; but by the corollary to (G1), q is divided by some prime; so some prime is not on the list; reject the assumption: there are infinitely many primes.

Note: Sometimes q, calculated this way, is itself prime: when the list is $\{2\}$, $q = 2 + 1 = 3$, and 3 is prime. Similarly, $2 \times 3 + 1 = 7$, $2 \times 3 \times 5 + 1 = 31$, $2 \times 3 \times 5 \times 7 + 1 = 211$, and $2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311$, where 7, 31, 211, and 2311 are all prime. But $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$. So we are not always *finding* a prime not on the list, but rather only showing that there *is* a prime not on it.

G3. For any $i > 1$, if i is the product of the primes $p_1, p_2 \dots p_a$, then no distinct collection of primes $q_1, q_2 \dots q_b$ is such that i is the product of them. (The *Fundamental Theorem* of Arithmetic)

For a proof, see the more arithmetic for Gödel numbering reference in the corresponding part of the next section.

E10.7. Determine the expressions that have the following Gödel numbers.

49 1944 $2^7 \times 3^3 \times 5^{11} \times 7^9 \times 11^7 \times 13^{13} \times 17^5$

E10.8. Which would come first in the official enumeration of formulas, $\mathcal{S}_1 \to \sim\mathcal{S}_2$ or $\mathcal{S}_2 \to \sim\mathcal{S}_2$? Explain. Hint: you should be able to do this without actually calculating the Gödel numbers.

10.2.3 The Big Set

Recall that a set Σ is consistent iff there is no $\mathcal{A}$ such that Σ implies both $\mathcal{A}$ and $\sim\mathcal{A}$. Now, a set Σ is *maximal* iff for any $\mathcal{A}$ the set implies one or the other.

Max A set Σ of formulas is *maximal* iff for any sentence $\mathcal{A}$, $\Sigma \vdash \mathcal{A}$ or $\Sigma \vdash \sim\mathcal{A}$.

Again, this is a syntactical notion. If a set is maximal, then it implies $\mathcal{A}$ or $\sim\mathcal{A}$ for any sentence $\mathcal{A}$; if it is consistent, then it does not imply both. We set out to construct a big set Σ'' from Σ', and show that Σ'' is both maximal and consistent.

CnsΣ'' Construct Σ'' from Σ' as follows: By T10.7$_s$, there is an enumeration, $\mathcal{Q}_1$, $\mathcal{Q}_2$... of all the formulas in $\mathcal{L}_s$. Consider this enumeration, and let Ω_0 (Omega$_0$) be the same as Σ'. Then for any $i > 0$, let

$$\Omega_i = \Omega_{i-1} \quad \text{if} \quad \Omega_{i-1} \vdash \sim\mathcal{Q}_i$$

else,

$$\Omega_i = \Omega_{i-1} \cup \{\mathcal{Q}_i\} \quad \text{if} \quad \Omega_{i-1} \nvdash \sim\mathcal{Q}_i$$

then,

$\Sigma'' = \bigcup_{i \geq 0} \Omega_i$ — that is, Σ'' is the union of all the Ω_is

Beginning with set Σ' ($= \Omega_0$), we consider the formulas in the enumeration $\mathcal{Q}_1$, $\mathcal{Q}_2$... one-by-one, adding a formula to the set just in case its negation is not already derivable. Σ'' contains all the members of Σ' together with all the formulas added this way. Observe that $\Sigma' \subseteq \Sigma''$. One might think of the Ω_is as constituting a big "sack" of formulas, and the $\mathcal{Q}_i$s as coming along on a conveyor belt: for a given $\mathcal{Q}_i$, if there is no way to derive its negation from formulas already in the sack, we throw the $\mathcal{Q}_i$ in; otherwise, we let it go on by. Of course, this is not a procedure we could complete in finite time. Rather, we give a *logical* condition which specifies, for any $\mathcal{Q}_i$ in the language, whether it is to be included in Σ'' or not. The important point is that some Σ'' meeting these conditions *exists*.

As an example, suppose $\Sigma' = \{\sim A \rightarrow B\}$ and consider an enumeration which begins A, $\sim A$, B, $\sim B \ldots$. Then,

$\Omega_0 = \Sigma'$; so $\Omega_0 = \{\sim A \rightarrow B\}$.

$\mathcal{Q}_1 = A$, and $\Omega_0 \nvdash \sim A$; so $\Omega_1 = \{\sim A \rightarrow B\} \cup \{A\} = \{\sim A \rightarrow B, A\}$.

(F) $\mathcal{Q}_2 = \sim A$, and $\Omega_1 \vdash \sim\sim A$; and Ω_2 is unchanged; so $\Omega_2 = \{\sim A \rightarrow B, A\}$.

$\mathcal{Q}_3 = B$, and $\Omega_2 \nvdash \sim B$; so $\Omega_3 = \{\sim A \rightarrow B, A\} \cup \{B\} = \{\sim A \rightarrow B, A, B\}$.

$\mathcal{Q}_4 = \sim B$, and $\Omega_3 \vdash \sim\sim B$; and Ω_4 is unchanged; so $\Omega_4 = \{\sim A \rightarrow B, A, B\}$.

So we include $\mathcal{Q}_i$ each time its negation is not implied. Ultimately, we will use this set to construct a model. For now, though, the point is simply to understand the condition under which a formula is included or excluded from the set.

We now show that if Σ' is consistent, then Σ'' is maximal and consistent. Perhaps the first is obvious: We guarantee that Σ'' is maximal by including $\mathcal{Q}_i$ as a member whenever $\sim\mathcal{Q}_i$ is not already a consequence.

T10.8$_s$. If Σ' is consistent, then Σ'' is maximal and consistent.

The proof comes to the demonstration of three results. Given the assumption that Σ' is consistent, we show, (a) Σ'' is maximal; (b) each Ω_i is consistent; and use this to show (c), Σ'' is consistent. Suppose Σ' is consistent.

(a) Σ'' is maximal. Suppose otherwise. Then there is some $\mathcal{Q}_i$ such that both $\Sigma'' \nvdash \mathcal{Q}_i$ and $\Sigma'' \nvdash \sim\mathcal{Q}_i$. For this i, by construction, each member of Ω_{i-1} is in Σ''; so if $\Omega_{i-1} \vdash \sim\mathcal{Q}_i$ then $\Sigma'' \vdash \sim\mathcal{Q}_i$; but $\Sigma'' \nvdash \sim\mathcal{Q}_i$; so $\Omega_{i-1} \nvdash \sim\mathcal{Q}_i$; so by construction, $\Omega_i = \Omega_{i-1} \cup \{\mathcal{Q}_i\}$; and by construction again, $\mathcal{Q}_i \in \Sigma''$; so $\Sigma'' \vdash \mathcal{Q}_i$. This is impossible; reject the assumption: Σ'' is maximal.

(b) Each Ω_i is consistent. By induction on the series of Ω_is.

Basis: $\Omega_0 = \Sigma'$ and Σ' is consistent; so Ω_0 is consistent.

Assp: For any i, $0 \leq i < k$, Ω_i is consistent.

Show: Ω_k is consistent.

Ω_k is either Ω_{k-1} or $\Omega_{k-1} \cup \{\mathcal{Q}_k\}$. Suppose the former; by assumption, Ω_{k-1} is consistent; so Ω_k is consistent. Suppose the latter; then by construction, $\Omega_{k-1} \nvdash \sim\mathcal{Q}_k$; so by T10.6$_s$, $\Omega_{k-1} \cup \{\mathcal{Q}_k\}$ is consistent; so Ω_k is consistent. So, either way, Ω_k is consistent.

Indct: For any i, Ω_i is consistent.

(c) Σ'' is consistent. Suppose Σ'' is not consistent; then there is some $\mathcal{A}$ such that $\Sigma'' \vdash \mathcal{A}$ and $\Sigma'' \vdash \sim\mathcal{A}$. Consider derivations *D1* and *D2* of these results, and the premises $\mathcal{Q}_i \dots \mathcal{Q}_j$ of these derivations. Where $\mathcal{Q}_j$ is the last of these premises in the enumeration of formulas, by the construction of Σ'', each of $\mathcal{Q}_i \dots \mathcal{Q}_j$ must be a member of Ω_j; so *D1* and *D2* are derivations from Ω_j; so Ω_j is inconsistent. But by the previous result, Ω_j is consistent. This is impossible; reject the assumption: Σ'' is consistent.

Because derivations of $\mathcal{A}$ and $\sim\mathcal{A}$ have only finitely many premises, all the premises in a derivation of a contradiction must show up in some Ω_j; so if Σ'' is inconsistent, then some Ω_j is inconsistent. But no Ω_j is inconsistent. So Σ'' is consistent. So we have what we set out to show. $\Sigma' \subseteq \Sigma''$, and if Σ' is consistent, then Σ'' is both maximal and consistent.

E10.9. (i) Suppose $\Sigma' = \{A \rightarrow \sim B\}$ and the enumeration of formulas begins A, $\sim A$, B, $\sim B \dots$. What are Ω_0, Ω_1, Ω_2, Ω_3, and Ω_4? (ii) What are they when the enumeration begins B, $\sim B$, A, $\sim A \dots$? In each case, produce a (sentential) model to show that the resultant Ω_4 is consistent.

10.2.4 The Model

We now construct a model M' for Σ'. In this sentential case, the specification is particularly simple.

CnsM′ For any atomic $\mathcal{S}$, let $\mathsf{M}'[\mathcal{S}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{S}$.

Notice that there clearly exists some such interpretation M': We assign T to every sentence letter that can be derived from Σ'', and F to the others. It will not be the case that we are in a position to do all the derivations, and so to know what are all the assignments to the atomics. Still, it must be that any atomic either is or is not a consequence of Σ', and so that there exists a corresponding interpretation M' on which those sentence letters either are or are not assigned T.

We now want to show that if Σ' is consistent, then M' is a model for Σ' — that if Σ' is consistent then $\mathsf{M}'[\Sigma'] = \mathsf{T}$. As we shall see, this results immediately from the following theorem.

T10.9$_s$. If Σ' is consistent, then for any sentence $\mathcal{B}$, of $\mathcal{L}_s$, $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

Suppose Σ' is consistent. Then by T10.8$_s$, Σ'' is maximal and consistent. Now by induction on the number of operators in $\mathcal{B}$, *Basis:* If $\mathcal{B}$ has no operators, then it is an atomic of the sort $\mathcal{S}$. But by the construction of M', $\mathsf{M}'[\mathcal{S}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{S}$; so $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

Assp: For any i, $0 \leq i < k$, if $\mathcal{B}$ has i operator symbols, then $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

Show: If $\mathcal{B}$ has k operator symbols, then $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

If $\mathcal{B}$ has k operator symbols, then it is of the form $\sim\mathcal{P}$ or $\mathcal{P} \rightarrow \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ have $< k$ operator symbols.

($\sim$) Suppose $\mathcal{B}$ is $\sim\mathcal{P}$. (i) Suppose $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$; then $\mathsf{M}'[\sim\mathcal{P}] = \mathsf{T}$; so by ST($\sim$), $\mathsf{M}'[\mathcal{P}] \neq \mathsf{T}$; so by assumption, $\Sigma'' \nvdash \mathcal{P}$; so by maximality, $\Sigma'' \vdash \sim\mathcal{P}$; which is to say, $\Sigma'' \vdash \mathcal{B}$. (ii) Suppose $\Sigma'' \vdash \mathcal{B}$; then $\Sigma'' \vdash \sim\mathcal{P}$; so by consistency, $\Sigma'' \nvdash \mathcal{P}$; so by assumption, $\mathsf{M}'[\mathcal{P}] \neq \mathsf{T}$; so by ST($\sim$), $\mathsf{M}'[\sim\mathcal{P}] = \mathsf{T}$; which is to say, $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$. So $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

($\rightarrow$) Suppose $\mathcal{B}$ is $\mathcal{P} \rightarrow \mathcal{Q}$. (i) Suppose $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$; then $\mathsf{M}'[\mathcal{P} \rightarrow \mathcal{Q}] = \mathsf{T}$; so by ST($\rightarrow$), $\mathsf{M}'[\mathcal{P}] \neq \mathsf{T}$ or $\mathsf{M}'[\mathcal{Q}] = \mathsf{T}$; so by assumption, $\Sigma'' \nvdash \mathcal{P}$ or $\Sigma'' \vdash \mathcal{Q}$. Suppose the latter; by A1, $\vdash \mathcal{Q} \rightarrow (\mathcal{P} \rightarrow \mathcal{Q})$; so by MP, $\Sigma'' \vdash \mathcal{P} \rightarrow \mathcal{Q}$. Suppose the former; then by maximality, $\Sigma'' \vdash \sim\mathcal{P}$; but by T3.9, $\vdash \sim\mathcal{P} \rightarrow (\mathcal{P} \rightarrow \mathcal{Q})$; so by MP, $\Sigma'' \vdash \mathcal{P} \rightarrow \mathcal{Q}$. So in either case, $\Sigma'' \vdash \mathcal{P} \rightarrow \mathcal{Q}$; where this is to say, $\Sigma'' \vdash \mathcal{B}$. (ii) Suppose $\Sigma'' \vdash \mathcal{B}$ but $\mathsf{M}'[\mathcal{B}] \neq \mathsf{T}$; by [homework], this is impossible: so if $\Sigma'' \vdash \mathcal{B}$, then $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$. So $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

If $\mathcal{B}$ has k operator symbols, then $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

Indct: For any $\mathcal{B}$, $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

So if Σ' is consistent, then for any $\mathcal{B} \in \Sigma''$, $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

The key to this is that Σ'' is both maximal and consistent. In (F), for example, $\Omega_0 = \{\sim A \rightarrow B\}$; so $\Omega_0 \nvdash A$ and $\Omega_0 \nvdash B$; if we were simply to follow our construction procedure as applied to this set, the result would have $\mathsf{M}'[A] \neq \mathsf{T}$ and $\mathsf{M}'[B] \neq \mathsf{T}$; but then $\mathsf{M}'[\sim A \rightarrow B] \neq \mathsf{T}$ and there is no model for Ω_0. But Ω_4 has A and B as members; so $\Omega_4 \vdash A$ and $\Omega_4 \vdash B$. So by the construction procedure, $\mathsf{M}'[A] = \mathsf{T}$ and $\mathsf{M}'[B] = \mathsf{T}$; so $\mathsf{M}'[\sim A \rightarrow B] = \mathsf{T}$. Thus it is the construction with maximality and consistency of Σ'' that puts us in a position to draw the parallel between the implications of Σ'' and what is true on M'. It is now a short step to seeing that we have a model for Σ' and so ($*$) that we have been after.

*E10.10. Complete the second half of the conditional case to complete the proof of T10.9_s. You should set up the entire induction, but may refer to the text for parts completed there, as the text refers to homework.

E10.11. (i) Where $\Sigma' = \{A \to \sim B\}$, and the enumeration of formulas are as in the first part of E10.9, what assignments does M' make to A and B? (ii) What assignments does it make on the second enumeration? Use a truth table to show, for each case, that the assignments result in a *model* for Σ'. Explain.

10.2.5 Final Result

The proof of sentential adequacy is now a simple matter of pulling together what we have done. First, it is a simple matter to show,

T10.10$_\text{s}$. If Σ' is consistent, then $\mathsf{M}'[\Sigma'] = \mathsf{T}$. $(*)$

Suppose Σ' is consistent but $\mathsf{M}'[\Sigma'] \neq \mathsf{T}$. From the latter, there is some formula $\mathcal{B} \in \Sigma'$ such that $\mathsf{M}'[\mathcal{B}] \neq \mathsf{T}$. Since $\mathcal{B} \in \Sigma'$, by construction, $\mathcal{B} \in \Sigma''$; so $\Sigma'' \vdash \mathcal{B}$; so, since Σ' is consistent, by T10.9$_s$, $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$. This is impossible; reject the assumption: if Σ' is consistent, then $\mathsf{M}'[\Sigma'] = \mathsf{T}$.

That is it! Going back to the beginning of our discussion of sentential adequacy, all we needed was $(*)$, and now we have it. So the final argument is as sketched before:

T10.11$_\text{s}$. If $\Gamma \vDash_s \mathcal{P}$, then $\Gamma \vdash \mathcal{P}$. (*sentential adequacy*)

Suppose $\Gamma \vDash_s \mathcal{P}$ but $\Gamma \nvdash \mathcal{P}$. Say, for the moment, that $\Gamma \vdash \sim\sim\mathcal{P}$; by T3.10, $\vdash \sim\sim\mathcal{P} \to \mathcal{P}$; so by MP, $\Gamma \vdash \mathcal{P}$; but this is impossible; so $\Gamma \nvdash \sim\sim\mathcal{P}$. Given this, by T10.6$_s$, $\Gamma \cup \{\sim\mathcal{P}\}$ is consistent; so by T10.10$_s$, there is a model M' such that $\mathsf{M}'[\Gamma \cup \{\sim\mathcal{P}\}] = \mathsf{T}$; so $\mathsf{M}'[\sim\mathcal{P}] = \mathsf{T}$; so by ST($\sim$), $\mathsf{M}'[\mathcal{P}] \neq \mathsf{T}$; so $\mathsf{M}'[\Gamma] = \mathsf{T}$ but $\mathsf{M}'[\mathcal{P}] \neq \mathsf{T}$; so by SV, $\Gamma \nvDash_s \mathcal{P}$. This is impossible; reject the assumption: if $\Gamma \vDash_s \mathcal{P}$, then $\Gamma \vdash \mathcal{P}$.

Try again to get the complete picture in your mind: The key is that consistent sets always have models. If there is no derivation of $\mathcal{P}$ from Γ, then $\Gamma \cup \{\sim\mathcal{P}\}$ is consistent; and if $\Gamma \cup \{\sim\mathcal{P}\}$ is consistent, then it has a model — so that $\Gamma \nvDash_s \mathcal{P}$. Thus, put the other way around, if $\Gamma \vDash_s \mathcal{P}$, then there is a derivation of $\mathcal{P}$ from Γ. We get the key point, that consistent sets have models, by finding a relation between consistent, and *maximal* consistent sets. If a set is both maximal and consistent, then it contains enough information about its atomics that a model for its atomics is a model for the whole.

It is obvious that the argument is not constructive — we do not see how to show that $\Gamma \vdash \mathcal{P}$ whenever $\Gamma \vDash_s \mathcal{P}$. But it is interesting to see why. The argument turns on the *existence* of our big sets under certain conditions, and so on the existence of models. We show that the sets must exist and have certain properties, though we are not in a position to find all their members. This puts us in a position to know the existence of derivations, though we do not say what they are.[2]

E10.12. Suppose our primitive operators are $\sim$ and $\wedge$ and the derivation system is *A2* from E3.4 on p. 81. Present a complete demonstration of adequacy for this derivation system — with all the definitions and theorems. You may simply appeal to the text for results that require no change.

10.3 Quantificational Adequacy: Basic Version

As promised, the demonstration of quantificational adequacy is parallel to what we have seen. Return to a quantificational language and to our regular quantificational semantic and derivation notions. The goal is to show that if $\Gamma \vDash \mathcal{P}$, then $\Gamma \vdash \mathcal{P}$. Certain complications are avoided if we suppose that the language $\mathcal{L}'$ includes infinitely many constants not in Γ, and does not include the '$=$' symbol for equality. The constants not already in Γ are required for the construction of our big sets. And without $=$ in the language, the model specification is simplified. We will work through the basic argument in this section and, dropping constraints on the language, return to the general case in the next. If you are confused at any stage, it may help to refer back to the parallel section for the sentential case.

Before launching into the main argument, it will be helpful to have a preliminary theorem. Where $D = \langle \mathcal{B}_1 \ldots \mathcal{B}_n \rangle$ is an *AD* derivation, and $\Sigma' = \{\mathcal{C}_1 \ldots \mathcal{C}_n\}$ is a set of formulas, for some constant a and variable x, say $D^{a}_{x} = \langle \mathcal{B}_1{}^{a}_{x} \ldots \mathcal{B}_n{}^{a}_{x} \rangle$ and $\Sigma'{}^{a}_{x} = \{\mathcal{C}_1{}^{a}_{x} \ldots \mathcal{C}_n{}^{a}_{x}\}$. By induction on the line numbers in D, we show,

T10.12. If D is a derivation from Σ', and x is a variable that does not appear in D, then for any constant a, D^{a}_{x} is a derivation from $\Sigma'{}^{a}_{x}$.

Basis: $\mathcal{B}_1$ is either a member of Σ' or an axiom.

(prem) If $\mathcal{B}_1$ is a member of Σ', then $\mathcal{B}_1{}^{a}_{x}$ is a member of $\Sigma'{}^{a}_{x}$; so $\langle \mathcal{B}_1{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

[2] In fact, there are constructive approaches to sentential adequacy. See, for example, Lemma 1.13 and Proposition 1.14 of Mendelson, *Introduction to Mathematical Logic*. Our primary purpose, however, is to set up the argument for the quantificational case, where such methods do not apply.

(eq) If $\mathcal{B}_1$ is an equality axiom, A6, A7 or A8, then it includes no constants; so $\mathcal{B}_1 = \mathcal{B}_1{}^{a}_{x}$; so $\mathcal{B}_1{}^{a}_{x}$ is an equality axiom, and $\langle \mathcal{B}_1{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

(A1) If $\mathcal{B}_1$ is an instance of A1, then it is of the form, $\mathcal{P} \rightarrow (\mathcal{Q} \rightarrow \mathcal{P})$; so $\mathcal{B}_1{}^{a}_{x}$ is $\mathcal{P}^{a}_{x} \rightarrow (\mathcal{Q}^{a}_{x} \rightarrow \mathcal{P}^{a}_{x})$; but this is an instance of A1; so if $\mathcal{B}_1$ is an instance of A1, then $\mathcal{B}_1{}^{a}_{x}$ is an instance of A1, and $\langle \mathcal{B}_1{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

(A2) Homework.

(A3) Homework.

(A4) If $\mathcal{B}_1$ is an instance of A4, then it is of the form, $\forall v \mathcal{P} \rightarrow \mathcal{P}^{v}_{t}$, for some variable v and term t that is free for v in $\mathcal{P}$. So $\mathcal{B}_1{}^{a}_{x} = [\forall v \mathcal{P} \rightarrow \mathcal{P}^{v}_{t}]^{a}_{x} = [\forall v \mathcal{P}]^{a}_{x} \rightarrow [\mathcal{P}^{v}_{t}]^{a}_{x}$. But since x does not appear in D, $x \neq v$; so $[\forall v \mathcal{P}]^{a}_{x} = \forall v [\mathcal{P}^{a}_{x}]$. And by T8.7, $[\mathcal{P}^{v}_{t}]^{a}_{x} = [\mathcal{P}^{a}_{x}]^{v}_{t^{a}_{x}}$. So $\mathcal{B}_1{}^{a}_{x} = \forall v [\mathcal{P}^{a}_{x}] \rightarrow [\mathcal{P}^{a}_{x}]^{v}_{t^{a}_{x}}$; and since x is new to D and t is free for v in $\mathcal{P}$, t^{a}_{x} is free for v in $\mathcal{P}^{a}_{x}$; so $\forall v [\mathcal{P}^{a}_{x}] \rightarrow [\mathcal{P}^{a}_{x}]^{v}_{t^{a}_{x}}$ is an instance of A4; so if $\mathcal{B}_1$ is an instance of A4, then $\mathcal{B}_1{}^{a}_{x}$ is an instance of A4, and $\langle \mathcal{B}_1{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

(A5) Homework.

Assp: For any i, $1 \leq i < k$, $\langle \mathcal{B}_1{}^{a}_{x} \dots \mathcal{B}_i{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

Show: $\langle \mathcal{B}_1{}^{a}_{x} \dots \mathcal{B}_k{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

$\mathcal{B}_k$ is a member of Σ', an axiom, or arises from previous lines by MP or Gen. If $\mathcal{B}_k$ is a member of Σ' or an axiom then, by reasoning as in the basis, $\langle \mathcal{B}_1 \dots \mathcal{B}_k \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$. So two cases remain.

(MP) Homework.

(Gen) If $\mathcal{B}_k$ arises by Gen, then there are some lines in D,

$$
\begin{array}{lll}
i & \mathcal{P} & \\
 & \vdots & \\
k & \forall v \mathcal{Q} & i \text{ Gen}
\end{array}
$$

where $i < k$ and $\mathcal{B}_k = \forall v \mathcal{P}$. By assumption $\mathcal{P}^{a}_{x}$ is a member of the derivation $\langle \mathcal{B}_1{}^{a}_{x} \dots \mathcal{B}_{k-1}{}^{a}_{x} \rangle$ from $\Sigma'{}^{a}_{x}$; so $\forall v \mathcal{P}^{a}_{x}$ follows in this new derivation by Gen. So $\langle \mathcal{B}_1{}^{a}_{x} \dots \mathcal{B}_k{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

So $\langle \mathcal{B}_1{}^{a}_{x} \dots \mathcal{B}_k{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

Indct: For any n, $\langle \mathcal{B}_1{}^{a}_{x} \dots \mathcal{B}_n{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

The reason this works is that none of the justifications change: switching x for a leaves each line justified for the same reasons as before. The only sticking point may be the case for A4. But we did the real work for this by induction in T8.7. And that result should be intuitive, once we see what it says. Given this, the rest is straightforward.

*E10.13. Finish the cases for A2, A3, A5 and MP to complete the proof of T10.12. You should set up the complete demonstration, but may refer to the text for cases completed there, as the text refers cases to homework.

E10.14. Where $\Sigma' = \{Ab\}$ and D is as follows,

1.	$\forall x{\sim}Ax \rightarrow {\sim}Ab$	A4
2.	$(\forall x{\sim}Ax \rightarrow {\sim}Ab) \rightarrow ({\sim}{\sim}Ab \rightarrow {\sim}\forall x{\sim}Ax)$	T3.13
3.	${\sim}{\sim}Ab \rightarrow {\sim}\forall x{\sim}Ax$	2,1 MP
4.	$Ab \rightarrow {\sim}{\sim}Ab$	T3.11
5.	$Ab \rightarrow {\sim}\forall x{\sim}Ax$	4,3 T3.2
6.	Ab	prem
7.	${\sim}\forall x{\sim}Ax$	5,6 MP
8.	$\exists x Ax$	7 abv

apply T10.12 to show that D^{b}_{y} is a derivation from $\Sigma'^{\,b}_{\,y}$. Do any of the justifications change? Explain.

10.3.1 Basic Idea

As before, our main argument turns on the idea that every consistent set has a model. Thus we begin with a definition and a theorem.

Con A set Σ of formulas is *consistent* iff there is no formula $\mathcal{A}$ such that $\Sigma \vdash \mathcal{A}$ and $\Sigma \vdash {\sim}\mathcal{A}$.

So a set of formulas is consistent just in case there is no way to derive a contradiction from it. Of course, now we are working with full quantificational languages, and so with our complete quantificational derivation systems.

For the following theorem, notice that Σ is a set of *formulas*, and $\mathcal{P}$ a *sentence* (a distinction without a difference in the sentential case). Again as before,

T10.6. For any set of formulas Σ and sentence $\mathcal{P}$, if $\Sigma \nvdash {\sim}\mathcal{P}$, then $\Sigma \cup \{\mathcal{P}\}$ is consistent.

For some sentence $\mathcal{P}$, suppose $\Sigma \nvdash {\sim}\mathcal{P}$ but $\Sigma \cup \{\mathcal{P}\}$ is not consistent. From the latter, there is some formula $\mathcal{A}$ such that $\Sigma \cup \{\mathcal{P}\} \vdash \mathcal{A}$ and $\Sigma \cup \{\mathcal{P}\} \vdash$

$\sim\mathcal{A}$; since $\mathcal{P}$ is a sentence, it has no free variables; so by DT, $\Sigma \vdash \mathcal{P} \to \mathcal{A}$ and $\Sigma \vdash \mathcal{P} \to \sim\mathcal{A}$; by T3.10, $\vdash \sim\sim\mathcal{P} \to \mathcal{P}$; so by T3.2, $\Sigma \vdash \sim\sim\mathcal{P} \to \mathcal{A}$ and $\Sigma \vdash \sim\sim\mathcal{P} \to \sim\mathcal{A}$; but by A3, $\vdash (\sim\sim\mathcal{P} \to \sim A) \to [(\sim\sim\mathcal{P} \to \mathcal{A}) \to \sim\mathcal{P}]$; so by two instances of MP, $\Sigma \vdash \sim\mathcal{P}$. This is impossible; reject the assumption: if $\Sigma \nvdash \sim\mathcal{P}$, then $\Sigma \cup \{\mathcal{P}\}$ is consistent.

Insofar as $\mathcal{P}$ is required to be a sentence, the restriction on applications of DT is sure to be met: since $\mathcal{P}$ has no free variables, no application of Gen is to a variable free in $\mathcal{P}$. So T10.6 does not apply to arbitrary formulas.

To the extent that T10.6 plays a direct role in our basic argument for adequacy, this point that it does not apply to arbitrary formulas might seem to present a problem about reaching our general result, that if $\Gamma \vDash \mathcal{P}$ then $\Gamma \vdash \mathcal{P}$, which is supposed to apply in the arbitrary case. But there is a way around the problem. For any formula $\mathcal{P}$, let its (*universal*) *closure* $\mathcal{P}^c$ be $\mathcal{P}$ prefixed by a universal quantifier for every variable free in $\mathcal{P}$. To make $\mathcal{P}^c$ unique, for some enumeration of variables, $x_1, x_2 \ldots$ let the quantifiers be in order of ascending subscripts. So if $\mathcal{P}$ has no free variables, $\mathcal{P}^c = \mathcal{P}$; if x_1 is free in $\mathcal{P}$, then $\mathcal{P}^c = \forall x_1\mathcal{P}$; if x_1 and x_3 are free in $\mathcal{P}$, then $\mathcal{P}^c = \forall x_1 \forall x_3\mathcal{P}$; and so forth. So for any formula $\mathcal{P}$, $\mathcal{P}^c$ is a *sentence*. As it turns out, we will be able to argue about arbitrary formulas $\mathcal{P}$, by using their closures $\mathcal{P}^c$ as intermediaries.

Suppose that the members of $\Gamma \cup \{\sim\mathcal{P}^c\} = \Sigma'$ are formulas of $\mathcal{L}'$. Then it will be sufficient for us to show that any consistent set of this sort has a model.

($\star$) For any consistent set Σ' of formulas in $\mathcal{L}'$, there is an interpretation M' such that $\mathsf{M}'[\Sigma'] = \mathsf{T}$.

Again, this sets up the key connection between syntactic and semantic notions — between consistency on the one hand, and truth on the other — that we will need for adequacy. Supposing ($\star$) we have the following,

1.	$\Gamma \cup \{\sim\mathcal{P}^c\}$ has a model	$\Longrightarrow$	$\Gamma \nvDash \mathcal{P}$	
2.	$\Gamma \cup \{\sim\mathcal{P}^c\}$ is consistent	$\Longrightarrow$	$\Gamma \cup \{\sim\mathcal{P}^c\}$ has a model	($\star$)
3.	$\Gamma \cup \{\sim\mathcal{P}^c\}$ is not consistent	$\Longrightarrow$	$\Gamma \vdash \mathcal{P}$	

(2) is just ($\star$). Observe that (1) and (3) switch between $\mathcal{P}^c$ and $\mathcal{P}$. (1) is by semantic reasoning: Suppose $\Gamma \cup \{\sim\mathcal{P}^c\}$ has a model; then there is some M such that $\mathsf{M}[\Gamma \cup \{\sim\mathcal{P}^c\}] = \mathsf{T}$; so $\mathsf{M}[\Gamma] = \mathsf{T}$ and $\mathsf{M}[\sim\mathcal{P}^c] = \mathsf{T}$; from the latter, by TI, for arbitrary d, $\mathsf{M}_{\mathsf{d}}[\sim\mathcal{P}^c] = \mathsf{S}$; so by SF($\sim$), $\mathsf{M}_{\mathsf{d}}[\mathcal{P}^c] \neq \mathsf{S}$; so by TI, $\mathsf{M}[\mathcal{P}^c] \neq \mathsf{T}$; so by repeated

applications of T7.7 on page 371, $\mathsf{M}[\mathcal{P}] \neq \mathsf{T}$; so $\mathsf{M}[\Gamma] = \mathsf{T}$ and $\mathsf{M}[\mathcal{P}] \neq \mathsf{T}$; so by QV, $\Gamma \not\models \mathcal{P}$. (3) is by syntactic reasoning: Suppose $\Gamma \cup \{\sim\mathcal{P}^c\}$ is not consistent; then since $\mathcal{P}^c$ is a sentence, by an application of T10.6, $\Gamma \vdash \sim\sim\mathcal{P}^c$; but by T3.10, $\vdash \sim\sim\mathcal{P}^c \rightarrow \mathcal{P}^c$; so by MP, $\Gamma \vdash \mathcal{P}^c$; and by repeated applications of A4 and MP, $\Gamma \vdash \mathcal{P}$.

Now suppose $\Gamma \models \mathcal{P}$; then from (1), $\Gamma \cup \{\sim\mathcal{P}^c\}$ does not have a model; so by (2), $\Gamma \cup \{\sim\mathcal{P}^c\}$ is not consistent; so by (3), $\Gamma \vdash \mathcal{P}$. So if $\Gamma \models \mathcal{P}$, then $\Gamma \vdash \mathcal{P}$, and this is the result we want. T7.7, according to which $\mathsf{M}[\mathcal{P}] = \mathsf{T}$ iff $\mathsf{M}[\forall x\mathcal{P}] = \mathsf{T}$, along with A4 and Gen, which let us derive $\mathcal{P}$ from $\forall x\mathcal{P}$ and vice versa, bridge between $\mathcal{P}$ and $\mathcal{P}^c$ so that our suppositions about formulas can be converted into claims about sentences and then back again.

Again, it remains to show $(\star)$, that every consistent set Σ' of formulas has a model. And, again, our strategy is to find a "big" set related to Σ' which can be used to specify a model for Σ'.

10.3.2 Gödel Numbering

As before, in constructing our big sets, we will want to line up expressions serially — one after another. The method merely expands our approach for the sentential case.

T10.7. There is an enumeration $\mathcal{Q}_1$, $\mathcal{Q}_2 \dots$ of all the formulas, terms, and the like, in $\mathcal{L}'$.

The proof is again by construction: We develop a method by which all the expressions of $\mathcal{L}'$ can be lined up. Then the collection of all formulas, taken in that order, is an an enumeration of all formulas; the collection of all terms, taken in that order, is an enumeration of all terms; and so forth.

Insofar as the collections of variable symbols, constant symbols, function symbols, sentence letters, and relation symbols in any quantificational language are countable, they are capable of being sorted into series, x_0, $x_1 \dots$ and a_0, $a_1 \dots$ and h^n_0, $h^n_1 \dots$ and $\mathcal{R}^n_0$, $\mathcal{R}^n_1 \dots$ for variables, constants, function symbols and relation symbols, respectively (where we think of sentence letters as 0-place relation symbols). Supposing that they are sorted into such series, begin by assigning to each symbol α in $\mathcal{L}'$ an integer $g[\alpha]$ called its *Gödel Number*.

a. $g[(] = 3$
b. $g[)] = 5$
c. $g[\sim] = 7$
d. $g[\rightarrow] = 9$
f. $g[\forall] = 13$
g. $g[x_i] = 15 + 10i$
h. $g[a_i] = 17 + 10i$
i. $g[h^n_i] = 19 + 10(2^n \times 3^i)$

*e. $g[=] = 11$ j. $g[\mathcal{R}^n_i] = 21 + 10(2^n \times 3^i)$

Officially, we do not yet have '=' in the language, but it is easy enough to leave it out for now. So, for example, $g[x_0] = 15$, $g[x_1] = 15 + 10 \times 1 = 25$, and $g[\mathcal{R}^2_1] = 21 + 10(2^2 \times 3^1) = 141$.

To see that each symbol gets a distinct Gödel number, first notice th at numbers in different categories cannot overlap: Each of (a) - (f) is obviously distinct and ≤ 13. But (g) - (j) are all greater than 13, and when divided by 10, the remainder is 5 for variables, 7 for constants 9 for function symbols, and 1 for relation symbols; so variables, constants, and function symbols all get different numbers. Second, different symbols get different numbers within the categories. This is obvious except in cases (i) and (j). For these we need to see that each n/i combination results in a different multiplier.

> Suppose this is not so, that there are some combinations n, i and m, j such that $2^n \times 3^i = 2^m \times 3^j$ but $n \neq m$ or $i \neq j$. If $n = m$ then, dividing both sides by 2^n, we get $3^i = 3^j$, so that $i = j$. So suppose $n \neq m$ and, without loss of generality, that $n > m$. Dividing each side by 2^m and 3^i, we get $2^{n-m} = 3^{j-i}$; since $n > m$, $n - m$ is a positive integer; so 2^{n-m} is > 1 and even. But 3^{i-j} is either < 1 or odd. Reject the assumption: if $2^n \times 3^i = 2^m \times 3^j$, then $n = m$ and $i = j$.

So each n/i combination gets a different multiplier, and we conclude that each symbol gets a different Gödel number. (This result is a special case of the Fundamental theorem of Arithmetic treated in the arithmetic fore Gödel numbering and more arithmetic for Gödel numbering references.)

Now, as before, assign Gödel numbers to expressions as follows: Where $\alpha_0, \alpha_1 \ldots \alpha_n$ are the symbols, in order from left to right, in some expression $\mathcal{Q}$,

$$g[\mathcal{Q}] = 2^{g[\alpha_0]} \times 3^{g[\alpha_1]} \times 5^{g[\alpha_2]} \times \ldots \times \pi_n{}^{g[\alpha_n]}$$

where 2, 3, 5... π_n are the first n prime numbers. So, for example, $g[\sim\sim\mathcal{R}^2_1 x_0 x_1] = 2^7 \times 3^7 \times 5^{141} \times 7^{15} \times 11^{25}$ — a relatively large integer (one with over 130 digits)! All the same, it is an integer, and different expressions get different Gödel numbers. Given a Gödel number, we can find the corresponding expression by finding its prime factorization; then if there are seven 2s in the factorization, the first symbol is $\sim$; if there are seven 3s, the second symbol is $\sim$; if there are one hundred forty one 5s, the third symbol is $\mathcal{R}^2_1$; and so forth. Notice that numbers for individual symbols are odd, where numbers for expressions are even.

So we can take the set of all formulas, the set of all terms, or whatever, and order their members according to their Gödel numbers — so that there is an enumeration $\mathcal{Q}_1, \mathcal{Q}_2 \ldots$ of all formulas, terms, and so forth. And this is what was to be shown.

More Arithmetic Relevant to Gödel Numbering

G3. For any $i > 1$, if i is the product of the primes $p_1, p_2 \dots p_a$, then no distinct collection of primes $q_1, q_2 \dots q_b$ is such that i is the product of them. (The *Fundamental Theorem* of Arithmetic)

Basis: The first integer $\geq 1 = 2$; but the only collection of primes such that their product is equal to 2 is the collection containing just 2 itself; so no distinct collection of primes is such that 2 is the product of them.

Assp: For any i, $1 \leq i < k$, if i is the product of primes $p_1 \dots p_a$, then no distinct collection of primes $q_1 \dots q_b$ is such that i is the product of them.

Show: k is such that if it is the product of the primes $p_1 \dots p_a$, then no distinct collection of primes $q_1 \dots q_b$ is such that k is the product of them.

Suppose there are distinct collections of primes $p_1 \dots p_a$ and $q_1 \dots q_b$ such that $k = p_1 \times \dots \times p_a = q_1 \times \dots \times q_b$; divide out terms common to both lists of primes; then for some subclasses of the original lists, $n = p_1 \times \dots \times p_c = q_1 \times \dots \times q_d$, where no member of $p_1 \dots p_c$ is a member of $q_1 \dots q_d$ and *vice versa* (of course this p_1 may be distinct from the one in the original list, and so forth). So $p_1 \neq q_1$; suppose, without loss of generality, that $p_1 > q_1$; and let $m = q_1(n/q_1 - n/p_1) = n - (q_1/p_1)n = n - q_1 \times p_2 \times \dots \times p_c$.

Some preliminary results: (i) $m < n \leq k$; so $m < k$. Further, n/q_1 and n/p_1 are integers, with the first greater than the second; so the difference is an integer > 0; any prime is > 1; so q_1 is > 1; so the product of q_1 and $(n/q_1 - n/p_1)$ is > 1; so $m > 1$. So the inductive assumption applies to m. (ii) q_1 divides n and q_1 divides $q_1 \times p_2 \times \dots \times p_c$; so $[n - q_1 \times p_2 \times \dots \times p_c]/q_1$ is an integer; so m/q_1 is an integer, and q_1 divides m. (iii) $(p_1 - q_1)/q_1 = p_1/q_1 - 1$; since p_1 is prime, this is no integer; so q_1 does not divide $(p_1 - q_1)$.

Notice that $m = (p_1 - q_1)(n/p_1)$; either $p_1 - q_1 = 1$ or it has some prime factorization, and n/p_1 has a prime factorization, $p_2 \times \dots \times p_c$; the product of the factorization(s) is a prime factorization of m. Given the cancellation of common terms to get n, q_1 is not a member of $p_2 \times \dots \times p_c$; by (iii), q_1 is not a member of the factorization of $p_1 - q_1$; so q_1 is not a member of this factorization of m. By (ii), q_1 divides m, and however many times it goes into m, by (G1), that number has a prime factorization; the product of q_1 and this factorization is a prime factorization of m; so q_1 is a member of some prime factorization of m. But by (i), the inductive assumption applies to m; so m has only one prime factorization. Reject the assumption: there are no distinct collections of primes, $p_1 \dots p_a$ and $q_1 \dots q_b$ such that $k = p_1 \times \dots \times p_a = q_1 \times \dots \times q_b$.

Indct: For any $i > 1$, if i is the product of the primes $p_1, p_2 \dots p_a$, then no distinct collection of primes $q_1, q_2 \dots q_b$ is such that i is the product of them.

E10.15. Find Gödel numbers for each of the following. Treat the first as a simple symbol. (For the last, you need not do the calculation!)

$\mathcal{R}^2_3 \qquad h^1_1 x_1 \qquad \forall x_2 \mathcal{R}^2_1 a_2 x_2$

E10.16. Determine the objects that have the following Gödel numbers.

$61 \qquad 2^{13} \times 3^{15} \times 5^3 \times 7^{15} \times 11^{11} \times 13^{15} \times 17^5$

10.3.3 The Big Set

This section, along with the next, constitutes the heart of our demonstration of adequacy. Last time, to build our big set we added formulas to Σ' to form a Σ'' that was both maximal and consistent. A set of formulas is consistent just in case there is no formula $\mathcal{A}$ such that both $\mathcal{A}$ and $\sim\mathcal{A}$ are consequences. To accommodate restrictions from T10.6, maximality is defined in terms of *sentences*.

Max A set Σ of formulas is *maximal* iff for any sentence $\mathcal{A}$, $\Sigma \vdash \mathcal{A}$ or $\Sigma \vdash \sim\mathcal{A}$.

This time, however, we need an additional property for our big sets. If a maximal and consistent set has $\forall x \mathcal{P}$ as a member, then it has $\mathcal{P}^x_a$ as a consequence for every constant a. (Be clear about why this is so.) But in a maximal and consistent set, the status of a universal $\forall x \mathcal{P}$ is not always reflected at the level of its instances. Thus, for example, though a set has $\mathcal{P}^x_a$ as a consequence for every constant a, it may consistently include $\sim\forall x \mathcal{P}$ as well — for it may be that a universal is falsified by some individual to which no constant is assigned. But when we come to showing by induction that there is a model for our big set, it will be important that the status of a universal *is* reflected at the level of its instances. We guarantee this by building the set to satisfy the following condition.

Scgt A set Σ of formulas is a *scapegoat* set iff for any sentence $\sim\forall x \mathcal{P}$, if $\Sigma \vdash \sim\forall x \mathcal{P}$, then there is some constant a such that $\Sigma \vdash \sim\mathcal{P}^x_a$.

Equivalently, Σ is a scapegoat set just in case any sentence $\exists x \mathcal{P}$ is such that if $\Sigma \vdash \exists x \mathcal{P}$, then there is some constant a such that $\Sigma \vdash \mathcal{P}^x_a$. In a scapegoat set, we assert the existence of a particular individual (a *scapegoat*) corresponding to any existential claim. Notice that, since $\sim\forall x \mathcal{P}$ is a sentence, $\sim\mathcal{P}^x_a$ is a sentence too.

So we set out to construct from Σ' a maximal, consistent, scapegoat set. As before, the idea is to line the formulas up, and consider them for inclusion one-by-one. In addition, this time, we consider an enumeration of constants c_1, $c_2 \ldots$ and for any included sentence of the form $\sim\forall x\mathcal{P}$, we include $\sim\mathcal{P}^x_c$ where c is a constant that does not so far appear in the construction. Notice that if, as we have assumed, $\mathcal{L}'$ includes infinitely many constants not in Γ, there are sure to *be* infinitely many constants not already in a Σ' built on Γ.

CnsΣ'' Construct Σ'' from Σ' as follows: By T10.7, there is an enumeration, $\mathcal{Q}_1$, $\mathcal{Q}_2 \ldots$ of all the sentences in $\mathcal{L}'$ and also an enumeration $c_1, c_2 \ldots$ of constants not in Σ'. Let $\Omega_0 = \Sigma'$. Then for any $i > 0$, let

$\Omega_i = \Omega_{i-1}$	if	$\Omega_{i-1} \vdash \sim\mathcal{Q}_i$
else,		
$\Omega_{i*} = \Omega_{i-1} \cup \{\mathcal{Q}_i\}$	if	$\Omega_{i-1} \nvdash \sim\mathcal{Q}_i$
and,		
$\Omega_i = \Omega_{i*}$	if	$\mathcal{Q}_i$ is not of the form $\sim\forall x\mathcal{P}$
$\Omega_i = \Omega_{i*} \cup \{\sim\mathcal{P}^x_c\}$	if	$\mathcal{Q}_i$ is of the form $\sim\forall x\mathcal{P}$; c the first constant not in Ω_{i*}
then,		
$\Sigma'' = \bigcup_{i \geq 0} \Omega_i$ — that is, Σ'' is the union of all the Ω_is		

Beginning with set Σ' ($= \Omega_0$), we consider the sentences in the enumeration $\mathcal{Q}_1$, $\mathcal{Q}_2 \ldots$ one-by-one, adding a sentence just in case its negation is not already derivable. In addition, if $\mathcal{Q}_i$ is of the sort $\sim\forall x\mathcal{P}$, we add an instance of it, using a new constant. This time, Ω_{i*} functions as an intermediate set. Observe that if c is not in Ω_{i*}, then c is not in $\sim\forall x\mathcal{P}$. Σ'' contains all the members of Σ', together with all the formulas added this way.

It remains to show that if Σ' is consistent, then Σ'' is a maximal, consistent, scapegoat set.

T10.8. If Σ' is consistent, then Σ'' is a maximal, consistent, scapegoat set.

The proof comes to showing (a) Σ'' is maximal. (b) If Σ' is consistent then each Ω_i is consistent. From this, (c) if Σ' is consistent then Σ'' is consistent. And (d) if Σ' is consistent, then Σ'' is a scapegoat set. Suppose Σ' is consistent.

(a) Σ'' is maximal. Suppose Σ'' is not maximal. Then there is some sentence $\mathcal{Q}_i$ such that both $\Sigma'' \nvdash \mathcal{Q}_i$ and $\Sigma'' \nvdash \sim\mathcal{Q}_i$. For this i, by construction, each member of Ω_{i-1} is in Σ''; so if $\Omega_{i-1} \vdash \sim\mathcal{Q}_i$ then $\Sigma'' \vdash \sim\mathcal{Q}_i$; but $\Sigma'' \nvdash \sim\mathcal{Q}_i$; so $\Omega_{i-1} \nvdash \sim\mathcal{Q}_i$; so by construction, $\Omega_{i*} = \Omega_{i-1} \cup \{\mathcal{Q}_i\}$; and by construction again, $\mathcal{Q}_i \in \Sigma''$; so $\Sigma'' \vdash \mathcal{Q}_i$. This is impossible; reject the assumption: Σ'' is maximal.

(b) Each Ω_i is consistent. By induction on the series of Ω_is.

Basis: $\Omega_0 = \Sigma'$ and Σ' is consistent; so Ω_0 is consistent.

Assp: For any i, $0 \leq i < k$, Ω_i is consistent.

Show: Ω_k is consistent.

Ω_k is either (i) Ω_{k-1}, (ii) $\Omega_{k*} = \Omega_{k-1} \cup \{\mathcal{Q}_k\}$, or (iii) $\Omega_{k*} \cup \{\sim\mathcal{P}^x_c\}$.

(i) Suppose Ω_k is Ω_{k-1}. By assumption, Ω_{k-1} is consistent; so Ω_k is consistent.

(ii) Suppose Ω_k is $\Omega_{k*} = \Omega_{k-1} \cup \{\mathcal{Q}_k\}$. Then by construction, $\Omega_{k-1} \nvdash \sim\mathcal{Q}_k$; so, since $\mathcal{Q}_k$ is a sentence, by T10.6, $\Omega_{k-1} \cup \{\mathcal{Q}_k\}$ is consistent; so Ω_{k*} is consistent, and Ω_k is consistent.

(iii) Suppose Ω_k is $\Omega_{k*} \cup \{\sim\mathcal{P}^x_c\}$ for c not in Ω_{k*} or in $\sim\forall x\mathcal{P}$. In this case, as in (ii) above, Ω_{k*} is consistent; and, by construction $\sim\forall x\mathcal{P} \in \Omega_{k*}$; so $\Omega_{k*} \vdash \sim\forall x\mathcal{P}$. Suppose Ω_k is inconsistent; then there are formulas $\mathcal{A}$ and $\sim\mathcal{A}$ such that $\Omega_k \vdash \mathcal{A}$ and $\Omega_k \vdash \sim\mathcal{A}$; so $\Omega_{k*} \cup \{\sim\mathcal{P}^x_c\} \vdash \mathcal{A}$ and $\Omega_{k*} \cup \{\sim\mathcal{P}^x_c\} \vdash \sim\mathcal{A}$. But since $\sim\mathcal{P}^x_c$ is a sentence, the restriction on DT is met, and both $\Omega_{k*} \vdash \sim\mathcal{P}^x_c \rightarrow \mathcal{A}$ and $\Omega_{k*} \vdash \sim\mathcal{P}^x_c \rightarrow \sim\mathcal{A}$; by A3, $\vdash (\sim\mathcal{P}^x_c \rightarrow \sim\mathcal{A}) \rightarrow [(\sim\mathcal{P}^x_c \rightarrow \mathcal{A}) \rightarrow \mathcal{P}^x_c]$; so by two instances of MP, $\Omega_{k*} \vdash \mathcal{P}^x_c$.

Consider some derivation of this result; by T10.12, we can switch c for some variable v that does not occur in Ω_{k*} or in the derivation, and the result is a derivation; so $\Omega_{k*}{}^{c}_{v} \vdash [\mathcal{P}^x_c]^c_v$; but since c does not occur in Ω_{k*} or in $\sim\forall x\mathcal{P}$, this is to say, $\Omega_{k*} \vdash \mathcal{P}^x_v$; so by Gen, $\Omega_{k*} \vdash \forall v\mathcal{P}^x_v$; but x is not free in $\forall v\mathcal{P}^x_v$ and x is free for v in $\mathcal{P}^x_v$, so by T3.27, $\vdash \forall v\mathcal{P}^x_v \rightarrow \forall x[\mathcal{P}^x_v]^v_x$; so by MP, $\Omega_{k*} \vdash \forall x[\mathcal{P}^x_v]^v_x$; and since v is not a variable in $\mathcal{P}$, it is not free in $\mathcal{P}$ and free for x in $\mathcal{P}$; so by T8.2, $[\mathcal{P}^x_v]^v_x = \mathcal{P}$; so $\Omega_{k*} \vdash \forall x\mathcal{P}$.

But $\Omega_{k*} \vdash \sim\forall x\mathcal{P}$. So Ω_{k*} is inconsistent. This is impossible; reject the assumption: Ω_k is consistent.

Ω_k is consistent

Indct: For any i, Ω_i is consistent.

(c) Σ'' is consistent. Suppose Σ'' is not consistent; then there is some $\mathcal{A}$ such that $\Sigma'' \vdash \mathcal{A}$ and $\Sigma'' \vdash \sim\mathcal{A}$. Consider derivations *D1* and *D2* of these results, and the premises $\mathcal{Q}_i \ldots \mathcal{Q}_j$ of these derivations. Where $\mathcal{Q}_j$ is the last of these premises in the enumeration of formulas, by the construction of Σ'', each of $\mathcal{Q}_i \ldots \mathcal{Q}_j$ must be a member of Ω_j; so *D1* and *D2* are derivations from Ω_j; so Ω_j is inconsistent. But by the previous result, Ω_j is consistent. This is impossible; reject the assumption: Σ'' is consistent.

(d) Σ'' is a scapegoat set. Suppose $\Sigma'' \vdash \mathcal{Q}_i$, for $\mathcal{Q}_i$ of the form $\sim\forall x\mathcal{P}$. By (c), Σ'' is consistent; so $\Sigma'' \nvdash \sim\sim\forall x\mathcal{P}$; which is to say, $\Sigma'' \nvdash \sim\mathcal{Q}_i$; so, $\Omega_{i-1} \nvdash \sim\mathcal{Q}_i$; so by construction, $\Omega_{i*} = \Omega_{i-1} \cup \{\sim\forall x\mathcal{P}\}$ and $\Omega_i = \Omega_{i*} \cup \{\sim\mathcal{P}^x_c\}$; so by construction, $\sim\mathcal{P}^x_c \in \Sigma''$; so $\Sigma'' \vdash \sim\mathcal{P}^x_c$. So if $\Sigma'' \vdash \sim\forall x\mathcal{P}$, then $\Sigma'' \vdash \sim\mathcal{P}^x_c$, and Σ'' is a scapegoat set.

In a pattern that should be familiar by now, we guarantee maximal scapegoat sets, by including instances as required. The most difficult case is (iii) for consistency. Having shown that $\Omega_{k*} \vdash \mathcal{P}^x_c$ for c not in Ω_{k*} or in $\mathcal{P}$, we want to generalize to show that $\Omega_{k*} \vdash \forall x\mathcal{P}$. But, in our derivation systems, generalization is on variables, not constants. To get the generalization we want, we first use T10.12 to replace c with an arbitrary variable v. From this, we might have moved immediately to $\forall x\mathcal{P}$ by the *ND* rule $\forall$I. However, in the above reasoning, we stick with the pattern of *AD* rules, applying Gen, and then T3.27 to switch bound variables, for the desired result, that contradicts $\sim\forall x\mathcal{P}$.

E10.17. Let $\Sigma' = \{\forall x{\sim}Bx, Ca\}$ and consider enumerations of sentences and extra constants in $\mathcal{L}'$ that begin, Aa, Ba, $\sim\forall xCx \ldots$ and $c_1, c_2 \ldots$. What are Ω_0, Ω_{1*}, Ω_1, Ω_{2*}, Ω_2, Ω_{3*}, Ω_3? Produce a model to show that the resultant set Ω_3 is consistent.

E10.18. Suppose some $\Omega_{i-1} = \{Ac_2, \forall x(Ax \rightarrow Bx)\}$. Show that Ω_{i*} is consistent, but Ω_i is not, if $\mathcal{Q}_i = \sim\forall xBx$, and we add $\sim\forall xBx$ with $\sim Bc_2$ to form Ω_{i*} and Ω_i. Why cannot this happen in the construction of Σ''?

10.3.4 The Model

We turn now to constructing the model M' for Σ'. As it turns out, the construction is simplified by our assumption that '=' does not appear in the language. A quantificational interpretation has a universe, with assignments to sentence letters, constants, function symbols, and relation symbols.

CnsM$'$ Let the universe U be the set of positive integers, $\{1, 2 \ldots\}$. Then, where a *variable-free* term consists just of function symbols and constants, consider an enumeration t_1, $t_2 \ldots$ of all the variable-free terms in $\mathcal{L}'$. If t_z is a constant, set $\mathsf{M}'[t_z] = \mathsf{z}$. If $t_z = h^n t_a \ldots t_b$ for some function symbol h^n and n variable-free terms $t_a \ldots t_b$, then let $\langle\langle \mathsf{a} \ldots \mathsf{b}\rangle, \mathsf{z}\rangle \in \mathsf{M}'[h^n]$. For a sentence letter $\mathcal{S}$, let $\mathsf{M}'[\mathcal{S}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{S}$. And for a relation symbol $\mathcal{R}^n$, let $\langle \mathsf{a} \ldots \mathsf{b}\rangle \in \mathsf{M}'[\mathcal{R}^n]$ iff $\Sigma'' \vdash \mathcal{R}^n t_a \ldots t_b$.[3]

Thus, for example, where t_1 and t_3 from the enumeration of terms are constants and $\Sigma'' \vdash \mathcal{R} t_1 t_3$, then $\mathsf{M}'[t_1] = 1$, $\mathsf{M}'[t_3] = 3$ and $\langle 1, 3\rangle \in \mathsf{M}'[\mathcal{R}]$. Given this, it should be clear *why* $\mathcal{R} t_1 t_3$ comes out satisfied on M$'$: Put generally, where $t_a \ldots t_b$ are constants, we set $\mathsf{M}'[t_a] = \mathsf{a}$, and ... and $\mathsf{M}'[t_b] = \mathsf{b}$; so by TA(c), for any variable assignment d, $\mathsf{M}'_\mathsf{d}[t_a] = \mathsf{a}$, and ... and $\mathsf{M}'_\mathsf{d}[t_b] = \mathsf{b}$. So by SF(r), $\mathsf{M}'_\mathsf{d}[\mathcal{R}^n t_a \ldots t_b] = \mathsf{S}$ iff $\langle \mathsf{a} \ldots \mathsf{b}\rangle \in \mathsf{M}'[\mathcal{R}^n]$; by construction, iff $\Sigma'' \vdash \mathcal{R}^n t_a \ldots t_b$. Just as in the sentential case, our idea is to make atomic sentences true on M$'$ just in case they are proved by Σ''.

Our aim has been to show that if Σ' is consistent, then Σ' has a model. We have constructed an interpretation M$'$, and now show what sentences are true on it. As in the sentential case, the main weight is carried by a preliminary theorem. And, as in the sentential case, the key is that we can appeal to special features of Σ'', this time that it is a maximal, consistent, scapegoat set. Notice that $\mathcal{B}$ is a *sentence*.

T10.9. If Σ' is consistent, then for any sentence $\mathcal{B}$ of $\mathcal{L}'$, $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

Suppose Σ' is consistent and $\mathcal{B}$ is a sentence of $\mathcal{L}'$. By T10.8, Σ'' is a maximal, consistent, scapegoat set. We begin with a preliminary result, which connects arbitrary variable-free terms to our treatment of constants in the example above: for any variable-free term t_z and variable assignment d, $\mathsf{M}'_\mathsf{d}[t_z] = \mathsf{z}$.

Suppose t_z is a variable-free term and d is an arbitrary variable assignment. By induction on the number of function symbols in t_z, $\mathsf{M}'_\mathsf{d}[t_z] = \mathsf{z}$.

Basis: If t_z has no function symbols, then it is a constant. In this case, by construction, $\mathsf{M}'[t_z] = \mathsf{z}$; so by TA(c), $\mathsf{M}'_\mathsf{d}[t_z] = \mathsf{z}$.

Assp: For any i, $0 \leq i < k$, if t_z has i function symbols, then $\mathsf{M}'_\mathsf{d}[t_z] = \mathsf{z}$.

[3] It is common to let U just be the set of variable-free terms in $\mathcal{L}'$, and the interpretation of a term be itself. There is nothing the matter with this. However, working with the integers emphasizes continuity with other models we have seen, and positions us for further results.

Show: If t_z has k function symbols, then $\mathsf{M}'_{\mathsf{d}}[t_z] = \mathsf{z}$.

If t_z has k function symbols, then it is of the form $h^n t_a \dots t_b$ for function symbol h^n and variable-free terms $t_a \dots t_b$ each with $< k$ function symbols. By TA(f), $\mathsf{M}'_{\mathsf{d}}[t_z] = \mathsf{M}'_{\mathsf{d}}[h^n t_a \dots t_b] = \mathsf{M}'[h^n]\langle \mathsf{M}'_{\mathsf{d}}[t_a] \dots \mathsf{M}'_{\mathsf{d}}[t_b]\rangle$; but by assumption, $\mathsf{M}'_{\mathsf{d}}[t_a] = \mathsf{a}$, and ...and $\mathsf{M}'_{\mathsf{d}}[t_b] = \mathsf{b}$; so $\mathsf{M}'_{\mathsf{d}}[t_z] = \mathsf{M}'[h^n]\langle \mathsf{a} \dots \mathsf{b}\rangle$. But since $t_z = h^n t_a \dots t_b$ is a variable-free term, by construction, $\langle\langle \mathsf{a} \dots \mathsf{b}\rangle, \mathsf{z}\rangle \in \mathsf{M}'[h^n]$; so we have $\mathsf{M}'_{\mathsf{d}}[t_z] = \mathsf{M}'[h^n]\langle \mathsf{a} \dots \mathsf{b}\rangle = \mathsf{z}$.

Indct: For any t_z, $\mathsf{M}'_{\mathsf{d}}[t_z] = \mathsf{z}$.

Given this, we are ready to show, by induction on the number of operators in $\mathcal{B}$, that $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$. Suppose $\mathcal{B}$ is a sentence.

Basis: If $\mathcal{B}$ is a sentence with no operators, then it is a sentence letter $\mathcal{S}$, or an atomic $\mathcal{R}^n t_a \dots t_b$ for relation symbol $\mathcal{R}^n$ and variable-free terms $t_a \dots t_b$. In the first case, by construction, $\mathsf{M}'[\mathcal{S}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{S}$. In the second case, by TI, $\mathsf{M}'[\mathcal{R}^n t_a \dots t_b] = \mathsf{T}$ iff for arbitrary d, $\mathsf{M}'_{\mathsf{d}}[\mathcal{R}^n t_a \dots t_b] = \mathsf{S}$; by SF(r), iff $\langle \mathsf{M}'_{\mathsf{d}}[t_a] \dots \mathsf{M}'_{\mathsf{d}}[t_b]\rangle \in \mathsf{M}'[\mathcal{R}^n]$; since $t_a \dots t_b$ are variable-free terms, by the above result, iff $\langle \mathsf{a} \dots \mathsf{b}\rangle \in \mathsf{M}'[\mathcal{R}^n]$; by construction, iff $\Sigma'' \vdash \mathcal{R}^n t_a \dots t_b$. In either case, then, $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

Assp: For any i, $0 \leq i < k$ if a sentence $\mathcal{B}$ has i operator symbols, then $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

Show: If a sentence $\mathcal{B}$ has k operator symbols, then $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

If $\mathcal{B}$ has k operator symbols, then it is of the form, $\sim\mathcal{P}$, $\mathcal{P} \to \mathcal{Q}$ or $\forall x \mathcal{P}$, for variable x and $\mathcal{P}$ and $\mathcal{Q}$ with $< k$ operator symbols.

($\sim$) Suppose $\mathcal{B}$ is $\sim\mathcal{P}$. Homework. Hint: given T8.6, your reasoning may be very much as in the sentential case.

($\to$) Suppose $\mathcal{B}$ is $\mathcal{P} \to \mathcal{Q}$. Homework.

($\forall$) Suppose $\mathcal{B}$ is $\forall x \mathcal{P}$. Then since $\mathcal{B}$ is a sentence, x is the only variable that could be free in $\mathcal{P}$.

(i) Suppose $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ but $\Sigma'' \nvdash \mathcal{B}$; from the latter, $\Sigma'' \nvdash \forall x \mathcal{P}$; since Σ'' is maximal, $\Sigma'' \vdash \sim\forall x \mathcal{P}$; and since Σ'' is a scapegoat set, for some constant c, $\Sigma'' \vdash \sim\mathcal{P}^x_c$; so by consistency, $\Sigma'' \nvdash \mathcal{P}^x_c$; but $\mathcal{P}^x_c$ is a sentence; so by assumption, $\mathsf{M}'[\mathcal{P}^x_c] \neq \mathsf{T}$; so by TI, for some d, $\mathsf{M}'_{\mathsf{d}}[\mathcal{P}^x_c] \neq \mathsf{S}$; but, where c is some t_a, by construction, $\mathsf{M}'[c] = \mathsf{a}$; so by TA(c), $\mathsf{M}'_{\mathsf{d}}[c] = \mathsf{a}$; so, since c is free for x in $\mathcal{P}$, by T10.2,

$\mathsf{M}'_{\mathsf{d}(x|\mathsf{a})}[\mathcal{P}] \neq \mathsf{S}$; so by SF($\forall$), $\mathsf{M}'_{\mathsf{d}}[\forall x \mathcal{P}] \neq \mathsf{S}$; so by TI, $\mathsf{M}'[\forall x \mathcal{P}] \neq \mathsf{T}$; and this is just to say, $\mathsf{M}'[\mathcal{B}] \neq \mathsf{T}$. But this is impossible; reject the assumption: if $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$, then $\Sigma'' \vdash \mathcal{B}$.

(ii) Suppose $\Sigma'' \vdash \mathcal{B}$ but $\mathsf{M}'[\mathcal{B}] \neq \mathsf{T}$; from the latter, $\mathsf{M}'[\forall x \mathcal{P}] \neq \mathsf{T}$; so by TI, there is some d such that $\mathsf{M}'_{\mathsf{d}}[\forall x \mathcal{P}] \neq \mathsf{S}$; so by SF($\forall$), there is some $\mathsf{a} \in \mathsf{U}$ such that $\mathsf{M}'_{\mathsf{d}(x|\mathsf{a})}[\mathcal{P}] \neq \mathsf{S}$; but for variable-free term t_a, by our above result, $\mathsf{M}'_{\mathsf{d}}[t_a] = \mathsf{a}$, and since t_a is variable-free, it is free for x in $\mathcal{P}$, so by T10.2, $\mathsf{M}'_{\mathsf{d}}[\mathcal{P}^x_{t_a}] \neq \mathsf{S}$; so by TI, $\mathsf{M}'[\mathcal{P}^x_{t_a}] \neq \mathsf{T}$; but $\mathcal{P}^x_{t_a}$ is a sentence; so by assumption, $\Sigma'' \nvdash \mathcal{P}^x_{t_a}$; so by the maximality of Σ'', $\Sigma'' \vdash \sim\mathcal{P}^x_{t_a}$; but t_a is free for x in $\mathcal{P}$, so by A4, $\vdash \forall x \mathcal{P} \to \mathcal{P}^x_{t_a}$; and by T3.13, $\vdash (\forall x \mathcal{P} \to \mathcal{P}^x_{t_a}) \to (\sim\mathcal{P}^x_{t_a} \to \sim\forall x \mathcal{P})$; so by a couple instances of MP, $\Sigma'' \vdash \sim\forall x \mathcal{P}$; so by the consistency of Σ'', $\Sigma'' \nvdash \forall x \mathcal{P}$; which is to say, $\Sigma'' \nvdash \mathcal{B}$. This is impossible; reject the assumption: if $\Sigma'' \vdash \mathcal{B}$, then $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$.

If $\mathcal{B}$ has k operator symbols, then $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

Indct: For any sentence $\mathcal{B}$, $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

So if Σ' is consistent, then for any sentence $\mathcal{B}$ of $\mathcal{L}'$, $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$. We are now just one step away from ($\star$). It will be easy to see that $\mathsf{M}'[\Sigma'] = \mathsf{T}$, and so to reach the final result.

E10.19. Complete the $\sim$ and $\to$ cases to complete the demonstration of T10.9. You should set up the complete demonstration, but may refer to the text for cases completed there, as the text refers cases to homework.

10.3.5 Final Result

And now we are in a position to get the final result. This works just as before. First,

T10.10. If Σ' is consistent, then $\mathsf{M}'[\Sigma'] = \mathsf{T}$. ($\star$)

Suppose Σ' is consistent, but $\mathsf{M}'[\Sigma'] \neq \mathsf{T}$. From the latter, there is some formula $\mathcal{B} \in \Sigma'$ such that $\mathsf{M}'[\mathcal{B}] \neq \mathsf{T}$. Since $\mathcal{B} \in \Sigma'$, by construction, $\mathcal{B} \in \Sigma''$, so $\Sigma'' \vdash \mathcal{B}$; so, where $\mathcal{B}^c$ is the universal closure of $\mathcal{B}$, by application of Gen as necessary, $\Sigma'' \vdash \mathcal{B}^c$; so since Σ' is consistent, by T10.9, $\mathsf{M}'[\mathcal{B}^c] = \mathsf{T}$; so by applications of T7.7 as necessary, $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$. This is impossible; reject the assumption: if Σ' is consistent, then $\mathsf{M}'[\Sigma'] = \mathsf{T}$.

Notice that this result applies to arbitrary sets of *formulas*. We are able to bridge between formulas and sentences by T10.7 and Gen. But now we have the $(\star)$ that we have needed for adequacy.

So that is it! All we needed for the proof of adequacy was $(\star)$. And we have it. So here is the final argument. Suppose the members of Γ and $\mathcal{P}$ are formulas of $\mathcal{L}'$.

T10.11. If $\Gamma \vDash \mathcal{P}$, then $\Gamma \vdash \mathcal{P}$. (*quantificational adequacy*)

Suppose $\Gamma \vDash \mathcal{P}$ but $\Gamma \nvdash \mathcal{P}$. Say, for the moment that $\Gamma \vdash \sim\sim\mathcal{P}^c$; by T3.10, $\vdash \sim\sim\mathcal{P}^c \to \mathcal{P}^c$; so by MP, $\Gamma \vdash \mathcal{P}^c$; so by repeated applications of A4 and MP, $\Gamma \vdash \mathcal{P}$; but this is impossible; so $\Gamma \nvdash \sim\sim\mathcal{P}^c$. Given this, since $\sim\sim\mathcal{P}^c$ is a sentence, by T10.6, $\Gamma \cup \{\sim\mathcal{P}^c\} = \Sigma'$ is consistent; so by T10.10, there is a model M' constructed as above such that $\mathsf{M}'[\Sigma'] = \mathsf{T}$. So $\mathsf{M}'[\Gamma] = \mathsf{T}$ and $\mathsf{M}'[\sim\mathcal{P}^c] = \mathsf{T}$; from the latter, by T8.6, $\mathsf{M}'[\mathcal{P}^c] \neq \mathsf{T}$; so by repeated applications of T7.7, $\mathsf{M}'[\mathcal{P}] \neq \mathsf{T}$; so by QV, $\Gamma \nvDash \mathcal{P}$. This is impossible; reject the assumption: if $\Gamma \vDash \mathcal{P}$ then $\Gamma \vdash \mathcal{P}$.

Again, you should try to get the complete picture in your mind: The key is that consistent sets always have models. If $\Gamma \cup \{\sim\mathcal{P}\}$ is not consistent, then there is a derivation of $\mathcal{P}$ from Γ. So if there is no derivation of $\mathcal{P}$ from Γ, $\Gamma \cup \{\sim\mathcal{P}\}$ is consistent and so must have a model — with the result that $\Gamma \nvDash \mathcal{P}$. We get the key point, that consistent sets have models, by finding a relation between consistent, and *maximal*, consistent, scapegoat sets. If a set is maximal and consistent and a scapegoat set, then it contains enough information to specify a model for the whole. The model for the big set then guarantees the existence of a model M for the original Γ. All of this is very much parallel to the sentential case.

E10.20. Consider a quantificational language $\mathcal{L}$ which has function symbols as usual but with $\wedge$, $\sim$, and $\exists$ as primitive operators. Suppose axioms and rules are as in *A4* of E10.3 on p. 473. You may suppose there is no symbol for equality, and there are infinitely many constants not in Γ. Provide a complete demonstration that *A4* is adequate. You may appeal to any results from the text whose demonstration remains unchanged, but should recreate parts whose demonstration is not the same.

Hints: As preliminaries you will need revised versions of DT and T10.12. In addition, a few quick theorems for derivations, along with an analog to one side of T7.7 might be helpful,

(a) $\vdash \exists y \mathcal{P}^x_y \to \exists x \mathcal{P}$ $\quad$ y free for x in $\mathcal{P}$ and not free in $\exists x \mathcal{P}$

(b) $\vdash \sim\exists x\mathcal{P} \rightarrow \sim\exists y\mathcal{P}^x_y$ $\quad$ y free for x in $\mathcal{P}$ and not free in $\exists x\mathcal{P}$

(c) $\sim\mathcal{P}^x_v \vdash \sim\exists x\mathcal{P}$ $\quad$ use $\exists$E with $\mathcal{Q}$ some $X \wedge \sim X$; note that $\vDash \sim(X \wedge \sim X)$

(7.6*) If $\mathsf{I}[\sim\exists x\mathcal{P}] = \mathsf{T}$ then $\mathsf{I}[\sim\mathcal{P}] = \mathsf{T}$

Then redefine key notions (such as 'scapegoat set') in terms of the existential quantifier, so that you can work cases directly within the new system. Say $\mathcal{P}^e$ is the *existential* closure of $\mathcal{P}$. Note that $\sim(\sim\mathcal{P})^e$ is equivalent to $\mathcal{P}^c$ (imagine replacing all the added universal quantifiers in $\mathcal{P}^c$ with $\sim\exists x\sim$ and using DN on inner double tildes). This will help with T10.10 and T10.11.

10.4 Quantificational Adequacy: Full Version

So far, we have shown that if $\Gamma \vDash \mathcal{P}$, then $\Gamma \vdash \mathcal{P}$ where the members of Γ and $\mathcal{P}$ are formulas of $\mathcal{L}'$. Now allow that the members of Γ and $\mathcal{P}$ are in an arbitrary quantificational language $\mathcal{L}$. Then we we shall require require not $(\star)$ with application just to $\mathcal{L}'$, but the more general,

($\star\star$) For any consistent set of formulas Σ, there is an interpretation M such that $\mathsf{M}[\Sigma] = \mathsf{T}$.

Given this, reasoning is exactly as before.

1.	$\Gamma \cup \{\sim\mathcal{P}^c\}$ has a model	$\Longrightarrow$	$\Gamma \nvDash \mathcal{P}$	
2.	$\Gamma \cup \{\sim\mathcal{P}^c\}$ is consistent	$\Longrightarrow$	$\Gamma \cup \{\sim\mathcal{P}^c\}$ has a model	$(\star\star)$
3.	$\Gamma \cup \{\sim\mathcal{P}^c\}$ is not consistent	$\Longrightarrow$	$\Gamma \vdash \mathcal{P}$	

Reasoning for (1) and (3) remains the same. (2) is $(\star\star)$. Now suppose $\Gamma \vDash \mathcal{P}$; then from (1), $\Gamma \cup \{\sim\mathcal{P}^c\}$ does not have a model; so by (2), $\Gamma \cup \{\sim\mathcal{P}^c\}$ is not consistent; so by (3), $\Gamma \vdash \mathcal{P}$. So if $\Gamma \vDash \mathcal{P}$, then $\Gamma \vdash \mathcal{P}$. Supposing that $(\star\star)$ has application to arbitrary sets of formulas, the result has application to arbitrary premises and conclusion. So we are left with two issues relative to our reasoning from before: $\mathcal{L}$ might lack the infinitely many constants not in the premises, and $\mathcal{L}$ might include equality.

10.4.1 Adding Constants

Suppose $\mathscr{L}$ does not have infinitely many constants not in Γ. This can happen in different ways. Perhaps $\mathscr{L}$ simply does not have infinitely many constants. Or perhaps the constants of $\mathscr{L}$ are a_1, $a_2 \ldots$ and $\Gamma = \{\mathcal{R}a_1, \mathcal{R}a_2 \ldots\}$; then $\mathscr{L}$ has infinitely many constants, but there are not any constants in $\mathscr{L}$ that do not appear in Γ. And we need the extra constants for construction of the maximal, consistent, scapegoat set. To avoid this sort of worry, we simply *add* infinitely many constants to form a language $\mathscr{L}'$ out of $\mathscr{L}$.

Cns$\mathscr{L}'$ Where $\mathscr{L}$ is a language whose constants are some of a_1, $a_2 \ldots$ let $\mathscr{L}'$ be like $\mathscr{L}$ but with the addition of new constants c_1, $c_2 \ldots$

By reasoning as in the countability reference on p. 36, insofar as they can be lined up, a_1, c_1, a_2, $c_2 \ldots$ the collection of constants remains countable, so that $\mathscr{L}'$ remains a perfectly legitimate quantificational language. Clearly, every formula of $\mathscr{L}$ remains a formula of $\mathscr{L}'$. Thus, where Σ is a set of formulas in language $\mathscr{L}$, let Σ' be like Σ except that its members are formulas of language $\mathscr{L}'$.

Our reasoning for ($\star$) has application to sets of the sort Σ'. That is, where $\mathscr{L}'$ has infinitely many constants not in Σ', we have been able to find a maximal, consistent, scapegoat set Σ'', and from this a model M' for Σ'. But, give an arbitrary Σ of formulas in $\mathscr{L}$, we need that *it* has a model M. That is, we shall have to establish a bridge between Σ and Σ', and between M' and M. Thus, to obtain ($\star\star$), we show,

2a.	Σ is consistent	$\Longrightarrow$	Σ' is consistent
2b.	Σ' is consistent	$\Longrightarrow$	Σ' has a model M'
2c.	Σ' has a model M'	$\Longrightarrow$	Σ has a model M

(2b) is just ($\star$) from before. And by a sort of hypothethical syllogism, together these yield ($\star\star$).

For the first result, we need that if Σ is consistent, then Σ' is consistent. Of course, Σ and Σ' contain just the same formulas, only sentences of the one are in a language with extra constants. But there might be *derivations* in $\mathscr{L}'$ from Σ' that are not derivations in $\mathscr{L}$ from Σ. So we need to show that these extra derivations do not result in contradiction. For this, the overall idea is simple: If we can derive a contradiction from Σ' in the enriched language then, by a modified version of that very derivation, we can derive a contradiction from Σ in the reduced language. So if there is no contradiction in the reduced language $\mathscr{L}$, then there can be no contradiction in the enriched language $\mathscr{L}'$. The argument is straightforward, given the preliminary result T10.12. Let Σ be a set of formulas in $\mathscr{L}$, and Σ' those same formulas in $\mathscr{L}'$. We show,

T10.13. If Σ is consistent, then Σ' is consistent.

Suppose Σ is consistent. If Σ' is not consistent, then there is a formula $\mathcal{A}$ in $\mathscr{L}'$ such that $\Sigma' \vdash \mathcal{A}$ and $\Sigma' \vdash \sim\mathcal{A}$; but by T9.4, $\vdash \mathcal{A} \to [\sim\mathcal{A} \to (\mathcal{A} \wedge \sim\mathcal{A})]$; so by two instances of MP, $\Sigma' \vdash \mathcal{A} \wedge \sim\mathcal{A}$. So if Σ' is not consistent, there is a derivation of a contradiction from Σ'. By induction on the number of new constants which appear in a derivation $D = \langle \mathcal{B}_1, \mathcal{B}_2 \ldots \rangle$, we show that no such D is a derivation of a contradiction from Σ'.

Basis: Suppose D contains no new constants and D is a derivation of some contradiction $\mathcal{A} \wedge \sim\mathcal{A}$ from Σ'. Since D contains no new constants, every member of D is also a formula of $\mathscr{L}$, so $D = \langle \mathcal{B}_1, \mathcal{B}_2 \ldots \rangle$ is a derivation of $\mathcal{A} \wedge \sim\mathcal{A}$ from Σ; so by T3.19 and T3.20 with MP, $\Sigma \vdash \mathcal{A}$ and $\Sigma \vdash \sim\mathcal{A}$; so Σ is not consistent. This is impossible; reject the assumption: D is not a derivation of a contradiction from Σ'.

Assp: For any i, $0 \leq i < k$, if D contains i new constants, then it is not a derivation of a contradiction from Σ'.

Show: If D contains k new constants, then it is not a derivation of a contradiction from Σ'.

Suppose D contains k new constants and is a derivation of a contradiction $\mathcal{A} \wedge \sim\mathcal{A}$ from Σ'. Where c is one of the new constants in D and x is a variable not in D, by T10.12, D^c_x is a derivation of $[\mathcal{A} \wedge \sim\mathcal{A}]^c_x$ from Σ'^c_x. But all the members of Σ' are in $\mathscr{L}$; so c does not appear in any member of Σ'; so $\Sigma'^c_x = \Sigma'$. And $[\mathcal{A} \wedge \sim\mathcal{A}]^c_x = \mathcal{A}^c_x \wedge \sim[\mathcal{A}^c_x]$. So D^c_x is a derivation of a contradiction from Σ'. But D^c_x has $k-1$ new constants and so, by assumption, is not a derivation of a contradiction from Σ'. This is impossible; reject the assumption: D is not a derivation of a contradiction from Σ'.

Indct: No derivation D is a derivation of a contradiction from Σ'.

So if Σ is consistent, then Σ' is consistent. So if we have a consistent set of sentences in $\mathscr{L}$, and convert to $\mathscr{L}'$ with additional constants, we can be sure that the converted set is consistent as well.

With the extra constants in-hand, all our reasoning goes through as before to show that there is a model M' for Σ'. Officially, though, an interpretation for some sentences in $\mathscr{L}'$ is not a model for some sentences in $\mathscr{L}$: a model for sentences in $\mathscr{L}$ has assignments for its constants, function symbols and relation symbols, where a model for $\mathscr{L}'$ has assignments for *its* constants, function symbols and relation symbols. A model M' for Σ', then, is not the same as a model M for Σ. But it is a short step to a solution.

CnsM Let M be like M' but without assignments to constants not in $\mathscr{L}$.

M is an interpretation for language $\mathscr{L}$. M and M' have exactly the same universe of discourse, and exactly the same interpretations for all the symbols that are in $\mathscr{L}$. It turns out that the evaluation of any formula in $\mathscr{L}$ is therefore the same on M as on M' — that is, for any $\mathscr{P}$ in $\mathscr{L}$, $\mathsf{M}[\mathscr{P}] = \mathsf{T}$ iff $\mathsf{M}'[\mathscr{P}] = \mathsf{T}$. Perhaps this is obvious. However, it is worthwhile to consider a proof. Thus we need the following matched pair of theorems (in fact, we show somewhat more than is necessary, as M and M' differ only by assignments to constants). The proofs are straightforward, and mostly left as an exercise. I do just enough to get you started.

Suppose $\mathscr{L}'$ extends $\mathscr{L}$ and M' is like M except that it makes assignments to constants, functions symbols and relation symbols in $\mathscr{L}'$ but not in $\mathscr{L}$.

T10.14. For any variable assignment d, and for any term t in $\mathscr{L}$, $\mathsf{M_d}[t] = \mathsf{M'_d}[t]$.

The argument is by induction on the number of function symbols in t. Let d be a variable assignment, and t a term in $\mathscr{L}$.

Basis: Homework

Assp: For any i, $0 \leq i < k$, if t has i function symbols, then $\mathsf{M_d}[t] = \mathsf{M'_d}[t]$.

Show: If t has k function symbols, then $\mathsf{M_d}[t] = \mathsf{M'_d}[t]$.

If t has k function symbols, then it is of the form, $h^n t_1 \ldots t_n$ for function symbol h^n and terms $t_1 \ldots t_n$ with $< k$ function symbols. By TA(f), $\mathsf{M_d}[t] = \mathsf{M_d}[h^n t_1 \ldots t_n] = \mathsf{M}[h^n]\langle \mathsf{M_d}[t_1] \ldots \mathsf{M_d}[t_n]\rangle$; similarly, $\mathsf{M'_d}[t] = \mathsf{M'_d}[h^n t_1 \ldots t_n] = \mathsf{M'}[h^n]\langle \mathsf{M'_d}[t_1] \ldots \mathsf{M'_d}[t_n]\rangle$. But by assumption, $\mathsf{M_d}[t_1] = \mathsf{M'_d}[t_1]$, and ... and $\mathsf{M_d}[t_n] = \mathsf{M'_d}[t_n]$; and by construction, $\mathsf{M}[h^n] = \mathsf{M'}[h^n]$; so $\mathsf{M}[h^n]\langle \mathsf{M_d}[t_1] \ldots \mathsf{M_d}[t_n]\rangle = \mathsf{M'}[h^n]\langle \mathsf{M'_d}[t_1] \ldots \mathsf{M'_d}[t_n]\rangle$; so $\mathsf{M_d}[t] = \mathsf{M'_d}[t]$.

Indct: For any t in $\mathscr{L}$, $\mathsf{M_d}[t] = \mathsf{M'_d}[t]$.

T10.15. For any variable assignment d, and for any formula $\mathscr{P}$ in $\mathscr{L}$, $\mathsf{M_d}[\mathscr{P}] = \mathsf{S}$ iff $\mathsf{M'_d}[\mathscr{P}] = \mathsf{S}$.

The argument is by induction on the number of operator symbols in $\mathcal{P}$. Let d be a variable assignment, and $\mathcal{P}$ a formula in $\mathcal{L}$.

Basis: If $\mathcal{P}$ has no operator symbols, then it is a sentence letter $\mathcal{S}$ or an atomic $\mathcal{R}^n t_1 \dots t_n$ for relation symbol $\mathcal{R}^n$ and terms $t_1 \dots t_n$ in $\mathcal{L}$. In the first case, by SF(s), $\mathsf{M_d}[\mathcal{S}] = \mathsf{S}$ iff $\mathsf{M}[\mathcal{S}] = \mathsf{T}$; by construction, iff $\mathsf{M'}[\mathcal{S}] = \mathsf{T}$; by SF(s), iff $\mathsf{M'_d}[\mathcal{S}] = \mathsf{S}$. In the second case, by SF(r), $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M_d}[\mathcal{R}^n t_1 \dots t_n] = \mathsf{S}$; iff $\langle \mathsf{M_d}[t_1] \dots \mathsf{M_d}[t_n]\rangle \in \mathsf{M}[\mathcal{R}^n]$; similarly, $\mathsf{M'_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M'_d}[\mathcal{R}^n t_1 \dots t_n] = \mathsf{S}$; iff $\langle \mathsf{M'_d}[t_1] \dots \mathsf{M'_d}[t_n]\rangle \in \mathsf{M'}[\mathcal{R}^n]$. But by T10.14, $\mathsf{M_d}[t_1] = \mathsf{M'_d}[t_1]$, and ... and $\mathsf{M_d}[t_n] = \mathsf{M'_d}[t_n]$; and by construction, $\mathsf{M}[\mathcal{R}^n] = \mathsf{M'}[\mathcal{R}^n]$; so $\langle \mathsf{M_d}[t_1] \dots \mathsf{M_d}[t_n]\rangle \in \mathsf{M}[\mathcal{R}^n]$ iff $\langle \mathsf{M'_d}[t_1] \dots \mathsf{M'_d}[t_n]\rangle \in \mathsf{M'}[\mathcal{R}^n]$; so $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M'_d}[\mathcal{P}] = \mathsf{S}$.

Assp: For any i, $0 \le i < k$, and any variable assignment d, if $\mathcal{P}$ has i operator symbols, $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M'_d}[\mathcal{P}] = \mathsf{S}$.

Show: Homework

Indct: For any formula $\mathcal{P}$ of $\mathcal{L}$, $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M'_d}[\mathcal{P}] = \mathsf{S}$.

And now we are in a position to show that M is indeed a model for Σ. In particular, it is easy to show,

T10.16. If $\mathsf{M'}[\Sigma'] = \mathsf{T}$, then $\mathsf{M}[\Sigma] = \mathsf{T}$.

Suppose $\mathsf{M'}[\Sigma'] = \mathsf{T}$, but $\mathsf{M}[\Sigma] \neq \mathsf{T}$. From the latter, there is some formula $\mathcal{B} \in \Sigma$ such that $\mathsf{M}[\mathcal{B}] \neq \mathsf{T}$; so by TI, for some d, $\mathsf{M_d}[\mathcal{B}] \neq \mathsf{S}$; so by T10.15, $\mathsf{M'_d}[\mathcal{B}] \neq \mathsf{S}$; so by TI, $\mathsf{M'}[\mathcal{B}] \neq \mathsf{T}$; and since $\mathcal{B} \in \Sigma$, we have $\mathcal{B} \in \Sigma'$; so $\mathsf{M'}[\Sigma'] \neq \mathsf{T}$. This is impossible; reject the assumption: if $\mathsf{M'}[\Sigma'] = \mathsf{T}$, then $\mathsf{M}[\Sigma] = \mathsf{T}$.

T10.13, T10.10, and T10.16 together yield,

T10.17. $\mathcal{L}$, if Σ is consistent, then Σ has a model M ($\mathcal{L}$ without equality).

Suppose Σ is consistent; then by T10.13, Σ' is consistent; so by T10.10, Σ' has a model $\mathsf{M'}$; so by T10.16, Σ has a model M.

And that is what we needed to recover the adequacy result for $\mathcal{L}$ without the constraint on constants. Where $\mathcal{L}$ does not include infinitely many constants not in Γ, we simply add them to form $\mathcal{L}'$. Our theorems from this section ensure that the results go through as before.

*E10.21. Complete the proof of T10.14. You should set up the complete induction, but may refer to the text, as the text refers to homework.

*E10.22. Complete the proof of T10.15. As usual, you should set up the complete induction, but may refer to the text for cases completed there, as the text refers to homework.

E10.23. Adapt the demonstration of T10.11 for the supposition that $\mathscr{L}$ need not be the same as $\mathscr{L}'$. You may appeal to theorems from this section.

10.4.2 Accommodating Equality

Dropping the assumption that language $\mathscr{L}$ lacks the symbol '=' for equality results in another sort of complication. In constructing our models, where t_1 and t_3 from the enumeration of variable-free terms are constants and $\Sigma'' \vdash \mathscr{R}t_1t_3$, we set $\mathsf{M}'[t_1] = 1$, $\mathsf{M}'[t_3] = 3$ and $\langle 1, 3\rangle \in \mathsf{M}'[\mathscr{R}]$. But suppose $\mathscr{R}$ is the equal sign, '='; then by our procedure, $\langle 1, 3\rangle \in \mathsf{M}'[=]$. But this is wrong! Where $\mathsf{U} = \{1, 2 \ldots\}$, the proper interpretation of '=' is $\{\langle 1, 1\rangle, \langle 2, 2\rangle \ldots\}$, and $\langle 1, 3\rangle$ is not a member of this set at all. So our procedure does not result in the specification of a legitimate model. The procedure works fine for relation symbols other than equality. There are no restrictions on assignments to other relation symbols, so nothing stops us from specifying interpretations as above. But there is a restriction on the interpretation of '='. So we cannot proceed blindly this way.

Here is the nub of a solution: Say $\Sigma'' \vdash a_1 = a_3$; then let the *set* $\{1, 3\}$ be an element of U, and let $\mathsf{M}'[a_1] = \mathsf{M}'[a_3] = \{1, 3\}$. Similarly, if $a_2 = a_4$ and $a_4 = a_5$ are consequences of Σ'', let $\{2, 4, 5\}$ be a member of U, and $\mathsf{M}'[a_2] = \mathsf{M}'[a_4] = \mathsf{M}'[a_5] = \{2, 4, 5\}$. That is, let U consist of certain *sets* of integers — where these sets are specified by atomic equalities that are consequences of Σ''. Then let $\mathsf{M}'[a_z]$ be the set of which z is a member. Given this, if $\Sigma'' \vdash \mathscr{R}^n t_a \ldots t_b$, then include the tuple consisting of the set assigned to t_a, and …and the set assigned to t_b, in the interpretation of $\mathscr{R}^n$. So on the above interpretation of the constants, if $\Sigma'' \vdash \mathscr{R}a_1a_4$, then $\langle\{1, 3\}, \{2, 4, 5\}\rangle \in \mathsf{M}'[\mathscr{R}]$. And if $\Sigma'' \vdash a_1 = a_3$, then $\langle\{1, 3\}, \{1, 3\}\rangle \in \mathsf{M}'[=]$. You should see why this is so. And it is just right! If $\{1, 3\} \in \mathsf{U}$, then $\langle\{1, 3\}, \{1, 3\}\rangle$ *should* be in $\mathsf{M}'[=]$. So we respond to the problem by a revision of the specification for CnsM'.

Let us now turn to the details. Put abstractly, the reason the argument in the basis of T10.9 works is that our model M' assigns each t in the enumeration of variable-free terms an object m such that whenever $\Sigma'' \vdash \mathscr{R}t$ then $\mathsf{m} \in \mathsf{M}'[\mathscr{R}]$; and for the universal case, it is important that for each object there is a constant to which it is assigned. We want an interpretation that preserves these features. And it will be important to demonstrate that our specifications are coherent. A model consists of a universe U, along with assignments to constants, function symbols, sentence letters, and relation symbols. We take up these elements, one after another.

The universe. The elements of our universe U are to be certain sets of integers.[4] Consider an enumeration t_1, $t_2 \ldots$ of all the variable-free terms in $\mathcal{L}'$, and let there be a relation $\simeq$ on the set $\{1, 2 \ldots\}$ of positive integers such that $\mathsf{i} \simeq \mathsf{j}$ iff $\Sigma'' \vdash t_i = t_j$. Let $\overline{\mathsf{n}}$ be the set of integers which stand in the $\simeq$ relation to n — that is, $\overline{\mathsf{n}} = \{\mathsf{z} \mid \mathsf{z} \simeq \mathsf{n}\}$. So whenever $\mathsf{z} \simeq \mathsf{n}$, then $\mathsf{z} \in \overline{\mathsf{n}}$. The universe U of M′ is then the collection of all these sets — that is,

CnsM′ For each integer greater than or equal to one, the universe includes the class corresponding to it. $\mathsf{U} = \{\overline{\mathsf{n}} \mid \mathsf{n} \geq 1\}$.

The way this works is really quite simple. If according to Σ'', t_1 equals only itself, then the only z such that $\mathsf{z} \simeq 1$ is 1; so $\overline{1} = \{1\}$, and this is a member of U. If, according to Σ'', t_1 equals just itself and t_2, then $1 \simeq 2$ so that $\overline{1} = \overline{2} = \{1, 2\}$, and this set is a member of U. If, according to Σ'', t_1 equals itself, t_2 and t_3, then $1 \simeq 2 \simeq 3$ so that $\overline{1} = \overline{2} = \overline{3} = \{1, 2, 3\}$, and this set is a member of U. And so forth.

In order to make progress, it will be convenient to establish some facts about the $\simeq$ relation, and about the sets in U. Recall that $\simeq$ is a relation on the *integers* which is specified relative to expressions in Σ'', so that $\mathsf{i} \simeq \mathsf{j}$ iff $\Sigma'' \vdash t_i = t_j$. First we show that $\simeq$ is *reflexive*, *symmetric*, and *transitive*.

> *Reflexivity.* For any i, $\mathsf{i} \simeq \mathsf{i}$. By T3.32, $\vdash t_i = t_i$; so $\Sigma'' \vdash t_i = t_i$; so by construction, $\mathsf{i} \simeq \mathsf{i}$.
>
> *Symmetry.* For any i and j, if $\mathsf{i} \simeq \mathsf{j}$, then $\mathsf{j} \simeq \mathsf{i}$. Suppose $\mathsf{i} \simeq \mathsf{j}$; then by construction, $\Sigma'' \vdash t_i = t_j$; but by T3.33, $\vdash t_i = t_j \rightarrow t_j = t_i$; so by MP, $\Sigma'' \vdash t_j = t_i$; so by construction, $\mathsf{j} \simeq \mathsf{i}$.
>
> *Transitivity.* For any i, j and k, if $\mathsf{i} \simeq \mathsf{j}$ and $\mathsf{j} \simeq \mathsf{k}$, then $\mathsf{i} \simeq \mathsf{k}$. Suppose $\mathsf{i} \simeq \mathsf{j}$ and $\mathsf{j} \simeq \mathsf{k}$; then by construction, $\Sigma'' \vdash t_i = t_j$ and $\Sigma'' \vdash t_j = t_k$; but by

[4] Again, it is common to let the universe be *sets of terms* in $\mathcal{L}'$. There is nothing the matter with this. However, working with the integers emphasizes continuity with other models we have seen, and positions us for further results.

T3.34, $\vdash t_i = t_j \rightarrow (t_j = t_k \rightarrow t_i = t_k)$; so by two instances of MP, $\Sigma'' \vdash t_i = t_k$; so by construction, $\mathsf{i} \simeq \mathsf{k}$.

A relation which is reflexive, symmetric and transitive is called an *equivalence* relation. As an equivalence relation, it divides or *partitions* the members of $\{1, 2 \ldots\}$ into mutually exclusive classes such that each member of a class bears $\simeq$ to each of the others in its partition, but not to integers outside the partition. More particularly, because $\simeq$ is an equivalence relation, the collections $\overline{\mathsf{n}} = \{\mathsf{z} \mid \mathsf{z} \simeq \mathsf{n}\}$ in U are characterized as follows.

Self-membership. For any n, $\mathsf{n} \in \overline{\mathsf{n}}$. By reflexivity, $\mathsf{n} \simeq \mathsf{n}$; so by construction, $\mathsf{n} \in \overline{\mathsf{n}}$. Corollary: Every integer i is a member of at least one class.

Uniqueness. For any i, i is an an element of at most one class. Suppose i is an element of more than one class; then there are some m and n such that $\mathsf{i} \in \overline{\mathsf{m}}$ and $\mathsf{i} \in \overline{\mathsf{n}}$ but $\overline{\mathsf{m}} \neq \overline{\mathsf{n}}$. Since $\overline{\mathsf{m}} \neq \overline{\mathsf{n}}$ there is some j such that $\mathsf{j} \in \overline{\mathsf{m}}$ and $\mathsf{j} \notin \overline{\mathsf{n}}$, or $\mathsf{j} \in \overline{\mathsf{n}}$ and $\mathsf{j} \notin \overline{\mathsf{m}}$; without loss of generality, suppose $\mathsf{j} \in \overline{\mathsf{m}}$ and $\mathsf{j} \notin \overline{\mathsf{n}}$. Since $\mathsf{j} \in \overline{\mathsf{m}}$, by construction, $\mathsf{j} \simeq \mathsf{m}$; and since $\mathsf{i} \in \overline{\mathsf{m}}$, by construction $\mathsf{i} \simeq \mathsf{m}$; so by symmetry, $\mathsf{m} \simeq \mathsf{i}$; so by transitivity, $\mathsf{j} \simeq \mathsf{i}$. Since $\mathsf{i} \in \overline{\mathsf{n}}$, by construction $\mathsf{i} \simeq \mathsf{n}$; so by transitivity again, $\mathsf{j} \simeq \mathsf{n}$; so by construction, $\mathsf{j} \in \overline{\mathsf{n}}$. This is impossible; reject the assumption: i is an element of at most one class.

Equality. For any m and n, $\mathsf{m} \simeq \mathsf{n}$ iff $\overline{\mathsf{m}} = \overline{\mathsf{n}}$. (i) Suppose $\mathsf{m} \simeq \mathsf{n}$. Then by construction, $\mathsf{m} \in \overline{\mathsf{n}}$; but by self-membership, $\mathsf{m} \in \overline{\mathsf{m}}$; so by uniqueness, $\overline{\mathsf{n}} = \overline{\mathsf{m}}$. Suppose $\overline{\mathsf{m}} = \overline{\mathsf{n}}$; by self-membership, $\mathsf{m} \in \overline{\mathsf{m}}$; so $\mathsf{m} \in \overline{\mathsf{n}}$; so by construction, $\mathsf{m} \simeq \mathsf{n}$.

Corresponding to the relations by which they are formed, classes characterized by self-membership, uniqueness and equality are *equivalence classes*. From self-membership and uniqueness, every n is a member of exactly one such class. And from equality, $\mathsf{m} \simeq \mathsf{n}$ just when $\overline{\mathsf{m}}$ is the very same thing as $\overline{\mathsf{n}}$. So, for example, if $1 \simeq 1$ and $2 \simeq 1$ (and nothing else), then $\overline{1} = \overline{2} = \{1, 2\}$. You should be able to see that these formal specifications develop just the informal picture with which we began.

Terms. The specification for constants is simple.

CnsM′ If t_z in the enumeration of variable-free terms t_1, $t_2 \ldots$ is a constant, then $\mathsf{M}'[t_z] = \overline{\mathsf{z}}$.

Thus, with self-membership, any constant t_z designates the equivalence class of which z is a member. In this case, we need to be sure that the specification picks out exactly one member of U for each constant. The specification would fail if the relation $\simeq$ generated classes such that some integer was an element of no class, or some integer was an element of more than one. But, as we have just seen, by self-membership and uniqueness, every z is a member of exactly one class. So far, so good!

CnsM′ If t_z in the enumeration of variable-free terms t_1, $t_2 \ldots$ is $h^n t_a \ldots t_b$ for function symbol h^n and variable-free terms $t_a \ldots t_b$, then $\langle\langle \overline{\mathsf{a}} \ldots \overline{\mathsf{b}}\rangle, \overline{\mathsf{z}}\rangle \in \mathsf{M}'[h^n]$.

Thus when the input to h^n is $\langle \overline{\mathsf{a}} \ldots \overline{\mathsf{b}}\rangle$, the output is $\overline{\mathsf{z}}$. This time, we must be sure that the result is a function — that (i) there is a defined output object for every input n-tuple, and (ii) there is at most one output object associated with any one input n-tuple. The former worry is easily dispatched. The second concern is that there might be some $t_m = h t_a$ and $t_n = h t_b$ in the list of variable-free terms, where $\overline{\mathsf{a}} = \overline{\mathsf{b}}$. Then $\langle \overline{\mathsf{a}}, \overline{\mathsf{m}}\rangle$, $\langle \overline{\mathsf{b}}, \overline{\mathsf{n}}\rangle \in \mathsf{M}'[h]$, and we fail to specify a function.

(i) There is at least one output object. Corresponding to any $\langle \overline{\mathsf{a}} \ldots \overline{\mathsf{b}}\rangle$ where $\overline{\mathsf{a}} \ldots \overline{\mathsf{b}}$ are members of U, there is some variable-free $t_z = h^n t_a \ldots t_b$ in the sequence t_1, $t_2 \ldots$; so by construction, $\langle\langle \overline{\mathsf{a}} \ldots \overline{\mathsf{b}}\rangle, \overline{\mathsf{z}}\rangle \in \mathsf{M}'[h^n]$. So $\mathsf{M}'[h^n]$ has a defined output object when the input is $\langle \overline{\mathsf{a}} \ldots \overline{\mathsf{b}}\rangle$.

(ii) There is at most one output object. Suppose $\langle\langle \overline{\mathsf{a}} \ldots \overline{\mathsf{c}}\rangle, \overline{\mathsf{m}}\rangle \in \mathsf{M}'[h^n]$ and $\langle\langle \overline{\mathsf{d}} \ldots \overline{\mathsf{f}}\rangle, \overline{\mathsf{n}}\rangle \in \mathsf{M}'[h^n]$, where $\langle \overline{\mathsf{a}} \ldots \overline{\mathsf{c}}\rangle = \langle \overline{\mathsf{d}} \ldots \overline{\mathsf{f}}\rangle$, but $\overline{\mathsf{m}} \neq \overline{\mathsf{n}}$. Since $\langle \overline{\mathsf{a}} \ldots \overline{\mathsf{c}}\rangle = \langle \overline{\mathsf{d}} \ldots \overline{\mathsf{f}}\rangle$, $\overline{\mathsf{a}} = \overline{\mathsf{d}}$, and …and $\overline{\mathsf{c}} = \overline{\mathsf{f}}$; so by equality, $\mathsf{a} \simeq \mathsf{d}$, and …and $\mathsf{c} \simeq \mathsf{f}$; so by construction, $\Sigma'' \vdash t_a = t_d$, and …and $\Sigma'' \vdash t_c = t_f$. Since $\langle\langle \overline{\mathsf{a}} \ldots \overline{\mathsf{c}}\rangle, \overline{\mathsf{m}}\rangle \in \mathsf{M}'[h^n]$ and $\langle\langle \overline{\mathsf{d}} \ldots \overline{\mathsf{f}}\rangle, \overline{\mathsf{n}}\rangle \in \mathsf{M}'[h^n]$, by construction, there are some variable-free terms, $t_m = h^n t_a \ldots t_c$ and $t_n = h^n t_d \ldots t_f$ in the enumeration; but by T3.36, $\vdash t_b = t_e \rightarrow h^n t_a \ldots t_b \ldots t_c = h^n t_a \ldots t_e \ldots t_c$, and so forth; so collecting repeated applications of this theorem with MP and T3.35, $\Sigma'' \vdash h^n t_a \ldots t_c = h^n t_d \ldots t_f$; but this is to say, $\Sigma'' \vdash t_m = t_n$; so by construction, $\mathsf{m} \simeq \mathsf{n}$; so by equality, $\overline{\mathsf{m}} = \overline{\mathsf{n}}$. This is impossible; reject the assumption: if $\langle\langle \overline{\mathsf{a}} \ldots \overline{\mathsf{c}}\rangle, \overline{\mathsf{m}}\rangle \in \mathsf{M}'[h^n]$ and $\langle\langle \overline{\mathsf{d}} \ldots \overline{\mathsf{f}}\rangle, \overline{\mathsf{n}}\rangle \in \mathsf{M}'[h^n]$, where $\langle \overline{\mathsf{a}} \ldots \overline{\mathsf{c}}\rangle = \langle \overline{\mathsf{d}} \ldots \overline{\mathsf{f}}\rangle$, then $\overline{\mathsf{m}} = \overline{\mathsf{n}}$.

So, as they should be, functions are well-defined.

We are now in a position to recover an analogue to the preliminary result for demonstration of T10.9: for any variable-free term t_z and variable assignment d, $\mathsf{M}'_{\mathsf{d}}[t_z] = \bar{\mathsf{z}}$. The argument is very much as before. Suppose t_z is a variable-free term. By induction on the number of function symbols in t_z.

Basis: If t_z has no function symbols, then it is a constant. In this case, by construction, $\mathsf{M}'[t_z] = \bar{\mathsf{z}}$; so by TA(c), $\mathsf{M}'_{\mathsf{d}}[t_z] = \bar{\mathsf{z}}$.

Assp: For any i, $0 \le i < k$, if t_z has i function symbols, then $\mathsf{M}'_{\mathsf{d}}[t_z] = \bar{\mathsf{z}}$.

Show: If t_z has k function symbols, then $\mathsf{M}'_{\mathsf{d}}[t_z] = \bar{\mathsf{z}}$.

If t_z has k function symbols, then it is of the form, $h^n t_a \dots t_b$ where $t_a \dots t_b$ have $< k$ function symbols. By TA(f) we have, $\mathsf{M}'_{\mathsf{d}}[t_z] = \mathsf{M}'_{\mathsf{d}}[h^n t_a \dots t_b] = \mathsf{M}'[h^n]\langle \mathsf{M}'_{\mathsf{d}}[t_a] \dots \mathsf{M}'_{\mathsf{d}}[t_b]\rangle$; but by assumption, $\mathsf{M}'_{\mathsf{d}}[t_a] = \bar{\mathsf{a}}$, and ... and $\mathsf{M}'_{\mathsf{d}}[t_b] = \bar{\mathsf{b}}$; so $\mathsf{M}'_{\mathsf{d}}[t_z] = \mathsf{M}'[h^n]\langle \bar{\mathsf{a}} \dots \bar{\mathsf{b}}\rangle$. But since $t_z = h^n t_a \dots t_b$ is a variable-free term, $\langle\langle \bar{\mathsf{a}} \dots \bar{\mathsf{b}}\rangle, \bar{\mathsf{z}}\rangle \in \mathsf{M}'[h^n]$; so $\mathsf{M}'[h^n]\langle \bar{\mathsf{a}} \dots \bar{\mathsf{b}}\rangle = \bar{\mathsf{z}}$; so $\mathsf{M}'_{\mathsf{d}}[t_z] = \bar{\mathsf{z}}$.

Indct: For any variable-free term t_z, $\mathsf{M}'_{\mathsf{d}}[t_z] = \bar{\mathsf{z}}$.

So the interepretation of any variable-free term is the equivalence class corresponding to its position in the enumeration of terms.

Atomics. The result we have just seen for terms makes the specification for atomics seem particularly natural. Sentence letters are easy. As before,

CnsM′ For a sentence letter $\mathcal{S}$, $\mathsf{M}'[\mathcal{S}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{S}$.

Then for relation symbols, the idea is as sketched above. We simply let the assignment be such as to make a variable-free atomic come out true iff it is a consequence of Σ''.

CnsM′ For a relation symbol $\mathcal{R}^n$, where $t_a \dots t_b$ are n members of the enumeration of variable-free terms, let $\langle \bar{\mathsf{a}} \dots \bar{\mathsf{b}}\rangle \in \mathsf{M}'[\mathcal{R}^n]$ iff $\Sigma'' \vdash \mathcal{R}^n t_a \dots t_b$.

To see that the specification for relation symbols is legitimate, we need to be clear that the specification is consistent — that we do not both assert and deny that some tuple is in the extension of $\mathcal{R}^n$, and we need to be sure that $\mathsf{M}'[=]$ is as it should be — that it is $\{\langle \bar{\mathsf{n}}, \bar{\mathsf{n}}\rangle \mid \bar{\mathsf{n}} \in \mathsf{U}\}$. The case for equality is easy. The former concern is that we might have some $\bar{\mathsf{a}} \in \mathsf{M}'[\mathcal{R}]$ and $\bar{\mathsf{b}} \notin \mathsf{M}'[\mathcal{R}]$ but $\bar{\mathsf{a}} = \bar{\mathsf{b}}$.

(i) The specification is consistent. Suppose otherwise. Then there is some $\langle\overline{\mathsf{a}}\ldots\overline{\mathsf{c}}\rangle \in \mathsf{M}'[\mathcal{R}^n]$ and $\langle\overline{\mathsf{d}}\ldots\overline{\mathsf{f}}\rangle \notin \mathsf{M}'[\mathcal{R}^n]$, where $\langle\overline{\mathsf{a}}\ldots\overline{\mathsf{c}}\rangle = \langle\overline{\mathsf{d}}\ldots\overline{\mathsf{f}}\rangle$. From the latter, $\overline{\mathsf{a}} = \overline{\mathsf{d}}$, and ... and $\overline{\mathsf{c}} = \overline{\mathsf{f}}$; so by equality, $\mathsf{a} \simeq \mathsf{d}$, and ... and $\mathsf{c} \simeq \mathsf{f}$; so by construction, $\Sigma'' \vdash t_a = t_d$, and ... and $\Sigma'' \vdash t_c = t_f$. But since $\langle\overline{\mathsf{a}}\ldots\overline{\mathsf{c}}\rangle \in \mathsf{M}'[\mathcal{R}^n]$ and $\langle\overline{\mathsf{d}}\ldots\overline{\mathsf{f}}\rangle \notin \mathsf{M}'[\mathcal{R}^n]$, by construction, $\Sigma'' \vdash \mathcal{R}^n t_a \ldots t_c$ and $\Sigma'' \nvdash \mathcal{R}^n t_d \ldots t_f$; and by T3.37, $\vdash t_b = t_e \to (\mathcal{R}^n t_a \ldots t_b \ldots t_c \to \mathcal{R}^n t_a \ldots t_e \ldots t_c)$, and so forth; so by repeated applications of this theorem with MP, $\Sigma'' \vdash \mathcal{R}^n t_d \ldots t_f$. This is impossible; reject the assumption: if $\langle\overline{\mathsf{a}}\ldots\overline{\mathsf{c}}\rangle \in \mathsf{M}'[\mathcal{R}^n]$ and $\langle\overline{\mathsf{d}}\ldots\overline{\mathsf{f}}\rangle \notin \mathsf{M}'[\mathcal{R}^n]$, then $\langle\overline{\mathsf{a}}\ldots\overline{\mathsf{c}}\rangle \neq \langle\overline{\mathsf{d}}\ldots\overline{\mathsf{f}}\rangle$.

(ii) The case for equality is easy. By equality, $\overline{\mathsf{m}} = \overline{\mathsf{n}}$ iff $\mathsf{m} \simeq \mathsf{n}$; by construction iff $\Sigma'' \vdash t_m = t_n$; by construction iff $\langle\overline{\mathsf{m}}, \overline{\mathsf{n}}\rangle \in \mathsf{M}'[=]$.

This completes the specification of M'. The specification is more complex than for the basic version, and we have had to work to demonstrate its consistency. Still, the result is a perfectly ordinary model M', with a domain, assignments to constants, assignments to function symbols, and assignments to relation symbols.

With this revised specification for M', the demonstration of T10.9 proceeds as before. Here is the key portion of the basis. We are showing that $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

Suppose $\mathcal{B}$ is an atomic $\mathcal{R}^n t_a \ldots t_b$; then by TI, $\mathsf{M}'[\mathcal{R}^n t_a \ldots t_b] = \mathsf{T}$ iff for arbitrary d, $\mathsf{M}'_{\mathsf{d}}[\mathcal{R}^n t_a \ldots t_b] = \mathsf{S}$; by SF(r), iff $\langle \mathsf{M}'_{\mathsf{d}}[t_a] \ldots \mathsf{M}'_{\mathsf{d}}[t_b]\rangle \in \mathsf{M}'[\mathcal{R}^n]$; since $t_a \ldots t_b$ are variable-free terms, as we have just seen, iff $\langle\overline{\mathsf{a}}\ldots\overline{\mathsf{b}}\rangle \in \mathsf{M}'[\mathcal{R}^n]$; by construction, iff $\Sigma'' \vdash \mathcal{R}^n t_a \ldots t_b$. So $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

So all that happens is that we depend on the conversion from individuals to sets of individuals for both assignments to terms, and assignments to relation symbols. Given this, the argument is exactly parallel to the one from before.

E10.24. Suppose the enumeration of variable-free terms begins, $a, b, f^1a, f^1b \ldots$ (so these are $t_1 \ldots t_4$) and, for these terms, $\Sigma'' \vdash$ just $a = a$, $b = b$, $f^1a = f^1a$, $f^1b = f^1b$, $a = f^1a$, and $f^1a = a$. What objects stand in the $\simeq$ relation? What are $\overline{1}$, $\overline{2}$, $\overline{3}$, and $\overline{4}$? Which corresponding sets are members of U?

E10.25. Return to the case from E10.24. Explain how $\simeq$ satisfies reflexivity, symmetry and transitivity. Explain how U satisfies self-membership, uniqueness and equality.

E10.26. Where Σ'' and U are as in the previous two exercises, what are $\mathsf{M}'[a]$, $\mathsf{M}'[b]$ and $\mathsf{M}'[f]$? Supposing that $\Sigma'' \vdash R^1a$, R^1f^1a and R^1f^1b, but $\Sigma'' \nvdash R^1b$, what is $\mathsf{M}'[R^1]$? According to the method, what is $\mathsf{M}'[=]$? Is this as it should be? Explain.

10.4.3 The Final Result

We are really done with the demonstration of adequacy. Perhaps, though, it will be helpful to draw some parts together. Begin with the basic definitions.

Con A set Σ of formulas is *consistent* iff there is no formula $\mathcal{A}$ such that $\Sigma \vdash \mathcal{A}$ and $\Sigma \vdash {\sim}\mathcal{A}$.

Max A set Σ of formulas is *maximal* iff for any sentence $\mathcal{A}$, $\Sigma \vdash \mathcal{A}$ or $\Sigma \vdash {\sim}\mathcal{A}$.

Scgt A set Σ of formulas is a *scapegoat* set iff for any sentence ${\sim}\forall x\mathcal{P}$, if $\Sigma \vdash {\sim}\forall x\mathcal{P}$, then there is some constant a such that $\Sigma \vdash {\sim}\mathcal{P}^x_a$.

Then we proceed in language $\mathcal{L}'$, for a maximal, consistent, scapegoat set Σ'' constructed from any consistent Σ'.

T10.6 For any set of formulas Σ and sentence $\mathcal{P}$, if $\Sigma \nvdash {\sim}\mathcal{P}$, then $\Sigma \cup \{\mathcal{P}\}$ is consistent.

T10.7 There is an enumeration $\mathcal{Q}_1$, $\mathcal{Q}_2 \ldots$ of all the formulas, terms, and the like, in $\mathcal{L}'$.

CnsΣ'' Construct Σ'' from Σ' as follows: By T10.7, there is an enumeration, $\mathcal{Q}_1$, $\mathcal{Q}_2 \ldots$ of all the sentences in $\mathcal{L}'$ and also an enumeration c_1, $c_2 \ldots$ of constants not in Σ'. Let $\Omega_0 = \Sigma'$. Then for any $i > 0$, let $\Omega_i = \Omega_{i-1}$ if $\Omega_{i-1} \vdash {\sim}\mathcal{Q}_i$. Otherwise, $\Omega_{i*} = \Omega_{i-1} \cup \{\mathcal{Q}_i\}$ if $\Omega_{i-1} \nvdash {\sim}\mathcal{Q}_i$. Then $\Omega_i = \Omega_{i*}$ if $\mathcal{Q}_i$ is not of the form ${\sim}\forall x\mathcal{P}$, and $\Omega_i = \Omega_{i*} \cup \{{\sim}\mathcal{P}^x_c\}$ if $\mathcal{Q}_i$ is of the form ${\sim}\forall x\mathcal{P}$, where c is the first constant not in Ω_{i*}. Then $\Sigma'' = \bigcup_{i \geq 0} \Omega_i$.

T10.8 If Σ' is consistent, then Σ'' is a maximal, consistent, scapegoat set.

Given the maximal, consistent, scapegoat set Σ'', there are results and a definition for a model M' such that $\mathsf{M}'[\Sigma'] = \mathsf{T}$.

CnsM′ $\mathsf{U} = \{\bar{\mathsf{n}} \mid \mathsf{n} \geq 1\}$. If t_z in an enumeration of variable-free terms t_1, $t_2 \ldots$ is a constant, then $\mathsf{M}'[t_z] = \bar{\mathsf{z}}$. If t_z is $\mathscr{h}^n t_a \ldots t_b$ for function symbol $\mathscr{h}^n$ and variable-free terms $t_a \ldots t_b$, then $\langle\langle \bar{\mathsf{a}} \ldots \bar{\mathsf{b}}\rangle, \bar{\mathsf{z}}\rangle \in \mathsf{M}'[\mathscr{h}^n]$. For a sentence letter $\mathscr{S}$, $\mathsf{M}'[\mathscr{S}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathscr{S}$. For a relation symbol $\mathscr{R}^n$, where $t_a \ldots t_b$ are n members of the enumeration of variable-free terms, let $\langle \bar{\mathsf{a}} \ldots \bar{\mathsf{b}}\rangle \in \mathsf{M}'[\mathscr{R}^n]$ iff $\Sigma'' \vdash \mathscr{R}^n t_a \ldots t_b$.

This modifies the relatively simple version where $\mathsf{U} = \{1, 2 \ldots\}$. And for an enumeration of variable-free terms, if t_z is a constant, $\mathsf{M}'[t_z] = \mathsf{z}$. If $t_z = \mathscr{h}^n t_a \ldots t_b$ for some relation symbol $\mathscr{h}^n$ and n variable-free terms $t_a \ldots t_b$, $\langle\langle \mathsf{a} \ldots \mathsf{b}\rangle, \mathsf{z}\rangle \in \mathsf{M}'[\mathscr{h}^n]$. For a sentence letter $\mathscr{S}$, $\mathsf{M}'[\mathscr{S}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathscr{S}$. And for a relation symbol $\mathscr{R}^n$, $\langle \mathsf{a} \ldots \mathsf{b}\rangle \in \mathsf{M}'[\mathscr{R}^n]$ iff $\Sigma'' \vdash \mathscr{R}^n t_a \ldots t_b$.

T10.9 If Σ' is consistent, then for any sentence $\mathscr{B}$ of $\mathscr{L}'$, $\mathsf{M}'[\mathscr{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathscr{B}$.

T10.10 If Σ' is consistent, then $\mathsf{M}'[\Sigma'] = \mathsf{T}$. $(\star)$

Then we have had to connect results for Σ' in $\mathscr{L}'$ to an arbitrary Σ in language $\mathscr{L}$.

T10.13 If Σ is consistent, then Σ' is consistent.

This is supported by T10.12 on which if D is a derivation from Σ', and x is a variable that does not appear in D, then for any constant a, D^a_x is a derivation from $\Sigma'^{\,a}_{\,x}$.

T10.16 If $\mathsf{M}'[\Sigma'] = \mathsf{T}$, then $\mathsf{M}[\Sigma] = \mathsf{T}$.

This is supported by the matched pair of theorems, T10.14 on which, if d is a variable assignment, then for any term t in $\mathscr{L}$, $\mathsf{M_d}[t] = \mathsf{M'_d}[t]$, and T10.15 on which, if d is a variable assignment, then for any formula $\mathscr{P}$ in $\mathscr{L}$, $\mathsf{M_d}[\mathscr{P}] = \mathsf{S}$ iff $\mathsf{M'_d}[\mathscr{P}] = \mathsf{S}$.

These theorems together yield,

T10.17. If Σ is consistent, then Σ has a model M. ($\mathscr{L}$ unconstrained) $(\star\star)$

This puts us in a position to recover the main result. Recall that our argument runs through $\mathscr{P}^c$ the universal closure of $\mathscr{P}$.

T10.11. If $\Gamma \vDash \mathscr{P}$, then $\Gamma \vdash \mathscr{P}$. (*quantificational adequacy*)

Suppose $\Gamma \vDash \mathscr{P}$ but $\Gamma \nvdash \mathscr{P}$. Say, for the moment that $\Gamma \vdash \sim\sim\mathscr{P}^c$; by T3.10, $\vdash \sim\sim\mathscr{P}^c \to \mathscr{P}^c$; so by MP, $\Gamma \vdash \mathscr{P}^c$; so by repeated applications of A4 and MP, $\Gamma \vdash \mathcal{P}$; but this is impossible; so $\Gamma \nvdash \sim\sim\mathcal{P}^c$. Given this, since $\sim\sim\mathcal{P}^c$ is a sentence, by T10.6, $\Gamma \cup \{\sim\mathcal{P}^c\}$ is consistent. Since $\Sigma = \Gamma \cup \{\sim\mathcal{P}^c\}$ is consistent, by T10.17, there is a model M constructed as above such that $\mathsf{M}[\Sigma] = \mathsf{T}$. So $\mathsf{M}[\Gamma] = \mathsf{T}$ and $\mathsf{M}[\sim\mathcal{P}^c] = \mathsf{T}$; from the latter, by T8.6, $\mathsf{M}[\mathcal{P}^c] \neq \mathsf{T}$; so by repeated applications of T7.7, $\mathsf{M}[\mathcal{P}] \neq \mathsf{T}$; so by QV, $\Gamma \nvDash \mathcal{P}$. This is impossible; reject the assumption: if $\Gamma \vDash \mathcal{P}$ then $\Gamma \vdash \mathcal{P}$.

The sentential version had parallels to Con, Max, CnsΣ'' and CnsM$'$ along with theorems T10.6_s - T10.11_s. (The distinction between ($\star$) and ($\star\star$) is a distinction without a difference in the sentential case.) The basic quantificational version requires these along with Sgt, T10.12 and the simple version of CnsM$'$. For the full version, we have had to appeal also to T10.13 and T10.16 (and so T10.17), and use the relatively complex specification for CnsM$'$.

Again, you should try to get the complete picture in your mind: As always, the key is that consistent sets have models. If $\Gamma \cup \{\sim\mathcal{P}\}$ is not consistent, then there is a derivation of $\mathcal{P}$ from Γ. So if there is no derivation of $\mathcal{P}$ from Γ, then $\Gamma \cup \{\sim\mathcal{P}\}$ is consistent, and so has a model — and the existence of a model for $\Gamma \cup \{\sim\mathcal{P}\}$ is sufficient to show that $\Gamma \nvDash \mathcal{P}$. Put the other way around, if $\Gamma \vDash \mathcal{P}$, then there is a derivation of $\mathcal{P}$ from Γ. We get the key point, that consistent sets have models, by finding a relation between consistent, and maximal consistent scapegoat sets. If a set is a maximal consistent scapegoat set, then it contains enough information to specify a model for the whole. The model for the big set then guarantees the existence of a model M for the original Γ.

E10.27. Return to the case from E10.20 on p. 500, but dropping the assumptions that there is no symbol for equality, and that $\mathcal{L}$ is identical to $\mathcal{L}'$. Add to the derivation system axioms,

A3 $\vdash t = t$

A4 $\vdash r = s \rightarrow (\mathcal{P} \rightarrow \mathcal{P}^{r}/_{s})$ — where s is free for replaced instances of r in $\mathcal{P}$

Provide a complete demonstration that this version of *A4* is adequate. You may appeal to any results from the text whose demonstration remains unchanged, but should recreate parts whose demonstration is not the same. Hint: You may find it helpful to demonstrate a relation to T8.5 as follows, T8.5* For any formula $\mathcal{P}$, terms s and t, constant c, and variable x, $[\mathcal{P}^{s}/_{t}]^{c}_{x}$ is the same formula as $[\mathcal{P}^{c}_{x}]^{s^{c}_{x}}/_{t^{c}_{x}}$ — where the same instance(s) of s are replaced in each case.

E10.28. We have shown from T10.4 that if a set of formulas has a model, then it is consistent; and now that if an arbitrary set of formulas is consistent, then it has a model — and one whose U is this set of sets of positive integers. Notice that any such U is *countable* insofar as its members can be put into correspondence with the integers (we might, say, order the members by their least elements). Considering what we showed in the more on countability reference on p. 50, how might this be a problem for the logic of real numbers? Hint: Think about the consequences sentences in an arbitrary Γ may have about the number of elements in U.

E10.29. For each of the following concepts, explain in an essay of about two pages, so that (college freshman) Hannah could understand. In your essay, you should (i) identify the objects to which the concept applies, (ii) give and explain the definition, and give and explicate examples (iii) where the concept applies, and (iv) where it does not. Your essay should exhibit an understanding of methods from the text.

a. The soundness of a derivation system, and its demonstration by mathematical induction.

b. The adequacy of a derivation system, and the basic strategy for its demonstration.

c. Maximality and consistency, and the reasons for them.

d. Scapegoat sets, and the reasons for them.

Theorems of Chapter 10

T10.1 For any interpretation I, variable assignment d, with terms t and r, if $\mathsf{I_d}[r] = \mathsf{o}$, then $\mathsf{I_{d(x|o)}}[t] = \mathsf{I_d}[t^x_r]$.

T10.2 For any interpretation I, variable assignment d, term r, and formula $\mathcal{Q}$, if $\mathsf{I_d}[r] = \mathsf{o}$, and r is free for x in $\mathcal{Q}$, then $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$.

T10.3 If $\Gamma \vdash_{AD} \mathcal{P}$, then $\Gamma \vDash \mathcal{P}$. (*Soundness*)

T10.4 If there is an interpretation M such that $\mathsf{M}[\Gamma] = \mathsf{T}$ (a *model* for Γ), then Γ is consistent.

T10.5 If there is an interpretation M such that $\mathsf{M}[\Gamma \cup \{\sim\mathcal{A}\}] = \mathsf{T}$, then $\Gamma \nvdash \mathcal{A}$.

T10.6$_s$ For any set of formulas Σ and sentence $\mathcal{P}$, if $\Sigma \nvdash \sim\mathcal{P}$, then $\Sigma \cup \{\mathcal{P}\}$ is consistent.

T10.6 For any set of formulas Σ and sentence $\mathcal{P}$, if $\Sigma \nvdash \sim\mathcal{P}$, then $\Sigma \cup \{\mathcal{P}\}$ is consistent.

T10.7$_s$ There is an enumeration $\mathcal{Q}_1, \mathcal{Q}_2 \ldots$ of all formulas in $\mathcal{L}_s$.

T10.7 There is an enumeration $\mathcal{Q}_1, \mathcal{Q}_2 \ldots$ of all the formulas, terms, and the like, in $\mathcal{L}'$.

T10.8$_s$ If Σ' is consistent, then Σ'' is maximal and consistent.

T10.8 If Σ' is consistent, then Σ'' is a maximal, consistent, scapegoat set.

T10.9$_s$ If Σ' is consistent, then for any sentence $\mathcal{B}$, of $\mathcal{L}_s$, $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

T10.9 If Σ' is consistent, then for any sentence $\mathcal{B}$ of $\mathcal{L}'$, $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

T10.10$_s$ If Σ' is consistent, then $\mathsf{M}'[\Sigma'] = \mathsf{T}$. $(*)$

T10.10 If Σ' is consistent, then $\mathsf{M}'[\Sigma'] = \mathsf{T}$. $(\star)$

T10.11$_s$ If $\Gamma \vDash_s \mathcal{P}$, then $\Gamma \vdash \mathcal{P}$. (*sentential adequacy*)

T10.11 If $\Gamma \vDash \mathcal{P}$, then $\Gamma \vdash \mathcal{P}$. (*quantificational adequacy*)

T10.12 If D is a derivation from Σ', and x is a variable that does not appear in D, then for any constant a, D^a_x is a derivation from $\Sigma'{}^a_x$.

T10.13 If Σ is consistent, then Σ' is consistent.

T10.14 For any variable assignment d, and for any term t in $\mathcal{L}$, $\mathsf{M_d}[t] = \mathsf{M'_d}[t]$.

T10.15 For any variable assignment d, and for any formula $\mathcal{P}$ in $\mathcal{L}$, $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M'_d}[\mathcal{P}] = \mathsf{S}$.

T10.16 If $\mathsf{M}'[\Sigma'] = \mathsf{T}$, then $\mathsf{M}[\Sigma] = \mathsf{T}$.

T10.17a If Σ is consistent, then Σ has a model M. ($\mathcal{L}$ without equality)

T10.17 If Σ is consistent, then Σ has a model M. ($\mathcal{L}$ unconstrained) $(\star\star)$

Chapter 11

More Main Results

In this chapter, we take up results which deepen our understanding of the power and limits of logic. The first sections restrict discussion to *sentential* forms, for discussion of *expressive completenes*, *unique readability* and *independence*. Then we turn to discussion of the conditions under which models are *isomorphic*, and transition to a discussion of submodels, and especially the Löwenheim-Skolem theorems, which help us see some conditions under which models are not isomorphic.[1]

11.1 Expressive Completeness

In chapter 5 on translation, we introduced the idea of a truth functional operator, where the truth value of the whole is a function of the truth values of the parts. We exhibited operators as truth functional by tables. Thus, if some ordinary expression $\mathscr{P}$ with components $\mathscr{A}$ and $\mathscr{B}$ has table,

(A)

$\mathscr{A}$	$\mathscr{B}$	$\mathscr{P}$
T	T	***T***
T	F	***F***
F	T	***F***
F	F	***F***

then it is truth functional. And we translate by an equivalent formal operator: in this case $\mathscr{A} \wedge \mathscr{B}$ does fine. Of course, not every such table, or truth function, is directly represented by one of our operators. Thus, if $\mathscr{P}$ is 'neither $\mathscr{A}$ nor $\mathscr{B}$' we have the table,

[1]This chapter is not in finished form. It contains some parts which I've had occasion to write up and found useful from time to time. But it's not worked into a fully-formed textbook chapter. Take it in the spirit with which it's provided!

(B)

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{P}$
T	T	***F***
T	F	***F***
F	T	***F***
F	F	***T***

where none of our operators is equivalent to this. But it takes only a little ingenuity to see that, say, $(\sim\mathcal{A} \wedge \sim\mathcal{B})$ or $\sim(\mathcal{A} \vee \mathcal{B})$ have the same table, and so result in a good translation. In chapter 5 (p. **??**), we claimed that for any table a truth functional operator may have, there is always some way to generate that table by means of our formal operators — and, in fact, by means of just the operators $\sim$ and $\wedge$, or just the operators $\sim$ and $\vee$, or just the operators $\sim$ and $\rightarrow$. As it turns out, it is also possible to express any truth function by means of just the operator $\mid$. In this section, we prove these results. First,

T11.1. It is possible to represent any truth function by means of an expression with just the operators $\sim$, $\wedge$, and $\vee$.

The proof of this result is simple. Given an arbitrary truth function, we provide a recipe for constructing an expression with the same table. Insofar as for any truth function it is always possible to construct an expression with the same table, there must always be a formal expression with the same table.

Suppose we are given an arbitrary truth function, in this case with four basic sentences as on the left.

(C)

	$\mathcal{S}_1$	$\mathcal{S}_2$	$\mathcal{S}_3$	$\mathcal{S}_4$	$\mathcal{P}$	
1	T	T	T	T	***F***	$\mathcal{C}_1 = \mathcal{S}_1 \wedge \mathcal{S}_2 \wedge \mathcal{S}_3 \wedge \mathcal{S}_4$
2	T	T	T	F	***F***	$\mathcal{C}_2 = \mathcal{S}_1 \wedge \mathcal{S}_2 \wedge \mathcal{S}_3\sim \wedge \mathcal{S}_4$
3	T	T	F	T	***T***	$\mathcal{C}_3 = \mathcal{S}_1 \wedge \mathcal{S}_2 \wedge \sim\mathcal{S}_3 \wedge \mathcal{S}_4$
4	T	T	F	F	***F***	$\mathcal{C}_4 = \mathcal{S}_1 \wedge \mathcal{S}_2 \wedge \sim\mathcal{S}_3 \wedge \sim\mathcal{S}_4$
5	T	F	T	T	***T***	$\mathcal{C}_5 = \mathcal{S}_1 \wedge \sim\mathcal{S}_2 \wedge \mathcal{S}_3 \wedge \mathcal{S}_4$
6	T	F	T	F	***F***	$\mathcal{C}_6 = \mathcal{S}_1 \wedge \sim\mathcal{S}_2 \wedge \mathcal{S}_3 \wedge \sim\mathcal{S}_4$
7	T	F	F	T	***F***	$\mathcal{C}_7 = \mathcal{S}_1 \wedge \sim\mathcal{S}_2 \wedge \sim\mathcal{S}_3 \wedge \mathcal{S}_4$
8	T	F	F	F	***F***	$\mathcal{C}_8 = \mathcal{S}_1 \wedge \sim\mathcal{S}_2 \wedge \sim\mathcal{S}_3 \wedge \sim\mathcal{S}_4$
9	F	T	T	T	***F***	$\mathcal{C}_9 = \sim\mathcal{S}_1 \wedge \mathcal{S}_2 \wedge \mathcal{S}_3 \wedge \mathcal{S}_4$
10	F	T	T	F	***F***	$\mathcal{C}_{10} = \sim\mathcal{S}_1 \wedge \mathcal{S}_2 \wedge \mathcal{S}_3 \wedge \sim\mathcal{S}_4$
11	F	T	F	T	***F***	$\mathcal{C}_{11} = \sim\mathcal{S}_1 \wedge \mathcal{S}_2 \wedge \sim\mathcal{S}_3 \wedge \mathcal{S}_4$
12	F	T	F	F	***T***	$\mathcal{C}_{12} = \sim\mathcal{S}_1 \wedge \mathcal{S}_2 \wedge \sim\mathcal{S}_3 \wedge \sim\mathcal{S}_4$
13	F	F	T	T	***T***	$\mathcal{C}_{13} = \sim\mathcal{S}_1 \wedge \sim\mathcal{S}_2 \wedge \mathcal{S}_3 \wedge \mathcal{S}_4$
14	F	F	T	F	***F***	$\mathcal{C}_{14} = \sim\mathcal{S}_1 \wedge \sim\mathcal{S}_2 \wedge \mathcal{S}_3 \wedge \sim\mathcal{S}_4$
15	F	F	F	T	***F***	$\mathcal{C}_{15} = \sim\mathcal{S}_1 \wedge \sim\mathcal{S}_2 \wedge \sim\mathcal{S}_3 \wedge \mathcal{S}_4$
16	F	F	F	F	***F***	$\mathcal{C}_{16} = \sim\mathcal{S}_1 \wedge \sim\mathcal{S}_2 \wedge \sim\mathcal{S}_3 \wedge \sim\mathcal{S}_4$

For this sentence $\mathcal{P}$ with basic sentences $\mathcal{S}_1 \ldots \mathcal{S}_n$, begin by constructing the *characteristic* sentence $\mathcal{C}_j$ corresponding to each row: If the interpretation I_j corresponding to row j has $\mathsf{I}_j[\mathcal{S}_i] = \mathsf{T}$, then let $\mathcal{S}'_i = \mathcal{S}_i$. If $\mathsf{I}_j[\mathcal{S}_i] = \mathsf{F}$, let $\mathcal{S}'_i = \sim\mathcal{S}_i$. Then the characteristic sentence $\mathcal{C}_j$ corresponding to I_j is the conjunction of each $\mathcal{S}'_i$. So $\mathcal{C}_j = \mathcal{S}'_1 \wedge \ldots \wedge \mathcal{S}'_n$ (with appropriate parentheses). These sentences are exhibited above. The characteristic sentences are true *only* on their corresponding rows. Thus $\mathcal{C}_4$ above is true only when $\mathsf{I}[\mathcal{S}_1] = \mathsf{T}$, $\mathsf{I}[\mathcal{S}_2] = \mathsf{T}$, $\mathsf{I}[\mathcal{S}_3] = \mathsf{F}$, and $\mathsf{I}[\mathcal{S}_4] = \mathsf{F}$.

Then, given the characteristic sentences, if $\mathcal{P}$ is F on every row, $\mathcal{S}_1 \wedge \sim\mathcal{S}_1$ has the same table as $\mathcal{P}$. Otherwise, where $\mathcal{P}$ is T on rows $a, b \ldots d$, $\mathcal{C}_a \vee \mathcal{C}_b \vee \ldots \mathcal{C}_d$ (with appropriate parentheses) has the same table as $\mathcal{P}$. Thus, for example, $\mathcal{C}_3 \vee \mathcal{C}_5 \vee \mathcal{C}_{12} \vee \mathcal{C}_{13}$, that is,

$$(\mathcal{S}_1 \wedge \mathcal{S}_2 \wedge \sim\mathcal{S}_3 \wedge \mathcal{S}_4) \vee (\mathcal{S}_1 \wedge \sim\mathcal{S}_2 \wedge \mathcal{S}_3 \wedge \mathcal{S}_4) \vee (\sim\mathcal{S}_1 \wedge \mathcal{S}_2 \wedge \sim\mathcal{S}_3 \wedge \sim\mathcal{S}_4) \vee (\sim\mathcal{S}_1 \wedge \sim\mathcal{S}_2 \wedge \mathcal{S}_3 \wedge \mathcal{S}_4)$$

has the same table as $\mathcal{P}$. Inserting parentheses, the resultant table is,

(D)

	$\mathcal{S}_1$	$\mathcal{S}_2$	$\mathcal{S}_3$	$\mathcal{S}_4$	$(\mathcal{C}_3$	$\vee$	$\mathcal{C}_5)$	$\vee$	$(\mathcal{C}_{12}$	$\vee$	$\mathcal{C}_{13})$	$\mathcal{P}$
1	T	T	T	T	F	F	F	***F***	F	F	F	***F***
2	T	T	T	F	F	F	F	***F***	F	F	F	***F***
3	T	T	F	T	T	T	F	***T***	F	F	F	***T***
4	T	T	F	F	F	F	F	***F***	F	F	F	***F***
5	T	F	T	T	F	T	T	***T***	F	F	F	***T***
6	T	F	T	F	F	F	F	***F***	F	F	F	***F***
7	T	F	F	T	F	F	F	***F***	F	F	F	***F***
8	T	F	F	F	F	F	F	***F***	F	F	F	***F***
9	F	T	T	T	F	F	F	***F***	F	F	F	***F***
10	F	T	T	F	F	F	F	***F***	F	F	F	***F***
11	F	T	F	T	F	F	F	***F***	F	F	F	***F***
12	F	T	F	F	F	F	F	***T***	T	T	F	***T***
13	F	F	T	T	F	F	F	***T***	F	T	T	***T***
14	F	F	T	F	F	F	F	***F***	F	F	F	***F***
15	F	F	F	T	F	F	F	***F***	F	F	F	***F***
16	F	F	F	F	F	F	F	***F***	F	F	F	***F***

And we have constructed an expression with the same table as $\mathcal{P}$. And similarly for any truth function with which we are confronted. So given any truth function, there is a formal expression with the same table.

In a by-now familiar pattern, the expressions produced by this method are not particularly elegant or efficient. Thus for the table,

(E)

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{P}$
T	T	***T***
T	F	***F***
F	T	***T***
F	F	***T***

by our method we get the expression $(\mathcal{A} \wedge \mathcal{B}) \vee (\sim\mathcal{A} \wedge \mathcal{B}) \vee (\sim\mathcal{A} \wedge \sim\mathcal{B})$. It has the right table. But, of course, $\mathcal{A} \rightarrow \mathcal{B}$ is much simpler! The point is not that the resultant expressions are elegant or efficient, but that for any truth function, there *exists* a formal expression that works the same way.

We have shown that we can represent any truth function by an expression with operators $\sim$, $\wedge$, and $\vee$. But any such expression is an abbreviation of one whose only operators are $\sim$ and $\rightarrow$. So we can represent any truth function by an expression with just operators $\sim$ and $\rightarrow$. And we can argue for other cases. Thus, for example,

T11.2. It is possible to represent any truth function by means of an expression with just the operators $\sim$ and $\wedge$.

Again, the proof is simple. Given T11.1, if we can show that any $\mathcal{P}$ whose operators are $\sim$, $\wedge$ and $\vee$ corresponds to a $\mathcal{P}^*$ whose operators are just $\sim$ and $\wedge$, such that $\mathcal{P}$ and $\mathcal{P}^*$ have the same table — such that $\mathsf{I}[\mathcal{P}] = \mathsf{I}[\mathcal{P}^*]$ for any I — we will have shown that any truth function can be represented by an expression with just $\sim$ and $\wedge$. To see that this is so, where $\mathcal{P}$ is an atomic $\mathcal{S}$, set $\mathcal{P}^* = \mathcal{S}$; where $\mathcal{P}$ is $\sim\mathcal{A}$, set $\mathcal{P}^* = \sim\mathcal{A}^*$; where $\mathcal{P}$ is $\mathcal{A} \wedge \mathcal{B}$, set $\mathcal{P}^* = \mathcal{A}^* \wedge \mathcal{B}^*$; and where $\mathcal{P}$ is $\mathcal{A} \vee \mathcal{B}$, set $\mathcal{P}^* = \sim(\sim\mathcal{A}^* \wedge \sim\mathcal{B}^*)$. Suppose the only operators in $\mathcal{P}$ are $\sim$, $\wedge$, and $\vee$, and consider an arbitrary interpretation I.

Basis: Where $\mathcal{P}$ is a sentence letter $\mathcal{S}$, then $\mathcal{P}^*$ is $\mathcal{S}$. So $\mathsf{I}[\mathcal{P}] = \mathsf{I}[\mathcal{P}^*]$.

Assp: For any i, $0 \leq i < k$, if $\mathcal{P}$ has i operator symbols, then $\mathsf{I}[\mathcal{P}] = \mathsf{I}[\mathcal{P}^*]$.

Show: If $\mathcal{P}$ has k operator symbols, then $\mathsf{I}[\mathcal{P}] = \mathsf{I}[\mathcal{P}^*]$.

If $\mathcal{P}$ has k operator symbols, then it is of the form $\sim\mathcal{A}$, $\mathcal{A} \wedge \mathcal{B}$, or $\mathcal{A} \vee \mathcal{B}$ where $\mathcal{A}$ and $\mathcal{B}$ have $< k$ operator symbols.

($\sim$) Suppose $\mathcal{P}$ is $\sim\mathcal{A}$; then $\mathcal{P}^*$ is $\sim\mathcal{A}^*$. $\mathsf{I}[\mathcal{P}] = \mathsf{T}$ iff $\mathsf{I}[\sim\mathcal{A}] = \mathsf{T}$; by ST($\sim$), iff $\mathsf{I}[\mathcal{A}] = \mathsf{F}$; by assumption iff $\mathsf{I}[\mathcal{A}^*] = \mathsf{F}$; by ST($\sim$), iff $\mathsf{I}[\sim\mathcal{A}^*] = \mathsf{T}$; iff $\mathsf{I}[\mathcal{P}^*] = \mathsf{T}$.

($\wedge$) Suppose $\mathcal{P}$ is $\mathcal{A} \wedge \mathcal{B}$; then $\mathcal{P}^*$ is $\mathcal{A}^* \wedge \mathcal{B}^*$. $\mathsf{I}[\mathcal{P}] = \mathsf{T}$ iff $\mathsf{I}[\mathcal{A} \wedge \mathcal{B}] = \mathsf{T}$; by ST′($\wedge$), iff $\mathsf{I}[\mathcal{A}] = \mathsf{T}$ and $\mathsf{I}[\mathcal{B}] = \mathsf{T}$; by assumption iff $\mathsf{I}[\mathcal{A}^*] = \mathsf{T}$ and $\mathsf{I}[\mathcal{B}^*] = \mathsf{T}$; by ST′($\wedge$), iff $\mathsf{I}[\mathcal{A}^* \wedge \mathcal{B}^*] = \mathsf{T}$; iff $\mathsf{I}[\mathcal{P}^*] = \mathsf{T}$.

($\vee$) Suppose $\mathcal{P}$ is $\mathcal{A} \vee \mathcal{B}$; then $\mathcal{P}^*$ is $\sim(\sim\mathcal{A}^* \wedge \sim\mathcal{B}^*)$. $\mathsf{I}[\mathcal{P}] = \mathsf{T}$ iff $\mathsf{I}[\mathcal{A} \vee \mathcal{B}] = \mathsf{T}$; by ST′($\vee$), iff $\mathsf{I}[\mathcal{A}] = \mathsf{T}$ or $\mathsf{I}[\mathcal{B}] = \mathsf{T}$; by assumption iff $\mathsf{I}[\mathcal{A}^*] = \mathsf{T}$ or $\mathsf{I}[\mathcal{B}^*] = \mathsf{T}$; by ST($\sim$), iff $\mathsf{I}[\sim\mathcal{A}^*] = \mathsf{F}$ or $\mathsf{I}[\sim\mathcal{B}^*] = \mathsf{F}$; by ST′($\wedge$), iff $\mathsf{I}[\sim\mathcal{A}^* \wedge \sim\mathcal{B}^*] = \mathsf{F}$; by ST($\sim$), iff $\mathsf{I}[\sim(\sim\mathcal{A}^* \wedge \sim\mathcal{B}^*)] = \mathsf{T}$; iff $\mathsf{I}[\mathcal{P}^*] = \mathsf{T}$.

If $\mathcal{P}$ has k operator symbols then $\mathsf{I}[\mathcal{P}] = \mathsf{I}[\mathcal{P}^*]$.

Indct: For any $\mathcal{P}$, $\mathsf{I}[\mathcal{P}] = \mathsf{I}[\mathcal{P}^*]$.

So if the operators in $\mathcal{P}$ are $\sim$, $\wedge$ and $\vee$, there is a $\mathcal{P}^*$ with just operators $\sim$ and $\wedge$ that has the same table. Perhaps this was obvious as soon as we saw that $\sim(\sim\mathcal{A} \wedge \sim\mathcal{B})$ has the same table as $\mathcal{A} \vee \mathcal{B}$. Since we can represent any truth function by an expression whose only operators are $\sim$, $\wedge$ and $\vee$, and we can represent any such $\mathcal{P}$ by a $\mathcal{P}^*$ whose only operators are $\sim$ and $\wedge$, we can represent any truth function by an expression with just operators $\sim$ and $\wedge$. And, by similar reasoning, we can represent any truth function by expressions whose only operators are $\sim$ and $\vee$, and by expressions whose only operator is $\mid$. This is left for homework.

In E8.11, we showed that if the operators in $\mathcal{P}$ are limited to $\rightarrow$, $\wedge$, $\vee$, and $\leftrightarrow$ then when the interpretation of every atomic is T, the interpretation of $\mathcal{P}$ is T. Perhaps this is obvious by consideration of the tables. It follows that not every truth function can be represented by expressions whose only operators are $\rightarrow$, $\wedge$, $\vee$, and $\leftrightarrow$; for there is no way to represent a function that is F on the top row, when all the atomics are T. Though it is much more difficult to establish, we showed in E8.20 that any expression whose only operators are $\sim$ and $\leftrightarrow$ (with at least four rows in its truth table) has an even number of Ts and Fs under its main operator. It follows that not every truth function can be represented by expressions whose only operators are $\sim$ and $\leftrightarrow$.

E11.1. Use the method of this section to find expressions with tables corresponding to $\mathcal{P}_1$, $\mathcal{P}_2$, and $\mathcal{P}_3$. Then show on a table that your expression for $\mathcal{P}_1$ in fact has the same truth function as $\mathcal{P}_1$.

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{P}_1$	$\mathcal{P}_2$	$\mathcal{P}_3$
T	T	T	F	T	F
T	T	F	T	T	F
T	F	T	T	F	T
T	F	F	F	F	F
F	T	T	F	F	T
F	T	F	T	F	F
F	F	T	F	F	T
F	F	F	T	F	T

E11.2. (i) Show that we can represent any truth function by expressions whose only operators are $\sim$ and $\vee$. (ii) Show that we can represent any truth function by expressions whose only operator is $\mid$. Hint: Given what we have shown above, it is enough to show that you can represent expressions whose only operators are $\sim$ and $\rightarrow$, or $\sim$ and $\wedge$.

E11.3. Show that it is not possible to represent arbitrary truth functions by expressions whose only operator is $\sim$. Hint: it is easy to show by induction that any such expression has at least one T and one F under its main operator.

11.2 Unique Readability

Unique readability is a result like our first case from chapter 8 (p. 387) where the conclusion may seem to obvious to merit argument. We show that every formula of $\mathcal{L}_s$ is parsed uniquely. Things are set up so that this is so. But suppose instead of FR($\to$) we had,

($*$) If $\mathcal{P}$ and $\mathcal{Q}$ are formulas, then $\mathcal{P} \to \mathcal{Q}$ is a *formula*.

without parentheses. Then, for atomics A, B and C, say, $A \to B$ is a formula so that $A \to B \to C$ is a formula. But again, $B \to C$ is a formula so that $A \to B \to C$ is a formula. So there are different ways to understand the parts of $A \to B \to C$. Suppose $\mathsf{I}[A] = \mathsf{I}[B] = \mathsf{I}[C] = \mathsf{F}$. Then on the first account, $\mathsf{I}[A \to B] = \mathsf{T}$ so that $\mathsf{I}[A \to B \to C] = \mathsf{F}$. But on the second account, $\mathsf{I}[B \to C] = \mathsf{T}$ so that $\mathsf{I}[A \to B \to C] = \mathsf{T}$. Thus it is important for our definitions that there is just one way to understand $\mathcal{P} \to \mathcal{Q}$. And we can demonstrate the result. According to unique readability,

T11.3. For any formula $\mathcal{P}$ of $\mathcal{L}_s$, exactly one of the following holds.

(s) $\mathcal{P}$ is a sentence letter.

($\sim$) There is a unique formula $\mathcal{A}$ such that $\mathcal{P}$ is $\sim\mathcal{A}$.

($\to$) There are unique formulas $\mathcal{A}$ and $\mathcal{B}$ such that $\mathcal{P}$ is $(\mathcal{A} \to \mathcal{B})$.

We build to this result by some preliminary theorems.

First, ignoring uniqueness,

T11.4. For any formula $\mathcal{P}$ of $\mathcal{L}_s$, at least one of the following holds: (i) $\mathcal{P}$ is a sentence letter; (ii) there is a formula $\mathcal{A}$ such that $\mathcal{P}$ is $\sim\mathcal{A}$; (iii) there are formulas $\mathcal{A}$ and $\mathcal{B}$ such that $\mathcal{P}$ is $(\mathcal{A} \to \mathcal{B})$.

This is a (trivial) induction on the number of operators in $\mathcal{P}$.

T11.5. For any formula $\mathcal{P}$ of $\mathcal{L}_s$, at most one of the following holds: (i) $\mathcal{P}$ is a sentence letter; (ii) there is a formula $\mathcal{A}$ such that $\mathcal{P}$ is $\sim\mathcal{A}$; (iii) there are formulas $\mathcal{A}$ and $\mathcal{B}$ such that $\mathcal{P}$ is $(\mathcal{A} \rightarrow \mathcal{B})$.

If $\mathcal{P}$ is a sentence letter it begins with a sentence letter; if $\mathcal{P}$ is $\sim\mathcal{A}$ it begins with '$\sim$'; and if $\mathcal{P}$ is $(\mathcal{A} \rightarrow \mathcal{B})$ it begins with '('. (i) Suppose $\mathcal{P}$ is a sentence letter; then it does not begin with '$\sim$' or '('; so not (ii) and not (iii). Suppose $\mathcal{P}$ is $\sim\mathcal{A}$; then it does not begin with a sentence letter or '('; so not (i) or (iii). Suppose $\mathcal{P}$ is $(\mathcal{A} \rightarrow \mathcal{B})$; then it does not begin with a sentence letter or '$\sim$' so not (i) or (ii).

By T11.4 and T11.5 together, For any formula $\mathcal{P}$ of $\mathcal{L}_s$, exactly one of, (i) $\mathcal{P}$ is a sentence letter; (ii) there is a formula $\mathcal{A}$ such that $\mathcal{P}$ is $\sim\mathcal{A}$; (iii) there are formulas $\mathcal{A}$ and $\mathcal{B}$ such that $\mathcal{P}$ is $(\mathcal{A} \rightarrow \mathcal{B})$.

For some expression $\mathcal{A}$ say $\mathcal{B}$ is an *initial segment* of $\mathcal{A}$ just in case there is some $\mathcal{C}$ such that $\mathcal{A} = \mathcal{B}\mathcal{C}$ — just in case $\mathcal{A}$ is the concatenation of $\mathcal{B}$ and $\mathcal{C}$. If $\mathcal{C}$ is a non-empty sequence so that $\mathcal{B}$ is not all of $\mathcal{A}$, then $\mathcal{B}$ is a *proper* initial segment of $\mathcal{A}$. So 'AB' is a proper initial segment of 'ABC'. To make progress on the uniqueness conditions, we show the following.

T11.6. No proper initial segment of a formula $\mathcal{A}$ is a formula. Suppose $\mathcal{A}$ is a formula.

Basis: If $\mathcal{A}$ is atomic, then $\mathcal{A} = \mathcal{B}\mathcal{C}$ only if $\mathcal{A} = \mathcal{C}$ and $\mathcal{B}$ is empty. But from T11.4 no empty sequence is a formula. So no proper initial segment of $\mathcal{A}$ is a formula.

Assp: For any i, $0 \leq i < k$, if $\mathcal{A}$ has i operator symbols, then no proper initial segment of $\mathcal{A}$ is a formula.

Show: If $\mathcal{A}$ has k operator symbols, then no proper initial segment of $\mathcal{A}$ is a formula. If $\mathcal{A}$ has k operator symbols then it is $\sim\mathcal{P}$ or $(\mathcal{P} \wedge \mathcal{Q})$ for formulas $\mathcal{P}$ and $\mathcal{Q}$ with $< k$ operator symbols.

($\sim$) $\mathcal{A}$ is $\sim\mathcal{P}$ for some formula $\mathcal{P}$. Suppose some proper initial segment of $\mathcal{A}$ is a formula; then for some formula $\mathcal{B}$, $\mathcal{A} = \mathcal{B}\mathcal{C}$. $\mathcal{B}$ is either empty or starts with '$\sim$'; so with T11.4 and T11.5, $\mathcal{B}$ is $\sim\mathcal{D}$ for some formula $\mathcal{D}$. So $\mathcal{A} = \sim\mathcal{P} = \sim\mathcal{D}\mathcal{C}$; so $\mathcal{P} = \mathcal{D}\mathcal{C}$; so $\mathcal{D}$ is a proper initial segment of $\mathcal{P}$; so by assumption, $\mathcal{D}$ is not a formula. Reject the assumption: no proper initial segment of $\mathcal{A}$ is a formula.

($\rightarrow$) $\mathcal{A}$ is $(\mathcal{P} \rightarrow \mathcal{Q})$. Suppose some proper initial segment of $\mathcal{A}$ is a formula; then for some formula $\mathcal{B}$, $\mathcal{A} = \mathcal{B}\mathcal{C}$. $\mathcal{B}$ is either empty or starts with '('; so with with T11.4 and T11.5, $\mathscr{B}$ is $(\mathscr{D} \rightarrow \mathscr{E})$ for some formulas $\mathscr{D}$ and $\mathscr{E}$; so $\mathscr{A} = (\mathscr{P} \rightarrow \mathscr{Q}) = (\mathscr{D} \rightarrow \mathscr{E})\mathscr{C}$; so $\mathscr{P} \rightarrow \mathscr{Q}) = \mathscr{D} \rightarrow \mathscr{E})\mathscr{C}$; so either $\mathscr{P} = \mathscr{D}$ or one is a proper initial segment of the other; suppose one is a proper initial segment of the other; then by assumption one or the other is not a formula; this is impossible. So $\mathscr{P} = \mathscr{D}$; so $\mathscr{Q}) = \mathscr{E})\mathscr{C}$; so $\mathscr{E}$ is a proper initial segment of $\mathscr{Q}$; so by assumption $\mathscr{E}$ is not a formula. Reject the assumption, no proper initial segment of $\mathscr{A}$ is a formula.

Indct: For any formula $\mathscr{A}$, no proper initial segment of $\mathscr{A}$ is a formula.

Observe that we "add" and "subtract" from sequences so that, for example $\sim\mathscr{P} = \sim\mathscr{Q}$ iff $\mathscr{P} = \mathscr{Q}$.

And now we are ready to establish T11.3 for unique readability. For any formula $\mathscr{P}$ of $\mathscr{L}_s$, by T11.4 and T11.5, exactly one of,

(i) $\mathscr{P}$ is a sentence letter.

(ii) There is a formula $\mathscr{A}$ such that $\mathscr{P}$ is $\sim\mathscr{A}$.

Uniqueness: Suppose there is a formula $\mathscr{B}$ such that $\sim\mathscr{A} = \sim\mathscr{B}$; then $\mathscr{A} = \mathscr{B}$. So there is a unique formula $\mathscr{A}$ such that $\mathscr{P} = \sim\mathscr{A}$.

(iii) There are formulas $\mathscr{A}$ and $\mathscr{B}$ such that $\mathscr{P}$ is $(\mathscr{A} \rightarrow \mathscr{B})$.

Uniqueness: Suppose there are formulas $\mathscr{C}$ and $\mathscr{D}$ such that $(\mathscr{A} \rightarrow \mathscr{B}) = (\mathscr{C} \rightarrow \mathscr{D})$; then $\mathscr{A} \rightarrow \mathscr{B}) = \mathscr{C} \rightarrow \mathscr{D})$; so either $\mathscr{A} = \mathscr{C}$ or one is a proper initial segment of the other; but by T11.6, neither is a proper initial segment of the other; so $\mathscr{A} = \mathscr{C}$; so $\mathscr{B}) = \mathscr{D})$; so $\mathscr{B} = \mathscr{D}$. So there are unique formulas $\mathscr{A}$ and $\mathscr{B}$ such that $\mathscr{P} = (\mathscr{A} \rightarrow \mathscr{B})$.

Thus T11.3 is established.

E11.4. Demonstrate T11.4 by induction on the length of $\mathscr{P}$.

E11.5. Show unique readability for the terms of $\mathscr{L}_q$, that for every term t of $\mathscr{L}_q$, exactly one of the following holds,

(v) t is a variable.

(c) t is a constant.

(f) There are unique function symbol h^n and terms $t_1 \dots t_n$ such that $t = h^n t_1 \dots t_n$.

Hint: The argument is based on TR; you will want to show that no proper initial segment of a term is a term.

E11.6. Show unique readability for the formulas of $\mathcal{L}_q$, that for every formula $\mathcal{P}$ of $\mathcal{L}_q$, exactly one of the following holds,

(s) $\mathcal{P}$ is a sentence letter.

(r) There are unique relation symbol $\mathcal{R}^n$ and terms $t_1 \dots t_n$ such that $\mathcal{P} = \mathcal{R}^n t_1 \dots t_n$.

($\sim$) There is a unique formula $\mathcal{A}$ such that $\mathcal{P} = \sim\mathcal{A}$.

($\rightarrow$) There are unique formulas $\mathcal{A}$ and $\mathcal{B}$ such that $\mathcal{P} = (\mathcal{A} \rightarrow \mathcal{B})$.

($\forall$) There are unique variable x and formula $\mathcal{A}$ such that $\mathcal{P} = \forall x \mathcal{A}$.

Hint: This time the argument is based on FR.

11.3 Independence

As we have seen, axiomatic systems are convenient insofar as their compact form makes reasoning about them relatively easy. Also, theoretically, axiomatic systems are attractive insofar as they expose what is at the base or foundation of logical systems. Given this latter aim, it is natural to wonder whether we could get the same results without one or more of our axioms. Say an axiom or rule is *independent* in a derivation system just in case its omission matters for what can be derived. In particular, then, an axiom is independent in a derivation system if *it* cannot be derived from the other axioms and rules. For suppose otherwise: that it can be derived from the other axioms and rules; then it is a theorem of the derivation system without the axiom, and any result of the system with the axiom can be derived using the theorem in place of the axiom; so the omission of the axiom does not matter for what can be derived, and the axiom is not independent. In this section, we show that A1, A2 and A3 of the sentential fragment of *AD* are independent of one another.

Say we want to show that A1 is independent of A2 and A3. When we showed, in chapter 8, that the sentential part of *AD* is weakly sound, we showed that A1, A2, A3 and their consequences have a certain feature — that there is no interpretation where a consequence is false. The basic idea here is to find a sort of "interpretation" on which A2, A3 and their consequences are sustained, but A1 is not. It follows that A1 is not among the consequences of A2 and A3, and so is independent of A2 and A3. Here is the key point: Any "interpretation" will do. In particular, consider the following tables which define a sort of numerical property for forms involving $\sim$ and $\rightarrow$.

A1($\sim$)

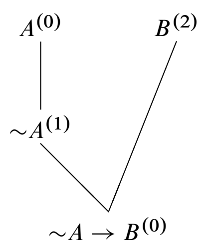
$\mathcal{P}$	$\sim\mathcal{P}$
0	1
1	1
2	0

A1($\rightarrow$)

$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{P} \rightarrow \mathcal{Q}$
0	0	0
0	1	2
0	2	2
1	0	2
1	1	2
1	2	0
2	0	0
2	1	0
2	2	0

Do not worry about what these tables "say"; it is sufficient that, given a numerical interpretation of the parts, we can always calculate the numerical value N of the whole. Thus, for example,

(F)



By A1($\sim$) row 1

By A1($\rightarrow$) row 6

if $\mathsf{N}[A] = 0$ and $\mathsf{N}[B] = 2$, then $\mathsf{N}[\sim A \rightarrow B] = 0$. The calculation is straightforward, based on the tables. And similarly for sentential forms of arbitrary complexity. Say a form is *select* iff it takes the value 0 on every numerical interpretation of its parts. (Compare the notion of semantic validity on which a form is valid iff it is T on every interpretation of its parts.) Again, do not worry about what the tables mean. They are constructed for the special purpose of demonstrating independence: We show that every consequence of A2 and A3 is select, but A1 is not. It follows that A1 is not a consequence of A2 and A3.

To see that A3 is select, and that A1 is not, all we have to do is complete the tables.

(G)

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \to (\mathcal{B} \to \mathcal{A})$		$(\sim\mathcal{B} \to \sim\mathcal{A}) \to [(\sim\mathcal{B} \to \mathcal{A}) \to \mathcal{B}]$						
0	0	***0***	0	1	2	1	***0***	1	2	0
0	1	***2***	2	1	2	1	***0***	1	2	0
0	2	***0***	0	0	2	1	***0***	0	0	2
1	0	***0***	2	1	2	1	***0***	1	2	0
1	1	***0***	2	1	2	1	***0***	1	2	0
1	2	***2***	0	0	2	1	***0***	0	2	0
2	0	***0***	2	1	2	0	***0***	1	0	0
2	1	***0***	0	1	2	0	***0***	1	0	2
2	2	***0***	0	0	0	0	***0***	0	2	0

Since A1 has twos in the second and sixth rows, A1 is not select. Since A3 has zeros in every row, it is select. Alternatively, for A1, we might have reasoned as follows,

> Suppose $\mathsf{N}[\mathcal{A}] = 0$ and $\mathsf{N}[\mathcal{B}] = 1$. Then by A1(→), $\mathsf{N}[\mathcal{B} \to \mathcal{A}] = 2$; so by A1(→) again, $\mathsf{N}[\mathcal{A} \to (\mathcal{B} \to \mathcal{A})] = 2$. Since there is such an assignment, $\mathcal{A} \to (\mathcal{B} \to \mathcal{A})$ is not select.

And the result is the same. To see that A2 is select, again, it is enough to complete the table — it is painful, but we can do it:

(H)

$\mathscr{A}$	$\mathscr{B}$	$\mathscr{C}$	$(\mathscr{A} \to$	$(\mathscr{B} \to \mathscr{C}))$	$\to$	$((\mathscr{A} \to \mathscr{B})$	$\to$	$(\mathscr{A} \to \mathscr{C}))$
0	0	0	0	0	***0***	0	0	0
0	0	1	2	2	***0***	0	2	2
0	0	2	2	2	***0***	0	2	2
0	1	0	2	2	***0***	2	0	0
0	1	1	2	2	***0***	2	0	2
0	1	2	0	0	***0***	2	0	2
0	2	0	0	0	***0***	2	0	0
0	2	1	0	0	***0***	2	0	2
0	2	2	0	0	***0***	2	0	2
1	0	0	2	0	***0***	2	0	2
1	0	1	0	2	***0***	2	0	2
1	0	2	0	2	***0***	2	0	0
1	1	0	0	2	***0***	2	0	2
1	1	1	0	2	***0***	2	0	2
1	1	2	2	0	***0***	2	0	0
1	2	0	2	0	***0***	0	2	2
1	2	1	2	0	***0***	0	2	2
1	2	2	2	0	***0***	0	0	0
2	0	0	0	0	***0***	0	0	0
2	0	1	0	2	***0***	0	0	0
2	0	2	0	2	***0***	0	0	0
2	1	0	0	2	***0***	0	0	0
2	1	1	0	2	***0***	0	0	0
2	1	2	0	0	***0***	0	0	0
2	2	0	0	0	***0***	0	0	0
2	2	1	0	0	***0***	0	0	0
2	2	2	0	0	***0***	0	0	0

So both A2 and A3 are select. But now we are in a position to show,

T11.7. A1 is independent of A2 and A3.

Consider any derivation $\langle \mathcal{Q}_1, \mathcal{Q}_2 \ldots \mathcal{Q}_n \rangle$ where there are no premises, and the only axioms are instances of A2 and A3. By induction on line number, for any i, $\mathcal{Q}_i$ is select.

Basis: $\mathcal{Q}_1$ is an instance of A2 or A3, and as we have just seen, instances of A2 and A3 are select. So $\mathcal{Q}_1$ is select.

Assp: For any i, $0 \leq i < k$, $\mathcal{Q}_i$ is select.

Show: $\mathcal{Q}_k$ is select.

$\mathcal{Q}_k$ is an instance of A2 or A3 or arises from previous lines by MP. If $\mathcal{Q}_k$ is an instance of A2 or A3, then by reasoning as in the basis, $\mathcal{Q}_k$ is select. If $\mathcal{Q}_k$ arises from previous lines by MP, then the derivation has some lines,

a. $\mathscr{B}$
b. $\mathscr{B} \rightarrow \mathscr{C}$
k. $\mathscr{C}$ $\qquad$ a,b MP

where $a, b < k$ and $\mathscr{C}$ is $\mathscr{Q}_k$. By assumption, $\mathscr{B}$ and $\mathscr{B} \rightarrow \mathscr{C}$ are select. But by A1($\rightarrow$), both $\mathscr{B}$ and $\mathscr{B} \rightarrow \mathscr{C}$ evaluate to 0 only in the case when $\mathscr{C}$ also evaluates to 0; so if both $\mathscr{B}$ and $\mathscr{B} \rightarrow \mathscr{C}$ are select, then $\mathscr{C}$ is select as well. So $\mathscr{Q}_k$ is select.

Indct: For any n, $\mathscr{Q}_n$ is select.

So A1 cannot be derived from A2 and A3 — which is to say, A1 is independent of A2 and A3.

E11.7. Use the following tables to show that A2 is independent of A1 and A3.

A2($\sim$)

$\mathscr{P}$	$\sim\mathscr{P}$
0	1
1	0
2	1

A2($\rightarrow$)

$\mathscr{P}$	$\mathscr{Q}$	$\mathscr{P} \rightarrow \mathscr{Q}$
0	0	0
0	1	2
0	2	1
1	0	0
1	1	2
1	2	0
2	0	0
2	1	0
2	2	0

E11.8. Use the table method to show that A3 is independent of A1 and A2. That is, (i) find appropriate tables for $\sim$ and $\rightarrow$, and (ii) use your tables to show by induction that A3 is independent of A1 and A2. Hint: You do not need three-valued interpretations, and have already done the work in E8.14.

11.4 Isomorphic Models

Interpretations are *isomorphic* when they are structurally similar. Say a function f from r^n to s is *onto* set s just in case for each $\mathsf{o} \in \mathsf{s}$ there is some $\langle \mathsf{m}_1 \dots \mathsf{m}_n \rangle \in \mathsf{r}^n$ such that $\langle \langle \mathsf{m}_1 \dots \mathsf{m}_n \rangle, \mathsf{o} \rangle \in \mathsf{f}$; a function is onto set s when it "reaches" every member of s. Then, IS For some language $\mathcal{L}$, interpretation I is *isomorphic* to interpretation I' iff there is a 1:1 function ι (iota) from the universe of I onto the universe of I' where: for any sentence letter $\mathcal{S}$, $\mathsf{I}[\mathcal{S}] = \mathsf{I}'[\mathcal{S}]$; for any constant c, $\mathsf{I}[c] = \mathsf{m}$ iff $\mathsf{I}'[c] = \iota(\mathsf{m})$; for any relation symbol $\mathcal{R}^n$, $\langle \mathsf{m}_a \dots \mathsf{m}_b \rangle \in \mathsf{I}[\mathcal{R}^n]$ iff $\langle \iota(\mathsf{m}_a) \dots \iota(\mathsf{m}_b) \rangle \in \mathsf{I}'(\mathcal{R}^n)$; and for any function symbol h^n, $\langle \langle \mathsf{m}_a \dots \mathsf{m}_b \rangle, \mathsf{o} \rangle \in \mathsf{I}[h^n]$ iff $\langle \langle \iota(\mathsf{m}_a) \dots \iota(\mathsf{m}_b) \rangle, \iota(\mathsf{o}) \rangle \in \mathsf{I}'[h^n]$.

If I is isomorphic to I', we write, $\mathsf{I} \cong \mathsf{I}'$. Notice that the condition on constants requires just that $\iota(\mathsf{I}[c]) = \mathsf{I}'[c]$; applying ι to the thing assigned to c by I, results in the thing assigned to c by I'. And similarly, the condition on function symbols requires that $\iota(\mathsf{I}[h^n]\langle \mathsf{m}_a \dots \mathsf{m}_b \rangle) = \mathsf{I}'[h^n]\langle \iota(\mathsf{m}_a) \dots \iota(\mathsf{m}_b) \rangle$; for we have $\mathsf{I}[h^n]\langle \mathsf{m}_a \dots \mathsf{m}_b \rangle = \mathsf{o}$, and $\iota(\mathsf{o}) = \mathsf{I}'[h^n]\langle \iota(\mathsf{m}_a) \dots \iota(\mathsf{m}_b) \rangle$. We might think of the two interpretations as already existing, and *finding* a function ι to exhibit them as isomorphic. Alternatively, given an interpretation I, and function ι from the universe of I onto some set U', we might think of I' as resulting from application of ι to I.

Here are some examples. In the first, it is perhaps particularly obvious that I and I' have the required structural similarity.

(I)

U :	Rover	Fido	Morris	Sylvester
	↓	↓	↓	↓
U′ :	Ralph	Fredo	Manny	Salvador

U = {Rover, Fido, Morris, Sylvester}. As represented by the arrows, function ι maps these onto a disjoint set U'. Then given I as below on the left, the corresponding isomorphic interpretation is I' as on the right.

$\mathsf{I}[r]$ = Rover	$\mathsf{I}'[r]$ = Ralph
$\mathsf{I}[m]$ = Morris	$\mathsf{I}'[m]$ = Manny
$\mathsf{I}[D]$ = {Rover, Fido}	$\mathsf{I}'[D]$ = {Ralph, Fredo}
$\mathsf{I}[C]$ = {Morris, Sylvester}	$\mathsf{I}'[C]$ = {Manny, Salvador}
$\mathsf{I}[P]$ = {⟨Rover, Morris⟩, ⟨Fido, Sylvester⟩}	$\mathsf{I}'[P]$ = {⟨Ralph, Manny⟩, ⟨Fredo, Salvador⟩}

On interpretation I, where Rover and Fido are dogs, and Morris and Sylvester are cats, we have that every dog pursues at least one cat. And, supposing that Ralph and Fredo are dogs, and Manny and Salvador are cats, the same properties and relations are preserved on I' — with only the particular individuals changed.

For a second case, let U be the same, but U' the very same set, only permuted or shuffled so that each object in U has a mate in U'.

(J)

U :	Rover	Fido	Morris	Sylvester
	↓	↓	↓	↓
U′ :	Rover	Morris	Fido	Sylvester

So ι maps members of U to members of the very same set. Then given I as before, the corresponding isomorphic interpretation is I' is as follows.

$\mathsf{I}[r]$ = Rover	$\mathsf{I}'[r]$ = Rover
$\mathsf{I}[m]$ = Morris	$\mathsf{I}'[m]$ = Fido
$\mathsf{I}[D]$ = {Rover, Fido}	$\mathsf{I}'[D]$ = {Rover, Morris}
$\mathsf{I}[C]$ = {Morris, Sylvester}	$\mathsf{I}'[C]$ = {Fido, Sylvester}
$\mathsf{I}[P]$ = {⟨Rover, Morris⟩, ⟨Fido, Sylvester⟩}	$\mathsf{I}'[P]$ = {⟨Rover, Fido⟩, ⟨Morris, Sylvester⟩}

This time, there is no simple way to understand $\mathsf{I}'[D]$ as the set of all dogs, and $\mathsf{I}'[C]$ as the set of all cats. And we cannot say that the interpretation of P reflects dogs pursuing cats. But Morris *plays the same role* in I' as Fido in I; and similarly Fido plays the same role in I' as Morris in I. Thus, on I', each thing in the interpretation of D is such that it stands in the relation P to at least one thing in the interpretation of C — and this is just as in interpretation I.

A final example switches to $\mathscr{L}_{NT}^{<}$ and has an infinite U. We let U be the set $\mathbb{N}$ of natural numbers, U' be the set $\mathbb{P}$ of positive integers, and ι be the function $n + 1$.

$$\text{(K)}\qquad \begin{array}{lccccc} \mathsf{U}: & 0 & 1 & 2 & 3 & \dots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \\ \mathsf{U}': & 1 & 2 & 3 & 4 & \dots \end{array}$$

Then where N is the standard interpretation for symbols of $\mathscr{L}_{NT}^{<}$,

$\mathsf{N}[\emptyset] = 0$

$\mathsf{N}[<] = \{\langle \mathsf{m}, \mathsf{n}\rangle \mid \mathsf{m}, \mathsf{n} \in \mathbb{N}$, and m is less than $\mathsf{n}\}$

$\mathsf{N}[S] = \{\langle \mathsf{m}, \mathsf{n}\rangle \mid \mathsf{m}, \mathsf{n} \in \mathbb{N}$, and n is the successor of $\mathsf{m}\}$

$\mathsf{N}[+] = \{\langle\langle \mathsf{m}, \mathsf{n}\rangle, \mathsf{o}\rangle \mid \mathsf{m}, \mathsf{n}, \mathsf{o} \in \mathbb{N}$, and m plus n equals $\mathsf{o}\}$

we obtain N' as follows,

$\mathsf{N}'[\emptyset] = 1$

$\mathsf{N}'[<] = \{\langle \mathsf{m}+1, \mathsf{n}+1\rangle \mid \mathsf{m}, \mathsf{n} \in \mathbb{N}$, and m is less than $\mathsf{n}\}$

$\mathsf{N}'[S] = \{\langle \mathsf{m}+1, \mathsf{n}+1\rangle \mid \mathsf{m}, \mathsf{n} \in \mathbb{N}$, and n is the successor of $\mathsf{m}\}$

$\mathsf{N}'[+] = \{\langle\langle \mathsf{m}+1, \mathsf{n}+1\rangle, \mathsf{o}+1\rangle \mid \mathsf{m}, \mathsf{n}, \mathsf{o} \in \mathbb{N}$, and m plus n equals $\mathsf{o}\}$

Observe that anything in N' is taken from $\mathbb{P}$. In this case, we build N' explicitly by the rule for isomorphisms — simply finding $\iota(\mathsf{m}) = \mathsf{m} + 1$ from the corresponding element of N.

11.4.1 Isomorphism implies Equivalence

Given these examples, perhaps it is obvious that when interpretations are isomorphic, they make all the same formulas true.[2] Say,

EE For some language $\mathcal{L}$, interpretations I and I' are *elementarily equivalent* iff for any formula $\mathcal{P}$, $\mathsf{I}[\mathcal{P}] = \mathsf{T}$ iff $\mathsf{I}'[\mathcal{P}] = \mathsf{T}$.

If I is elementarily equivalent to I', write $\mathsf{I} \equiv \mathsf{I}'$. We show that isomorphic interpretations are elementarily equivalent. This is straightforward given a matched pair of results, of the sort we have often seen before.

T11.8. For some language $\mathcal{L}$, if interpretations $\mathsf{D} \cong \mathsf{H}$, and assignments d for D and h for H are such that for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$, then for any term t, $\iota(\mathsf{D_d}[t]) = \mathsf{H_h}[t]$.

Suppose $\mathsf{D} \cong \mathsf{H}$, and corresponding assignments d and h are such that for any x, $\iota(\mathsf{d}(x)) = \mathsf{h}(x)$. By induction on the number of operator symbols in t.

Basis: If t has no function symbols, then it is a variable or a constant. If t is a variable x, then by TA(v), $\mathsf{D_d}[x] = \mathsf{d}(x)$; so $\iota(\mathsf{D_d}[x]) = \iota(\mathsf{d}[x])$; but we have supposed $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$; and by TA(v) again, $\mathsf{h}[x] = \mathsf{H_h}[x]$; so $\iota(\mathsf{D_d}[x]) = \mathsf{H_h}[x]$. If t is a constant c, then by TA(c), $\mathsf{D_d}[c] = \mathsf{D}[c]$; so $\iota(\mathsf{D_d}[c]) = \iota(\mathsf{D}[c])$; but since $\mathsf{D} \cong \mathsf{H}$, $\iota(\mathsf{D}[c]) = \mathsf{H}[c]$; and by TA(c) again, $\mathsf{H}[c] = \mathsf{H_h}[c]$; so $\iota(\mathsf{D_d}[c]) = \mathsf{H_h}[c]$.

Assp: For any i, $0 \le i < k$ if t has i function symbols, then $\iota(\mathsf{D_d}[t]) = \mathsf{H_h}[t]$.

Show: If t has k function symbols, then $\iota(\mathsf{D_d}[t]) = \mathsf{H_h}[t]$.

If t has k function symbols, then it is of the form $h^n t_1 \dots t_n$ for relation symbol h^n and terms $t_1 \dots t_n$ with $< k$ function symbols. Then $\mathsf{D_d}[t] = \mathsf{D_d}[h^n t_1 \dots t_n]$; by TA(f), $\mathsf{D_d}[h^n t_1 \dots t_n] = \mathsf{D}[h^n]\langle \mathsf{D_d}[\mathsf{t}_1] \dots \mathsf{D_d}[\mathsf{t}_n]\rangle$. So $\iota(\mathsf{D_d}[t]) = \iota(\mathsf{D}[h^n]\langle \mathsf{D_d}[\mathsf{t}_1] \dots \mathsf{D_d}[\mathsf{t}_n]\rangle)$; but since $\mathsf{D} \cong \mathsf{H}$, $\iota(\mathsf{D}[h^n]\langle \mathsf{D_d}[\mathsf{t}_1] \dots \mathsf{D_d}[\mathsf{t}_n]\rangle) = \mathsf{H}[h^n]\langle \iota(\mathsf{D_d}[\mathsf{t}_1]) \dots \iota(\mathsf{D_d}[\mathsf{t}_n])\rangle$; and by assumption, $\iota(\mathsf{D_d}[t_1]) = \mathsf{H_h}[t_1]$, and …and $\iota(\mathsf{D_d}[t_n]) = \mathsf{H_h}[t_n]$; so $\mathsf{H}[h^n]\langle \iota(\mathsf{D_d}[\mathsf{t}_1]) \dots \iota(\mathsf{D_d}[\mathsf{t}_n])\rangle = \mathsf{H}[h^n]\langle \mathsf{H_h}[\mathsf{t}_1] \dots \mathsf{H_h}[\mathsf{t}_n]\rangle$; and by TA(f), $\mathsf{H}[h^n]\langle \mathsf{H_h}[\mathsf{t}_1] \dots \mathsf{H_h}[\mathsf{t}_n]\rangle = \mathsf{H_h}[h^n t_1 \dots t_n]$; which is just $\mathsf{H_h}[t]$; so $\iota(\mathsf{D_d}[t]) = \mathsf{H_h}[t]$.

[2] In *Reason, Truth and History*, Hilary Putnam makes this point to show that truth values of sentences are not sufficient to fix the interpretation of a language. As we shall see in this section, the technical point is clear enough. It is another matter whether it bears the philosophical weight he means for it to bear!

Indct: For any t, $\iota(\mathsf{D_d}[t]) = \mathsf{H_h}[t]$.

So when D and H are isomorphic, and for any variable x, ι maps $\mathsf{d}[x]$ to $\mathsf{h}[x]$, then for any term t, ι maps $\mathsf{D_d}[t]$ to $\mathsf{H_h}[t]$.

Now we are in a position to extend the result to one for satisfaction of formulas. If D and H are isomorphic, and for any variable x, ι maps $\mathsf{d}[x]$ to $\mathsf{h}[x]$, then a formula $\mathcal{P}$ will be satisfied on D with d just in case it is satisfied on H with h.

T11.9. For some language $\mathcal{L}$, if interpretations $\mathsf{D} \cong \mathsf{H}$, and assignments d for D and h for H are such that for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$, then for any formula $\mathcal{P}$, $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

By induction on the number of operators in $\mathcal{P}$. Suppose $\mathsf{D} \cong \mathsf{H}$.

Basis: Suppose $\mathcal{P}$ has no operator symbols and d and h are such that for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$. If $\mathcal{P}$ has no operator symbols, then it is sentence letter $\mathcal{S}$ or an atomic $\mathcal{R}^n t_1 \ldots t_n$ for relation symbol $\mathcal{R}^n$ and terms $t_1 \ldots t_n$. Suppose the former; then by SF(s), $\mathsf{D_d}[\mathcal{S}] = \mathsf{S}$ iff $\mathsf{D}[\mathcal{S}] = \mathsf{T}$; since $\mathsf{D} \cong \mathsf{H}$ iff $\mathsf{H}[\mathcal{S}] = \mathsf{T}$; by SF(s), iff $\mathsf{H_h}[\mathcal{S}] = \mathsf{S}$. Suppose the latter; by SF(r), $\mathsf{D_d}[\mathcal{R}^n t_1 \ldots t_n] = \mathsf{S}$ iff $\langle \mathsf{D_d}[t_1] \ldots \mathsf{D_d}[t_n] \rangle \in \mathsf{D}[\mathcal{R}^n]$; since $\mathsf{D} \cong \mathsf{H}$, iff $\langle \iota(\mathsf{D_d}[t_1]) \ldots \iota(\mathsf{D_d}[t_n]) \rangle \in \mathsf{H}[\mathcal{R}^n]$; since $\mathsf{D} \cong \mathsf{H}$ and $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$, by T11.8, iff $\langle \mathsf{H_h}[t_1] \ldots \mathsf{H_h}[t_n]) \rangle \in \mathsf{H}[\mathcal{R}^n]$; by SF(r), iff $\mathsf{H_h}[\mathcal{R}^n t_1 \ldots t_n] = \mathsf{S}$.

Assp: For any i, $0 \le i < k$, for d and h such that for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$ and $\mathcal{P}$ with i operator symbols, $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

Show: For d and h such that for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$ and $\mathcal{P}$ with k operator symbols, $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

If $\mathcal{P}$ has k operator symbols, then it is of the form $\sim\mathcal{A}$, $\mathcal{A} \to \mathcal{B}$, or $\forall x \mathcal{A}$ for variable x and formulas $\mathcal{A}$ and $\mathcal{B}$ with $< k$ operator symbols. Suppose for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$.

($\sim$) Suppose $\mathcal{P}$ is of the form $\sim\mathcal{A}$. Then $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{D_d}[\sim\mathcal{A}] = \mathsf{S}$; by SF($\sim$), iff $\mathsf{D_d}[\mathcal{A}] \neq \mathsf{S}$; by assumption, iff $\mathsf{H_h}[\mathcal{A}] \neq \mathsf{S}$; by SF($\sim$), iff $\mathsf{H_h}[\sim\mathcal{A}] = \mathsf{S}$; iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

($\to$) Homework.

($\forall$) Suppose $\mathcal{P}$ is of the form $\forall x \mathcal{A}$. Then $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{D_d}[\forall x \mathcal{A}] = \mathsf{S}$; by SF($\forall$), iff for any $\mathsf{m} \in \mathsf{U_D}$, $\mathsf{D_{d(x|m)}}[\mathcal{A}] = \mathsf{S}$. Similarly, $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{H_h}[\forall x \mathcal{A}] = \mathsf{S}$; by SF($\forall$), iff for any $\mathsf{n} \in \mathsf{U_H}$, $\mathsf{H_{h(x|n)}}[\mathcal{A}] = \mathsf{S}$. (i)

Suppose $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$ but $\mathsf{D_d}[\mathcal{P}] \neq \mathsf{S}$; then any $\mathsf{n} \in \mathsf{U_H}$ is such that $\mathsf{H_{h(\mathit{x}|n)}}[\mathcal{A}] = \mathsf{S}$, but there is some $\mathsf{m} \in \mathsf{U_D}$ such that $\mathsf{D_{d(\mathit{x}|m)}}[\mathcal{A}] \neq \mathsf{S}$. From the latter, insofar as $\mathsf{d}(x|\mathsf{m})$ and $\mathsf{h}(x|\iota(\mathsf{m}))$ have each member related by ι, the assumption applies and, $\mathsf{H_{h(\mathit{x}|\iota(m))}}[\mathcal{A}] \neq \mathsf{S}$; so there is an $\mathsf{n} \in \mathsf{U_H}$ such that $\mathsf{H_{h(\mathit{x}|n)}}[\mathcal{A}] \neq \mathsf{S}$; this is impossible; reject the assumption: if $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$, then $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$. (ii) Similarly, [by homework] if $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$, then $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$. Hint: given $\mathsf{h}(x|\mathsf{n})$, there must be an m such that $\iota(\mathsf{m}) = \mathsf{n}$; then $\mathsf{d}(x|\mathsf{m})$ and $\mathsf{h}(x|\mathsf{n})$ are related so that the assumption applies.

For d and h such that for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$ and $\mathcal{P}$ with k operator symbols, $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

Indct: For d and h such that for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$, and any $\mathcal{P}$, $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

As often occurs, the most difficult case is for the quantifier. The key is that the assumption applies to $\mathsf{D_d}[\mathcal{P}]$ and $\mathsf{H_h}[\mathcal{P}]$ for *any* assignments d and h related so that for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$. Supposing that d and h are so related, there is no reason to think that $\mathsf{d}(x|\mathsf{m})$ and h remain in that relation. The problem is solved with a corresponding modification to h: with $\mathsf{d}(x|\mathsf{m})$; we modify h so that the assignment to x simply is $\iota(\mathsf{m})$. Thus $\mathsf{d}(x|\mathsf{m})$ and $\mathsf{h}(x|\iota(\mathsf{m}))$ are related so that the assumption applies.

Now it is a simple matter to show that isomorphic models are elementarily equivalent.

T11.10. If $\mathsf{D} \cong \mathsf{H}$, then $\mathsf{D} \equiv \mathsf{H}$.

Suppose $\mathsf{D} \cong \mathsf{H}$. By TI, $\mathsf{D}[\mathcal{P}] \neq \mathsf{T}$ iff there is some assignment d such that $\mathsf{D_d}[\mathcal{P}] \neq \mathsf{S}$; since $\mathsf{D} \cong \mathsf{H}$, where d and h are related as in T11.9, iff $\mathsf{H_h}[\mathcal{P}] \neq \mathsf{S}$; by TI, iff $\mathsf{H}[\mathcal{P}] \neq \mathsf{T}$. So $\mathsf{D}[\mathcal{P}] = \mathsf{T}$ iff $\mathsf{H}[\mathcal{P}] = \mathsf{T}$; and $\mathsf{D} \equiv \mathsf{H}$.

Thus it is only the structures of interpretations up to isomorphism that matter for the truth values of formulas. And such structures are completely sufficient to determine truth values of formulas. It is another question whether truth values of formulas are sufficient to determine models, even up to isomorphism.

*E11.9. Complete the proof of T11.9. You should set up the complete induction, but may refer to the text, as the text refers to homework.

E11.10. (i) Explain what truth value the sentence $\forall x(Dx \rightarrow \exists y(Cy \wedge Pxy))$ has on interpretation I and then I' in example (I). Explain what truth values it has on I and then I' in example (J). (ii) Explain what truth value the sentence $S\emptyset + S\emptyset = SS\emptyset$ has on interpretations N and N' in example (K). Are these results as you expect? Explain.

11.4.2 When Equivalence implies Isomorphism

It turns out that when the universe of discourse is finite, elementary equivalence is sufficient to show isomorphism. Suppose $\mathsf{U_D}$ is finite and interpretations D and H are elementarily equivalent, so that every formula has the same truth value on the two interpretations. We find a sequence of formulas which contain sufficient information to show that D and H are isomorphic.

For some language $\mathscr{L}$, suppose $\mathsf{D} \equiv \mathsf{H}$ and $\mathsf{U_D} = \{\mathsf{m}_1, \mathsf{m}_2 \ldots \mathsf{m}_n\}$. For an enumeration $x_1, x_2 \ldots$ of the variables, consider some assignment d such that $\mathsf{d}[x_1] = \mathsf{m}_1$, $\mathsf{d}[x_2] = \mathsf{m}_2$, and ... and $\mathsf{d}[x_n] = \mathsf{m}_n$, and let $\mathscr{C}_0$ be the open formula,

$$[(x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge \ldots \wedge x_1 \neq x_n) \wedge (x_2 \neq x_3 \wedge \ldots \wedge x_2 \neq x_n) \wedge (x_{n-1} \neq x_n)] \wedge \\ \forall v(v = x_1 \vee v = x_2 \vee \ldots \vee v = x_n)$$

with appropriate parentheses. You should see this expression on analogy with quantity expressions from chapter 5 on translation. Its existential closure, that is, $\exists x_1 \exists x_2 \ldots x_n \mathscr{C}_0$ is true just when there are exactly n things.

Now consider an enumeration, $\mathscr{A}_1, \mathscr{A}_2 \ldots$ of those atomic formulas in $\mathscr{L}$ whose only variables are $x_1 \ldots x_n$. And set $\mathscr{C}_i = \mathscr{C}_{i-1} \wedge \mathscr{A}_i$ if $\mathsf{D_d}[\mathscr{A}_i] = \mathsf{S}$, and otherwise, $\mathscr{C}_i = \mathscr{C}_{i-1} \wedge \sim\!\mathscr{A}_i$. It is easy to see that for any i, $\mathsf{D_d}[\mathscr{C}_i] = \mathsf{S}$. The argument is by induction on i.

T11.11. For any i, $\mathsf{D_d}[\mathscr{C}_i] = \mathsf{S}$.

Basis: For any a and b such that $1 \leq a, b \leq n$ and $a \neq b$, since x_a and x_b are assigned distinct members of $\mathsf{U_D}$, $\mathsf{D_d}[x_a = x_b] \neq \mathsf{S}$; so by SF($\sim$), $\mathsf{D_d}[x_a \neq x_b] = \mathsf{S}$; so by repeated applications of SF($\wedge$), $\mathsf{D_d}[(x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge \ldots \wedge x_1 \neq x_n) \wedge (x_2 \neq x_3 \wedge \ldots \wedge x_2 \neq x_n) \wedge (x_{n-1} \neq x_n)] = \mathsf{S}$. And since each member of $\mathsf{U_D}$ is assigned to some variable in $x_1 \ldots x_n$, for any $\mathsf{m} \in \mathsf{U_D}$, there is some a, $1 \leq a \leq n$ such that $\mathsf{D}_{\mathsf{d}(v|\mathsf{m})}[v = x_a] = \mathsf{S}$. So by repeated applications of SF($\vee$), for any $\mathsf{m} \in \mathsf{U_D}$, $\mathsf{D}_{\mathsf{d}(v|\mathsf{m})}[v = x_1 \vee v = x_2 \vee \ldots v = x_n] = \mathsf{S}$; so by SF($\forall$), $\mathsf{D_d}[\forall v(v = x_1 \vee v = x_2 \vee \ldots v = x_n)] = \mathsf{S}$; so by SF($\wedge$), $\mathsf{D_d}[\mathscr{C}_0] = \mathsf{S}$.

Assp: For any i, $0 \leq i < k$, $\mathsf{D_d}[\mathcal{C}_i] = \mathsf{S}$.

Show: $\mathsf{D_d}[\mathcal{C}_k] = \mathsf{S}$.

$\mathcal{C}_k$ is of the form $\mathcal{C}_{k-1} \wedge \mathcal{A}_k$ or $\mathcal{C}_{k-1} \wedge \sim\mathcal{A}_k$. In the first case, by assumption, $\mathsf{D_d}[\mathcal{C}_{k-1}] = \mathsf{S}$, and by construction, $\mathsf{D_d}[\mathcal{A}_k] = \mathsf{S}$; so by SF($\wedge$), $\mathsf{D_d}[\mathcal{C}_{k-1} \wedge \mathcal{A}_k] = \mathsf{S}$; which is to say, $\mathsf{D_d}[\mathcal{C}_k] = \mathsf{S}$. In the second case, again $\mathsf{D_d}[\mathcal{C}_{k-1}] = \mathsf{S}$; and by construction, $\mathsf{D_d}[\mathcal{A}_k] \neq \mathsf{S}$; so by SF($\sim$), $\mathsf{D_d}[\sim\mathcal{A}_k] = \mathsf{S}$; so by SF($\wedge$), $\mathsf{D_d}[\mathcal{C}_{k-1} \wedge \sim\mathcal{A}_k] = \mathsf{S}$; which is to say, $\mathsf{D_d}[\mathcal{C}_k] = \mathsf{S}$.

Indct: For any i, $\mathsf{D_d}[\mathcal{C}_i] = \mathsf{S}$.

So these formulas, though increasingly long, are all satisfied on assignment d.

Now, for the specification of an isomorphism between the interpretations, we set out to show there is a corresponding assignment h on which all the same expressions are satisfied. First, for any $\mathcal{C}_i$, consider its existential closure, $\exists x_1 \ldots \exists x_n \mathcal{C}_i$. It is easy to see that for any $\mathcal{C}_i$, $\mathsf{H}[\exists x_1 \ldots \exists x_n \mathcal{C}_i] = \mathsf{T}$. Suppose otherwise; then since $\mathsf{D} \equiv \mathsf{H}$, $\mathsf{D}[\exists x_1 \ldots \exists x_n \mathcal{C}_i] \neq \mathsf{T}$; so by TI, there is some assignment d' such that $\mathsf{D_{d'}}[\exists x_1 \ldots \exists x_n \mathcal{C}_i] \neq \mathsf{S}$; so, since the closure of $\mathcal{C}_i$ has no free variables, by T8.4, $\mathsf{D_d}[\exists x_1 \ldots \exists x_n \mathcal{C}_i] \neq \mathsf{S}$; so by repeated application of SF($\exists$), $\mathsf{D_d}[\mathcal{C}_i] \neq \mathsf{S}$; but by T11.11, this is impossible; reject the assumption: $\mathsf{H}[\exists x_1 \ldots \exists x_n \mathcal{C}_i] = \mathsf{T}$. When the existential is not satisfied on d, as we remove the quantifiers, in each case, the resultant formula without a quantifier is unsatisfied on $\mathsf{d}(x|\mathsf{m})$ for any $\mathsf{m} \in \mathsf{U_D}$; so it is unsatisfied when $\mathsf{m} = \mathsf{d}[x]$ — so that the formula without the quantifier is unsatisfied on the original d. Observe that there are thus exactly n members of $\mathsf{U_H}$: $\mathsf{H}[\exists x_1 \ldots \exists x_n \mathcal{C}_0] = \mathsf{T}$; and, as we have already noted, this can be the case iff there are exactly n members of $\mathsf{U_H}$.

Now for some assignment h', let h range over assignments that differ from h' at most in assignment to $x_1 \ldots x_n$. Set $\Omega_i = \{\mathsf{h} \mid \mathsf{H_h}[\mathcal{C}_i] = \mathsf{S}\}$, and $\Omega = \bigcap_{i \geq 0} \Omega_i$. Observe: (i) No Ω_i is empty. Since $\mathsf{H}[\exists x_1 \ldots \exists x_n \mathcal{C}_i] = \mathsf{T}$, by TI, for any assignment h^*, $\mathsf{H_{h^*}}[\exists x_1 \ldots \exists x_n \mathcal{C}_i] = \mathsf{S}$; so $\mathsf{H_{h'}}[\exists x_1 \ldots \exists x_n \mathcal{C}_i] = \mathsf{S}$; so by repeated applications of SF($\exists$), there is some h such that $\mathsf{H_h}[\mathcal{C}_i] = \mathsf{S}$. When the quantifiers come off, the result is some assignment that differs at most in assignments to $x_1 \ldots x_n$ and so some assignment in Ω_i. (ii) For any $j \geq i$, $\Omega_j \subseteq \Omega_i$. Suppose otherwise; then there is some h such that $\mathsf{h} \in \Omega_j$ but $\mathsf{h} \notin \Omega_i$; so by construction, $\mathsf{H_h}[\mathcal{C}_j] = \mathsf{S}$ but $\mathsf{H_h}[\mathcal{C}_i] \neq \mathsf{S}$; if $j = i$ this is impossible; so suppose $j > i$; then $\mathcal{C}_j$ is of the sort, $\mathcal{C}_i \wedge \mathcal{B}_{i+1} \wedge \mathcal{B}_{i+2} \wedge \ldots \wedge \mathcal{B}_j$ where $\mathcal{B}_{i+1} \ldots \mathcal{B}_j$ are either atomics or negated atomics; so by repeated application of SF($\wedge$), $\mathsf{H_h}[\mathcal{C}_i] = \mathsf{S}$; this is impossible; reject the assumption: $\Omega_j \subseteq \Omega_i$. (iii) Finally, there are at most finitely many assignments of the sort h. Since any h differs from h′ at most in assignments to $x_1 \dots x_n$, and there are just n members of U_H, there are n^n assignments of the sort h.

From these results it follows that Ω is non-empty. Suppose otherwise. Then for any h, there is some Ω_i such that h $\notin \Omega_i$. But there are only finitely many assignments of the sort h. So we may consider finitely many $\Omega_a \dots \Omega_b$ from which for any h there is some Ω_i such that h $\notin \Omega_i$. But where each subscript in $a \dots b$ is $\leq b$, for each Ω_i, $\Omega_b \subseteq \Omega_i$; and since each h is missing from at least one Ω_i, we have that Ω_b is therefore empty. Ω_b must lack each of the assignments missing from prior members of the sequence. But this is impossible; reject the assumption: Ω is not empty. So we have what we wanted: any h in Ω is an assignment that satisfies every $\mathcal{C}_i$.

Now we are ready to specify a mapping for our isomorphism! Indeed, we are ready to show,

T11.12. If D $\equiv$ H and U_D is finite, then D $\cong$ H.

Suppose D $\equiv$ H and U_D is finite. Then there are Ω and formulas $\mathcal{C}_i$ as above. For some particular h $\in \Omega$, for any i, $1 \leq i \leq n$, let $\iota(\mathsf{d}[x_i]) = \mathsf{h}[x_i]$. Since h $\in \Omega$, for any $\mathcal{C}_i$, $\mathsf{H_h}[\mathcal{C}_i] = \mathsf{S}$. So $\mathsf{H_h}[\mathcal{C}_0] = \mathsf{S}$. So h assigns each x_i to a different member of U_H, and ι is onto U_H, as it should be. We now set out to show that the other conditions for isomorphism are met.

Sentence letters. Since D $\equiv$ H, for any sentence letter $\mathcal{S}$, $\mathsf{D}[\mathcal{S}] = \mathsf{T}$; iff $\mathsf{H}[\mathcal{S}] = \mathsf{T}$; so $\mathsf{D}[\mathcal{S}] = \mathsf{H}[\mathcal{S}]$.

Constants. We require that for any constant c, $\mathsf{D}[c] = \mathsf{m}_i$ iff $\mathsf{H}[c] = \iota(\mathsf{m}_i)$. (i) For some constant c, suppose $\mathsf{D}[c] = \mathsf{m}_i$. Since $\mathsf{d}[x_i] = \mathsf{m}_i$, $\iota(\mathsf{m}_i) = \iota(\mathsf{d}[x_i]) = \mathsf{h}[x_i]$. By TA(c), $\mathsf{D_d}[c] = \mathsf{D}[c] = \mathsf{m}_i$; and by TA(v), $\mathsf{D_d}[x_i] = \mathsf{d}[x_i] = \mathsf{m}_i$; so $\mathsf{D_d}[c] = \mathsf{D_d}[x_i]$; so $\langle \mathsf{D_d}[c], \mathsf{D_d}[x_i] \rangle \in \mathsf{D}[=]$; so by SF(r), $\mathsf{D_d}[c = x_i] = \mathsf{S}$; so $c = x_i$ is a conjunct in some $\mathcal{C}_n$; but $\mathsf{H_h}[\mathcal{C}_n] = \mathsf{S}$; so by repeated applications of SF($\wedge$), $\mathsf{H_h}[c = x_i] = \mathsf{S}$; so by SF(r), $\langle \mathsf{H_h}[c], \mathsf{H_h}[x_i] \rangle \in \mathsf{H}[=]$; so $\mathsf{H_h}[c] = \mathsf{H_h}[x_i]$; but by TA(c), $\mathsf{H_h}[c] = \mathsf{H}[c]$, and by TA(v), $\mathsf{H_h}[x_i] = \mathsf{h}[x_i]$; so $\mathsf{H}[c] = \mathsf{h}[x_i]$; so $\mathsf{H}[c] = \iota(\mathsf{m}_i)$.

(ii) Suppose $\mathsf{D}[c] \neq \mathsf{m}_i$. As before, $\iota(\mathsf{m}_i) = \mathsf{h}[x_i]$; and $\mathsf{D_d}[x_i] = \mathsf{m}_i$. But by TA(c), $\mathsf{D_d}[c] = \mathsf{D}[c]$; so $\mathsf{D_d}[c] \neq \mathsf{m}_i$; so $\mathsf{D_d}[c] \neq \mathsf{D_d}[x_i]$; so $\langle \mathsf{D_d}[c], \mathsf{D_d}[x_i] \rangle \notin \mathsf{D}[=]$; so by SF(r), $\mathsf{D_d}[c = x_i] \neq \mathsf{S}$; so $c \neq x_i$ is a conjunct in some $\mathcal{C}_n$; but $\mathsf{H_h}[\mathcal{C}_n] = \mathsf{S}$; so by repeated applications of SF($\wedge$), $\mathsf{H_h}[c \neq x_i] = \mathsf{S}$; so by SF($\sim$), and SF(r), $\langle \mathsf{H_h}[c], \mathsf{H_h}[x_i] \rangle \notin \mathsf{H}[=]$; so $\mathsf{H_h}[c] \neq \mathsf{H_h}[x_i]$; but by TA(c), $\mathsf{H_h}[c] = \mathsf{H}[c]$, and by TA(v), $\mathsf{H_h}[x_i] = \mathsf{h}[x_i]$; so $\mathsf{H}[c] \neq \mathsf{h}[x_i]$; so $\mathsf{H}[c] \neq \iota(\mathsf{m}_i)$.

Relation Symbols. We require that for any relation symbol $\mathcal{R}^n$, $\langle \mathsf{m}_a \ldots \mathsf{m}_b \rangle \in \mathsf{D}[\mathcal{R}^n]$ iff $\langle \iota(\mathsf{m}_a) \ldots \iota(\mathsf{m}_b) \rangle \in \mathsf{H}(\mathcal{R}^n)$. (i) Suppose $\langle \mathsf{m}_a \ldots \mathsf{m}_b \rangle \in \mathsf{D}[\mathcal{R}^n]$. Since $\mathsf{d}[x_a] = \mathsf{m}_a$, and …and $\mathsf{d}[x_b] = \mathsf{m}_b$ we have, $\iota(\mathsf{m}_a) = \iota(\mathsf{d}[x_a]) = \mathsf{h}[x_a]$, and …and $\iota(\mathsf{m}_b) = \iota(\mathsf{d}[x_b]) = \mathsf{h}[x_b]$, and also by TA(v), $\mathsf{D_d}[x_a] = \mathsf{m}_a$, and …and $\mathsf{D_d}[x_b] = \mathsf{m}_b$; so $\langle \mathsf{D_d}[x_a], \ldots \mathsf{D_d}[x_b] \rangle \in \mathsf{D}[\mathcal{R}^n]$; so by SF(r), $\mathsf{D_d}[\mathcal{R}^n x_a \ldots x_b] = \mathsf{S}$; so $\mathcal{R}^n x_a \ldots x_b$ is a conjunct of some $\mathcal{C}_n$; but $\mathsf{H_h}[\mathcal{C}_n] = \mathsf{S}$; so by repeated applications of SF($\wedge$), $\mathsf{H_h}[\mathcal{R}^n x_a \ldots x_b] = \mathsf{S}$; so by SF(r), $\langle \mathsf{H_h}[x_a], \ldots \mathsf{H_h}[x_b] \rangle \in \mathsf{H}[\mathcal{R}^n]$; but by TA(v), $\mathsf{H_h}[x_a] = \mathsf{h}[x_a] = \iota(\mathsf{m}_a)$, and …and $\mathsf{H_h}[x_b] = \mathsf{h}[x_b] = \iota(\mathsf{m}_b)$; so $\langle \iota(\mathsf{m}_a) \ldots \iota(\mathsf{m}_b) \rangle \in \mathsf{H}[\mathcal{R}^n]$.

(ii) Suppose $\langle \mathsf{m}_a \ldots \mathsf{m}_b \rangle \not\in \mathsf{D}[\mathcal{R}^n]$. As before, $\iota(\mathsf{m}_a) = \mathsf{h}[x_a]$, and …and $\iota(\mathsf{m}_b) = \mathsf{h}[x_b]$; similarly, $\mathsf{D_d}[x_a] = \mathsf{m}_a$, and …and $\mathsf{D_d}[x_b] = \mathsf{m}_b$; so $\langle \mathsf{D_d}[x_a], \ldots \mathsf{D_d}[x_b] \rangle \not\in \mathsf{D}[\mathcal{R}^n]$; so by SF(r), $\mathsf{D_d}[\mathcal{R}^n x_a \ldots x_b] \neq \mathsf{S}$; and $\sim\mathcal{R}^n x_a \ldots x_b$ is a conjunct of some $\mathcal{C}_n$; but $\mathsf{H_h}[\mathcal{C}_n] = \mathsf{S}$; so by repeated applications of SF($\wedge$), $\mathsf{H_h}[\sim\mathcal{R}^n x_a \ldots x_b] = \mathsf{S}$; so by SF($\sim$) and SF(r), $\langle \mathsf{H_h}[x_a], \ldots \mathsf{H_h}[x_b] \rangle \not\in \mathsf{H}[\mathcal{R}^n]$; but as before, $\mathsf{H_h}[x_a] = \iota(\mathsf{m}_a)$, and …and $\mathsf{H_h}[x_b] = \iota(\mathsf{m}_b)$; so $\langle \iota(\mathsf{m}_a) \ldots \iota(\mathsf{m}_b) \rangle \not\in \mathsf{H}[\mathcal{R}^n]$.

Function symbols. We require that for any function symbol h^n, $\langle \langle \mathsf{m}_a \ldots \mathsf{m}_b \rangle, \mathsf{m}_c \rangle \in \mathsf{D}[h^n]$ iff $\langle \langle \iota(\mathsf{m}_a) \ldots \iota(\mathsf{m}_b) \rangle, \iota(\mathsf{m}_c) \rangle \in \mathsf{H}[h^n]$. (i) Suppose $\langle \langle \mathsf{m}_a \ldots \mathsf{m}_b \rangle, \mathsf{m}_c \rangle \in \mathsf{D}[h^n]$. Since $\mathsf{d}[x_a] = \mathsf{m}_a$, and …and $\mathsf{d}[x_b] = \mathsf{m}_b$, and $\mathsf{d}[x_c] = \mathsf{m}_c$, we have, $\iota(\mathsf{m}_a) = \iota(\mathsf{d}[x_a]) = \mathsf{h}[x_a]$, and …and $\iota(\mathsf{m}_b) = \iota(\mathsf{d}[x_b]) = \mathsf{h}[x_b]$, and $\iota(\mathsf{m}_c) = \iota(\mathsf{d}[x_c]) = \mathsf{h}[x_c]$; and also by TA(v), $\mathsf{D_d}[x_a] = \mathsf{m}_a$, and …and $\mathsf{D_d}[x_b] = \mathsf{m}_b$, and $\mathsf{D_d}[x_c] = \mathsf{m}_c$; so $\langle \langle \mathsf{D_d}[x_a] \ldots \mathsf{D_d}[x_b] \rangle, \mathsf{D_d}[x_c] \rangle \in \mathsf{D}[h^n]$; so $\mathsf{D}[h^n]\langle \mathsf{D_d}[x_a] \ldots \mathsf{D_d}[x_b] \rangle = \mathsf{D_d}[x_c]$; so by TA(f), $\mathsf{D_d}[h^n x_a \ldots x_b] = \mathsf{D_d}[x_c]$; so $\langle \mathsf{D_d}[h^n x_a \ldots x_b], \mathsf{D_d}[x_c] \rangle \in \mathsf{D}[=]$; so by SF(r), $\mathsf{D_d}[h^n x_a \ldots x_b = x_c] = \mathsf{S}$; so $h^n x_a \ldots x_b = x_c$ is a conjunct of some $\mathcal{C}_n$; but $\mathsf{H_h}[\mathcal{C}_n] = \mathsf{S}$; so by repeated applications of SF($\wedge$), $\mathsf{H_h}[h^n x_a \ldots x_b = x_c] = \mathsf{S}$; so by SF(r), $\langle \mathsf{H_h}[h^n x_a \ldots x_b], \mathsf{H_h}[x_c] \rangle \in \mathsf{H}[=]$; so $\mathsf{H_h}[h^n x_a \ldots x_b] = \mathsf{H_h}[x_c]$; but by TA(f), $\mathsf{H_h}[h^n x_a \ldots x_b] = \mathsf{H}[h^n]\langle \mathsf{H_h}[x_a] \ldots \mathsf{H_h}[x_b] \rangle$; so $\mathsf{H}[h^n]\langle \mathsf{H_h}[x_a] \ldots \mathsf{H_h}[x_b] \rangle = \mathsf{H_h}[x_c]$; so $\langle \langle \mathsf{H_h}[x_a] \ldots \mathsf{H_h}[x_b] \rangle, \mathsf{H_h}[x_c] \rangle \in \mathsf{H}[h^n]$; but by TA(v), $\mathsf{H_h}[x_a] = \mathsf{h}[x_a] = \iota(\mathsf{m}_a)$, and …$\mathsf{H_h}[x_b] = \mathsf{h}[x_b] = \iota(\mathsf{m}_b)$, and $\mathsf{H_h}[x_c] = \mathsf{h}[x_c] = \iota(\mathsf{m}_c)$; so $\langle \langle \iota(\mathsf{m}_a) \ldots \iota(\mathsf{m}_b) \rangle, \iota(\mathsf{m}_c) \rangle \in \mathsf{H}[h^n]$.

(ii) Suppose $\langle \langle \mathsf{m}_a \ldots \mathsf{m}_b \rangle, \mathsf{m}_c \rangle \not\in \mathsf{D}[h^n]$. As before, $\iota(\mathsf{m}_a) = \mathsf{h}[x_a]$, and …and $\iota(\mathsf{m}_b) = \mathsf{h}[x_b]$, and $\iota(\mathsf{m}_c) = \mathsf{h}[x_c]$; and also $\mathsf{D_d}[x_a] = \mathsf{m}_a$, and …and $\mathsf{D_d}[x_b] = \mathsf{m}_b$, and $\mathsf{D_d}[x_c] = \mathsf{m}_c$; so $\langle \langle \mathsf{D_d}[x_a] \ldots \mathsf{D_d}[x_b] \rangle, \mathsf{D_d}[x_c] \rangle \not\in \mathsf{D}[h^n]$; so $\mathsf{D}[h^n]\langle \mathsf{D_d}[x_a] \ldots \mathsf{D_d}[x_b] \rangle \neq \mathsf{D_d}[x_c]$; so by TA(f), $\mathsf{D_d}[h^n x_a \ldots x_b] \neq \mathsf{D_d}[x_c]$; so $\langle \mathsf{D_d}[h^n x_a \ldots x_b], \mathsf{D_d}[x_c] \rangle \not\in \mathsf{D}[=]$; so by SF(r), $\mathsf{D_d}[h^n x_a \ldots x_b = x_c] \neq \mathsf{S}$; so $h^n x_a \ldots x_b \neq x_c$ is a conjunct of some $\mathcal{C}_n$; but $\mathsf{H_h}[\mathcal{C}_n] = \mathsf{S}$;

so by repeated applications of SF($\wedge$), $\mathsf{H_h}[\hbar^n x_a \ldots x_b \neq x_c] = \mathsf{S}$; so by SF($\sim$) and SF(r), $\langle \mathsf{H_h}[\hbar^n x_a \ldots x_b], \mathsf{H_h}[x_c]\rangle \notin \mathsf{H}[=]$; so $\mathsf{H_h}[\hbar^n x_a \ldots x_b] \neq \mathsf{H_h}[x_c]$; but by TA(f), $\mathsf{H_h}[\hbar^n x_a \ldots x_b] = \mathsf{H}[\hbar^n]\langle \mathsf{H_h}[x_a] \ldots \mathsf{H_h}[x_b]\rangle$; and $\mathsf{H}[\hbar^n]\langle \mathsf{H_h}[x_a] \ldots \mathsf{H_h}[x_b]\rangle \neq \mathsf{H_h}[x_c]$; so $\langle\langle \mathsf{H_h}[x_a] \ldots \mathsf{H_h}[x_b]\rangle, \mathsf{H_h}[x_c]\rangle \notin \mathsf{H}[\hbar^n]$; but as before, $\mathsf{H_h}[x_a] = \iota(\mathsf{m}_a)$, and $\ldots \mathsf{H_h}[x_b] = \iota(\mathsf{m}_b)$, and $\mathsf{H_h}[x_c] = \iota(\mathsf{m}_c)$; so $\langle\langle \iota(\mathsf{m}_a) \ldots \iota(\mathsf{m}_b)\rangle, \iota(\mathsf{m}_c)\rangle \notin \mathsf{H}[\hbar^n]$.

Thus elementary equivalence is sufficient for isomorphism in the case where the universe of discourse is finite. This is an interesting result! Consider any interpretation D with a finite $\mathsf{U_D}$, and the set of formulas Δ (Delta) true on D. By our result, any other model H that makes all the formulas in Δ true — any H such that $\mathsf{D} \equiv \mathsf{H}$ — is such that D is isomorphic to H. As we shall shortly see, the situation is not so straightforward when $\mathsf{U_D}$ is infinite.

11.5 Compactness and Isomorphism

Compactness takes the link between syntax and semantics from adequacy, and combines it with the finite length of derivations. The result is simple enough, and puts us in a position to obtain a range of further conclusions.

ST A set Σ of formulas is *satisfiable* iff it has a model. Σ is *finitely satisfiable* iff every finite subset of it has a model.

Now compactness draws a connection between satisfiability, and finite satisfiability,

T11.13. A set of formulas Σ is satisfiable iff it is finitely satisfiable. (*compactness*)

(i) Suppose Σ is satisfiable, but not finitely satisfiable. Then there is some M such that $\mathsf{M}[\Sigma] = \mathsf{T}$; but there is a finite $\Sigma' \subseteq \Sigma$ such that any M′ has $\mathsf{M}'[\Sigma'] \neq \mathsf{T}$; so $\mathsf{M}[\Sigma'] \neq \mathsf{T}$; so there is a formula $\mathcal{P} \in \Sigma'$ such that $\mathsf{M}[\mathcal{P}] \neq \mathsf{T}$; but since $\Sigma' \subseteq \Sigma$, $\mathcal{P} \in \Sigma$; so $\mathsf{M}[\Sigma] \neq \mathsf{T}$. This is impossible; reject the assumption: if Σ is satisfiable, then it is finitely satisfiable.

(ii) Suppose Σ is finitely satisfiable, but not satisfiable. By T10.17, if Σ is consistent, then it has a model M. But since Σ is not satisfiable, it has no model; so it is not consistent; so there is some formula $\mathcal{A}$ such that $\Sigma \vdash \mathcal{A}$ and $\Sigma \vdash \sim\mathcal{A}$; consider derivations of these results, and the set Σ^* of premises of these derivations; since derivations are finite, Σ^* is finite; and since Σ^* includes all the premises, $\Sigma^* \vdash \mathcal{A}$ and $\Sigma^* \vdash \sim\mathcal{A}$; so by soundness, $\Sigma^* \vDash \mathcal{A}$ and $\Sigma^* \vDash \sim\mathcal{A}$; since Σ is finitely satisfiable, there must be some model M^*

such that $\mathsf{M}^*[\Sigma^*] = \mathsf{T}$; then by QV, $\mathsf{M}^*[\mathcal{A}] = \mathsf{T}$ and $\mathsf{M}^*[\sim\mathcal{A}] = \mathsf{T}$. But by T7.5, there is no M^* and $\mathcal{A}$ such that $\mathsf{M}^*[\mathcal{A}] = \mathsf{T}$ and $\mathsf{M}^*[\sim\mathcal{A}] = \mathsf{T}$. This is impossible; reject the assumption: if Σ is finitely satisfiable, then it is satisfiable.

This theorem puts us in a position to reason from finite satisfiability to satisfiability. And the results of such reasoning may be startling. Consider again the standard interpretation N1 for $\mathcal{L}_{NT}^{<}$,

$\mathsf{N}[\emptyset] = 0$

$\mathsf{N}[<] = \{\langle \mathsf{m}, \mathsf{n}\rangle \mid \mathsf{m}, \mathsf{n} \in \mathbb{N}$, and m is less than $\mathsf{n}\}$

$\mathsf{N}[S] = \{\langle \mathsf{m}, \mathsf{n}\rangle \mid \mathsf{m}, \mathsf{n} \in \mathbb{N}$, and n is the successor of $\mathsf{m}\}$

$\mathsf{N}[+] = \{\langle\langle \mathsf{m}, \mathsf{n}\rangle, \mathsf{o}\rangle \mid \mathsf{m}, \mathsf{n}, \mathsf{o} \in \mathbb{N}$, and m plus n equals $\mathsf{o}\}$

$\mathsf{N}[\times] = \{\langle\langle \mathsf{m}, \mathsf{n}\rangle, \mathsf{o}\rangle \mid \mathsf{m}, \mathsf{n}, \mathsf{o} \in \mathbb{N}$, and m times n equals $\mathsf{o}\}$

Let Σ include all the sentences true on N. Now consider a language $\mathcal{L}'$ like $\mathcal{L}_{NT}^{<}$ but with the addition of a single constant c. And consider a set of sentences,

$$\Sigma' = \Sigma \cup \{\emptyset < c, S\emptyset < c, SS\emptyset < c, SSS\emptyset < c, SSSS\emptyset < c \ldots\}$$

that is like Σ but with the addition of sentences asserting that c is greater than each integer. Clearly there is no such individual on the standard interpretation N. A finite subset of Σ' can have at most finitely many of these sentences as members. Thus a finite subset of Σ' is a subset of,,

$$\Sigma \cup \{\emptyset < c, S\emptyset < c, SS\emptyset < c \ldots \overbrace{SS\ldots S}^{nS\text{'s}}\emptyset < c\}$$

for some n. But any such set is finitely satisfiable: Simply let the interpretation N' be like N but with $\mathsf{N}[c] = n + 1$. It follows from T11.13 that Σ' has a model M'. But, further, by reasoning as for T10.16, a model M like M' but without the assignment to c is a model of $\mathcal{L}_{NT}^{<}$ for all the sentences in Σ. So $\mathsf{N} \equiv \mathsf{M}$. But $\mathsf{N} \not\cong \mathsf{M}$. For there must be a member of U_M with infinitely many members of U_M that stand in the $<$ relation to it. [Clean this up.]

It is worth observing that we have demonstrated the existence of a model for the completely nonstandard M by appeal to the more standard models M' for finite subsets of Σ', through the compactness theorem. Also, it is now clear that there can be no analog to the result of the previous section for models with an infinite domain: For models with an infinite domain, elementary equivalence does not in general imply isomorphism. In the next section, we begin to see just how general this phenomenon is.

11.6 Submodels and Löwenheim-Skolem

The construction for the adequacy theorem gives us a countable model for any consistent set of sentences. Already, this suggests that sentences for some models do not always have the same size domain. Suppose Σ has a model I. Then by T10.4, Σ is consistent; so by T10.17, Σ has a model M — where the universe of this latter model is constructed of disjoint sets of integers. But this means that if Σ has a model at all, then it has a countable model, for we might order the members of $\mathsf{U_M}$ by, say, their least elements into a countable series. In fact, we might set up a function ι from each set in $\mathsf{U_M}$ to its least element, to establish an isomorphic interpretation M^* whose universe just *is* a set of integers. Then by T11.10, $\mathsf{M}^*[\Sigma] = \mathsf{T}$. So consider any model whose universe is not countable; it must be elementarily equivalent to one whose universe is a countable set of integers. But, of course, there is no one-to-one map from an uncountable universe to a countable one, so the models are not isomorphic.

This sort of result is strengthened in an interesting way by the Löwenheim-Skolem theorems. In the first form, we show that every model has a *submodel* with a countable domain.

11.6.1 Submodels

SM A model M of a language $\mathscr{L}$ is a *submodel* of model N ($\mathsf{M} \subseteq \mathsf{N}$) iff

1. $\mathsf{U_M} \subseteq \mathsf{U_N}$,
2. For any sentence letter $\mathscr{S}$, $\mathsf{M}[\mathscr{S}] = \mathsf{N}[\mathscr{S}]$,
3. For any constant c of $\mathscr{L}$, $\mathsf{M}(c) = \mathsf{N}(c)$,
4. For any function symbol h^n of $\mathscr{L}$ and any $\langle \mathsf{a}_1 \dots \mathsf{a}_n \rangle$ from the members of $\mathsf{U_M}$, $\langle\langle \mathsf{a}_1 \dots \mathsf{a}_n \rangle, \mathsf{b}\rangle \in \mathsf{M}(h^n)$ iff $\langle\langle \mathsf{a}_1 \dots \mathsf{a}_n \rangle, \mathsf{b}\rangle \in \mathsf{N}(h^n)$,
5. For any relation symbol $\mathscr{R}^n$ of $\mathscr{L}$ and any $\langle \mathsf{a}_1 \dots \mathsf{a}_n \rangle$ from the members of $\mathsf{U_M}$, $\langle \mathsf{a}_1 \dots \mathsf{a}_n \rangle \in \mathsf{M}(\mathscr{R}^n)$ iff $\langle \mathsf{a}_1 \dots \mathsf{a}_n \rangle \in \mathsf{N}(\mathscr{R}^n)$.

The interpretation of h^n and of $\mathscr{R}^n$ on M are the *restrictions* of their respective interpretations on N. Observe that a submodel is completely determined, once its domain is given. A submodel is not well defined if it does not include objects for the interpretation of the constants, and the closure of its functions.

ES Say d is a variable assignment into the members of $\mathsf{U_M}$. Then M is an *elementary submodel* of N iff $\mathsf{M} \subseteq \mathsf{N}$ and for any formula $\mathscr{P}$ of $\mathscr{L}$ and any such d, $\mathsf{M_d}[\mathscr{P}] = \mathsf{S}$ iff $\mathsf{N_d}[\mathscr{P}] = \mathsf{S}$.

If M is an elementary submodel of N, we write, $\mathsf{M} \prec \mathsf{N}$. First,

T11.14. If $\mathsf{M} \prec \mathsf{N}$ then for any sentence $\mathcal{P}$ of $\mathcal{L}$, $\mathsf{M}[\mathcal{P}] = \mathsf{T}$ iff $\mathsf{N}[\mathcal{P}] = \mathsf{T}$.

Suppose $\mathsf{M} \prec \mathsf{N}$ and consider some sentence $\mathcal{P}$. By TI, $\mathsf{M}[\mathcal{P}] = \mathsf{T}$ iff $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ for every assignment d into $\mathsf{U_M}$; since $\mathcal{P}$ is a sentence, by T8.4, iff for some particular assignment h, $\mathsf{M_h}[\mathcal{P}] = \mathsf{S}$; since $\mathsf{M} \prec \mathsf{N}$, iff $\mathsf{N_h}[\mathcal{P}] = \mathsf{S}$; since $\mathcal{P}$ is a sentence, by T8.4, iff $\mathsf{N_d}[\mathcal{P}] = \mathsf{S}$ for every d into $\mathsf{U_N}$; by TI, iff $\mathsf{N}[\mathcal{P}] = \mathsf{T}$. So $\mathsf{M}[\mathcal{P}] = \mathsf{T}$ iff $\mathsf{N}[\mathcal{P}] = \mathsf{T}$.

This much is clear. It is not so easy demonstrate the conditions under which a submodel is an elementary submodel. We make a beginning with the following theorems.

T11.15. Suppose $\mathsf{M} \subseteq \mathsf{N}$ and d is a variable assignment into $\mathsf{U_M}$. Then for any term t, $\mathsf{M_d}[t] = \mathsf{N_d}[t]$.

By induction on the number of function symbols in t. Suppose $\mathsf{M} \subseteq \mathsf{N}$ and d is a variable assignment into $\mathsf{U_M}$.

Basis: Suppose t has no function symbols. Then t is a variable x or a constant c. (i) Suppose t is a constant c. Then $\mathsf{M_d}[t]$ is $\mathsf{M_d}[c]$; by TA(c) this is $\mathsf{M}[c]$; and since $\mathsf{M} \subseteq \mathsf{N}$, this is $\mathsf{N}[c]$; by TA(c) again, this is $\mathsf{N_d}[c]$; which is just $\mathsf{N_d}[t]$. (ii) Suppose t is a variable x. Then $\mathsf{M_d}[t]$ is $\mathsf{M_d}[x]$; by TA(v), this is $\mathsf{d}[x]$ and by TA(v) again, this is $\mathsf{N_d}[x]$; which is just $\mathsf{N_d}[t]$.

Assp: For any i, $0 \leq i < k$, if t has i function symbols, then $\mathsf{M_d}[t] = \mathsf{N_d}[t]$.

Show: If t has k function symbols, $\mathsf{M_d}[t] = \mathsf{N_d}[t]$.

If t has k function symbols, then it is of the form $h^n t_1 \dots t_n$ for some terms $t_1 \dots t_n$ with $< k$ function symbols. So $\mathsf{M_d}[t]$ is $\mathsf{M_d}[h^n t_1 \dots t_n]$; by TA(f) this is $\mathsf{M}[h^n]\langle \mathsf{M_d}[t_1], \dots \mathsf{M_d}[t_n]\rangle$; since $\mathsf{M} \subseteq \mathsf{N}$, with the assumption, this is $\mathsf{N}[h^n]\langle \mathsf{N_d}[t_1], \dots \mathsf{N_d}[t_n]\rangle$; by TA(f), this is $\mathsf{N_d}[h^n t_1 \dots t_n]$; which is just $\mathsf{N_d}[t]$.

Indct: For any term t, $\mathsf{M_d}[t] = \mathsf{N_d}[t]$.

T11.16. Suppose that $\mathsf{M} \subseteq \mathsf{N}$ and that for any formula $\mathcal{P}$ and every variable assignment d such that $\mathsf{N_d}[\exists x \mathcal{P}] = \mathsf{S}$ there is an $\mathsf{m} \in \mathsf{U_M}$ such that $\mathsf{N_{d(x|m)}}[\mathcal{P}] = \mathsf{S}$. Then $\mathsf{M} \prec \mathsf{N}$.

Suppose $\mathsf{M} \subseteq \mathsf{N}$ and that for any formula $\mathcal{P}$ and every variable assignment d such that $\mathsf{N_d}[\exists x \mathcal{P}] = \mathsf{S}$ there is an $\mathsf{m} \in \mathsf{U_M}$ such that $\mathsf{N_{d(x|m)}}[\mathcal{P}] = \mathsf{S}$. We show by induction on the number of operators in $\mathcal{P}$, that for d any assignment into the members of $\mathsf{U_M}$, $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{N_d}[\mathcal{P}] = \mathsf{S}$.

Basis: If $\mathcal{P}$ is atomic then it is either a sentence letter $\mathcal{S}$ or an atomic of the form $\mathcal{R}^n t_1 \dots t_n$ for some relation symbol $\mathcal{R}^n$ and terms $t_1 \dots t_n$. (i) Suppose $\mathcal{P}$ is $\mathcal{S}$. Then $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M_d}[\mathcal{S}] = \mathsf{S}$; by SF(s), iff $\mathsf{M}[\mathcal{S}] = \mathsf{T}$; since $\mathsf{M} \subseteq \mathsf{N}$, iff $\mathsf{N}[\mathcal{S}] = \mathsf{T}$; by SF(s), iff $\mathsf{N_d}[\mathcal{S}] = \mathsf{S}$; iff $\mathsf{N_d}[\mathcal{P}] = \mathsf{S}$. (ii) Suppose $\mathcal{P}$ is $\mathcal{R}^n t_1 \dots t_n$. Then $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M_d}[\mathcal{R}^n t_1 \dots t_n] = \mathsf{S}$; by SF(r) iff $\langle \mathsf{M_d}[t_1], \dots \mathsf{M_d}[t_n] \rangle \in \mathsf{M}[\mathcal{R}^n]$; since $\mathsf{M} \subseteq \mathsf{N}$ with T11.15 iff $\langle \mathsf{N_d}[t_1], \dots \mathsf{N_d}[t_n] \rangle \in \mathsf{N}[\mathcal{R}^n]$; by SF(r) iff $\mathsf{N_d}[\mathcal{R}^n t_1 \dots t_n] = \mathsf{S}$; iff $\mathsf{N_d}[\mathcal{P}] = \mathsf{S}$.

Assp: For any i, $0 \le i < k$, for d any assignment into the members of $\mathsf{U_M}$, if $\mathcal{P}$ has i operator symbols, then $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{N_d}[\mathcal{P}] = \mathsf{S}$.

Show: If $\mathcal{P}$ has k operator symbols, then for d any assignment into the members of $\mathsf{U_M}$, $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{N_d}[\mathcal{P}] = \mathsf{S}$.

If $\mathcal{P}$ has k operator symbols, then it is of the form $\sim\mathcal{A}$, $\mathcal{A} \to \mathcal{B}$ or $\exists x \mathcal{A}$ for variable x and formulas A and $\mathcal{B}$ with $< k$ operator symbols (treating universally quantified expressions as equivalent to existentially quantified ones). Let d be an assignment into the members of $\mathsf{U_M}$.

($\sim$) Suppose $\mathcal{P}$ is $\sim A$. $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M_d}[\sim\mathcal{A}] = \mathsf{S}$; by SF($\sim$) iff $\mathsf{M_d}[\mathcal{A}] \neq \mathsf{S}$; by assumption iff $\mathsf{N_d}[\mathcal{A}] \neq \mathsf{S}$; by SF($\sim$) iff $\mathsf{N_d}[\sim\mathcal{A}] = \mathsf{S}$; iff $\mathsf{N_d}[\mathcal{P}] = \mathsf{S}$.

($\to$) Homework.

($\exists$) Suppose $\mathcal{P}$ is $\exists x \mathcal{A}$. (i) Suppose $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$; then $\mathsf{M_d}[\exists x \mathcal{A}] = \mathsf{S}$; so by SF($\exists$), there is some $\mathsf{o} \in \mathsf{U_M}$ such that $\mathsf{M_{d(x|o)}}[\mathcal{A}] = \mathsf{S}$; so since $\mathsf{d}(x|\mathsf{o})$ is an assignment into the members of $\mathsf{U_M}$, by assumption, $\mathsf{N_{d(x|o)}}[\mathcal{A}] = \mathsf{S}$; so by SF($\exists$), $\mathsf{N_d}[\exists x \mathcal{A}] = \mathsf{S}$; so $\mathsf{N_d}[\mathcal{P}] = \mathsf{S}$. (ii) Suppose $\mathsf{N_d}[\mathcal{P}] = \mathsf{S}$; then $\mathsf{N_d}[\exists x \mathcal{A}] = \mathsf{S}$; so by the assumption of the theorem, there is an $\mathsf{m} \in \mathsf{U_M}$ such that $\mathsf{N_{d(x|m)}}[\mathcal{A}] = \mathsf{S}$; since $\mathsf{d}(x|\mathsf{m})$ is an assignment into the members of $\mathsf{U_M}$, by assumption $\mathsf{M_{d(x|m)}}[\mathcal{A}] = \mathsf{S}$; so by SF($\exists$), $\mathsf{M_d}[\exists x \mathcal{A}] = \mathsf{S}$; so $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$. So $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{N_d}[\mathcal{P}] = \mathsf{S}$.

In any case, if $\mathcal{P}$ has k operator symbols, $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{N_d}[\mathcal{P}] = \mathsf{S}$.

Indct: For any $\mathcal{P}$, $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{N_d}[\mathcal{P}] = \mathsf{S}$.

So the result works, only so long as the quantifier case is guaranteed by "witnesses" for each existential claim in the universe of the submodel. The Löwenheim Skolem Theorem takes advantage of what we have done by producing a model in which these witnesses are present.

11.6.2 Downward Löwenheim-Skolem

The Löwenheim Skolem Theorem takes advantage of what we have just done by producing a model in which the required witnesses are present.

$\mathsf{U_M}$ Consider some model N and suppose a well-ordering of the objects of $\mathsf{U_N}$. We construct a countable submodel M as follows. Let $\mathsf{A_0}$ be a countable subset of $\mathsf{U_N}$. We construct a series $\mathsf{A_0}$, $\mathsf{A_1}$, $\mathsf{A_2}$ .... For a formula of the form $\exists x\mathcal{P}$ in the language $\mathcal{L}$, and a variable assignment d into A_i, let d' be like d for the initial segment that assigns to variables free in $\mathcal{P}$, and after assigns to a constant object $\mathsf{m_0}$ in $\mathsf{A_0}$. Then for any $\mathcal{P}$ and d such that $\mathsf{N_d}[\exists x\mathcal{P}] = \mathsf{S}$, find the first object o in the well-ordering of $\mathsf{U_N}$ such that $\mathsf{N}_{\mathsf{d}'(x|\mathsf{o})}[\mathcal{P}] = \mathsf{S}$. To form A_{i+1}, augment A_i with all the objects obtained this way. Because there are countably many formulas, and countably many initial segments of the variable assignments, countably many objects are added to form A_{i+1}, and if A_i is countable, A_{i+1} is countable. Let $\mathsf{U_M}$ be $\bigcup_{i\geq 0}\mathsf{A}_i$. Again, if each A_i is countable, $\mathsf{U_M}$ is countable.

There may be uncountably many variable assignments into a given A_i. However, for a given formula $\mathcal{P}$, no matter how may assignments there may be on which it is satisfied, there can be at most countably many initial segments of the sort d'. So at most countably many objects are added. The functions from formulas and variable assignments to individuals are *Skolem* functions, and we consider the closure of A under the set of all Skolem functions.

T11.17. With $\mathsf{U_M}$ constructed as above, a submodel M of N is well-defined.

Clearly $\mathsf{U_M} \subseteq \mathsf{U_N}$. For constants, consider the case when $\exists x\mathcal{P}$ is $\exists x(x = c)$; then at any stage i, $\mathsf{M}_{\mathsf{d}'(x|\mathsf{o})}[x = c] = \mathsf{S}$ iff $\mathsf{o} = \mathsf{M}[c]$. So $\mathsf{M}[c]$ is a member of A_{i+1} and so of $\mathsf{U_M}$. Similarly, for functions, consider the case when $\exists x\mathcal{P}$ is $\exists x(h^n v_1 \dots v_n = x)$ for some function symbol h^n and variables $v_1 \dots v_n$ and x. For any d, consider some d' which assigns objects to each of the variables $v_1 \dots v_n$; then there there is some A_i such that d' is an assignment into it; so by construction, A_{i+1} includes an object o

such that $\mathsf{N}_{\mathsf{d}'(x|\mathsf{o})}[h^n v_1 \dots v_n = x] = \mathsf{S}$. But this must be the object $\mathsf{N}[h^n]\langle \mathsf{N}_{\mathsf{d}'}[v_1], \dots \mathsf{N}_{\mathsf{d}'}[v_1]\rangle$.

T11.18. For any model N there is an $\mathsf{M} \prec \mathsf{N}$ such that M has a countable domain. (*Löwenheim-Skolem*)

To show $\mathsf{M} \prec \mathsf{N}$ by T11.16, it remains to show that for any formula $\mathcal{P}$ and every variable assignment d such that $\mathsf{N}_{\mathsf{d}}[\exists x \mathcal{P}] = \mathsf{S}$ there is an $\mathsf{m} \in \mathsf{U}_{\mathsf{M}}$ such that $\mathsf{N}_{\mathsf{d}(x|\mathsf{m})}[\mathcal{P}] = \mathsf{S}$. But this is easy. Suppose $\mathsf{N}_{\mathsf{d}}[\exists x \mathcal{P}] = \mathsf{S}$; then where d and d' agree on assignments to all the free variables in $\mathcal{P}$, by T8.4, $\mathsf{N}_{\mathsf{d}'}[\exists x \mathcal{P}] = \mathsf{S}$. But all assignments from d' are elements of some A_i; so by construction there is object m such that $\mathsf{N}_{\mathsf{d}'(x|\mathsf{m})}[\mathcal{P}] = \mathsf{S}$ in A_{i+1} and so in U_{M}; and since d and d' agree on their assignments to all the free variables in $\mathcal{P}$, by T8.4, $\mathsf{N}_{\mathsf{d}(x|\mathsf{m})}[\mathcal{P}] = \mathsf{S}$.

[applications]

11.6.3 Upward Löwenheim-Skolem

Part IV

Logic and Arithmetic: Incompleteness and Computability

Introductory

In Part III we showed that our semantical and syntactical logical notions are related as we want them to be: exactly the same arguments are semantically valid as are provable. So,

$$\text{(A)} \qquad \Gamma \vdash \mathcal{P} \quad \text{iff} \quad \Gamma \vDash \mathcal{P}$$

Thus our derivation system is both sound and adequate, as it should be. In this part, however, we encounter a series of limiting results — with particular application to arithmetic and computing.

First, it is natural to think mathematics is characterized by proofs and derivations. Thus, one might anticipate that there would be some system of premises Δ such that for any $\mathcal{P}$ in $\mathcal{L}_{NT}$, we would have,

$$\text{(B)} \qquad \Delta \vdash \mathcal{P} \quad \text{iff} \quad \mathsf{N}[\mathcal{P}] = \mathsf{T}$$

where N is the standard interpretation of number theory. Note the difference between our claims. In (A) derivations are matched to entailments; in (B) derivations (and so entailments) are matched to truths on an interpretation. Perhaps inspired by suspicions about the existence or nature of numbers, one might expect that derivations would even entirely replace the notion of mathematical truth. And Q or PA may already seem to be deductive systems as in (B). But we shall see that there can be no such deductive system. From Gödel's first incompleteness theorem, under certain constraints, no consistent deductive system has as consequences either $\mathcal{P}$ or $\sim\mathcal{P}$ for every $\mathcal{P}$ of $\mathcal{L}_{NT}$; any such theory is (negation) *incomplete*. But then, subject to those constraints, any consistent deductive system must omit some truths of arithmetic from among its consequences.[3]

Suppose there is no one-to-one map between truths of arithmetic and consequences of our theories. Rather, we propose a theory R(eal) whose consequences

[3] Gödel's groundbreaking paper is "On the Formally Undecidable Propositions of *Principia Mathematica* and Related Systems."

are unproblematically true, and another theory I(deal) whose consequences outrun those of R and whose literal truth is therefore somehow suspect. Perhaps R is sufficient only for something like basic arithmetic, whereas I seems to quantify over all members of a far-flung infinite domain. Even though not itself a vehicle for truth, theory I may be useful under certain circumstances. Suppose,

(a) For any $\mathcal{P}$ in the scope of R, if $\mathcal{P}$ is not true, then $R \vdash \sim\mathcal{P}$

(b) I *extends* R: If $R \vdash \mathcal{P}$ then $I \vdash \mathcal{P}$

(c) I is *consistent*: There is no $\mathcal{P}$ such that $I \vdash \mathcal{P}$ and $I \vdash \sim\mathcal{P}$

Then theory I may be treated as a tool for achieving results in the scope of R: Suppose $\mathcal{P}$ is a result in the scope of R, and $I \vdash \mathcal{P}$; then by consistency, $I \nvdash \sim\mathcal{P}$; and because I extends R, $R \nvdash \sim\mathcal{P}$; so by (a), $\mathcal{P}$ is true. This is (a sketch of) the famous 'Hilbert program' for mathematics, which aims to make sense of infinitary mathematics based not on the truth but rather the consistency of theory I.

Because consistency is a syntactical result about proof systems, not itself about far-flung mathematical structures, one might have hoped for proofs of consistency from real, rather than ideal, theories. But Gödel's second incompleteness theorem tells us that derivation systems extending PA cannot prove even their own consistency. So a weaker "real" theory will not be able to prove the consistency of PA and its extensions. But this seems to remove a demonstration of (c) and so to doom the Hilbert strategy.[4]

Even though no one derivation system has as consequences every mathematical truth, derivations remain useful, and mathematicians continue to do proofs! Given that we care about them, there is a question about the automation of proofs. Say a property or relation is *effectively decidable* iff there is an algorithm or program that for any given case, decides in a finite number of steps whether the property or relation applies. Abstracting from the limitations of particular computing devices, we shall

[4]We are familiar with the Pythagorean Theorem according to which the hypotenuse and sides of a right triangle are such that $a^2 = b^2 + c^2$. In the 1600s Fermat famously proposed that there are no integers a, b, c such that $a^n = b^n + c^n$ for $n > 2$; so, for example, there are no a, b, c such that $a^3 = b^3 + c^3$. In 1995 Andrew Wiles proved that this is so. But Wiles's proof requires some fantastically abstract (and difficult) mathematics. Even if Wiles's abstract theory (I) is not *true* Hilbert could still accept the demonstration of Fermat's (real) theorem so long as I is shown to be *consistent*. Gödel's result seems to doom this strategy. Of course, one might simply accept Wiles's proof on the ground that his advanced mathematics is *true* so that its consequences are true as well. But this is a topic in philosophy of mathematics, not logic! See, for example, Shapiro, *Thinking About Mathematics* for an introduction to options in the philosophy of mathematics. Our limiting results may very well stimulate interest in that field!

identify a class of relations which are decidable. A corollary of Gödel's first theorem is that validity in systems like *ND* and *AD* is not among the decidable relations. Thus there are interesting limits on the decidable relations — where it is possible also to look back through this lense at Gödel's first theorem.

Chapter 12 lays down background required for chapters that follow. It begins with a discussion of *recursive functions*, and concludes with a few essential results, including a demonstration of the incompleteness of arithmetic. Chapters 13 and 14 deepen and extend those results in different ways. Chapter 13 includes Gödel's own argument for incompleteness from the construction of a sentence such that neither it nor its negation is provable, along with demonstration of the second incompleteness theorem. Chapter 14 again shows that there must exist a sentence such that neither it nor its negation is provable, but this time in association with an account of computability. Chapter 12 is required for either chapter 13 or chapter 14; but those chapters may be taken in either order.

Chapter 12

Recursive Functions and Q

A formal *theory* consists of a language, with some axioms and proof system. Q and PA are example theories. A theory T is (negation) *complete* iff for any sentence $\mathcal{P}$ in its language $\mathcal{L}$, either $T \vdash \mathcal{P}$ or $T \vdash \sim\mathcal{P}$. Observe again that a derivation system is adequate when it proves every entailment of some premises. Our standard logic does that. Granting then, the adequacy of the logic, negation completeness is a matter of premises proving a sufficiently robust set of consequences — proving consequences which include $\mathcal{P}$ or $\sim\mathcal{P}$ for every $\mathcal{P}$ in the language.

Let us pause to consider why completeness matters. From E8.27, as soon as a language $\mathcal{L}$ has an interpretation I, for any sentence $\mathcal{P}$ in $\mathcal{L}$, either $\mathsf{I}[\mathcal{P}] = \mathsf{T}$ or $\mathsf{I}[\sim\mathcal{P}] = \mathsf{T}$. So if we set out to characterize by means of a theory the sentences that are true on some interpretation, our theory is bound to omit some sentences unless it is such that for any $\mathcal{P}$, either $T \vdash \mathcal{P}$ or $T \vdash \sim\mathcal{P}$. To the extent that we desire a characterization of all true sentences in some domain, of arithmetic or whatever, a complete theory is a desirable theory.[1]

By itself negation completeness is no extraordinary thing. Consider a theory whose language has just two sentence letters A and B, along with the usual sentential operators and rules. The axioms of our theory are just A and $\sim B$. On a truth table, there is just one row were these axioms are both true, and on that row, any $\mathcal{P}$ in the language is either T or F, so that one of $\mathcal{P}$ or $\sim\mathcal{P}$ is T.

[1] We thus restrict ourselves to consideration of *sentences* as theorems — or, equivalently treat open formulas as equivalent to their universal closures (see p. 489)

(A)

A	B	A	$\sim B$	/	$\mathscr{P}$	$\sim\mathscr{P}$
T	T	***T***	***F***		–	–
T	F	***T***	***T***		***T/F***	***F/T***
F	T	***F***	***F***		–	–
F	F	***F***	***T***		–	–

So for any $\mathscr{P}$, either $A, \sim B \vDash \mathscr{P}$ or $A, \sim B \vDash \sim\mathscr{P}$. But from the adequacy of the derivation system if $\Gamma \vDash \mathscr{P}$, then $\Gamma \vdash \mathscr{P}$ (T10.11, p. 485); so for any $\mathscr{P}$, either $A, \sim B \vdash \mathscr{P}$ or $A, \sim B \vdash \sim\mathscr{P}$. So our little theory with its restricted language is negation complete. Contrast this with a theory that has the same language and rules, but A as its only axiom. In this case, it is easy to see from truth tables that, say, $A \nvDash B$ and $A \nvDash \sim B$. But by soundness, if $\Gamma \vdash \mathscr{P}$ then $\Gamma \vDash \mathscr{P}$ (T10.3, p. 472); it follows that $A \nvdash B$ and $A \nvdash \sim B$. So this theory is not negation complete.

These theories are not very interesting. However, let $\mathscr{L}_{NT}^{S+}$ be a language like $\mathscr{L}_{NT}$ whose only function symbols are S and $+$ (without $\times$), and let $\mathscr{L}_{NT}^{\times}$ be a language like $\mathscr{L}_{NT}$ whose only function symbol is $\times$ (without S and $+$). Then there is a complete theory for the arithmetic of $\mathscr{L}_{NT}^{S+}$ (*Presburger Arithmetic*), and a complete theory for the arithmetic of $\mathscr{L}_{NT}^{\times}$ (*Skolem Arithmetic*).[2] These are interesting and powerful theories. So, again, by itself negation completeness is not so extraordinary.

However there is no complete theory for the arithmetic of $\mathscr{L}_{NT}$ which includes all of S, $+$ and $\times$. It turns out that theories are something like superheros. In the ordinary case, a complete, and so a "happy" life is at least within reach. However, as theories acquire certain powers, they take on a "fatal flaw" just because of their powers — where this flaw makes completeness unattainable. On its face, theory Q does not appear particularly heroic. We have seen already in E7.21 that Q $\nvdash x \times y = y \times x$ and Q $\nvdash \sim(x \times y = y \times x)$. So Q is negation incomplete. PA which does prove $x \times y = y \times x$ along with other standard results in arithmetic might seem a more likely candidate for heroism. But Q includes already features sufficient to generate the flaw which appears also in any theories, like PA, which have at least all the powers of Q. It is our task to identify this flaw.

It turns out that a system with the powers of Q including S, $+$ and $\times$ can express and capture all the *recursive* functions — and a system with these powers must have the fatal flaw. Thus, in this chapter we focus on the recursive functions, and associate them with powers of our formal systems. We begin in 12.1 saying what recursive functions are; then in 12.2 and 12.3 we show that Q expresses and captures the recursive functions; 12.4 extends the range of recursive functions to include a function

[2]For demonstration of completeness for Presburger Arithmetic, see Fisher, *Formal Number Theory and Computability* chapter 7 along with Boolos, Burgess and Jeffrey, *Computability and Logic* chapter 24.

that identifies proofs. Finally, from these results, section 12.5 concludes with some applications, including the incompleteness of arithmetic.

12.1 Recursive Functions

In chapter 6 (p. 318) for Q and PA we had axioms of the sort,

a. $x + \emptyset = x$
b. $x + Sy = S(x + y)$

and

c. $x \times \emptyset = \emptyset$
d. $x \times Sy = (x \times y) + x$

These enable us to derive $x + y$ and $x \times y$ for arbitrary values of x and y. Thus, by (a) $2 + 0 = 2$; so by (b) $2 + 1 = 3$; and by (b) again, $2 + 2 = 4$; and so forth. From the values at any one stage, we are in a position to calculate values at the next. And similarly for multiplication. From E6.35 on p. 319, all this should be familiar.

While axioms thus supply effective means for calculating the values of these functions, the functions themselves might be similarly *identified* or *specified*. So, given a successor function $\mathsf{suc}(\mathsf{x})$, we may identify the functions $\mathsf{plus}(\mathsf{x}, \mathsf{y})$:

a. $\mathsf{plus}(\mathsf{x}, 0) = \mathsf{x}$
b. $\mathsf{plus}(\mathsf{x}, \mathsf{suc}(\mathsf{y})) = \mathsf{suc}(\mathsf{plus}(\mathsf{x}, \mathsf{y}))$

and $\mathsf{times}(\mathsf{x}, \mathsf{y})$:

c. $\mathsf{times}(\mathsf{x}, 0) = 0$
d. $\mathsf{times}(\mathsf{x}, \mathsf{suc}(\mathsf{y})) = \mathsf{plus}(\mathsf{times}(\mathsf{x}, \mathsf{y}), \mathsf{x})$

For ease of reading, let us typically revert to the more ordinary notation S, $\mathbf{+}$ and $\mathbf{\times}$ for these functions, though we stick with the (emphasized) sans serif font. We have been thinking of functions as certain complex sets. Thus the plus function is a set with elements $\{\ldots \langle\langle 2, 0\rangle, 2\rangle, \langle\langle 2, 1\rangle, 3\rangle, \langle\langle 2, 2\rangle, 4\rangle \ldots\}$. Our specification picks out this set. From the first clause, $\mathsf{plus}(\mathsf{x}, \mathsf{y})$ has $\langle\langle 2, 0\rangle, 2\rangle$ as a member; given this, $\langle\langle 2, 1\rangle, 3\rangle$ is a member; and so forth. So the two clauses work together to specify the plus function. And similarly for times.

But these are not the only sets which may be specified this way. Thus the standard factorial $\mathsf{fact}(\mathsf{x})$:

e. $\mathsf{fact}(0) = \mathsf{S0}$
f. $\mathsf{fact}(\mathsf{Sy}) = \mathsf{fact}(\mathsf{y}) \mathbf{\times} \mathsf{Sy}$

Again, we will often revert to the more typical $\mathsf{x!}$ notation. Zero factorial is one. And the factorial of Sy multiplies $1 \mathbf{\times} 2 \mathbf{\times} \ldots \mathbf{\times}\ \mathsf{y}$ by Sy. Similarly $\mathsf{power}(\mathsf{x}, \mathsf{y})$:

g. $\mathsf{power}(x, 0) = S0$
h. $\mathsf{power}(x, Sy) = \mathsf{power}(x, y) \times x$

Any number to the power of zero is one ($x^0 = 1$). And then x^{Sy} multiplies $x^y = x \times x \ldots \times x$ (y times) by another x.

We shall be interested in a class of functions, the *recursive* functions, which may be specified (in part) by this strategy. To make progress, we turn to a general account in five stages.

12.1.1 Initial Functions

Our examples have simply taken $\mathsf{suc}(x)$ as given. Similarly, we shall require a stock of *initial functions*. There are initial functions of three different types.

First, we shall continue to include $\mathsf{suc}(x)$ among the initial functions. So $\mathsf{suc}(x) = \{\langle 0, 1\rangle, \langle 1, 2\rangle, \langle 2, 3\rangle \ldots\}$.

Second, $\mathsf{zero}(x)$ is a function which returns zero for any input value. So $\mathsf{zero}(x) = \{\langle 0, 0\rangle, \langle 1, 0\rangle, \langle 2, 0\rangle \ldots\}$.

Finally, for any $1 \leq k \leq j$, we require a collection of *identity* functions $\mathsf{idnt}^j_k(x_1 \ldots x_j)$. Each idnt^j_k function has j places and simply returns the value from the k^{th} place. Thus $\mathsf{idnt}^3_2(4, 5, 6) = 5$. So, $\mathsf{idnt}^3_2 = \{\ldots \langle\langle 1, 2, 3\rangle, 2\rangle \ldots \langle\langle 4, 5, 6\rangle, 5\rangle \ldots\}$. And in the simplest case, $\mathsf{idnt}^1_1(x) = x$.

12.1.2 Composition

In our examples, we have let one function be *composed* from others — as when we consider $\mathsf{times}(x, \mathsf{suc}(y))$ or the like. Say $\vec{x}$, $\vec{y}$ and $\vec{z}$ represent (possibly empty) sequences of variables $x_1 \ldots x_n$, $y_1 \ldots y_n$ and $z_1 \ldots z_n$.

CM Let $g(\vec{y})$ and $h(\vec{x}, w, \vec{z})$ be any functions. Then $f(\vec{x}, \vec{y}, \vec{z})$ is defined by *composition* from $g(\vec{y})$ and $h(\vec{x}, w, \vec{z})$ iff $f(\vec{x}, \vec{y}, \vec{z}) = h(\vec{x}, g(\vec{y}), \vec{z})$.

So $h(\vec{x}, w, \vec{z})$ gets its value in the w-place from $g(\vec{y})$. Here is a simple example: $f(y, z) = \mathsf{zero}(y) + z$ results by composition from substitution of $\mathsf{zero}(y)$ into $\mathsf{plus}(w, z)$; so $\mathsf{plus}(w, z)$ gets its value in the w-place from $\mathsf{zero}(y)$. The result is the set with members, $\{\ldots \langle\langle 2, 0\rangle, 0\rangle, \langle\langle 2, 1\rangle, 1\rangle, \langle\langle 2, 2\rangle, 2\rangle \ldots\}$. Given, say, input $\langle 2, 2\rangle$, $\mathsf{zero}(y)$ takes the input 2 and supplies a zero to the first place of the $\mathsf{plus}(x, y)$ function; then from $\mathsf{plus}(x, y)$ the result is a sum of 0 and 2 which is 2. And similarly in other cases. In contrast, $\mathsf{zero}(x + y)$ has members $\{\ldots \langle\langle 2, 0\rangle, 0\rangle, \langle\langle 2, 1\rangle, 0\rangle, \langle\langle 2, 2\rangle, 0\rangle \ldots\}$. You should see how this works.

12.1.3 Recursion

For each of our examples, $\mathsf{plus(x, y)}$, $\mathsf{times(x, y)}$, $\mathsf{fact(y)}$, and $\mathsf{power(x, y)}$, the value of the function is set for $\mathsf{y} = 0$ and then for $\mathsf{suc(y)}$ given its value for y. These illustrate the method of recursion. Put generally,

RC Given some functions $\mathsf{g}(\vec{\mathsf{x}})$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$, $\mathsf{f}(\vec{\mathsf{x}}, \mathsf{y})$ is defined by *recursion* when,

$$\mathsf{f}(\vec{\mathsf{x}}, 0) = \mathsf{g}(\vec{\mathsf{x}})$$
$$\mathsf{f}(\vec{\mathsf{x}}, \mathsf{Sy}) = \mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{f}(\vec{\mathsf{x}}, \mathsf{y}))$$

We adopt the general scheme so that we can operate on recursive functions in a consistent way. However the general scheme includes flexibility that is not always required. In the cases of plus, times and power, $\vec{\mathsf{x}}$ reduces to a simple variable x; for fact, $\vec{\mathsf{x}}$ disappears altogether, so that the function $\mathsf{g}(\vec{\mathsf{x}})$ reduces to a constant. And, as we shall see, the function $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$ need not depend on each of its variables x, y and u.

However, by clever use of our initial functions, it is possible to see each of our sample functions on this pattern. Thus for $\mathsf{plus(x, y)}$, set $\mathsf{gplus(x)} = \mathsf{idnt}^1_1\mathsf{(x)}$ and $\mathsf{hplus(x, y, u)} = \mathsf{suc(idnt}^3_3\mathsf{(x, y, u))}$. Then,

a′ $\mathsf{plus(x, 0)} = \mathsf{idnt}^1_1\mathsf{(x)}$
b′ $\mathsf{plus(x, Sy)} = \mathsf{suc(idnt}^3_3\mathsf{(x, y, plus(x, y)))}$

$\mathsf{plus(x, 0)}$ is set to $\mathsf{gplus(x)}$ and $\mathsf{plus(x, Sy)}$ to $\mathsf{hplus}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{plus(x, y)})$. And these work as they should: $\mathsf{idnt}^1_1\mathsf{(x)} = \mathsf{x}$ and $\mathsf{suc(idnt}^3_3\mathsf{(x, y, plus(x, y)))}$ is the same as $\mathsf{suc(plus(x, y))}$. So we recover the conditions (a) and (b) from above.

Similarly, for $\mathsf{times(x, y)}$, we can let $\mathsf{gtimes(x)} = \mathsf{zero(x)}$ and $\mathsf{htimes(x, y, u)} = \mathsf{plus(idnt}^3_3\mathsf{(x, y, u), x)}$. Then,

c′ $\mathsf{times(x, 0)} = \mathsf{zero(x)}$
d′ $\mathsf{times(x, Sy)} = \mathsf{plus(idnt}^3_3\mathsf{(x, y, times(x, y)), x)}$

So $\mathsf{times(x, 0)} = 0$ and $\mathsf{times(x, Sy)} = \mathsf{plus(times(x, y), x))}$, and all is well. Observe that we would obtain the same result with $\mathsf{htimes(x, y, u)} = \mathsf{plus(u, idnt}^3_1\mathsf{(x, y, u))}$ or perhaps, $\mathsf{plus(idnt}^3_3\mathsf{(x, y, u), idnt}^3_1\mathsf{(x, y, u))}$. The role of the identity functions in these formulations is to preserve h as a function of x, y and u, even where not each place is required — as the y-place is not required for times, and so to adhere to the official form which makes $\mathsf{h(x, y, u)}$ a function of variables in each place. And there are these different ways to produce a function of all the variables to achieve the desired result.

In the case of $\mathsf{fact(y)}$, there are no places to the $\vec{\mathsf{x}}$ vector. So gfact is reduced to a zero-place function, that is, to a constant, and hfact to a function of y and u.

In contrast, for $\mathsf{times}(x, y)$, $\vec{x}$ retains one place, so $\mathsf{gtimes}(x)$ is not reduced to a constant; rather $\mathsf{gtimes}(x) = \mathsf{zero}(x)$ remains a full-fledged function — only one which returns the same value for every value of x. For $\mathsf{fact}(y)$, set $\mathsf{gfact} = \mathsf{suc}(0)$ and $\mathsf{hfact}(y, u) = \mathsf{times}(u, \mathsf{suc}(y))$. Again, identity functions work to preserve h as a function y, and u, even where not each place is required, in order to adhere to the official form. However, there is no requirement that the places be picked out by identity functions! In this case, each variable is used in a natural way, so identity functions are not required. It is left as an exercise to show that gfact and hfact identify the same function as constraints (e), (f), and to then to find $\mathsf{gpower}(x)$ and $\mathsf{hpower}(x, y, u)$.

12.1.4 Regular Minimization

So far, the method of our examples is easily matched to the capacities of computing devices. To find the value of a recursive function, begin by finding values for $y = 0$, and then calculate other values, from one stage to the next. But this is just what computing devices do well. So, for example, in the syntax of the Ruby language,[3] given some functions `g(x)` and `h(x,y,u)`,

(B)

```
def recfunc(a,b)
 k = g(a)
 for y in 0..b-1
  k = h(a,y,k)
 end
 return k
end
```

Using `g(a)` this program calculates the value of `k` for input `(a,0)`. And then, given the current value of `y`, and of `k` for input `(a,y)`, repeatedly uses `h` to calculate `k` for the next value of `y`, until it finally reaches and returns the value of `k` for input `(a,b)`. Observe that the calculation of `recfunc(a,b)` requires exactly `b` iterations before it completes.

But there is a different repetitive mechanism available for computing devices — where this mechanism does not begin with a fixed number of iterations. Suppose we have some function `g(a,b)` with values `g(a,0)`, `g(a,1)`, `g(a,2)`... where for each `a` there are at least some values of `b` such that `g(a,b)` = `0`. For any value of `a`, suppose we want the least `b` such that `g(a,b)` = `0`. Then we might reason as follows.

[3] Ruby is convenient insofar as it is interpreted and so easy to run, and available at no cost on multiple platforms (see http://www.ruby-lang.org/en/downloads/). We depend only on very basic features familiar from most any exposure to computing.

The Recursion Theorem

One may wonder whether our specification $\mathsf{f}(x, y)$ by recursion from $\mathsf{g}(\vec{x})$ and $\mathsf{h}(\vec{x}, y, u)$ results in a unique function. However it is possible to show that it does.

RT Suppose $\mathsf{g}(\vec{x})$ and $\mathsf{h}(\vec{x}, y, u)$ are total functions on $\mathcal{N}$; then there exists a unique function $\mathsf{f}(\vec{x}, y)$ such that,

(r) For any $\vec{x}$ and $y \in \omega$,

a. $\mathsf{f}(\vec{x}, 0) = \mathsf{g}(\vec{x})$

b. $\mathsf{f}(\vec{x}, \mathsf{suc}(y)) = \mathsf{h}(\vec{x}, y, \mathsf{f}(\vec{x}, y))$

We identify this function as a union of functions which may be constructed by means of g and h. The *domain* of a total function from r^n to s is always r^n; for a partial function, the domain of the function is that subset of r^n whose members are matched by the function to members of s (for background see the set theory reference p. 117). Say a (maybe partial) function $s(\vec{x}, y)$ is *acceptable* iff,

i. If $\langle\vec{x}, 0\rangle \in \mathsf{dom}(s)$, then $s(\vec{x}, 0) = \mathsf{g}(\vec{x})$

ii. If $\langle\vec{x}, \mathsf{suc}(n)\rangle \in \mathsf{dom}(s)$, then $\langle\vec{x}, n\rangle \in \mathsf{dom}(s)$ and $s(\vec{x}, \mathsf{suc}(n)) = \mathsf{h}(\vec{x}, n, s(\vec{x}, n))$

A function with members $\{\langle\langle\vec{x}, 0\rangle, \mathsf{g}(\vec{x})\rangle, \langle\langle\vec{x}, 1\rangle, \mathsf{h}(\vec{x}, 0, \mathsf{g}(\vec{x}))\rangle\}$ would satisfy (i) and (ii). A function which satisfies (r) is acceptable, though not every function which is acceptable satisfies (r); we show that exactly one acceptable function satisfies (r). Let F be the collection of all acceptable functions, and f be $\bigcup F$. Thus $\langle\langle\vec{x}, n\rangle, a\rangle \in f$ iff $\langle\langle\vec{x}, n\rangle, a\rangle$ is a member of some acceptable s; iff $s(\vec{x}, n) = a$ for some acceptable s. We sketch reasoning to show that f has the right features.

I. For any acceptable s and s', if $\langle\langle\vec{x}, n\rangle, a\rangle \in s$ and $\langle\langle\vec{x}, n\rangle, b\rangle \in s'$, then $a = b$. By induction on n: Suppose $\langle\langle\vec{x}, 0\rangle, a\rangle \in s$ and $\langle\langle\vec{x}, 0\rangle, b\rangle \in s'$; then by (i), $a = b = \mathsf{g}(\vec{x})$. Assume that if $\langle\langle\vec{x}, k\rangle, a\rangle \in s$ and $\langle\langle\vec{x}, k\rangle, b\rangle \in s'$ then $a = b$. Show that if $\langle\langle\vec{x}, \mathsf{suc}(k)\rangle, c\rangle \in s$ and $\langle\langle\vec{x}, \mathsf{suc}(k)\rangle, d\rangle \in s'$ then $c = d$. Suppose $\langle\langle\vec{x}, \mathsf{suc}(k)\rangle, c\rangle \in s$ and $\langle\langle\vec{x}, \mathsf{suc}(k)\rangle, d\rangle \in s'$. Then by (ii) $c = \mathsf{h}(\vec{x}, k, s(\vec{x}, k))$ and $d = \mathsf{h}(\vec{x}, k, s'(\vec{x}, k))$. But by by assumption $s(\vec{x}, k) = s'(\vec{x}, k)$; so $c = d$.

II. $\mathsf{dom}(f)$ includes every $\langle\vec{x}, n\rangle$. By induction on n: For any $\vec{x}$, $\{\langle\langle\vec{x}, 0\rangle, \mathsf{g}(\vec{x})\rangle\}$ is itself an acceptable function. Assume that for any $\vec{x}$, $\langle\vec{x}, k\rangle \in \mathsf{dom}(f)$. Show that for any $\vec{x}$, $\langle\vec{x}, \mathsf{suc}(k)\rangle \in \mathsf{dom}(f)$. Suppose otherwise, and consider a function, $s = f \cup \{\langle\langle\vec{x}, \mathsf{suc}(k)\rangle, \mathsf{h}(\vec{x}, k, f(\vec{x}, k))\rangle\}$. But we may show that s so defined is an acceptable function; and since s is acceptable, it is a subset of f; so $\langle\vec{x}, \mathsf{suc}(k)\rangle \in \mathsf{dom}(f)$. Reject the assumption.

III. Now by (I), if $\langle\langle\vec{x}, n\rangle, a\rangle \in f$ and $\langle\langle\vec{x}, n\rangle, b\rangle \in f$, then $a = b$; so f is a function; and by (II) the domain of f includes every $\langle\vec{x}, n\rangle$; by construction it is easy to see that f is itself acceptable. From these, f satisfies (r). Suppose some f' also satisfies (r); then f' is acceptable; so by construction, f' is a subset of f; but since f' satisfies (r), it's domain includes every $\langle\vec{x}, n\rangle$; so $f' = f$. So (r) is uniquely satisfied.

*We employ *weak* induction from the induction schemes reference p. 388. Enderton, *Elements of Set Theory*, and Drake and Singh, *Intermediate Set Theory*, include nice discussions of this result.

(C)

```
def minfunc(a)
  y = 0
  until g(a,y) == 0
    y = y+1
  end
  return y
end
```

This program begins with `y = 0` and tests each value of `g(a,y)` until it returns a value of `0`. Once it finds this value, `minfunc(a)` is set equal to `y`. Given `g(a,b)`, then, `minfunc(a)` calculates a function which returns some value of `y` for any input value a.

But, as before, we might reason similarly to *specify* functions so calculated. For this, recall that a function is *total* iff it is defined on all members of its domain. Say a function $g(\vec{x}, y)$ is *regular* iff it is total and for all values of $\vec{x}$ there is at least one y such that $g(\vec{x}, y) = 0$. Then,

RM If $g(\vec{x}, y)$ is a regular function, the function $f(\vec{x}) = \mu y[g(\vec{x}, y)]$ which for each $\vec{x}$ takes as its value the least y such that $g(\vec{x}, y) = 0$ is defined by *regular minimization* from $g(\vec{x}, y)$.

For a simple example, consider a domain which consists of nonempty sets of integers with $g(x, y)$ such that $g(x, y) = 0$ if $y \in x$ and otherwise $g(x, y) = 1$. Then for any set x, $f(x) = \mu y[g(x, y)]$ is the least element of x.

12.1.5 Final Definition

Finally, our sample functions are *cumulative*. Thus $\mathsf{plus}(x, y)$ depends on $\mathsf{suc}(x)$; $\mathsf{times}(x, y)$, on $\mathsf{plus}(x, y)$, and so forth. We are thus led to our final account.

RF A function f_k is *recursive* iff there is a series of functions $f_0, f_1 \ldots f_k$ such that for any $i \leq k$,

(i) f_i is an initial function $\mathsf{suc}(x)$, $\mathsf{zero}(x)$ or $\mathsf{idnt}^j_k(x_1 \ldots x_j)$.

(c) There are $a, b < i$ such that $f_i(\vec{x}, \vec{y}, \vec{z})$ results by composition from $f_a(\vec{y})$ and $f_b(\vec{x}, w, \vec{z})$.

(r) There are $a, b < i$ such that $f_i(\vec{x}, y)$ results by recursion from $f_a(\vec{x})$ and $f_b(\vec{x}, y, u)$.

(m) There is some $a < i$ such that $f_i(\vec{x})$ results by regular minimization from $f_a(\vec{x}, y)$.

If there is a series of functions $f_0, f_1 \ldots f_k$ such that for any $i \leq k$, just (i), (c) or (r), then (PR) f_k is *primitive recursive*.

So any recursive function results from a series of functions each of which satisfies one of these conditions. And such a series demonstrates that its members are recursive. For a simple example, plus is primitive recursive.

(D)	1. $\mathsf{idnt}^1_1(x)$	initial function
	2. $\mathsf{idnt}^3_3(x, y, u)$	initial function
	3. $\mathsf{suc}(w)$	initial function
	4. $\mathsf{suc}(\mathsf{idnt}^3_3(x, y, u))$	2,3 composition
	5. $\mathsf{plus}(x, y)$	1,4 recursion

From this list by itself, one might reasonably wonder whether $\mathsf{plus}(x, y)$, so defined, is the addition function we know and love. What follows, given primitive recursive functions $\mathsf{idnt}^1_1(x)$ and $\mathsf{suc}(\mathsf{idnt}^3_3(x, y, u))$ is that a primitive recursive function results by recursion from them. It turns out that this is the addition function. It is left as an exercise to exhibit $\mathsf{times}(x, y)$, $\mathsf{fact}(x)$ and $\mathsf{power}(x, y)$ as primitive recursive as well.

*E12.1. (a) Show that the proposed gfact and $\mathsf{hfact}(y, u)$ result in conditions (e) and (f). Then (b) produce a defininition for $\mathsf{power}(x, y)$ by finding functions $\mathsf{gpower}(x)$, and $\mathsf{hpower}(x, y, u)$ and then show that they have the same result as conditions (g) and (h).

E12.2. Generate a sequence of functions sufficient to show that $\mathsf{power}(x, y)$ is primitive recursive.

E12.3. Install some convenient version of Ruby on your computing platform (see `http://www.ruby-lang.org/en/downloads/`) and open `recursive1.rb` from the text website (`http://rocket.csusb.edu/~troy/int-ml.html`). Extend the sequence of functions started there to include `fact(x)` and `power(x,y)`. Calculate some values of these functions and print the results, along with your program (do not worry if these latter functions run slowly for even moderate values of `x` and `y`). This assignment does not require any particular computing expertise — especially, there should be no appeal to functions except from earlier in the chain. (This exercise suggests a point, to be developed in chapter 14, that recursive functions are *computable*.)

12.2 Expressing Recursive Functions

Having identified the recursive functions, we turn now to the first of two powers to be associated with theory incompleteness. In this case, it is an *expressive* power. Say a theory is *sound* iff its axioms are true and its proof system is sound. So all the theorems of a sound theory are true. Then we shall be able to show that if a theory is sound and its interpreted language *expresses* all the recursive functions, it must be negation incomplete. In this section, then, we show that $\mathscr{L}_{NT}$, on its standard interpretation, expresses the recursive functions.

12.2.1 Definition and Basic Results

For a language $\mathscr{L}$ and interpretation I, suppose that for each $\mathsf{m} \in \mathsf{U}$, a variable-free term $\overline{\mathsf{m}}$ is such that, in the sense of definition AI, $\mathsf{I}(\overline{\mathsf{m}}) = \mathsf{m}$ — so for any variable assignment d, $\mathsf{I_d}[\overline{\mathsf{m}}] = \mathsf{m}$. The simplest way for this to happen is if each $\mathsf{m} \in \mathsf{U}$ has exactly one constant assigned to it; then for any m, $\overline{\mathsf{m}}$ is the constant to which m is assigned. But the standard interpretation for number theory N also has the special feature that variable-free terms are assigned to each member of U. On this interpretation different variable-free terms may be assigned the same object (as $SS\emptyset$ and $S\emptyset + S\emptyset$ are each assigned 2). However, on the standard interpretation for number theory, for any n, we simply take as $\overline{\mathsf{n}}$, $S \ldots S\emptyset$ with n repetitions of the successor operator. So $\overline{0}$ abbreviates the term $\emptyset$, $\overline{1}$ the term $S\emptyset$, etc.

Given this, we shall say that a formula $\mathscr{R}(x)$ *expresses* a relation $\mathsf{R}(\mathsf{x})$ on interpretation I, just in case if $\mathsf{m} \in \mathsf{R}$ then $\mathsf{I}[\mathscr{R}(\overline{\mathsf{m}})] = \mathsf{T}$ and if $\mathsf{m} \notin \mathsf{R}$ then $\mathsf{I}[\sim\mathscr{R}(\overline{\mathsf{m}})] = \mathsf{T}$. So the formula is true when the individual is a member of the relation and false when it is not. To express a relation on an interpretation, a formula must "say" which individuals fall under the relation. Expressing a relation is closely related to translation. A formula $\mathscr{R}(x)$ expresses a relation $\mathsf{R}(\mathsf{x})$ when every sentence $\mathscr{R}(\overline{\mathsf{m}})$ is a good translation of the sentence $\mathsf{m} \in \mathsf{R}$ on the single intended interpretation I (compare chapter 5). So there is a single intended interpretation I, and a corresponding class of good translations when $\mathscr{R}(x)$ expresses $\mathsf{R}(\mathsf{x})$ on the interpretation I. Thus, generalizing,

EXr For any language $\mathscr{L}$, interpretation I, and objects $\mathsf{m}_1 \ldots \mathsf{m}_n \in \mathsf{U}$, relation $\mathsf{R}(\mathsf{x}_1 \ldots \mathsf{x}_n)$ is *expressed* by formula $\mathscr{R}(x_1 \ldots x_n)$ iff,

(i) If $\langle \mathsf{m}_1 \ldots \mathsf{m}_n \rangle \in \mathsf{R}$ then $\mathsf{I}[\mathscr{R}(\overline{\mathsf{m}}_1 \ldots \overline{\mathsf{m}}_n)] = \mathsf{T}$

(ii) If $\langle \mathsf{m}_1 \ldots \mathsf{m}_n \rangle \notin \mathsf{R}$ then $\mathsf{I}[\sim\mathscr{R}(\overline{\mathsf{m}}_1 \ldots \overline{\mathsf{m}}_n)] = \mathsf{T}$

Similarly, a one-place function $\mathsf{f(x)}$ has members of the sort $\langle \mathsf{x}, \mathsf{v}\rangle$ and so is really a kind of two-place relation. Thus to express a function $\mathsf{f(x)}$, we require a formula $\mathcal{F}(x, v)$ where if $\langle \mathsf{m}, \mathsf{a}\rangle \in \mathsf{f}$, then $\mathsf{I}[\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] = \mathsf{T}$. It would be natural to go on to require that if $\langle \mathsf{m}, \mathsf{a}\rangle \notin \mathsf{f}$ then $\mathsf{I}[\sim\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] = \mathsf{T}$. However this is not necessary once we build in another feature of functions — that they have a *unique* output for each input value. Thus we shall require,

EXf For any language $\mathcal{L}$, interpretation I, and objects $\mathsf{m_1 \dots m_n, a} \in \mathsf{U}$, function $\mathsf{f(x_1 \dots x_n)}$ is *expressed* by formula $\mathcal{F}(x_1 \dots x_n, v)$ iff,

if $\langle\langle \mathsf{m_1 \dots m_n}\rangle, \mathsf{a}\rangle \in \mathsf{f}$ then

(i) $\mathsf{I}[\mathcal{F}(\overline{\mathsf{m}}_1 \dots \overline{\mathsf{m}}_n, \overline{\mathsf{a}})] = \mathsf{T}$

(ii) $\mathsf{I}[\forall z(\mathcal{F}(\overline{\mathsf{m}}_1 \dots \overline{\mathsf{m}}_n, z) \rightarrow z = \overline{\mathsf{a}})] = \mathsf{T}$

From (i), $\mathcal{F}$ is true for $\overline{\mathsf{a}}$; from (ii) any z for for which it is true is identical to $\overline{\mathsf{a}}$.

Let us illustrate these definitions with some first applications. First, on any interpretation with the required variable-free terms, the formula $x = y$ expresses the equality relation $\mathsf{EQ(x, y)}$. For if $\langle \mathsf{m}, \mathsf{n}\rangle \in \mathsf{EQ}$ then $\mathsf{I}[\overline{\mathsf{m}}] = \mathsf{I}[\overline{\mathsf{n}}]$ so that $\mathsf{I}[\overline{\mathsf{m}} = \overline{\mathsf{n}}] = \mathsf{T}$; and if $\langle \mathsf{m}, \mathsf{n}\rangle \notin \mathsf{EQ}$ then $\mathsf{I}[\overline{\mathsf{m}}] \neq \mathsf{I}[\overline{\mathsf{n}}]$ so that $\mathsf{I}[\overline{\mathsf{m}} \neq \overline{\mathsf{n}}] = \mathsf{T}$. This works because $\mathsf{I}[=]$ just is the equality relation EQ.[4] Similarly, on the standard interpretation N for number theory, $\mathsf{suc(x)}$ is expressed by $Sx = v$, $\mathsf{plus(x, y)}$ by $x + y = v$, and $\mathsf{times(x, y)}$ by $x \times y = v$. Taking just the addition case, suppose $\langle\langle \mathsf{m}, \mathsf{n}\rangle, \mathsf{a}\rangle \in \mathsf{plus}$; then $\mathsf{N}[\overline{\mathsf{m}} + \overline{\mathsf{n}} = \overline{\mathsf{a}}] = \mathsf{T}$. And because addition is a function, $\mathsf{N}[\forall z((\overline{\mathsf{m}} + \overline{\mathsf{n}} = z) \rightarrow z = \overline{\mathsf{a}})] = \mathsf{T}$. Again, this works because $\mathsf{N}[+]$ just is the plus function. And similarly in the other cases. Put more generally,

T12.1. For an interpretation with the required variable-free terms assigned to members of the universe: (a) If $\mathcal{R}$ is a relation symbol and R is a relation, and $\mathsf{I}[\mathcal{R}] = \mathsf{R(x_1 \dots x_n)}$, then $\mathsf{R(x_1 \dots x_n)}$ is expressed by $\mathcal{R}x_1 \dots x_n$. And (b) if $\mathscr{h}$ is a function symbol and h is a function and $\mathsf{I}[\mathscr{h}] = \mathsf{h(x_1 \dots x_n)}$ then $\mathsf{h(x_1 \dots x_n)}$ is expressed by $\mathscr{h}x_1 \dots x_n = v$.

It is possible to argue semantically for these claims. However, as for translation, we take the project of demonstrating expression to be one of *providing* or supplying relevant formulas. So the theorem is immediate.

[4]Observe that inside the square brackets '=' is a relation symbol of the object language whose interpretation is built into I; outside square brackets '=' is a metalinguistic symbol used to indicate equality.

Also, as we have suggested, (i) and (ii) of condition EXf taken together are sufficient to generate a condition like EXr(ii). Recall from the set theory reference (p. 117) that a function is *total* just in case it has an output for any input.

T12.2. Suppose total function $\mathsf{f}(\mathsf{x}_1 \dots \mathsf{x}_\mathsf{n})$ is expressed by formula $\mathcal{F}(x_1 \dots x_n, y)$; then if $\langle\langle \mathsf{m}_1 \dots \mathsf{m}_\mathsf{n}\rangle, \mathsf{a}\rangle \notin \mathsf{f}$, $\mathsf{I}[\sim\mathcal{F}(\overline{\mathsf{m}}_1 \dots \overline{\mathsf{m}}_\mathsf{n}, \overline{\mathsf{a}})] = \mathsf{T}$.

For simplicity, consider just a one-place function $\mathsf{f}(\mathsf{x})$. Suppose $\mathsf{f}(\mathsf{x})$ is expressed by $\mathcal{F}(x, y)$ and $\langle \mathsf{m}, \mathsf{a}\rangle \notin \mathsf{f}$. Then since f is total, there is some b such that $\langle \mathsf{m}, \mathsf{b}\rangle \in \mathsf{f}$ for $\mathsf{a} \neq \mathsf{b}$ and so $\langle \mathsf{a}, \mathsf{b}\rangle \notin \textsc{eq}$. Suppose $\mathsf{I}[\sim\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] \neq \mathsf{T}$; then by TI, for some d, $\mathsf{I}_\mathsf{d}[\sim\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] \neq \mathsf{S}$; let h be a particular assignment of this sort; so $\mathsf{I}_\mathsf{h}[\sim\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] \neq \mathsf{S}$; so by SF($\sim$), $\mathsf{I}_\mathsf{h}[\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] = \mathsf{S}$.

But since $\langle \mathsf{m}, \mathsf{b}\rangle \in \mathsf{f}$ by EXf(ii), $\mathsf{I}[\forall z(\mathcal{F}(\overline{\mathsf{m}}, z) \to z = \overline{\mathsf{b}})] = \mathsf{T}$; so by TI, for any d, $\mathsf{I}_\mathsf{d}[\forall z(\mathcal{F}(\overline{\mathsf{m}}, z) \to z = \overline{\mathsf{b}})] = \mathsf{S}$; so $\mathsf{I}_\mathsf{h}[\forall z(\mathcal{F}(\overline{\mathsf{m}}, z) \to z = \overline{\mathsf{b}})] = \mathsf{S}$; so by SF($\forall$), $\mathsf{I}_{\mathsf{h}(z|\mathsf{a})}[\mathcal{F}(\overline{\mathsf{m}}, z) \to z = \overline{\mathsf{b}}] = \mathsf{S}$; so since $\mathsf{I}_\mathsf{h}[\overline{\mathsf{a}}] = \mathsf{a}$, by T10.2, $\mathsf{I}_\mathsf{h}[\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}}) \to \overline{\mathsf{a}} = \overline{\mathsf{b}}] = \mathsf{S}$; so by SF($\to$), $\mathsf{I}_\mathsf{h}[\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] \neq \mathsf{S}$ or $\mathsf{I}_\mathsf{h}[\overline{\mathsf{a}} = \overline{\mathsf{b}}] = \mathsf{S}$; so $\mathsf{I}_\mathsf{h}[\overline{\mathsf{a}} = \overline{\mathsf{b}}] = \mathsf{S}$; but $\mathsf{I}_\mathsf{h}[\overline{\mathsf{a}}] = \mathsf{a}$ and $\mathsf{I}_\mathsf{h}[\overline{\mathsf{b}}] = \mathsf{b}$; so by SF(r), $\langle \mathsf{a}, \mathsf{b}\rangle \in \mathsf{I}[=]$; so $\langle \mathsf{a}, \mathsf{b}\rangle \in \textsc{eq}$. This is impossible; reject the assumption: If $\mathsf{f}(\mathsf{x})$ is expressed by $\mathcal{F}(x, y)$ and $\langle \mathsf{m}, \mathsf{a}\rangle \notin \mathsf{f}$, then $\mathsf{I}[\sim\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] = \mathsf{T}$.

So if both $\langle \mathsf{m}, \mathsf{a}\rangle \notin \mathsf{f}$ and $\mathsf{I}[\sim\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] \neq \mathsf{T}$, with condition EXf(i), we end up with an assignment where both $\mathsf{I}_\mathsf{h}[\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] = \mathsf{S}$ and $\mathsf{I}_\mathsf{h}[\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{b}})] = \mathsf{S}$. But this violates the uniqueness constraint EXf(ii). So if $\langle \mathsf{m}, \mathsf{a}\rangle \notin \mathsf{f}$ then $\mathsf{I}[\sim\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] = \mathsf{T}$. So this gives us the same kind of constraint for functions as for relations.

E12.4. Provide semantic arguments to prove both parts of T12.1. So, for the first part assume that $\mathsf{I}[\mathcal{R}(x_1 \dots x_n)] = \textsc{r}(\mathsf{x}_1 \dots \mathsf{x}_\mathsf{n})$. Then show (i) if $\langle \mathsf{m}_1 \dots \mathsf{m}_\mathsf{n}\rangle \in \textsc{r}$ then $\mathsf{I}[\mathcal{R}(\overline{\mathsf{m}}_1 \dots \overline{\mathsf{m}}_\mathsf{n})] = \mathsf{T}$; and (ii) if $\langle \mathsf{m}_1 \dots \mathsf{m}_\mathsf{n}\rangle \notin \textsc{r}$ then $\mathsf{I}[\sim\mathcal{R}(\overline{\mathsf{m}}_1 \dots \overline{\mathsf{m}}_\mathsf{n})] = \mathsf{T}$. And similarly for the second part based on EXf, where you may treat $\langle\langle \mathsf{m}_1 \dots \mathsf{m}_\mathsf{n}\rangle, \mathsf{a}\rangle$ as the same object as $\langle \mathsf{m}_1 \dots \mathsf{m}_\mathsf{n}, \mathsf{a}\rangle$.

12.2.2 Core Result

So far, on interpretation N, we have been able to express the relation eq, and the functions, suc, plus, and times. But our aim is to show that, on the standard interpretation N of $\mathcal{L}_{NT}$, every recursive function $\mathsf{f}(\vec{\mathsf{x}})$ is expressed by some formula $\mathcal{F}(\vec{x}, v)$.

But it is not obvious that this can be done. At least some functions must remain inexpressible in any language that has a countable vocabulary, and so in $\mathcal{L}_{NT}$. We shall see a concrete example later in the chapter. For now, consider a straightforward diagonal argument. By reasoning as from T10.7 (p. 478) there is an enumeration of all the formulas in a countable language. Isolate just formulas $\mathscr{P}_0, \mathscr{P}_1, \mathscr{P}_2\ldots$ that express functions of one variable, and consider the functions $\mathsf{f}_0(\mathsf{x})$, $\mathsf{f}_1(\mathsf{x})$, $\mathsf{f}_2(\mathsf{x})\ldots$ so expressed. These are all the expressible functions of one variable. Consider a grid with the functions listed down the left-hand column, and their values for each integer from left-to-right.

	0	1	2	...
$\mathsf{f}_0(\mathsf{x})$	$\mathbf{f_0(0)}$	$\mathsf{f}_0(1)$	$\mathsf{f}_0(2)$	
$\mathsf{f}_1(\mathsf{x})$	$\mathsf{f}_1(0)$	$\mathbf{f_1(1)}$	$\mathsf{f}_1(2)$	
$\mathsf{f}_2(\mathsf{x})$	$\mathsf{f}_2(0)$	$\mathsf{f}_2(1)$	$\mathbf{f_2(2)}$	
$\vdots$				

Moving along the diagonal, consider a function $\mathsf{f}_d(\mathsf{x})$ such that for any n, $\mathsf{f}_d(\mathsf{n}) = \mathsf{f}_n(\mathsf{n}) + 1$. So $\mathsf{f}_d(\mathsf{x})$ is $\{\langle 0, \mathsf{f}_0(0)+1\rangle, \langle 1, \mathsf{f}_1(1)+1\rangle, \langle 2, \mathsf{f}_2(2)+1\rangle, \ldots\}$. So for any integer n, this function finds the value of f_n along the diagonal, and adds one. But $\mathsf{f}_d(\mathsf{x})$ cannot be any of the expressible functions. It differs from $\mathsf{f}_0(\mathsf{x})$ insofar as $\mathsf{f}_d(0) \neq \mathsf{f}_0(0)$; it differs from $\mathsf{f}_1(\mathsf{x})$ insofar as $\mathsf{f}_d(1) \neq \mathsf{f}_1(1)$; and so forth. So $\mathsf{f}_d(\mathsf{x})$ is an inexpressible function. Though it has a unique output for every input value, there is no finite formula sufficient to express it.

We have already seen that $\mathsf{plus}(\mathsf{x}, \mathsf{y})$ and $\mathsf{times}(\mathsf{x}, \mathsf{y})$ are expressible in $\mathscr{L}_{NT}$. But there is no obvious mechanism in $\mathscr{L}_{NT}$ to express, say, $\mathsf{fact}(\mathsf{x})$. Given that not all functions are expressible, it is a significant matter, then, to see that all the recursive functions are expressible with interpretation N in $\mathscr{L}_{NT}$. Our main argument shall be an induction on the sequence of recursive functions. For one key case, we defer discussion into the next section.

T12.3. On the standard interpretation N of $\mathscr{L}_{NT}$, each recursive function $\mathsf{f}(\vec{\mathsf{x}})$ is expressed by some formula $\mathscr{F}(\vec{x}, v)$.

For any recursive function f_a there is a sequence of functions $\mathsf{f}_0, \mathsf{f}_1 \ldots \mathsf{f}_a$ such that each member is an initial function or arises from previous members by composition, recursion or regular minimization. By induction on functions in this sequence.

Basis: f_0 is an initial function $\mathsf{suc}(\mathsf{x})$, $\mathsf{zero}(\mathsf{x})$, or $\mathsf{idnt}^j_k(\mathsf{x}_1 \ldots \mathsf{x}_j)$.

(s) f_0 is $\mathsf{suc}(\mathsf{x})$. Then by T12.1, f_0 is expressed by $\mathscr{F}(x, v) =_{def} Sx = v$.

(z) f_0 is $\mathsf{zero}(\mathsf{x})$. Then f_0 is expressed by $\mathscr{F}(x, v) =_{def} x = x \wedge v = \emptyset$. Suppose $\langle \mathsf{m}, \mathsf{a}\rangle \in \mathsf{zero}$. Then since a is zero, $\mathsf{N}[\overline{\mathsf{m}} = \overline{\mathsf{m}} \wedge \overline{\mathsf{a}} = \emptyset] = \mathsf{T}$.

And any z that is zero is equal to a — so that $\mathsf{N}[\forall z(\overline{\mathsf{m}} = \overline{\mathsf{m}} \wedge z = \emptyset \to z = \overline{\mathsf{a}})] = \mathsf{T}$.

(i) $\mathsf{f_0}$ is $\mathsf{idnt}^{\mathsf{j}}_{\mathsf{k}}(\mathsf{x_1} \ldots \mathsf{x_j})$. Then $\mathsf{f_0}$ is expressed by $\mathcal{F}(x_1 \ldots x_j, v) =_{\text{def}} (x_1 = x_1 \wedge \ldots \wedge x_j = x_j) \wedge x_k = v$.[5] Suppose $\langle\langle \mathsf{m_1} \ldots \mathsf{m_j}\rangle, \mathsf{a}\rangle \in \mathsf{idnt}^{\mathsf{j}}_{\mathsf{k}}$. Then since $\mathsf{a} = \mathsf{m_k}$, $\mathsf{N}[(\overline{\mathsf{m}}_1 = \overline{\mathsf{m}}_1 \wedge \ldots \wedge \overline{\mathsf{m}}_{\mathsf{j}} = \overline{\mathsf{m}}_{\mathsf{j}}) \wedge \overline{\mathsf{m}}_{\mathsf{k}} = \overline{\mathsf{a}}] = \mathsf{T}$. And any $z = \mathsf{m_k}$ is equal to a — so that $\mathsf{N}[\forall z((\overline{\mathsf{m}}_1 = \overline{\mathsf{m}}_1 \wedge \ldots \wedge \overline{\mathsf{m}}_{\mathsf{j}} = \overline{\mathsf{m}}_{\mathsf{j}} \wedge \overline{\mathsf{m}}_{\mathsf{k}} = z) \to z = \overline{\mathsf{a}})] = \mathsf{T}$.

Assp: For any i, $0 \le i < k$, $\mathsf{f_i}(\vec{\mathsf{x}})$ is expressed by some $\mathcal{F}(\vec{x}, v)$

Show: $\mathsf{f_k}(\mathsf{x})$ is expressed by some $\mathcal{F}(\vec{x}, v)$.

$\mathsf{f_k}$ is either an initial function or arises from previous members by composition, recursion or regular minimization. If it is an initial function then as in the basis. So suppose $\mathsf{f_k}$ arises from previous members.

(c) $\mathsf{f_k}(\vec{\mathsf{x}}, \vec{\mathsf{y}}, \vec{\mathsf{z}})$ arises by composition from $\mathsf{g}(\vec{\mathsf{y}})$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{w}, \vec{\mathsf{z}})$. By assumption $\mathsf{g}(\vec{\mathsf{y}})$ is expressed by some $\mathcal{G}(\vec{y}, w)$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{w}, \vec{\mathsf{z}})$ by $\mathcal{H}(\vec{x}, w, \vec{z}, v)$; then their composition $\mathsf{f}(\vec{\mathsf{x}}, \vec{\mathsf{y}}, \vec{\mathsf{z}})$ is expressed by $\mathcal{F}(\vec{x}, \vec{y}, \vec{z}, v) =_{\text{def}} \exists w[\mathcal{G}(\vec{y}, w) \wedge \mathcal{H}(\vec{x}, w, \vec{z}, v)]$. For simplicity, consider a case where $\vec{\mathsf{x}}$ and $\vec{\mathsf{z}}$ drop out and $\vec{\mathsf{y}}$ is a single variable y; so $\mathcal{F}(y, v) =_{\text{def}} \exists w[\mathcal{G}(y, w) \wedge \mathcal{H}(w, v)]$. Suppose $\langle \mathsf{m}, \mathsf{a}\rangle \in \mathsf{f_k}$; then by composition there is some b such that $\langle \mathsf{m}, \mathsf{b}\rangle \in \mathsf{g}$ and $\langle \mathsf{b}, \mathsf{a}\rangle \in \mathsf{h}$. Because $\mathcal{G}$ and $\mathcal{H}$ express g and h, $\mathsf{N}[\mathcal{G}(\overline{\mathsf{m}}, \overline{\mathsf{b}})] = \mathsf{T}$ and $\mathsf{N}[\mathcal{H}(\overline{\mathsf{b}}, \overline{\mathsf{a}})] = \mathsf{T}$; so $\mathsf{N}[\mathcal{G}(\overline{\mathsf{m}}, \overline{\mathsf{b}}) \wedge \mathcal{H}(\overline{\mathsf{b}}, \overline{\mathsf{a}})] = \mathsf{T}$, and $\mathsf{N}[\exists w(\mathcal{G}(\overline{\mathsf{m}}, w) \wedge \mathcal{H}(w, \overline{\mathsf{a}}))] = \mathsf{T}$. Further, by expression, $\mathsf{N}[\forall z(\mathcal{G}(\overline{\mathsf{m}}, z) \to z = \overline{\mathsf{b}})] = \mathsf{T}$ and $\mathsf{N}[\forall z(\mathcal{H}(\overline{\mathsf{b}}, z) \to z = \overline{\mathsf{a}})] = \mathsf{T}$; so that for a given m, there is just one $w = \mathsf{b}$ and so one $z = \mathsf{a}$ to satisfy $\mathcal{G}(\overline{\mathsf{m}}, w) \wedge \mathcal{H}(w, z)$ and $\mathsf{N}[\forall z(\exists w(\mathcal{G}(\overline{\mathsf{m}}, w) \wedge \mathcal{H}(w, z)) \to z = \overline{\mathsf{a}})] = \mathsf{T}$.

(r) $\mathsf{f_k}(\vec{\mathsf{x}}, \mathsf{y})$ arises by recursion from $\mathsf{g}(\vec{\mathsf{x}})$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$. By assumption $\mathsf{g}(\vec{\mathsf{x}})$ is expressed by some $\mathcal{G}(\vec{x}, v)$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$ is expressed by $\mathcal{H}(\vec{x}, y, u, v)$. And the expression of $\mathsf{f_k}(\vec{\mathsf{x}}, \mathsf{y})$ in terms of $\mathcal{G}$ and $\mathcal{H}$ utilizes Gödel's β-function, as developed in the next section.

(m) $\mathsf{f_k}(\vec{\mathsf{x}})$ arises by regular minimization from $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$. By assumption, $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$ is expressed by some $\mathcal{G}(\vec{x}, y, z)$. Then $\mathsf{f_k}(\vec{\mathsf{x}})$ is expressed by $\mathcal{F}(\vec{x}, v) =_{\text{def}} \mathcal{G}(\vec{x}, v, \emptyset) \wedge (\forall y < v){\sim}\mathcal{G}(\vec{x}, y, \emptyset)$. Suppose $\vec{x}$ reduces to a single variable and $\langle \mathsf{m}, \mathsf{a}\rangle \in \mathsf{f}$; then $\langle\langle \mathsf{m}, \mathsf{a}\rangle, 0\rangle \in \mathsf{g}$ and for any

[5] Perhaps it will have occurred to the reader that $\mathsf{idnt}^3_2(\mathsf{x}, \mathsf{y}, \mathsf{z})$, say, is expressed by $x = x \wedge z = z \wedge y = v$ as well as $x = x \wedge y = y \wedge z = z \wedge y = v$ — where the first is relatively "efficient" insofar as it saves a conjunct. But we are after a different "efficiency" of notation and demonstration, where the formulation above serves our purposes nicely.

$\mathsf{n} < \mathsf{a}$, $\langle\langle \mathsf{m}, \mathsf{n}\rangle, 0\rangle \notin \mathsf{g}$. So because $\mathscr{G}$ expresses g, $\mathsf{N}[\mathscr{G}(\overline{\mathsf{m}}, \overline{\mathsf{a}}, \emptyset) \wedge (\forall y < \overline{\mathsf{a}})\sim\mathscr{G}(\overline{\mathsf{m}}, y, \emptyset)] = \mathsf{T}$. And the result is unique: for any $\mathsf{k} < \mathsf{a}$, $\mathsf{N}[\mathscr{G}(\overline{\mathsf{m}}, \overline{\mathsf{k}}, \emptyset)] \neq \mathsf{T}$; so when $z < \mathsf{a}$, the value of the conjunction $\mathsf{N}[\mathscr{G}(\overline{\mathsf{m}}, z, \emptyset) \wedge (\forall y < z)\sim\mathscr{G}(\overline{\mathsf{m}}, y, \emptyset)] \neq \mathsf{T}$. And since $\mathsf{N}[\mathscr{G}(\overline{\mathsf{m}}, \overline{\mathsf{a}}, \emptyset)] = \mathsf{T}$, $\mathsf{N}[\sim\mathscr{G}(\overline{\mathsf{m}}, \overline{\mathsf{a}}, \emptyset)] \neq \mathsf{T}$, and any case where $\mathsf{k} > \mathsf{a}$ has $\mathsf{N}[(\forall y < \overline{\mathsf{k}})\sim\mathscr{G}(\overline{\mathsf{m}}, y, \emptyset)] \neq \mathsf{T}$; so the conjunction $\mathsf{N}[\mathscr{G}(\overline{\mathsf{m}}, z, \emptyset) \wedge (\forall y < z)\sim\mathscr{G}(\overline{\mathsf{m}}, y, \emptyset)] \neq \mathsf{T}$. So the only case in which $\mathscr{F}(\overline{\mathsf{m}}, z) = \mathscr{G}(\overline{\mathsf{m}}, z, \emptyset) \wedge (\forall y < z)\sim\mathscr{G}(\overline{\mathsf{m}}, y, \emptyset)$ is satisfied when z is a, and $\mathsf{N}[\forall z(\mathscr{F}(\overline{\mathsf{m}}, z) \rightarrow z = \overline{\mathsf{a}})] = \mathsf{T}$.

Indct: Any recursive $\mathsf{f}(\vec{\mathsf{x}})$ is expressed by some $\mathscr{F}(\vec{x}, v)$

Some of the reasoning is merely sketched — however, the general idea should be clear. There might be formulas other than the stated $\mathscr{F}(\vec{x}, v)$ to express a recursive $\mathsf{f}(\vec{\mathsf{x}})$ — for example, if $\mathscr{F}(\vec{x}, v)$ expresses $\mathsf{f}(\vec{\mathsf{x}})$, then so does $\mathscr{F}(\vec{x}, v) \wedge \mathscr{A}$ for any logical truth $\mathscr{A}$. We shall see an important alternative in the following. Let us say that $\mathscr{F}(\vec{x}, v)$ so-described is the *original* formula by which $\mathsf{f}(\vec{\mathsf{x}})$ is expressed. It remains to fill out the case for the recursion clause. This is the task of the next section.

*E12.5. From T13.3 there is some formula to express any recursive function: the argument by induction works by showing how to *construct* a formula for each recursive function. Following the method of our induction, write down formulas to express the following recursive functions.

a. $\mathsf{suc}(\mathsf{zero}(\mathsf{x}))$

b. $\mathsf{idnt}^3_2(\mathsf{x}, \mathsf{suc}(\mathsf{zero}(\mathsf{x})), \mathsf{z})$

Hint: As setup for the compositions, give each function a different output variable, where the output to one is the input to the next.

*E12.6. Fill out semantic reasoning to demonstrate that proposed (original) formulas satisfy the conditions for expression for the (z), (i), (c) and (m) clauses to T12.3. For case (m), rather than go to the unabbreviated form for the bounded quantifier it will be fine to anticipate T12.6 to apply the (obvious) semantic clause directly. Hints: So, for example, for (c) you will apply semantic definitions to show that $\mathsf{N}[\exists w(\mathscr{G}(\overline{\mathsf{m}}, w) \wedge \mathscr{H}(w, \overline{\mathsf{a}}))] = \mathsf{T}$ and that $\mathsf{N}[\forall z(\exists w(\mathscr{G}(\overline{\mathsf{m}}, w) \wedge \mathscr{H}(w, z)) \rightarrow z = \overline{\mathsf{a}})] = \mathsf{T}$; in places you may find that T10.2 will smooth the result; and for (m) at one stage it will be helpful to observe that for any n, $\mathsf{n} < \mathsf{a} \vee \mathsf{n} = \mathsf{a} \vee \mathsf{n} > \mathsf{a}$ and reason separately for each case.

12.2.3 The β-Function

Suppose a recursive function $\mathsf{f(m,n) = a}$. Then for the given value of m, there is a sequence $\mathsf{k_0, k_1 \ldots k_n}$ with $\mathsf{k_n = a}$, such that $\mathsf{k_0}$ takes some initial value, and each of the other members is specially related to the one before. Thus, in the simple case of $\mathsf{plus(m,n)}$, if $\mathsf{m = 2}$ then $\mathsf{k_0 = 2}$, and each $\mathsf{k_i}$ is the successor of the one before. So corresponding to $\mathsf{2 + 5 = 7}$ is the sequence,

$$\mathsf{2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7}$$

whose first member is set by $\mathsf{gplus(2)}$, where subsequent members result from the one before by $\mathsf{plus(2,Sy) = hplus(2,y,plus(2,y))}$, whose last member is 7. And, generalizing, we shall be in a position to express recursive functions if we can express the existence of *sequences* of integers so defined. We shall be able to say $\mathsf{f(\overline{m},\overline{n}) = \overline{a}}$ if we can say "there is a sequence whose first member is $\mathsf{g(m)}$, with members related one to another by $\mathsf{f(m,Sy) = h(m,y,f(m,y))}$, whose $\mathsf{n^{th}}$ member is a." This is a mouthful. And $\mathscr{L}_{NT}$ is not obviously equipped to do it. In, particular, $\mathscr{L}_{NT}$ has straightforward mechanisms for asserting the existence of integers — but on its face, it is not clear how to assert the existence of the arbitrary sequences which result from the recursion clause.

But Gödel shows a way out. We have already seen an instance of the general strategy we shall require in our discussion of Gödel numbering from chapter 10 (p. 478). In that case, we took a sequence of integers (keyed to vocabulary), $g_0, g_1 \ldots g_n$ and collected them into a single Gödel number $G = 2^{g_0} \times 3^{g_1} \times \ldots \times \pi_n^{g_n}$ where 2, $3 \ldots \pi_n$ are the first n primes. By the fundamental theorem of arithmetic, any number has a unique prime factorization, so the original sequence is recovered from G by factoring to find the power of 2, the power of 3 and so forth. So the single integer G represents the original sequence. And $\mathscr{L}_{NT}$ has no problem expressing the existence of a single integer! Unfortunately, however, this particular way out is unavailable to us insofar as it involves exponentiation, and the resources of $\mathscr{L}_{NT}$ so-far include only S, $+$ and $\times$.[6]

All the same, within the resources of $\mathscr{L}_{NT}$, by the Chinese remainder theorem (whose history reaches to ancient China), there must be *pairs* of integers sufficient to represent any sequence. Consider the *remainder* function $\mathsf{rm(x,y)}$ which returns the remainder after x is divided by y. The *remainder* of x divided by y equals z just in case $\mathsf{z < y}$ and for some w, $\mathsf{x = (y \times w) + z}$. Then let,

[6] Some treatments begin with a language including exponentiation precisely in order to smooth the exposition at this stage. But our results are all the more interesting insofar as even the relatively weak $\mathscr{L}_{NT}$ retains powers sufficient for the fatal flaw.

$$\beta(\mathsf{p},\mathsf{q},\mathsf{i}) =_{\text{def}} \mathsf{rm}[\mathsf{p},\mathsf{S}(\mathsf{q}\times\mathsf{S}(\mathsf{i}))]$$

So for some fixed values of p and q the β function yields different remainders for different values of i. By the Chinese remainder theorem, for any sequence $\mathsf{k}_0, \mathsf{k}_1 \ldots \mathsf{k}_\mathsf{n}$ there are some p and q such that for $\mathsf{i} \leq \mathsf{n}$, $\beta(\mathsf{p},\mathsf{q},\mathsf{i}) = \mathsf{k}_\mathsf{i}$. So p and q together code the sequence, and the β-function returns member k_i as a function of p, q and i. Intuitively, when we divide p by $\mathsf{S}(\mathsf{q}\times\mathsf{S}(\mathsf{i}))$, for $\mathsf{i} \leq \mathsf{n}$, the result is a series of $n+1$ remainders. The theorem tells us that *any* series $\mathsf{k}_0, \mathsf{k}_1 \ldots \mathsf{k}_\mathsf{n}$ may be so represented (see the beta function reference).

Here is a simple example. Suppose k_0, k_1 and k_2 are $5, 2, 3$. So the last subscript in the series $\mathsf{n} = 2$. As developed in the beta function reference, the proof of the remainder theorem asks us first to find $\mathsf{s} = \mathsf{max}(\mathsf{n}, 5, 2, 3) = 5$, and then to set $\mathsf{q} = \mathsf{s}! = 120$. So $\beta(\mathsf{p},\mathsf{q},\mathsf{i}) = \mathsf{rm}[\mathsf{p},\mathsf{S}(120\times\mathsf{S}(\mathsf{i}))]$. So as i ranges between 0 and $\mathsf{n} = 2$, we are looking at,

$$\mathsf{rm}(\mathsf{p},121) \qquad \mathsf{rm}(\mathsf{p},241) \qquad \mathsf{rm}(\mathsf{p},361)$$

But 121, 241 and 361 so constructed must have no common factor other than 1; and the remainder theorem then tells us that as p varies between 0 and $121\times241\times361 - 1 = 10527120$ the remainders take on every possible sequence of remainder values. But the remainders will be values up to 120, 240 and 360, which is to say, $\mathsf{q} = \mathsf{s}!$ is large enough that our simple sequence must therefore appear among the sequences of remainders. In this case, $\mathsf{p} = 5219340$ gives $\mathsf{rm}(\mathsf{p},121) = 5$, $\mathsf{rm}(\mathsf{p},241) = 3$ and $\mathsf{rm}(\mathsf{p},361) = 2$. There may be easier ways to generate this sequence. But there is no shortage of integers (!) so there are no worries about using large ones, and by this method Gödel gives a perfectly general way to represent the arbitrary finite sequence.

And we can express the β-function with the resources of $\mathscr{L}_{\text{NT}}$. Thus, for $\beta(\mathsf{p},\mathsf{q},\mathsf{i})$,

$$\mathcal{B}(p,q,i,v) =_{\text{def}} (\exists w \leq p)[p = (S(q\times Si)\times w) + v \wedge v < S(q\times Si)]$$

So v is the remainder after p is divided by $S(q\times Si)$. And for appropriate choice of p and q, the variable v takes on the values k_0 through k_n as i runs through the values $\emptyset$ to n.

Now return to our claim that when a recursive function $\mathsf{f}(\mathsf{m},\mathsf{n}) = \mathsf{a}$ there is a sequence $\mathsf{k}_0, \mathsf{k}_1 \ldots \mathsf{k}_\mathsf{n}$ with $\mathsf{k}_\mathsf{n} = \mathsf{a}$ such that k_0 takes some initial value, and each of the other members is related to the one before according to some other recursive function. More officially, a function $\mathsf{f}(\vec{\mathsf{x}},\mathsf{y}) = \mathsf{z}$ just in case there is a sequence $\mathsf{k}_0, \mathsf{k}_1 \ldots \mathsf{k}_\mathsf{y}$ with,

Arithmetic for the *Beta* Function

Say $\mathsf{rm}(c,d)$ is the remainder of c/d. For a sequence, d_0, $d_1 \ldots d_n$, let $|D|$ be the product $d_0 \times d_1 \times \ldots \times d_n$. We say d_0, $d_1 \ldots d_n$ are *relatively prime* if no two members have a common factor other than 1. Then,

I. For any relatively prime sequence $d_0, d_1 \ldots d_n$, the sequences of remainders $\mathsf{rm}(c,d_0), \mathsf{rm}(c,d_1)\ldots\mathsf{rm}(c,d_n)$ as c runs from 0 to $|D|-1$ are all different from each other.

   Suppose otherwise. Then there are c_1 and c_2, $0 \leq c_1 < c_2 < |D|$ such that $\mathsf{rm}(c_1,d_0), \mathsf{rm}(c_1,d_1)\ldots\mathsf{rm}(c_1,d_n)$ is the same as $\mathsf{rm}(c_2,d_0)$, $\mathsf{rm}(c_2,d_1)\ldots\mathsf{rm}(c_2,d_n)$. So for each d_i, $\mathsf{rm}(c_1,d_i) = \mathsf{rm}(c_2,d_i)$; say $c_1 = ad_i + r$ and $c_2 = bd_i + r$; then since the remainders are equal, $c_2 - c_1 = bd_i - ad_i$; so each d_i divides $c_1 - c_2$ evenly. So each d_i collects a distinct set of prime factors of $c_2 - c_1$; and since $c_2 - c_1$ is divided by any product of its primes, $c_2 - c_1$ is divided by $|D|$. So $|D| \leq c_2 - c_1$. But $0 \leq c_1 < c_2 < |D|$ so $c_2 - c_1 < |D|$. Reject the assumption: The sequences of remainders as c runs from 0 to $|D|-1$ are distinct.

II. The sequences of remainders $\mathsf{rm}(c,d_0), \mathsf{rm}(c,d_1)\ldots\mathsf{rm}(c,d_n)$ as c runs from 0 to $|D|-1$ are all the possible sequences of remainders.

   There are d_i possible remainders a number might have when divided by d_i, $(0, 1, \ldots d_i - 1)$. But if $\mathsf{rm}(c,d_0)$ takes d_0 possible values, $\mathsf{rm}(c,d_1)$ may take its d_1 values for each value of $\mathsf{rm}(c,d_0)$; etc. So the there are $|D|$ possible sequences of remainders. But as c runs from 0 to $|D|-1$, by (I), there are $|D|$ different sequences. So there are all the possible sequences.

III. Let s be the maximum of $n, k_0, k_1 \ldots k_n$. Then for $0 \leq i < n$, the numbers $d_i = s!(i+1)+1$ are each greater than any k_j and are relatively prime.

   Since s is the the maximum of $n, k_0, k_1 \ldots k_n$, the first is obvious. To see that the d_i are relatively prime, suppose otherwise. Then for some j, k, $1 \leq j < k \leq n+1$, $s!j+1$ and $s!k+1$ have a common factor p. But any number up to s leaves remainder 1 when dividing $s!j+1$; so $p > s$. And since p divides $s!j+1$ and $s!k+1$ it divides their difference, $s!(k-j)$; but if p divides $s!$, then it does not evenly divide $s!j+1$; so p does not divide $s!$; so p divides $k-j$. But $1 \leq j < k \leq n+1$; so $k-j \leq n$; so $p \leq n$; so $p \leq s$. Reject the assumption: the d_i are relatively prime.

IV. For any $k_0, k_1 \ldots k_n$, we can find a pair of numbers p, q such that for $i \leq n$, $\beta(p,q,i) = k_i$.

   With s as above, set $q = s!$, and let $\beta(p,q,i) = \mathsf{rm}(p, q(i+1)+1)$. By (III), for $0 \leq i \leq n$ the numbers $q_i = q(i+1)+1$ are relatively prime. So by (II), there are all the possible sequences of remainders as p ranges from 0 to $|D|-1$. And since by (III) each of the q_i is greater than any k_i, the sequence $k_0, k_1 \ldots k_n$ is among the possible sequences of remainders. So there is some p such that the k_i are $\mathsf{rm}(p, q(i+1)+1)$.

(i) $\mathsf{k}_0 = \mathsf{g}(\vec{\mathsf{x}})$

(ii) if $\mathsf{i} < \mathsf{y}$, then $\mathsf{k}_{\mathsf{Si}} = \mathsf{h}(\vec{\mathsf{x}}, \mathsf{i}, \mathsf{k}_\mathsf{i})$

(iii) $\mathsf{k}_\mathsf{y} = \mathsf{z}$

Put in terms of the β-function, this requires, $\mathsf{f}(\vec{\mathsf{x}}, \mathsf{y}) = \mathsf{z}$ just in case there are some p, q such that,

(i) $\beta(\mathsf{p}, \mathsf{q}, 0) = \mathsf{g}(\vec{\mathsf{x}})$

(ii) if $\mathsf{i} < \mathsf{y}$, then $\beta(\mathsf{p}, \mathsf{q}, \mathsf{Si}) = \mathsf{h}(\vec{\mathsf{x}}, \mathsf{i}, \beta(\mathsf{p}, \mathsf{q}, \mathsf{i}))$

(iii) $\beta(\mathsf{p}, \mathsf{q}, \mathsf{y}) = \mathsf{z}$

By assumption, $\mathsf{g}(\vec{\mathsf{x}})$ is expressed by some $\mathscr{G}(\vec{x}, v)$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$ by some $\mathscr{H}(\vec{x}, y, u, v)$. So we can express the combination of these conditions as follows. $\mathsf{f}(\vec{\mathsf{x}}, \mathsf{y})$ is expressed by $\mathscr{F}(\vec{x}, y, z) =_{\text{def}}$

$$\exists p \exists q\{\exists v[\mathscr{B}(p, q, \emptyset, v) \wedge \mathscr{G}(\vec{x}, v)] \wedge$$

$$(\forall i < y)\exists u \exists v[\mathscr{B}(p, q, i, u) \wedge \mathscr{B}(p, q, Si, v) \wedge \mathscr{H}(\vec{x}, i, u, v)] \wedge$$

$$\mathscr{B}(p, q, y, z)\}$$

So $\mathscr{G}$ is satisfied by the first member; then for any $i < y$, $\mathscr{H}$ is satisfied by the i^{th} member and and its successor; and the y^{th} member of the series is z.

In the case of factorial, we have $\mathscr{G}(v) =_{\text{def}} (v = S\emptyset)$ and $\mathscr{H}(y, u, v) =_{\text{def}} (v = Sy \times u)$. So the factorial function is expressed by $\mathscr{F}(y, z) =_{\text{def}}$

$$\exists p \exists q\{\exists v[\mathscr{B}(p, q, \emptyset, v) \wedge v = S\emptyset] \wedge$$

$$(\forall i < y)\exists u \exists v[\mathscr{B}(p, q, i, u) \wedge \mathscr{B}(p, q, Si, v) \wedge v = Si \times u] \wedge$$

$$\mathscr{B}(p, q, y, z)\}$$

This expression is long — particularly if expanded to unabbreviate the β-function, but it is just right. If $\langle \mathsf{n}, \mathsf{a} \rangle \in \mathsf{fac}$, then $\mathsf{N}[\mathscr{F}(\overline{\mathsf{n}}, \overline{\mathsf{a}})] = \mathsf{T}$ and the expression satisfies uniqueness as well. And similarly in the general case. So with $\mathscr{L}_{\text{NT}}$ we satisfy the recursive clause for T12.3. So its demonstration is complete, and $\mathscr{L}_{\text{NT}}$ has the resources to express any recursive function.

E12.7. Suppose k_0, k_1, k_2 and k_3 are $3, 4, 0, 2$. By the method of the text, find values of p and q so that $\beta(\mathsf{i}) = \mathsf{k}_\mathsf{i}$. Use your values of p and q to calculate $\beta(\mathsf{p}, \mathsf{q}, 0)$, $\beta(\mathsf{p}, \mathsf{q}, 1)$, $\beta(\mathsf{p}, \mathsf{q}, 2)$ and $\beta(\mathsf{p}, \mathsf{q}, 3)$. You will need some programmable device to search for the value of p. In Ruby, a routine along the following lines, with numerical values for a, b, c and d should suffice.

```
def loop
  p = 0
  until p % a == 3 and p % b == 4 and p % c == 0 and p % d == 2
    p = p+1
    puts "p = #{p}"
  end
  return p
end
puts "p = #{loop}"
```

In Ruby `x % y` returns the remainder of x divided by y. So, for this routine, you insert the denominators and then search (by brute force) for the value of p that returns the right remainders. Be prepared for it to take a while!

E12.8. Produce a formula to show that $\mathscr{L}_{NT}$ expresses the plus function by the initial functions with the beta function. You need not reduce the beta form to its primitive expression!

E12.9. Say a function f_k is *simple* iff there is a series of functions $\mathsf{f}_0, \mathsf{f}_1 \ldots \mathsf{f}_\mathsf{k}$ such that for any $\mathsf{i} \leq \mathsf{k}$,

(b) f_0 is $\mathsf{plus}(\mathsf{x}, \mathsf{y})$

(r) There are $\mathsf{a}, \mathsf{b} < \mathsf{i}$ such that $\mathsf{f}_\mathsf{i}(\vec{\mathsf{x}}, \vec{\mathsf{y}})$ is $\mathsf{plus}(\mathsf{f}_\mathsf{a}(\vec{\mathsf{x}}), \mathsf{f}_\mathsf{b}(\vec{\mathsf{y}}))$

Show that on the standard interpretation N of $\mathscr{L}_{NT}$ each simple $\mathsf{f}(\vec{\mathsf{x}})$ is expressed by some formula $\mathscr{F}(\vec{x}, v)$. You may appeal to T10.2 as appropriate — and your reasoning may have the "quick" character of T12.3. Hint: (r) yields functions by a sort of "double" composition.

12.3 Capturing Recursive Functions

The second of the powers to be associated with theory incompleteness has to do with the theory's *proof* system. In section 12.5 we shall be able to show that if a theory is consistent and *captures* recursive functions, then it is negation incomplete. In this section, we show that Q, and so any theory that includes Q, captures the recursive functions.

12.3.1 Definition and Basic Results

Where expression requires that if objects stand in a given relation, then a corresponding formula be true, capture requires that when objects stand in a relation, a corresponding formula be *provable* in the theory.

CP For any language $\mathscr{L}$, interpretation I, objects $\mathsf{m}_1 \ldots \mathsf{m}_n, \mathsf{a} \in \mathsf{U}$ and theory T,

(r) Relation $\mathsf{R}(\mathsf{x}_1 \ldots \mathsf{x}_n)$ is *captured* by formula $\mathscr{R}(x_1 \ldots x_n, y)$ in T just in case,

(i) If $\langle \mathsf{m}_1 \ldots \mathsf{m}_n \rangle \in \mathsf{R}$ then $T \vdash \mathscr{R}(\overline{\mathsf{m}}_1 \ldots \overline{\mathsf{m}}_n)$

(ii) If $\langle \mathsf{m}_1 \ldots \mathsf{m}_n \rangle \notin \mathsf{R}$ then $T \vdash \sim\mathscr{R}(\overline{\mathsf{m}}_1 \ldots \overline{\mathsf{m}}_n)$

(f) Function $\mathsf{f}(\mathsf{x}_1 \ldots \mathsf{x}_n)$ is *captured* by formula $\mathscr{F}(x_1 \ldots x_n, y)$ in T just in case,

if $\langle\langle \mathsf{m}_1 \ldots \mathsf{m}_n \rangle, \mathsf{a} \rangle \in \mathsf{f}$ then

(i) $T \vdash \mathscr{F}(\overline{\mathsf{m}}_1 \ldots \overline{\mathsf{m}}_n, \overline{\mathsf{a}})$

(ii) $T \vdash \forall z(\mathscr{F}(\overline{\mathsf{m}}_1 \ldots \overline{\mathsf{m}}_n, z) \rightarrow z = \overline{\mathsf{a}})$

As a first result, and to see how these definitions work, it is easy to see that in a theory at least as strong as Q, conditions (f.i) and (f.ii) combine to yield a result like (r.ii).

T12.4. If T includes Q and total function $\mathsf{f}(\mathsf{x}_1 \ldots \mathsf{x}_n)$ is captured by formula $\mathscr{F}(x_1 \ldots x_n, y)$ so that conditions (f.i) and (f.ii) hold, then if $\langle\langle \mathsf{m}_1 \ldots \mathsf{m}_n \rangle, \mathsf{a} \rangle \notin \mathsf{f}$ then $T \vdash \sim\mathscr{F}(\overline{\mathsf{m}}_1 \ldots \overline{\mathsf{m}}_n, \overline{\mathsf{a}})$.

Suppose $\mathsf{f}(\mathsf{x}_1 \ldots \mathsf{x}_n)$ is captured by $\mathscr{F}(x_1 \ldots x_n, y)$ and $\langle\langle \mathsf{m}_1 \ldots \mathsf{m}_n \rangle, \mathsf{a} \rangle \notin \mathsf{f}$. Then, since f is total, there is some $\mathsf{b} \neq \mathsf{a}$ such that $\langle\langle \mathsf{m}_1 \ldots \mathsf{m}_n \rangle, \mathsf{b} \rangle \in \mathsf{f}$; so by (f.i), $T \vdash \mathscr{F}(\overline{\mathsf{m}}_1 \ldots \overline{\mathsf{m}}_n, \overline{\mathsf{b}})$; and instantiating (f.ii) to $\overline{\mathsf{a}}$, $T \vdash \mathscr{F}(\overline{\mathsf{m}}_1 \ldots \overline{\mathsf{m}}_n, \overline{\mathsf{a}}) \rightarrow \overline{\mathsf{a}} = \overline{\mathsf{b}}$. But since $\mathsf{a} \neq \mathsf{b}$, and T includes Q, by T8.14, $T \vdash \overline{\mathsf{a}} \neq \overline{\mathsf{b}}$; so by MT, $T \vdash \sim\mathscr{F}(\overline{\mathsf{m}}_1 \ldots \overline{\mathsf{m}}_n, \overline{\mathsf{a}})$.

Our aim is to show that recursive functions are captured in Q. In chapter 8, we showed that Q correctly decides atomic sentences of $\mathscr{L}_{NT}$. As a preliminary to showing that Q captures the recursive functions, in this section we extend that result to show that Q correctly decides a broadened range of sentences.

To understand the result to which we build in this section, we need to identify some important subclasses of formulas in $\mathscr{L}_{NT}$: the Δ_0, Σ_1 and Π_1 formulas.

Δ_0 (b) If $\mathcal{P}$ is of the form $s = t$, $s < t$ or $s \leq t$ for terms s and t, then $\mathcal{P}$ is a Δ_0 formula.

(s) If $\mathcal{P}$ and $\mathcal{Q}$ are Δ_0 formulas, then so are $\sim\mathcal{P}$, and $(\mathcal{P} \rightarrow \mathcal{Q})$.

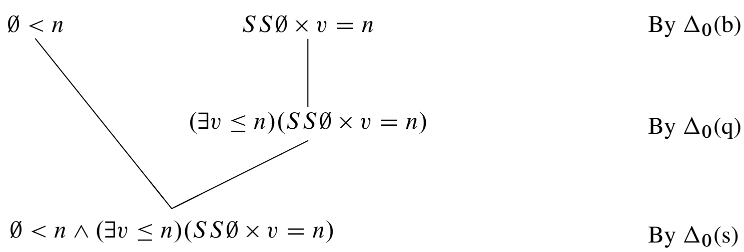
(q) If $\mathcal{P}$ is a Δ_0 formula, then so are $(\forall x \leq t)\mathcal{P}$ and $(\forall x < t)\mathcal{P}$ where x does not appear in t.

(c) Nothing else is a Δ_0 formula.

Σ_1 A formula is *strictly* Σ_1 iff it is of the form $\exists x_1 \exists x_2 \ldots \exists x_n \mathcal{P}$ for Δ_0 $\mathcal{P}$. A formula is Σ_1 iff it is equivalent to a strictly Σ_1 formula.

Π_1 A formula is *strictly* Π_1 iff it is of the form $\forall x_1 \forall x_2 \ldots \forall x_n \mathcal{P}$ for Δ_0 $\mathcal{P}$. A formula is Π_1 iff it is equivalent to a strictly Π_1 formula.

Given the soundness and adequacy of our derivation systems, we may understand equivalence in either the semantic or syntactical sense so that $\mathcal{P}$ and $\mathcal{Q}$ are equivalent just in case $\models \mathcal{P} \leftrightarrow \mathcal{Q}$ or $\vdash \mathcal{P} \leftrightarrow \mathcal{Q}$. A Δ_0 formula is (trivially) both Σ_1 and Π_1 insofar as it is preceeded by a block of zero unbounded quantifiers. We allow the usual abbreviations and so $\wedge$, $\vee$ and $\leftrightarrow$ and bounded existential quantifiers. So, for example, $n \neq \emptyset \wedge (\exists v \leq n)(SS\emptyset \times v = n)$ is Δ_0 by a tree that works like ones we have seen many times before.



It turns out that this formula is true just in case n is an even number other than zero. For a Δ_0 formula, all is as usual, except quantifiers are bounded. Its existential quantification,

(E) $\exists n[\emptyset < n \wedge (\exists v \leq n)(SS\emptyset \times v = n)]$

is strictly Σ_1, for it consists of an (in this case single) unbounded existential quantifier followed by a Δ_0 formula. This sentence asserts the existence of an even number other than zero. Observe that,

(F) $k = k \wedge \exists n[\emptyset < n \wedge (\exists v \leq n)(SS\emptyset \times v = n)]$

is not strictly Σ_1. For it does not have the existential quantifier attached as main operator to a Δ_0 formula. However, by standard quantifier placement rules, the unbounded existential quantifier can be pulled out to the front to form an equivalent strictly Σ_1 sentence. Because (F) is equivalent to a sentence that is strictly Σ_1, it too is Σ_1. Finally, by reasoning as for QN in ND, observe that the negation of a Σ_1 formula is not Σ_1 — rather it is Π_1, and the negation of a Π_1 formula is Σ_1.

We shall show that Q correctly decides Δ_0 sentences: if $\mathscr{P}$ is Δ_0 and $\mathsf{N}[\mathscr{P}] = \mathsf{T}$ then $\mathsf{Q} \vdash_{ND} \mathscr{P}$, and if $\mathsf{N}[\mathscr{P}] \neq \mathsf{T}$ then $\mathsf{Q} \vdash_{ND} \sim\mathscr{P}$. Further, Q *proves* true Σ_1 sentences: if $\mathscr{P}$ is Σ_1 and $\mathsf{N}[\mathscr{P}] = \mathsf{T}$, then $\mathsf{Q} \vdash_{ND} \mathscr{P}$. Observe that for a Σ_1 formula $\mathscr{P}$, if $\mathsf{N}[\mathscr{P}] \neq \mathsf{T}$, then $\mathsf{N}[\sim\mathscr{P}] = \mathsf{T}$ — but $\sim\mathscr{P}$ is not Σ_1. So, though we show Q correctly decides Δ_0 sentences and proves true Σ_1 sentences, we will not have shown that Q proves $\sim\mathscr{P}$ when $\mathsf{N}[\mathscr{P}] \neq \mathsf{T}$ and so not have shown that Q decides all Σ_1 sentences.

We begin with some preliminary theorems to set up the main result. These are not hard, but need to be wrapped up before we can attack the main problem. First some semantic theorems that work like derived clauses to SF for inequalities and bounded quantifiers. We could not obtain these in chapter 7 because they rely on theorems from chapter 8 (and since they are not inductions, they did not belong in chapter 8). However, we introduce them now in order to make progress.

T12.5. On the standard interpretation N for $\mathscr{L}_{NT}$, (i) $\mathsf{N_d}[s \leq t] = \mathsf{S}$ iff $\mathsf{N_d}[s] \leq \mathsf{N_d}[t]$, and (ii) $\mathsf{N_d}[s < t] = \mathsf{S}$ iff $\mathsf{N_d}[s] < \mathsf{N_d}[t]$.

(i) By abv $\mathsf{N_d}[s \leq \mathsf{t}] = \mathsf{S}$ iff $\mathsf{N_d}[\exists v(v + s = t)] = \mathsf{S}$, where v is not free in s or t; by SF($\exists$), iff there is some $\mathsf{m} \in \mathsf{U}$ such that $\mathsf{N_{d(v|m)}}[v + s = t] = \mathsf{S}$. But $\mathsf{d}(v|\mathsf{m})[v] = \mathsf{m}$; so by TA(v), $\mathsf{N_{d(v|m)}}[v] = \mathsf{m}$; so by TA(f), $\mathsf{N_{d(v|m)}}[v + s] = \mathsf{N}[+]\langle \mathsf{m}, \mathsf{N_{d(v|m)}}[s]\rangle = \mathsf{m} + \mathsf{N_{d(v|m)}}[s]$. So by SF(r), $\mathsf{N_{d(v|m)}}[v + s = t] = \mathsf{S}$ iff $\langle \mathsf{m} + \mathsf{N_{d(v|m)}}[s], \mathsf{N_{d(v|m)}}[t]\rangle \in \mathsf{N}[=]$; iff $\mathsf{m} + \mathsf{N_{d(v|m)}}[s] = \mathsf{N_{d(v|m)}}[t]$. But since v is not free in s or t, d and $\mathsf{d}(v|\mathsf{m})$ make the same assignments to variables free in s and t; so by T8.3, $\mathsf{N_d}[s] = \mathsf{N_{d(v|m)}}[s]$ and $\mathsf{N_d}[t] = \mathsf{N_{d(v|m)}}[t]$; so $\mathsf{m} + \mathsf{N_{d(v|m)}}[s] = \mathsf{N_{d(v|m)}}[t]$ iff $\mathsf{m} + \mathsf{N_d}[s] = \mathsf{N_d}[t]$; and there exists such an m just in case $\mathsf{N_d}[s] \leq \mathsf{N_d}[t]$. So $\mathsf{N_d}[s \leq \mathsf{t}] = \mathsf{S}$ iff $\mathsf{N_d}[s] \leq \mathsf{N_d}[t]$.

(ii) is homework.

As an immediate corollary, $\mathsf{N_d}[s \leq \mathsf{t}] \neq \mathsf{S}$ just in case $\mathsf{N_d}[s] > \mathsf{N_d}[t]$; and similarly for >.

T12.6. On the standard interpretation N for $\mathcal{L}_{NT}$, (i) $\mathsf{N_d}[(\forall x \leq t)\mathcal{P}] = \mathsf{S}$ iff for every $\mathsf{m} \leq \mathsf{N_d}[t]$, $\mathsf{N_{d(x|m)}}[\mathcal{P}] = \mathsf{S}$ and (ii), $\mathsf{N_d}[(\forall x < t)\mathcal{P}] = \mathsf{S}$ iff for every $\mathsf{m} < \mathsf{N_d}[t]$, $\mathsf{N_{d(x|m)}}[\mathcal{P}] = \mathsf{S}$.

(i) By abv $\mathsf{N_d}[(\forall x \leq t)\mathcal{P}] = \mathsf{S}$ iff $\mathsf{N_d}[\forall x(x \leq t \to \mathcal{P})] = \mathsf{S}$ where x does not appear in t; by SF($\forall$), iff for any $\mathsf{m} \in \mathsf{U}$, $\mathsf{N_{d(x|m)}}[x \leq t \to \mathcal{P}] = \mathsf{S}$; by SF($\to$), iff for any $\mathsf{m} \in \mathsf{U}$, $\mathsf{N_{d(x|m)}}[x \leq t] \neq \mathsf{S}$ or $\mathsf{N_{d(x|m)}}[\mathcal{P}] = \mathsf{S}$; which is to say, iff for any $\mathsf{m} \in \mathsf{U}$, if $\mathsf{N_{d(x|m)}}[x \leq t] = \mathsf{S}$, then $\mathsf{N_{d(x|m)}}[\mathcal{P}] = \mathsf{S}$. But $\mathsf{d}(x|\mathsf{m})[x] = \mathsf{m}$; so $\mathsf{N_{d(x|m)}}[x] = \mathsf{m}$; and since x is not free in t, d and $\mathsf{d}(x|\mathsf{m})$ agree on assignments to variables free in t; so by T8.3, $\mathsf{N_{d(x|m)}}[t] = \mathsf{N_d}[t]$; so with T12.5, $\mathsf{N_{d(x|m)}}[x \leq t] = \mathsf{S}$ iff $\mathsf{m} \leq \mathsf{N_d}[t]$; so $\mathsf{N_d}[(\forall x \leq t)\mathcal{P}] = \mathsf{S}$ iff for any m, if $\mathsf{m} \leq \mathsf{N_d}[t]$, then $\mathsf{N_{d(x|m)}}[\mathcal{P}] = \mathsf{S}$.

(ii) is homework.

T12.7. On the standard interpretation N for $\mathcal{L}_{NT}$, (i) $\mathsf{N_d}[(\exists x \leq t)\mathcal{P}] = \mathsf{S}$ iff for some $\mathsf{m} \leq \mathsf{N_d}[t]$, $\mathsf{N_{d(x|m)}}[\mathcal{P}] = \mathsf{S}$ and (ii), $\mathsf{N_d}[(\exists x < t)\mathcal{P}] = \mathsf{S}$ iff for some $\mathsf{m} < \mathsf{N_d}[t]$, $\mathsf{N_{d(x|m)}}[\mathcal{P}] = \mathsf{S}$.

Homework

We are finally ready for the results to which we have been building: First, Q correctly decides Δ_0 sentences of $\mathcal{L}_{NT}$.

T12.8. For any Δ_0 sentence $\mathcal{P}$, if $\mathsf{N}[\mathcal{P}] = \mathsf{T}$, then $\mathrm{Q} \vdash_{ND} \mathcal{P}$, and if $\mathsf{N}[\mathcal{P}] \neq \mathsf{T}$, then $\mathrm{Q} \vdash_{ND} \sim\mathcal{P}$.

By induction on the number of operators in $\mathcal{P}$.

Basis: If $\mathcal{P}$ is an an atomic Δ_0 sentence it is $t = s$, $t \leq s$ or $t < s$. So by T8.14, if $\mathsf{N}[\mathcal{P}] = \mathsf{T}$, $\mathrm{Q} \vdash_{ND} \mathcal{P}$, and if $\mathsf{N}[\mathcal{P}] \neq \mathsf{T}$, $\mathrm{Q} \vdash_{ND} \sim\mathcal{P}$.

Assp: For any $i, 0 \leq i < k$, if a Δ_0 setntence $\mathcal{P}$ has i operator symbols, then if $\mathsf{N}[\mathcal{P}] = \mathsf{T}$, $\mathrm{Q} \vdash_{ND} \mathcal{P}$ and if $\mathsf{N}[\mathcal{P}] \neq \mathsf{T}$, $\mathrm{Q} \vdash_{ND} \sim\mathcal{P}$.

Show: If a Δ_0 sentence $\mathcal{P}$ has k operator symbols, then if $\mathsf{N}[\mathcal{P}] = \mathsf{T}$, $\mathrm{Q} \vdash_{ND} \mathcal{P}$ and if $\mathsf{N}[\mathcal{P}] \neq \mathsf{T}$, $\mathrm{Q} \vdash_{ND} \sim\mathcal{P}$.

If a Δ_0 sentence $\mathcal{P}$ has k operator symbols, then it is of the form $\sim\mathcal{A}$, $\mathcal{A} \to \mathcal{B}$, $(\forall x \leq t)\mathcal{A}$ or $(\forall x < t)\mathcal{A}$ where $\mathcal{A}$, $\mathcal{B}$ have $< k$ operator symbols and x does not appear in t.

($\sim$) $\mathcal{P}$ is $\sim\mathcal{A}$. (i) Suppose $\mathsf{N}[\mathcal{P}] = \mathsf{T}$; then $\mathsf{N}[\sim\mathcal{A}] = \mathsf{T}$; so by T8.6, $\mathsf{N}[\mathcal{A}] \neq \mathsf{T}$; so by assumption, $\mathsf{Q} \vdash_{ND} \sim\mathcal{A}$; so $\mathsf{Q} \vdash_{ND} \mathcal{P}$. (ii) Suppose $\mathsf{N}[\mathcal{P}] \neq \mathsf{T}$; then $\mathsf{N}[\sim\mathcal{A}] \neq \mathsf{T}$; so by T8.6, $\mathsf{N}[\mathcal{A}] = \mathsf{T}$; so by assumption $\mathsf{Q} \vdash_{ND} \mathcal{A}$; so by DN, $\mathsf{Q} \vdash_{ND} \sim\sim\mathcal{A}$; so $\mathsf{Q} \vdash_{ND} \sim\mathcal{P}$.

($\rightarrow$) $\mathcal{P}$ is $\mathcal{A} \rightarrow \mathcal{B}$. (i) Suppose $\mathsf{N}[\mathcal{A} \rightarrow \mathcal{B}] = \mathsf{T}$; then by T8.6, $\mathsf{N}[\mathcal{A}] \neq \mathsf{T}$ or $\mathsf{N}[\mathcal{B}] = \mathsf{T}$. So by assumption, $\mathsf{Q} \vdash_{ND} \sim\mathcal{A}$ or $\mathsf{Q} \vdash_{ND} \mathcal{B}$. So by $\vee$I twice $\mathsf{Q} \vdash_{ND} \sim\mathcal{A} \vee \mathcal{B}$ or $\mathsf{Q} \vdash_{ND} \sim\mathcal{A} \vee \mathcal{B}$; so $\mathsf{Q} \vdash_{ND} \sim\mathcal{A} \vee \mathcal{B}$; so by Impl, $\mathsf{Q} \vdash_{ND} \mathcal{A} \rightarrow \mathcal{B}$. Part (ii) is homework.

($\forall \leq$) $\mathcal{P}$ is $(\forall x \leq t)\mathcal{A}(x)$. Since $\mathcal{P}$ is a sentence, x is the only variable free in $\mathcal{A}$; in particular, since x does not appear in t, t must be variable-free; so $\mathsf{N_d}[t] = \mathsf{N}[t]$ and where $\mathsf{N}[t] = \mathsf{n}$, by T8.13, $\mathsf{Q} \vdash_{ND} t = \overline{\mathsf{n}}$; so by =E, $\mathsf{Q} \vdash_{ND} \mathcal{P}$ just in case $\mathsf{Q} \vdash_{ND} (\forall x \leq \overline{\mathsf{n}})\mathcal{A}(x)$.

(i) Suppose $\mathsf{N}[\mathcal{P}] = \mathsf{T}$; then $\mathsf{N}[(\forall x \leq t)\mathcal{A}(x)] = \mathsf{T}$; so by TI, for any d, $\mathsf{N_d}[(\forall x \leq t)\mathcal{A}(x)] = \mathsf{S}$; so by T12.6, for any $\mathsf{m} \leq \mathsf{N_d}[t]$, $\mathsf{N_{d(x|m)}}[\mathcal{A}(x)] = \mathsf{S}$; so where $\mathsf{N_d}[\mathsf{t}] = \mathsf{N}[t] = \mathsf{n}$, for any $\mathsf{m} \leq \mathsf{n}$, $\mathsf{N_{d(x|m)}}[\mathcal{A}(x)] = \mathsf{S}$; but $\mathsf{N_d}[\overline{\mathsf{m}}] = \mathsf{m}$, so with T10.2, for any $\mathsf{m} \leq \mathsf{n}$, $\mathsf{N_d}[\mathcal{A}(\overline{\mathsf{m}})] = \mathsf{S}$; since x is the only variable free in $\mathcal{A}$, $\mathcal{A}(\overline{\mathsf{m}})$ is a sentence; so with T8.5, for any $\mathsf{m} \leq \mathsf{n}$, $\mathsf{N}[\mathcal{A}(\overline{\mathsf{m}})] = \mathsf{T}$; so $\mathsf{N}[\mathcal{A}(\emptyset)] = \mathsf{T}$ and $\mathsf{N}[\mathcal{A}(\overline{1})] = \mathsf{T}$ and ... and $\mathsf{N}[\mathcal{A}(\overline{\mathsf{n}})] = \mathsf{T}$; so by assumption, $\mathsf{Q} \vdash_{ND} \mathcal{A}(\emptyset)$ and $\mathsf{Q} \vdash_{ND} \mathcal{A}(\overline{1})$ and ... and $\mathsf{Q} \vdash_{ND} \mathcal{A}(\overline{\mathsf{n}})$; so by T8.21, $\mathsf{Q} \vdash_{ND} (\forall x \leq \overline{\mathsf{n}})\mathcal{A}(x)$; so with our preliminary result, $\mathsf{Q} \vdash_{ND} \mathcal{P}$.

(ii) Suppose $\mathsf{N}[\mathcal{P}] \neq \mathsf{T}$; then $\mathsf{N}[(\forall x \leq t)\mathcal{A}(x)] \neq \mathsf{T}$; so by TI, for some d, $\mathsf{N_d}[(\forall x \leq t)\mathcal{A}(x)] \neq \mathsf{S}$; so by T12.6, for some $\mathsf{m} \leq \mathsf{N_d}[t]$, $\mathsf{N_{d(x|m)}}[\mathcal{A}(x)] \neq \mathsf{S}$; so where $\mathsf{N_d}[\mathsf{t}] = \mathsf{N}[t] = \mathsf{n}$, for some $\mathsf{m} \leq \mathsf{n}$, $\mathsf{N_{d(x|m)}}[\mathcal{A}(x)] \neq \mathsf{S}$; but $\mathsf{N_d}[\overline{\mathsf{m}}] = \mathsf{m}$, so with T10.2, for some $\mathsf{m} \leq \mathsf{n}$, $\mathsf{N_d}[\mathcal{A}(\overline{\mathsf{m}})] \neq \mathsf{S}$; so by TI, for some $\mathsf{m} \leq \mathsf{n}$, $\mathsf{N}[\mathcal{A}(\overline{\mathsf{m}})] \neq \mathsf{T}$; so by assumption for some $\mathsf{m} \leq \mathsf{n}$, $\mathsf{Q} \vdash_{ND} \sim\mathcal{A}(\overline{\mathsf{m}})$; so by T8.20, $\mathsf{Q} \vdash_{ND} (\exists x \leq \overline{\mathsf{n}})\sim\mathcal{A}(x)$; so by bounded quantifier negation (BQN), $\mathsf{Q} \vdash_{ND} \sim(\forall x \leq \overline{\mathsf{n}})\mathcal{A}(x)$; so with our preliminary result, $\mathsf{Q} \vdash_{ND} \sim\mathcal{P}$.

($\forall <$) homework.

Indct: So for any Δ_0 sentence $\mathcal{P}$, if $\mathsf{N}[\mathcal{P}] = \mathsf{T}$, then $\mathsf{Q} \vdash_{ND} \mathcal{P}$, and if $\mathsf{N}[\mathcal{P}] \neq \mathsf{T}$, then $\mathsf{Q} \vdash_{ND} \sim\mathcal{P}$.

And now, Q proves true Σ_1 sentences.

T12.9. For any (strict) Σ_1 sentence $\mathcal{P}$ if $\mathsf{N}[\mathcal{P}] = \mathsf{T}$, then $\mathsf{Q} \vdash_{ND} \mathcal{P}$.

This is a simple induction on the number of unbounded existential quantifiers in $\mathscr{P}$. Hint: If $\mathscr{P}$ has no unbounded existential quantifiers, then it is Δ_0. Otherwise, if $\exists x\mathscr{P}$ is true, it will be easy to show that for some m, $\mathscr{P}(\overline{\mathsf{m}})$ is true; you can then apply your assumption, and $\exists$I.

Corollary: For any Σ_1 sentence $\mathscr{P}$, if $\mathsf{N}[\mathscr{P}] = \mathsf{T}$, then $\mathsf{Q} \vdash_{ND} \mathscr{P}$. Suppose a Σ_1 $\mathscr{P}$ is such that $\mathsf{N}[\mathscr{P}] = \mathsf{T}$; then by equivalence there is some strict Σ_1 $\mathscr{P}^*$ such that $\mathsf{N}[\mathscr{P}^*] = \mathsf{T}$; so by the main theorem, $\mathsf{Q} \vdash_{ND} \mathscr{P}^*$; and by equivalence again, $\mathsf{Q} \vdash_{ND} \mathscr{P}$.

This completes what we set out to show in this subsection. These results should seem intuitive: Q proves results about particular numbers, $1 + 1 = 2$ and the like. But Δ_0 sentences assert (potentially complex) particular facts about numbers — and we show that Q proves any Δ_0 sentence. Similarly, any Σ_1 sentence is true *because* of some particular fact about numbers; since Q proves that particular fact, it is sufficient to prove the Σ_1 sentence.

E12.10. Complete the demonstration of T12.5 - T12.7 by showing the remaining parts. These should be straightforward, given parts worked in the text.

*E12.11. (i) Complete the demonstration of T12.8 by finishing the remaining cases. You should set up the entire argument, but may appeal to the text for parts already completed, as the text appeals to homework. (ii) Show directly cases ($\exists \leq$) and ($\exists <$).

E12.12. Provide an argument to demonstrate T12.9.

12.3.2 Basic Result

We now set out to show that Q captures all the recursive functions. We begin showing that the original formulas by which we have expressed recursive functions are Σ_1. After that, we get our result in in two forms. First a straightforward basic version. However, this version gets a result slightly weaker than the one we would like. But it is easily strengthened to the final form.

First, then, an argument that the original formulas by which we have expressed recursive functions are Σ_1. This argument merely reviews the strategy from T12.3 for expression to show that each formula is equivalent to a strictly Σ_1 formula and so is Σ_1.

T12.10. The original formula by which any recursive function is expressed is Σ_1.

By induction on the sequence of recursive functions.

Basis: From T12.3, $\mathsf{suc(x)}$ is originally expressed by $Sx = v$; $\mathsf{zero(x)}$ by $x = x \wedge v = \emptyset$ and $\mathsf{idnt}^{\mathsf{j}}_{\mathsf{k}}(\mathsf{x}_1 \ldots \mathsf{x}_\mathsf{j})$ by $(x_1 = x_1 \wedge \ldots \wedge x_j = x_j) \wedge x_k = v$. These are all Δ_0, and therefore Σ_1.

Assp: For any any i, $0 \leq i < k$, the original formula $\mathcal{F}(\vec{x}, v)$ by which $\mathsf{f_i}(\vec{\mathsf{x}})$ is expressed is Σ_1

Show: The original formula $\mathcal{F}(\vec{x}, v)$ by which $\mathsf{f_k}(\vec{\mathsf{x}})$ is expressed is Σ_1

$\mathsf{f_k}$ is either an initial function or arises from previous members by composition, recursion or regular minimization. If it is an initial function, then as in the basis. So suppose $\mathsf{f_k}$ arises from previous members.

(c) $\mathsf{f_k}(\vec{\mathsf{x}}, \vec{\mathsf{y}}, \vec{\mathsf{z}})$ arises by composition from $\mathsf{g}(\vec{\mathsf{y}})$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{w}, \vec{\mathsf{z}})$. By assumption $\mathsf{g}(\vec{\mathsf{y}})$ is expressed by some Σ_1 formula equivalent to $\exists \vec{j}\mathcal{G}(\vec{y}, w)$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{w}, \vec{\mathsf{z}})$ by a Σ_1 formula equivalent to $\exists \vec{k}\mathcal{H}(\vec{x}, w, \vec{z}, v)$ where $\mathcal{G}$ and $\mathcal{H}$ are individually Δ_0. Then their original composition $\mathcal{F}(\vec{x}, \vec{y}, \vec{z}, v)$ is equivalent to $\exists w[\exists \vec{j}\mathcal{G}(\vec{y}, w) \wedge \exists \vec{k}\mathcal{H}(\vec{x}, w, \vec{z}, v)]$; and by standard quantifier placement rules, this is equivalent to $\exists w \exists \vec{j} \exists \vec{k}[\mathcal{G}(\vec{y}, w) \wedge \mathcal{H}(\vec{x}, w, \vec{z}, v)]$, where this is Σ_1.

(r) $\mathsf{f_k}(\vec{\mathsf{x}}, \mathsf{y})$ arises by recursion from $\mathsf{g}(\vec{\mathsf{x}})$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$. By assumption $\mathsf{g}(\vec{\mathsf{x}})$ is expressed by some Σ_1 formula $\exists \vec{j}\mathcal{G}(\vec{x}, v)$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$ by $\exists \vec{k}\mathcal{H}(\vec{x}, y, u, v)$. And, as before, the β-function $\mathcal{B}(p, q, i, v)$ is expressed by,

$$(\exists w \leq p)[p = (S(q \times Si) \times w) + v \wedge v < S(q \times Si)]$$

where this is Δ_0. Then the original formula $\mathcal{F}(\vec{x}, y, z)$ by which $\mathsf{f_k}(\vec{\mathsf{x}}, \mathsf{y})$ is expressed is equivalent to,

$\exists p \exists q\{\exists v[\mathcal{B}(p, q, \emptyset, v) \wedge \exists \vec{j}\mathcal{G}(\vec{x}, v)] \wedge$
$(\forall i < y)\exists u \exists v[\mathcal{B}(p, q, i, u) \wedge \mathcal{B}(p, q, Si, v) \wedge \exists \vec{k}\mathcal{H}(\vec{x}, i, u, v)] \wedge \mathcal{B}(p, q, y, z)\}$

This time, standard quantifier placement rules are not enough to identify the formula as Σ_1. We can pull the initial v and $\vec{j}$ quantifiers out. And the $\vec{k}$ quantifiers come out with the u and v quantifiers. The problem is getting these past the bounded universal i quantifier.

For this, we use a sort of trick: For a simplified case, consider $(\forall i < y)\exists v\mathcal{P}(i, v)$; this requires that for each $\mathsf{i} < \mathsf{y}$ there is at least one v

that makes $\mathscr{P}(i, v)$ true; for each $\mathsf{i} < \mathsf{y}$ consider the least such v, and let a be the greatest member of this collection. Then $(\forall i < y)(\exists v < \overline{\mathsf{a}})\mathscr{P}(i, v)$ is equivalent to the original expression — for there is an $\mathsf{i} < \mathsf{a}$ to satisfy $\mathscr{P}$ just in case there is some i to satisfy $\mathscr{P}$. And therefore, no matter what y may be, $\exists j(\forall i < y)(\exists v < j)\mathscr{P}(i, v)$ is true iff the original expression is true. So the existential quantifier comes past the bounded universal, leaving behind a bounded existential "shadow." Thus the existential u, v and $\vec{k}$ quantifiers come to the front, and the result is Σ_1.

(m) $\mathsf{f_k}(\vec{\mathsf{x}})$ arises by regular minimization from $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$. By assumption, $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$ is expressed by some $\exists\vec{j}\mathscr{G}(\vec{x}, y, z)$. Then the original expression by which $\mathsf{f_k}(\vec{\mathsf{x}})$ is expressed is equivalent to $\exists\vec{j}\mathscr{G}(\vec{x}, v, \emptyset) \wedge (\forall y < v){\sim}\exists\vec{j}\mathscr{G}(\vec{x}, y, \emptyset)$; but since $\mathscr{G}$ expresses a function, ${\sim}\exists\vec{j}\mathscr{G}(\vec{x}, y, \emptyset)$ just when $\exists z[\exists\vec{j}\mathscr{G}(\vec{x}, y, z) \wedge z \neq \emptyset]$; so the original expression is equivalent to, $\exists\vec{j}\mathscr{G}(\vec{x}, v, \emptyset) \wedge (\forall y < v)\exists z[\exists\vec{j}\mathscr{G}(\vec{x}, y, z) \wedge z \neq \emptyset]$. The first set of j quantifiers come directly to the front, and the second set, together with the z quantifier come out, as in the previous case, leaving bounded existential quantifiers behind. So the result is Σ_1.

Indct: The original formula by which any recursive function is expressed is Σ_1.

It is not proper to drag an existential quantifier out past a universal quantifier; however, it is legitimate to drag an existential past a *bounded* universal, with a bounded existential quantifier left behind as "shadow" or "witness."

Now for our main result. Here is the sense in which our result is weaker than we might like: Rather than Q, let us suppose we are in a system $\mathrm{Q_s}$, *strengthened* Q, which has (as an axiom or) a theorem *uniqueness of remainder* as follows,

$$\forall y[((\exists w \leq m)[m = Sn \times w + \overline{\mathsf{a}} \wedge \overline{\mathsf{a}} < Sn] \wedge (\exists w \leq m)[m = Sn \times w + y \wedge y < Sn]) \rightarrow \overline{\mathsf{a}} = y]$$

If $\overline{\mathsf{a}}$ is the remainder of $m/(n+1)$ and y is the remainder of $m/(n+1)$ then $\overline{\mathsf{a}} = y$. As we shall see, PA is a system of this sort (see *Def*[*rm*] in chapter 13) though, insofar as m and n are free variables rather than numerals, Q is not. Notice that m and n are free in this formulation; if they are instantiated to p and $q \times Si$ respectively, from uniqueness for remainder there immediately follows a parallel uniqueness result for the β-function.

$$\forall y[(\mathscr{B}(p, q, i, \overline{\mathsf{a}}) \wedge \mathscr{B}(p, q, i, y)) \rightarrow \overline{\mathsf{a}} = y]$$

Further, if $\langle\langle \mathsf{p}, \mathsf{q}, \mathsf{i}\rangle, \mathsf{a}\rangle \in \beta$ then since $\mathscr{B}$ expresses the β-function, $\mathsf{N}[\mathscr{B}(\overline{\mathsf{p}}, \overline{\mathsf{q}}, \overline{\mathsf{i}}, \overline{\mathsf{a}})] = \mathsf{T}$; and since $\mathscr{B}$ is Δ_0, by T12.8, Q $\vdash_{ND}$ $\mathscr{B}(\overline{\mathsf{p}}, \overline{\mathsf{q}}, \overline{\mathsf{i}}, \overline{\mathsf{a}})$. From this, with uniqueness, it is immediate that $\mathrm{Q_s} \vdash_{ND} \forall y[\mathscr{B}(\overline{\mathsf{p}}, \overline{\mathsf{q}}, \overline{\mathsf{i}}, y) \rightarrow y = \overline{\mathsf{a}}]$. So $\mathscr{B}$ *captures* β in $\mathrm{Q_s}$.

Now we are positioned to offer a perfectly straightforward argument for capture of the recursive functions in $\mathrm{Q_s}$. Again our main argument is an induction on the sequence of recursive functions. We show that $\mathrm{Q_s}$ captures the initial functions, and then that it captures functions from composition, recursion and regular minimization.

T12.11. On the standard interpretation N for $\mathscr{L}_{NT}$, any recursive function is captured in $\mathrm{Q_s}$ by the original formula by which it is expressed.

By induction on the sequence of recursive functions.

Basis: $\mathsf{f_0}$ is an initial function $\mathsf{suc(x)}$, $\mathsf{zero(x)}$, or $\mathsf{idnt}^{\mathsf{j}}_{\mathsf{k}}(\mathsf{x_1} \ldots \mathsf{x_j})$.

(s) The original formula $\mathscr{F}(x, v)$ by which $\mathsf{suc(x)}$ is expressed is $Sx = v$. Suppose $\langle \mathsf{m}, \mathsf{a}\rangle \in \mathsf{suc}$.

(i) Since $Sx = v$ expresses $\mathsf{suc(x)}$, $\mathsf{N}[S\overline{\mathsf{m}} = \overline{\mathsf{a}}] = \mathsf{T}$; so, since it is Δ_0, by T12.8, Q $\vdash_{ND}$ $S\overline{\mathsf{m}} = \overline{\mathsf{a}}$; so $\mathrm{Q_s} \vdash_{ND} \mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})$.

(ii) Reason as follows,

1.	$S\overline{\mathsf{m}} = \overline{\mathsf{a}}$	from (i)
2.	$\quad S\overline{\mathsf{m}} = j$	A (g, →I)
3.	$\quad j = \overline{\mathsf{a}}$	1,2 =E
4.	$S\overline{\mathsf{m}} = j \rightarrow j = \overline{\mathsf{a}}$	2-3 →I
5.	$\forall z(S\overline{\mathsf{m}} = z \rightarrow z = \overline{\mathsf{a}})$	4 ∀I

So $\mathrm{Q_s} \vdash_{ND} \forall z[\mathscr{F}(\overline{\mathsf{m}}, z) \rightarrow z = \overline{\mathsf{a}}]$.

(oth) It is left as homework to show that $\mathsf{zero(x)}$ is captured by $x = x \wedge v = \emptyset$ and $\mathsf{idnt}^{\mathsf{j}}_{\mathsf{k}}(\mathsf{x_1} \ldots \mathsf{x_j})$ by $(x_1 = x_1 \wedge \ldots \wedge x_j = x_j) \wedge x_k = v$.

Assp: For any i, $0 \leq i < k$, $\mathsf{f_i}(\vec{\mathsf{x}})$ is captured in $\mathrm{Q_s}$ by the original formula by which it is expressed.

Show: $\mathsf{f_k}(\vec{\mathsf{x}})$ is captured in $\mathrm{Q_s}$ by the original formula by which it is expressed.

$\mathsf{f_k}$ is either an initial function or arises from previous members by composition, recursion or regular minimization. If it is an initial function, then as in the basis. So suppose $\mathsf{f_k}$ arises from previous members.

(c) $\mathsf{f_k}(\vec{\mathsf{x}}, \vec{\mathsf{y}}, \vec{\mathsf{z}})$ arises by composition from $\mathsf{g}(\vec{\mathsf{y}})$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{w}, \vec{\mathsf{z}})$. By assumption $\mathsf{g}(\vec{\mathsf{y}})$ is captured by some $\mathscr{G}(\vec{y}, w)$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{w}, \vec{\mathsf{z}})$ by $\mathscr{H}(\vec{x}, w, \vec{z}, v)$; the original formula $\mathscr{F}(\vec{x}, \vec{y}, \vec{z}, v)$ by which the composition $\mathsf{f}(\vec{\mathsf{x}}, \vec{\mathsf{y}}, \vec{\mathsf{z}})$

is expressed is $\exists w[\mathscr{G}(\vec{y}, w) \wedge \mathscr{H}(\vec{x}, w, \vec{z}, v)]$. For simplicity, consider a case where $\vec{\mathsf{x}}$ and $\vec{\mathsf{z}}$ drop out and $\vec{\mathsf{y}}$ is a single variable y. Suppose $\langle \mathsf{m}, \mathsf{a}\rangle \in \mathsf{f_k}$; then by composition there is some b such that $\langle \mathsf{m}, \mathsf{b}\rangle \in \mathsf{g}$ and $\langle \mathsf{b}, \mathsf{a}\rangle \in \mathsf{h}$.

(i) Since $\langle \mathsf{m}, \mathsf{a}\rangle \in \mathsf{f_k}$, and $\mathscr{F}(y, v)$ expresses f, $\mathsf{N}[\mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] = \mathsf{T}$; so, since $\mathscr{F}(y, v)$ is Σ_1, by T12.9, $\mathrm{Q_s} \vdash_{ND} \mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})$.

(ii) Since $\mathscr{G}(y, w)$ captures $\mathsf{g(y)}$ and $\mathscr{H}(w, v)$ captures $\mathsf{h(w)}$, by assumption $\mathrm{Q_s} \vdash_{ND} \forall z(\mathscr{G}(\overline{\mathsf{m}}, z) \rightarrow z = \overline{\mathsf{b}})$ and $\mathrm{Q_s} \vdash_{ND} \forall z(\mathscr{H}(\overline{\mathsf{b}}, z) \rightarrow z = \overline{\mathsf{a}})$. It is then a simple derivation for you to show that $\mathrm{Q_s} \vdash_{ND} \forall z(\exists w[\mathscr{G}(\overline{\mathsf{m}}, w) \wedge \mathscr{H}(w, z)] \rightarrow z = \overline{\mathsf{a}})$.

(r) $\mathsf{f_k}(\vec{\mathsf{x}}, \mathsf{y})$ arises by recursion from $\mathsf{g}(\vec{\mathsf{x}})$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$. By assumption $\mathsf{g}(\vec{\mathsf{x}})$ is captured by some $\mathscr{G}(\vec{x}, v)$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$ by $\mathscr{H}(\vec{x}, y, u, v)$; the original formula $\mathscr{F}(\vec{x}, y, z)$ by which $\mathsf{f_k}(\vec{\mathsf{x}}, \mathsf{y})$ is expressed is,

$$\exists p \exists q\{\exists v[\mathscr{B}(p, q, \emptyset, v) \wedge \mathscr{G}(\vec{x}, v)] \wedge (\forall i < y)\exists u \exists v[\mathscr{B}(p, q, i, u) \wedge \mathscr{B}(p, q, Si, v) \wedge \mathscr{H}(\vec{x}, i, u, v)] \wedge \mathscr{B}(p, q, y, z)\}$$

Suppose $\vec{\mathsf{x}}$ reduces to a single variable and $\langle \mathsf{m}, \mathsf{n}, \mathsf{a}\rangle \in \mathsf{f_k}$. (i) Then since $\mathscr{F}(x, y, z)$ expresses f, $\mathsf{N}[\mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{n}}, \overline{\mathsf{a}})] = \mathsf{T}$; so, since $\mathscr{F}(x, y, z)$ is Σ_1, by T12.9, $\mathrm{Q_s} \vdash_{ND} \mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{n}}, \overline{\mathsf{a}})$. And (ii) by T12.12, immediately following, $\mathrm{Q_s} \vdash_{ND} \forall w[\mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{n}}, w) \rightarrow w = \overline{\mathsf{a}}]$.

(m) $\mathsf{f_k}(\vec{\mathsf{x}})$ arises by regular minimization from $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$. By assumption, $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$ is captured by some $\mathscr{G}(\vec{x}, y, z)$; the original formula by $\mathscr{F}(\vec{x}, v)$ by which $\mathsf{f_k}(\vec{\mathsf{x}})$ is expressed is $\mathscr{G}(\vec{x}, v, \emptyset) \wedge (\forall y < v) \sim \mathscr{G}(\vec{x}, y, \emptyset)$. Suppose $\vec{x}$ reduces to a single variable and $\langle \mathsf{m}, \mathsf{a}\rangle \in \mathsf{f_k}$.

(i) Since $\langle \mathsf{m}, \mathsf{a}\rangle \in \mathsf{f_k}$, and $\mathscr{F}(x, v)$ expresses f, $\mathsf{N}[\mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] = \mathsf{T}$; so since $\mathscr{F}(x, v)$ is Σ_1, by T12.9, $\mathrm{Q_s} \vdash_{ND} \mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})$.

(ii) Reason as follows,

1.	$\mathscr{G}(\overline{\mathsf{m}}, \overline{\mathsf{a}}, \emptyset) \wedge (\forall y < \overline{\mathsf{a}}) \sim\mathscr{G}(\overline{\mathsf{m}}, y, \emptyset)$	from (i)
2.	$j < \overline{\mathsf{a}} \vee j = \overline{\mathsf{a}} \vee \overline{\mathsf{a}} < j$	T8.19
3.	$\quad \mathscr{G}(\overline{\mathsf{m}}, j, \emptyset) \wedge (\forall y < j) \sim\mathscr{G}(\overline{\mathsf{m}}, y, \emptyset)$	A (g, $\rightarrow$I)
4.	$\quad\quad j < \overline{\mathsf{a}}$	A (c, $\sim$I)
5.	$\quad\quad \mathscr{G}(\overline{\mathsf{m}}, j, \emptyset)$	3 $\wedge$E
6.	$\quad\quad (\forall y < \overline{\mathsf{a}}) \sim\mathscr{G}(\overline{\mathsf{m}}, y, \emptyset)$	1 $\wedge$E
7.	$\quad\quad \sim\mathscr{G}(\overline{\mathsf{m}}, j, \emptyset)$	6,4 ($\forall$E)
8.	$\quad\quad \bot$	5,7 $\bot$I
9.	$\quad j \not< \overline{\mathsf{a}}$	4-8 $\sim$I
10.	$\quad\quad \overline{\mathsf{a}} < j$	A (c, $\sim$I)
11.	$\quad\quad \mathscr{G}(\overline{\mathsf{m}}, \overline{\mathsf{a}}, \emptyset)$	1 $\wedge$E
12.	$\quad\quad (\forall y < j) \sim\mathscr{G}(\overline{\mathsf{m}}, y, \emptyset)$	3 $\wedge$E
13.	$\quad\quad \sim\mathscr{G}(\overline{\mathsf{m}}, \overline{\mathsf{a}}, \emptyset)$	12,10 ($\forall$E)
14.	$\quad\quad \bot$	11,13 $\bot$I
15.	$\quad \overline{\mathsf{a}} \not< j$	10-14 $\sim$I
16.	$\quad j = \overline{\mathsf{a}}$	2,9,15 DS
17.	$[\mathscr{G}(\overline{\mathsf{m}}, j, \emptyset) \wedge (\forall y < j) \sim\mathscr{G}(\overline{\mathsf{m}}, y, \emptyset)] \rightarrow j = \overline{\mathsf{a}}$	3-16 $\rightarrow$I
18.	$\forall z([\mathscr{G}(\overline{\mathsf{m}}, z, \emptyset) \wedge (\forall y < z) \sim\mathscr{G}(\overline{\mathsf{m}}, y, \emptyset)] \rightarrow z = \overline{\mathsf{a}})$	17 $\forall$I

So $\mathrm{Q_s} \vdash_{ND} \forall z([\mathscr{G}(\overline{\mathsf{m}}, z, \emptyset) \wedge (\forall y < z) \sim\mathscr{G}(\overline{\mathsf{m}}, y, \emptyset)] \rightarrow z = \overline{\mathsf{a}})$.

Indct: Any recursive $\mathsf{f}(\vec{\mathsf{x}})$ is captured by the original formula by which it is expressed in $\mathrm{Q_s}$.

For this argument, we simply rely on the ability of Q to prove particular truths, and so the Σ_1 sentences that express recursive functions. The uniqueness clauses are not Σ_1, so we have to show them directly. The case for recursion remains outstanding, and is addressed in the theorem immediately following.

T12.12. Suppose $\mathsf{f}(\vec{\mathsf{x}}, \mathsf{y})$ results by recursion from functions $\mathsf{g}(\vec{\mathsf{x}})$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$ where $\mathsf{g}(\vec{\mathsf{x}})$ is captured by some $\mathscr{G}(\vec{x}, v)$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$ by $\mathscr{H}(\vec{x}, y, u, v)$. Then for the original expression $\mathscr{F}(\vec{x}, y, z)$ of $\mathsf{f}(\vec{\mathsf{x}}, \mathsf{y})$, if $\langle\langle \mathsf{m}_1 \ldots \mathsf{m}_\mathsf{b}, \mathsf{n}\rangle, \mathsf{a}\rangle \in \mathsf{f}$, $\mathrm{Q_s} \vdash \forall w[\mathscr{F}(\overline{\mathsf{m}}_1 \ldots \overline{\mathsf{m}}_\mathsf{b}, \overline{\mathsf{n}}, w) \rightarrow w = \overline{\mathsf{a}}]$.

Suppose $\vec{\mathsf{x}}$ reduces to a single variable and $\langle \mathsf{m}, \mathsf{n}, \mathsf{a}\rangle \in \mathsf{f}$. When $\langle \mathsf{m}, \mathsf{n}, \mathsf{a}\rangle \in \mathsf{f}$, there are $\mathsf{k}_0 \ldots \mathsf{k}_\mathsf{n}$ such that $\mathsf{k}_\mathsf{n} = \mathsf{a}$; $\mathsf{k}_0 = \mathsf{g}(\mathsf{m})$; for $0 \leq \mathsf{i} < \mathsf{n}$, there are p, q such that $\beta(\mathsf{p}, \mathsf{q}, \mathsf{i}) = \mathsf{k}_\mathsf{i}$; $\beta(\mathsf{p}, \mathsf{q}, \mathsf{Si}) = \mathsf{k}_{\mathsf{Si}}$; and $\mathsf{h}(\mathsf{m}, \mathsf{i}, \mathsf{k}_\mathsf{i}) = \mathsf{k}_{\mathsf{Si}}$. The argument is by induction on the value of n from $\mathsf{f}(\mathsf{m}, \mathsf{n}) = \mathsf{a}$. Observe that $\mathscr{F}$ is long, and we shall better be able to manage the formulas given its general form $\exists p \exists q[\mathscr{P} \wedge \mathscr{Q} \wedge \mathscr{B}]$. Also, given the structure of the definition for this recursion clause, it will be convenient to lapse into induction scheme III from the induction schemes reference on p. 388, making the assumption for a single member of the series n, and then showing that it holds for the next. Thus, beginning with the basis, we then assume $Q_s \vdash \forall w[\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{n}}, w) \rightarrow w = \overline{\mathsf{k}}_{\mathsf{n}}]$, and show $Q_s \vdash \forall w[\mathcal{F}(\overline{\mathsf{m}}, S\overline{\mathsf{n}}, w) \rightarrow w = \overline{\mathsf{k}}_{S\mathsf{n}}]$.

Basis: Suppose $\mathsf{n} = 0$. From capture, $Q_s \vdash_{ND} \forall z[\mathcal{G}(\overline{\mathsf{m}}, z) \rightarrow z = \overline{\mathsf{k}}_0]$. By uniqueness of remainder (and generalizing on p and q), $Q_s \vdash_{ND} \forall p \forall q \forall y[(\mathcal{B}(p, q, \emptyset, \overline{\mathsf{k}}_0) \wedge \mathcal{B}(p, q, \emptyset, y)) \rightarrow \overline{\mathsf{k}}_0 = y]$. $\mathcal{F}$ is of the sort, $\exists p \exists q\{\exists v[\mathcal{B}(p, q, \emptyset, v) \wedge \mathcal{G}(\vec{x}, v)] \wedge \mathcal{Q} \wedge \mathcal{B}(p, q, \emptyset, z)\}$. You need to show $Q_s \vdash \forall w[\exists p \exists q\{\exists v[\mathcal{B}(p, q, \emptyset, v) \wedge \mathcal{G}(\overline{\mathsf{m}}, v)] \wedge \mathcal{Q} \wedge \mathcal{B}(p, q, \emptyset, w)\} \rightarrow w = \overline{\mathsf{k}}_0]$. This is straightforward. So $Q_s \vdash \forall w[\mathcal{F}(\overline{\mathsf{m}}, \emptyset, w) \rightarrow w = \overline{\mathsf{k}}_0]$.

Assp: $Q_s \vdash \forall w[\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{n}}, w) \rightarrow w = \overline{\mathsf{k}}_{\mathsf{n}}]$

Show: $Q_s \vdash \forall w[\mathcal{F}(\overline{\mathsf{m}}, S\overline{\mathsf{n}}, w) \rightarrow w = \overline{\mathsf{k}}_{S\mathsf{n}}]$

From capture, $Q_s \vdash_{ND} \forall w[\mathcal{H}(\overline{\mathsf{m}}, \overline{\mathsf{n}}, \overline{\mathsf{k}}_{\mathsf{n}}, w) \rightarrow w = \overline{\mathsf{k}}_{S\mathsf{n}}]$. And again we make an appeal to uniqueness:

1.	$\forall w[\mathcal{F}(\overline{m}, \overline{n}, w) \rightarrow w = \overline{k}_{n}]$	by assumption
2.	$\forall w[\mathcal{H}(\overline{m}, \overline{n}, \overline{k}_{n}, w) \rightarrow w = \overline{k}_{Sn}]$	by capture
3.	$\forall p \forall q \forall y[(\mathcal{B}(p, q, S\overline{n}, \overline{k}_{Sn}) \wedge \mathcal{B}(p, q, S\overline{n}, y)) \rightarrow \overline{k}_{Sn} = y]$	uniqueness
4.	$\mathcal{F}(\overline{m}, S\overline{n}, j)$	A (g, $\rightarrow$I)
5.	$\exists p \exists q[\mathcal{P}(p, q, \overline{m}) \wedge \mathcal{Q}(p, q, \overline{m}, S\overline{n}) \wedge \mathcal{B}(p, q, S\overline{n}, j)]$	4 abv
6.	$\exists q[\mathcal{P}(p, q, \overline{m}) \wedge \mathcal{Q}(p, q, \overline{m}, S\overline{n}) \wedge \mathcal{B}(p, q, S\overline{n}, j)]$	A (g, 5$\exists$E)
7.	$\mathcal{P}(p, q, \overline{m}) \wedge \mathcal{Q}(p, q, \overline{m}, S\overline{n}) \wedge \mathcal{B}(p, q, S\overline{n}, j)$	A (g, 6$\exists$E)
8.	$\exists v[\mathcal{B}(p, q, \emptyset, v) \wedge \mathcal{G}(\overline{m}, v)]$	7 $\wedge$E ($\mathcal{P}$)
9.	$(\forall i < S\overline{n})\exists u \exists v[\mathcal{B}(p, q, i, u) \wedge \mathcal{B}(p, q, Si, v) \wedge \mathcal{H}(\overline{m}, i, u, v)]$	7 $\wedge$E ($\mathcal{Q}$)
10.	$\mathcal{B}(p, q, S\overline{n}, j)$	7 $\wedge$E
11.	$\overline{n} < S\overline{n}$	T8.14
12.	$\exists u \exists v[\mathcal{B}(p, q, \overline{n}, u) \wedge \mathcal{B}(p, q, S\overline{n}, v) \wedge \mathcal{H}(\overline{m}, \overline{n}, u, v)]$	9,11 ($\forall$E)
13.	$\exists v[\mathcal{B}(p, q, \overline{n}, u) \wedge \mathcal{B}(p, q, S\overline{n}, v) \wedge \mathcal{H}(\overline{m}, \overline{n}, u, v)]$	A (g, 12$\exists$E)
14.	$\mathcal{B}(p, q, \overline{n}, u) \wedge \mathcal{B}(p, q, S\overline{n}, v) \wedge \mathcal{H}(\overline{m}, \overline{n}, u, v)$	A (g, 13$\exists$E)
15.	$\mathcal{B}(p, q, \overline{n}, u)$	14 $\wedge$E
16.	$(\forall i < \overline{n})\exists u \exists v[\mathcal{B}(p, q, i, u) \wedge \mathcal{B}(p, q, Si, v) \wedge \mathcal{H}(\overline{m}, i, u, v)]$	9 with T8.21
17.	$\mathcal{F}(\overline{m}, \overline{n}, u)$	8,16,15 with $\exists$I
18.	$u = \overline{k}_{n}$	1,17 with $\forall$E
19.	$\mathcal{H}(\overline{m}, \overline{n}, u, v)$	14 $\wedge$E
20.	$\mathcal{H}(\overline{m}, \overline{n}, \overline{k}_{n}, v)$	19,18 =E
21.	$v = \overline{k}_{Sn}$	2,20 with $\forall$E
22.	$\mathcal{B}(p, q, S\overline{n}, v)$	14 $\wedge$E
23.	$\mathcal{B}(p, q, S\overline{n}, \overline{k}_{Sn})$	22,21 =E
24.	$j = \overline{k}_{Sn}$	3,10,23 with $\forall$E
25.	$j = \overline{k}_{Sn}$	13,14-24 $\exists$E
26.	$j = \overline{k}_{Sn}$	12,13-25 $\exists$E
27.	$j = \overline{k}_{Sn}$	6,7-26 $\exists$E
28.	$j = \overline{k}_{Sn}$	5,6-27 $\exists$E
29.	$\mathcal{F}(\overline{m}, S\overline{n}, j) \rightarrow j = \overline{k}_{Sn}$	4-28 $\rightarrow$I
30.	$\forall w[\mathcal{F}(\overline{m}, S\overline{n}, w) \rightarrow w = \overline{k}_{Sn}]$	29 $\forall$I

Lines 8 - 10 of show the content of the assumptions on 4 - 7 which are too long to display in expanded form. Once we are able to show $\mathcal{F}(\overline{m}, \overline{n}, u)$ at (17), the inductive assumption lets us "pin" u onto $\overline{k}_{n}$. Then uniqueness conditions for $\mathcal{H}$ and $\mathcal{B}$ allow us to move to unique outputs for $\mathcal{H}$ and $\mathcal{B}$ and so for $\mathcal{F}$. Line 16 perhaps obviously follows from (9), but its derivation may be obscure: by T8.14, Q $\vdash \overline{0} < S\overline{n}$ and ... and Q $\vdash \overline{n-1} < S\overline{n}$; so where $\mathcal{A}$ is the formula quantified on (9) by ($\forall$E), Q $\vdash \mathcal{A}(\overline{0})$ and ... and Q $\vdash \mathcal{A}(\overline{n-1})$; then with

T8.21 it follows that $\mathsf{Q} \vdash (\forall i < \overline{\mathsf{n}})\mathcal{A}(i)$.

Indct: For any n, $\mathrm{Q_s} \vdash_{ND} \forall w[\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{n}}, w) \rightarrow w = \overline{\mathsf{k}}_{\mathsf{n}}]$.

Observe that in both the basis and show clauses we require the generalized uniqueness for $\mathcal{B}$: this is because it is being applied inside assumptions for ∃E, where p and q are arbitrary variables, not numerals $\overline{\mathsf{p}}$ and $\overline{\mathsf{q}}$, to which the ordinary notion of capture for $\mathcal{B}$ would apply. So $\forall w[\mathcal{F}(\overline{\mathsf{m}}, \overline{\mathsf{n}}, w) \rightarrow w = \overline{\mathsf{a}}]$. So we satisfy the recursive clause for T12.11. So the theorem is proved. And we have shown that $\mathrm{Q_s}$ has the resources to capture any recursive function.

This theorem has a number of attractive features: We show that recursive functions are captured directly by the original formulas by which they are expressed. A byproduct is that recursive functions are captured by Σ_1 formulas. The argument is a straightforward induction on the sequence of recursive functions, of a type we have seen before. But we do not show that recursive functions are captured in Q. It is that to which we now turn.

*E12.13. Complete the demonstration of T12.11 by completing the remaining cases, including the basis and part (ii) of the case for composition.

*E12.14. Produce a derivation to show the basis of T12.12.

E12.15. Return to the simple functions from from E12.9. Show that on the standard interpretation N of $\mathcal{L}_{NT}$ each simple function $\mathsf{f}(\vec{\mathsf{x}})$ is captured in $\mathrm{Q_s}$ by the formula used to express it. Restrict appeal to external theorems just to your result from E12.9 and T8.14 as appropriate.

12.3.3 The result strengthened

T12.11 shows that the recursive functions are captured in $\mathrm{Q_s}$ by their Σ_1 original expressers. As we have suggested, this argument is easily strengthened to show that the recursive functions are captured in Q. To do so, we give up the capture by original expressers, though we retain the result that the recursive functions are captured by Σ_1 formulas.

In the previous section, we appealed to uniqueness of remainder for the β-function. In $\mathrm{Q_s}$, the original formula $\mathcal{B}$ captures the β-function, and gives a strengthened uniqueness result important for T12.12. But we can simulate this effect by some easy theorems. Recall that the β-function is originally expressed by a Δ_0 formula $\mathcal{B}$.

T12.13. If a total function $\mathsf{f}(\vec{\mathsf{x}})$ is expressed by a Δ_0 formula $\mathscr{F}(\vec{x}, v)$, then $\mathscr{F}'(\vec{x}, v) =_{\text{def}} \mathscr{F}(\vec{x}, v) \wedge (\forall z \leq v)[\mathscr{F}(\vec{x}, z) \rightarrow z = v]$ is Δ_0 and captures f in Q.

Suppose a total $\mathsf{f}(\vec{\mathsf{x}})$ is expressed by a Δ_0 formula $\mathscr{F}(\vec{x}, v)$. Suppose $\vec{\mathsf{x}}$ reduces to a single variable and $\langle \mathsf{m}, \mathsf{a} \rangle \in \mathsf{f}$. (a) Then, $\mathsf{N}[\mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] = \mathsf{T}$; and since $\mathscr{F}$ is Δ_0, by T12.8, Q $\vdash_{ND} \mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})$. (b) Suppose $\mathsf{n} \neq \mathsf{a}$; then $\langle \mathsf{m}, \mathsf{n} \rangle \notin \mathsf{f}$; so with T12.2, $\mathsf{N}[\sim\mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{n}})] = \mathsf{T}$ and $\mathsf{N}[\mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{n}})] \neq \mathsf{T}$; so by T12.8, Q $\vdash_{ND} \sim\mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{n}})$.

(i) From (a), Q $\vdash \mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}})$. And $\vdash \overline{\mathsf{a}} = \overline{\mathsf{a}}$, so $\vdash \mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}}) \rightarrow \overline{\mathsf{a}} = \overline{\mathsf{a}}$; and from (b), for $\mathsf{q} < \mathsf{a}$, Q $\vdash \sim\mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{q}})$; so trivially, Q $\vdash \mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{q}}) \rightarrow \overline{\mathsf{q}} = \overline{\mathsf{a}}$; so for any $\mathsf{p} \leq \mathsf{a}$, Q $\vdash \mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{p}}) \rightarrow \overline{\mathsf{p}} = \overline{\mathsf{a}}$; so by T8.21, Q $\vdash (\forall z \leq \overline{\mathsf{a}})(\mathscr{F}(\overline{\mathsf{m}}, z) \rightarrow z = \overline{\mathsf{a}})$. So with $\wedge$I, Q $\vdash \mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}}) \wedge (\forall z \leq \overline{\mathsf{a}})(\mathscr{F}(\overline{\mathsf{m}}, z) \rightarrow z = \overline{\mathsf{a}})$; which is to say, Q $\vdash \mathscr{F}'(\overline{\mathsf{m}}, \overline{\mathsf{a}})$.

(ii) Hint: You need to show Q $\vdash \forall w([\mathscr{F}(\overline{\mathsf{m}}, w) \wedge (\forall z \leq w)(\mathscr{F}(\overline{\mathsf{m}}, z) \rightarrow z = w)] \rightarrow w = \overline{\mathsf{a}})$. Take as premises $\mathscr{F}(\overline{\mathsf{m}}, \overline{\mathsf{a}}) \wedge (\forall z \leq \overline{\mathsf{a}})(\mathscr{F}(\overline{\mathsf{m}}, z) \rightarrow z = \overline{\mathsf{a}})$ from (i), along with $j \leq \overline{\mathsf{a}} \vee \overline{\mathsf{a}} \leq j$ from T8.19.

So if conditions (a) and (b) are met, $\mathscr{F}'$ captures f. $\mathscr{F}'$ is not the same as the original $\mathscr{F}$ to express the function. Still, since the Δ_0 $\mathscr{B}$ expresses the β-function, $\mathscr{B}'$ captures it in Q.

Intuitively, the second conjunct of $\mathscr{F}'$ asserts explicitly that at most one v satisfies $\mathscr{F}'$. Thus it is not surprising that formulas of the sort $\mathscr{F}'$ yield a uniqueness result.

T12.14. For $\mathscr{F}'(\vec{x}, v) =_{\text{def}} \mathscr{F}(\vec{x}, v) \wedge (\forall z \leq v)[\mathscr{F}(\vec{x}, z) \rightarrow z = v]$ as above, for any n, Q $\vdash \forall \vec{x} \forall y[(\mathscr{F}'(\vec{x}, \overline{\mathsf{n}}) \wedge \mathscr{F}'(\vec{x}, y)) \rightarrow y = \overline{\mathsf{n}}]$.

Suppose $\vec{x}$ reduces to a single variable and reason as follows,

1.	$\forall x(x \leq \overline{\mathsf{n}} \vee \overline{\mathsf{n}} \leq x)$	T8.19
2.	$\mathscr{F}'(j,\overline{\mathsf{n}}) \wedge \mathscr{F}'(j,k)$	A (g →I)
3.	$\mathscr{F}(j,\overline{\mathsf{n}}) \wedge (\forall z \leq \overline{\mathsf{n}})(\mathscr{F}(j,z) \rightarrow z = \overline{\mathsf{n}})$	2 ∧E (unabv)
4.	$\mathscr{F}(j,k) \wedge (\forall z \leq k)(\mathscr{F}(j,z) \rightarrow z = k)$	2 ∧E (unabv)
5.	$k \leq \overline{\mathsf{n}} \vee \overline{\mathsf{n}} \leq k$	1 ∀E
6.	$k \leq \overline{\mathsf{n}}$	A (g 5∨E)
7.	$(\forall z \leq \overline{\mathsf{n}})(\mathscr{F}(j,z) \rightarrow z = \overline{\mathsf{n}})$	3 ∧E
8.	$\mathscr{F}(j,k) \rightarrow k = \overline{\mathsf{n}}$	7,6 (∀E)
9.	$\mathscr{F}(j,k)$	4 ∧E
10.	$k = \overline{\mathsf{n}}$	8,9 →E
11.	$\overline{\mathsf{n}} \leq k$	A (g 5∨E)
	⋮	
12.	$k = \overline{\mathsf{n}}$	
13.	$k = \overline{\mathsf{n}}$	5,6-10,11-12 ∨E
14.	$(\mathscr{F}'(j,\overline{\mathsf{n}}) \wedge \mathscr{F}'(j,k)) \rightarrow k = \overline{\mathsf{n}}$	2-13 →I
15.	$\forall y[(\mathscr{F}'(j,\overline{\mathsf{n}}) \wedge \mathscr{F}'(j,y)) \rightarrow y = \overline{\mathsf{n}}]$	14 ∀I
16.	$\forall x \forall y[(\mathscr{F}'(x,\overline{\mathsf{n}}) \wedge \mathscr{F}'(x,y)) \rightarrow y = \overline{\mathsf{n}}]$	15 ∀I

Reasoning for the second subderivation is similar to the first.

So where p, q and v are universally quantified we shall have, $\mathsf{Q} \vdash \forall p \forall q \forall v[(\mathscr{B}'(p,q,\overline{\mathsf{m}},\overline{\mathsf{n}}) \wedge \mathscr{B}'(p,q,\overline{\mathsf{m}},v)) \rightarrow v = \overline{\mathsf{n}}]$. This is what we had before except applied to $\mathscr{B}'$ rather than $\mathscr{B}$.

Observe also that insofar as $\mathscr{F}'(\vec{x},v)$ is built on an $\mathscr{F}(\vec{x},v)$ that expresses $\mathsf{f}(\vec{\mathsf{x}})$, $\mathscr{F}'(\vec{x},v)$ continues to expresses $\mathsf{f}(\vec{\mathsf{x}})$. Perhaps this is obvious given what $\mathscr{F}'$ says. However, we can argue for the result directly.

T12.15. If $\mathscr{F}(\vec{x},v)$ expresses a total $\mathsf{f}(\vec{\mathsf{x}})$, then $\mathscr{F}'(\vec{x},v) = \mathscr{F}(\vec{x},v) \wedge (\forall z \leq v)[\mathscr{F}(\vec{x},z) \rightarrow z = v]$ expresses $\mathsf{f}(\vec{\mathsf{x}})$.

Suppose $\vec{\mathsf{x}}$ reduces to a single variable and total $\mathsf{f}(\mathsf{x})$ is expressed by $\mathscr{F}(x,v)$. Suppose $\langle \mathsf{m},\mathsf{a}\rangle \in \mathsf{f}$. (a) By expression, $\mathsf{N}[\mathscr{F}(\overline{\mathsf{m}},\overline{\mathsf{a}})] = \mathsf{T}$. (b) Suppose $\mathsf{n} \neq \mathsf{a}$; then $\langle \mathsf{m},\mathsf{n}\rangle \notin \mathsf{f}$; so with T12.2, $\mathsf{N}[\sim\mathscr{F}(\overline{\mathsf{m}},\overline{\mathsf{n}})] = \mathsf{T}$.

(i) Suppose $\mathsf{N}[\mathscr{F}'(\overline{\mathsf{m}},\overline{\mathsf{a}})] \neq \mathsf{T}$. This is impossible. You will need applications of T12.6 and T10.2; observe that for $\mathsf{n} \leq \mathsf{a}$ either $\mathsf{n} = \mathsf{a}$ or $\mathsf{n} < \mathsf{a}$ (so that $\mathsf{n} \neq \mathsf{a}$).

(ii) Suppose $\mathsf{N}[\forall w([\mathscr{F}(\overline{\mathsf{m}},w) \wedge (\forall z \leq w)(\mathscr{F}(\overline{\mathsf{m}},z) \rightarrow z = w)] \rightarrow w = \overline{\mathsf{a}})] \neq \mathsf{T}$. This is impossible. This time, you will be able to reason that for any n either $\mathsf{n} = \mathsf{a}$ or $\mathsf{n} \neq \mathsf{a}$.

And now we are in a position to recover the main result, except that the recursive functions are captured in Q rather than Q_s.

T12.16. Any recursive function is captured by a Σ_1 formula in Q

The β-function is total and expressed by a Δ_0 formula $\mathscr{B}(p, q, i, v)$; so by T12.15 and T12.13 there is a Δ_0 formula $\mathscr{B}'(p, q, i, v)$ that expresses and captures it in Q. For any $\mathsf{f}(\vec{\mathsf{x}})$ originally expressed by $\mathscr{F}(\vec{x}, v)$, let $\mathscr{F}^\dagger$ be like $\mathscr{F}$ except that instances of $\mathscr{B}$ are replaced by $\mathscr{B}'$. Since $\mathscr{B}'$ is Δ_0, $\mathscr{F}^\dagger$ remains Σ_1.

The argument is now a matter of showing that demonstrations of T12.3, T12.11 and T12.12 go through with application to these formulas and in Q. But the argument is nearly trivial: everything is the same as before with formulas of the sort $\mathscr{F}^\dagger$ replacing $\mathscr{F}$.

Be clear that expressions of the sort $\mathscr{F}^\dagger$ might appear all along in the show part of T12.3, T12.11 and T12.12. Expressions from the basis do not involve $\mathscr{B}$. It is included by recursion; after that, composition and regular minimization might be applied to expressions of any sort, and so to ones which involve $\mathscr{B}$ as well.

As in for the case of expression, formulas other than $\mathscr{F}^\dagger(\vec{x}, v)$ might capture the recursive functions — for example, if $\mathscr{F}^\dagger(\vec{x}, v)$ captures $\mathsf{f}(\vec{\mathsf{x}})$, then so does $\mathscr{F}^\dagger(\vec{x}, v) \wedge \mathscr{A}$ for any theorem $\mathscr{A}$. Let us say that $\mathscr{F}^\dagger(\vec{x}, v)$ is the *canonical* formula that captures $\mathsf{f}(\vec{\mathsf{x}})$ in Q. Of course, the canonical formula which captures $\mathsf{f}(\vec{\mathsf{x}})$ need not be the same as the corresponding original formula — for the β-function is not captured by its original formula (and so any formula which includes a β-function fails to be original). Because the β-function is captured by a Δ_0 formula we do, however, retain the result that every recursive function is captured in Q by some Σ_1 formula.

For the rest of this chapter, unless otherwise noted, when we assert the existence of a formula to express or some capture recursive function, we shall have in mind the *canonical* formula. Thus a function is expressed and captured by the same formula.

E12.16. Provide an argument to demonstrate (ii) of T12.13.

E12.17. Finish the derivation for T12.14 by completing the second subderivation.

E12.18. Complete the demonstration of T12.15.

*E12.19. Work carefully through the demonstration of T12.16 by setting up revised arguments T12.3†, T12.11† and T12.12†. As feasible, you may simply explain how parts differ from the originals.

12.4 More Recursive Functions

Now that we have seen what the recursive functions are, and the powers of our logical systems to express and capture recursive functions, we turn to extending their range. In fact, in this section, we shall generate a series of functions that are *primitive* recursive. In addition to the initial functions, so far, we have seen that plus, times, fact and power are primitive recursive. As we increase the range of (primitive) recursive functions, it immediately follows that our logical systems have the power to express and capture all the same functions.

12.4.1 Preliminary Functions

We begin with some simple primitive recursive functions that will serve as a foundation for things to come.

Predecessor with cutoff. Set the predecessor of zero to zero itself, and for any other value to the one before. Since $\mathsf{pred(y)}$ is a one-place function, gpred is a constant, in this case, $\mathsf{gpred} = 0$. And $\mathsf{hpred} = \mathsf{idnt}^2_1(\mathsf{y}, \mathsf{u})$. So, as we expect for $\mathsf{pred(y)}$,

$$\mathsf{pred}(0) = 0$$
$$\mathsf{pred}(\mathsf{suc}(\mathsf{y})) = \mathsf{y}$$

So predecessor is a primitive recursive function.

Subtraction with cutoff. When $\mathsf{y} \geq \mathsf{x}$, $\mathsf{subc}(\mathsf{x}, \mathsf{y}) = 0$. Otherwise $\mathsf{subc}(\mathsf{x}, \mathsf{y}) = \mathsf{x} - \mathsf{y}$. For $\mathsf{subc}(\mathsf{x}, \mathsf{y})$, set $\mathsf{gsubc}(\mathsf{x}) = \mathsf{idnt}^1_1(\mathsf{x})$. And $\mathsf{hsubc}(\mathsf{x}, \mathsf{y}, \mathsf{u}) = \mathsf{pred}(\mathsf{idnt}^3_3(\mathsf{x}, \mathsf{y}, \mathsf{u}))$. So,

$$\mathsf{subc}(\mathsf{x}, 0) = \mathsf{x}$$
$$\mathsf{subc}(\mathsf{x}, \mathsf{suc}(\mathsf{y})) = \mathsf{pred}(\mathsf{subc}(\mathsf{x}, \mathsf{y}))$$

So as y increases by one, the difference decreases by one. Informally, indicate $\mathsf{subc}(\mathsf{x}, \mathsf{y}) = (\mathsf{x} \dot{-} \mathsf{y})$.

Absolute value. $\mathsf{absval(x - y)} = (\mathsf{x} \dot{-} \mathsf{y}) + (\mathsf{y} \dot{-} \mathsf{x})$. So we find the absolute value of the difference between x and y by doing the subtraction with cutoff both ways. One direction yields zero. The other yields the value we want. So the sum comes out to the absolute value. This is a function with two arguments (only separated by '-' rather than comma to remind us of the nature of the function). This function results entirely by composition, without a recursion clause. Informally, we indicate absolute value in the usual way, $\mathsf{absval(x - y)} = |\mathsf{x - y}|$.

Sign. The function sg(y) is zero when y is zero and otherwise one. For sg(y), set $\mathsf{gsg} = 0$. And $\mathsf{hsg(y, u)} = \mathsf{suc(zero(idnt}^2_1\mathsf{(y, u)))}$. So,

$$\mathsf{sg}(0) = 0$$
$$\mathsf{sg(suc(y))} = \mathsf{suc(zero(y))}$$

So the sign of any successor is just the successor of zero, which is one.

Converse sign. The function csg(y) is one when y is zero and otherwise zero. So it inverts sg. For csg(y), set $\mathsf{gcsg} = \mathsf{suc}(0)$. And $\mathsf{hcsg(y, u)} = \mathsf{zero(idnt}^2_1\mathsf{(y, u))}$. So,

$$\mathsf{csg}(0) = \mathsf{suc}(0)$$
$$\mathsf{csg(suc(y))} = \mathsf{zero(y)}$$

So the converse sign of any successor is just zero. Informally, we indicate the converse sign with a bar, $\overline{\mathsf{sg}}(\mathsf{y})$.

E12.20. Consider again your file `recursive1.rb` from E12.3. Extend your sequence of functions to include `pred(x)`, `subc(x,y)`, `absval(x - y)`, `sg(x)`, and `csg(x)`. Calculate some values of these functions and print the results, along with your program. Again, there should be no appeal to functions except from earlier in the chain.

12.4.2 Characteristic Functions

The characteristic function $\mathsf{ch_R}(\vec{\mathsf{x}})$ of a relation R takes the value 0 when $\vec{\mathsf{x}} \in \mathsf{R}$ and 1 when $\vec{\mathsf{x}} \notin \mathsf{R}$.

(CF) For any function $\mathsf{p}(\vec{\mathsf{x}})$, $\mathsf{sg(p}(\vec{\mathsf{x}}))$ is the *characteristic* function of the relation R such that $\vec{\mathsf{x}} \in \mathsf{R}$ iff $\mathsf{sg(p}(\vec{\mathsf{x}})) = 0$.

So a characteristic function for relation R takes the value 0 if $\mathsf{R}(\vec{\mathsf{x}})$ is true, and 1 if $\mathsf{R}(\vec{\mathsf{x}})$ is not true.[7] A (*primitive*) *recursive* property or relation is one that has a (primitive) recursive characteristic function. When a function p already takes just the values 0 and 1 so that $\mathsf{sg}(\mathsf{p}(\vec{\mathsf{x}})) = \mathsf{p}(\vec{\mathsf{x}})$, we generally omit sg from our specifications.

These definitions immediately result in corollaries to T12.3 and T12.16.

T12.3 (corollary). On the standard interpretation N of $\mathscr{L}_{NT}$, each recursive relation $\mathsf{R}(\vec{\mathsf{x}})$ is expressed by some formula $\mathcal{R}(\vec{x})$.

> Suppose $\mathsf{R}(\vec{\mathsf{x}})$ is a recursive relation; then has a recursive and so total characteristic function $\mathsf{ch}_\mathsf{R}(\vec{\mathsf{x}})$; so by T12.3 there is some formula $\mathcal{R}(\vec{x}, y)$ that expresses $\mathsf{ch}_\mathsf{R}(\vec{\mathsf{x}})$. So in the case where $\vec{x}$ reduces to a single variable, if $\mathsf{m} \in \mathsf{R}$, then $\langle \mathsf{m}, 0\rangle \in \mathsf{ch}_\mathsf{R}$; and by expression, $\mathsf{I}[\mathcal{R}(\overline{\mathsf{m}}, \emptyset)] = \mathsf{T}$; and if $\mathsf{m} \notin \mathsf{R}$, then $\langle \mathsf{m}, 0\rangle \notin \mathsf{ch}_\mathsf{R}$, so that with T12.2, $\mathsf{I}[\sim\mathcal{R}(\overline{\mathsf{m}}, \emptyset)] = \mathsf{T}$. So, generally, $\mathcal{R}(\vec{x}, \emptyset)$ expresses $\mathsf{R}(\vec{\mathsf{x}})$.

T12.16 (corollary). Any recursive relation is captured by a Σ_1 formula in Q.

> Suppose $\mathsf{R}(\vec{\mathsf{x}})$ is a recursive relation; then it has a recursive and so total characteristic function $\mathsf{ch}_\mathsf{R}(\vec{\mathsf{x}})$; so by T12.16 there is some Σ_1 formula $\mathcal{R}(\vec{x}, y)$ that captures $\mathsf{ch}_\mathsf{R}(\vec{\mathsf{x}})$. So in the case where $\vec{x}$ reduces to a single variable, if $\mathsf{m} \in \mathsf{R}$, then $\langle \mathsf{m}, 0\rangle \in \mathsf{ch}_\mathsf{R}$; and by capture $T \vdash \mathcal{R}(\overline{\mathsf{m}}, \emptyset)$; and if $\mathsf{m} \notin \mathsf{R}$, then $\langle \mathsf{m}, 0\rangle \notin \mathsf{ch}_\mathsf{R}$; so by capture with T12.4, $T \vdash \sim\mathcal{R}(\overline{\mathsf{m}}, \emptyset)$. So, generally $\mathcal{R}(\vec{x}, \emptyset)$ captures $\mathsf{R}(\vec{\mathsf{x}})$.

So our results for the expression and capture of recursive functions extend directly to the expression and capture of recursive relations: a recursive relation has a recursive characteristic function; as such, the function is expressed and captured; so, as we have just seen, the corresponding relation is expressed and captured.

Equality. Say $\mathsf{t}(\vec{\mathsf{x}})$ is a *recursive term* just in case it is a variable, constant, or a recursive function. Then for any recursive terms $\mathsf{s}(\vec{\mathsf{x}})$ and $\mathsf{t}(\vec{\mathsf{y}})$, $\mathsf{EQ}(\mathsf{s}(\vec{\mathsf{x}}), \mathsf{t}(\vec{\mathsf{y}}))$ — typically rendered $\mathsf{s}(\vec{\mathsf{x}}) = \mathsf{t}(\vec{\mathsf{y}})$, is a recursive relation with characteristic function $\mathsf{ch}_{\mathsf{EQ}}(\vec{\mathsf{x}}, \vec{\mathsf{y}}) = \mathsf{sg}|\mathsf{s}(\vec{\mathsf{x}}) \text{ - } \mathsf{t}(\vec{\mathsf{y}})|$. When $\mathsf{s}(\vec{\mathsf{x}})$ is equal to $\mathsf{t}(\vec{\mathsf{y}})$, the absolute value of the difference is zero so the value of sg is zero. But when $\mathsf{s}(\vec{\mathsf{x}})$ is other than $\mathsf{t}(\vec{\mathsf{y}})$, the absolute value of the difference is other than zero, so value of sg is one. And, supposing that $\mathsf{s}(\vec{\mathsf{x}})$ and $\mathsf{t}(\vec{\mathsf{x}})$ are recursive, this characteristic function is a composition of recursive functions. So the result is recursive. So $\mathsf{s}(\vec{\mathsf{x}}) = \mathsf{t}(\vec{\mathsf{y}})$ is a recursive relation.

[7] It is perhaps more common to reverse the values of zero and one for the characteristic function. However, the choice is arbitrary, and this choice is technically convenient.

A couple of observations: First, be clear that EQ is the standard relation we all know and love. The trick is to show that it is recursive. We are not *given* that EQ is a recursive relation — so we demonstrate that it is, by showing that it has a recursive characteristic function. Second, one might think that we could express $\mathsf{f}(\vec{\mathsf{x}}) = \mathsf{g}(\vec{\mathsf{y}})$ by some relatively simple expression that would compose expressions for the functions with equality as, $\exists u \exists v[\mathscr{F}(\vec{x}, u) \wedge \mathscr{G}(\vec{y}, v) \wedge u = v]$. This would be fine. However we have offered a general account which, as is often the case for these things, need not be the most efficient. Where $\mathsf{sg}|\mathsf{f}(\vec{\mathsf{x}}) - \mathsf{g}(\vec{\mathsf{y}})|$ is expressed and captured by some $\mathscr{S}(\vec{x}, \vec{y}, v)$ our approach, which works by modification of the characteristic function, generates the relatively complex, $\mathscr{E}(\vec{x}, \vec{y}) =_{\text{def}} \mathscr{S}(\vec{x}, \vec{y}, \emptyset)$.

Inequality. The relation $\text{LEQ}(\mathsf{s}(\vec{\mathsf{x}}), \mathsf{t}(\vec{\mathsf{y}}))$ has characteristic function $\mathsf{sg}(\mathsf{s}(\vec{\mathsf{x}}) \dot{-} \mathsf{t}(\vec{\mathsf{y}}))$. When $\mathsf{s}(\vec{\mathsf{x}}) \leq \mathsf{t}(\vec{\mathsf{y}})$, $\mathsf{s}(\vec{\mathsf{x}}) \dot{-} \mathsf{t}(\vec{\mathsf{y}}) = 0$; so $\mathsf{sg} = 0$; Otherwise the value is 1. The relation $\text{LESS}(\mathsf{s}(\vec{\mathsf{x}}), \mathsf{t}(\vec{\mathsf{y}}))$ has characteristic function $\mathsf{sg}(\mathsf{suc}(\mathsf{s}(\vec{\mathsf{x}})) \dot{-} \mathsf{t}(\vec{\mathsf{y}}))$. When $\mathsf{s}(\vec{\mathsf{x}}) < \mathsf{t}(\vec{\mathsf{y}})$, $\mathsf{suc}(\mathsf{s}(\vec{\mathsf{x}})) \dot{-} \mathsf{t}(\vec{\mathsf{y}}) = 0$; so $\mathsf{sg} = 0$. Otherwise the value is 1. These are typically represented $\mathsf{s}(\vec{\mathsf{x}}) \leq \mathsf{t}(\vec{\mathsf{y}})$ and $\mathsf{s}(\vec{\mathsf{x}}) < \mathsf{t}(\vec{\mathsf{y}})$.

With equality and inequality, we have atomic recursive relations. And we set out to exhibit ones that are more complex in the usual way.

Truth functions. Suppose $\mathsf{P}(\vec{\mathsf{x}})$ and $\mathsf{Q}(\vec{\mathsf{x}})$ are recursive relations. Then $\text{NEG}(\mathsf{P}(\vec{\mathsf{x}}))$ and $\text{DSJ}(\mathsf{P}(\vec{\mathsf{x}}), \mathsf{Q}(\vec{\mathsf{x}}))$ are recursive relations. Suppose $\mathsf{ch}_{\mathsf{P}}(\vec{\mathsf{x}})$ and $\mathsf{ch}_{\mathsf{Q}}(\vec{\mathsf{x}})$ are the characteristic functions of $\mathsf{P}(\vec{\mathsf{x}})$ and $\mathsf{Q}(\vec{\mathsf{x}})$.

$\text{NEG}(\mathsf{P}(\vec{\mathsf{x}}))$ (typically $\sim\mathsf{P}(\vec{\mathsf{x}})$) has characteristic function $\overline{\mathsf{sg}}(\mathsf{ch}_{\mathsf{P}}(\vec{\mathsf{x}}))$. When $\mathsf{P}(\vec{\mathsf{x}})$ does not obtain, the characteristic function of $\mathsf{P}(\vec{\mathsf{x}})$ takes value one, so the converse sign goes to zero. And when when $\mathsf{P}(\vec{\mathsf{x}})$ does obtain, its characteristic function is zero, so the converse sign is one — which is as it should be.

$\text{DSJ}(\mathsf{P}(\vec{\mathsf{x}}), \mathsf{Q}(\vec{\mathsf{y}}))$ (typically $\mathsf{P}(\vec{\mathsf{x}}) \vee \mathsf{Q}(\vec{\mathsf{y}})$) has characteristic function $\mathsf{ch}_{\mathsf{P}}(\vec{\mathsf{x}}) \times \mathsf{ch}_{\mathsf{Q}}(\vec{\mathsf{y}})$. When one of $\mathsf{P}(\vec{\mathsf{x}})$ or $\mathsf{Q}(\vec{\mathsf{y}})$ is true, the disjunction is true; but in this case, at least one characteristic function, and so the product of functions goes to zero. If neither $\mathsf{P}(\vec{\mathsf{x}})$ nor $\mathsf{Q}(\vec{\mathsf{y}})$ is true, the disjunction is not true; in this case, both characteristic functions, and so the product of functions take the value one.

Other truth functions are definable in the same terms as for negation and disjunction. So, for example, $\text{IMP}(\mathsf{P}(\vec{\mathsf{x}}), \mathsf{Q}(\vec{\mathsf{y}}))$ that is, $\mathsf{P}(\vec{\mathsf{x}}) \rightarrow \mathsf{Q}(\vec{\mathsf{y}})$ is just $\sim\mathsf{P}(\vec{\mathsf{x}}) \vee \mathsf{Q}(\vec{\mathsf{y}})$.

Bounded quantifiers: Consider a relation $\mathsf{S}(\vec{\mathsf{x}}, \mathsf{z}) = (\exists \mathsf{y} \leq \mathsf{z})\mathsf{P}(\vec{\mathsf{x}}, \mathsf{z}, \mathsf{y})$ which obtains when there is a y less than or equal to z such that $\mathsf{P}(\vec{\mathsf{x}}, \mathsf{z}, \mathsf{y})$. As usual, y is distinct from the bound z (compare the language of arithmetic reference). But z may appear as a variable of the relation P (as for *factor* or *prime number* just below); so we give it a place in our general form. Given $ch_{P}(\vec{x}, z, y)$, consider a further relation $\mathrm{R}(\vec{x}, z, v)$ corresponding to $(\exists y \leq v)\mathrm{P}(\vec{x}, z, y)$. So R treats the bound as a separate variable, and will let us reason by induction as the bound ranges from 0 to z. If we can find $ch_{R}(\vec{x}, z, v)$ then $ch_{S}(\vec{x}, z)$ is automatic as $ch_{R}(\vec{x}, z, z)$. For this $ch_{R}(\vec{x}, z, v)$ set,

$$gch_{R}(\vec{x}, z) = ch_{P}(\vec{x}, z, 0)$$
$$hch_{R}(\vec{x}, z, v, u) = u \times ch_{P}(\vec{x}, z, Sv)$$

In the simple case where $\vec{x}$ drops out, $ch_{R}(z, 0) = ch_{P}(z, 0)$. And $ch_{R}(z, Sv) = ch_{R}(z, v) \times ch_{P}(z, Sv)$. In the case where v is a successor, the result is,

$$ch_{R}(z, v) = ch_{P}(z, 0) \times ch_{P}(z, 1) \times \ldots \times ch_{P}(z, v)$$

Think of these as grouped to the left. So the result has $ch_{R}(z, n) = 1$ unless and until one of the members is zero, and then stays zero. So the function for $\mathrm{R}(z, n)$ goes to zero just in case $\mathrm{P}(z, v)$ is true for some value between 0 and n. So set $ch_{S}(\vec{x}, z) = ch_{R}(\vec{x}, z, z)$ — so the characteristic function for the bounded quantifier runs the R function up to the bound z.

For $(\exists y < z)\mathrm{P}(\vec{x}, z, y)$, it simplest simply to take $(\exists y \leq z)(y \neq z \wedge \mathrm{P}(\vec{x}, z, y))$. For $(\forall z \leq y)\mathrm{P}(\vec{x}, z)$ and $(\forall z < y)\mathrm{P}(\vec{x}, z)$, we may consider $\sim(\exists z \leq y)\sim\mathrm{P}(\vec{x}, z)$; and similarly in the other case. And we are done by previous results.

Least element: Let $m(\vec{x}, z) = (\mu y \leq z)\mathrm{P}(\vec{x}, z, y)$ be the least $y \leq z$ such that $\mathrm{P}(\vec{x}, z, y)$ if one exists, and otherwise z. Again, the bound may be a variable free in P. Then if $\mathrm{P}(\vec{x}, z, y)$ is a recursive relation, $(\mu y \leq z)\mathrm{P}(\vec{x}, z, y)$ is a recursive function. First take $\mathrm{R}(\vec{x}, z, v)$ for $(\exists y \leq v)\mathrm{P}(\vec{x}, z, y)$ and $ch_{R}(\vec{x}, z, v)$ as described above. So $ch_{R}(\vec{x}, z, v)$ goes to 0 when P is true for some $j \leq v$. Then, second, we introduce a function $q(\vec{x}, z, v)$ whose output is the value of $(\mu y \leq v)\mathrm{P}(\vec{x}, z, y)$. Given this, very much as before, $m(\vec{x}, z)$ is automatic as $q(\vec{x}, z, z)$. For $q(\vec{x}, z, v)$ set,

$$gq(\vec{x}, z) = zero(ch_{R}(\vec{x}, z, 0))$$
$$hq(\vec{x}, z, v, u) = u + ch_{R}(\vec{x}, z, v)$$

So in the simple case where $\vec{x}$ drops out, $q(z, 0) = 0$; for the least $y \leq 0$ that satisfies any $\mathrm{P}(z, y)$ can only be 0. And then $q(z, Sv) = q(z, v) + ch_{R}(z, v)$. The result is,

$$q(z, Sn) = 0 + ch_{R}(z, 0) + \ldots + ch_{R}(z, n)$$

where ch_{R} is 1 until it hits a member that is P and then goes to 0 and stays there. Set the first member to the side. Then since this series starts with $v = 0$ and ends with $v = n$ it has Sn members. So if all the values are 1 it evaluates to Sn. If there is some a such that $ch_{R}(z, a)$ is zero, then all the members prior to it are 1 and the sum is a.

So set $m(\vec{x}, z) = q(\vec{x}, z, z)$, so that we take the sum up to the limit z. Observe that $(\mu y \leq z)P(\vec{x}, z, y) = z$ does not require that $P(\vec{x}, z, z)$ — only that no $a < z$ is such that $P(\vec{x}, z, a)$.

Selection by cases. Suppose $f_0(\vec{x}) \ldots f_k(\vec{x})$ are recursive functions and $C_0(\vec{x}) \ldots C_k(\vec{x})$ are mutually exclusive recursive relations. Then $f(\vec{x})/C_0 \ldots C_k$ defined as follows is recursive.

$$f(\vec{x}) = \begin{cases} f_0(\vec{x}) \text{ if } C_0(\vec{x}) \\ f_1(\vec{x}) \text{ if } C_1(\vec{x}) \\ \vdots \\ f_k(\vec{x}) \text{ if } C_k(\vec{x}) \\ \text{and otherwise } a \end{cases}$$

Observe that, $f(\vec{x}) =$

$$[\overline{sg}(ch_{C_0}(\vec{x})) \times f_0(\vec{x}) + \overline{sg}(ch_{C_1}(\vec{x})) \times f_1(\vec{x}) + \ldots + \overline{sg}(ch_{C_k}(\vec{x})) \times f_k(\vec{x})] + [ch_{C_0}(\vec{x}) \times ch_{C_1}(\vec{x}) \times \ldots \times ch_{C_k}(\vec{x}) \times a]$$

works as we want. Each of the first terms in this sum is 0 unless the C_i is met in which case $\overline{sg}(ch_{C_i}(\vec{x}))$ is 1 and the term goes to $f_i(\vec{x})$. The final term is 0 unless no condition C_i is met, in which case it is a. So $f(\vec{x})$ is a composition of recursive functions, and itself recursive.

We turn now to some applications that will be particularly useful for things to come. In many ways, the project is like a cool translation exercise — pitched at the level of functions.

Factor. Let $\text{FCTR}(m, n)$ be the relation that obtains between m and n when $m + 1$ evenly divides n (typically, $m \mid n$). Division is by $m + 1$ to avoid worries about division by zero.[8] Then $m \mid n$ is recursive. This relation is defined as follows.

$$(\exists y \leq n)(Sm \times y = n)$$

Observe that this makes (the predecessor of) both 1 and n factors of n, and any number a factor of zero. Since each part is recursive, the whole is recursive. The argument is from the parts to the whole: $Sm \times y = n$ has a recursive characteristic

[8]In fact, this is a (minor) complication at this stage, but it will be helpful down the road. See p. 644n11.

function; so the bounded quantification has a recursive characteristic function; so the factor relation is recursive.

Prime number. Say $\textsc{prime}(n)$ is true just when n is a prime number. This property is defined as follows.

$$n > 1 \wedge (\forall j < n)[j \mid n \rightarrow (Sj = 1 \vee Sj = n)]$$

So n is greater than 1 and the successor of any number that divides it is either $\overline{1}$ or n itself.

Prime sequence. Say the primes are π_0, π_1.... Let the value of the function $pi(n)$ (usually $\boldsymbol{\pi}(n)$) be π_n. Then $\boldsymbol{\pi}(n)$ is defined by recursion as follows.

$gpi = suc(suc(0))$
$hpi(y, u) = (\mu y \leq u! + 1)(u < y \wedge \textsc{prime}(y))$

So the first prime, $\boldsymbol{\pi}(0) = 2$. And $\boldsymbol{\pi}(Sn) = (\mu y \leq \boldsymbol{\pi}(n)! + 1)(\boldsymbol{\pi}(n) < y \wedge \textsc{prime}(y))$. So at any stage, the next prime is the least prime which is greater than $\boldsymbol{\pi}(n)$. This depends on the point that all the primes $\leq \pi_n$ are included in the product $\boldsymbol{\pi}(n)!$ Let $p(n) = \pi_0 \times \pi_1 \times \ldots \times \pi_n$. By a standard argument (see G2 in the arithmetic for Gödel numbering reference, p. 480), $p(n) + 1$ is not divisible by any of the primes up to π_n; so either $p(n) + 1$ is itself prime, or there is some prime greater than π_n but less than $p(n) + 1$. But since $\boldsymbol{\pi}(n)!$ is a product including all the primes up to π_n, $p(n) \leq \boldsymbol{\pi}(n)!$; so either $\boldsymbol{\pi}(n)! + 1$ is prime or there is a prime greater than π_n but less than $\boldsymbol{\pi}(n)! + 1$ — and the next prime is sure to appear in the specified range.

Prime exponent. Let $exp(n, i)$ be the (possibly 0) exponent of π_i in the unique prime factorization of n. Then $exp(n, i)$ is recursive. This function may be defined as follows.

$$(\mu x \leq n)[pred(\boldsymbol{\pi}_i^x) \mid n \wedge pred(\boldsymbol{\pi}_i^{x+1}) \nmid n]$$

And, of course, $\boldsymbol{\pi}_i$ is just $\boldsymbol{\pi}(i)$. Observe that no exponent in the prime factorization of n is greater than n itself — for any $x \geq 2$, $x^n \geq n$ — so the bound is safe. This function returns the first x such that $\boldsymbol{\pi}_i^x$ divides n but $\boldsymbol{\pi}_i^{x+1}$ does not.

Prime length. Say a prime π_a is *included* in the factorization of n just in case there is some $b \geq a$ and $e > 0$ such that (the predecessor of) π_b^e is a factor of n. So we think of a prime factorization as,

$$\pi_0^{e_0} \times \pi_1^{e_1} \times \ldots \times \pi_b^{e_b}$$

where $e_b > 0$, but exponents for prior members of the series may be zero or not. Then $len(n)$ is the number of primes included in the prime factorization of n; so $len(0) = len(1) = 0$ and otherwise, since the series of primes begins with zero, $len(n) = b + 1$. For this set,

$$len(n) =_{def} (\mu y \leq n)(\forall z : y \leq z \leq n) exp(n, z) = 0$$

Officially: $(\mu y \leq n)(\forall z \leq n)[z \geq y \rightarrow exp(n, z) = 0]$. So we find the least y such that none of the primes between π_y and π_n are part of the factorization of n; but then all of the primes prior to it are members of the factorization so that y numbers the length of the factorization. This depends on its being the case that $n < \pi_n$ so that primes greater than or equal π_n are never included in the factorization of n.

E12.21. Returning to your file `recursive1.rb` from E12.3 and E12.20, extend the sequence of functions to include the characteristic function for $\text{FCTR}(m, n)$. You will need to begin with `cheq(a,b)` for the characteristic function of $a = b$ and then the characteristic function of $Sm \times y = n$. Then you will require a function like $ch_R(m, n, v)$ corresponding to $(\exists y \leq v)(Sm \times y = n)$. Calculate some values of these functions and print the results, along with your program.

E12.22. Continue in your file `recursive1.rb` to build the characteristic function for $\text{PRIME}(n)$. You will have to build gradually to this result (where the universal quantifier appears as $\sim(\exists j \leq n)(j \neq n \wedge \sim P)$. You will need `chless(a,b)` and then `chneg(a)`, `chdsj(a,b)`, `chimp(a,b)`, and `chand(a,b)` for the relevant truth functions. With these in hand, you can build a function `chp(n,j)` corresponding to $j \neq n \vee \sim(j \mid n \rightarrow (Sj = 0 \vee Sj = n))$. And with that, you can obtain a function like $R(n, j, v)$ and then the characteristic function of the bounded existential. Then, finally, build `prime(n)`. Calculate some values of these functions and print the results, along with your program.

E12.23. Continue in your file `recursive1.rb` to generate $\mathsf{lcm}(m, n)$ the least common multiple of Sm and Sn — that is, $(\mu y \leq Sm \times Sn)[y > 0 \wedge m \mid y \wedge n \mid y]$. For this you will need the characteristic function of $y > 0 \wedge m \mid y \wedge n \mid y$; and then one like $ch_R(m, n, v)$ corresponding to $(\exists y \leq v)[y > 0 \wedge m \mid y \wedge n \mid y]$. Then you will be able to find the function like $q(m, n, v)$ corresponding to $(\mu y \leq v)[y > 0 \wedge m \mid y \wedge n \mid y]$ and finally the lcm.

E12.24. Provide definitions for the recursive functions $rm(m, n)$ and $qt(m, n)$ for the remainder and quotient of $m/n + 1$.

*E12.25. Functions $f_1(\vec{x}, y)$ and $f_2(\vec{x}, y)$ are defined by *simultaneous* (mutual) recursion just in case,

$f_1(\vec{x}, 0) = g_1(\vec{x})$

$f_2(\vec{x}, 0) = g_2(\vec{x})$

$f_1(\vec{x}, Sy) = h_1(\vec{x}, y, f_1(\vec{x}, y), f_2(\vec{x}, y))$

$f_2(\vec{x}, Sy) = h_2(\vec{x}, y, f_1(\vec{x}, y), f_2(\vec{x}, y))$

Show that f_1 and f_2 so defined are recursive. Hint: Let $F(\vec{x}, y) = \pi_0^{f_1(\vec{x},y)} \times \pi_1^{f_2(\vec{x},y)}$; then find $G(\vec{x})$ in terms of g_1 and g_2, and $H(\vec{x}, y, u)$ in terms of h_1 and h_2 so that $F(\vec{x}, 0) = G(\vec{x})$ and $F(\vec{x}, Sy) = H(\vec{x}, y, F(\vec{x}, y))$. So $F(\vec{x}, y)$ is recursive. Then $f_1(\vec{x}, y) = exp(F(\vec{x}, y), 0)$ and $f_2(\vec{x}, y) = exp(F(\vec{x}, y), 1)$; so f_1 and f_2 are recursive.

12.4.3 Arithmetization

Our aim in this section is to assign numbers to to expressions and sequences of expressions in $\mathscr{L}_{NT}$ and build a (primitive) recursive property $\textsc{prfq}(m, n)$ which is true just in case m numbers a sequence of expressions that is a proof of the expression numbered by n. This requires a number of steps. In this part, we develop at least the notion of a *sentential* proof which should be sufficient for the general idea. The next section develops details for the the full quantificational case.

Gödel numbers. We begin with a strategy familiar from 10.2.2 and 10.3.2 (to which you may find it helpful to refer), now adapted to $\mathscr{L}_{NT}$. The idea is to assign numbers to symbols and expressions of $\mathscr{L}_{NT}$. Then we shall be able to operate on the associated numbers by means of ordinary numerical functions. Insofar as the variable symbols in any quantificational language are countable, they are capable of being sorted into series, x_0, x_1 . . . Supposing that this is done, begin by assigning to each symbol α in $\mathscr{L}_{\text{NT}}$ an integer $g[\alpha]$ called its *Gödel Number*.

a.	$g[(] = 3$	f.	$g[\forall] = 13$
b.	$g[)] = 5$	g.	$g[\emptyset] = 15$
c.	$g[\sim] = 7$	h.	$g[S] = 17$
d.	$g[\rightarrow] = 9$	i.	$g[+] = 19$
e.	$g[=] = 11$	j.	$g[\times] = 21$

k. $g[x_i] = 23 + 2i$

So, for example, $g[x_5] = 23 + 2 \times 5 = 33$. Clearly each symbol gets a unique Gödel number, and Gödel numbers for individual symbols are odd positive integers.[9]

Now we are in a position to assign a Gödel number to each formula as follows: Where $\alpha_0, \alpha_1 \ldots \alpha_n$ are the symbols, in order from left to right, in some expression $\mathcal{Q}$,

$$g[\mathcal{Q}] = 2^{g[\alpha_0]} \times 3^{g[\alpha_1]} \times 5^{g[\alpha_2]} \times \ldots \times \boldsymbol{\pi}_n{}^{g[\alpha_n]}$$

where 2, 3, 5... π_n are the first n prime numbers. So, for example, $g[x_0 \times x_5] = 2^{23} \times 3^{21} \times 5^{33}$. This is a big integer. But it is an integer, and different expressions get different Gödel numbers. Given a Gödel number, we can find the corresponding expression by finding its prime factorization; then if there are twenty-three 2s in the factorization, the first symbol is x_0; if there are twenty-one 3s, the second symbol is $\times$; and so forth. Notice that numbers for individual symbols are odd, where numbers for expressions are even.

Now consider a sequence of expressions, $\mathcal{Q}_0$, $\mathcal{Q}_1 \ldots \mathcal{Q}_n$ (as in an axiomatic derivation). These expressions have Gödel numbers g_0, $g_1 \ldots$, g_n. Then,

$$\boldsymbol{\pi}_0^{g_0} \times \boldsymbol{\pi}_1^{g_1}, \times \boldsymbol{\pi}_2^{g_2} \times \ldots \times \boldsymbol{\pi}_n^{g_n}$$

is the *super* Gödel number for the sequence $\mathcal{Q}_0$, $\mathcal{Q}_1 \ldots \mathcal{Q}_n$. Again, given a super Gödel number, we can find the corresponding expressions by finding its prime factorization; then, if there are g_0 2s, we can proceed to the prime factorization of g_0, to discover the symbols of the first expression; and so forth. Observe that super Gödel numbers are even, but are distinct from Gödel numbers for expressions, insofar as the exponent of 2 in the factorization of any expression is odd (the first element of any expression is a symbol and so has an odd number); and the exponent of 2 in the

[9] There are many ways to do this, we pick just one.

factorization of any super Gödel number is even (the first element of a sequence is an expression and so has an even number).

Recall that $\mathsf{exp}(\mathsf{n},\mathsf{i})$ returns the exponent of π_i in the prime factorization of n. So for a Gödel number n, $\mathsf{exp}(\mathsf{n},\mathsf{i})$ returns the code of α_i; and for a super Gödel number n, $\mathsf{exp}(\mathsf{n},\mathsf{i})$ returns the code of $\mathcal{Q}_i$.

Where $\mathcal{P}$ is any expression, let $\ulcorner\mathcal{P}\urcorner$ be its Gödel number; and $\overline{\ulcorner\mathcal{P}\urcorner}$ the standard numeral for its Gödel number. Indicate individual symbol codes with angle quotes around the symbol. So $\langle\emptyset\rangle = 15$ but $\ulcorner\emptyset\urcorner = 2^{15}$ — for we take the number of the bracketed *expression*.

Concatenation. Suppose m and n number expressions or sequences of expressions. Then the function $\mathsf{cncat}(\mathsf{m},\mathsf{n})$ — ordinarily indicated $\mathsf{m}\star\mathsf{n}$, returns the Gödel number of the expression or sequence with Gödel number m followed by the expression or sequence with Gödel number n. So $\ulcorner x \times y\urcorner \star \ulcorner = z\urcorner = \ulcorner x \times y = z\urcorner$, for some numbered variables x, y and z. This function is (primitive) recursive. Recall that $\mathsf{len}(\mathsf{n})$ is recursive and returns the number of distinct prime factors of n. Set $\mathsf{m}\star\mathsf{n}$ to,

$$(\mu x \leq B_{m,n})[x \geq 1 \wedge (\forall i < len(m))\{exp(x,i) = exp(m,i)\} \wedge (\forall i < len(n))\{exp(x, i + len(m)) = exp(n,i)\}]$$

We search for the least number x (greater than or equal to one) such that exponents of initial primes in its factorization match the exponents of primes in m and exponents of primes later match eponents of primes in n. The bounded quantifiers take $\mathsf{i} < \mathsf{len}(\mathsf{m})$ and $\mathsf{i} < \mathsf{len}(\mathsf{n})$ insofar as len returns the number of primes, but $\mathsf{exp}(\mathsf{x},\mathsf{i})$ starts the list of primes at 0; so if $\mathsf{len}(\mathsf{m}) = 3$, its primes are π_0, π_1 and π_2. So the first $\mathsf{len}(\mathsf{m})$ exponents of x are the same as the exponents in m, and the next $\mathsf{len}(\mathsf{n})$ exponents of x are the same as the exponents in n.

To ensure that the function is recursive, we use the bounded least element quantifier as main operator, where $\mathsf{B}_{\mathsf{m},\mathsf{n}}$ is the bound under which we search for x. In this case it is sufficient to set

$$B_{m,n} = \left(\boldsymbol{\pi}_{len(m)+len(n)}^{m+n}\right)^{len(m)+len(n)}$$

The idea is that all the primes in x will be $\leq \boldsymbol{\pi}_{\mathsf{len(m)+len(n)}}$. And any exponent in the factorization of m must be $\leq \mathsf{m}$ and any exponent for n must be $\leq \mathsf{n}$; so that $\mathsf{m} + \mathsf{n}$ is greater than any exponent in the factorization of x. So B results from multiplying a prime larger than any in x to a power greater than that of any in x together as many times as there are primes in x; so x must be smaller than B.

Observe that corresponding to association for multiplication $(\mathsf{m} \star \mathsf{n}) \star \mathsf{o} = \mathsf{m} \star (\mathsf{n} \star \mathsf{o})$; so we often drop parentheses for the concatenation operation. Also the requirement that $\mathsf{m} \star \mathsf{n} \geq 1$ does not usually matter since we will be interested in cases with $\mathsf{m}, \mathsf{n} > 1$; it does, however have the advantage that $\mathsf{m} \star \mathsf{n}$ is always equivalent to the product of its primes — where this will smooth results down the road (see, for example T13.47i,m).

Terms and Atomics. $\textsc{term}(\mathsf{n})$ is true iff n is the Gödel number of a term. Think of the trees on which we show that an expression is a term. Put formally, for any term t_n, there is a *term sequence* $t_0, t_1 \ldots t_n$ such that each expression is either,

a. $\emptyset$

b. a variable

c. St_j where t_j occurs earlier in the sequence

d. $+t_i t_j$ where t_i and t_j occur earlier in the sequence

e. $\times t_i t_j$ where t_i and t_j occur earlier in the sequence

where we represent terms in unabbreviated form. A term is the last element of such a sequence. Let us try to say this.

First, $\textsc{var}(\mathsf{n})$ is true just in case n is the Gödel number of a variable — conceived as an expression, rather than a symbol. Then $\textsc{var}$ is (primitive) recursive. Set,

$$\textsc{var}(\mathsf{n}) =_{\text{def}} (\exists \mathsf{x} \leq \mathsf{n})(\mathsf{n} = 2^{23+2\mathsf{x}})$$

If there is such an x, then n must be the Gödel number of a variable. And it is clear that this x is less than n itself. So the result is recursive.

Now $\textsc{termseq}(\mathsf{m}, \mathsf{n})$ is true when m is the super Gödel number of a sequence of terms whose last member has Gödel number n. For $\textsc{termseq}(\mathsf{m}, \mathsf{n})$ set,

$$\begin{aligned}
&\mathsf{exp}(\mathsf{m}, \mathsf{len}(\mathsf{m}) \dot{-} 1) = \mathsf{n} \wedge \mathsf{m} > 1 \wedge (\forall \mathsf{k} < \mathsf{len}(\mathsf{m}))\{\\
&\mathsf{exp}(\mathsf{m}, \mathsf{k}) = \ulcorner \emptyset \urcorner \vee \textsc{var}(\mathsf{exp}(\mathsf{m}, \mathsf{k})) \vee\\
&(\exists \mathsf{j} < \mathsf{k})[\mathsf{exp}(\mathsf{m}, \mathsf{k}) = \ulcorner S \urcorner \star \mathsf{exp}(\mathsf{m}, \mathsf{j})] \vee\\
&(\exists \mathsf{i} < \mathsf{k})(\exists \mathsf{j} < \mathsf{k})[\mathsf{exp}(\mathsf{m}, \mathsf{k}) = \ulcorner + \urcorner \star \mathsf{exp}(\mathsf{m}, \mathsf{i}) \star \mathsf{exp}(\mathsf{m}, \mathsf{j})] \vee\\
&(\exists \mathsf{i} < \mathsf{k})(\exists \mathsf{j} < \mathsf{k})[\mathsf{exp}(\mathsf{m}, \mathsf{k}) = \ulcorner \times \urcorner \star \mathsf{exp}(\mathsf{m}, \mathsf{i}) \star \mathsf{exp}(\mathsf{m}, \mathsf{j})]\}
\end{aligned}$$

Recall that $\mathsf{len}(\mathsf{m})$ returns the number of primes in the prime factorization of m; so supposing that m is other than zero or one, $\mathsf{len}(\mathsf{m}) \geq 1$ and if there is one prime it is π_0, if there are two primes they are π_0 and π_1, etc. So the last member of the sequence has Gödel number n and any member of the sequence is a constant or a variable, or made up in the usual way by prior members.

Then set $\textsc{term}(\mathsf{n})$ as follows,

$$\textsc{term}(\mathsf{n}) =_{\text{def}} (\exists \mathsf{x} \leq \mathsf{B_n})\textsc{termseq}(\mathsf{x}, \mathsf{n})$$

If some x numbers a term sequence for n, then n is a term. In this case, Gödel numbers of all prior members in a standard sequence ending in n are less than n. Further, the number of members in the sequence is the same as the number of variables and constants together with the number of function symbols in the term (one member for each variable and constant, and another corresponding to each function symbol); so the number of members in the sequence is the same as $\mathsf{len(n)}$; so all the primes in the sequence are $< \boldsymbol{\pi}_{\mathsf{len(n)}}$. So multiply $\boldsymbol{\pi}^{\mathsf{n}}_{\mathsf{len(n)}}$ together $\mathsf{len(n)}$ times and set $\mathsf{B_n} = (\boldsymbol{\pi}^{\mathsf{n}}_{\mathsf{len(n)}})^{\mathsf{len(n)}}$. We take a prime $\boldsymbol{\pi}_{\mathsf{len(n)}}$ greater than all the primes in the sequence, to a power n greater than all the powers in the sequence, and multiply it together as many times as there are members of the sequence. The result must be greater than x, the number of the term sequence.

Finally $\textsc{atomic}(\mathsf{n})$ is true iff n is the number of an atomic formula. The only atomic formulas of $\mathscr{L}_{NT}$ are of the form $= t_1 t_2$. So it is sufficient to set,

$$\textsc{atomic}(\mathsf{n}) =_{\text{def}} (\exists \mathsf{x} \leq \mathsf{n})(\exists \mathsf{y} \leq \mathsf{n})[\textsc{term}(\mathsf{x}) \wedge \textsc{term}(\mathsf{y}) \wedge \mathsf{n} = \ulcorner = \urcorner \star \mathsf{x} \star \mathsf{y}]$$

Clearly the numbers of t_1 and t_2 are $\leq \mathsf{n}$ itself.

Formulas. $\textsc{wff}(\mathsf{n})$ is to be true iff n is the number of a (well-formed) formula. Again, think of the tree by which a formula is formed. There is a sequence of which each member is,

a. an atomic

b. $\sim\mathcal{P}$ for some previous member of the sequence $\mathcal{P}$

c. $(\mathcal{P} \rightarrow \mathcal{Q})$ for previous members of the sequence $\mathcal{P}$ and $\mathcal{Q}$

d. $\forall x \mathcal{P}$ for some previous member of the sequence $\mathcal{P}$ and variable x

So, on the model of what has gone before, we let $\textsc{formseq}(\mathsf{m}, \mathsf{n})$ be true when m is the super Gödel number of a sequence of formulas whose last member has Gödel number n. For $\textsc{formseq}(\mathsf{m}, \mathsf{n})$ set,

$\mathsf{exp}(m, \mathsf{len}(m) \dot{-} 1) = n \wedge m > 1 \wedge (\forall k < \mathsf{len}(m))\{$
$\textsc{atomic}(\mathsf{exp}(m, k)) \vee$
$(\exists j < k)[\mathsf{exp}(m, k) = \ulcorner\sim\urcorner \star \mathsf{exp}(m, j)] \vee$
$(\exists i < k)(\exists j < k)[\mathsf{exp}(m, k) = \ulcorner(\urcorner \star \mathsf{exp}(m, i) \star \ulcorner\rightarrow\urcorner \star \mathsf{exp}(m, j) \star \ulcorner)\urcorner] \vee$
$(\exists i < k)(\exists j < n)[\textsc{var}(j) \wedge \mathsf{exp}(m, k) = \ulcorner\forall\urcorner \star j \star \mathsf{exp}(m, i)]\}$

So a formula is the last member of a sequence each member of which is an atomic, or formed from previous members in the usual way. Clearly the number of a variable in an expression with number n is itself $\leq n$. Then,

$$\textsc{wff}(n) =_{\text{def}} (\exists x \leq B_n)\textsc{formseq}(x, n)$$

An expression is a formula iff there is a formula sequence of which it is the last member. Again, Gödel numbers of prior formulas in a standard sequence are $\leq n$. And there are as many members of the sequence as there are atomics and operator symbols in the formula numbered n. So all the primes are $\leq \boldsymbol{\pi}_{\mathsf{len}(n)}$; so multiply $\boldsymbol{\pi}^n_{\mathsf{len}(n)}$ together $\mathsf{len}(n)$ times and set $B_n = \left(\boldsymbol{\pi}^n_{\mathsf{len}(n)}\right)^{\mathsf{len}(n)}$.

Sentential Proof. $\textsc{prfads}(m, n)$ is to be true iff m is the super Gödel number of a sequence of formulas that is a (sentential) proof of the formula with Gödel number n. We revert to the relatively simple axiomatic system of chapter 3. So, for example, A1 is of the sort, $(\mathcal{P} \rightarrow (\mathcal{Q} \rightarrow \mathcal{P}))$, and the only rule is MP. For the sentential case we need, $\textsc{axiomads}(n)$ true when n is the number of an axiom. For this,

$\textsc{axiomad1}(n) =_{\text{def}} (\exists x \leq n)(\exists y \leq n)[\textsc{wff}(x) \wedge \textsc{wff}(y) \wedge n = \ulcorner(\urcorner \star x \star \ulcorner\rightarrow\urcorner \star \ulcorner(\urcorner \star y \star \ulcorner\rightarrow\urcorner \star x \star \ulcorner))\urcorner]$
$\textsc{axiomad2}(n) =_{\text{def}}$ Homework.
$\textsc{axiomad3}(n) =_{\text{def}}$ Homework.

Then,

$$\textsc{axiomads}(n) =_{\text{def}} \textsc{axiomad1}(n) \vee \textsc{axiomad2}(n) \vee \textsc{axiomad3}(n)$$

In the next section, we will add all the logical axioms plus the axioms for Q. But this is all that is required for proofs of theorems of sentential logic.

Now $\mathsf{cnd}(n, o) = m$ when $n = \ulcorner\mathcal{P}\urcorner$, $o = \ulcorner\mathcal{Q}\urcorner$ and $m = \ulcorner(\mathcal{P} \rightarrow \mathcal{Q})\urcorner$; for good measure we include $\mathsf{neg}(n)$ and $\mathsf{unv}(v, n)$. And $\textsc{mp}(m, n, o)$ is true when the formula with Gödel number o follows from ones with numbers m and n.

$$\mathsf{cnd}(n, o) = \ulcorner(\urcorner \star n \star \ulcorner\rightarrow\urcorner \star o \star \ulcorner)\urcorner$$

$$\mathsf{neg}(n) = \ulcorner\sim\urcorner \star n$$

$$\mathsf{unv}(v, n) = \ulcorner\forall\urcorner \star v \star n$$

$$\textsc{mp}(m, n, o) =_{\text{def}} \mathsf{cnd}(n, o) = m$$

So for MP, m numbers the conditional, n its antecedent, and o the consequent.

And PRFADS(m, n) when m is the super Gödel number of a sequence that is a proof whose last member has Gödel number n. This works like TERMSEQ and FORMSEQ. For PRFADS set,

$$\mathsf{exp}(m, \mathsf{len}(m) \dot{-} 1) = n \wedge m > 1 \wedge (\forall k < \mathsf{len}(m))\{$$
$$\textsc{axiomads}(\mathsf{exp}(m, k)) \vee$$
$$(\exists i < k)(\exists j < k)\textsc{mp}(\mathsf{exp}(m, i), \mathsf{exp}(m, j), \mathsf{exp}(m, k))\}$$

So every formula is either an axiom or follows from previous members by MP. It is a significant matter to have shown that there is such a function! Again, in the next section, we will extend this notion to include the rule Gen.

This construction for PRFADS exhibits the essential steps that are required for the parallel relation PRFQ(m, n) for theorems of Q. That discussion is taken up in the following section, and adds considerable detail. It is not clear that the detail is required for understanding results to follow — though of course, to the extent that those results rely on the recursive PRFQ relation, the detail underlies *proof* of the results!

E12.26. Find Gödel numbers for each of the following. Treat the first as an expression, rather than as simple symbol; the last is a sequence of expressions. For the latter two, you need not do the calculation!

$$x_2 \qquad x_0 = x_1 \qquad x_0 = x_1, \emptyset = x_0, \emptyset = x_1$$

E12.27. Complete the cases for AXIOMAD2(n) and AXIOMAD3(n).

E12.28. In chapter 8 we define the notion of a *normal* sentential form (p. 393). Supposing that our numbering system is modified to include $\ulcorner\vee\urcorner$ and $\ulcorner\wedge\urcorner$ and using ATOMIC from above, define a recursive relation NORM(n) for $\mathscr{L}_{NT}$. Hint: You will need a formula sequence to do this.

12.4.4 Completing the Construction

Quantifier rules for derivations include axioms like (A4), $(\forall v \mathcal{P} \to \mathcal{P}^{v}_{s})$ where term s is free for variable v in $\mathcal{P}$. This is easy enough to apply in practice. But it takes some work to represent. We tackle the problem piece-by-piece.

Substitution in terms. Say $\mathsf{t} = \ulcorner t \urcorner$, $\mathsf{v} = \ulcorner v \urcorner$, and $\mathsf{s} = \ulcorner s \urcorner$ for some terms s, t, and variable v. Then $\textsc{termsub}(\mathsf{t}, \mathsf{v}, \mathsf{s}, \mathsf{u})$ is true when u is the Gödel number of t^{v}_{s}. For this, we begin with a term sequence (with Gödel number m) for t, and consider a parallel sequence, not necessarily a term sequence (with Gödel number n), that includes modified versions of the terms in the sequence with Gödel number m. For $\textsc{tsubseq}(\mathsf{m}, \mathsf{n}, \mathsf{t}, \mathsf{v}, \mathsf{s}, \mathsf{u})$ set,

$$
\begin{aligned}
&\textsc{termseq}(\mathsf{m},\mathsf{t}) \wedge \mathsf{len}(\mathsf{m}) = \mathsf{len}(\mathsf{n}) \wedge \mathsf{exp}(\mathsf{n}, \mathsf{len}(\mathsf{n}) \dot{-} 1) = \mathsf{u} \wedge (\forall \mathsf{k} < \mathsf{len}(\mathsf{m}))\{\\
&[\mathsf{exp}(\mathsf{m},\mathsf{k}) = \ulcorner \emptyset \urcorner \wedge \mathsf{exp}(\mathsf{n},\mathsf{k}) = \ulcorner \emptyset \urcorner] \vee\\
&[\textsc{var}(\mathsf{exp}(\mathsf{m},\mathsf{k})) \wedge \mathsf{exp}(\mathsf{m},\mathsf{k}) \neq \mathsf{v} \wedge \mathsf{exp}(\mathsf{n},\mathsf{k}) = \mathsf{exp}(\mathsf{m},\mathsf{k})] \vee\\
&[\textsc{var}(\mathsf{exp}(\mathsf{m},\mathsf{k})) \wedge \mathsf{exp}(\mathsf{m},\mathsf{k}) = \mathsf{v} \wedge \mathsf{exp}(\mathsf{n},\mathsf{k}) = \mathsf{s}] \vee\\
&(\exists \mathsf{i} < \mathsf{k})[\mathsf{exp}(\mathsf{m},\mathsf{k}) = \ulcorner S \urcorner \star \mathsf{exp}(\mathsf{m},\mathsf{i}) \wedge \mathsf{exp}(\mathsf{n},\mathsf{k}) = \ulcorner S \urcorner \star \mathsf{exp}(\mathsf{n},\mathsf{i})] \vee\\
&(\exists \mathsf{i} < \mathsf{k})(\exists \mathsf{j} < \mathsf{k})[\mathsf{exp}(\mathsf{m},\mathsf{k}) = \ulcorner + \urcorner \star \mathsf{exp}(\mathsf{m},\mathsf{i}) \star \mathsf{exp}(\mathsf{m},\mathsf{j}) \wedge \mathsf{exp}(\mathsf{n},\mathsf{k}) = \ulcorner + \urcorner \star \mathsf{exp}(\mathsf{n},\mathsf{i}) \star \mathsf{exp}(\mathsf{n},\mathsf{j})] \vee\\
&(\exists \mathsf{i} < \mathsf{k})(\exists \mathsf{j} < \mathsf{k})[\mathsf{exp}(\mathsf{m},\mathsf{k}) = \ulcorner \times \urcorner \star \mathsf{exp}(\mathsf{m},\mathsf{i}) \star \mathsf{exp}(\mathsf{m},\mathsf{j}) \wedge \mathsf{exp}(\mathsf{n},\mathsf{k}) = \ulcorner \times \urcorner \star \mathsf{exp}(\mathsf{n},\mathsf{i}) \star \mathsf{exp}(\mathsf{n},\mathsf{j})]\}
\end{aligned}
$$

So the sequence for t^{v}_{s} (numbered by n) is like one of our "unabbreviating trees" from chapter 2. In any place where the sequence for t (numbered by m) numbers $\emptyset$, the sequence for t^{v}_{s} numbers $\emptyset$. Where the sequence for t numbers a variable other than v, the sequence for t^{v}_{s} numbers the same variable. But where the sequence for t numbers variable v, the sequence for t^{v}_{s} numbers s. Then later parts are built out of prior in parallel. The second sequence may not itself be a *term* sequence, insofar as it need not include all the antecedents to s (just as an unabbreviating tree would not include all the parts of a resultant term or formula).

Now set $\textsc{termsub}(\mathsf{t}, \mathsf{v}, \mathsf{s}, \mathsf{u})$ as follows,

$$\textsc{termsub}(\mathsf{t},\mathsf{v},\mathsf{s},\mathsf{u}) =_{\text{def}} (\exists \mathsf{x} \leq \mathsf{X})(\exists \mathsf{y} \leq \mathsf{Y})\textsc{tsubseq}(\mathsf{x},\mathsf{y},\mathsf{t},\mathsf{v},\mathsf{s},\mathsf{u})$$

In this case, reasoning as for $\textsc{wff}$, the Gödel numbers in a standard sequence with number m are less than t and numbers in the sequence with number n less than u. And primes in the sequence range up to $\boldsymbol{\pi}_{\mathsf{len(t)}}$. So it is sufficient to set $\mathsf{X} = \left(\boldsymbol{\pi}^{\mathsf{t}}_{\mathsf{len(t)}}\right)^{\mathsf{len(t)}}$ and $\mathsf{Y} = \left(\boldsymbol{\pi}^{\mathsf{u}}_{\mathsf{len(t)}}\right)^{\mathsf{len(t)}}$.

Substitution in atomics. Say $\mathsf{p} = \ulcorner \mathcal{P} \urcorner$, $\mathsf{v} = \ulcorner v \urcorner$, and $\mathsf{s} = \ulcorner s \urcorner$ for some atomic formula $\mathcal{P}$, variable v and term s. Then $\textsc{atomsub}(\mathsf{p}, \mathsf{v}, \mathsf{s}, \mathsf{q})$ is true when q is the Gödel number of $\mathcal{P}^{v}_{s}$. The condition is straightforward given TERMSUB. For $\textsc{atomsub}(\mathsf{p}, \mathsf{v}, \mathsf{s}, \mathsf{q})$,

$$(\exists a \le p)(\exists b \le p)(\exists a' \le q)(\exists b' \le q)[\textsc{term}(a) \wedge \textsc{term}(b) \wedge p = \ulcorner = \urcorner \star a \star b \wedge \textsc{termsub}(a, v, s, a') \wedge \textsc{termsub}(b, v, s, b') \wedge q = \ulcorner = \urcorner \star a' \star b']$$

$\mathcal{P}^{v}_{s}$ simply substitutes into the terms on either side of the equal sign.

Substitution into formulas. Where $\mathsf{p} = \ulcorner \mathcal{P} \urcorner$, $\mathsf{v} = \ulcorner v \urcorner$, and $\mathsf{s} = \ulcorner s \urcorner$ for an arbitrary formula $\mathcal{P}$, variable v and term s, $\textsc{formsub}(\mathsf{p}, \mathsf{v}, \mathsf{s}, \mathsf{q})$ is true when q is the Gödel number of $\mathcal{P}^{v}_{s}$. In the general case, $\mathcal{P}^{v}_{s}$ is complicated insofar as s replaces only *free* instances of v. Again, we build a parallel sequence with number n. No replacements are carried forward in subformulas beginning with a quantifier binding instances of variable v. For $\textsc{fsubseq}(\mathsf{m}, \mathsf{n}, \mathsf{p}, \mathsf{v}, \mathsf{s}, \mathsf{q})$ set,

$$\begin{aligned}
&\textsc{formseq}(m, p) \wedge len(m) = len(n) \wedge exp(n, len(n) \dot{-} 1) = q \wedge (\forall k < len(m))\{\\
&[\textsc{atomic}(exp(m, k)) \wedge \textsc{atomsub}(exp(m, k), v, s, exp(n, k))] \vee\\
&(\exists i < k)[exp(m, k) = neg(exp(m, i)) \wedge exp(n, k) = neg(exp(n, i))] \vee\\
&(\exists i < k)(\exists j < k)[exp(m, k) = cnd(exp(m, i), exp(m, j)) \wedge exp(n, k) = cnd(exp(n, i), exp(n, j))] \vee\\
&(\exists i < k)(\exists j < p)[\textsc{var}(j) \wedge j \neq v \wedge exp(m, k) = unv(j, exp(m, i)) \wedge exp(n, k) = unv(j, exp(n, i))] \vee\\
&(\exists i < k)(\exists j < p)[\textsc{var}(j) \wedge j = v \wedge exp(m, k) = unv(j, exp(m, i)) \wedge exp(n, k) = exp(m, k)]\}
\end{aligned}$$

So substitutions are made in atomics, and carried forward in the parallel sequence — so long as no quantifier binds variable v, at which stage, the sequence reverts to the form without substitution.

And $\textsc{formsub}(\mathsf{p}, \mathsf{v}, \mathsf{s}, \mathsf{q})$ is,

$$\textsc{formsub}(p, v, s, q) =_{\text{def}} (\exists x \le X)(\exists y \le Y)\textsc{fsubseq}(x, y, p, v, s, q)$$

Again, set $X = \left(\pi^{p}_{len(p)}\right)^{len(p)}$ and $Y = \left(\pi^{q}_{len(p)}\right)^{len(p)}$.

Given $\textsc{formsub}(\mathsf{p}, \mathsf{v}, \mathsf{s}, \mathsf{q})$, there is a corresponding function $formusb(\mathsf{p}, \mathsf{v}, \mathsf{s}) = (\mu q \le Z)\textsc{formsub}(\mathsf{p}, \mathsf{v}, \mathsf{s}, \mathsf{q})$. In this case, the number of symbols in $\mathcal{P}^{v}_{s}$ is sure to be no greater than the number of symbols in $\mathcal{P}$ times the number of symbols in s. And any symbol is s or an element of $\mathcal{P}$; so the Gödel number of each symbol is no greater than the maximum of p and s and thus $\mathsf{p} + \mathsf{s}$. So it is sufficient to set $Z = \left(\pi^{p+s}_{len(p)\times len(s)}\right)^{len(p)\times len(s)}$. Again, we take a prime at least great as that of any symbol, to a power greater than that of any exponent, and multiply it as many times as there are symbols.

Free and bound variables. $\text{FREE}(p, v)$ is true when v is the Gödel number of a variable that is free in a term or formula with Gödel number p. For a given variable x_i initially assigned number $23 + 2i$, $\ulcorner x_i \urcorner = 2^{23+2i}$; and $\ulcorner x_{i+1} \urcorner \times 2^2 = 2^{23+2i+2}$ is the number of the next variable. In particular then, for v the number of a variable, $v \times 2^2$ (that is $v \times 4$) numbers a different variable. The idea is that if there is some change in an expression upon substitution of a variable different from v, then v must have been free in the original expression. For terms and formulas respectively,

$$\text{FREEt}(t, v) =_{\text{def}} \sim\text{TERMSUB}(t, v, v \times 4, t)$$

$$\text{FREEf}(p, v) =_{\text{def}} \sim\text{FORMSUB}(p, v, v \times 4, p)$$

So v is free if the result upon substitution is other than the original expression.

Given $\text{FREEf}(p, v)$, it is a simple matter to specify $\text{SENT}(n)$ true when n numbers a sentence.

$$\text{SENT}(n) =_{\text{def}} \text{WFF}(n) \wedge (\forall x < n)[\text{VAR}(x) \rightarrow \sim\text{FREEf}(n, x)]$$

So n numbers a sentence if it numbers a formula and nothing is a number of a variable free in the formula numbered by n.

Finally, suppose $s = \ulcorner s \urcorner$ and $v = \ulcorner v \urcorner$; then $\text{FREEFOR}(s, v, u)$ is true iff s is free for v in the formula numbered by u. For this, we set up a modified formula sequence, that identifies just "admissable" subformulas — ones where s is free for v in the formula numbered by u. For $\text{FFSEQ}(m, s, v, u)$ set,

$$\exp(m, \text{len}(m) \dot{-} 1) = u \wedge m > 1 \wedge (\forall k < \text{len}(m))\{$$
$$\text{ATOMIC}(\exp(m, k)) \vee$$
$$(\exists j < k)[\exp(m, k) = \text{neg}(\exp(m, j))] \vee$$
$$(\exists i < k)(\exists j < k)[\exp(m, k) = \text{cnd}(\exp(m, i), \exp(m, j))] \vee$$
$$(\exists p \leq u)[\text{WFF}(p) \wedge \exp(m, k) = \text{unv}(v, p)] \vee$$
$$(\exists i < k)(\exists j \leq u)[\text{VAR}(j) \wedge j \neq v \wedge (\sim\text{FREEt}(s, j) \vee \sim\text{FREEf}(\exp(m, i), v)) \wedge \exp(m, k) = \text{unv}(j, \exp(m, i))]\}$$

If the main operator of a subformula $\mathcal{Q}$ binds variable v, then no variables in s are bound upon substitution, because there are no substitutions — as only free instances of v are replaced; observe that this $\mathcal{Q}$ need not appear earlier in the sequence, as any formula with the v quantifier satisfies the condition. Alternatively, if the main operator binds a different variable, we require either that the variable is not free in s (so that no instances are bound upon substitution) or that v is not free in $\mathcal{Q}$ (so that there are no substitutions). Given this,

$$\text{FREEFOR}(s, v, u) =_{\text{def}} (\exists x \leq B_u)\text{FFSEQ}(x, s, v, u)$$

In this case, every member of the sequence for FFSEQ is a member of the FORMSEQ for u so $\mathsf{B_u}$ may be set as before.

Proofs. After all this work, we are finally ready for all the axioms of AD and of Q. AXIOMAD4(n) obtains when n is the Gödel number of an instance of A4. Intuitively, AXIOMAD4(n) just in case there is an s such that,

$$(\exists p \leq n)(\exists v \leq n)[\text{WFF}(p) \wedge \text{VAR}(v) \wedge \text{TERM}(s) \wedge \text{FREEFOR}(s, v, p) \wedge n = \text{cnd}(\text{unv}(v, p), \text{formsub}(p, v, s))]$$

So there is a formula $\mathcal{P}$, variable v and term s where s is free for v in $\mathcal{P}$; and the axiom is of the form, $(\forall v \mathcal{P} \rightarrow \mathcal{P}^v_s)$. Unfortunately, our statement is inadequate insofar as s is left free. We cannot simply supply a prefix ∃s as the result would not be recursively specified. It is tempting to add a bounded $(\exists s \leq n)$ with the idea that the number of s must be smaller than the number of $\mathcal{P}^v_s$. This almost works. The difficulty is the (rarely encountered) situation where the quantified variable v is not free in $\mathcal{P}$ (as when a quantifier is added to some $\mathcal{P}$ that is already a sentence); in this case, $\mathcal{P}^v_s$ is just $\mathcal{P}$, and there is nothing to say that s is less than n. Here is a way to do the job. Set AXIOMAD4(n) as,

$$\begin{aligned}&(\exists p \leq n)(\exists v \leq n)\{\text{WFF}(p) \wedge \text{VAR}(v) \wedge [\\ &\quad (\sim\text{FREE}(v, p) \wedge n = \text{cnd}(\text{unv}(v, p), p)) \vee \\ &\quad (\exists s \leq n)(\text{FREE}(v, p) \wedge \text{TERM}(s) \wedge \text{FREEFOR}(s, v, p) \wedge n = \text{cnd}(\text{unv}(v, p), \text{formsub}(p, v, s))]\}\end{aligned}$$

When $\sim\text{FREE}(v, p)$, $p = \text{formsub}(p, v, s)$; and when $\text{FREE}(v, p)$, $s \leq \text{formsub}(p, v, s)$. Either way, n is set to $\text{cnd}(\text{unv}(v, p), \text{formsub}(p, v, s))$. The result, then is primitive recursive and equivalent to our original intuitive specification.

Given what we have done, AXIOMAD5(n) is straightforward. GEN(m, n) holds when n is the Gödel number of a formula that follows by Gen from a formula with Gödel number m. And axioms for equality are not hard. A couple are worked as examples. For AXIOMAD6(n),

$$\text{AXIOMAD6}(n) =_{\text{def}} (\exists v \leq n)[\text{VAR}(v) \wedge n = v \star \ulcorner = \urcorner \star v]$$

For "simplicity" I drop the unabbreviated style of the original formulas. Axiom seven is of the sort, $(x_i = y) \rightarrow (h^n x_1 \ldots x_i \ldots x_n = h^n x_1 \ldots y \ldots x_n)$ for relation symbol h and variables $x_1 \ldots x_n$ and y. In $\mathcal{L}_{NT}$ the function symbol is S, $+$ or $\times$. Because just a single replacement is made, we do not want to use TERMSUB. However, we are in a position simply to list all the combinations in which one variable is replaced. So, for AXIOMAD7(n),

$$(\exists s \le n)(\exists t \le n)(\exists x \le n)(\exists y \le n)\{\textsc{var}(x) \land \textsc{var}(y) \land n = \ulcorner(=\urcorner \star x \star y \star \ulcorner\to\ =\urcorner \star s \star t \star \ulcorner)\urcorner \land$$
$$([s = \ulcorner S\urcorner \star x \land t = \ulcorner S\urcorner \star y] \lor$$
$$(\exists z < n)[\textsc{var}(z) \land ((s = \ulcorner+\urcorner \star x \star z \land t = \ulcorner+\urcorner \star y \star z) \lor (s = \ulcorner+\urcorner \star z \star x \land t = \ulcorner+\urcorner \star z \star y))] \lor$$
$$(\exists z < n)[\textsc{var}(z) \land ((s = \ulcorner\times\urcorner \star x \star z \land t = \ulcorner\times\urcorner \star y \star z) \lor (s = \ulcorner\times\urcorner \star z \star x \land t = \ulcorner\times\urcorner \star z \star y))])\}$$

So there is a term s and a term t which replaces one instance of x in s with y. Then the axiom is of the sort $=xy \to\ =st$. Axiom eight is similar. It is stated in terms of atomics of the sort $\mathcal{R}^n x_1 \dots x_n$ for relation symbol $\mathcal{R}$ and variables $x_1 \dots x_n$. In $\mathcal{L}_{NT}$ the relation symbol is the equals sign, so these atomics are of the form, $x = y$. Again, because just a single replacement is made, we do not want to use FORMSUB. However, we may proceed by analogy with AXIOMAD7. This is left as an exercise. Thus we have a complete AXIOMAD and with that PRFAD. For the latter, it is convenient to introduce a relation ICON(m, n, o) true when the formula with Gödel number o is an *immediate consequence* of ones numbered m and n

$$\textsc{icon}(m,n,o) =_{def} \textsc{mp}(m,n,o) \lor (m = n \land \textsc{gen}(n,o))$$

The axioms of Q are particular sentences. So, for example, axiom Q2 is of the sort, $(Sx = Sy) \to (x = y)$. Let x and y be x_0 and x_1 respectively. Then,

$$\textsc{axiomq2}(n) =_{def} n = \ulcorner(Sx = Sy) \to (x = y)\urcorner$$

For "ease of reading," I do not reduce it to unabbreviated form. Other axioms of Q may be treated in the same way. And now it is straightforward to produce AXIOMQ(n) and PRFQ(m, n).

It is worth noting that with AXIOMPA7(n),

$$(\exists p \le n)(\exists v \le n)[\textsc{wff}(p) \land \textsc{var}(v) \land n =$$
$$cnd(neg(cnd(formsub(p, v, \ulcorner\emptyset\urcorner), neg(unv(v, cnd(p, formsub(p, v, \ulcorner S\urcorner\star v)))))), unv(v, p))]$$

we have also AXIOMPA(n) and PRFPA(m, n) for PA.[10]

It is a significant matter to have found these functions. Now we put them to work.

*E12.29. (i) Complete the construction with recursive relations for AXIOMAD5(n), GEN(m, n), AXIOMAD8(n), and so AXIOMAD(n) and PRFAD(m, n). (ii) Complete the remaining axioms for Robinson arithmetic, and then AXIOMQ(n) and PRFQ(m, n). (iii) Construct also AXIOMQP(n), like AXIOMQ less AXIOMQ7, and then AXIOMPA(n) and PRFPA(m, n).

[10] If you follow it out, the last line above unpacks to,

$$\ulcorner(\sim(\urcorner * formsub(p, v, \ulcorner\emptyset\urcorner) * \ulcorner\to \sim\forall\urcorner * v * \ulcorner(\urcorner * p * \ulcorner\to\urcorner * formsub(p, v, \ulcorner S\urcorner \star v) * \ulcorner)) \to \forall\urcorner * v * p * \ulcorner)\urcorner$$

which numbers instances of PA7 (where the conjunction is unpacked to its primitive form).

E12.30. Supposing now that our numbering system is modified to include $\ulcorner\vee\urcorner$, $\ulcorner\wedge\urcorner$ and $\ulcorner\exists\urcorner$, and with the obvious modification of FORMSEQ to accommodate the new operators and with functions dsj, cnj and exs, construct function UNABBSEQ(m, n, p, q) such that m numbers a formula sequence for p (which may contain abbreviations) and n numbers a sequence whose last member is the unabbreviated version of p. Then construct UNABB(p, q) where q is the number of the unabbreviation of p. Hint you may want to think again about "unabbreviating trees" from chapter 2 along with FSUBSEQ as a model.

12.5 Essential Results

In this section, we develop some first fruits of our labor. We shall need some initial theorems, important in their own right. With these theorems in hand, our results follow in short order. The results are developed and extended in later chapters. But it is worth putting them on the table at the start. (And some results at this stage provide a fitting cap to our labors.) We have expended a great deal of energy showing that, under appropriate conditons, recursive functions can be expressed and captured, and then that there exist certain recursive functions and relations including PRFQ. Now we put these results to work.

12.5.1 Preliminary Theorems

A couple of definitions: If f is a function from (an initial segment of) N onto some set — so that the objects in the set are f(0), f(1)... say f *enumerates* the members of the set. A set is *recursively* enumerable if there is a recursive function that enumerates it. Also, say T is a *recursively axiomatized* formal theory if there is a recursive relation PRFT(m, n) which holds just in case m is the super Gödel number of a proof in T of the formula with Gödel number n. We have seen that Q is recursively axiomatized; but so is PA and any reasonable theory whose axioms and rules are recursively described.

T12.17. If T is a recursively axiomatized formal theory then the set of theorems of T is recursively enumerable.

Consider pairs $\langle p, t\rangle$ where p numbers a proof of the theorem numbered t, each such pair itself associated with a number, $2^p \times 3^t$. Then there is a recursive function from the integers to these *codes* as follows.

$$\text{code}(0) = \mu z(\exists p < z)(\exists t < z)[z = 2^p \times 3^t \wedge \text{PRFT}(p, t)]$$

First Results of Chapter 12

T12.1 For an interpretation with the required variable-free terms: (a) If $\mathcal{R}$ is a relation symbol and R is a relation, and $\mathsf{I}[\mathcal{R}] = \mathsf{R}(\mathsf{x}_1 \dots \mathsf{x}_n)$, then $\mathsf{R}(\mathsf{x}_1 \dots \mathsf{x}_n)$ is expressed by $\mathcal{R}x_1 \dots x_n$. And (b) if h is a function symbol and h is a function and $\mathsf{I}[h] = \mathsf{h}(\mathsf{x}_1 \dots \mathsf{x}_n)$ then $\mathsf{h}(\mathsf{x}_1 \dots \mathsf{x}_n)$ is expressed by $hx_1 \dots x_n = v$.

T12.2 Suppose total function $\mathsf{f}(\mathsf{x}_1 \dots \mathsf{x}_n)$ is expressed by formula $\mathcal{F}(x_1 \dots x_n, y)$; then if $\langle\langle \mathsf{m}_1 \dots \mathsf{m}_n\rangle, \mathsf{a}\rangle \notin \mathsf{f}$, $\mathsf{I}[\sim\mathcal{F}(\overline{\mathsf{m}}_1 \dots \overline{\mathsf{m}}_n, \overline{\mathsf{a}})] = \mathsf{T}$.

T12.3 On the standard interpretation N of $\mathcal{L}_{NT}$, each recursive function $\mathsf{f}(\vec{\mathsf{x}})$ is expressed by some formula $\mathcal{F}(\vec{x}, v)$. Corollary: On the standard interpretation N of $\mathcal{L}_{NT}$, each recursive relation $\mathsf{R}(\vec{\mathsf{x}})$ is expressed by some formula $\mathcal{R}(\vec{x})$.

T12.4 If T includes Q and total function $\mathsf{f}(\mathsf{x}_1 \dots \mathsf{x}_n)$ is captured by formula $\mathcal{F}(x_1 \dots x_n, y)$ so that conditions (f.i) and (f.ii) hold, then if $\langle\langle \mathsf{m}_1 \dots \mathsf{m}_n\rangle, \mathsf{a}\rangle \notin \mathsf{f}$ then $T \vdash \sim\mathcal{F}(\overline{\mathsf{m}}_1 \dots \overline{\mathsf{m}}_n, \overline{\mathsf{a}})$.

T12.5 On the standard interpretation N for $\mathcal{L}_{NT}$, (i) $\mathsf{N_d}[s \leq t] = \mathsf{S}$ iff $\mathsf{N_d}[s] \leq \mathsf{N_d}[t]$, and (ii) $\mathsf{N_d}[s < t] = \mathsf{S}$ iff $\mathsf{N_d}[s] < \mathsf{N_d}[t]$.

T12.6 On the standard interpretation N for $\mathcal{L}_{NT}$, (i) $\mathsf{N_d}[(\forall x \leq t)\mathcal{P}] = \mathsf{S}$ iff for every $\mathsf{m} \leq \mathsf{N_d}[t]$, $\mathsf{N}_{\mathsf{d}(x|\mathsf{m})}[\mathcal{P}] = \mathsf{S}$ and (ii), $\mathsf{N_d}[(\forall x < t)\mathcal{P}] = \mathsf{S}$ iff for every $\mathsf{m} < \mathsf{N_d}[t]$, $\mathsf{N}_{\mathsf{d}(x|\mathsf{m})}[\mathcal{P}] = \mathsf{S}$.

T12.7 On the standard interpretation N for $\mathcal{L}_{NT}$, (i) $\mathsf{N_d}[(\exists x \leq t)\mathcal{P}] = \mathsf{S}$ iff for some $\mathsf{m} \leq \mathsf{N_d}[t]$, $\mathsf{N}_{\mathsf{d}(x|\mathsf{m})}[\mathcal{P}] = \mathsf{S}$ and (ii), $\mathsf{N_d}[(\exists x < t)\mathcal{P}] = \mathsf{S}$ iff for some $\mathsf{m} < \mathsf{N_d}[t]$, $\mathsf{N}_{\mathsf{d}(x|\mathsf{m})}[\mathcal{P}] = \mathsf{S}$.

T12.8 For any Δ_0 sentence $\mathcal{P}$, if $\mathsf{N}[\mathcal{P}] = \mathsf{T}$, then Q $\vdash_{ND} \mathcal{P}$, and if $\mathsf{N}[\mathcal{P}] \neq \mathsf{T}$, then Q $\vdash_{ND} \sim\mathcal{P}$.

T12.9 For any Σ_1 sentence $\mathcal{P}$ if $\mathsf{N}[\mathcal{P}] = \mathsf{T}$, then Q $\vdash_{ND} \mathcal{P}$.

T12.10 The original formula by which any recursive function is expressed is Σ_1.

T12.11 On the standard interpretation N for $\mathcal{L}_{NT}$, any recursive formula is captured by the original formula by which it is expressed in $\mathrm{Q_s}$.

T12.12 Suppose $\mathsf{f}(\vec{\mathsf{x}}, \mathsf{y})$ results by recursion from functions $\mathsf{g}(\vec{\mathsf{x}})$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$ where $\mathsf{g}(\vec{\mathsf{x}})$ is captured by some $\mathcal{G}(\vec{x}, z)$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$ by $\mathcal{H}(\vec{x}, y, u, z)$. Then for the original expression $\mathcal{F}(\vec{x}, y, z)$ of $\mathsf{f}(\vec{\mathsf{x}}, \mathsf{y})$, if $\langle\langle \mathsf{m}_1 \dots \mathsf{m}_b, \mathsf{n}\rangle, \mathsf{a}\rangle \in \mathsf{f}$, $\mathrm{Q_s} \vdash \forall w[\mathcal{F}(\overline{\mathsf{m}}_1 \dots \overline{\mathsf{m}}_b, \overline{\mathsf{n}}, w) \rightarrow w = \overline{\mathsf{a}}]$.

T12.13 If a total function $\mathsf{f}(\mathsf{x}_1 \dots \mathsf{x}_n)$ is expressed by a Δ_0 formula $\mathcal{F}(x_1 \dots x_n, y)$, then there is a Δ_0 formula $\mathcal{F}'$ that captures f in Q.

T12.14 For $\mathcal{F}'(\vec{x}, y) =_{\text{def}} \mathcal{F}(\vec{x}, y) \wedge (\forall z \leq y)[\mathcal{F}(\vec{x}, z) \rightarrow z = y]$, and for any n, Q $\vdash \forall\vec{x}\forall y[(\mathcal{F}'(\vec{x}, \overline{\mathsf{n}}) \wedge \mathcal{F}'(\vec{x}, y)) \rightarrow y = \overline{\mathsf{n}}]$.

T12.15 If $\mathcal{F}(\vec{x}, y)$ expresses a total $\mathsf{f}(\vec{\mathsf{x}})$, then $\mathcal{F}'(\vec{x}, y) = \mathcal{F}(\vec{x}, y) \wedge (\forall z < y)[\mathcal{F}(\vec{x}, z) \rightarrow z = y]$ expresses $\mathsf{f}(\vec{\mathsf{x}})$.

T12.16 Any recursive function is captured by a Σ_1 formula in Q. Corollary: Any recursive relation is captured by a Σ_1 formula in Q.

$$\mathsf{code(Sn)} = \mu \mathsf{z}(\exists \mathsf{p} < \mathsf{z})(\exists \mathsf{t} < \mathsf{z})[\mathsf{z} > \mathsf{code(n)} \wedge \mathsf{z} = 2^{\mathsf{p}} \times 3^{\mathsf{t}} \wedge \textsc{prft}(\mathsf{p}, \mathsf{t})]$$

So $\mathsf{0}$ is associated with the least integer that codes a proof of a sentence, $\mathsf{1}$ with the next, and so forth. Then,

$$\mathsf{enum(n)} = \mathsf{exp(code(n), 1)}$$

returns the Gödel number of theorem n in this ordering.

Recall that $\boldsymbol{\pi}_1$ is 3; so $\mathsf{exp(code(n), 1)}$ returns the number of the proved formula. A given theorem might appear more than once in the enumeration, corresponding to codes with different proofs of it, but this is no problem, as each theorem appears in some position(s) of the list. Observe that we have, for the first time, made use of regular minimization — so that this function is recursive but not *primitive* recursive. Supposing that T has an infinite number of theorems, there is always some z at which the characteristic function upon which the minimization operates returns zero — so that the function is well-defined. So the theorems of a recursively axiomatized formal theory T are recursively enumerable.

Suppose we add that T is consistent and negation complete. Then there is a recursive relation $\textsc{thrmt}(\mathsf{p})$ true just of numbers for theorems of T: Intuitively, we can enumerate the theorems; then if T is consistent and negation complete, for any sentence $\mathcal{P}$, exactly one of $\mathcal{P}$ or $\sim\mathcal{P}$ must show up in the enumeration. So we can search through the list until we find either $\mathcal{P}$ or $\sim\mathcal{P}$ — and if the one we find is $\mathcal{P}$, then $\mathcal{P}$ is a theorem. In particular, we find $\mathcal{P}$ or $\sim\mathcal{P}$ at the position, $\mu\mathsf{n}[\mathsf{enum(n)} = \ulcorner\mathcal{P}\urcorner \vee \mathsf{enum(n)} = \ulcorner\sim\mathcal{P}\urcorner]$. Recall that if p is the number of a formula $\mathcal{P}$, $\mathsf{neg(p)}$ is the number of $\sim\mathcal{P}$. Then,

T12.18. For any recursively axiomatized, consistent, negation complete formal theory T there is a recursive relation $\textsc{thrmt}(\mathsf{p})$ true just in case p numbers a theorem of T. Set,

$$\mathsf{pos(p)} = \mu\mathsf{n}([\sim\textsc{sent}(\mathsf{p}) \wedge \mathsf{n} = 0] \vee [\textsc{sent}(\mathsf{p}) \wedge (\mathsf{enum(n)} = \mathsf{p} \vee \mathsf{enum(n)} = \mathsf{neg(p)})])$$

$$\textsc{thrmt}(\mathsf{p}) =_{\text{def}} \mathsf{enum(pos(p))} = \mathsf{p}$$

First, $\mathsf{pos(p)}$ takes one of three values: if p does not number a sentence it is just $\mathsf{0}$; if p appears in the enumeration of theorems it is the position of p; and if $\mathsf{neg(p)}$ appears in the enumeration of theorems, it is the position of $\mathsf{neg(p)}$. Then $\textsc{thrmt}(\mathsf{p})$ is true just in case pos takes the second option — just in case p numbers a sentence and p rather than $\mathsf{neg(p)}$ appears in the enumeration of theorems. Observe that $\mathsf{pos(p)}$ returns $\mathsf{0}$ both when p does not number a sentence, and when p is the number of the first theorem in the enumeration. But when $\mathsf{pos(p)} = \mathsf{0}$, $\mathsf{enum(pos(p))}$ always numbers the first theorem of the enumeration — so that if p is not the number of a sentence $\textsc{thrmt}(\mathsf{p})$ is false, and when p is the number of the first theorem it is true (as it should be). Again, we appeal to regular minimization. It is only because T is negation complete that the function to which the minimization operator applies is regular. So long as p numbers a sentence, the characteristic function for the second square brackets is sure to go to zero for one disjunct or the other, and when p does not number a sentence, the function for the first square brackets goes to zero. So the function is well-defined.

Now consider a formula $\mathcal{P}(x)$ with free variable x. The *diagonalization* of $\mathcal{P}$ is the formula $\exists x(x = \overline{\ulcorner \mathcal{P} \urcorner} \wedge \mathcal{P}(x))$. So the diagonalization of $\mathcal{P}$ is true just when $\mathcal{P}$ applies to its own Gödel number. To understand this nomenclature, consider a grid with formulas listed down the left in order of their Gödel numbers and the integer Gödel numbers across the top.

	a	b	c	...
$\mathcal{P}_{\mathsf{a}}(x)$	$\boldsymbol{\mathcal{P}_{\mathsf{a}}(\overline{\mathsf{a}})}$	$\mathcal{P}_{\mathsf{a}}(\overline{\mathsf{b}})$	$\mathcal{P}_{\mathsf{a}}(\overline{\mathsf{c}})$	
$\mathcal{P}_{\mathsf{b}}(x)$	$\mathcal{P}_{\mathsf{b}}(\overline{\mathsf{a}})$	$\boldsymbol{\mathcal{P}_{\mathsf{b}}(\overline{\mathsf{b}})}$	$\mathcal{P}_{\mathsf{b}}(\overline{\mathsf{c}})$	
$\mathcal{P}_{\mathsf{c}}(x)$	$\mathcal{P}_{\mathsf{c}}(\overline{\mathsf{a}})$	$\mathcal{P}_{\mathsf{c}}(\overline{\mathsf{b}})$	$\boldsymbol{\mathcal{P}_{\mathsf{c}}(\overline{\mathsf{c}})}$	
$\vdots$				

So, going down the main diagonal, formulas are of the sort $\mathcal{P}_{\mathsf{n}}(\overline{\mathsf{n}})$ where the formula numbered n is applied to its Gödel number n.

Let $\mathsf{num(n)}$ be the Gödel number of the standard numeral for n. So,

$$\mathsf{num(0)} = \ulcorner \emptyset \urcorner$$
$$\mathsf{num(Sy)} = \ulcorner S \urcorner \star \mathsf{num(y)}$$

So num is (primitive) recursive. Now $\mathsf{diag(n)}$ is the Gödel number of the diagonalization of the formula with Gödel number n.

$$\mathsf{diag(n)} =_{\text{def}} \ulcorner \exists x(x = \urcorner \star \mathsf{num(n)} \star \ulcorner \wedge \urcorner \star \mathsf{n} \star \ulcorner) \urcorner$$

It should be clear enough how to unabbreviate $\ulcorner \exists \urcorner$ and $\ulcorner \wedge \urcorner$. Since $\mathsf{diag(n)}$ is recursive, for any theory T extending Q there is a formula $Diag(x, y)$ that captures it. So if $\mathsf{diag(m)} = \mathsf{n}$, then $T \vdash Diag(\overline{\mathsf{m}}, \overline{\mathsf{n}})$ and $T \vdash \forall z[Diag(\overline{\mathsf{m}}, z) \rightarrow z = \overline{\mathsf{n}}]$.

T12.19. Let T be any theory that extends Q. Then for any formula $\mathcal{F}(y)$ containing just the variable y free, there is a sentence $\mathcal{H}$ such that $T \vdash \mathcal{H} \leftrightarrow \mathcal{F}(\overline{\ulcorner \mathcal{H} \urcorner})$. The *Diagonal Lemma*.

Suppose T extends Q; since $\mathsf{diag}(\mathsf{n})$ is recursive, there is a formula $Diag(x, y)$ that captures diag. Let $\mathcal{A}(x) =_{\text{def}} \exists y[\mathcal{F}(y) \wedge Diag(x, y)]$ and $\mathsf{a} = \ulcorner \mathcal{A} \urcorner$, the Gödel number of $\mathcal{A}$. Intuitively, $\mathcal{A}$ says $\mathcal{F}$ applies to the diagonalization of x. Then set $\mathcal{H} =_{\text{def}} \exists x(x = \overline{\mathsf{a}} \wedge \exists y[\mathcal{F}(y) \wedge Diag(x, y)])$ and $\mathsf{h} = \ulcorner \mathcal{H} \urcorner$, the Gödel number of $\mathcal{H}$. $\mathcal{H}$ is the diagonalization of $\mathcal{A}$; so $\mathsf{diag}(\mathsf{a}) = \mathsf{h}$. Intuitively, then $\mathcal{H}$ says that $\mathcal{F}$ applies to the diagonalization of $\mathcal{A}$, which is just to say that according to $\mathcal{H}$, $\mathcal{F}(\overline{\ulcorner \mathcal{H} \urcorner})$. Reason as follows.

1.	$\mathcal{H} \leftrightarrow \exists x(x = \overline{\mathsf{a}} \wedge \exists y[\mathcal{F}(y) \wedge Diag(x, y)])$	from def $\mathcal{H}$
2.	$Diag(\overline{\mathsf{a}}, \overline{\mathsf{h}})$	from capture
3.	$\forall z(Diag(\overline{\mathsf{a}}, z) \rightarrow z = \overline{\mathsf{h}})$	from capture
4.	$\quad \mathcal{H}$	A ($g \leftrightarrow$I)
5.	$\quad \exists x(x = \overline{\mathsf{a}} \wedge \exists y[\mathcal{F}(y) \wedge Diag(x, y)])$	1,4 $\leftrightarrow$E
6.	$\quad\quad j = \overline{\mathsf{a}} \wedge \exists y[\mathcal{F}(y) \wedge Diag(j, y)]$	A (g 5$\exists$E)
7.	$\quad\quad j = \overline{\mathsf{a}}$	6 $\wedge$E
8.	$\quad\quad \exists y[\mathcal{F}(y) \wedge Diag(j, y)]$	6 $\wedge$E
9.	$\quad\quad\quad \mathcal{F}(k) \wedge Diag(j, k)$	A (g 8$\exists$E)
10.	$\quad\quad\quad \mathcal{F}(k)$	9 $\wedge$E
11.	$\quad\quad\quad Diag(j, k)$	9 $\wedge$E
12.	$\quad\quad\quad Diag(\overline{\mathsf{a}}, k)$	11,7 =E
13.	$\quad\quad\quad Diag(\overline{\mathsf{a}}, k) \rightarrow k = \overline{\mathsf{h}}$	3 $\forall$E
14.	$\quad\quad\quad k = \overline{\mathsf{h}}$	13,12 $\rightarrow$E
15.	$\quad\quad\quad \mathcal{F}(\overline{\mathsf{h}})$	10,14 =E
16.	$\quad\quad \mathcal{F}(\overline{\mathsf{h}})$	8,9-15 $\exists$E
17.	$\quad \mathcal{F}(\overline{\mathsf{h}})$	5,6-16 $\exists$E
18.	$\quad \mathcal{F}(\overline{\mathsf{h}})$	A $g \leftrightarrow$I
19.	$\quad \mathcal{F}(\overline{\mathsf{h}}) \wedge Diag(\overline{\mathsf{a}}, \overline{\mathsf{h}})$	18,2 $\wedge$I
20.	$\quad \exists y[\mathcal{F}(y) \wedge Diag(\overline{\mathsf{a}}, y)]$	19 $\exists$I
21.	$\quad \overline{\mathsf{a}} = \overline{\mathsf{a}}$	=I
22.	$\quad \overline{\mathsf{a}} = \overline{\mathsf{a}} \wedge \exists y[\mathcal{F}(y) \wedge Diag(\overline{\mathsf{a}}, y)]$	21,20 $\wedge$I
23.	$\quad \exists x(x = \overline{\mathsf{a}} \wedge \exists y[\mathcal{F}(y) \wedge Diag(x, y)])$	22 $\exists$I
24.	$\quad \mathcal{H}$	1,23 $\leftrightarrow$E
25.	$\mathcal{H} \leftrightarrow \mathcal{F}(\overline{\mathsf{h}})$	4-17,18-24 $\leftrightarrow$I
26.	$\mathcal{H} \leftrightarrow \mathcal{F}(\overline{\ulcorner \mathcal{H} \urcorner})$	25 abv

So $T \vdash \mathcal{H} \leftrightarrow \mathcal{F}(\overline{\ulcorner \mathcal{H} \urcorner})$.

If n is such that $\mathsf{f(n)} = \mathsf{n}$, then n is said to be a *fixed point* for f. And by a (possibly strained) analogy, $\mathscr{H}$ is said to be a "fixed point" for $\mathscr{F}(y)$.

Now we are very close to the incompleteness of arithmetic. As a final preliminary,

T12.20. For no consistent theory T that extends Q is there a recursive relation $\textsc{thrmt}(\mathsf{n})$ that is true just in case n is a Gödel number of a theorem of T.

> Consider a consistent theory extending Q; and suppose there is a recursive relation $\textsc{thrmt}(\mathsf{n})$ true just in case n numbers a theorem of T. Since T extends Q and $\textsc{thrmt}$ is recursive, with T12.16 there is some formula *Thrmt*(y) that captures $\textsc{thrmt}$, and so a formula $\sim$*Thrmt*(y). And again since T extends Q, by the diagonal lemma T12.19, there is a formula $\mathscr{H}$ with Gödel number $\ulcorner\mathscr{H}\urcorner = \mathsf{h}$ such that,
>
> $$T \vdash \mathscr{H} \leftrightarrow \sim Thrmt(\overline{\ulcorner\mathscr{H}\urcorner})$$
>
> Suppose $T \nvdash \mathscr{H}$; then $\mathscr{H}$ is not a theorem of T so that $\mathsf{h} \notin \textsc{thrmt}$; so by capture, $T \vdash \sim Thrmt(\overline{\ulcorner\mathscr{H}\urcorner})$; so by $\leftrightarrow$E, $T \vdash \mathscr{H}$. This is impossible; reject the assumption: $T \vdash \mathscr{H}$. But then $\mathscr{H}$ is a theorem of T; so $\mathsf{h} \in \textsc{thrmt}$; so by capture, $T \vdash Thrmt(\overline{\ulcorner\mathscr{H}\urcorner})$; so by NB, $T \vdash \sim\mathscr{H}$, and T is inconsistent; but by hypothesis, T is consistent. Reject the original assumption: there is no recursive relation $\textsc{thrmt}$.

Given a recursive $\textsc{thrmt}$ there is $\sim$*Thrmt*; but we show there is no such $\textsc{thrmt}$; so we have not yet found a sentence $\mathscr{G}$ such that PA $\vdash \mathscr{G} \leftrightarrow \sim Thrmt(\overline{\ulcorner\mathscr{G}\urcorner})$. That waits for the next chapter. From T12.18 any recursively axiomatized, consistent, *negation complete* formal theory has a recursive relation $\textsc{thrmt}(\mathsf{n})$ true just in case n numbers a theorem. But from T12.20 for no consistent theory extending Q is there such a relation. This already suggests results to follow.

E12.31. Let T be any theory extending Q and $\textsc{sbtht}(\mathsf{n})$ a recursive function such that if $\textsc{sbtht}(\mathsf{n})$ then n numbers a theorem of T (one such function is sure to be $\textsc{thrmads}(\mathsf{n})$ for the theorems of sentential logic). Use the diagonal lemma to find a sentence $\mathscr{H}$ such that $T \vdash \mathscr{H}$ but $\ulcorner\mathscr{H}\urcorner \notin \textsc{sbtht}$. Demonstrate your results.

*E12.32. Let T be any theory that extends Q. For any formulas $\mathscr{F}_1(y)$ and $\mathscr{F}_2(y)$, generalize the diagonal lemma to find sentences $\mathscr{H}_1$ and $\mathscr{H}_2$ such that,

$$T \vdash \mathcal{H}_1 \leftrightarrow \mathcal{F}_1(\overline{\ulcorner \mathcal{H}_2 \urcorner})$$
$$T \vdash \mathcal{H}_2 \leftrightarrow \mathcal{F}_2(\overline{\ulcorner \mathcal{H}_1 \urcorner})$$

Demonstrate your result. Hint: You will want to generalize the notion of diagonalization so that the *alternation* of formulas $\mathcal{F}_1(z)$, $\mathcal{F}_2(z)$, with a formula $\mathcal{P}$ is $\exists w \exists x \exists y(w = \overline{\ulcorner \mathcal{P} \urcorner} \wedge x = \overline{\ulcorner \mathcal{F}_2 \urcorner} \wedge y = \overline{\ulcorner \mathcal{F}_1 \urcorner} \wedge \exists z(\mathcal{F}_1(z) \wedge \mathcal{P}))$. Then you can find a recursive function $\mathsf{alt}(\mathsf{p}, \mathsf{f}_1, \mathsf{f}_2)$ whose output is the number of the alternation of formulas numbered p, f_1 and f_2, where this function is captured by some formula $Alt(w, x, y, z)$ that itself has Gödel number a. Then $\mathsf{alt}(\overline{\mathsf{a}}, \overline{\mathsf{f}}_1, \overline{\mathsf{f}}_2)$ and $\mathsf{alt}(\overline{\mathsf{a}}, \overline{\mathsf{f}}_2, \overline{\mathsf{f}}_1)$ number the formulas you need for $\mathcal{H}_1$ and $\mathcal{H}_2$.

E12.33. Use your version of the diagonal lemma from E12.32 to provide an alternate demonstration of T12.20. Hint: You will be able to set up sentences such that the first says the second is not a theorem, while the second says the first is a theorem.

12.5.2 First Applications

Here are three quick results from our theorems. Do not let the simplicity of their proof (if the proof can seem simple after all we have done) distract from the significance of their content!

The Incompleteness of Arithmetic.

We are finally ready for *the incompleteness of arithmetic*.

T12.21. No consistent, recursively axiomatizable theory extending Q is negation complete.

Consider a theory T that is a consistent, recursively axiomatizable extension of Q. Then since T consistent and extends Q, by T12.20, there is no recursive relation $\textsc{thrmt}(\mathsf{n})$ true iff n is the Gödel number of a theorem. Suppose T is negation complete; then since T is also consistent and recursively axiomatized, by T12.18 there is a recursive relation $\textsc{thrmt}(\mathsf{n})$ true iff n is the Gödel number of a theorem. This is impossible, reject the assumption: T is not negation complete.

It immediately follows that Q and PA are not negation complete. But similarly for *any* consistent recursively axiomatizable theory that extends Q. We already knew that there were formulas $\mathcal{P}$ such that Q $\nvdash \mathcal{P}$ and Q $\nvdash \sim\mathcal{P}$. But we did not already have this result for PA; and we certainly did not have the result generally for recursively axiomatizable theories extending Q.

There are other ways to obtain this result. We explore Gödel's own strategy in the next chapter. And we shall see an approach from computability in chapter 14. However, this first argument is sufficient to establish the point.

The Decision Problem

It is a short step from the result that if Q is consistent, then no recursive relation identifies the theorems of Q, to the result that if Q is consistent, then no recursive relation identifies the theorems of predicate logic.

T12.22. If Q is consistent, then no recursive relation $\textsc{thrmpl}(\mathsf{n})$ is true iff n numbers a theorem of predicate logic.

Suppose otherwise, that Q is consistent and some recursive relation $\textsc{thrmpl}(\mathsf{n})$ is true iff n numbers a theorem of predicate logic. Let $\mathcal{Q}$ be the conjunction of the axioms of Q; then $\mathcal{P}$ is a theorem of Q iff $\vdash \mathcal{Q} \rightarrow \mathcal{P}$. Let $\mathsf{q} = \ulcorner\mathcal{Q}\urcorner$; then,

$$\textsc{thrmq}(\mathsf{n}) =_{\text{def}} \textsc{thrmpl}(\mathsf{cnd}(\mathsf{q}, \mathsf{n}))$$

defines a recursive function true iff n numbers a theorem of Q. But, given the consistency of Q, by T12.20, there is no function $\textsc{thrmq}(\mathsf{n})$. Reject the assumption, if Q is consistent, then there is no recursive relation $\textsc{thrmpl}(\mathsf{n})$ true iff n numbers a theorem of predicate logic.

And, of course, given that Q *is* consistent, it follows that no recursive relation numbers the theorems of predicate logic. From T12.20 no recursive relation numbers the theorems of Q. Now we see that this result extends to the theorems of predicate logic. At at this stage, these results may seem to be a sort of curiosity about what recursive functions do. They gain significance when, as we have already hinted can be done, we identify the recursive functions with the *computable* functions in chapter 14.

Tarski's Theorems

A couple of related theorems fall under this heading. Say $\textsf{TRUE}(\mathsf{n})$ is true iff n numbers a true sentence of some language $\mathcal{L}$. We do not assume that $\textsf{TRUE}(\mathsf{n})$ is recursive — only that, by definition, it applies to numbers of true sentences. Suppose $True(x)$ expresses $\textsf{TRUE}(\mathsf{n})$. Then by expression, $\mathsf{I}[True(\overline{\ulcorner\mathcal{P}\urcorner})] = \mathsf{T}$ iff $\ulcorner\mathcal{P}\urcorner \in \textsf{TRUE}$; and this iff $\mathsf{I}[\mathcal{P}] = \mathsf{T}$. So, with some manipulation,

$$\mathsf{I}[True(\overline{\ulcorner\mathcal{P}\urcorner}) \leftrightarrow \mathcal{P}] = \mathsf{T}$$

Let us say T is a *truth theory* for language $\mathcal{L}$, iff for any sentence of $\mathcal{L}$, T proves this result.

$$T \vdash True(\overline{\ulcorner\mathcal{P}\urcorner}) \leftrightarrow \mathcal{P}$$

Nothing prevents theories of this sort. However, a first theorem is to the effect that theories in our range cannot be theories of truth for their own language $\mathcal{L}$.

T12.23. No recursively axiomatized consistent theory extending Q is a theory of truth for its own language $\mathcal{L}$.

Suppose otherwise, that a recursively axiomatized consistent T extending Q is a theory of truth for its own $\mathcal{L}$. Since T extends Q, by the diagonal lemma, there is a sentence $\mathcal{F}$ (a false or liar sentence) such that

$$T \vdash \mathcal{F} \leftrightarrow \sim True(\overline{\ulcorner\mathcal{F}\urcorner})$$

But since T is a truth theory, $T \vdash True(\overline{\ulcorner\mathcal{F}\urcorner}) \leftrightarrow \mathcal{F}$; so $T \vdash True(\overline{\ulcorner\mathcal{F}\urcorner}) \leftrightarrow \sim True(\overline{\ulcorner\mathcal{F}\urcorner})$; so T is inconsistent. Reject the assumption: T is not a truth theory for its language $\mathcal{L}$.

This theorem explains our standard jump to the metalanguage when we give conditions like ST and SF. Nothing prevents stating truth conditions — trouble results when a theory purports to give conditions for all the sentences in its own language.

A second theorem takes on the slightly stronger (but still plausible) assumption that Q is a sound theory, so that all of its theorems are true. Under this condition, there is trouble even expressing a truth predicate for language $\mathcal{L}$ in that language $\mathcal{L}$.

T12.24. If Q is sound, and $\mathcal{L}$ includes $\mathcal{L}_{NT}$ then there is no *True* to express $\textsf{TRUE}$ in $\mathcal{L}$.

Suppose otherwise, that Q is sound and some formula *True*(x) expresses TRUE(n) in $\mathscr{L}$; since Q is a theory that extends Q, by the diagonal lemma, there is a sentence $\mathscr{F}$ such that $\mathsf{Q} \vdash \mathscr{F} \leftrightarrow \sim True(\overline{\ulcorner \mathscr{F} \urcorner})$; since the theorems of Q are true, $\mathsf{N}[\mathscr{F} \leftrightarrow \sim True(\overline{\ulcorner \mathscr{F} \urcorner})] = \mathsf{T}$; so with a bit of manipulation,

$$\mathsf{N}[\mathscr{F}] = \mathsf{T} \text{ iff } \mathsf{N}[\sim True(\overline{\ulcorner \mathscr{F} \urcorner})] = \mathsf{T}; \text{ iff } \mathsf{N}[True(\overline{\ulcorner \mathscr{F} \urcorner})] \neq \mathsf{T}$$

(i) Suppose $\mathsf{N}[True(\overline{\ulcorner \mathscr{F} \urcorner})] \neq \mathsf{T}$; then by expression, $\ulcorner \mathscr{F} \urcorner \notin$ TRUE, so that $\mathsf{N}[\mathscr{F}] \neq \mathsf{T}$; so by the above equivalence, $\mathsf{N}[True(\overline{\ulcorner \mathscr{F} \urcorner})] = \mathsf{T}$; reject the assumption. (ii) So $\mathsf{N}[True(\overline{\ulcorner \mathscr{F} \urcorner})] = \mathsf{T}$; but then by the equivalence, $\mathsf{N}[\mathscr{F}] \neq \mathsf{T}$; so $\ulcorner \mathscr{F} \urcorner \notin$ TRUE; so by expression, $\mathsf{N}[\sim True(\overline{\ulcorner \mathscr{F} \urcorner})] = \mathsf{T}$; so $\mathsf{N}[True(\overline{\ulcorner \mathscr{F} \urcorner})] \neq \mathsf{T}$; this is impossible.

Reject the original assumption: no formula *True*(x) expresses TRUE(n).

Observe that some numerical properties are both expressed and captured — as the recursive relations. And if a property can be captured by a recursively axiomatized consistent theory extending Q, then it can be expressed.[11] As we have seen, even though THRMQ(n) is a relation on the integers, it is not not a recursive relation. It can however be *expressed* by the formula, $\exists x Prfq(x, n)$. In the following (T14.10) we show that that every function captured by a consistent recursively axiomatized theory extending Q is recursive; it follows that THRMQ(n) is expressed but not captured. And now we have seen a relation TRUE(n) not even expressed in $\mathscr{L}_{NT}$.

This is a decent start into the results of Part IV of the text. In the following, we turn to deepening and extending them in different directions.

E12.34. Use the alternate version of the diagonal lemma from E12.32 to provide alternate demonstrations of T12.23 and T12.24. Include the "bit of minipulation" left out of the text for T12.24.

E12.35. For each of the following concepts, explain in an essay of about two pages, so that (college freshman) Hannah could understand. In your essay, you should (i) identify the objects to which the concept applies, (ii) give and explain the definition, and give and explicate examples (iii) where the concept applies, and (iv) where it does not. Your essay should exhibit an understanding of methods from the text.

[11] Since we use the same canonical formulas for expression and capture, it is perhaps obvious that canonical capture in a *sound* theory implies expression. Further, from T14.10 if a function can be captured by a consistent recursively axiomatized theory extending Q it is recursive; so by T12.3 it is expressed on the standard interpretation N for $\mathscr{L}_{NT}$.

Final Results of Chapter 12

T12.17 If T is a recursively axiomatized formal theory then the set of theorems of T is recursively enumerable.

T12.18 For any recursively axiomatized, consistent, negation complete formal theory T there is a recursive relation THRMT(n) true just in case n numbers a theorem of T.

T12.19 Let T be any theory that extends Q. Then for any formula $\mathscr{F}(y)$ containing just the variable y free, there is a sentence $\mathscr{H}$ such that $T \vdash \mathscr{H} \leftrightarrow \mathscr{F}(\overline{\ulcorner \mathscr{H} \urcorner})$. The *Diagonal Lemma*.

T12.20 For no consistent theory T that extends Q is there a recursive relation THRMT(n) that is true just in case n is a Gödel number of a theorem of T.

T12.21 No consistent, recursively axiomatizable extension of Q is negation complete. The *incompleteness of arithmetic*.

T12.22 If Q is consistent, then no recursive relation THRMPL(n) is true iff n numbers a theorem of predicate logic

T12.23 No recursively axiomatized consistent theory extending Q is a theory of truth for its own language $\mathscr{L}$.

T12.24 If Q is sound, and $\mathscr{L}$ includes $\mathscr{L}_{NT}$ then there is no *True* to express TRUE in $\mathscr{L}$.

a. The recursive functions and the role of the beta function in their expression and capture.

b. The essential elements from this chapter contributing to the proof of the incompleteness of arithmetic.

c. The essential elements from this chapter contributing to the proof of that no recursive relation identifies the theorems of predicate logic

d. The essential elements from this chapter contributing to the proof of Tarski's theorem.

Chapter 13

Gödel's Theorems

We have seen a demonstration of the incompleteness of arithmetic. In this chapter, we take another run at that result, this time by Gödel's original strategy of producing sentences that are true iff not provable. This enables us to extend and deepen the incompleteness result, and puts us in a position to take up Gödel's second incompleteness theorem, according to which theories (of a certain sort) are not sufficient for demonstrations of *consistency*.

13.1 Gödel's First Theorem

Recall that the diagonalization of a formula $\mathscr{P}(x)$ is $\exists x(x = \overline{\ulcorner \mathscr{P} \urcorner} \wedge \mathscr{P}(x))$. In addition, there is a recursive function $\mathsf{diag}(\mathsf{n})$ which numbers the diagonalization of the formula with number n and, if T is recursively axiomatized, a recursive relation $\textsc{prft}(\mathsf{m}, \mathsf{n})$ true when m numbers a proof of the formula with number n. Our previous argument for incompleteness required $\textsc{prft}(\mathsf{m}, \mathsf{n})$ for T12.17, and a $Diag(x, y)$ to capture $\mathsf{diag}(\mathsf{n})$ for the diagonal lemma. Under the assumption that there is a $\textsc{thrmt}$ and so a formula $\sim$*Thrmt*, we applied the diagonal lemma to obtain an $\mathscr{H}$ such that $T \vdash \mathscr{H} \leftrightarrow {\sim}Thrmt(\overline{\ulcorner \mathscr{H} \urcorner})$; but this is impossible — so that there is no $\textsc{thrmt}$. And from this we argued that there must be a sentence such that neither it nor its negation is provable — without any suggestion what that sentence might be. This time, by related methods, we construct a particular sentence such that neither it nor its negation is provable.

13.1.1 Semantic Version

Consider some recursively axiomatized theory T whose language includes $\mathscr{L}_{NT}$. Since $\textsc{prft}(\mathsf{m},\mathsf{n})$ and $\mathsf{diag}(\mathsf{n})$ are recursive, they are *expressed* by some formulas $Prft(x,y)$ and $Diag(x,y)$. Let $\mathcal{A}(z) =_{def} \sim\exists x\exists y(Prft(x,y) \wedge Diag(z,y))$, and $\mathsf{a} = \ulcorner\mathcal{A}\urcorner$. So $\mathcal{A}$ says nothing numbers a proof of the diagonalization of a formula with number z. Then,

$$\mathscr{G} =_{def} \exists z(z = \bar{\mathsf{a}} \wedge \sim\exists x\exists y(Prft(x,y) \wedge Diag(z,y)))$$

So $\mathscr{G}$ is the diagonalization of $\mathcal{A}$, and intuitively $\mathscr{G}$ "says" that nothing numbers a proof of it. Let $\mathsf{g} = \ulcorner\mathscr{G}\urcorner$. Observe that $\mathscr{G}$ is defined relative to *Prft* for T; so each T yields its own Gödel sentence (if it were not ugly, we might sensibly introduce subscripts $\mathscr{G}_T$). Thus,

T13.1. For any recursively axiomatized theory T whose language includes $\mathscr{L}_{NT}$, $\mathscr{G}$ is true iff it is unprovable in T ($\mathsf{N}[\mathscr{G}] = \mathsf{T}$ iff $T \nvdash \mathscr{G}$).

Consider a recursively axiomatized theory T whose language includes $\mathscr{L}_{NT}$ and the formula $\mathscr{G}$ as described above. Skipping some steps, (i) Suppose $\mathsf{N}[\mathscr{G}] = \mathsf{T}$; then for any d, $\mathsf{N_d}[\mathscr{G}] = \mathsf{S}$; so with T10.2, $\mathsf{N_d}[\sim\exists x\exists y(Prft(x,y) \wedge Diag(\bar{\mathsf{a}},y))] = \mathsf{S}$; so there are no m,n such that $\mathsf{N}[Prft(\bar{\mathsf{m}},\bar{\mathsf{n}})] = \mathsf{T}$ and $\mathsf{N}[Diag(\bar{\mathsf{a}},\bar{\mathsf{n}})] = \mathsf{T}$; so by expression, there are no m,n such that $\langle\mathsf{m},\mathsf{n}\rangle \in \textsc{prft}$ and $\langle\mathsf{a},\mathsf{n}\rangle \in \mathsf{diag}$; but $\mathsf{diag}(\mathsf{a}) = \mathsf{g}$; so no m numbers a proof of $\mathscr{G}$, which is to say $T \nvdash \mathscr{G}$. (ii) Suppose $\mathsf{N}[\mathscr{G}] \neq \mathsf{T}$; then there is some d such that $\mathsf{N_d}[\mathscr{G}] \neq \mathsf{S}$ and for any $\mathsf{n} \in \mathbb{N}$, $\mathsf{N_{d(z|n)}}[z = \bar{\mathsf{a}} \wedge \sim\exists x\exists y(Prft(x,y) \wedge Diag(z,y))] \neq \mathsf{S}$; so $\mathsf{N_{d(z|a)}}[z = \bar{\mathsf{a}} \wedge \sim\exists x\exists y(Prft(x,y) \wedge Diag(z,y))] \neq \mathsf{S}$; so by T10.2, $\mathsf{N_d}[\sim\exists x\exists y(Prft(x,y) \wedge Diag(\bar{\mathsf{a}},y))] \neq \mathsf{S}$; so $\mathsf{N_d}[\exists x\exists y(Prft(x,y) \wedge Diag(\bar{\mathsf{a}},y))] = \mathsf{S}$; so there are m and n such that both $Prft(\bar{\mathsf{m}},\bar{\mathsf{n}})$ and $Diag(\bar{\mathsf{a}},\bar{\mathsf{n}})$ are S on N with d; so $\mathsf{N}[\sim Prft(\bar{\mathsf{m}},\bar{\mathsf{n}})] \neq \mathsf{T}$ and $\mathsf{N}[\sim Diag(\bar{\mathsf{a}},\bar{\mathsf{n}})] \neq \mathsf{T}$; and by expression $\langle\mathsf{m},\mathsf{n}\rangle \in \textsc{prft}$ and $\langle\mathsf{a},\mathsf{n}\rangle \in \mathsf{diag}$; but again, $\mathsf{diag}(\mathsf{a}) = \mathsf{g}$; so $\langle\mathsf{m},\mathsf{g}\rangle \in \textsc{prft}$; so $T \vdash \mathscr{G}$; so by transposition, if $T \nvdash \mathscr{G}$, then $\mathsf{N}[\mathscr{G}] = \mathsf{T}$.

It is not a difficult exercise to fill in the details. Intuitively this result should seem right. Suppose $\mathscr{G}$ "says" that it is unprovable: then if it is true it is unprovable; and if it is unprovable it is true; so it is true iff it is unprovable.

Now suppose that T is a recursively axiomatized, and *sound* theory (so that its theorems are true), whose language includes $\mathscr{L}_{NT}$. Then T is negation incomplete.

T13.2. If T is a recursively axiomatized sound theory whose language includes $\mathscr{L}_{NT}$, then T is negation incomplete.

Suppose T is a recursively axiomatized theory whose language includes $\mathscr{L}_{\text{NT}}$; then there is a sentence $\mathscr{G}$ to which the conditions for T13.1 apply. (i) Suppose $T \vdash \mathscr{G}$; then, since T is sound, $\mathscr{G}$ is true; so by T13.1, $T \nvdash \mathscr{G}$; reject the assumption, $T \nvdash \mathscr{G}$. Suppose $T \vdash \sim\mathscr{G}$; then since T is sound, $\sim\mathscr{G}$ is true; so $\mathscr{G}$ is not true; so by T13.1, $T \vdash \mathscr{G}$; so by soundness again, $\mathscr{G}$ is true; reject the assumption: $T \nvdash \sim\mathscr{G}$.

So $\mathscr{G}$ is a sentence such that if T is a recursively axiomatized sound theory whose language includes $\mathscr{L}_{\text{NT}}$, neither $\mathscr{G}$ nor its negation is a theorem. And, from T13.1, given that $\mathscr{G}$ is unprovable, if T is a recursively axiomatized theory whose language includes $\mathscr{L}_{\text{NT}}$, then $\mathscr{G}$ is a *true* non-theorem. This version of the incompleteness result depends on the ability to express $\mathscr{G}$, together with the soundness of theory T.

13.1.2 Syntactic Version

Gödel's first theorem is usually presented with the capture and consistency, rather than the expression and soundness constraints. We turn now to a version of this first sort which, again, builds a particular sentence such that neither it nor its negation is provable.

Since $\textsf{PRFT}(\mathsf{m}, \mathsf{n})$ and $\mathsf{diag}(\mathsf{n})$ are recursive, in theories extending Q they are *captured* by canonical formulas $Prft(x, y)$ and $Diag(x, y)$. As before, let $\mathscr{A}(z) =_{\text{def}} \sim\exists x\exists y(Prft(x, y) \wedge Diag(z, y))$, and $\mathsf{a} = \ulcorner\mathscr{A}\urcorner$. So $\mathscr{A}$ says nothing numbers a proof of the diagonalization of a formula with number z. Then,

$$\mathscr{G} =_{\text{def}} \exists z(z = \overline{\mathsf{a}} \wedge \sim\exists x\exists y(Prft(x, y) \wedge Diag(z, y)))$$

So $\mathscr{G}$ is the diagonalization of $\mathscr{A}$; let g be the Gödel number of $\mathscr{G}$. This time, we shall be able to establish in T the relation between $\mathscr{G}$ and its proof. Reasoning as for the diagonal lemma,

T13.3. Let T be any recursively axiomatized theory extending Q; then $T \vdash \mathscr{G} \leftrightarrow \sim\exists x Prft(x, \overline{\ulcorner\mathscr{G}\urcorner})$.

Since T is recursively axiomatized, there is a recursive $\textsf{PRFT}$ and since T extends Q there are *Prft* and *Diag* that capture $\textsf{PRFT}$ and diag. From the definition of $\mathscr{G}$, $T \vdash \mathscr{G} \leftrightarrow \exists z(z = \overline{\mathsf{a}} \wedge \sim\exists x\exists y[Prft(x, y) \wedge Diag(z, y)])$; from capture $T \vdash Diag(\overline{\mathsf{a}}, \overline{\mathsf{g}})$; and $T \vdash \forall z(Diag(\overline{\mathsf{a}}, z) \rightarrow z = \overline{\mathsf{g}})$. From these it follows that $T \vdash \mathscr{G} \leftrightarrow \sim\exists x Prft(x, \overline{\mathsf{g}})$; which is to say, $T \vdash \mathscr{G} \leftrightarrow \sim\exists x Prft(x, \overline{\ulcorner\mathscr{G}\urcorner})$ (homework).

From the diagonal lemma, under appropriate conditions, given a formula $\mathscr{F}(y)$, there is some $\mathscr{H}$ such that $T \vdash \mathscr{H} \leftrightarrow \mathscr{F}(\overline{\ulcorner\mathscr{H}\urcorner})$. Under the assumption that there is THRMT, we applied this to show there would be some $\mathscr{H}$ such that $T \vdash \mathscr{H} \leftrightarrow \sim Thrmt(\overline{\ulcorner\mathscr{H}\urcorner})$. This led to contradiction. In this case, however, we show that there really is a particular sentence $\mathscr{G}$ such that $T \vdash \mathscr{G} \leftrightarrow \sim\exists x Prft(x, \overline{\ulcorner\mathscr{G}\urcorner})$.

Our idea is to show that if T is a consistent, recursively axiomatized theory extending Q, then $T \nvdash \mathscr{G}$ and $T \nvdash \sim\mathscr{G}$. The first is easy enough.

T13.4. If T is a consistent, recursively axiomatized theory extending Q, then $T \nvdash \mathscr{G}$.

> Suppose T is a consistent recursively axiomatized theory extending Q. Suppose $T \vdash \mathscr{G}$; then since T is recursively axiomatized, for some m, PRFT(m, g); and since T extends Q, by capture, $T \vdash Prft(\overline{\mathsf{m}}, \overline{\mathsf{g}})$; so by $\exists$I, $T \vdash \exists x Prft(x, \overline{\mathsf{g}})$, which is to say, $T \vdash \exists x Prft(x, \overline{\ulcorner\mathscr{G}\urcorner})$. But since $T \vdash \mathscr{G}$, by T13.3, $T \vdash \sim\exists x Prft(x, \overline{\ulcorner\mathscr{G}\urcorner})$. So T is inconsistent; reject the assumption: $T \nvdash \mathscr{G}$.

That is the first half of what we are after. But we can't quite get that if T is a consistent, recursively axiomatized theory extending Q, then $T \nvdash \sim\mathscr{G}$. Rather, we need a strengthened notion of consistency. Say a theory T is *ω-incomplete* iff for some $\mathscr{P}(x)$, T can prove each $\mathscr{P}(\overline{\mathsf{m}})$ but T cannot go on to prove $\forall x\mathscr{P}(x)$. Equivalently, T is ω-incomplete iff for every m, it can prove each $T \vdash \sim\mathscr{P}(\overline{\mathsf{m}})$ but $T \nvdash \sim\exists x\mathscr{P}(x)$. We have seen that Q is ω-incomplete: we can prove, say $\overline{\mathsf{n}} \times \overline{\mathsf{m}} = \overline{\mathsf{m}} \times \overline{\mathsf{n}}$ for every m and n, but cannot go on to prove the corresponding universal generalization $\forall x\forall y(x \times y = y \times x)$. Say T is *ω-inconsistent* iff for some $\mathscr{P}(x)$, T proves each $\mathscr{P}(\overline{\mathsf{m}})$ but also proves $\sim\forall x\mathscr{P}(x)$. Equivalently, T is ω-inconsistent iff for every m, it can prove each $T \vdash \sim\mathscr{P}(\overline{\mathsf{m}})$ and $T \vdash \exists x\mathscr{P}(x)$. ω-incompleteness is a theoretical weakness — there are some things true but not provable. But ω-inconsistency is a theoretical disaster: It is not possible for the theorems of an ω-inconsistent theory all to be true on any interpretation (assuming some $\overline{\mathsf{m}}$ for each $\mathsf{m} \in \mathsf{U}$). ω-inconsistency is not itself inconsistency — for we do not have any sentence such that $T \vdash \mathscr{P}$ and $T \vdash \sim\mathscr{P}$. But inconsistent theories are automatically ω-inconsistent — for from contradiction all consequences follow (including each $\mathscr{P}(\overline{\mathsf{m}})$ and also $\sim\forall x\mathscr{P}(x)$); transposing, ω-consistent theories are consistent. Now we show,

T13.5. If T is an ω-consistent, recursively axiomatized theory extending Q, then $T \nvdash \sim\mathscr{G}$.

> Suppose T is an ω-consistent recursively axiomatized theory extending Q. Suppose $T \vdash \sim\mathscr{G}$; since T is ω-consistent, it is consistent, so $T \nvdash \mathscr{G}$; so since T is recursively axiomatized, for all m, $\langle \mathsf{m}, \mathsf{g}\rangle \notin$ PRFT; and since T extends Q,

by capture, $T \vdash \sim Prft(\overline{\mathsf{m}}, \overline{\mathsf{g}})$; and since T is ω-consistent, $T \nvdash \exists x Prft(x, \overline{\mathsf{g}})$; which is to say, $T \nvdash \exists x Prft(x, \overline{\ulcorner \mathcal{G} \urcorner})$. But since $T \vdash \sim\mathcal{G}$, by T13.3 with NB, $T \vdash \exists x Prft(x, \overline{\ulcorner \mathcal{G} \urcorner})$. This is impossible; reject the assumption: $T \nvdash \sim\mathcal{G}$.

So if a recursively axiomatized theory extending Q has the relevant *consistency* properties, then it is negation incomplete. Further, insofar as T canonically captures the recursive functions, it expresses the recursive functions; so by T13.1, $\mathcal{G}$ is true iff $T \nvdash \mathcal{G}$. So if T is a consistent recursively axiomatized theory extending Q, then $\mathcal{G}$ is both unprovable and true.

This is roughly the form in which Gödel proved the incompleteness of arithmetic in 1931: If T is a consistent, recursively axiomatized theory extending Q, then $T \nvdash \mathcal{G}$; and if T is an ω-consistent, recursively axiomatized theory extending Q, then $T \nvdash \sim\mathcal{G}$. Since we believe that standard theories including Q and PA are consistent and ω-consistent, this sufficient for the incompleteness of arithmetic.

E13.1. Fill in the details for the argument of T13.1.

*E13.2. Complete the demonstration of T13.3 by providing a derivation to show $T \vdash \mathcal{G} \leftrightarrow \sim\exists x Prft(x, \overline{\ulcorner \mathcal{G} \urcorner})$. The demonstration for the diagonal lemma is a model, though steps will be adapted to the particular form of these sentences.

13.1.3 Rosser's Sentence

But it is possible to drop the special assumption of ω-consistency by means of a sentence somewhat different from $\mathcal{G}$.[1] Recall that $\mathsf{neg(n)}$ is the Gödel number of the negation of the sentence with number n. So $\overline{\text{PRFT}}(\mathsf{m}, \mathsf{n}) =_{\text{def}} \text{PRFT}(\mathsf{m}, \mathsf{neg(n)})$ obtains when m numbers a proof of the negation of the sentence numbered n. Since it is recursive, it is captured by some $\overline{Prft}(x, y)$. Set,

$$RPrft(x, y) =_{\text{def}} Prft(x, y) \wedge (\forall w \leq x) \sim\overline{Prft}(w, y)$$

So $RPrft(x, y)$ just in case x numbers a proof of the sentence numbered y and no number less than or equal to x is a proof of the negation of that sentence. Now, working as before, set $\mathcal{A}'(z) =_{\text{def}} \sim\exists x \exists y (RPrft(x, y) \wedge Diag(z, y))$, and $\mathsf{a} = \ulcorner \mathcal{A}' \urcorner$. So $\mathcal{A}'$ says nothing numbers an R-proof of the diagonalization of a formula with number z. Then,

[1] Barkley Rosser, "Extensions of Some Theorems of Gödel and Church."

$$\mathcal{R} =_{\text{def}} \exists z(z = \bar{\mathsf{a}} \wedge \sim\exists x \exists y(RPrft(x, y) \wedge Diag(z, y)))$$

So $\mathcal{R}$ is the diagonalization of $\mathcal{A}'$; let r be the Gödel number of $\mathcal{R}$. And $\mathcal{R}$ has the key syntactic property just like $\mathcal{G}$. Again, reasoning as we did for the diagonal lemma,

T13.6. Let T be any recursively axiomatized theory extending Q; then $T \vdash \mathcal{R} \leftrightarrow \sim\exists x RPrft(x, \overline{\ulcorner \mathcal{R} \urcorner})$.

You can show this just as for T13.3.

Now the first half of the incompleteness result is straightforward.

T13.7. If T is a consistent, recursively axiomatized theory extending Q, then $T \nvdash \mathcal{R}$.

Suppose T is a consistent recursively axiomatized theory extending Q. Suppose $T \vdash \mathcal{R}$; then since T is recursively axiomatized, for some m, $\textsf{PRFT}(\mathsf{m}, \mathsf{r})$; and since T extends Q, by capture, $T \vdash Prft(\overline{\mathsf{m}}, \overline{\mathsf{r}})$. But by consistency, $T \nvdash \sim\mathcal{R}$; so for all n, and in particular all $\mathsf{n} \leq \mathsf{m}$, $\langle \mathsf{n}, \mathsf{r} \rangle \notin \overline{\textsf{PRFT}}$; so by capture, $T \vdash \sim\overline{Prft}(\overline{\mathsf{n}}, \overline{\mathsf{r}})$; so by T8.21, $T \vdash (\forall w \leq \overline{\mathsf{m}})\sim\overline{Prft}(w, \overline{\mathsf{r}})$; so $T \vdash Prft(\overline{\mathsf{m}}, \overline{\mathsf{r}}) \wedge (\forall w \leq \overline{\mathsf{m}})\sim\overline{Prft}(w, \overline{\mathsf{r}})$; so $T \vdash RPrft(\overline{\mathsf{m}}, \overline{\mathsf{r}})$; so $T \vdash \exists x RPrft(x, \overline{\mathsf{r}})$, which is to say, $T \vdash \exists x RPrft(x, \overline{\ulcorner \mathcal{R} \urcorner})$. But since $T \vdash \mathcal{R}$, by T13.6, $T \vdash \sim\exists x RPrft(x, \overline{\ulcorner \mathcal{R} \urcorner})$; so T is inconsistent. This is impossible; reject the assumption: $T \nvdash \mathcal{R}$.

So, with consistency, it is not much harder to prove $T \vdash \exists x RPrft(x, \overline{\ulcorner \mathcal{R} \urcorner})$ from the assumption that $T \vdash \mathcal{R}$ than to prove $T \vdash \exists x Prft(x, \overline{\ulcorner \mathcal{G} \urcorner})$ from the assumption that $T \vdash \mathcal{G}$.

Reasoning for the other direction is somewhat more involved, but still straightforward.

T13.8. If T is a consistent, recursively axiomatized theory extending Q, then $T \nvdash \sim\mathcal{R}$.

Suppose T is a consistent recursively axiomatized theory extending Q. Suppose $T \vdash \sim\mathcal{R}$. Then since T is recursively axiomatized, for some m, $\langle \mathsf{m}, \mathsf{r} \rangle \in \overline{\textsf{PRFT}}$; and since T extends Q, by capture, $T \vdash \overline{Prft}(\overline{\mathsf{m}}, \overline{\mathsf{r}})$. By consistency, $T \nvdash \mathcal{R}$; so for any n, and in particular, any $\mathsf{n} \leq \mathsf{m}$, $\langle \mathsf{n}, \mathsf{r} \rangle \notin \textsf{PRFT}$; so by capture, $T \vdash \sim Prft(\overline{\mathsf{n}}, \overline{\mathsf{r}})$; and by T8.21, $T \vdash (\forall w \leq \overline{\mathsf{m}})\sim Prft(w, \overline{\mathsf{r}})$. Now reason as follows.

1.	$\sim\mathcal{R}$	from T
2.	$\overline{Prft}(\overline{\mathsf{m}},\bar{\mathsf{r}})$	capture
3.	$(\forall w \leq \overline{\mathsf{m}})\sim Prft(w,\bar{\mathsf{r}})$	capture and T8.21
4.	$\mathcal{R} \leftrightarrow \sim\exists x RPrft(x,\bar{\mathsf{r}})$	from T13.6
5.	$\exists x RPrft(x,\bar{\mathsf{r}})$	1,4 NB
6.	$\exists x[Prft(x,\bar{\mathsf{r}}) \wedge (\forall w \leq x)\sim\overline{Prft}(w,\bar{\mathsf{r}})]$	5 abv
7.	$Prft(j,\bar{\mathsf{r}}) \wedge (\forall w \leq j)\sim\overline{Prft}(w,\bar{\mathsf{r}})]$	A (g, 6∃E)
8.	$j \leq \overline{\mathsf{m}} \vee \overline{\mathsf{m}} \leq j$	T8.19
9.	$j \leq \overline{\mathsf{m}}$	A (g 8∨E)
10.	$Prft(j,\bar{\mathsf{r}})$	7 ∧ E
11.	$\sim Prft(j,\bar{\mathsf{r}})$	3,9 (∀E)
12.	$\bot$	10,11 ⊥I
13.	$\overline{\mathsf{m}} \leq j$	A (g, 8∨E)
14.	$(\forall w \leq j)\sim\overline{Prft}(w,\bar{\mathsf{r}})]$	7 ∧E
15.	$\sim\overline{Prft}(\overline{\mathsf{m}},\bar{\mathsf{r}})$	14,13 (∀E)
16.	$\bot$	2,15 ⊥I
17.	$\bot$	8,9-12,13-16 ∨E
18.	$\bot$	6,7-17 ∃E

So $T \vdash \bot$, that is $T \vdash Z \wedge \sim Z$ and T is inconsistent. Reject the assumption, $T \nvdash \sim\mathcal{R}$.

In the previous case, with $\mathcal{G}$, we had no way to convert $\exists x Prft(x,\bar{\mathsf{g}})$ to a contradiction with $\sim Prft(\bar{0},\bar{\mathsf{g}})$, $\sim Prft(\bar{1},\bar{\mathsf{g}})\ldots$; that is why we needed ω-consistency. We can, however, move from $\sim Prft(\bar{0},\bar{\mathsf{r}})$, $\sim Prft(\bar{1},\bar{\mathsf{r}})\ \ldots \sim Prft(\overline{\mathsf{m}},\bar{\mathsf{r}})$ to a *bounded* quantification $(\forall w \leq \overline{\mathsf{m}})\sim Prft(w,\bar{\mathsf{r}})$ or equivalently $\sim(\exists w \leq \overline{\mathsf{m}})Prft(w,\bar{\mathsf{r}})$. Then the special nature of $\mathcal{R}$ aids the argument: From $RPrft(j,\bar{\mathsf{r}})$ suppose $j \leq \mathsf{m}$; then $Prft(j,\bar{\mathsf{r}})$ and we contradict the bounded quantification in the usual way. Suppose $j \geq \mathsf{m}$; then *RPrft* is designed so that nothing less than j (including $\overline{\mathsf{m}}$) numbers a proof of $\mathsf{neg}(\mathsf{r})$; but we have $\overline{Prft}(\overline{\mathsf{m}},\bar{\mathsf{r}})$ from the assumption. So $T \nvdash \mathcal{R}$ and $T \nvdash \sim\mathcal{R}$

Let us close this section with some reflections on what we have shown. First,

$$\text{Q is sound} \Longrightarrow \text{Q is } \omega\text{-consistent} \Longrightarrow \text{Q is consistent}$$

So our results are progressively stronger, as the assumptions have become correspondingly weaker. But,

$$\text{capture} \Longrightarrow \text{expression}$$

So the second requirement is increased as we move from expression to capture.

Second, we have not shown that there are truths of $\mathcal{L}_{NT}$ not provable in any recursively axiomatizable, consistent theory extending Q. Rather, what we have shown is that for any recursively axiomatizable consistent theory extending Q, there are some truths of $\mathcal{L}_{NT}$ not provable in that theory. For a given recursively axiomatizable theory, there will be a given relation $\textsc{prft}(\mathsf{m}, \mathsf{n})$ and $Prft(x, y)$ depending on the particular axioms of that theory — and so unique sentences $\mathcal{G}$ and $\mathcal{R}$ constructed as above. In particular, given that a theory cannot prove, say, $\mathcal{R}$, we might simply *add* $\mathcal{R}$ to its axioms; then of course there is a derivation of $\mathcal{R}$ from the axioms of the revised theory! But then the new theory will generate a new relation $\textsc{prft}(\mathsf{m}, \mathsf{n})$ and a new $Prft(x, y)$ and so a new unprovable sentence $\mathcal{R}'$. So any theory extending Q is negation incomplete.

But it is worth a word about what are theories extending Q. Any such theory should build in equivalents of the $\mathcal{L}_{NT}$ vocabulary $\emptyset$, S, $+$, and $\times$ — and should have a predicate *Nat*(*x*) to identify a class of objects to count as the numbers. Then if the theory makes the axioms of Q true on these objects, it is incomplete. Straightforward extensions of Q are ones like PA which simply add to its axioms. But ordinary ZF set theory also falls into this category — for it is possible to define a class of sets, say, $\oslash$, $\{\oslash\}$, $\{\oslash, \{\oslash\}\}$, $\{\oslash, \{\oslash\}, \{\oslash, \{\oslash\}\}\}\ldots$ where any n is the set of all the numbers prior to it, along with operations on sets which obey the axioms of Q.[2] It follows that ZF is negation incomplete. In contrast, the domain for the standard theory of real numbers has all the entities required to do arithmetic. However that theory does not have a predicate $Nat(x)$ to pick out the natural numbers, and cannot recapitulate the theory of natural numbers on any subclass of its domain. So our incompleteness theorem does not get a grip, and in fact the theory of real numbers is demonstrably complete. Observe, though, that it is a *weakness* in this theory of real numbers, its inability to specify a certain class that makes room for its completeness.[3]

E13.3. Demonstrate T13.6.

---

[2] For discussion, see any introduction to set theory, for example, Enderton, *Elements of Set Theory*, chapter 4.

[3] There are real numbers $\mathsf{0}$ and $\mathsf{1}$; so it is natural to identify the integers with $\mathsf{0}$, $\mathsf{0} + \mathsf{1}$, $\mathsf{0} + \mathsf{1} + \mathsf{1}$ and so forth. The difficulty is to define a property within the theory of real numbers that picks out just the members of this series, as we have been able to define infinite recursive properties in $\mathcal{L}_{NT}$. The completeness of the theory of real numbers was originally proved by Tarski, and is discussed in books on model theory, for example, Hodges *A Shorter Model Theory*, theorems 2.7.2 and 7.4.4.

13.2 Gödel's Second Theorem: Overview

We turn now to Gödel's second incompleteness theorem on the unprovability of consistency. The discussion is divided into four main parts. First, in this section, Gödel's second theorem is proved subject to three *derivability conditions*. Then we turn to the derivability conditions themselves. The first is easy. But the second and third require extended discussion. There is some background (section 13.3). Then discussion of the second condition (section 13.4), and the third condition (section 13.5). This completes the proof. We conclude with some reflections and consequences from our results (section 13.6). There are alternative approaches to the second theorem (for references see section 3 of Raatikainen, "Gödel's Incompleteness Theorems"). Our's is a straight-ahead development of the standard approach based on the derivability conditions. This is, surely, a natural place to start. Textbooks ordinarily end their discussion of the second theorem with the demonstration from the derivability conditions, offering just some general perspective on how the conditions are to be obtained.[4] However, even if you decide to bypass the details, this general perspective will be enhanced if you have some object at which to "wave" as you pass them by.

For this discussion we switch to theories including PA. The result is that that PA and its its extensions cannot prove their own consistency. The reason for this switch will become vivid in demonstration of the derivability conditions — as many arguments that would have been by induction are forced into the theory and so are by IN. Coinciding with the move to PA we revert to considering original rather than canonical formulas to capture recursive functions: this avoids some complication, and since PA has all the resources of Q_s, all our incompleteness results are preserved.[5]

Main argument. We have seen that for recursively axiomatized theories there is a recursive relation $\textsc{prft}(\mathsf{m},\mathsf{n})$. Since it is recursive, in theories extending Q, this relation is captured by a corresponding $\mathit{Prft}(x, y)$. Let

[4] So, for example, "the details of this are long and tedious, and will not be discussed here" (George and Velleman, *Philosophies of Mathematics*, 201; and "the proofs of the [second and third derivability conditions] are omitted from virtually all books on the level of this one, not because they involve any terribly difficult new ideas, but because the innumerable routine verifications they — and especially the last — require would take up too much time and patience" (Boolos, Burgess and Jeffrey, *Computability and Logic*, 234.) The only other (relatively) complete development in English that I have been able to track down is Tourlakis, *Lectures in Logic and Set Theory: I*.

[5] But the argument goes through for certain theories weaker than PA. Of relevance to Hilbert, it goes through for *primitive recursive arithmetic* (PRA) — whose theorems are like those of PA with application of the induction schema restricted to only Π_1 formulas. Though he is not entirely clear, arguably, PRA is Hilbert's real theory R (see p. 547). We set aside such details.

$$Prvt(y) =_{\text{def}} \exists x Prft(x, y)$$

So $Prvt(y)$ just when something numbers a proof of the formula numbered y — when the formula numbered by y is provable. Insofar as the quantifier is unbounded, there is no suggestion that there is a corresponding recursive relation — in fact, we have seen in T12.20 that no recursive relation is true just of numbers for the theorems of Q. Let,

$$Cont =_{\text{def}} \sim Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner})$$

So *Cont* is true just in case there is no proof of $\overline{0} = \overline{1}$. There are different ways to express consistency, but for theories extending Q this does as well as any other. Let T extend Q. Suppose T is inconsistent; then it proves anything; so $T \vdash \overline{0} = \overline{1}$. Suppose $T \vdash \overline{0} = \overline{1}$; since T extends Q, $T \vdash \overline{0} \neq \overline{1}$; so T proves a contradiction and is inconsistent. So T is inconsistent iff $T \vdash \overline{0} = \overline{1}$; and, transposing, T is consistent iff $T \nvdash \overline{0} = \overline{1}$ (for further discussion see 13.6.1).

The second theorem is this simple result: Under certain conditions, if T is consistent, then $T \nvdash Cont$. If it is consistent, then T cannot prove its own consistency. Suppose the first theorem applies to T, and suppose we could show,

$$(**) \qquad T \vdash Cont \to \sim Prvt(\overline{\ulcorner \mathscr{G} \urcorner})$$

Then, given what has gone before, we could make the following very simple argument. Suppose T is a recursively axiomatized theory extending Q.

> By T13.3, $T \vdash \mathscr{G} \leftrightarrow \sim\exists x Prft(x, \overline{\ulcorner \mathscr{G} \urcorner})$, which is to say, $T \vdash \mathscr{G} \leftrightarrow \sim Prvt(\overline{\ulcorner \mathscr{G} \urcorner})$; from this and $(**)$, $T \vdash Cont \to \mathscr{G}$; so if $T \vdash Cont$ then $T \vdash \mathscr{G}$; but from the first theorem (T13.4), if T is consistent, then $T \nvdash \mathscr{G}$; so if T is consistent, $T \nvdash Cont$.

So the argument reduces to showing $(**)$. Observe that, in reasoning for T13.4 we have already shown,

$$T \text{ is consistent} \Longrightarrow T \nvdash \mathscr{G}$$

So the argument reduces to showing that T *proves* what we have already seen is so. There is nothing mysterious about this: *Cont*, *Prvt* and the like are formulas, and so just the sort of thing to which our proof apparatus applies.

Let us abbreviate $Prvt(\overline{\ulcorner \mathscr{P} \urcorner})$ by $\Box\mathscr{P}$. Observe that this obscures the corner quotes. Still, we shall find it useful. So we need $T \vdash Cont \to \sim\Box\mathscr{G}$, which is just to say, $T \vdash \sim\Box(\overline{0} = \overline{1}) \rightarrow \sim\Box\mathscr{G}$. Suppose T satisfies the following *derivability conditions*.

D1. If $T \vdash \mathscr{P}$ then $T \vdash \Box\mathscr{P}$

D2. $T \vdash \Box(\mathscr{P} \rightarrow \mathscr{Q}) \rightarrow (\Box\mathscr{P} \rightarrow \Box\mathscr{Q})$

D3. $T \vdash \Box\mathscr{P} \rightarrow \Box\Box\mathscr{P}$

Then we shall be able to show $T \vdash \mathit{Cont} \rightarrow \sim\Box\mathscr{G}$.

The utility of $\Box$ in this context is that D1 - D3 are exactly the conditions that define a standard modal logic, K4 — and it is not surprising that *provability* should correspond to a kind of necessity.[6] There is an elegant natural derivation system for this modal logic. For this you might check out Roy, Natural Derivations for Priest §2 (but in the nomenclature there borrowed from Priest, the system is $NK\tau$). However rather than explain and introduce a new derivation system, we obtain a version of K4 simply by adding A1 - A3 and MP from AD_s to D1 - D3. So K4 has D1 as a new rule, and D2 and D3 as new axioms. Since A1 - A3 and MP remain, we have all the theorems from before. Thus, as a simple example,

(A)

1.	$\sim\mathscr{P} \rightarrow (\mathscr{P} \rightarrow \mathscr{Q})$	T3.9
2.	$\Box[\sim\mathscr{P} \rightarrow (\mathscr{P} \rightarrow \mathscr{Q})]$	1 D1
3.	$\Box[\sim\mathscr{P} \rightarrow (\mathscr{P} \rightarrow \mathscr{Q})] \rightarrow [\Box\sim\mathscr{P} \rightarrow \Box(\mathscr{P} \rightarrow \mathscr{Q})]$	D2
4.	$\Box\sim\mathscr{P} \rightarrow \Box(\mathscr{P} \rightarrow \mathscr{Q})$	3,2 MP

So in this system $\vdash \Box\sim\mathscr{P} \rightarrow \Box(\mathscr{P} \rightarrow \mathscr{Q})$.

Now, given that $T \vdash \mathscr{G} \rightarrow \sim\exists x \mathit{Prft}(x, \overline{\ulcorner\mathscr{G}\urcorner})$ from T13.3 we shall be able to show that $T \vdash \mathit{Cont} \rightarrow \sim\Box\mathscr{G}$.

T13.9. Let T be a recursively axiomatized theory extending Q. Then supposing T satisfies the derivability conditions and so the K4 logic of provability, $T \vdash \mathit{Cont} \rightarrow \sim\mathit{Prvt}(\overline{\ulcorner\mathscr{G}\urcorner})$.

[6]While K4 correctly represents these principles, it is not a complete logic of provability. We get a complete system if we add to K4 a rule according to which from $\Box\mathscr{P} \rightarrow \mathscr{P}$ we may infer $\mathscr{P}$. For discussion see subsection 13.6.2 and Boolos, *The Logic of Provability*.

1.	$\mathscr{G} \rightarrow \sim\Box\mathscr{G}$	from T13.3
2.	$\Box(\mathscr{G} \rightarrow \sim\Box\mathscr{G})$	1 D1
3.	$\Box(\mathscr{G} \rightarrow \sim\Box\mathscr{G}) \rightarrow (\Box\mathscr{G} \rightarrow \Box\sim\Box\mathscr{G})$	D2
4.	$\Box\mathscr{G} \rightarrow \Box\sim\Box\mathscr{G}$	3,2 MP
5.	$\Box\sim\Box\mathscr{G} \rightarrow \Box(\Box\mathscr{G} \rightarrow \overline{0} = \overline{1})$	(A)
6.	$\Box\mathscr{G} \rightarrow \Box(\Box\mathscr{G} \rightarrow \overline{0} = \overline{1})$	4,5 T3.2
7.	$\Box(\Box\mathscr{G} \rightarrow \overline{0} = \overline{1}) \rightarrow (\Box\Box\mathscr{G} \rightarrow \Box(\overline{0} = \overline{1}))$	D2
8.	$\Box\mathscr{G} \rightarrow (\Box\Box\mathscr{G} \rightarrow \Box(\overline{0} = \overline{1}))$	6,7 T3.2
9.	$[\Box\mathscr{G} \rightarrow (\Box\Box\mathscr{G} \rightarrow \Box(\overline{0} = \overline{1}))] \rightarrow [(\Box\mathscr{G} \rightarrow \Box\Box\mathscr{G}) \rightarrow (\Box\mathscr{G} \rightarrow \Box(\overline{0} = \overline{1}))]$	A2
10.	$(\Box\mathscr{G} \rightarrow \Box\Box\mathscr{G}) \rightarrow (\Box\mathscr{G} \rightarrow \Box(\overline{0} = \overline{1}))$	9,8 MP
11.	$\Box\mathscr{G} \rightarrow \Box\Box\mathscr{G}$	D3
12.	$\Box\mathscr{G} \rightarrow \Box(\overline{0} = \overline{1})$	10,11 MP
13.	$[\Box\mathscr{G} \rightarrow \Box(\overline{0} = \overline{1})] \rightarrow [\sim\Box(\overline{0} = \overline{1}) \rightarrow \sim\Box\mathscr{G}]$	T3.13
14.	$\sim\Box(\overline{0} = \overline{1}) \rightarrow \sim\Box\mathscr{G}$	13,12 MP

Which is to say, $T \vdash Cont \rightarrow \sim Prvt(\overline{\ulcorner\mathscr{G}\urcorner})$.

As usual for an axiomatic derivation, the reasoning is not entirely transparent. However we are at the stage where, given the derivability conditions, T proves the result. Given this, reason as before,

T13.10. Let T be a recursively axiomatized theory extending Q. Then supposing T satisfies the derivability conditions, if T is consistent, $T \nvdash Cont$.

Suppose T is a recursively axiomatized theory extending Q that satisfies the derivability conditions. Then by T13.9, $T \vdash Cont \rightarrow \sim Prvt(\overline{\ulcorner\mathscr{G}\urcorner})$; and by T13.3, $T \vdash \mathscr{G} \leftrightarrow \sim Prvt(\overline{\ulcorner\mathscr{G}\urcorner})$; so $T \vdash Cont \rightarrow \mathscr{G}$; so if $T \vdash Cont$ then $T \vdash \mathscr{G}$; but from the first incompleteness theorem (T13.4), if T is consistent, then $T \nvdash \mathscr{G}$; so if T is consistent, $T \nvdash Cont$.

One might wonder about the significance of this theorem: If T were inconsistent, it *would* prove *Cont*. So a failure to prove *Cont* is no reason to think that T is inconsistent. And a proof of *Cont* might itself be an indication of inconsistency! The interesting point here results from using one theory to prove the consistency of another. Recall the main Hilbert strategy as outlined in the introduction to Part IV; a key component is the demonstration by means of some real theory R that an ideal theory I is consistent. But, supposing that PA cannot prove its own consistency, we can be sure that no *weaker* theory can prove the consistecy of PA. And if PA cannot prove even the consistency of PA, then PA and theories weaker than PA cannot be used to prove the consistency of theories *stronger* than PA.[7] So a leg of the Hilbert

[7] And the same goes for Hilbert's PRA (see note 5).

strategy seems to be removed. Observe, however, that the theorem does not show that the consistency of PA is unprovable: a theory stronger than PA at least in some respects might still prove the consistency of PA.[8] This may be a straightforward theorem of the second theory. Of course, as a means of demonstrating consistency such an argument may seem problematic insofar as one requires some reason for thinking the second theory sound which does not already attach to the first, and so already show that the first theory is consistent.

Another theorem is easy to show, and left as an exercise.

T13.11. Let T be a recursively axiomatized theory extending Q. Then supposing T satisfies the derivability conditions and so the K4 logic of provability, $T \vdash \mathit{Cont} \leftrightarrow \sim\mathit{Prvt}(\overline{\ulcorner \mathit{Cont} \urcorner})$.

Hints: (i) Show that $T \vdash \mathit{Cont} \rightarrow \sim\Box\mathit{Cont}$; you can do this starting with $\mathit{Cont} \rightarrow \sim\Box\mathscr{G}$ from T13.9 and $\sim\Box\mathscr{G} \rightarrow \mathscr{G}$ from T13.3. Then (ii) show $T \vdash \sim\Box\mathit{Cont} \rightarrow \mathit{Cont}$; for this, use T3.39 with T3.9 to show $T \vdash \overline{0} = \overline{1} \rightarrow \mathit{Cont}$; then you should be able to obtain $\sim\Box\mathit{Cont} \rightarrow \sim\Box(\overline{0} = \overline{1})$ which is to say $\sim\Box\mathit{Cont} \rightarrow \mathit{Cont}$. Together these give the desired result.

From this theorem, supposing the derivability conditions, *Cont* is another $\mathscr{P}$ which, like $\mathscr{G}$, is such that $T \vdash \mathscr{P} \leftrightarrow \sim\mathit{Prvt}(\overline{\ulcorner \mathscr{P} \urcorner})$; so *Cont* is another fixed point for $\sim\mathit{Prvt}(x)$. It follows that *Cont* is another sentence such that both it and its negation are unprovable. Interestingly, *Cont* uses the notion of provability, but is not constructed so as to say anything about its *own* provability — and so this instance of incompleteness does not depend on self-reference for the unprovable sentence.

We have shown that the second theorem holds for a theory if it meets the derivability conditions. But this is not to show that the theorem holds for any theories! In order to tie the result to something concrete, we turn now to showing that PA meets the derivability conditions, and so that PA, and theories extending PA, satisfy the theorem.

Demonstration of the first condition is simple.

T13.12. Suppose T is a recursively axiomatized theory extending Q. Then if $T \vdash \mathscr{P}$, then $T \vdash \Box\mathscr{P}$.

[8] G. Gentzen shows this very thing, "The Consistency of Elementary Number Theory," and "New Version of the Consistency Proof for Elementary Number Theory," both in *The Collected Papers of Gehard Gentzen*, ed. Szabo. See also Gentzen, "The Concept of Infinite in Mathematics" also in Szabo, along with Pohlers, *Proof Theory*, chpater 1, and Takeuti, *Proof Theory*, §12.

Suppose $T \vdash \mathcal{P}$; then since T is recursively axiomatized, for some m, $\textsc{prft}(\mathsf{m}, \ulcorner\mathcal{P}\urcorner)$; and since T extends Q, there is a *Prft* that captures $\textsc{prft}$; so $T \vdash \mathit{Prft}(\overline{\mathsf{m}}, \overline{\ulcorner\mathcal{P}\urcorner})$; so by ∃I, $T \vdash \exists x \mathit{Prft}(x, \overline{\ulcorner\mathcal{P}\urcorner})$; so $T \vdash \mathit{Prvt}(\overline{\ulcorner\mathcal{P}\urcorner})$; so $T \vdash \Box\mathcal{P}$.

The next conditions are considerably more difficult. We build gradually to the required results in PA.

E13.4. (i) Produce derivations to show both parts of T13.11. (ii) Use your result to demonstrate that T is negation incomplete — that if T is recursively axiomatized theory extending Q that satisfies the derivability conditions, then if T is consistent, $T \nvdash \mathit{Cont}$, and if T is ω-consistent, $T \nvdash \sim\mathit{Cont}$.

13.3 The Derivability Conditions: Background

In this section we develop some results required for demonstration of derivability conditions two and three. We proceed by introducing functions and relations into PA by *definition*, and then proving some results about them.

13.3.1 Remarks on Definition

So far, we have taken a language, as $\mathcal{L}_q$ or $\mathcal{L}_{NT}$ as basic, and introduced any additional symbols, for example $\leq$, as means of *abbreviation* for expressions in the original language. But in more complex contexts — especially involving function symbols, it will be convenient to *extend* the language by the definition of new symbols. Thus given a theory T in language $\mathcal{L}$, we might introduce symbols and corresponding axioms to obtain T' and $\mathcal{L}'$ as follows,

Symbol	*Axiom*	*Condition*
$\exists$	$\exists x\mathcal{P} \leftrightarrow \sim\forall x\sim\mathcal{P}$	
$\leq$	$x \leq y \leftrightarrow \exists z(z + x = y)$	
$\emptyset$	$y = \emptyset \leftrightarrow \forall x(x \notin y)$	$T \vdash \exists! y\forall x(x \notin y)$
S	$y = Sx \leftrightarrow \forall z[z \in y \leftrightarrow (z \in x \vee z = x)]$	$T \vdash \exists! y\forall z[z \in y \leftrightarrow (z \in x \vee z = x)]$

We are familiar with the first two cases. Strictly, the first lists an axiom schema, representing different axioms for different instances of $\mathcal{P}$. So far, we have thought of

Additional Theorems of PA

*T13.13. *The following are theorems of PA*:

(a) PA $\vdash (r \leq s \wedge s \leq t) \rightarrow r \leq t$

(b) PA $\vdash (r < s \wedge s < t) \rightarrow r < t$

(c) PA $\vdash (r \leq s \wedge s < t) \rightarrow r < t$

(d) PA $\vdash \emptyset \leq t$

(e) PA $\vdash \emptyset < St$

(f) PA $\vdash t \neq \emptyset \leftrightarrow \emptyset < t$

(g) PA $\vdash t > \emptyset \rightarrow \exists y(t = Sy)$ $\quad y$ not in t.

(h) PA $\vdash t < St$

(i) PA $\vdash St = s \rightarrow t < s$

(j) PA $\vdash s \leq t \leftrightarrow Ss \leq St$

(k) PA $\vdash s < t \leftrightarrow Ss < St$

(l) PA $\vdash s < t \leftrightarrow Ss \leq t$

(m) PA $\vdash s \leq t \leftrightarrow s < t \vee s = t$

(n) PA $\vdash s < St \leftrightarrow s < t \vee s = t$

(o) PA $\vdash s \leq St \leftrightarrow s \leq t \vee s = St$

(p) PA $\vdash s < t \vee s = t \vee t < s$

(q) PA $\vdash s \leq t \vee t < s$

(r) PA $\vdash s \leq t \leftrightarrow t \not< s$

(s) PA $\vdash t < s \rightarrow t \neq s$

(t) PA $\vdash (s \leq t \wedge t \leq s) \rightarrow s = t$

(u) PA $\vdash s \leq s + t$

(v) PA $\vdash r \leq s \leftrightarrow r + t \leq s + t$

(w) PA $\vdash r < s \leftrightarrow r + t < s + t$

(x) PA $\vdash (r \leq s \wedge t \leq u) \rightarrow r + t \leq s + u$

(y) PA $\vdash (r < s \wedge t \leq u) \rightarrow r + t < s + u$

(z) PA $\vdash \emptyset < t \rightarrow s \leq s \times t$

(aa) PA $\vdash r \leq s \rightarrow r \times t \leq s \times t$

(ab) PA $\vdash r \times s > \emptyset \rightarrow s > \emptyset$

(ac) PA $\vdash (r > \overline{1} \wedge s > \emptyset) \rightarrow r \times s > s$

(ad) PA $\vdash (t > \emptyset \wedge r < s) \rightarrow r \times t < s \times t$

(ae) PA $\vdash (r < s \wedge t < u) \rightarrow r \times t < s \times u$

(af) PA $\vdash \forall x[(\forall z < x)\mathcal{P}^x_z \rightarrow \mathcal{P}] \rightarrow \forall x\mathcal{P}$ $\quad$ *strong induction (a)*

(ag) PA $\vdash \mathcal{P}^x_\emptyset \wedge \forall x[(\forall z \leq x)\mathcal{P}^x_z \rightarrow \mathcal{P}^x_{Sx}] \rightarrow \forall x\mathcal{P}$ $\quad$ *strong induction (b)*

(ah) PA $\vdash \exists x\mathcal{P} \rightarrow \exists x[\mathcal{P} \wedge (\forall z < x)\sim\mathcal{P}^x_z]$ $\quad$ *least number principle*

Some of these are related to results we obtained in chapter 8 for Q. But there results were of the sort, for any n, Q $\vdash t < \overline{n} \vee t = \overline{n} \vee \overline{n} < t$; with PA, the induction is in the logic rather than in the metalanguage, and we obtain the universal quantifier (or rather, an arbitrary term which may be a free variable) in the object formula.

these as *abbreviations* — and as such the listed axioms are of the sort $\mathcal{Q} \leftrightarrow \mathcal{Q}$ with the abbreviated form on one side, and the unabbreviated on the other. A theory is not extended by the addition of an "axiom" of this sort. But is possible to see the symbols as *new* vocabulary. In all four cases T' includes a new axiom. The last two require also a uniqueness condition in the original T. For these, let $\exists! y\mathcal{P}(y)$ abbreviate $\exists y[\mathcal{P}(y) \wedge \forall z(\mathcal{P}(z) \rightarrow z = y)]$ or equivalently $\exists y\mathcal{P}(y) \wedge \forall y\forall z[(\mathcal{P}(y) \wedge \mathcal{P}(z)) \rightarrow y = z]$ so that *exactly one* thing is $\mathcal{P}$. Then the cases for a constant and function symbol are standard examples from set theory, where zero and successor are defined (the condition for successor sets $Sx = x \cup \{x\}$ so that the members of Sx are x and all the members of x). The details of the examples are not important; we illustrate only the idea of definition. We begin with a formal account, and extend it in different directions.

Basic Account

Consider some theory T and language $\mathcal{L}$. We will consider a language $\mathcal{L}'$ extended with some new symbol and theory T' extended with the corresponding axiom. There are separate cases for a relation symbol, operator symbol, constant symbol and function symbol.

Relation symbol. To introduce a new relation symbol $\mathcal{R}\vec{x}$ we require an axiom in the extended theory such that,

$$T' \vdash \mathcal{R}(\vec{x}) \leftrightarrow \mathcal{Q}(\vec{x})$$

where $\mathcal{Q}(\vec{x})$ is in $\mathcal{L}$. Then for a formula $\mathcal{F}'$ including the new symbol, there should be a conversion $\mathfrak{C}$ such that $\mathfrak{C}[\mathcal{F}'] = \mathcal{F}$ for $\mathcal{F}$ in the original $\mathcal{L}$, and

$$T' \vdash \mathcal{F}' \qquad \text{iff} \qquad T \vdash \mathfrak{C}[\mathcal{F}']$$

So $\mathfrak{C}[\mathcal{F}']$ is like our unabbreviated formula, always available in the original T when $\mathcal{F}'$ is a theorem of T'. The conversion for a relation $\mathcal{R}\vec{\mathfrak{z}}$ is straightforward. Make sure the bound variables of $\mathcal{Q}$ do not overlap the variables of $\vec{\mathfrak{z}}$. Then $\mathfrak{C}[\mathcal{F}'] = \mathcal{F}'^{\mathcal{R}\vec{\mathfrak{z}}}_{\mathcal{Q}(\vec{\mathfrak{z}})}$. So, from the example above,

$$T' \vdash x \leq y \leftrightarrow \exists z(z + x = y).$$

So $\mathcal{R}(x, y) = x \leq y$ and $\mathcal{Q}(x, y) = \exists z(z + x = y)$. Suppose $\mathcal{F}' = \forall z(a \leq z)$. Then we want to instantiate x and y from the axiom to a and z. But z is not free for y in the axiom. We solve the problem by revising bound variables; so $T' \vdash x \leq$

$y \leftrightarrow \exists w(w + x = y)$ and then $T' \vdash a \leq z \leftrightarrow \exists w(w + a = z)$. So $\mathfrak{C}[\mathcal{F}']$ replaces $(a \leq z)$ in $\mathcal{F}'$ with $\exists w(w + a = z)$ to obtain $\forall z \exists w(w + a = z)$.

Operator symbol. Extend notation in the obvious way so that $\mathcal{O}[\vec{\mathcal{P}}]$ indicates that operator symbol $\mathcal{O}$ operates on formulas $\mathcal{P}_1 \dots \mathcal{P}_n$. To introduce a new operator symbol $\mathcal{O}[\vec{\mathcal{P}}]$ we require axioms in the extended theory such that,

$$T' \vdash \mathcal{O}[\vec{\mathcal{P}}] \leftrightarrow \mathcal{Q}[\vec{\mathcal{P}}]$$

where $\mathcal{Q}[\vec{\mathcal{P}}]$ is an expression in $\mathcal{L}$. Again for $\mathcal{F}'$ including the new symbol, there should be a conversion $\mathfrak{C}$ such that $\mathfrak{C}[\mathcal{F}'] = \mathcal{F}$ for $\mathcal{F}$ in the original $\mathcal{L}$ and $T' \vdash \mathcal{F}'$ iff $T \vdash \mathfrak{C}[\mathcal{F}']$. This time set $\mathfrak{C}[\mathcal{F}'] = \mathcal{F}'^{\mathcal{O}[\vec{\mathcal{P}}]}_{\mathcal{Q}[\vec{\mathcal{P}}]}$. Thus, from example above, we are given $T' \vdash \exists z Rxz \leftrightarrow \sim\forall z \sim Rxz$. Suppose $\mathcal{F}' = \forall x \exists z Rxz$. Then $\mathfrak{C}[\mathcal{F}'] = \forall x \sim\forall z \sim Rxz$.

Constant symbol. To introduce a new constant symbol we require an axiom in the extended theory, along with a condition in the original theory such that,

$$T' \vdash y = c \leftrightarrow \mathcal{Q}(y) \qquad \text{and} \qquad T \vdash \exists! y \mathcal{Q}(y)$$

Again for a formula $\mathcal{F}'$ including the new symbol, we expect a conversion $\mathfrak{C}$ such that $\mathfrak{C}[\mathcal{F}'] = \mathcal{F}$, where $T' \vdash \mathcal{F}'$ iff $T \vdash \mathfrak{C}[\mathcal{F}]$. Let z be a variable that does not appear in $\mathcal{F}'$ or $\mathcal{Q}$. Then

$$\mathfrak{C}[\mathcal{F}'] = \exists z(\mathcal{Q}(z) \wedge \mathcal{F}'^{c}_{z})$$

So, from the example above, we are given $T' \vdash y = \emptyset \leftrightarrow \forall x(x \notin y)$; suppose $\mathcal{F}' = \exists x(\emptyset \in x)$. Then z is a variable that does not appear in $\mathcal{F}'$ or $\mathcal{Q}$ — in $\exists x(\emptyset \in x)$ or $\forall x(x \notin y)$. So $\mathfrak{C}[\mathcal{F}'] = \exists z[\forall x(x \notin z) \wedge \exists x(z \in x)]$.

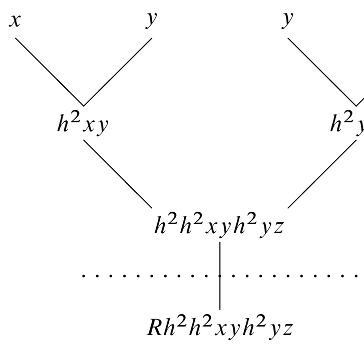
Function symbol. To introduce a function symbol, there is an axiom and condition,

$$T' \vdash y = h\vec{x} \leftrightarrow \mathcal{Q}(\vec{x}, y) \qquad \text{and} \qquad T \vdash \exists! y \mathcal{Q}(\vec{x}, y)$$

The conversion for a function symbol works like that for constants when a single instance of $h\vec{\mathfrak{z}}$ appears in $\mathcal{F}'$. Again, make sure the bound variables of $\mathcal{Q}$ do not overlap the variables of $\vec{\mathfrak{z}}$ and let z be a variable that does not appear in $\mathcal{F}'$ or in $\mathcal{Q}$. Then it is sufficient to set $\mathfrak{C}[\mathcal{F}'] = \exists z(\mathcal{Q}(\vec{\mathfrak{z}}, z) \wedge \mathcal{F}'^{h\vec{\mathfrak{z}}}_{z})$. In general, however, $\mathcal{F}'$ may include multiple instances of h, including one in the scope of another. For the general case, begin where $\mathcal{F}'$ is an atomic $\mathcal{R}' = \mathcal{R}t_1 \dots t_n$ and $t_1 \dots t_n$ may involve instances of $h\vec{\mathfrak{z}}$. Order instances of $h\vec{\mathfrak{z}}$ in $\mathcal{R}'$ from the left (or, on a chapter 2 tree, from the bottom) into a list $h\vec{\mathfrak{z}}_1, h\vec{\mathfrak{z}}_2, \dots h\vec{\mathfrak{z}}_m$, so that when $i < j$, no $h\vec{\mathfrak{z}}_i$

appears in the scope of $\mathscr{h}\vec{\mathscr{t}}_j$. Then set $\mathcal{R}_0 = \mathcal{R}'$, and for $i \geq 1$, $\mathcal{R}_i = \exists z(\mathcal{Q}(\vec{\mathscr{t}}_i, z) \wedge (\mathcal{R}_{i-1})^{\mathscr{h}\vec{\mathscr{t}}_i}_z)$. Then $\mathfrak{C}[\mathcal{R}'] = \mathcal{R}_m$ and for an arbitrary $\mathcal{F}'$, $\mathfrak{C}[\mathcal{F}'] = \mathcal{F}'^{\mathcal{R}'}_{\mathcal{R}_m}$. So, for example, if $\mathcal{R}' = \mathcal{R}_0 = Rh^2h^2xyh^2yz$, the tree is as follows,

(B)



So instances of $\mathscr{h}\mathscr{q}\mathscr{r}$ are ordered $\langle h^2h^2xyh^2yz, h^2xy, h^2yz\rangle$. Then we use $\mathcal{Q}$ to replace instances of $\mathscr{h}$, working our way up through the tree. So,

$$\mathcal{R}_0 = Rh^2h^2xyh^2yz$$

$$\mathcal{R}_1 = \exists u[\mathcal{Q}h^2xyh^2yzu \wedge Ru]$$

$$\mathcal{R}_2 = \exists v(\mathcal{Q}xyv \wedge \exists u[\mathcal{Q}vh^2yzu \wedge Ru])$$

$$\mathcal{R}_3 = \exists w[\mathcal{Q}yzw \wedge \exists v(\mathcal{Q}xyv \wedge \exists u[\mathcal{Q}vwu \wedge Ru])]$$

$\mathcal{R}_1$ uses $\mathcal{Q}$ to replace all of $h^2h^2xyh^2yz$, operating on the terms h^2xy and h^2yz. $\mathcal{R}_2$ uses $\mathcal{Q}$ to replace h^2xy in $\mathcal{R}_1$, and $\mathcal{R}_3$ uses $\mathcal{Q}$ to replace h^2yz in $\mathcal{R}_2$. Observe that free variables are the same as in $\mathcal{R}'$.

To show that this works, that $T' \vdash \mathcal{F}'$ iff $T \vdash \mathcal{F}$ we need a couple of theorems. The idea is to show that $T' \vdash \mathcal{F}' \leftrightarrow \mathcal{F}$ and then that $T' \vdash \mathcal{F}$ iff $T \vdash \mathcal{F}$. Together, these give the result we want. First,

T13.14. For a defined symbol, with its associated axiom and conversion procedure, $T' \vdash \mathcal{F}' \leftrightarrow \mathcal{F}$.

(r) For a relation symbol, we are given $T' \vdash \mathcal{R}\vec{x} \leftrightarrow \mathcal{Q}(\vec{x})$; then so long as the bound variables of $\mathcal{Q}$ do not overlap the variables of $\mathcal{R}\vec{\mathscr{t}}$ (which we guarantee by reasoning as for T3.27) $\vec{\mathscr{t}}$ is free for $\vec{x}$ in $\mathcal{Q}$, so $T' \vdash \mathcal{R}\vec{\mathscr{t}} \leftrightarrow \mathcal{Q}(\vec{\mathscr{t}})$; so by T9.9, $T' \vdash \mathcal{F}' \leftrightarrow \mathcal{F}'^{\mathcal{R}\vec{\mathscr{t}}}_{\mathcal{Q}(\vec{\mathscr{t}})}$; so $T' \vdash \mathcal{F}' \leftrightarrow \mathcal{F}$.

(o) For an operator symbol, we are given $T' \vdash \mathcal{O}[\vec{\mathcal{P}}] \leftrightarrow \mathcal{Q}[\vec{\mathcal{P}}]$; so by T9.9, $T' \vdash \mathcal{F}' \leftrightarrow \mathcal{F}'^{\mathcal{O}[\vec{\mathcal{P}}]}_{\mathcal{Q}[\vec{\mathcal{P}}]}$; so $T' \vdash \mathcal{F}' \leftrightarrow \mathcal{F}$.

(c) The case for constants is left as an exercise.

(f) For a function symbol $\mathscr{h}$, begin with a derivation to show $T' \vdash \mathcal{R}_{i-1} \leftrightarrow \mathcal{R}_i$. Given $\mathcal{R}_{i-1}[\mathscr{h}(\vec{\mathfrak{z}})]$, $\mathcal{R}_i(\vec{\mathfrak{z}})$ is $\exists z(\mathcal{Q}(\vec{\mathfrak{z}}, z) \wedge \mathcal{R}_{i-1}[z])$. We have as an axiom that $T' \vdash y = \mathscr{h}\vec{x} \leftrightarrow \mathcal{Q}(\vec{x}, y)$.

1.	$\mathcal{R}_{i-1}[\mathscr{h}(\vec{\mathfrak{z}})]$	A ($g \leftrightarrow$I)
2.	$\mathscr{h}(\vec{\mathfrak{z}}) = \mathscr{h}(\vec{\mathfrak{z}}) \leftrightarrow \mathcal{Q}(\vec{\mathfrak{z}}, \mathscr{h}(\vec{\mathfrak{z}}))$	from T'
3.	$\mathscr{h}\vec{\mathfrak{z}} = \mathscr{h}\vec{\mathfrak{z}}$	=I
4.	$\mathcal{Q}(\vec{\mathfrak{z}}, \mathscr{h}(\vec{\mathfrak{z}}))$	2,3 $\leftrightarrow$E
5.	$\mathcal{Q}(\vec{\mathfrak{z}}, \mathscr{h}(\vec{\mathfrak{z}})) \wedge \mathcal{R}_{i-1}[\mathscr{h}(\vec{\mathfrak{z}})]$	1,4 $\wedge$I
6.	$\exists z(\mathcal{Q}(\vec{\mathfrak{z}}, z) \wedge \mathcal{R}_{i-1}[z])$	5 $\exists$I
7.	$\exists z(\mathcal{Q}(\vec{\mathfrak{z}}, z) \wedge \mathcal{R}_{i-1}[z])$	A ($g \leftrightarrow$I)
8.	$\mathcal{Q}(\vec{\mathfrak{z}}, j) \wedge \mathcal{R}_{i-1}[j]$	A (g 7$\exists$E)
9.	$\mathcal{Q}(\vec{\mathfrak{z}}, j)$	8 $\wedge$E
10.	$j = \mathscr{h}(\vec{\mathfrak{z}}) \leftrightarrow \mathcal{Q}(\vec{\mathfrak{z}}, j)$	from T'
11.	$j = \mathscr{h}(\vec{\mathfrak{z}})$	10,9 $\leftrightarrow$E
12.	$\mathcal{R}_{i-1}[j]$	8 $\wedge$E
13.	$\mathcal{R}_{i-1}[\mathscr{h}(\vec{\mathfrak{z}})]$	11,12 =E
14.	$\mathcal{R}_{i-1}[\mathscr{h}(\vec{\mathfrak{z}})]$	7,8-13 $\exists$E
15.	$\mathcal{R}_{i-1}[\mathscr{h}(\vec{\mathfrak{z}})] \leftrightarrow \exists z(\mathcal{Q}(\vec{\mathfrak{z}}, z) \wedge \mathcal{R}_{i-1}[z])$	1-6,7-14 $\leftrightarrow$I

Things are arranged so that the variables of $\vec{\mathfrak{z}}$ are not bound upon substitution into $\mathcal{Q}$. So instances of the axiom at (2) and (10) and $\exists$I at (6) satisfy constraints. So $T' \vdash \mathcal{R}_{i-1} \leftrightarrow \mathcal{R}_i$; and by repeated applications of this theorem, $T' \vdash \mathcal{R}' \leftrightarrow \mathcal{R}_m$; so by T9.9, $T' \vdash \mathcal{F}' \leftrightarrow \mathcal{F}'^{\mathcal{R}'}_{\mathcal{R}_m}$; so $T' \vdash \mathcal{F}' \leftrightarrow \mathcal{F}$.

So far, so good, but this only says what the extended T' proves — that the richer T' proves $\mathcal{F}'$ iff it proves $\mathcal{F}$. But we want to see that T' proves $\mathcal{F}'$ iff the original T proves $\mathcal{F}$. We bridge the gap between T and T' by an additional theorem.

T13.15. For a T and $\mathcal{L}$, given a defined symbol with its associated axiom, and for any formula $\mathcal{F}$ in the original $\mathcal{L}$, $T' \vdash \mathcal{F}$ iff $T \vdash \mathcal{F}$.

Since T' proves everything T proves, the direction from right to left is obvious. So suppose $T' \vdash \mathcal{F}$; by soundness, $T' \vDash \mathcal{F}$; we show $T \vDash \mathcal{F}$; so that, by adequacy, $T \vdash \mathcal{F}$. To show $T \vDash \mathcal{F}$, suppose there is a model M such that $\mathsf{M}[T] = \mathsf{T}$; our aim is to show $\mathsf{M}[\mathcal{F}] = \mathsf{T}$.

(r) Relation symbol. Extend M to a model M' like M except that for arbitrary d, $\langle \mathsf{d}[x_1] \ldots \mathsf{d}[x_n] \rangle \in \mathsf{M}'[\mathcal{R}]$ iff $\mathsf{M}_{\mathsf{d}}[\mathcal{Q}(x_1 \ldots x_n)] = \mathsf{S}$; iff $\mathsf{M}'_{\mathsf{d}}[\mathcal{Q}(x_1 \ldots x_n)] = \mathsf{S}$ (the latter by T10.15 since M and M' agree on assignments to symbols in $\mathcal{Q}$). Since M' and M agree on assignments to symbols other than $\mathcal{R}$, by T10.15 $\mathsf{M}'[T] = \mathsf{T}$. And $\mathsf{M}'[\mathcal{R}\vec{x} \leftrightarrow \mathcal{Q}(\vec{x})] = \mathsf{T}$: suppose otherwise; then by TI there is some d such that $\mathsf{M}'_{\mathsf{d}}[\mathcal{R}x_1 \ldots x_n \leftrightarrow \mathcal{Q}(x_1 \ldots x_n)] \neq \mathsf{S}$; so by SF($\leftrightarrow$), $\mathsf{M}'_{\mathsf{d}}[\mathcal{R}x_1 \ldots x_n] \neq \mathsf{S}$ and $\mathsf{M}'_{\mathsf{d}}[\mathcal{Q}(x_1 \ldots x_n)] = \mathsf{S}$ (or the other way around); so $\langle \mathsf{d}[x_1] \ldots \mathsf{d}[x_n] \rangle \notin \mathsf{M}'[\mathcal{R}]$ and $\mathsf{M}'_{\mathsf{d}}[\mathcal{Q}(x_1 \ldots x_n)] = \mathsf{S}$; but by construction, this is impossible; and similarly in the other case; reject the assumption, $\mathsf{M}'[\mathcal{R}\vec{x} \leftrightarrow \mathcal{Q}(\vec{x})] = \mathsf{T}$. So $\mathsf{M}'[T'] = \mathsf{T}$; so since $T' \vDash \mathcal{F}$, $\mathsf{M}'[\mathcal{F}] = \mathsf{T}$; and by T10.15 again, $\mathsf{M}[\mathcal{F}] = \mathsf{T}$; and since this reasoning applies for arbitrary M, $T \vDash \mathcal{F}$.

(o) Operator symbol. We we do not usually think of the specification for an operator as part of an interpretation and, so long as this is so, cannot extend an interpretation for operator symbols as above. Still, it is possible to provide an equivalent to the usual formulation on which operator symbols are interpreted. For any $\mathcal{P}$ and M, let $|\mathcal{P}|_{\mathsf{M}}$ be the set of all variable assignments on which $\mathcal{P}$ is satisfied. So $\mathcal{P}$ is T when $|\mathcal{P}|_{\mathsf{M}}$ is the set of all assignments, and $\mathcal{P}$ is F when $|\mathcal{P}|_{\mathsf{M}}$ is the empty set. We have understood the interpretation of a relation symbol as a set of tuples — and so as a specification of the set of interpretations on which the relation symbol is satisfied. After that, for an n-place operator $\mathcal{O}$, $\mathsf{M}[\mathcal{O}]$ is a function with members $\langle\langle V_1 \ldots V_n\rangle, V\rangle$ where $V_1 \ldots V_n$ and V are sets of assignments; and $\mathcal{O}[\mathcal{P}_1 \ldots \mathcal{P}_n]$ is satisfied on d just in case $\mathsf{d} \in \mathsf{M}[\mathcal{O}]\langle|\mathcal{P}_1|_{\mathsf{M}} \ldots |\mathcal{P}_n|_{\mathsf{M}}\rangle$. So, for example, conjunction is a function that takes $|\mathcal{P}_1|_{\mathsf{M}}$ and $|\mathcal{P}_2|_{\mathsf{M}}$ to $|\mathcal{P}_1|_{\mathsf{M}} \cap |\mathcal{P}_2|_{\mathsf{M}}$ — a conjunction $\mathcal{P}_1 \wedge \mathcal{P}_2$ is satisfied on d just in case d is among the assignments that satisfy both $\mathcal{P}_1$ and $\mathcal{P}_2$. And an existential x-quantifier takes $|\mathcal{P}|_{\mathsf{M}}$ to the set of all assignments that have an x-variant in $|\mathcal{P}|_{\mathsf{M}}$.[9]

Now extend M to a model M' like M except that $\mathsf{d} \in \mathsf{M}'[\mathcal{O}]\langle|\mathcal{P}_1|_{\mathsf{M}} \ldots |\mathcal{P}_n|_{\mathsf{M}}\rangle$ iff $\mathsf{M}_{\mathsf{d}}[\mathcal{Q}(\mathcal{P}_1 \ldots \mathcal{P}_n)] = \mathsf{S}$; iff $\mathsf{M}'_{\mathsf{d}}[\mathcal{Q}(\mathcal{P}_1 \ldots \mathcal{P}_n)] = \mathsf{S}$ (this by a simple extension of T10.15). Again since M' and M agree on assignments to symbols other than $\mathcal{O}$, with T10.15, $\mathsf{M}'[T] = \mathsf{T}$. And $\mathsf{M}'[\mathcal{O}(\vec{\mathcal{P}}) \leftrightarrow \mathcal{Q}(\vec{\mathcal{P}})] = \mathsf{T}$: suppose otherwise; then by TI there is some d such that $\mathsf{M}'_{\mathsf{d}}[\mathcal{O}(\vec{\mathcal{P}}) \leftrightarrow \mathcal{Q}(\vec{\mathcal{P}})] \neq \mathsf{S}$; so by SF($\leftrightarrow$), $\mathsf{M}'_{\mathsf{d}}[\mathcal{O}(\vec{\mathcal{P}})] \neq \mathsf{S}$ and $\mathsf{M}'_{\mathsf{d}}[\mathcal{Q}(\vec{\mathcal{P}})] = \mathsf{S}$ (or the other way around); from the second, by construction, $\mathsf{d} \in \mathsf{M}'[\mathcal{O}]\langle|\mathcal{P}_1|_{\mathsf{M}} \ldots |\mathcal{P}_n|_{\mathsf{M}}\rangle$; so $\mathsf{M}'_{\mathsf{d}}[\mathcal{O}(\vec{\mathcal{P}})] = \mathsf{S}$; this is impossible; and similarly in the other direction; reject the assumption: $\mathsf{M}'[\mathcal{O}(\vec{\mathcal{P}}) \leftrightarrow \mathcal{Q}(\vec{\mathcal{P}})] = \mathsf{T}$. So $\mathsf{M}'[T'] = \mathsf{T}$; so since $T' \vDash \mathcal{F}$,

[9] These examples are illustrative. For the primitive operators, let $\overline{|\mathcal{P}|_{\mathsf{M}}}$ be the complement of $|\mathcal{P}|_{\mathsf{M}}$. Then $|{\sim}\mathcal{P}|_{\mathsf{M}} = \overline{|\mathcal{P}|_{\mathsf{M}}}$, $|\mathcal{P} \rightarrow \mathcal{Q}|_{\mathsf{M}} = \overline{|\mathcal{P}|_{\mathsf{M}}} \cup |\mathcal{Q}|_{\mathsf{M}}$, and $\mathsf{d} \in |\forall x\mathcal{P}|_{\mathsf{M}}$ just in case all of its x-variants are in $|\mathcal{P}|_{\mathsf{M}}$.

$\mathsf{M}'[\mathcal{F}] = \mathsf{T}$; and by T10.15 again, $\mathsf{M}[\mathcal{F}] = \mathsf{T}$; and since this reasoning applies for arbitrary M, $T \vDash \mathcal{F}$.

(c) The case for constants is left as an exercise.

(f) Function symbol. Since $T \vdash \exists! y\mathcal{Q}(\vec{x}, y)$, by soundness $T \vDash \exists! y\mathcal{Q}(\vec{x}, y)$; so since $\mathsf{M}[T] = \mathsf{T}$, $\mathsf{M}[\exists! y\mathcal{Q}(\vec{x}, y)] = \mathsf{T}$; so by TI, for any d, $\mathsf{M}_{\mathsf{d}}[\exists! y\mathcal{Q}(\vec{x}, y)] = \mathsf{S}$, and there is exactly one $\mathsf{m} \in \mathsf{U}$ such that $\mathsf{M}_{\mathsf{d}(y|\mathsf{m})}[\mathcal{Q}(\vec{x}, y)] = \mathsf{S}$. Extend M to a model M' like M except that for arbitrary d, $\langle\langle \mathsf{d}[x_1] \ldots \mathsf{d}[x_n]\rangle, \mathsf{m}\rangle \in \mathsf{M}'[\mathscr{h}]$ iff $\mathsf{M}_{\mathsf{d}(y|\mathsf{m})}[\mathcal{Q}(x_1 \ldots x_n, y)] = \mathsf{S}$; by T10.15 iff $\mathsf{M}'_{\mathsf{d}(y|\mathsf{m})}[\mathcal{Q}(x_1 \ldots x_n, y)] = \mathsf{S}$. Since M' and M agree on assignments to symbols other than $\mathscr{h}$, by T10.15 $\mathsf{M}'[T] = \mathsf{T}$. And $\mathsf{M}'[y = \mathscr{h}\vec{x} \leftrightarrow \mathcal{Q}(\vec{x}, y)] = \mathsf{T}$: suppose otherwise; then by TI there is some h such that $\mathsf{M}'_{\mathsf{h}}[y = \mathscr{h}\vec{x} \leftrightarrow \mathcal{Q}(\vec{x}, y)] \neq \mathsf{S}$; so by SF($\leftrightarrow$), $\mathsf{M}'_{\mathsf{h}}[y = \mathscr{h}\vec{x}] \neq \mathsf{S}$ and $\mathsf{M}'_{\mathsf{h}}[\mathcal{Q}(\vec{x}, y)] = \mathsf{S}$ (or the other way around). Where for some a, $\mathsf{h}(y) = \mathsf{a}$, $\mathsf{h} = \mathsf{h}(y|\mathsf{a})$, and $\mathsf{M}'_{\mathsf{h}(y|\mathsf{a})}[\mathcal{Q}(x_1 \ldots x_n, y)] = \mathsf{S}$; so by construction with TA(f), $\mathsf{M}'_{\mathsf{h}}[\mathscr{h}x_1 \ldots x_n] = \mathsf{a}$; and since $\mathsf{h}(y) = \mathsf{a}$, $\mathsf{M}'_{\mathsf{h}}[y] = \mathsf{a}$; so $\mathsf{M}'_{\mathsf{h}}[y = \mathscr{h}x_1 \ldots x_n] = \mathsf{S}$; this is impossible; and similarly in the other case; reject the assumption, $\mathsf{M}'[y = \mathscr{h}\vec{x} \leftrightarrow \mathcal{Q}(\vec{x}, y)] = \mathsf{T}$. So $\mathsf{M}'[T'] = \mathsf{T}$; so since $T' \vDash \mathcal{F}$, $\mathsf{M}'[\mathcal{F}] = \mathsf{T}$; and by T10.15 again, $\mathsf{M}[\mathcal{F}] = \mathsf{T}$; and since this reasoning applies for arbitrary M, $T \vDash \mathcal{F}$.

These reasonings work insofar as M and M' give the same results for a $\mathcal{Q}$ in the original $\mathcal{L}$. It is, in fact, important to show that the specifications are consistent — that we do not both assert and deny that some objects are in the interpretation of a symbol. But this is easily done. Here one case and the start for another.

(r) The specification for a relation symbol is consistent: Suppose otherwise; that is, suppose there are some assignments d and h such that $\langle\langle \mathsf{d}[x_1] \ldots \mathsf{d}[x_n]\rangle, \mathsf{m}\rangle \in \mathsf{M}'[\mathscr{h}]$ and $\langle\langle \mathsf{h}[x_1] \ldots \mathsf{h}[x_n]\rangle, \mathsf{m}\rangle \notin \mathsf{M}'[\mathscr{h}]$ but $\mathsf{d}[x_1] = \mathsf{h}[x_1]$ and ... and $\mathsf{d}[x_n] = \mathsf{h}[x_n]$. From the first, $\mathsf{M}_{\mathsf{d}(y|\mathsf{m})}[\mathcal{Q}(x_1 \ldots x_n, y)] = \mathsf{S}$; from the second, $\mathsf{M}_{\mathsf{h}(y|\mathsf{m})}[\mathcal{Q}(x_1 \ldots x_n, y)] \neq \mathsf{S}$; but $\mathsf{d(y|m)}$ and $\mathsf{h(y|m)}$ make the same assignments to variables free in $\mathcal{Q}(\vec{x}, y)$; so by T8.4, $\mathsf{M}_{\mathsf{d}(y|\mathsf{m})}[\mathcal{Q}(\vec{x}, y)] = \mathsf{M}_{\mathsf{h}(y|\mathsf{m})}[\mathcal{Q}(\vec{x}, y)]$; so $\mathsf{M}_{\mathsf{h}(y|\mathsf{m})}[\mathcal{Q}(\vec{x}, y)] = \mathsf{S}$; reject the assumption: if $\mathsf{d}[x_1] = \mathsf{h}[x_1]$ and ... and $\mathsf{d}[x_n] = \mathsf{h}[x_n]$ and $\langle\langle \mathsf{d}[x_1] \ldots \mathsf{d}[x_n]\rangle, \mathsf{m}\rangle \in \mathsf{M}'[\mathscr{h}]$ then $\langle\langle \mathsf{h}[x_1] \ldots \mathsf{h}[x_n]\rangle, \mathsf{m}\rangle \in \mathsf{M}'[\mathscr{h}]$.

(o) The specification for an operator symbol is consistent: Suppose otherwise; that is, suppose $\mathsf{d} \in \mathsf{M}'[\mathcal{O}]\langle|\mathcal{A}_1|_{\mathsf{M}'} \ldots |\mathcal{A}_n|_{\mathsf{M}'}\rangle$ and $\mathsf{d} \notin \mathsf{M}'[\mathcal{O}]\langle|\mathcal{B}_1|_{\mathsf{M}'} \ldots |\mathcal{B}_n|_{\mathsf{M}'}\rangle$ but $|\mathcal{A}_1|_{\mathsf{M}'} = |\mathcal{B}_1|_{\mathsf{M}'}$ and ... and $|\mathcal{A}_n|_{\mathsf{M}'} = |\mathcal{B}_n|_{\mathsf{M}'}$. From the first, $\mathsf{M}'_{\mathsf{d}}[\mathcal{Q}(\mathcal{A}_1 \ldots \mathcal{A}_n)] = \mathsf{S}$ and from the second, $\mathsf{M}'_{\mathsf{d}}[\mathcal{Q}(\mathcal{B}_1 \ldots \mathcal{B}_n)] \neq \mathsf{S}$. Now reasoning is similar except with T9.10 instead of T8.4.

And now our desired result is simple. The basic idea is that for some T and $\mathscr{L}$ with a defined constant, relation symbol or function symbol, from T13.14 $T' \vdash \mathcal{F}' \leftrightarrow \mathcal{F}$ and from T13.15 $T' \vdash \mathcal{F}$ iff $T \vdash \mathcal{F}$; so that $T' \vdash \mathcal{F}'$ iff $T \vdash \mathcal{F}$. Put more generally,

T13.16. For some defined symbols, with their associated axioms and conversion procedures, $T' \vdash \mathcal{F}'$ iff $T \vdash \mathcal{F}$.

Consider a sequence of formulas $\mathcal{F}_0 \ldots \mathcal{F}_n$ and theories $T_0 \ldots T_n$ ordered according to the number of new symbols where for any i, $\mathcal{F}_i = \mathfrak{C}[\mathcal{F}_{i+1}]$. By our results, $T_{i+1} \vdash \mathcal{F}_{i+1} \leftrightarrow \mathcal{F}_i$, and $T_{i+1} \vdash \mathcal{F}_i$ iff $T_i \vdash \mathcal{F}_i$. It follows that $T_{i+1} \vdash \mathcal{F}_{i+1}$ iff $T_i \vdash \mathcal{F}_i$. And by a simple induction, $T_n \vdash \mathcal{F}_n$ iff $T_0 \vdash \mathcal{F}_0$, which is to say $T' \vdash \mathcal{F}'$ iff $T \vdash \mathcal{F}$.

In the following, we will be clear about when new symbols and associated axioms are introduced, and about the conditions under which this may be done. In light of the results we have achieved however, we will not generally distinguish between a theory and its definitional extensions.

It is worth remarking on the increased requirement for definition relative to capture. In particular, for a function, capture requires $T \vdash \forall z[\mathcal{F}(\overline{\mathsf{m}}_1 \ldots \overline{\mathsf{m}}_n, z) \rightarrow z = \overline{\mathsf{a}}]$. For definition, from uniqueness, the comparable condition is $T \vdash \forall y \forall z[(\mathcal{F}(\vec{x}, y) \wedge \mathcal{F}(\vec{x}, z)) \rightarrow y = z]$. So definition builds in a sort of generality not required in the other case. Q is great about proving particular facts — but not so great when it comes to generality (this was a sticking point about the shift between Q and Q_s in chapter 12 (p. 577 and below). But this is just the sort of thing PA is fitted to do.[10]

E13.5. Supposing that $T' \vdash y = \hbar^2 uv \leftrightarrow \mathcal{Q}(u, v, y)$ use the method of the text to find $\mathfrak{C}[A \wedge Bh^2h^2xy]$.

E13.6. (i) From the definitions in p. 637n9 and the standard abbreviations, show that the conditions in the main text for $\wedge$ and $\exists$ obtain. (ii) What is the condition for $\vee$? Hint: it should not involve complement.

*E13.7. Show T13.13af and T13.13ah. Hard core: show each of the results in T13.13.

[10]Is definition so described *necessary* for reasoning to follow? We might continue to think in terms of abbreviation — or even unabbreviated formulas themselves, so that there are no *new* symbols. Even so, the conditions on such formulas would be like those for definition, so that the overall argument would remain the same.

E13.8. (i) Complete the unfinished cases for constants in T13.14 and T13.15. (ii) Show consistency results for operator, relation and constant symbols.

First applications

Here are a couple of quick results that will be helpful as we move forward. First, if PA defines some functions $h(\vec{x}, w, \vec{z})$ and $g(\vec{y})$, then PA defines their composition $f(\vec{x}, \vec{y}, \vec{z}) = h(\vec{x}, g(\vec{y}), \vec{z})$. We introduce a definition and then show that the condition is met. This pattern will repeat many times.

T13.17. If PA defines some $h(\vec{x}, w, \vec{z})$ and $g(\vec{y})$, then PA defines $f(\vec{x}, \vec{y}, \vec{z}) = h(\vec{x}, g(\vec{y}), \vec{z})$. Suppose PA defines some $h(\vec{x}, w, \vec{z})$ and $g(\vec{y})$. Let,

Def$[f(\vec{x}, \vec{y}, \vec{z})]$ PA $\vdash v = f(\vec{x}, \vec{y}, \vec{z}) \leftrightarrow v = h(\vec{x}, g(\vec{y}), \vec{z})$. Then,

(i) PA $\vdash \exists v[v = h(\vec{x}, g(\vec{y}), \vec{z})]$

1.	$h(\vec{x}, g(\vec{y}), \vec{z}) = h(\vec{x}, g(\vec{y}), \vec{z})$	=I
2.	$\exists v[v = h(\vec{x}, g(\vec{y}), \vec{z})]$	1 ∃I

(ii) PA $\vdash \forall u \forall v[(u = h(\vec{x}, g(\vec{y}), \vec{z}) \wedge v = h(\vec{x}, g(\vec{y}), \vec{z})) \rightarrow u = v]$

1.	$j = h(\vec{x}, g(\vec{y}), \vec{z}) \wedge k = h(\vec{x}, g(\vec{y}), \vec{z})$	A ($g \rightarrow$I)
2.	$j = h(\vec{x}, g(\vec{y}), \vec{z})$	1 ∧E
3.	$k = h(\vec{x}, g(\vec{y}), \vec{z})$	1 ∧E
4.	$j = k$	2,3 =E
5.	$(j = h(\vec{x}, g(\vec{y}), \vec{z}) \wedge k = h(\vec{x}, g(\vec{y}), \vec{z})) \rightarrow j = k$	1-4 →I
6.	$\forall v[(j = h(\vec{x}, g(\vec{y}), \vec{z}) \wedge v = h(\vec{x}, g(\vec{y}), \vec{z})) \rightarrow j = v]$	5 ∀I
7.	$\forall u \forall v[(u = h(\vec{x}, g(\vec{y}), \vec{z}) \wedge v = h(\vec{x}, g(\vec{y}), \vec{z})) \rightarrow u = v]$	6 ∀I

So PA $\vdash \exists! v[v = h(\vec{x}, g(\vec{y}), \vec{z})]$ and PA defines $f(\vec{x}, \vec{y}, \vec{z})$.

In addition, we can introduce a function for *minimization*. The idea is to set $v = \mu y \mathcal{Q}(\vec{x}, y) \leftrightarrow [\mathcal{Q}(\vec{x}, v) \wedge (\forall z < v) \sim \mathcal{Q}(\vec{x}, z)]$. In the ordinary case, a new function symbol $\hbar$ is introduced with an axiom of the sort $v = \hbar\vec{x} \leftrightarrow \mathcal{Q}(\vec{x}, v)$ under the condition $T \vdash \exists! v \mathcal{Q}(\vec{x}, v)$. But, in this case, the situation is simplified by the following theorem.

T13.18. If PA $\vdash \exists v \mathcal{Q}(\vec{x}, v)$, then PA $\vdash \exists! v[\mathcal{Q}(\vec{x}, v) \wedge (\forall z < v) \sim \mathcal{Q}(\vec{x}, v)]$.

(i) Suppose PA $\vdash \exists v \mathcal{Q}(\vec{x}, v)$. Then by the least number principle T13.13ah, PA $\vdash \exists v[\mathcal{Q}(\vec{x}, v) \wedge (\forall z < v) \sim \mathcal{Q}(\vec{x}, v)]$.

(ii) Further, PA $\vdash \forall u\forall v[(\mathcal{Q}(\vec{x},u) \wedge (\forall z < u){\sim}\mathcal{Q}(\vec{x},z) \wedge \mathcal{Q}(\vec{x},v) \wedge (\forall z < v){\sim}\mathcal{Q}(\vec{x},z)) \rightarrow u = v]$.

1.	$\mathcal{Q}(\vec{x},j) \wedge (\forall z < j){\sim}\mathcal{Q}(\vec{x},z) \wedge \mathcal{Q}(\vec{x},k) \wedge (\forall z < k){\sim}\mathcal{Q}(\vec{x},z)$	A ($g \rightarrow$I)
2.	$j < k \vee j = k \vee k < j$	T13.13p
3.	$j < k$	A (c ∼I)
4.	$(\forall z < k){\sim}\mathcal{Q}(\vec{x},z)$	1 ∧E
5.	${\sim}\mathcal{Q}(\vec{x},j)$	4,3 (∀E)
6.	$\mathcal{Q}(\vec{x},j)$	1 ∧E
7.	$\bot$	6,5 ⊥I
8.	${\sim}(j < k)$	3-7 ∼I
9.	$k < j$	A (c ∼I)
10.	$(\forall z < j){\sim}\mathcal{Q}(\vec{x},z)$	1 ∧E
11.	${\sim}\mathcal{Q}(\vec{x},k)$	10,9 (∀E)
12.	$\mathcal{Q}(\vec{x},k)$	1 ∧E
13.	$\bot$	12,11, ⊥I
14.	${\sim}(k < j)$	9-13 ∼I
15.	$j = k$	2,8,14 DS
16.	$(\mathcal{Q}(\vec{x},j) \wedge (\forall z < j){\sim}\mathcal{Q}(\vec{x},z) \wedge \mathcal{Q}(\vec{x},k) \wedge (\forall z < k){\sim}\mathcal{Q}(\vec{x},z)) \rightarrow j = k$	1-15 →I
17.	$\forall v[(\mathcal{Q}(\vec{x},j) \wedge (\forall z < j){\sim}\mathcal{Q}(\vec{x},z) \wedge \mathcal{Q}(\vec{x},v) \wedge (\forall z < v){\sim}\mathcal{Q}(\vec{x},z)) \rightarrow j = v]$	16 ∀I
18.	$\forall u\forall v[(\mathcal{Q}(\vec{x},u) \wedge (\forall z < u){\sim}\mathcal{Q}(\vec{x},z) \wedge \mathcal{Q}(\vec{x},v) \wedge (\forall z < v){\sim}\mathcal{Q}(\vec{x},z)) \rightarrow u = v]$	17 ∀I

So under the condition $\exists v\mathcal{Q}(\vec{x},v)$, we have $\exists! v[\mathcal{Q}(\vec{x},v) \wedge (\forall z < v){\sim}\mathcal{Q}(\vec{x},v)]$. As from the strengthened capture result (chapter 12, p. 583) this is because the bounded quantifier builds in that at most one thing satisfies the expression. Thus we may define functions for minimization and bounded minimization under revised conditions. Let,

Def$[\mu v\mathcal{Q}(\vec{x},v)]$ PA $\vdash v = \mu v\mathcal{Q}(\vec{x},v) \leftrightarrow [\mathcal{Q}(\vec{x},v) \wedge (\forall z < v){\sim}\mathcal{Q}(\vec{x},v)]$

(i) PA $\vdash \exists v[\mathcal{Q}(\vec{x},v) \wedge (\forall z < v){\sim}\mathcal{Q}(\vec{x},v)]$.

(ii) $\forall u\forall v[(\mathcal{Q}(\vec{x},u) \wedge (\forall z < u){\sim}\mathcal{Q}(\vec{x},z) \wedge \mathcal{Q}(\vec{x},v) \wedge (\forall z < v){\sim}\mathcal{Q}(\vec{x},z)) \rightarrow u = v]$

But given T13.18, these conditions are met so long as PA $\vdash \exists v\mathcal{Q}(\vec{x},v)$.

And,

Def$[(\mu y \leq z)\mathcal{Q}(\vec{x},z,y)]$ PA $\vdash v = (\mu y \leq z)\mathcal{Q}(\vec{x},z,y) \leftrightarrow v = \mu y[y = z \vee \mathcal{Q}(\vec{x},z,y)]$

Let $m(\vec{x},z) = \mu y[y = z \vee \mathcal{Q}(\vec{x},z,y)]$ then we require,

(i) PA $\vdash \exists v(v = m(\vec{x}, z))$

(ii) PA $\vdash \forall u \forall v([u = m(\vec{x}, z) \wedge v = m(\vec{x}, z)] \rightarrow u = v)$

These conditions are trivially met so long as $m(\vec{x}, z)$ is defined; and for this, the existential condition PA $\vdash \exists y[y = z \vee \mathcal{Q}(\vec{x}, z, y)]$ follows immediately from PA $\vdash z = z$; so the conditions for bounded minimization are automatically satisfied.

Given these notions, we may write down some immediate, simple results.

*T13.19. Let $m(\vec{x}) = \mu v \mathcal{Q}(\vec{x}, v)$; then,

(a) PA $\vdash \mathcal{Q}(\vec{x}, m(\vec{x})) \wedge (\forall z < m(\vec{x})) \sim \mathcal{Q}(\vec{x}, z)$

(b) PA $\vdash \mathcal{Q}(\vec{x}, m(\vec{x}))$

(c) PA $\vdash (\forall z < m(\vec{x})) \sim \mathcal{Q}(\vec{x}, z)$

(d) PA $\vdash \mathcal{Q}(\vec{x}, v) \rightarrow m(\vec{x}) \leq v$

Because it is always possible to switch bound variables so that $\mathcal{Q}$ is converted to an equivalent $\mathcal{Q}'$ whose bound variables do not overlap with variables free in $m(\vec{x})$, we simply assume $m(\vec{x})$ is free for v in $\mathcal{Q}(\vec{x}, v)$ (and we will generally make this move). Thus (a) follows from the definition $v = m(\vec{x}) \leftrightarrow [\mathcal{Q}(\vec{x}, v) \wedge (\forall z < v) \sim \mathcal{Q}(\vec{x}, v)]$ with v instantiated to $m(\vec{x})$ together with $m(\vec{x}) = m(\vec{x})$. Both conjuncts, and so (b) and (c) follow from (a). And (d) can be done in eight or nine lines with (c).

Of these, (a) - (c) simply observe that the definition applies to the function defined. From (d), the least v such that $\mathcal{Q}(\vec{x}, v)$ is always $\leq$ an arbitrary v such that $\mathcal{Q}(\vec{x}, v)$.

In addition, a couple of results for bounded minimization.

T13.20. The following result in PA,

(a) PA $\vdash (\mu y \leq \emptyset)\mathcal{Q}(\vec{x}, \emptyset, y) = \emptyset$

(b) If PA $\vdash (\exists v \leq t(u))\mathcal{Q}(\vec{x}, u, v)$ then (i) PA defines $\mu v \mathcal{Q}(\vec{x}, u, v)$ and (ii) PA $\vdash (\mu v \leq t(u))\mathcal{Q}(\vec{x}, u, v) = \mu v \mathcal{Q}(\vec{x}, u, v)$.

Hints: (a) follows easily from the definition. For (b), the existential for (i) follows simply from $(\exists v \leq t(u))\mathcal{Q}(\vec{x}, u, v)$. For (ii),

1.	$(\exists v \leq t(u))\mathcal{Q}(\vec{x}, u, v)$	P
2.	$n(\vec{x}, u) = (\mu v \leq t(u))\mathcal{Q}(\vec{x}, u, v)$	abv
3.	$n(\vec{x}, u) = \mu v[v = t(u) \vee \mathcal{Q}(\vec{x}, u, v)]$	2 def
4.	$n(\vec{x}, u) = t(u) \vee \mathcal{Q}(\vec{x}, u, n(\vec{x}, u))$	3 T13.19b
5.	$\mathcal{Q}(\vec{x}, u, j)$	A (g 1($\exists$E))
6.	$j \leq t(u)$	
7.	$j < t(u) \vee j = t(u)$	6 T13.13m
8.	$j = t(u)$	A (g 7$\vee$E)
9.	$t(u) = n(\vec{x}, u) \vee t(u) \neq n(\vec{x}, u)$	T3.1
10.	$t(u) = n(\vec{x}, u)$	A (g 9$\vee$E)
11.	$\mathcal{Q}(\vec{x}, u, t(u))$	5,8 =E
12.	$\mathcal{Q}(\vec{x}, u, n(\vec{x}, u))$	11,10 =E
13.	$t(u) \neq n(\vec{x}, u)$	A (g 9$\vee$E)
14.	$\mathcal{Q}(\vec{x}, u, n(\vec{x}, u))$	4,13 DS
15.	$\mathcal{Q}(\vec{x}, u, n(\vec{x}, u))$	9,10-12,13-14 $\vee$E
16.	$j < t(u)$	A (g 7$\vee$E)
17.	$j = t(u) \vee \mathcal{Q}(\vec{x}, u, j)$	5 $\vee$I
18.	$n(\vec{x}, u) \leq j$	3,17 T13.19d
19.	$n(\vec{x}, u) < t(u)$	18,16 T13.13c
20.	$n(\vec{x}, u) \neq t(u)$	19 T13.13s
21.	$\mathcal{Q}(\vec{x}, u, n(\vec{x}, u))$	4,20 DS
22.	$\mathcal{Q}(\vec{x}, u, n(\vec{x}, u))$	7,8-15,16-21 $\vee$E
23.	$(\forall w < n(\vec{x}, u)){\sim}[w = t(u) \vee \mathcal{Q}(\vec{x}, u, w)]$	3 T13.19c
24.	$l < n(\vec{x}, u)$	A (g ($\forall$I))
25.	${\sim}[l = t(u) \vee \mathcal{Q}(\vec{x}, u, l)]$	23,24 ($\forall$E)
26.	$l \neq t(u) \wedge {\sim}\mathcal{Q}(\vec{x}, u, l)$	25 DeM
27.	${\sim}\mathcal{Q}(\vec{x}, u, l)$	26 $\wedge$E
28.	$(\forall w < n(\vec{x}, u)){\sim}\mathcal{Q}(\vec{x}, u, w)$	24-27 ($\forall$I)
29.	$\mathcal{Q}(\vec{x}, u, n(\vec{x}, u)) \wedge (\forall w < n(\vec{x}, u)){\sim}\mathcal{Q}(\vec{x}, u, w)$	22,28 $\wedge$I
30.	$n(\vec{x}, u) = \mu v\mathcal{Q}(\vec{x}, u, v)$	29 def
31.	$n(\vec{x}, u) = \mu v\mathcal{Q}(\vec{x}, u, v)$	1,5-30 ($\exists$E)
32.	$(\mu v \leq t(u))\mathcal{Q}(\vec{x}, u, v) = \mu v\mathcal{Q}(\vec{x}, u, v)$	31 abv

$t(u)$ is the bound, there is a $j \leq t(u)$ such that $\mathcal{Q}(\vec{x}, u, j)$, and $n(\vec{x}, u)$ is the least $v \leq t(u)$ such that $\mathcal{Q}(\vec{x}, u, v)$. Recall that, generally, when $n(\vec{x}, u) = t(u)$, $n(\vec{x}, u)$ need not be such that $\mathcal{Q}(\vec{x}, u, n(\vec{x}, u))$; but if $j = t(u) = n(\vec{x}, u)$, we have from the premise that $\mathcal{Q}(\vec{x}, u, n(\vec{x}, u))$. And in any case when $n(\vec{x}, u)$ is other than the bound, $\mathcal{Q}(\vec{x}, u, n(\vec{x}, u))$. In each case, then, the least v such that $\mathcal{Q}(\vec{x}, u, v)$ is the same as $n(\vec{x}, u)$.

From T13.20a it does not matter about $\mathcal{Q}$, the least y under the bound $\emptyset$ is always $\emptyset$. T13.20b converts between a bounded minimization and one without a bound; thus when T13.20b applies, results from from T13.19 for unbounded minimization apply to the bounded case.

*E13.9. Produce the quick derivation to show T13.19d.

E13.10. Complete the unfinished parts of T13.20.

13.3.2 Definitions for recursive functions

Our aim is to show $T \vdash \mathbb{C}ont \to \sim\mathbb{P}rvt(\overline{\ulcorner \mathcal{G} \urcorner})$ — where this corresponds to our previous result that if T is consistent, then $T \nvdash \mathcal{G}$. For this it is no surprise that we shall want to define and manipulate functions corresponding to the recursive functions of chapter 12. Thus we begin by showing that PA defines relations and functions corresponding to recursive relations and functions.

Insofar as we understand what a theorem of PA *is*, not all of the *demonstrations* are required to *understand* the argument — and some may obscure the overall flow. Thus, for our main argument, we often list results (with hints), shifting demonstrations into exercises and answers to exercises. To retain demonstration of results, a great many exercises are in fact worked in the answers section. Also since the only constant in $\mathcal{L}_{NT}$ is $\emptyset$, there is no need to reserve letters for constants. Thus it is convenient to suppose that all of $a \ldots z$ are variables of the language.

The core result

The main argument is an induction on the sequence of recursive functions. However, with an eye to the β-function, we begin showing that PA defines remainder $rm(m, n)$ and quotient $qt(m, n)$ functions corresponding to $\mathsf{m}/(\mathsf{n}+1)$. Division is by $\mathsf{n}+1$ to avoid the possibility of division by zero.[11]

*$Def[rm]$ Let PA $\vdash v = rm(m, n) \leftrightarrow (\exists w \leq m)[m = Sn \times w + v \wedge v < Sn]$.

[11] A choice is made: Another option is define the functions so that an arbitrary value is assigned for division by zero (as for example Boolos, *The Logic of Provability*, p. 27). Our selection makes for somewhat unintuitive statements of that which is intuitively true — rather than (relatively) intuitive statements including that which is intuitively undefined or false.

(i) PA $\vdash \exists x(\exists w \leq m)[m = Sn \times w + x \wedge x < Sn]$. Hint: This is an argument by IN on m. It is easy to show $\exists x(\exists w \leq \emptyset)[\emptyset = Sn \times w + x \wedge x < Sn]$, from $\emptyset = Sn \times \emptyset + \emptyset \wedge \emptyset < Sn$ with ($\exists$I) and $\exists$I. Then you want to show that if the result holds for j, it holds for Sj. For remainder k, $k < n \vee k = n$. In the first case Sj is divided by leaving the quotient l the same, and incrementing k; in the second case Sj is divided by Sl with remainder zero.

(ii) PA $\vdash \forall x \forall y[((\exists w \leq m)[m = Sn \times w + x \wedge x < Sn] \wedge (\exists w \leq m)[m = Sn \times w + y \wedge y < Sn]) \rightarrow x = y]$. Hint: This does not require IN, but is an involved derivation all the same. Once you instantiate the bounded existential quantifiers to quotients p with remainder j and q with remainder k, you have $p < q \vee p = q \vee q < p$. When $p = q$, $j = k$ follows easily with cancellation for addition. And the other cases contradict. So, if $p < q$, you will be able to set up an l such that $Sl + p = q$, and show $j \not< Sn$. And similarly in the other case.

Def$[qt]$ Let PA $\vdash v = qt(m,n) \leftrightarrow m = Sn \times v + rm(m,n)$.

(i) PA $\vdash \exists x[m = Sn \times x + rm(m,n)]$. Hint: By =I, $rm(m,n) = rm(m,n)$; so with *Def*$[rm]$, $(\exists w \leq m)[m = Sn \times w + rm(m,n) \wedge rm(m,n) < Sn]$; and the result follows easily.

(ii) PA $\vdash \forall x \forall y[(m = Sn \times x + rm(m,n) \wedge m = Sn \times y + rm(m,n)) \rightarrow x = y]$. Hint: This is easy with cancellation laws for addition and multiplication.

Def$[\beta]$ PA $\vdash \beta(p,q,i) = rm(p, q \times Si)$.

Since this is a composition of functions, immediate from T13.17.

Observe that, from the definition, PA $\vdash v = \beta(p,q,i) \leftrightarrow (\exists w \leq p)[p = S(q \times Si) \times w + v \wedge v < S(q \times Si)]$, which is to say PA $\vdash v = \beta(p,q,i) \leftrightarrow \mathscr{B}(p,q,i,v)$, where $\mathscr{B}$ is the original formula to express the beta function.

And now our main argument that PA defines relations and functions corresponding to recursive relations and functions. The main result is for functions; relations follow as an easy corollary. But we shall not be able to show that PA defines relations and functions corresponding to *all* the recursive relations and functions: Say an application of regular minimization to generate $\mathsf{f}(\vec{\mathsf{x}})$ from $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$ is (PA) *friendly* just in case PA $\vdash \exists y \mathscr{G}(\vec{x}, y, \emptyset)$ where $\mathscr{G}(\vec{x}, y, v)$ is the original formula that expresses and captures $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$; and a recursive function is (PA) *friendly* just in case it is an initial function or arises by applications of composition, recursion or friendly regular minimization. Observe that all *primitive* recursive functions are automatically friendly insofar as they involve no applications of minimization at all.

*T13.21. For any friendly recursive function $\mathsf{r}(\vec{\mathsf{x}})$ and original formula $\mathcal{R}(\vec{x}, v)$ by which it is expressed and captured, PA defines a function $\mathbb{r}(\vec{x})$ such that PA $\vdash v = \mathbb{r}(\vec{x}) \leftrightarrow \mathcal{R}(\vec{x}, v)$.

By induction on the sequence of recursive functions.

Basis: $\mathsf{r_0}(\vec{\mathsf{x}})$ is an initial function $\mathsf{suc(x)}$, $\mathsf{zero(x)}$ or $\mathsf{idnt^j_k(x_1 \ldots x_j)}$.

(s) $\mathsf{r_0}(\vec{\mathsf{x}})$ is $\mathsf{suc(x)}$. Let PA $\vdash v = \mathbb{suc}(x) \leftrightarrow Sx = v$. But $Sx = v$ is the original formula $Suc(x, v)$ by which $\mathsf{suc(x)}$ is expressed and captured; so PA $\vdash v = \mathbb{suc}(x) \leftrightarrow Suc(x, v)$. And by reasoning as follows,

1.	$Sx = Sx$	=I
2.	$\exists y(Sx = y)$	1 ∃I

1.	$Sx = j \wedge Sx = k$	A ($g \to$I)
2.	$Sx = j$	1 ∧E
3.	$Sx = k$	1 ∧E
4.	$j = k$	2,3 =E
5.	$(Sx = j \wedge Sx = k) \to j = k$	1-4 →I
6.	$\forall z[(Sx = j \wedge Sx = z) \to j = z]$	5 ∀I
7.	$\forall y \forall z[(Sx = y \wedge Sx = z) \to y = z]$	6 ∀I

PA $\vdash \exists! y(Sx = y)$. So PA defines $\mathbb{suc}(x)$.

(z) $\mathsf{r_0}(\vec{\mathsf{x}})$ is $\mathsf{zero(x)}$. Let PA $\vdash v = \mathbb{zero}(x) \leftrightarrow x = x \wedge v = \emptyset$. Then PA $\vdash v = \mathbb{zero}(x) \leftrightarrow Zero(x, v)$. And by (homework) PA defines $\mathbb{zero}(x)$.

(i) $\mathsf{r_0}(\vec{\mathsf{x}})$ is $\mathsf{idnt^j_k(x_1 \ldots x_j)}$. Let PA $\vdash v = \mathbb{idnt}^j_k(x_1 \ldots x_j) \leftrightarrow (x_1 = x_1 \wedge \ldots \wedge x_j = x_j) \wedge x_k = v$. Then PA $\vdash v = \mathbb{idnt}^j_k(x_1 \ldots x_j) \leftrightarrow Idnt^j_k(x_1 \ldots x_j, v)$. And by (homework) PA defines $\mathbb{idnt}^j_k(x_1 \ldots x_j)$.

Assp: For any i, $0 \le i < k$, and $\mathsf{r_i}(\vec{\mathsf{x}})$ with $\mathcal{R}_i(\vec{x}, v)$, PA defines $\mathbb{r}_i(\vec{x})$ such that PA $\vdash v = \mathbb{r}_i(\vec{x}) \leftrightarrow \mathcal{R}_i(\vec{x}, v)$.

Show: PA defines $\mathbb{r}_k(\vec{x})$ such that PA $\vdash v = \mathbb{r}_k(\vec{x}) \leftrightarrow \mathcal{R}_k(\vec{x}, v)$.

$\mathsf{r_k}(\vec{\mathsf{x}})$ is either an initial function or arises by composition, recursion or PA friendly regular minimization. If $\mathsf{r_k}(\vec{\mathsf{x}})$ is an initial function, then reason as in the basis. So suppose one of the other cases.

(c) $\mathsf{r_k}(\vec{\mathsf{x}}, \vec{\mathsf{y}}, \vec{\mathsf{z}})$ is $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{g}(\vec{\mathsf{y}}), \vec{\mathsf{z}})$ for some $\mathsf{h_i}(\vec{\mathsf{x}}, \mathsf{w}, \vec{\mathsf{z}})$ and $\mathsf{g_j}(\vec{\mathsf{y}})$ where $\mathsf{i, j < k}$. By assumption PA defines $\mathbb{h}(\vec{x}, w, \vec{z})$ such that PA $\vdash v = \mathbb{h}(\vec{x}, w, \vec{z}) \leftrightarrow \mathcal{H}(\vec{x}, w, \vec{z}, v)$ and PA defines $\mathbb{g}(\vec{y})$ such that PA $\vdash w = \mathbb{g}(\vec{y}) \leftrightarrow$

$\mathscr{G}(\vec{y}, w)$. Let PA $\vdash \mathbb{r}_k(\vec{x}, \vec{y}, \vec{z}) = \mathbb{h}(\vec{x}, \mathbb{g}(\vec{y}), \vec{z})$. Then by T13.17 PA defines $\mathbb{r}_k$. And, where the original $\mathcal{R}_k$ is of the sort $\exists w[\mathscr{G}(\vec{y}, w) \wedge \mathscr{H}(\vec{x}, w, \vec{z}, v)]$, PA $\vdash v = \mathbb{r}_k(\vec{x}, \vec{y}, \vec{z}) \leftrightarrow \mathcal{R}_k(\vec{x}, \vec{y}, \vec{z}, v)$. Thus, dropping $\vec{x}$ and $\vec{z}$ and reducing $\vec{y}$ to a single variable,

1.	$\mathbb{r}(y) = \mathbb{h}(\mathbb{g}(y))$	def
2.	$v = \mathbb{h}(w) \leftrightarrow \mathscr{H}(w, v)$	by assp
3.	$w = \mathbb{g}(y) \leftrightarrow \mathscr{G}(y, w)$	by assp
4.	$\quad v = \mathbb{r}(y)$	A ($g \leftrightarrow$I)
5.	$\quad v = \mathbb{h}(\mathbb{g}(y))$	1,4 =E
6.	$\quad \mathbb{g}(y) = \mathbb{g}(y)$	=I
7.	$\quad \mathbb{g}(y) = \mathbb{g}(y) \leftrightarrow \mathscr{G}(y, \mathbb{g}(y))$	3 ∀E
8.	$\quad \mathscr{G}(y, \mathbb{g}(y))$	7,6 ↔E
9.	$\quad \mathbb{h}(\mathbb{g}(y)) = \mathbb{h}(\mathbb{g}(y))$	=I
10.	$\quad \mathbb{h}(\mathbb{g}(y)) = \mathbb{h}(\mathbb{g}(y)) \leftrightarrow \mathscr{H}(\mathbb{g}(y), \mathbb{h}(\mathbb{g}(y)))$	2 ∀E
11.	$\quad \mathscr{H}(\mathbb{g}(y), \mathbb{h}(\mathbb{g}(y)))$	10,9 ↔E
12.	$\quad \mathscr{H}(\mathbb{g}(y), v)$	11,5 =E
13.	$\quad \mathscr{G}(y, \mathbb{g}(y)) \wedge \mathscr{H}(\mathbb{g}(y), v)$	8,12 ∧I
14.	$\quad \exists w[\mathscr{G}(y, w) \wedge \mathscr{H}(w, v)]$	13 ∃I
15.	$\quad \exists w[\mathscr{G}(y, w) \wedge \mathscr{H}(w, v)]$	A ($g \leftrightarrow$I)
16.	$\quad\quad \mathscr{G}(y, j) \wedge \mathscr{H}(j, v)$	A (g 15∃E)
17.	$\quad\quad j = \mathbb{g}(y) \leftrightarrow \mathscr{G}(y, j)$	3 ∀E
18.	$\quad\quad \mathscr{G}(y, j)$	16 ∧E
19.	$\quad\quad j = \mathbb{g}(y)$	17,18 ↔E
20.	$\quad\quad v = \mathbb{h}(j) \leftrightarrow \mathscr{H}(j, v)$	2 ∀E
21.	$\quad\quad \mathscr{H}(j, v)$	16 ∧E
22.	$\quad\quad v = \mathbb{h}(j)$	20,21 ↔E
23.	$\quad\quad v = \mathbb{h}(\mathbb{g}(y))$	22,19 =E
24.	$\quad\quad v = \mathbb{r}(y)$	1,23 =E
25.	$\quad v = \mathbb{r}(y)$	15,16-24 ∃E
26.	$v = \mathbb{r}(y) \leftrightarrow \exists w[\mathscr{G}(y, w) \wedge \mathscr{H}(w, v)]$	4-14,15-25 ↔I

In the first subderivation, as usual, we suppose that quantifiers are arranged so that substitutions are allowed — and in particular so that $\mathbb{g}(y)$ is free for w in $\mathscr{H}(w, v)$ and $\mathscr{G}(y, w)$. And with dropped variables restored we have that PA $\vdash v = \mathbb{r}_k(\vec{x}, \vec{y}, \vec{z}) \leftrightarrow \exists w[\mathscr{G}(\vec{y}, w) \wedge \mathscr{H}(\vec{x}, w, \vec{z}, v)]$ which is to say, PA $\vdash v = \mathbb{r}_k(\vec{x}) \leftrightarrow \mathcal{R}_k(\vec{x}, v)$.

(r) $\mathsf{r_k}(\vec{\mathsf{x}}, \mathsf{y})$ arises by recursion from some $\mathsf{g_i}(\vec{\mathsf{x}})$ and $\mathsf{h_j}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$ where $\mathsf{i}, \mathsf{j} < \mathsf{k}$. By assumption PA defines $\mathbb{g}(\vec{x})$ such that PA $\vdash v = \mathbb{g}(\vec{x}) \leftrightarrow \mathscr{G}(\vec{x}, v)$ and PA defines $\mathbb{h}(\vec{x}, y, u)$ such that PA $\vdash v = \mathbb{h}(\vec{x}, y, u) \leftrightarrow$

$\mathcal{H}(\vec{x}, y, u, v)$. Let PA $\vdash z = \mathbb{r}_k(\vec{x}, y) \leftrightarrow$

$$\exists p \exists q[\beta(p, q, \emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < y)\mathbb{h}(\vec{x}, i, \beta(p, q, i)) = \beta(p, q, Si) \wedge \beta(p, q, y) = z]$$

By the argument of the next section, PA defines $\mathbb{r}(\vec{x}, y)$. And where the original $\mathcal{R}(\vec{x}, y, z) =$

$$\exists p \exists q\{\exists v[\mathcal{B}(p, q, \emptyset, v) \wedge \mathcal{G}(\vec{x}, v)] \wedge (\forall i < y)\exists u \exists v[\mathcal{B}(p, q, i, u) \wedge \mathcal{B}(p, q, Si, v) \wedge \mathcal{H}(\vec{x}, i, u, v)] \wedge \mathcal{B}(p, q, y, z)\}$$

we require PA $\vdash z = \mathbb{r}_k(\vec{x}, y) \leftrightarrow \mathcal{R}_k(\vec{x}, y, z)$. Here is the argument from left to right.

1.	$v = \beta(p, q, i) \leftrightarrow \mathcal{B}(p, q, i, v)$	def β
2.	$v = \mathbb{g}(\vec{x}) \leftrightarrow \mathcal{G}(\vec{x}, v)$	assp
3.	$v = \mathbb{h}(\vec{x}, y, u) \leftrightarrow \mathcal{H}(\vec{x}, y, u, v)$	assp
4.	$z = \mathbb{r}(\vec{x}, y)$	A ($g \rightarrow$I)
5.	$\exists p \exists q[\beta(p, q, \emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < y)\mathbb{h}(\vec{x}, i, \beta(p, q, i)) = \beta(p, q, Si) \wedge \beta(p, q, y) = z]$	4 def $\mathbb{r}$
6.	$\beta(a, b, \emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < y)\mathbb{h}(\vec{x}, i, \beta(a, b, i)) = \beta(a, b, Si) \wedge \beta(a, b, y) = z$	A (g 5$\exists$E)
7.	$\beta(a, b, \emptyset) = \mathbb{g}(\vec{x})$	6 $\wedge$E
8.	$\mathcal{G}(\vec{x}, \mathbb{g}(\vec{x}))$	from 2
9.	$\mathcal{B}(a, b, \emptyset, \beta(a, b, \emptyset))$	from 1
10.	$\mathcal{B}(a, b, \emptyset, \mathbb{g}(\vec{x}))$	7,9 =E
11.	$\mathcal{B}(a, b, \emptyset, \mathbb{g}(\vec{x})) \wedge \mathcal{G}(\vec{x}, \mathbb{g}(\vec{x}))$	10,8 $\wedge$I
12.	$\exists v[\mathcal{B}(a, b, \emptyset, v) \wedge \mathcal{G}(\vec{x}, v)]$	11 $\exists$I
13.	$(\forall i < y)\mathbb{h}(\vec{x}, i, \beta(a, b, i)) = \beta(a, b, Si)$	6 $\wedge$E
14.	$l < y$	A (g ($\forall$I))
15.	$\mathbb{h}(\vec{x}, l, \beta(a, b, l)) = \beta(a, b, Sl)$	13,14 ($\forall$E)
16.	$\mathcal{B}(a, b, l, \beta(a, b, l))$	from 1
17.	$\mathcal{B}(a, b, Sl, \beta(a, b, Sl))$	from 1
18.	$\mathcal{H}(\vec{x}, l, \beta(a, b, l), \mathbb{h}(\vec{x}, l, \beta(a, b, l)))$	from 3
19.	$\mathcal{H}(\vec{x}, l, \beta(a, b, l), \beta(a, b, Sl))$	18,15 =E
20.	$\mathcal{B}(a, b, l, \beta(a, b, l)) \wedge \mathcal{B}(a, b, Sl, \beta(a, b, Sl)) \wedge \mathcal{H}(\vec{x}, l, \beta(a, b, l), \beta(a, b, Sl))$	16,17,19 $\wedge$I
21.	$\exists u \exists v[\mathcal{B}(a, b, l, u) \wedge \mathcal{B}(a, b, Sl, v) \wedge \mathcal{H}(\vec{x}, l, u, v)]$	20 $\exists$I
22.	$(\forall i < y)\exists u \exists v[\mathcal{B}(a, b, i, u) \wedge \mathcal{B}(a, b, Si, v) \wedge \mathcal{H}(\vec{x}, i, u, v)]$	14-21 ($\forall$I)
22.	$\beta(a, b, y) = z$	6 $\wedge$E
23.	$\mathcal{B}(a, b, y, \beta(a, b, y))$	from 1
24.	$\mathcal{B}(a, b, y, z)$	23,22 =E
25.	$\exists v[\mathcal{B}(a, b, \emptyset, v) \wedge \mathcal{G}(\vec{x}, v)] \wedge (\forall i < y)\exists u \exists v[\mathcal{B}(a, b, i, u) \wedge \mathcal{B}(a, b, Si, v) \wedge \mathcal{H}(\vec{x}, i, u, v)] \wedge \mathcal{B}(a, b, y, z)$	12,22,24 $\wedge$I
26.	$\exists p \exists q\{\exists v[\mathcal{B}(p, q, \emptyset, v) \wedge \mathcal{G}(\vec{x}, v)] \wedge (\forall i < y)\exists u \exists v[\mathcal{B}(p, q, i, u) \wedge \mathcal{B}(p, q, Si, v) \wedge \mathcal{H}(\vec{x}, i, u, v)] \wedge \mathcal{B}(p, q, y, z)\}$	25 $\exists$I
27.	$\mathcal{R}(\vec{x}, y, z)$	26 def
28.	$\mathcal{R}(\vec{x}, y, z)$	5,6-27 $\exists$E
29.	$z = \mathbb{r}(\vec{x}, y) \rightarrow \mathcal{R}(\vec{x}, y, z)$	4-28 $\rightarrow$I

The other direction is left as an exercise.

(m) $\mathsf{f}_k(\vec{\mathsf{x}})$ arises by friendly regular minimization from $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$. By assumption PA defines $g(\vec{x}, y)$ such that PA $\vdash v = g(\vec{x}, y) \leftrightarrow \mathcal{G}(\vec{x}, y, v)$ where $\mathcal{G}$ is the original formula to express and capture g. Let PA $\vdash r_k(\vec{x}) = \mu y \mathcal{G}(\vec{x}, y, \emptyset)$. Since the minimization is friendly, PA $\vdash \exists y \mathcal{G}(\vec{x}, y, \emptyset)$; so by T13.19, PA defines $r_k(\vec{x})$. And by definition, PA $\vdash v = r_k(\vec{x}) \leftrightarrow \mathcal{G}(\vec{x}, v, \emptyset) \wedge (\forall y < v){\sim}\mathcal{G}(\vec{x}, y, \emptyset)$. So PA $\vdash v = r_k(\vec{x}) \leftrightarrow \mathcal{R}_k(\vec{x}, v)$.

Indct: For any friendly recursive function $\mathsf{r}(\vec{\mathsf{x}})$ and the original formula $\mathcal{R}(\vec{x}, v)$ by which it is expressed and captured, PA defines a function $r(\vec{x})$ such that PA $\vdash v = r(\vec{x}) \leftrightarrow \mathcal{R}(\vec{x}, v)$ (subject to the recursion clause) .

*E13.11. Complete the justifications for *Def*[*rm*] and *Def*[*qt*].

*E13.12. Complete the unfinished cases to T13.21. You should set up the entire induction, but may refer to the text as the text refers unfinished cases to homework.

The Recursion Clause

We turn now to a series of results with the aim of showing that PA defines r in the case when r arises by recursion. This will require a series of definitions and results in PA. Some of the functions so defined parallel ones that will result from recursive functions. However, insofar as we have not yet proved the core result, we cannot use it! So we are showing directly that PA gives the required results.

Uniqueness. It will be easiest to begin with the uniqueness clause. Where $\mathcal{F}(\vec{x}, y, v)$ is our formula,

$$\exists p \exists q[\beta(p, q, \emptyset) = g(\vec{x}) \wedge (\forall i < y) h(\vec{x}, i, \beta(p, q, i)) = \beta(p, q, Si) \wedge \beta(p, q, y) = z]$$

we want PA $\vdash \forall m \forall n[(\mathcal{F}(\vec{x}, y, m) \wedge \mathcal{F}(\vec{x}, y, n)) \to m = n]$. The argument is structured very much as for the parallel uniqueness case in Q (T12.12) except that the argument is in PA and so by IN, and uniqueness conditions are simplified by the use of function symbols. The argument is simplified — but that does not mean that it is simple!

T13.22. With $\mathcal{F}(\vec{x}, y, v)$ as described above, PA $\vdash \forall m \forall n[(\mathcal{F}(\vec{x}, y, m) \wedge \mathcal{F}(\vec{x}, y, n)) \to m = n]$.

First theorems of chapter 13

T13.1 For any recursively axiomatized theory T whose language includes $\mathscr{L}_{NT}$, $\mathscr{G}$ is true iff it is unprovable in T (iff $T \nvdash \mathscr{G}$).

T13.2 If T is a recursively axiomatized sound theory whose language includes $\mathscr{L}_{NT}$, then T is negation incomplete.

T13.3 Let T be any recursively axiomatized theory extending Q; then $T \vdash \mathscr{G} \leftrightarrow \sim\exists x Prft(x, \overline{\ulcorner \mathscr{G} \urcorner})$.

T13.4 If T is a consistent, recursively axiomatized theory extending Q, then $T \nvdash \mathscr{G}$.

T13.5 If T is an ω-consistent, recursively axiomatized theory extending Q, then $T \nvdash \sim\mathscr{G}$.

T13.6 Let T be any recursively axiomatized theory extending Q; then $T \vdash \mathscr{R} \leftrightarrow \sim\exists x RPrft(x, \overline{\ulcorner \mathscr{R} \urcorner})$.

T13.7 If T is a consistent, recursively axiomatized theory extending Q, then $T \nvdash \mathscr{R}$.

T13.8 If T is a consistent, recursively axiomatized theory extending Q, then $T \nvdash \sim\mathscr{R}$.

T13.9 Let T be a recursively axiomatized theory extending Q. Then supposing T satisfies the derivability conditions and so the K4 logic of provability, $T \vdash Cont \rightarrow \sim Prvt(\overline{\ulcorner \mathscr{G} \urcorner})$.

T13.10 Let T be a recursively axiomatized theory extending Q. Then supposing T satisfies the derivability conditions, if T is consistent, $T \nvdash Cont$.

T13.11 Let T be a recursively axiomatized theory extending Q. Then supposing T satisfies the derivability conditions and so the K4 logic of provability, $T \vdash Cont \leftrightarrow \sim Prvt(\overline{\ulcorner Cont \urcorner})$.

T13.12 Suppose T is a recursively axiomatized theory extending Q. Then if $T \vdash \mathscr{P}$, then $T \vdash \Box\mathscr{P}$.

T13.13 This lists a number of straightforward theorems of PA.

T13.14 For a defined symbol, with its associated axiom and conversion procedure, $T' \vdash \mathscr{F}' \leftrightarrow \mathscr{F}$.

T13.15 For a T and $\mathscr{L}$, given a defined symbol with its associated axiom, and for any formula $\mathscr{F}$ in the original $\mathscr{L}$, $T' \vdash \mathscr{F}$ iff $T \vdash \mathscr{F}$.

T13.16 For some defined symbols, with their associated axioms and conversion procedures, $T' \vdash \mathscr{F}'$ iff $T \vdash \mathscr{F}$.

T13.17 If PA defines some $h(\vec{x}, w, \vec{z})$ and $g(\vec{y})$, then PA defines $f(\vec{x}, \vec{y}, \vec{z}) = h(\vec{x}, g(\vec{y}), \vec{z})$.

T13.18 If PA $\vdash \exists v \mathscr{Q}(\vec{x}, v)$, then PA $\vdash \exists! v[\mathscr{Q}(\vec{x}, v) \wedge (\forall z < v)\sim\mathscr{Q}(\vec{x}, v)]$.

T13.19 Where $m(\vec{x}) = \mu v \mathscr{Q}(\vec{x}, v)$, (a) PA $\vdash \mathscr{Q}(\vec{x}, m(\vec{x})) \wedge (\forall z < m(\vec{x}))\sim\mathscr{Q}(\vec{x}, z)$; (b) PA $\vdash \mathscr{Q}(\vec{x}, m(\vec{x}))$; (c) PA $\vdash (\forall z < m(\vec{x}))\sim\mathscr{Q}(\vec{x}, z)$; (d) PA $\vdash \mathscr{Q}(\vec{x}, v) \rightarrow m(\vec{x}) \leq v$.

T13.20 (a) PA $\vdash (\mu y \leq \emptyset)\mathscr{Q}(\vec{x}, \emptyset, y) = \emptyset$; (b) if PA $\vdash (\exists v \leq t(u))\mathscr{Q}(\vec{x}, u, v)$ then (i) PA defines $\mu v \mathscr{Q}(\vec{x}, u, v)$ and (ii) PA $\vdash (\mu v \leq t(u))\mathscr{Q}(\vec{x}, u, v) = \mu v \mathscr{Q}(\vec{x}, u, v)$.

For the zero case you need to show $\forall m \forall n[(\mathscr{F}(\vec{x}, \emptyset, m) \wedge \mathscr{F}(\vec{x}, \emptyset, n)) \rightarrow m = n]$. This is simple enough and left as an exercise. Given the zero case, here is the main argument by IN.

1.	$\forall m \forall n[(\mathscr{F}(\vec{x}, \emptyset, m) \wedge \mathscr{F}(\vec{x}, \emptyset, n)) \rightarrow m = n]$	zero case
2.	$\forall m \forall n[(\mathscr{F}(\vec{x}, j, m) \wedge \mathscr{F}(\vec{x}, j, n)) \rightarrow m = n]$	A (g →I)
3.	$\mathscr{F}(\vec{x}, Sj, u) \wedge \mathscr{F}(\vec{x}, Sj, v)$	A (g →I)
4.	$\exists p \exists q[\beta(p, q, \emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < Sj)\mathbb{h}(\vec{x}, i, \beta(p, q, i)) = \beta(p, q, Si) \wedge \beta(p, q, Sj) = u]$	3 ∧E
5.	$\exists p \exists q[\beta(p, q, \emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < Sj)\mathbb{h}(\vec{x}, i, \beta(p, q, i)) = \beta(p, q, Si) \wedge \beta(p, q, Sj) = v]$	3 ∧E
6.	$\beta(a, b, \emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < Sj)\mathbb{h}(\vec{x}, i, \beta(a, b, i)) = \beta(a, b, Si) \wedge \beta(a, b, Sj) = u$	A (g 4∃E)
7.	$\beta(a, b, \emptyset) = \mathbb{g}(\vec{x})$	6 ∧E
8.	$(\forall i < Sj)\mathbb{h}(\vec{x}, i, \beta(a, b, i)) = \beta(a, b, Si)$	6 ∧E
9.	$\beta(a, b, Sj) = u$	6 ∧E
10.	$\beta(c, d, \emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < Sj)\mathbb{h}(\vec{x}, i, \beta(c, d, i)) = \beta(c, d, Si) \wedge \beta(c, d, Sj) = v$	A (g 5∃E)
11.	$\beta(c, d, \emptyset) = \mathbb{g}(\vec{x})$	10 ∧E
12.	$(\forall i < Sj)\mathbb{h}(\vec{x}, i, \beta(c, d, i)) = \beta(c, d, Si)$	10 ∧E
13.	$\beta(c, d, Sj) = v$	10 ∧E
14.	$j < Sj$	T13.13h
15.	$\mathbb{h}(\vec{x}, j, \beta(a, b, j)) = \beta(a, b, Sj)$	8,14 (∀E)
16.	$\mathbb{h}(\vec{x}, j, \beta(c, d, j)) = \beta(c, d, Sj)$	12,14 (∀E)
17.	$k < j$	A (g (∀I))
18.	$k < Sj$	17, T13.13n
19.	$\mathbb{h}(\vec{x}, k, \beta(a, b, k)) = \beta(a, b, Sk)$	8,18 (∀E)
20.	$(\forall i < j)\mathbb{h}(\vec{x}, i, \beta(a, b, i)) = \beta(a, b, Si)$	17-19 (∀I)
21.	$\beta(a, b, j) = \beta(a, b, j)$	=I
22.	$\beta(a, b, \emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < j)\mathbb{h}(\vec{x}, i, \beta(a, b, i)) = \beta(a, b, Si) \wedge \beta(a, b, j) = \beta(a, b, j)$	7,20,21 ∧I
23.	$\exists p \exists q[\beta(p, q, \emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < j)\mathbb{h}(\vec{x}, i, \beta(p, q, i)) = \beta(p, q, Si) \wedge \beta(p, q, j) = \beta(a, b, j)]$	22 ∃I
24.	$\mathscr{F}(\vec{x}, j, \beta(a, b, j))$	23 abv
25.	$k < j$	A (g (∀I))
26.	$k < Sj$	25, T13.13n
27.	$\mathbb{h}(\vec{x}, k, \beta(c, d, k)) = \beta(c, d, Sk)$	12,26 (∀E)
28.	$(\forall i < j)\mathbb{h}(\vec{x}, i, \beta(c, d, i)) = \beta(c, d, Si)$	25-27 (∀I)
29.	$\beta(c, d, j) = \beta(c, d, j)$	=I
30.	$\beta(c, d, \emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < j)\mathbb{h}(\vec{x}, i, \beta(c, d, i)) = \beta(c, d, Si) \wedge \beta(c, d, j) = \beta(c, d, j)$	11,28,29 ∧I
31.	$\exists p \exists q[\beta(p, q, \emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < j)\mathbb{h}(\vec{x}, i, \beta(p, q, i)) = \beta(p, q, Si) \wedge \beta(p, q, j) = \beta(c, d, j)]$	30 ∃I
32.	$\mathscr{F}(\vec{x}, j, \beta(c, d, j))$	31 abv
33.	$\beta(a, b, j) = \beta(c, d, j)$	2,24,32 ∀E
34.	$\mathbb{h}(\vec{x}, j, \beta(c, d, j)) = \beta(a, b, Sj)$	15,33 =E
35.	$\beta(a, b, Sj) = \beta(c, d, Sj)$	34,16 =E
36.	$u = v$	9,13,35 =E
37.	$u = v$	5,10-36 ∃E
38.	$u = v$	4,6-37 ∃E
39.	$(\mathscr{F}(\vec{x}, Sj, u) \wedge \mathscr{F}(\vec{x}, Sj, v)) \rightarrow u = v$	3-38 →I
40.	$\forall m \forall n[(\mathscr{F}(\vec{x}, Sj, m) \wedge \mathscr{F}(\vec{x}, Sj, n)) \rightarrow m = n]$	39 ∀I
41.	$\forall m \forall n[(\mathscr{F}(\vec{x}, j, m) \wedge \mathscr{F}(\vec{x}, j, n)) \rightarrow m = n] \rightarrow \forall m \forall n[(\mathscr{F}(\vec{x}, Sj, m) \wedge \mathscr{F}(\vec{x}, Sj, n)) \rightarrow m = n]$	2-40 →I
42.	$\forall y\{\forall m \forall n[(\mathscr{F}(\vec{x}, y, m) \wedge \mathscr{F}(\vec{x}, y, n)) \rightarrow m = n] \rightarrow \forall m \forall n[(\mathscr{F}(\vec{x}, Sy, m) \wedge \mathscr{F}(\vec{x}, Sy, n)) \rightarrow m = n]\}$	41 ∀I
43.	$\forall y \forall m \forall n[(\mathscr{F}(\vec{x}, y, m) \wedge \mathscr{F}(\vec{x}, y, n)) \rightarrow m = n]$	1,42 IN
44.	$\forall m \forall n[(\mathscr{F}(\vec{x}, y, m) \wedge \mathscr{F}(\vec{x}, y, n)) \rightarrow m = n]$	43 ∀E

As before, the key to this argument is attaining $\mathscr{F}(\vec{x}, j, \beta(a, b, j))$ and $\mathscr{F}(\vec{x}, j, \beta(c, d, j))$ on lines (24) and (32). From these the assumption on (2) comes into play, and the result follows with other equalities.

*E13.13. Complete the demonstration for T13.22 by completing the demonstration of the zero case.

Existence. Considerably more difficult is the existential condition. To show this, we must show the Chinese remainder theorem in PA. Though we have resources to state the β-function, we do not yet have all that is required to duplicate reasoning from the beta function reference (for example, factorial). Thus we shall have to proceed in a different way. In particular, we specially depend on the *least common multiple* of a sequence of values. Again, we build by a series of results.

First, subtraction with cutoff. The definition is not recursive as before. However the effect is the same: $x \dot{-} y$ works like subtraction when $x \geq y$, and otherwise goes to $\emptyset$.

*$Def[\dot{-}]$ PA $\vdash v = x \dot{-} y \leftrightarrow x = y + v \vee (x < y \wedge v = \emptyset)$

(i) PA $\vdash \exists v[x = y + v \vee (x < y \wedge v = \emptyset)]$

(ii) PA $\vdash \forall m \forall n[([x = y+m \vee (x < y \wedge m = \emptyset)] \wedge [x = y+n \vee (x < y \wedge n = \emptyset)]) \rightarrow m = n]$

The proof of (i) and (ii) is left as an exercise. So PA defines ($\dot{-}$). And it proves a series of intuitive results.

*T13.23. The following result in PA:

(a) PA $\vdash a \geq b \rightarrow a = b + (a \dot{-} b)$

(b) PA $\vdash b \geq a \rightarrow a \dot{-} b = \emptyset$

(c) PA $\vdash a \dot{-} b \leq a$

(d) PA $\vdash (a \leq r \wedge r \leq s) \rightarrow r \dot{-} a \leq s \dot{-} a$

(e) PA $\vdash (a \leq r \wedge r < s) \rightarrow r \dot{-} a < s \dot{-} a$

*(f) PA $\vdash a > b \rightarrow a \dot{-} b > \emptyset$

(g) PA $\vdash a \dot{-} \emptyset = a$

(h) PA $\vdash Sa \dot{-} a = \overline{1}$

(i) PA $\vdash a > \emptyset \to a \dot{-} \overline{1} < a$

(j) PA $\vdash a \geq Sb \to a \dot{-} b = S(a \dot{-} Sb)$

(k) PA $\vdash a = Sa \dot{-} \overline{1}$

*(l) PA $\vdash a \geq c \to (a \dot{-} c) + b = (a + b) \dot{-} c$

(m) PA $\vdash (a \geq b \wedge b \geq c) \to a \dot{-} (b \dot{-} c) = (a \dot{-} b) + c$

*(n) PA $\vdash (a \dot{-} b) \dot{-} c = a \dot{-} (b + c)$

(o) PA $\vdash (a + c) \dot{-} (b + c) = a \dot{-} b$

*(p) PA $\vdash a \times (b \dot{-} c) = a \times b \dot{-} a \times c$

Hints. (f): with the assumption you can get both $a = Sj + b$ and $a = b + (a \dot{-} b)$; then you have what you need with T6.68. (l): with the assumption $a \geq c$ you have also $a + b \geq c$; so that both $a = c + (a \dot{-} c)$ and $a + b = c + [(a + b) \dot{-} c]$; then =E and T6.68 do the work. (m): You can get this with a couple applications of (l). (n): First, $a \geq b + c \vee a < b + c$; in the second case, $a \geq b \vee a < b$; in each of these cases, both sides equal $\emptyset$; for the first main option, you will be able to show that $(b + c) + [(a \dot{-} b) \dot{-} c] = (b + c) + [a \dot{-} (b + c)]$ and apply T6.68. (p): First $a = \emptyset \vee a > \emptyset$; in the first case, both sides equal $\emptyset$; then in the second case, $b \geq c \vee b < c$; again in the first of these cases, both sides equal $\emptyset$; in the last case, you will be able to show $ac + a(b \dot{-} c) = ac + (ab \dot{-} ac)$ and apply T6.68.

Many of these state standard results for subtraction — except where the inequalities are required to protect against cases when $a \dot{-} b$ goes to $\emptyset$. (a) and (b) extract basic information from the definition upon which rest depend. (c) - (k) are simple subtraction facts. And (l) - (p) are some results for association and distribution.

Next *factor*. Again, consistent with remainder and quotient, we say $m|n$ when $m + 1$ divides n.

Def[|] PA $\vdash m|n \leftrightarrow \exists q(Sm \times q = n)$

Since factor is a relation, no condition is required over and above the axiom so that the definition is good as it stands. And, again, PA proves a series of results. These are reasonably intuitive. Observe, however that our choice to divide by $m + 1$ means that, as in T13.24a below, $\emptyset|a$.

*T13.24. The following result in PA:

(a) PA $\vdash \emptyset | a$

(b) PA $\vdash a | Sa$

(c) PA $\vdash a | \emptyset$

(d) PA $\vdash a|b \rightarrow a|(b \times c)$

(e) PA $\vdash (a > \emptyset \wedge b > \emptyset) \rightarrow [(a \dot{-} \overline{1})|c \wedge (b \dot{-} \overline{1})|d \rightarrow (ab \dot{-} \overline{1})|cd]$

(f) PA $\vdash (a|Sb \wedge b|c) \rightarrow a|c$

*(g) PA $\vdash a|b \rightarrow [a|(b + c) \leftrightarrow a|c]$

(h) PA $\vdash (b \geq c \wedge a|b) \rightarrow [a|(b \dot{-} c) \leftrightarrow a|c]$

(i) PA $\vdash b > a \rightarrow b \nmid Sa$

(j) PA $\vdash a|b \leftrightarrow rm(b, a) = \emptyset$

*(k) PA $\vdash rm[a + (y \times Sd), d] = rm(a, d)$

*(l) PA $\vdash Sd \times z \leq a \rightarrow z \leq qt(a, d)$

*(m) PA $\vdash a \geq y \times Sd \rightarrow rm[a \dot{-} (y \times Sd), d] = rm(a, d)$

Hints. (g): The assumption $a|b$ gives $Sa \times j = b$; then $a|(b + c)$ gives $Sa \times k = b + c$; you will have to show $j \leq k$ so that $l + j = k$; $a|c$ follows with these; then $a|c$ gives $Sa \times k = c$ and you will be able to substitute for both b and c to get $(Sa \times j) + (Sa \times k) = b + c$; the result follows with this. (k): From the assumption you have $a = (Sd \times j) + r \wedge r < Sd$; and if you assert $a + (y \times Sd) = a + (y \times Sd)$ by =I you should be able to show $a + (y \times Sd) = Sd \times (j + y) + r \wedge r < Sd$; then with $j + y \leq a + (y \times Sd)$ you can apply (∃I) and the definition. (l): With $r = rm(a, d)$ and $q = qt(a, d)$ by *Def*[*qt*] you have $a = Sd \times q + r \wedge r < Sd$; assume $Sd \times z \leq a$ for →I and $z > q$ for ∼I; then you should be able to show $a < Sd \times z$ to contradict the assumption for →I. (m): Again let $r = rm(a, d)$ and $q = qt(a, d)$; then by *Def*[*qt*] you have $a = Sd \times q + r \wedge r < Sd$; assume $a \geq y \times Sd$ for →I; you should be able to show $a \dot{-} (y \times Sd) = Sd(q \dot{-} y) + r \wedge r < Sd$ toward $(\exists w < a \dot{-} (y \times Sd))[a \dot{-} (y \times Sd) = Sd \times w + r \wedge r < Sd]$ by (∃I), to apply *Def*[*rm*].

So (a) (the successor of) $\emptyset$ divides any number; (b) (the successor of) a divides Sa; and (c) any number divides into $\emptyset$ zero times. (d) if a divides b then it divides $b \times c$; (e) where subtraction compensates for successor, if a divides c and b divides d, ab divides cd; and (f) if a divides Sb and (the successor of) b divides c, then a divides c. (g) is like $(b + c)/a = b/a + c/a$ so that dividing the sum breaks into dividing the members; (h) is the comparable principle for subtraction. From (i) if $b > a$, then (the successor of) b does not divide Sa. (j) makes the obvious connection between reminder and factor. In (k) the remainder of the second part $(y \times Sd)$ is $\emptyset$ so that the remainder of the sum is just whatever there is from the first $rm(a, d)$; (m) is the comparable principle for subtraction. The intervening (l) is required for (m) and tells us that if z multiples of (the successor of) d come to $\leq a$, then $z \leq qt(a, d)$ — since the quotient maximizes the multiples of (the successor of) d that are $\leq a$.

And now PA defines relations *prime* and *relatively prime*. Prime has its usual sense. And numbers are relatively prime when they have no common divisor other than one — though they may not therefore individually be prime. Though division is by successor, these notions are given their usual sense by adjusting the numbers that are said to "divide."

Def[*Pr*] PA $\vdash Pr(n) \leftrightarrow \overline{1} < n \wedge \forall x[x|n \rightarrow (x = \emptyset \vee Sx = n)]$

Def[*Rp*] PA $\vdash Rp(a, b) \leftrightarrow \forall x[(x|a \wedge x|b) \rightarrow x = \emptyset]$

Since these are relations, no condition is required over and above the axioms. For any b we get $Rp(\overline{1}, b)$ since the only number that divides both $\overline{1}$ and b is (the successor of) $\emptyset$. And $Rp(\emptyset, \overline{1})$: anything divides $\emptyset$, so (the successor of) $\emptyset$ divides $\emptyset$; and the only number that divides $S\emptyset$ is (the successor of) $\emptyset$. But for $a \neq \emptyset$ (and so $Sa \neq \overline{1}$), $\sim Rp(\emptyset, Sa)$, for when $a \neq \emptyset$, both $\emptyset$ and Sa are divided by (the successor of) a and so by a number other than (the successor of) $\emptyset$.

It will be helpful to introduce a couple of subsidiary notions. When $G(a, b, i)$ we say that i is *good*, and $d(a, b)$ is (zero or) the *least* such good when a and b are greater than zero.

Def[*G*] PA $\vdash G(a, b, i) \leftrightarrow \exists x \exists y(ax + i = by)$

Def[*d*] PA $\vdash d(a, b) = \mu v[(a > \emptyset \wedge b > \emptyset) \rightarrow G(a, b, Sv)]$

(i) PA $\vdash \exists v[(a > \emptyset \wedge b > \emptyset) \rightarrow G(a, b, Sv)]$

Begin with $b = \emptyset \vee b > \emptyset$ and go for the existentially quantified goal. In the second case, there is some l such that $b = Sl$ and it is easy to show $a \times \emptyset + b = b \times \overline{1}$ and generalize.

If a or b is not greater than $\emptyset$ then $d(a, b)$ is just $\emptyset$. Otherwise, the notion is more significant.

Again, PA proves a series of results. Observe again that if we are interested in whether a prime divides some b we are interested in whether $Pr(Sa) \wedge a|b$ since it is the successor that is divided into b.

*T13.25. The following result in PA:

(a) $\text{PA} \vdash \sim Pr(\emptyset)$

(b) $\text{PA} \vdash \sim Pr(\overline{1})$

(c) $\text{PA} \vdash Pr(\overline{2})$

*(d) $\text{PA} \vdash \forall x[x > \overline{1} \rightarrow \exists z(Pr(Sz) \wedge z|x)]$

*(e) $\text{PA} \vdash Rp(a, b) \leftrightarrow \sim\exists x[Pr(Sx) \wedge x|a \wedge x|b]$

(f) $\text{PA} \vdash \forall x \forall y[G(a, b, x) \rightarrow G(a, b, x \times y)]$

*(g) $\text{PA} \vdash (a > \emptyset \wedge b > \emptyset) \rightarrow \forall x \forall y[(G(a, b, x) \wedge G(a, b, y) \wedge x \geq y) \rightarrow G(a, b, x \dot{-} y)]$

*(h) $\text{PA} \vdash [Rp(a, b) \wedge a > \emptyset \wedge b > \emptyset] \rightarrow G(a, b, \overline{1})$

*(i) $\text{PA} \vdash [Pr(Sa) \wedge a|(b \times c)] \rightarrow (a|b \vee a|c)$

Hints. (c): This is straightforward with T13.24i. (d): You can do this by the second form of strong induction T13.13ag; the zero case is trivial; to reach $\forall x\{(\forall y \leq x)[y > \overline{1} \rightarrow \exists z(Pr(Sz) \wedge z|y)] \rightarrow [Sx > \overline{1} \rightarrow \exists z(Pr(Sz) \wedge z|Sx)]\}$ assume $(\forall y \leq k)[y > \overline{1} \rightarrow \exists z(Pr(Sz) \wedge z|y)]$ and $Sk > \overline{1}$; then Sk is prime or not; if it is prime, the result is immediate; if it is not, you will be able to show $Sj \leq k$ and apply the assumption. (e): From left to right, under the assumption for $\leftrightarrow$I assume $\exists x[Pr(Sx) \wedge x|a \wedge x|b]$ and $Pr(Sj) \wedge j|a \wedge j|b$ for $\sim$I and $\exists$E; then you should be able to show that $\overline{1} < Sj$ and $\overline{1} \not< Sj$; in the other direction, under the assumption for $\leftrightarrow$I and then $j|a \wedge j|b$ for $\rightarrow$I, $j = \emptyset \vee j > \emptyset$ by T13.13f; the latter is impossible, which gives the result you want. (g): Under the assumptions

$a > \emptyset \wedge b > \emptyset$ and then $G(a,b,i) \wedge G(a,b,j) \wedge i \geq j$ for $\rightarrow$I and then $ap + i = bq$ and $ar + j = bs$ for $\exists$E, starting with $(bq + bar) + (bsa \dot{-} bs) = (bq + bar) + (bsa \dot{-} bs)$ by =I, with some effort, you will be able to show $a[(p + bs) + (br \dot{-} r)] + (i \dot{-} j) = b[(q + ar) + (sa \dot{-} s)]$ and generalize. (i): Under the assumption $Pr(Sa) \wedge a|(b \times c)$ assume $a \nmid b$ with the idea of obtaining $a \nmid b \rightarrow a|c$ for Impl; set out to show $Rp(b, Sa)$ for an application of T13.25h to get $\exists x \exists y[bx + \overline{1} = Sa \times y]$; with this, you will have $bp + \overline{1} = Sa \times q$ by $\exists$E; and you should be able to show $a|cbp$ and $a|(cbp + c)$ for an application of T13.24g.

T13.25h is important. But the argument is relatively complex; it has the following main stages.

1.	$[(a > \emptyset \wedge b > \emptyset) \rightarrow G(a,b,Sd(a,b))] \wedge (\forall y < d(a,b)) \sim[(a > \emptyset \wedge \wedge b > \emptyset) \rightarrow G(a,b,Sy)]$	def d
2.	$(a > \emptyset \wedge b > \emptyset) \rightarrow G(a,b,Sd(a,b))$	1 $\wedge$E
3.	$Rp(a,b) \wedge a > \emptyset \wedge b > \emptyset$	A (g $\rightarrow$I)
4.	$Rp(a,b)$	3 $\wedge$E
5.	$\forall x[(x \vert a \wedge x \vert b) \rightarrow x = \emptyset]$	4 def
6.	$a > \emptyset \wedge b > \emptyset$	3 $\wedge$E
7.	$G(a,b,Sd(a,b))$	2,6 $\rightarrow$E
8.	$G(a,b,a)$	[a]
9.	$G(a,b,b)$	[b]
10.	$\forall x[G(a,b,x) \rightarrow d(a,b) \vert x]$	[c]
11.	$d(a,b) \vert a$	8,10 $\forall$E
12.	$d(a,b) \vert b$	9,10 $\forall$E
13.	$d(a,b) \vert a \wedge d(a,b) \vert b$	11,12 $\wedge$I
14.	$d(a,b) = \emptyset$	5,13 $\forall$E
15.	$G(a,b,\overline{1})$	7,14 =E
16.	$[Rp(a,b) \wedge a > \emptyset \wedge b > \emptyset] \rightarrow G(a,b,\overline{1})$	3-15 $\rightarrow$I

Hint. For (c) let $q = qt(i, d(a,b))$ and $r = rm(i, d(a,b))$ then from the definitions you have $i = (Sd(a,b) \times q) + r$ and $r < Sd(a,b)$ and from (1) of the main argument $(\forall y < d(a,b)) \sim[(a > \emptyset \wedge b > \emptyset) \rightarrow G(a,b,Sy)]$; then under the assumption $G(a,b,i)$ for $\rightarrow$I you should be able to show $G(a,b,i \dot{-} (Sd(a,b) \times q))$ using (6) from the main argument with (f) and (g); but also $i \dot{-} (Sd(a,b) \times q) = r$ so that $G(a,b,r)$. Now the assumption that r is a successor leads to contradiction; so $r = \emptyset$ and $d(a,b)|i$.

T13.25(a) - (c) are simple particular facts. From (d) every number greater than one is divided by some prime (which may or may not be itself). From (e), a and b are relatively prime iff there is no prime that divides them both; in one direction this is obvious — if a prime divides them both, then they are not relatively prime; in the other direction, if some number other than (the successor of) zero divides them both, then some prime of it divides them both. (f) and (g) let you manipulate G; they are required for (h) which is in turn required for (i). (h) is an instance of Bézout's lemma according to which there are x and y such that $ax + d = by$ when d is the greatest common divisor of a and b; if a and b are relatively prime, their greatest common divisor is one. (i) is sometimes known as Euclid's lemma: if Sa is prime and Sa divides $b \times c$ then Sa divides b or c; if Sa is prime and divides $b \times c$ then it must appear in the factorization of b or the factorization of c — so that it divides one or the other.

Now *least common multiple*. Given a function $m(i)$, $lcm\{m(i) \mid i < k\}$ is the least $y > \emptyset$ such that for any $i < k$, $Sm(i)$ divides y. We avoid worries about the case when $m(i) = \emptyset$ by our usual account of factor. And since $y > \emptyset$ it is possible to define a predecessor to the least common multiple, helpful when switching between the numerator and denominator of fractions.

**Def*[*lcm*] $lcm\{m(i) \mid i < k\} = \mu v[v > \emptyset \wedge (\forall i < k)m(i)|v]$

(i) PA $\vdash \exists x[x > \emptyset \wedge (\forall i < k)m(i)|x]$

Hint: This is an argument by IN on k. For the basis, you may assert that $\overline{1} > \emptyset$; then the argument is trivial. For the main argument, under the assumptions $\exists x[x > \emptyset \wedge (\forall i < j)m(i)|x]$ for $\rightarrow$I and $a > \emptyset \wedge (\forall i < j)m(i)|a$ for $\exists$E, set out to show $a \times Sm(j) > \emptyset \wedge (\forall i < Sj)m(i)|(a \times Sm(j))$ and generalize.

Because *lcm* is defined by minimization, only the existence condition is required. As a matter of notation, let $l[m]_k = lcm\{m(i) \mid i < k\}$ and, where m is understood, let $l_k = lcm\{m(i) : i < k\}$.

Def[*plm*] $v = plm\{m(i) \mid i < k\} \leftrightarrow Sv = lcm\{m(i) \mid i < k\}$

(i) PA $\vdash \exists v(Sv = l_k)$

(ii) PA $\vdash \forall x \forall y[(Sx = l_k \wedge Sy = l_k) \rightarrow x = y]$

Again, let $p[m]_k = plm\{m(i) \mid i < k\}$ and, where m is understood, $p_k = plm\{m(i) \mid i < k\}$.

*T13.26. The following result in PA:

(a) PA $\vdash l_{\emptyset} = \overline{1}$

(b) PA $\vdash j < k \rightarrow m(j)|l_k$

*(c) PA $\vdash (\forall i < k)m(i)|x \rightarrow p_k|x$

*(d) PA $\vdash \forall n[(Pr(Sn) \wedge n|l_k) \rightarrow (\exists i < k)n|Sm(i)]$

Hints. (c): Let $q = qt(x, p_k)$ and $r = rm(x, p_k)$; assume $(\forall i < k)m(i)|x$ for $\rightarrow$I; you have $(\forall y < l_k)\sim[y > \emptyset \wedge (\forall i < k)m(i)|y]$ from def l_k with T13.19c; you should be able to apply this to show that $r = \emptyset$ and so that $p_k|x$. (d): This is an induction on k. The basis is straightforward given $l_{\emptyset} = \overline{1}$ from T13.26a; for the main argument, you have $(\forall i < j)m(i)|l_j$ from def l_j; under assumptions $\forall n[(Pr(Sn) \wedge n|l_j) \rightarrow (\exists i < j)n|Sm(i)]$ and $Pr(Sa) \wedge a|l_{Sj}$ for $\rightarrow$I, you should be able to use T13.26c to show $p_{Sj}|(l_j \times Sm(j))$; and from this $a|l_j \vee a|Sm(j)$; in either case, you have your result.

(a) for any function $m(i)$, the least common multiple for $i < 0$ defaults to $\overline{1}$. (b) applies the definition for the result that when $j < k$, $m(j)$ divides $lcm\{m(i)\,|\,i < k\}$. (c) is perhaps best conceived by prime factorization: the least common multiple of some collection has all the primes of its members and no more; but any number into which all the members of the collection divide must include all those primes; so the least common multiple divides it as well. (d) is the related result that if a prime divides the least common multiple of some collection, then it divides some member of the collection.

Finally we arrive at the Chinese Remainder Theorem. Let $m(i)$ be a function such that (successors of) its values are relatively prime; $h(i)$ is a function whose values are to be matched by remainders. Then the theorem tells us that if for all $i < k$, $m(i) > \emptyset$ and $m(i) \geq h(i)$, and if for all $i < j < k$, $Rp(Sm(i), Sm(j))$, then $\exists p(\forall i < k)rm(p, m(i)) = h(i)$. So the remainder of p and $m(i)$ matches the value of $h(i)$.

*T13.27. PA $\vdash [(\forall i < k)(m(i) > \emptyset \wedge m(i) \geq h(i)) \wedge \forall i \forall j(i < j \wedge j < k \rightarrow Rp(Sm(i), Sm(j)))] \rightarrow \exists p(\forall i < k)rm(p, m(i)) = h(i)$. Let,

$\mathcal{A}(k) =_{\text{def}} (\forall i < k)(m(i) > \emptyset \wedge m(i) \geq h(i)) \wedge \forall i \forall j(i < j \wedge j < k \rightarrow Rp(Sm(i), Sm(j)))$

$\mathcal{B}(k) =_{\text{def}} \exists p(\forall i < k)rm(p, m(i)) = h(i)$.

So we want PA $\vdash \mathcal{A}(k) \rightarrow \mathcal{B}(k)$. By induction on n we show $\forall n[n \leq k \rightarrow (\mathcal{A}(n) \rightarrow \mathcal{B}(n))]$. The result follows immediately with $k \leq k$. Here is the overall structure of the argument:

1.	$\emptyset \leq k \to (\mathscr{A}(\emptyset) \to \mathscr{B}(\emptyset))$	[a]
2.	$a \leq k \to (\mathscr{A}(a) \to \mathscr{B}(a))$	A (g →I)
3.	$Sa \leq k$	A (g →I)
4.	$a < k$	3 T13.13l
5.	$a \leq k$	4 T13.13m
6.	$\mathscr{A}(a) \to \mathscr{B}(a)$	2,5 →E
7.	$\mathscr{A}(Sa)$	A (g →I)
8.	$[(\forall i < a)(m(i) > \emptyset \wedge m(i) \geq h(i)) \wedge \forall i \forall j((i < j \wedge j < a) \to \mathcal{R}p(Sm(i), Sm(j)))] \to$ $\exists p(\forall i < a)\mathit{rm}(p, m(i)) = h(i)$	6 abv
9.	$(\forall i < Sa)(m(i) > \emptyset \wedge m(i) \geq h(i)) \wedge \forall i \forall j((i < j \wedge j < Sa) \to \mathcal{R}p(Sm(i), Sm(j)))$	7 abv
10.	$(\forall i < Sa)(m(i) > \emptyset \wedge m(i) \geq h(i))$	9 ∧E
11.	$\forall i \forall j((i < j \wedge j < Sa) \to \mathcal{R}p(Sm(i), Sm(j)))$	9 ∧E
12.	$\exists p(\forall i < a)\mathit{rm}(p, m(i)) = h(i)$	[b]
13.	$(\forall i < a)\mathit{rm}(r, m(i)) = h(i)$	A (g 12∃E)
14.	$\mathcal{R}p(l[m]_a, Sm(a))$	[c]
15.	$Sm(a) > \emptyset$	T13.13e
16.	$l_a > \emptyset$	def l_a
17.	$G(l_a, Sm(a), \overline{1})$	14,15,16 T13.25h
18.	$G(l_a, Sm(a), r + (l_a \dot{-} \overline{1}) \times h(a))$	17 T13.25f
19.	$\exists x \exists y(l_a \times x + [r + (l_a \dot{-} \overline{1}) \times h(a)] = Sm(a) \times y)$	18 def $\boldsymbol{G}$
20.	$l_a \times b + [r + (l_a \dot{-} \overline{1}) \times h(a)] = Sm(a) \times c$	A (g 19∃E)
21.	$s = l_a \times (b + h(a)) + r$	def
22.	$s = Sm(a) \times c + h(a)$	[d]
23.	$(\forall i < Sa)\mathit{rm}(s, m(i)) = h(i)$	[e]
24.	$\exists p(\forall i < Sa)\mathit{rm}(p, m(i)) = h(i)$	23 ∃I
25.	$\mathscr{B}(Sa)$	24 abv
26.	$\mathscr{B}(Sa)$	19,20-25 ∃E
27.	$\mathscr{B}(Sa)$	12,13-26 ∃E
28.	$\mathscr{A}(Sa) \to \mathscr{B}(Sa)$	7-27 →I
29.	$Sa \leq k \to (\mathscr{A}(Sa) \to \mathscr{B}(Sa))$	3-28 →I
30.	$[a \leq k \to (\mathscr{A}(a) \to \mathscr{B}(a))] \to [Sa \leq k \to (\mathscr{A}(Sa) \to \mathscr{B}(Sa))]$	2-29 →I
31.	$\forall n([n \leq k \to (\mathscr{A}(n) \to \mathscr{B}(n))] \to [Sn \leq k \to (\mathscr{A}(Sn) \to \mathscr{B}(Sn))])$	30 ∀I
32.	$(\forall n \leq k)(\mathscr{A}(n) \to \mathscr{B}(n))$	1,31 IN
33.	$k \leq k$	T13.13m
34.	$\mathscr{A}(k) \to \mathscr{B}(k)$	32,33 (∀E)

Hints. (c): Suppose otherwise; with T13.25e there is a u such that $Pr(Su) \wedge u|l_a \wedge u|Sm(a)$; then with T13.26d there is a $v < a$ such that $u|Sm(v)$ so that with (11) $\mathcal{R}p(Sm(v), Sm(a))$. But this is impossible with $u|Sm(a), u|Sm(v)$ and T13.25e. (d): By *Def[lcm]*, $l_a > \emptyset$ so that $h(a)l_a > h(a)$. Then with T13.23a and T13.23p you can show $s = (l_a \times b + [r + (l_a \dot{-} \overline{1}) \times h(a)]) + h(a)$ and apply (20). (e): Suppose for (∀I) $u < Sa$; then $u < a \vee u = a$. In the first case, with T13.26b and T13.24d $m(u)|l_a(b + h(a))$; so that there is a v such that $Sm(u)v = l_a(b + h(a))$; then using (21) and T13.24k, $\mathit{rm}(d, m(u)) =$

$rm(s, m(u))$; so that you can apply (13). In the second case, with (22) and T13.24k $rm(d, m(u)) = rm(h(u), m(u))$; but from (10), $m(u) \geq h(u)$ and you will be able to show that $rm(h(u), m(u)) = h(u)$.

The core of this derivation is to obtain (21) and (22) and from them (23). For a claim about all $i < Sa$, s appears in the forms from both (21) and (22). For any $i < a$ and x, $m(i)$ divides $l_a x$ evenly; so $m(i)$ divides the first term from (21) evenly; so the remainder of $m(i)$ and s is the same as the remainder of $m(i)$ with r — and with (13) this is just $h(i)$. But the multiplier $b + h(a)$ is chosen so that from (20) and (21), we get (22); so when $i = a$, $m(i)$ divides the first term evenly, and since $m(i) \geq h(a)$ again the remainder of $m(i)$ and s is $h(i)$. Putting these together, for any $i < Sa$, the remainder of $m(i)$ and s is $h(i)$. The "trick" to this is in the construction of s so that remainders for $i < a$ stay the same, but the remainder at a is $h(a)$.[12]

For our final result in this section, we require a couple notions for maximum value. First *maxp* for the greatest of a *pair* of values, and then *maxs* for the maximum from a *set*.

Def[*maxp*] PA $\vdash maxp(x, y) = \mu v[v \geq x \wedge v \geq y]$

(i) PA $\vdash \exists v[v \geq x \wedge v \geq y]$

Hint: $x \geq y \vee y > x$; in either case the result is easy.

Def[*maxs*] PA $\vdash maxs\{m(i) \mid i < k\} = \mu v[(\forall i < k)m(i) \leq v]$

(i) PA $\vdash \exists v[(\forall i < k)m(i) \leq v]$

Hint: First obtain *maxp* and T13.28a. Then the argument is by IN on k. For the show you will have assumptions of the sort $(\forall i < j)m(i) \leq l$ and $a < Sj$; then $a < j \vee a = j$; in either case you will be able to show that $m(a) \leq maxp(l, m(j))$.

So $maxp(x, y)$ is the maximum of x and y, and $maxs\{m(i) \mid i < k\}$ is the maximum from $m(i)$ with $i < k$. As a matter of notation, let $maxs[m]_k = maxs\{m(i) \mid i < k\}$ and where m is understood, $maxs_k = maxs\{m(i) \mid i < k\}$. A couple of results are immediate with T13.19b.

T13.28. The following result in PA.

[12]For this construction see Boolos, *The Logic of Provability*, 30-31.

(a) PA $\vdash maxp(x, y) \geq x \wedge maxp(x, y) \geq y$

(b) PA $\vdash (\forall i < k)m(i) \leq maxs_k$

These simply state the obvious: that the maximum is greater than or equal to the rest. From (a) the maximum is the greater of the the two in the pair; from (b) the maximum is the greatest of the values of the function.

Now we are in a position to generate some results for the β function. With values of q and $m(i)$ as below, we may demonstrate the antecedent to the *CRT* (T13.27), and so obtain its consequent — where this is a result for the β-function.

*T13.29. PA $\vdash \exists p \exists q(\forall i < k)\beta(p, q, i) = h(i)$.

Let $r =_{\text{def}} maxp(k, maxs[h]_k)$;

$s =_{\text{def}} Sr$;

$q =_{\text{def}} lcm\{i \mid i < s\}$;

$m(i) =_{\text{def}} q \times Si$.

Recall from *Def*[*beta*] that PA $\vdash \beta(p, q, i) = rm(p, q \times Si)$. And we may reason,

1.	$(\forall i < k)(m(i) > \emptyset \wedge m(i) \geq h(i))$	[i]
2.	$\forall i \forall j[(i < j \wedge j < k) \to Rp(Sm(i), Sm(j))]$	[ii]
3.	$\exists p(\forall i < k)rm(p, m(i)) = h(i)$	1,2 T13.27
4.	$m(i) = q \times Si$	def
5.	$\exists p(\forall i < k)rm(p, q \times Si) = h(i)$	3,4 =E
6.	$\beta(p, q, i) = rm(p, q \times Si)$	def
7.	$\exists p(\forall i < k)\beta(p, q, i) = h(i)$	5,6 =E
8.	$\quad(\forall i < k)\beta(p, q, i) = h(i)$	A (g 7∃E)
9.	$\quad\exists q(\forall i < k)\beta(p, q, i) = h(i)$	8 ∃I
10.	$\quad\exists p \exists q(\forall i < k)\beta(p, q, i) = h(i)$	9 ∃I
11.	$\exists p \exists q(\forall i < k)\beta(p, q, i) = h(i)$	7,8-10 ∃E

So the demonstration reduces to that of (i) and (ii), the two conjuncts to the antecedent of *CRT* (T13.27). (i): Under the assumption $j < k$ for (∀I) it will be easy to show $m(j) > \emptyset$; then you will be able to use T13.28 to show $h(j) < s$; but also with T13.26b that $r|q$ and from this that $s \leq q$ which gives $s \leq q \times Sj$ and the result you want. (ii): Here is the main outline of the argument.

1.	$i < j \wedge j < k$	A g $\rightarrow$I
2.	$i < j$	1 $\wedge$E
3.	$j < k$	1 $\wedge$E
4.	$\sim Rp(Sm(i), Sm(j))$	A (c $\sim$I)
5.	$\exists x[Pr(Sx) \wedge x\|S(q \times Si) \wedge x\|S(q \times Sj)]$	4 T13.25e
6.	$Pr(Sa) \wedge a\|S(q \times Si) \wedge a\|S(q \times Sj)$	A (c 5$\exists$E)
7.	$Pr(Sa)$	6 $\wedge$E
8.	$a\|S(q \times Si)$	6 $\wedge$E
9.	$a\|S(q \times Sj)$	6 $\wedge$E
10.	$a\|q(j \dot{-} i)$	[a]
11.	$a\|q \vee a\|(j \dot{-} i)$	7,10 T13.25i
12.	$a\|q$	A (g 11$\vee$E)
13.	$a\|q$	12 R
14.	$a\|(j \dot{-} i)$	A (g 11$\vee$E)
15.	$a\|q$	[b]
16.	$a\|q$	11,12-13,14-15 $\vee$E
17.	$a\|(q \times Si)$	16 T13.24d
18.	$S(q \times Si) > q \times Si$	T13.13h
19.	$S(q \times Si) \geq q \times Si$	18 T13.13m
20.	$a\|(S(q \times Si) \dot{-} (q \times Si))$	19,8,17 T13.24h
21.	$a\|\overline{1}$	20 T13.23h
22.	$S\emptyset < Sa$	def Pr
23.	$\emptyset < a$	22 T13.13k
24.	$a \nmid \overline{1}$	23 T13.24i
25.	$\bot$	21,24 $\bot$I
26.	$\bot$	5,6-25 $\exists$E
27.	$Rp(Sm(i), Sm(j))$	4-26 $\sim$E
28.	$(i < j \wedge j < k) \rightarrow Rp(Sm(i), Sm(j))]$	1-27 $\rightarrow$I
29.	$\forall i \forall j[(i < j \wedge j < k) \rightarrow Rp(Sm(i), Sm(j))]$	28 $\forall$I

Hints. (a): With $i < j$ you will be able to show $a|(S(q \times Sj) \dot{-} S(q \times Si))$; and with some work that $S(q \times Sj) \dot{-} S(q \times Si) = q(j \dot{-} i)$. (b): With $i < j$, you have $j \dot{-} i > \emptyset$; so there is an l such that $Sl + \emptyset = j \dot{-} i$; you will be able to show $a|Sl$ and with T13.26b, $l|q$ so with T13.24f, $a|q$.

Now a theorem that uses this result to show that a β-function for values $< k$ can always be extended to another like it but with an arbitrary k^{th} value. We show that given $\beta(a, b, i)$ there are sure to be p and q such that $\beta(p, q, i)$ is like $\beta(a, b, i)$ for $i < k$ and for arbitrary n, $\beta(p, q, k) = n$. This is because we may *define* a function h which is like $\beta(a, b, i)$ for $i < k$ and otherwise n — and find p, q such that $\beta(p, q, i)$ matches it. As a preliminary,

Def[$h(i)$] PA $\vdash v = h(i) \leftrightarrow [(i < k \wedge v = \beta(a, b, i)) \vee (i \geq k \wedge v = n)]$

(i) PA $\vdash \exists v[(i < k \wedge v = \beta(a,b,i)) \vee (i \geq k \wedge v = n)]$

(ii) PA $\vdash \forall x \forall y[([(i < k \wedge x = \beta(a,b,i)) \vee (i \geq k \wedge x = n)] \wedge [(i < k \wedge y = \beta(a,b,i)) \vee (i \geq k \wedge y = n)]) \rightarrow x = y]$

Then,

*T13.30. PA $\vdash \exists p \exists q[(\forall i < k)\beta(p,q,i) = \beta(a,b,i) \wedge \beta(p,q,k) = n]$.

Hints: From *Def*[$h(i)$] you have $(k < k \wedge h(k) = \beta(a,b,k)) \vee (k \geq k \wedge h(k) = n)$ and $(l < k \wedge h(l) = \beta(a,b,l)) \vee (l \geq k \wedge h(l) = n)$; and from T13.29 applied to Sk, $\exists p \exists q(\forall i < Sk)\beta(p,q,i) = h(i)$; then with $(\forall i < Sk)\beta(c,d,i) = h(i)$ for $\exists$E, you will be able to show that $\beta(c,d,k) = n$ and under $l < k$ for ($\forall$I) that $\beta(c,d,l) = \beta(a,b,l)$.

For application of this theorem, it is important that free variables are universally quantified. So the theorem is effectively $\forall k \forall n \forall a \forall b \exists p \exists q[(\forall i < k)\beta(p,q,i) = \beta(a,b,i) \wedge \beta(p,q,k) = n]$

And finally the result we have been after in this section: As before, let $\mathscr{F}(\vec{x}, y, v)$ be our formula,

$$\exists p \exists q[\beta(p,q,\emptyset) = \mathbbm{g}(\vec{x}) \wedge (\forall i < y)\mathbbm{h}(\vec{x}, i, \beta(p,q,i)) = \beta(p,q,Si) \wedge \beta(p,q,y) = v]$$

Then we want, PA $\vdash \exists v \mathscr{F}(\vec{x}, y, v)$.

*T13.31. For $\mathscr{F}$ as above, PA $\vdash \exists v \mathscr{F}(\vec{x}, y, v)$.

Let $\mathscr{F}(\vec{x}, y, v)$ be as above; the argument is by IN on y. The zero case is left as an exercise. Here is the main argument.

1.	$\exists v\mathscr{F}(\vec{x}, \emptyset, v)$	zero case
2.	$\exists v\mathscr{F}(\vec{x}, j, v)$	A (g →I)
3.	$\exists v\exists p\exists q[\beta(p,q,\emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < j)\mathbb{h}(\vec{x}, i, \beta(p,q,i)) = \beta(p,q,Si) \wedge \beta(p,q,j) = v]$	2 abv
4.	$\beta(a,b,\emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < j)\mathbb{h}(\vec{x}, i, \beta(a,b,i)) = \beta(a,b,Si) \wedge \beta(a,b,j) = z$	A (g 3∃E)
5.	$\beta(a,b,\emptyset) = \mathbb{g}(\vec{x})$	4 ∧E
6.	$(\forall i < j)\mathbb{h}(\vec{x}, i, \beta(a,b,i)) = \beta(a,b,Si)$	4 ∧E
7.	$\exists p\exists q[(\forall i < Sj)\beta(p,q,i) = \beta(a,b,i) \wedge \beta(p,q,Sj) = \mathbb{h}(\vec{x}, j, \beta(a,b,j))]$	T13.30 ∀E
8.	$(\forall i < Sj)\beta(c,d,i) = \beta(a,b,i) \wedge \beta(c,d,Sj) = \mathbb{h}(\vec{x}, j, \beta(a,b,j))$	A (g 7∃E)
9.	$(\forall i < Sj)\beta(c,d,i) = \beta(a,b,i)$	8 ∧E
10.	$\beta(c,d,Sj) = \mathbb{h}(\vec{x}, j, \beta(a,b,j))$	8 ∧E
11.	$\emptyset < Sj$	T13.13e
12.	$\beta(c,d,\emptyset) = \beta(a,b,\emptyset)$	9,11 (∀E)
13.	$\beta(c,d,\emptyset) = \mathbb{g}(\vec{x})$	5,12 =E
14.	$l < Sj$	A (g (∀I))
15.	$\beta(c,d,l) = \beta(a,b,l)$	9,14 (∀E)
16.	$l < j \vee l = j$	14 T13.13n
17.	$l < j$	A (g 16∨E)
18.	$\mathbb{h}(\vec{x}, l, \beta(a,b,l)) = \beta(a,b,Sl)$	6,17 (∀E)
19.	$Sl < Sj$	17 T13.13k
20.	$\beta(c,d,Sl) = \beta(a,b,Sl)$	9,19 ∀E
21.	$\mathbb{h}(\vec{x}, l, \beta(a,b,l)) = \beta(c,d,Sl)$	18,20 =E
22.	$l = j$	A (g 16∨E)
23.	$\mathbb{h}(\vec{x}, l, \beta(a,b,l)) = \beta(c,d,Sl)$	10,22 =E
24.	$\mathbb{h}(\vec{x}, l, \beta(c,d,l)) = \beta(c,d,Sl)$	15,23 =E
25.	$\mathbb{h}(\vec{x}, l, \beta(c,d,l)) = \beta(c,d,Sl)$	16,17-21,22-24 ∨E
26.	$(\forall i < Sj)\mathbb{h}(\vec{x}, i, \beta(c,d,i)) = \beta(c,d,Si)$	14-25 (∀I)
27.	$\beta(c,d,Sj) = \beta(c,d,Sj)$	=I
28.	$\beta(c,d,\emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < Sj)\mathbb{h}(\vec{x}, i, \beta(c,d,i)) = \beta(c,d,Si) \wedge \beta(c,d,Sj) = \beta(c,d,Sj)$	13,26,27 ∧I
29.	$\exists v\exists p\exists q[\beta(p,q,\emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < Sj)\mathbb{h}(\vec{x}, i, \beta(p,q,i)) = \beta(p,q,Si) \wedge \beta(p,q,Sj) = v]$	28 ∃I
30.	$\exists v\mathscr{F}(\vec{x}, Sj, v)$	29 abv
31.	$\exists v\mathscr{F}(\vec{x}, Sj, v)$	7,8-30 ∃E
32.	$\exists v\mathscr{F}(\vec{x}, Sj, v)$	3,4-31 ∃E
33.	$\exists v\mathscr{F}(\vec{x}, j, v) \rightarrow \exists v\mathscr{F}(\vec{x}, Sj, v)$	2-32 →I
34.	$\forall y[\exists v\mathscr{F}(\vec{x}, y, v) \rightarrow \exists v\mathscr{F}(\vec{x}, Sy, v)]$	33 ∀I
35.	$\exists v\mathscr{F}(\vec{x}, y, v)$	1,34 IN

From the assumption, there are a, b such that the β-function has the right features for every $i < j$. With T13.30 there are c, d such that the β-function has the right features for $i < Sj$. The derivation establishes that this is so and generalizes.

This completes the demonstration of T13.21! So for any friendly recursive function $\mathsf{r}(\vec{\mathsf{x}})$ and original formula $\mathscr{R}(\vec{x}, v)$ by which it is expressed and captured, PA defines a function $\mathbb{r}(\vec{x})$ such that PA $\vdash v = \mathbb{r}(\vec{x}) \leftrightarrow \mathscr{R}(\vec{x}, v)$. In particular, then, PA defines functions corresponding to all the primitive recursive functions from chapter 12.

In addition, say a recursive relation is *friendly* iff it has a friendly characteristic function. Then as a simple corollary, PA defines relations corresponding to each friendly recursive relation, equivalent to the original formulas used to express them.

T13.32. For any friendly recursive relation $\mathsf{R}(\vec{\mathsf{x}})$ with characteristic function $\mathsf{ch}_{\mathsf{R}}(\vec{\mathsf{x}})$, PA defines a relation $\mathbb{R}(\vec{x})$ such that PA $\vdash \mathbb{R}(\vec{x}) \leftrightarrow \mathbb{ch}_{\mathsf{R}}(\vec{x}) = \emptyset$. As a simple corollary, where $\mathsf{R}(\vec{\mathsf{x}})$ is originally captured by $\mathcal{R}(\vec{x}, \emptyset)$, PA $\vdash \mathbb{R}(\vec{x}) \leftrightarrow \mathcal{R}(\vec{x}, \emptyset)$.

Suppose a friendly recursive relation R has recursive characteristic function $\mathsf{ch}_{\mathsf{R}}(\vec{\mathsf{x}})$. Since R is friendly, it has a friendly characteristic function that is defined in PA. Set,

$$\text{PA} \vdash \mathbb{R}(\vec{x}) \leftrightarrow \mathbb{ch}_{\mathsf{R}}(\vec{x}) = \emptyset$$

Then PA defines $\mathbb{R}(\vec{x})$. In fact, however, for relations defined in chapter 12 we will want to define relations whose structure matches the structure of functions there defined. For this, it will be helpful to obtain the same result by an (informal) induction.

(a) Say an *atomic* recursive relation is one like EQ, LEQ or LESS whose characteristic function does not depend on the characteristic functions of other recursive relations. Then let,

$$\text{PA} \vdash \mathbb{R}(\vec{x}) \leftrightarrow \mathbb{ch}_{\mathsf{R}}(\vec{x}) = \emptyset$$

(b) Now suppose PA $\vdash \mathbb{P}_1(\vec{x}) \leftrightarrow \mathbb{ch}_{\mathsf{P}_1}(\vec{x}) = \emptyset$ and …and PA $\vdash \mathbb{P}_n(\vec{x}) \leftrightarrow \mathbb{ch}_{\mathsf{P}_n}(\vec{x}) = \emptyset$. And consider a recursive operator $\mathsf{OP}(\mathsf{P}_1(\vec{\mathsf{x}}) \ldots \mathsf{P}_n(\vec{\mathsf{x}}))$ with characteristic function $\mathsf{f}(\mathsf{ch}_{\mathsf{P}_1}(\vec{\mathsf{x}}) \ldots \mathsf{ch}_{\mathsf{P}_n}(\vec{\mathsf{x}}))$. Since $\mathsf{f}(\mathsf{ch}_{\mathsf{P}_1}(\vec{\mathsf{x}}) \ldots \mathsf{ch}_{\mathsf{P}_n}(\vec{\mathsf{x}}))$ is friendly, PA defines $\mathbb{f}(\vec{x})$. Let $\mathbb{c}_{\mathsf{P}}(\vec{x}) = \mu v[(\mathbb{P}(\vec{x}) \wedge v = \emptyset) \vee ({\sim}\mathbb{P}(\vec{x}) \wedge v = \overline{1})]$ and set,

$$\text{PA} \vdash \mathbb{Op}(\mathbb{P}_1(\vec{x}) \ldots \mathbb{P}_n(\vec{x})) \leftrightarrow \mathbb{f}(\mathbb{c}_{\mathsf{P}_1}(\vec{x}) \ldots \mathbb{c}_{\mathsf{P}_n}(\vec{x})) = \emptyset$$

From this axiom, $\mathbb{Op}$ is defined by an expression including $\mathbb{c}_{\mathsf{P}_1} \ldots \mathbb{c}_{\mathsf{P}_n}$ of which $\mathbb{P}_1 \ldots \mathbb{P}_n$ are parts. So it works like the axiom from 13.3.1. But by T13.38 (which we shall see shortly), PA $\vdash \mathbb{ch}_{\mathsf{P}}(\vec{x}) = \emptyset \vee \mathbb{ch}_{\mathsf{P}}(\vec{x}) = \overline{1}$; and it is easy to see, PA $\vdash \mathbb{c}_{\mathsf{P}}(\vec{x}) = \mathbb{ch}_{\mathsf{P}}(\vec{x})$; so that PA $\vdash \mathbb{Op}(\mathbb{P}_1(\vec{x}) \ldots \mathbb{P}_n(\vec{x})) \leftrightarrow \mathbb{f}(\mathbb{ch}_{\mathsf{P}_1}(\vec{x}) \ldots \mathbb{ch}_{\mathsf{P}_n}(\vec{x})) = \emptyset$. Now for any $\mathsf{R}(\vec{\mathsf{x}}) = \mathsf{OP}(\mathsf{P}_1(\vec{\mathsf{x}}) \ldots \mathsf{P}_n(\vec{\mathsf{x}}))$ set,

$$\text{PA} \vdash \mathbb{R}(\vec{x}) \leftrightarrow \mathbb{O}p(\mathbb{P}_1(\vec{x}) \ldots \mathbb{P}_n(\vec{x}))$$

Then PA $\vdash \mathbb{R}(\vec{x}) \leftrightarrow \mathbb{f}(\mathbb{ch}_{\mathsf{P}_1}(\vec{x}) \ldots \mathbb{ch}_{\mathsf{P}_n}(\vec{x})) = \emptyset$; which is to say, PA $\vdash \mathbb{R}(\vec{x}) \leftrightarrow \mathbb{ch}_{\mathsf{R}}(\vec{x}) = \emptyset$.

(d) So for any primitive recursive relation defined in chapter 12, PA $\vdash \mathbb{R}(\vec{x}) \leftrightarrow \mathbb{ch}_{\mathsf{R}}(\vec{x}) = \emptyset$. Further, with T13.21, PA $\vdash v = \mathbb{ch}_{\mathsf{R}}(\vec{x}) \leftrightarrow \mathcal{R}(\vec{x}, v)$; so PA $\vdash \emptyset = \mathbb{ch}_{\mathsf{R}}(\vec{x}) \leftrightarrow \mathcal{R}(\vec{x}, \emptyset)$; so PA $\vdash \mathbb{R}(\vec{x}) \leftrightarrow \mathcal{R}(\vec{x}, \emptyset)$.

So for example, from part (a) we have, say, PA $\vdash \mathbb{E}q(\vec{x}) \leftrightarrow \mathbb{ch}_{\mathsf{EQ}}(\vec{x}) = \emptyset$. For part (b), $\mathsf{DSJ}(\mathsf{P}(\vec{\mathsf{x}}), \mathsf{Q}(\vec{\mathsf{x}}))$ has characteristic function $\mathsf{times}(\mathsf{ch}_{\mathsf{P}}(\vec{\mathsf{x}}), \mathsf{ch}_{\mathsf{Q}}(\vec{\mathsf{x}}))$; so we set PA $\vdash \mathbb{D}sj(\mathbb{P}(\vec{x}), \mathbb{Q}(\vec{x})) \leftrightarrow \mathbb{times}(\mathbb{ch}_{\mathsf{P}}(\vec{x}), \mathbb{ch}_{\mathsf{Q}}(\vec{x})) = \emptyset$; then where $\mathsf{R}(\vec{\mathsf{x}}) = \mathsf{DSJ}(\mathsf{P}(\vec{\mathsf{x}}), \mathsf{Q}(\vec{\mathsf{x}}))$, PA $\vdash \mathbb{R}(\vec{x}) \leftrightarrow \mathbb{D}sj(\mathbb{P}(\vec{x}), \mathbb{Q}(\vec{x}))$. Thus PA defines both functions and relations corresponding to the friendly recursive functions and relations, equivalent to the original formulas used to express and capture them.

*E13.14. Show (i) and (ii) for *Def*[$\dot{-}$]. Then show T13.23 (a) and (o). Hard core: show all of the results in T13.23.

*E13.15. Show T13.24d and T13.24i. Hard core: show all of the results in T13.24.

*E13.16. Provide a complete demonstration of T13.25h including the justification for d. Hard core: Show all of the results from T13.25.

*E13.17. Show the condition for *Def*[*lcm*] and provide a demonstration for T13.26d. Hard core: show all of the results for *Def*[*lcm*], *Def*[*plm*] and T13.26.

*E13.18. Provide derivations to show each of [a] - [e] to complete the derivation for T13.27.

E13.19. Provide a derivation to show the condition of *Def*[*maxs*]. Hard core: Provide justifications for *Def*[*maxs*] and *Def*[*maxp*]; and show the results in T13.28.

*E13.20. Complete the demonstration for T13.29.

Font conventions

At different stages, we employ different fonts for items of different sorts. For the most part, this is straightforward. Here we collect our conventions together.

1. Expressions of symbolic object languages are given in italics; these include the function (lowercase) and relation (first letter uppercase) symbols abbreviated or defined in Q and PA.

   function, *Relation*

2. Objects from the semantic account are indicated by a sans-serif font; these include recursive functions (lowercase) and relations (small-caps) — and bold when special symbols are used.

   $\mathsf{function}$, $\mathsf{RELATION}$,

3. The language for description of expressions in the formal object language uses script variables,

   $\mathscr{P}$, $\mathscr{p}$

4. The language for description of metalinguistic expressions uses Fraktur variables,

   $\mathfrak{A}$, $\mathfrak{a}$

5. Function and relation symbols introduced into PA from recursive functions and relations by T13.21 and T13.32 have their first character in a "hollow" blackboard bold font — these are not automatically equivalent to ones that may be described in (1), though we may set out to demonstrate equivalence.

   $\mathbb{f}$*unction*, $\mathbb{R}$*elation*

6. Object expressions for computer languages are given in a typewriter font,

   `Expression`

7. In addition, for informal inductions italic i, j generally index objects arranged in series, but i, j when the objects are specifically the members of $\mathbb{N}$.

*E13.21. Show T13.30. Hard core: show the conditions for $Def[h(i)]$.

*E13.22. Complete the demonstration of T13.31 by showing the zero case.

E13.23. Give the demonstration to show PA $\vdash \mathbb{O}p(\mathbb{P}_1(\vec{x}) \ldots \mathbb{P}_n(\vec{x})) \leftrightarrow \mathbb{f}(\mathbb{ch}_{\mathsf{P}_1}(\vec{x}) \ldots \mathbb{ch}_{\mathsf{P}_n}(\vec{x})) = \emptyset$ from (b) of T13.32.

13.4 The Second Condition: $\Box(\mathcal{P} \to \mathcal{Q}) \to (\Box\mathcal{P} \to \Box\mathcal{Q})$

We turn now to demonstration of the second derivability condition. Again there is some background — after which demonstration of the condition itself is straightforward. The overall idea is simple: Suppose both $\Box(\mathcal{P} \to \mathcal{Q})$ and $\Box\mathcal{P}$. Then there are j and k such that $\textsf{PRFT}(\mathsf{j}, \ulcorner\mathcal{P} \to \mathcal{Q}\urcorner)$ and $\textsf{PRFT}(\mathsf{k}, \ulcorner\mathcal{P}\urcorner)$. Intuitively, then, $\mathsf{l} = \mathsf{j} \star \mathsf{k} \star 2^{\ulcorner\mathcal{Q}\urcorner}$ numbers a proof of $\mathcal{Q}$ — for we prove $\mathcal{P} \to \mathcal{Q}$ and $\mathcal{P}$, so that $\mathcal{Q}$ follows immediately as the last line by MP. So $\textsf{PRFT}(\mathsf{l}, \ulcorner\mathcal{Q}\urcorner)$, and $\Box\mathcal{Q}$ follows from the assumptions. The task is to prove all of this in PA.

13.4.1 Some Applications

Having shown that PA defines recursive functions, we require some results about them. To start, observe that $\mathbb{plus}(x, y)$, say, is defined by a complex expression through recursion, and so is not the same expression as our old friend $x + y$. Thus it is not obvious that our standard means for manipulation of $+$ apply to $\mathbb{plus}$. We could recover our ordinary results if we could show PA $\vdash x + y = \mathbb{plus}(x, y)$. And similar comments apply to other ordinary functions and relations. Thus initially we seek to show that defined relations functions are equivalent to ones with which we are familiar. Again many details are shifted to exercises and/or answers to exercises.

Equivalencies. We begin with equivalences between functions and relations already defined in PA, and ones that result by T13.21 and T13.32. So we begin with functions and relations from $\mathcal{L}_{\text{NT}}$ including S, $+$, $\times$, $=$, $\leq$, $<$, truth functional operators, bounded quantifiers and bounded minimization.

As a preliminary, we require a result that is fundamental to every case where a function is defined by recursion. As above let $\mathcal{F}(\vec{x}, y, v)$ be,

$$\exists p \exists q[\beta(p, q, \emptyset) = \mathbb{g}(\vec{x}) \wedge (\forall i < y)\mathbb{h}(\vec{x}, i, \beta(p, q, i)) = \beta(p, q, Si) \wedge \beta(p, q, y) = v]$$

and suppose PA $\vdash v = f(\vec{x}, y) \leftrightarrow \mathcal{F}(\vec{x}, y, v)$ so that $f(\vec{x}, y)$ is defined by recursion. Then the standard recursive conditions apply. That is,

T13.33. Suppose $f(\vec{x}, y)$ is defined by $g(\vec{x})$ and $h(\vec{x}, y, u)$ so that PA $\vdash v = f(\vec{x}, y) \leftrightarrow \mathcal{F}(\vec{x}, y, v)$. Then,

(a) PA $\vdash f(\vec{x}, \emptyset) = g(\vec{x})$

(b) PA $\vdash f(\vec{x}, S(y)) = h(\vec{x}, y, f(\vec{x}, y))$

Hint: (a) follows easily in 6 lines with $\exists p \exists q[\beta(p, q, \emptyset) = g(\vec{x}) \wedge (\forall i < \emptyset) h(\vec{x}, i, \beta(p, q, i)) = \beta(p, q, Si) \wedge \beta(p, q, \emptyset) = f(\vec{x}, \emptyset)]$. For (b),

1.	$\exists p \exists q[\beta(p,q,\emptyset) = g(\vec{x}) \wedge (\forall i < Sy) h(\vec{x}, i, \beta(p,q,i)) = \beta(p,q,Si) \wedge \beta(p,q,Sy) = f(\vec{x}, Sy)]$	def
2.	$\beta(a,b,\emptyset) = g(\vec{x}) \wedge (\forall i < Sy) h(\vec{x}, i, \beta(a,b,i)) = \beta(a,b,Si) \wedge \beta(a,b,Sy) = f(\vec{x}, Sy)$	A (g 1∃E)
3.	$(\forall i < Sy) h(\vec{x}, i, \beta(a,b,i)) = \beta(a,b,Si)$	2 ∧E
4.	$y < Sy$	T13.13h
5.	$h(\vec{x}, y, \beta(a,b,y)) = \beta(a,b,Sy)$	3,4 (∀E)
6.	$\beta(a,b,Sy) = f(\vec{x}, Sy)$	2 ∧E
7.	$f(\vec{x}, Sy) = h(\vec{x}, y, \beta(a,b,y))$	5,6 =E
8.	$\beta(a,b,\emptyset) = g(\vec{x})$	2 ∧E
9.	$j < y$	A (g (∀I))
10.	$j < Sy$	9 and T13.13h
11.	$h(\vec{x}, j, \beta(a,b,j)) = \beta(a,b,Sj)$	3,10 (∀E)
12.	$(\forall i < y) h(\vec{x}, i, \beta(a,b,i)) = \beta(a,b,Si)$	9-11 (∀I)
13.	$\beta(a,b,y) = \beta(a,b,y)$	=I
14.	$\beta(a,b,\emptyset) = g(\vec{x}) \wedge (\forall i < y) h(\vec{x}, i, \beta(a,b,i)) = \beta(a,b,Si) \wedge \beta(a,b,y) = \beta(a,b,y)$	8,12,13 ∧I
15.	$\exists p \exists q[\beta(p,q,\emptyset) = g(\vec{x}) \wedge (\forall i < y) h(\vec{x}, i, \beta(p,q,i)) = \beta(p,q,Si) \wedge \beta(p,q,y) = \beta(a,b,y)]$	14 ∃I
16.	$f(\vec{x}, y) = \beta(a,b,y)$	15 def
17.	$f(\vec{x}, Sy) = h(\vec{x}, y, f(\vec{x}, y))$	7,16 =E
18.	$f(\vec{x}, S(y)) = h(\vec{x}, y, f(\vec{x}, y))$	1,2-17 ∃E

The key stages of this argument are at (7) which has the result with $\beta(a, b, y)$ where we want $f(\vec{x}, y)$ and then (16) which shows they are one and the same.

From this theorem, our defined functions behave like ones we have seen before, with clauses for the basis and then for successor. This lets us manipulate the functions very much as before. The importance of this point will emerge shortly, in application to recursive cases.

With this theorem we are in a position to show that definitions of functions and relations from chapter 12 are "coordinate" with definitions in PA.

CF The definition of a recursive function is *coordinate* with its definition in PA iff,

(i) $\mathsf{f}(\vec{\mathsf{x}})$ is an initial function $\mathsf{init}(\vec{\mathsf{x}})$ and $f(\vec{x})$ is $init(\vec{x})$

(c) $\mathsf{f}(\vec{\mathsf{x}}, \vec{\mathsf{y}}, \vec{\mathsf{z}})$ is defined from $\mathsf{g}(\vec{\mathsf{y}})$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{w}, \vec{\mathsf{z}})$ by composition so that $\mathsf{f}(\vec{\mathsf{x}}, \vec{\mathsf{y}}, \vec{\mathsf{z}}) = \mathsf{h}(\vec{\mathsf{x}}, \mathsf{g}(\vec{\mathsf{y}}), \vec{\mathsf{z}})$, and for coordinate $g(\vec{x})$ and $h(\vec{x}, w, \vec{z})$, PA $\vdash f(\vec{x}, \vec{y}, \vec{z}) \leftrightarrow h(\vec{x}, g(\vec{y}), \vec{z})$.

(r) $\mathsf{f}(\vec{\mathsf{x}}, \mathsf{y})$ is defined from $\mathsf{g}(\vec{\mathsf{x}})$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$ by recursion so that $\mathsf{f}(\vec{\mathsf{x}}, 0) = \mathsf{g}(\vec{\mathsf{x}})$ and $\mathsf{f}(\vec{\mathsf{x}}, \mathsf{Sy}) = \mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{f}(\vec{\mathsf{x}}, \mathsf{y}))$ and for coordinate $g(\vec{x})$ and $h(\vec{x}, y, u)$, PA $\vdash f(\vec{x}, \emptyset) = g(\vec{x})$ and PA $\vdash f(\vec{x}, Sy) = h(\vec{x}, y, f(\vec{x}, y))$.

(m) $\mathsf{f}(\vec{\mathsf{x}}, \mathsf{y})$ is defined from $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$ by friendly regular minimization so that $\mathsf{f}(\vec{\mathsf{x}}) = \mu\mathsf{y}[\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})]$ and for coordinate $g(\vec{x}, y)$, PA $\vdash f(\vec{x}) = \mu y[g(\vec{x}, y)]$.

CR The definition of a recursive relation is *coordinate* with its definition in PA iff,

(a) $\mathsf{R}(\vec{\mathsf{x}})$ is an atomic $\mathsf{ATOM}(\vec{\mathsf{x}})$ and $\mathbb{R}(\vec{x})$ is $Atom(\vec{x})$.

(o) $\mathsf{R}(\vec{\mathsf{x}})$ is defined from an operator OP and relations $\mathsf{P}_1(\vec{\mathsf{x}}) \ldots \mathsf{P}_n(\vec{\mathsf{x}})$ so that $\mathsf{R}(\vec{\mathsf{x}})$ is $\mathsf{OP}(\mathsf{P}_1(\vec{\mathsf{x}}) \ldots \mathsf{P}_n(\vec{\mathsf{x}}))$ and for coordinate $\mathbb{P}_1(\vec{x}) \ldots \mathbb{P}_n(\vec{x})$, PA $\vdash \mathbb{R}(\vec{x}) \leftrightarrow Op(\mathbb{P}_1(\vec{x}) \ldots \mathbb{P}_n(\vec{x}))$.

T13.34. (a) For any friendly recursive function $\mathsf{r}(\vec{\mathsf{x}})$ and original formula $\mathcal{R}(\vec{x}, v)$ by which it is expressed and captured, PA defines a coordinate function $r(\vec{x})$ such that PA $\vdash v = r(\vec{x}) \leftrightarrow \mathcal{R}(\vec{x}, v)$. And (b) for any friendly recursive relation $\mathsf{R}(\vec{\mathsf{x}})$ with characteristic function $\mathsf{ch_R}(\vec{\mathsf{x}})$, PA defines a coordinate relation $\mathbb{R}(\vec{x})$ such that PA $\vdash \mathbb{R}(\vec{x}) \leftrightarrow ch_{\mathsf{R}}(\vec{x}) = \emptyset$.

The argument is by simple review of arguments for T13.21 and T13.32 together with T13.33.

From this theorem we simply "write down" claims for defined functions and releations directly from the recursive definitions. So, for example from the definition for $\mathsf{plus}(\mathsf{x}, \mathsf{y})$ on p. 554, PA $\vdash plus(x, \emptyset) = idnt^1_1(x)$ and PA $\vdash plus(x, Sy) = suc(idnt^3_3(x, y, plus(x, y)))$. Again, the defined symbol $plus$ is not the same as the primitive symbol $+$. But now we are in a position to show that the functions are equivalent.

T13.35. The following result in PA.

(a) PA $\vdash suc(x) = Sx$

1.	$v = suc(x) \leftrightarrow Sx = v$	def suc
2.	$suc(x) = suc(x) \leftrightarrow Sx = suc(x)$	1 ∀E
3.	$suc(x) = suc(x)$	=I
4.	$suc(x) = Sx$	2,3 =E

(b) PA $\vdash$ $\mathbb{zero}(x) = \emptyset$

(c) PA $\vdash$ $\mathbb{idnt}^j_k(x_1 \dots x_j) = x_k$

(d) PA $\vdash$ $\mathbb{plus}(x, y) = x + y$

(e) PA $\vdash$ $\mathbb{times}(x, y) = x \times y$

The first line of (a) is from T13.21. Arguments for (a) - (c) are very much the same and nearly trivial. Arguments for (d) and (e) are by IN. Here is the case for (d) as an example.

1.	$\mathbb{gplus}(x) = \mathbb{idnt}^1_1(x)$	def from plus, T13.34
2.	$\mathbb{gplus}(x) = x$	1 with T13.35c
3.	$\mathbb{plus}(x, \emptyset) = \mathbb{gplus}(x)$	T13.34
4.	$\mathbb{plus}(x, \emptyset) = x$	3,2 =E
5.	$x + \emptyset = x$	T6.41
6.	$\mathbb{plus}(x, \emptyset) = x + \emptyset$	4,5 =E
7.	$\quad \mathbb{plus}(x, j) = x + j$	A (g →I)
8.	$\quad \mathbb{plus}(x, Sj) = \mathbb{hplus}(x, j, \mathbb{plus}(x, j))$	T13.34
9.	$\quad \mathbb{hplus}(x, j, u) = \mathbb{suc}(\mathbb{idnt}^3_3(x, j, u))$	def from plus, T13.34
10.	$\quad \mathbb{hplus}(x, j, u) = Su$	9 with T13.35a,c
11.	$\quad \mathbb{hplus}(x, j, \mathbb{plus}(x, j)) = S\,\mathbb{plus}(x, j)$	10 ∀E
12.	$\quad \mathbb{plus}(x, Sj) = S\,\mathbb{plus}(x, j)$	8,11 =E
13.	$\quad \mathbb{plus}(x, Sj) = S(x + j)$	12,7 =E
14.	$\quad S(x + j) = x + Sj$	T6.42
15.	$\quad \mathbb{plus}(x, Sj) = x + Sj$	13,14 =E
16.	$[\mathbb{plus}(x, j) = x + j] \rightarrow [\mathbb{plus}(x, Sj) = x + Sj]$	7-15 →I
17.	$\forall y([\mathbb{plus}(x, y) = x + y] \rightarrow [\mathbb{plus}(x, Sy) = x + Sy])$	16 ∀I
18.	$\mathbb{plus}(x, y) = x + y$	6,17 IN

Again, we simply write down the expressions on (1) and (9) with T13.34; and on (3) and (8) T13.34 makes the conditions for $\mathbb{plus}(x, y)$ work like the ones for $x + y$ — so that with zero and inductive cases, the equivalence results by IN.

So this theorem establishes the equivalences we expect for the defined symbols $\mathbb{suc}$, $\mathbb{zero}$, $\mathbb{idnt}$, $\mathbb{plus}$ and $\mathbb{times}$. Again, $+$, $\times$ and the like are primitive symbols of $\mathscr{L}_{NT}$ where $\mathbb{plus}$ and $\mathbb{times}$ are defined according to our induction from the corresponding recursive functions. Having shown that the functions are equivalent, however, we may manipulate the one with all the results we have achieved for the other.

Some additional results will be facilitated by a couple of auxiliary definitions. $pred(y)$, $sg(y)$ and $csg(y)$ are defined directly, without appeal to recursive functions — but still behave as we expect.

Def[*pred*] PA $\vdash pred(y) = y \dot{-} \overline{1}$

Since this is a composition of functions, immediate by T13.17.

Def[*sg*] PA $\vdash v = sg(y) \leftrightarrow (y = \emptyset \wedge v = \emptyset) \vee (y > \emptyset \wedge v = S\emptyset)$

(i) PA $\vdash \exists v[(y = \emptyset \wedge v = \emptyset) \vee (y > \emptyset \wedge v = \overline{1})]$

(ii) PA $\vdash \forall u \forall v\{[((y = \emptyset \wedge u = \emptyset) \vee (y > \emptyset \wedge u = \overline{1})) \wedge ((y = \emptyset \wedge v = \emptyset) \vee (y > \emptyset \wedge v = \overline{1}))] \rightarrow u = v\}$

Def[*csg*] PA $\vdash v = csg(y) \leftrightarrow (y = \emptyset \wedge v = \overline{1}) \vee (y > \emptyset \wedge v = \emptyset)$

(i) PA $\vdash \exists v[(y = \emptyset \wedge v = \overline{1}) \vee (y > \emptyset \wedge v = \emptyset)]$

(ii) PA $\vdash \forall u \forall v\{[((y = \emptyset \wedge u = \overline{1}) \vee (y > \emptyset \wedge u = \emptyset)) \wedge ((y = \emptyset \wedge v = \overline{1}) \vee (y > \emptyset \wedge v = \emptyset))] \rightarrow u = v\}$

And some basic results on these notions,

T13.36. The following result in PA.

(a) PA $\vdash pred(\emptyset) = \emptyset$

(b) PA $\vdash pred(\overline{1}) = \emptyset$

(c) PA $\vdash y > \emptyset \rightarrow Spred(y) = y$

(d) PA $\vdash pred(Sy) = y$

(e) PA $\vdash y = \emptyset \leftrightarrow sg(y) = \emptyset$

(f) PA $\vdash y > \emptyset \leftrightarrow sg(y) = \overline{1}$

(g) PA $\vdash y = \emptyset \leftrightarrow csg(y) = \overline{1}$

(h) PA $\vdash y > \emptyset \leftrightarrow csg(y) = \emptyset$

(a) - (d) recover from the definition some basic results for *pred*. (e) and (f) extract basic information for the behavior of *sg*; and then (g) and (h) for *csg*.

And given these notions in PA, we can build on them for another set of equivalents.

*T13.37. The following result in PA.

(a) PA $\vdash \mathbb{pred}(y) = pred(y)$

*(b) PA $\vdash \mathbb{subc}(x, y) = x \dot{-} y$

(c) PA $\vdash \mathbb{absval}(x \text{ - } y) = (x \dot{-} y) + (y \dot{-} x)$

(d) PA $\vdash \mathbb{sg}(y) = sg(y)$

(e) PA $\vdash \mathbb{csg}(y) = csg(y)$

*(f) PA $\vdash \mathbb{Eq}(x, y) \leftrightarrow x = y$

(g) PA $\vdash \mathbb{Leq}(x, y) \leftrightarrow x \leq y$

(h) PA $\vdash \mathbb{Less}(x, y) \leftrightarrow x < y$

*(i) PA $\vdash \mathbb{Neg}(\mathbb{P}(\vec{x})) \leftrightarrow \sim\mathbb{P}(\vec{x})$

(j) PA $\vdash \mathbb{Dsj}(\mathbb{P}(\vec{x}), \mathbb{Q}(\vec{y})) \leftrightarrow \mathbb{P}(\vec{x}) \vee \mathbb{Q}(\vec{y})$

Hints. (b): This works in the usual way up to the point in the show stage where you get $\mathbb{subc}(x, Sj) = pred(x \dot{-} j)$; then it will take some work to show $x \dot{-} Sj = pred(x \dot{-} j)$; for this begin with $x \leq j \vee x > j$ by T13.13q; the first case is straightforward; for the second, you will be able to show $S(x \dot{-} Sj) = Spred(x \dot{-} j)$ and apply T6.40. (f): For this relation, you have $\mathbb{Eq}(x, y) \leftrightarrow \mathbb{sg}(\mathbb{absval}(x \text{ - } y)) = \emptyset$ from the def EQ and T13.34; this gives $\mathbb{Eq}(x, y) \leftrightarrow [(x \dot{-} y) + (y \dot{-} x)] = \emptyset$; now for $\leftrightarrow$I, the case from $x = y$ is easy; from $\mathbb{Eq}(x, y)$, you have $x \geq y \vee x < y$ from T13.13q; the cases are not hard and similar (since $x < y$ gives $y \geq x$). (i): This is straightforward with $\mathbb{P}(\vec{x}) \leftrightarrow \mathbb{ch}_{\mathsf{P}}(\vec{x}) = \emptyset$ and $\mathbb{Neg}(\mathbb{P}(\vec{x})) \leftrightarrow \mathbb{csg}(\mathbb{ch}_{\mathsf{P}}(\vec{x})) = \emptyset$ from NEG with T13.34.

So this theorem delivers the equivalences we expect for $\mathbb{pred}$, $\mathbb{subc}$, $\mathbb{absval}$, $\mathbb{sg}$, $\mathbb{csg}$, $\mathbb{Eq}$, $\mathbb{Leq}$, $\mathbb{Less}$, $\mathbb{Neg}$, and $\mathbb{Dsj}$. Given this, we will typically move without comment from some PA $\vdash \mathbb{Dsj}(\mathbb{A}, \mathbb{B})$ given from T13.34 to PA $\vdash \mathbb{A} \vee \mathbb{B}$. And similarly in other cases.

We pause to remark on a on a simple consequence for characteristic functions. Recall from (CF) that a characteristic function is (officially) of the sort $\mathsf{sg}(\mathsf{p}(\vec{\mathsf{x}}))$ so that, T13.38. For any recursive characteristic function $\mathsf{ch}_{\mathsf{R}}(\vec{\mathsf{x}})$, PA $\vdash \mathbb{ch}_{\mathsf{R}}(\vec{x}) = \emptyset \vee \mathbb{ch}_{\mathsf{R}}(\vec{x}) = \overline{1}$.

From (CF), $\mathsf{ch}_{\mathsf{R}}(\vec{\mathsf{x}})$ is of the sort $\mathsf{sg}(\mathsf{p}(\vec{\mathsf{x}}))$; so with T13.34, PA $\vdash \mathbb{ch}_{\mathsf{R}}(\vec{x}) = \mathbb{sg}(\mathbb{p}(\vec{x}))$. The result is nearly immediate with PA $\vdash \mathbb{p}(\vec{x}) = \emptyset \vee \mathbb{p}(\vec{x}) > \emptyset$ and results for $\mathbb{sg}$.

It is worth observing that this theorem, which depends on results for functions through T13.37d, is independent of any applications of T13.32 or T13.34b for relations. There is therefore no problem about appeal to T13.38 in the demonstration of T13.32.

Now reasoning for the bounded quantifiers, bounded minimization and a couple relations built on them.

*T13.39. The following result in PA.

*(a) PA $\vdash (\exists y \leq z)\mathbb{P}(\vec{x}, z, y) \leftrightarrow (\exists y \leq z)\mathcal{P}(\vec{x}, z, y)$

(b) PA $\vdash (\exists y < z)\mathbb{P}(\vec{x}, z, y) \leftrightarrow (\exists y < z)\mathcal{P}(\vec{x}, z, y)$

(c) PA $\vdash (\forall y \leq z)\mathbb{P}(\vec{x}, z, y) \leftrightarrow (\forall y \leq z)\mathcal{P}(\vec{x}, z, y)$

(d) PA $\vdash (\forall y < z)\mathbb{P}(\vec{x}, z, y) \leftrightarrow (\forall y < z)\mathcal{P}(\vec{x}, z, y)$

*(e) PA $\vdash (\mathbb{\mu} y \leq z)\mathbb{P}(\vec{x}, z, y) \leftrightarrow (\mu y \leq z)\mathcal{P}(\vec{x}, z, y)$

(f) PA $\vdash \mathbb{Fctr}(m, n) \leftrightarrow m|n$

*(g) PA $\vdash \mathbb{Prime}(n) \leftrightarrow Pr(n)$

Hints. (a): Recall from chapter 12 that $\mathsf{s}(\vec{\mathsf{x}}, \mathsf{z}) = (\exists \mathsf{y} \leq \mathsf{z})\mathsf{P}(\vec{\mathsf{x}}, \mathsf{z}, \mathsf{y})$ is defined by means of a $\mathsf{R}(\vec{\mathsf{x}}, \mathsf{z}, \mathsf{n})$ corresponding to $(\exists \mathsf{y} \leq \mathsf{n})\mathsf{P}(\vec{\mathsf{x}}, \mathsf{z}, \mathsf{y})$; the main argument is to show by IN that PA $\vdash \mathbb{ch}_{\mathsf{R}}(\vec{x}, z, n) = \emptyset \leftrightarrow (\exists y \leq n)\mathbb{P}(\vec{x}, z, y)$. You have $\mathbb{P}(\vec{x}, z, y) \leftrightarrow \mathbb{ch}_{\mathsf{P}}(\vec{x}, z, y) = \emptyset$ from T13.32. For the zero case, you have $\mathbb{ch}_{\mathsf{R}}(\vec{x}, z, \emptyset) = \mathbb{gch}_{\mathsf{R}}(\vec{x}, z)$, and $\mathbb{gch}_{\mathsf{R}}(\vec{x}, z) = \mathbb{ch}_{\mathsf{P}}(\vec{x}, z, \emptyset)$ from the definitions with T13.34; for the main reasoning, you have $\mathbb{ch}_{\mathsf{R}}(\vec{x}, z, Sj) = \mathbb{hch}_{\mathsf{R}}(\vec{x}, z, j, \mathbb{ch}_{\mathsf{R}}(x, z, j))$, and $\mathbb{hch}_{\mathsf{R}}(\vec{x}, z, j, u) = \mathbb{times}[u, \mathbb{ch}_{\mathsf{P}}(\vec{x}, z, \mathbb{suc}(j))]$ from the definitions with T13.34; once you have finished the induction, it is a simple matter of applying $\mathbb{ch}_{\mathsf{S}}(\vec{x}, z) = \mathbb{ch}_{\mathsf{R}}(\vec{x}, z, z)$ from the definition, and where where $\mathbb{S}(\vec{x}, z)$ just abbreviates $(\exists y \leq z)\mathbb{P}(\vec{x}, z, y)$, applying $\mathbb{S}(\vec{x}, z) \leftrightarrow \mathbb{ch}_{\mathsf{S}}(\vec{x}, z) = \emptyset$ to get $(\exists y \leq z)\mathbb{P}(\vec{x}, z, y) \leftrightarrow (\exists y \leq z)\mathbb{P}(\vec{x}, z, y)$. (f) and (g): Given previous results, the left and right sides have nearly matching definitions except that the recursive side includes a bounded quantifier —

so that you have to work to show the bound obtains for one direction of the biconditional.

The argument for T13.39e is particularly involved. Recall from chapter 12 that $\mathsf{m}(\vec{\mathsf{x}}, \mathsf{z}) = (\mu \mathsf{y} \le \mathsf{z})\mathsf{P}(\vec{\mathsf{x}}, \mathsf{z}, \mathsf{y})$ is defined by means of $\mathsf{R}(\vec{\mathsf{x}}, \mathsf{z}, \mathsf{n})$ corresponding to $(\exists \mathsf{y} \le \mathsf{n})\mathsf{P}(\vec{\mathsf{x}}, \mathsf{z}, \mathsf{y})$ and $\mathsf{q}(\vec{\mathsf{x}}, \mathsf{z}, \mathsf{n})$ corresponding to $(\mu \mathsf{y} \le \mathsf{n})\mathsf{P}(\vec{\mathsf{x}}, \mathsf{z}, \mathsf{y})$. The main reasoning is by IN to show $\mathbb{q}(\vec{x}, z, n) = (\mu y \le n)\mathbb{P}(\vec{x}, z, y)$; here are the main outlines of that part.

1.	$\mathbb{q}(\vec{x}, z, \emptyset) = (\mu y \le \emptyset)\mathbb{P}(\vec{x}, z, y)$	[a]
2.	$\mathbb{ch}_{\mathsf{R}}(\vec{x}, z, j) = \emptyset \lor \mathbb{ch}_{\mathsf{R}}(\vec{x}, z, j) = \overline{1}$	T13.38
3.	$\mathbb{ch}_{\mathsf{R}}(\vec{x}, z, j) = \emptyset \leftrightarrow (\exists y \le j)\mathbb{P}(x, z, y)$	from T13.39a
4.	$\mathbb{q}(\vec{x}, z, Sj) = \mathbb{hq}(\vec{x}, z, j, \mathbb{q}(\vec{x}, z, j))$	T13.33b
5.	$\mathbb{hq}(\vec{x}, z, j, u) = \mathbb{plus}(u, \mathbb{ch}_{\mathsf{R}}(\vec{x}, z, j))$	def from least, T13.34
6.	$\mathbb{hq}(\vec{x}, z, j, u) = u + \mathbb{ch}_{\mathsf{R}}(\vec{x}, z, j)$	5 T13.35d
7.	$\mathbb{hq}(\vec{x}, z, j, \mathbb{q}(\vec{x}, z, j)) = \mathbb{q}(\vec{x}, z, j) + \mathbb{ch}_{\mathsf{R}}(\vec{x}, z, j)$	6 $\forall$E
8.	$\mathbb{q}(\vec{x}, z, Sj) = \mathbb{q}(\vec{x}, z, j) + \mathbb{ch}_{\mathsf{R}}(\vec{x}, z, j)$	4,7 =E
9.	$\mathbb{q}(\vec{x}, z, j) = (\mu y \le j)\mathbb{P}(\vec{x}, z, y)$	A (g $\to$I)
10.	$a = \mathbb{q}(\vec{x}, z, j)$	abv
11.	$b = \mathbb{q}(\vec{x}, z, Sj)$	abv
12.	$b = a + \mathbb{ch}_{\mathsf{R}}(\vec{x}, z, j)$	8,10,11 =E
13.	$a = (\mu y \le j)\mathbb{P}(\vec{x}, z, y)$	9,10 =E
14.	$a = \mu y[y = j \lor \mathbb{P}(\vec{x}, z, y)]$	13 def
15.	$(\forall w < a)[w \ne j \land \sim\mathbb{P}(\vec{x}, z, w)]$	14 T13.19c
16.	$a = j \lor \mathbb{P}(\vec{x}, z, a)$	14 T13.19b
17.	$a = j$	A (g 16$\lor$E)
18.	$\sim\mathbb{P}(\vec{x}, z, j) \lor \mathbb{P}(\vec{x}, z, j)$	T3.1
19.	$\sim\mathbb{P}(\vec{x}, z, j)$	A (g 18$\lor$E)
20.	$[b = Sj \lor \mathbb{P}(\vec{x}, z, b)] \land (\forall w < b)(w \ne Sj \land \sim\mathbb{P}(\vec{x}, z, w))$	[b]
21.	$\mathbb{P}(\vec{x}, z, j)$	A (g18$\lor$E)
22.	$[b = Sj \lor \mathbb{P}(\vec{x}, z, b)] \land (\forall w < b)(w \ne Sj \land \sim\mathbb{P}(\vec{x}, z, w))$	[c]
23.	$[b = Sj \lor \mathbb{P}(\vec{x}, z, b)] \land (\forall w < b)(w \ne Sj \land \sim\mathbb{P}(\vec{x}, z, w))$	18,19-20,21-22 $\lor$E
24.	$\mathbb{P}(\vec{x}, z, a)$	A (g 16$\lor$E)
25.	$[b = Sj \lor \mathbb{P}(\vec{x}, z, b)] \land (\forall w < b)(w \ne Sj \land \sim\mathbb{P}(\vec{x}, z, w))$	[d]
26.	$[b = Sj \lor \mathbb{P}(\vec{x}, z, b)] \land (\forall w < b)(w \ne Sj \land \sim\mathbb{P}(\vec{x}, z, w))$	16,17-23,24-25 $\lor$E
27.	$b = \mu y[y = Sj \lor \mathbb{P}(\vec{x}, z, j)]$	26 def μ
28.	$b = (\mu y \le Sj)\mathbb{P}(\vec{x}, z, y)$	27 def
29.	$\mathbb{q}(\vec{x}, z, Sj) = (\mu y \le Sj)\mathbb{P}(\vec{x}, z, y)$	28 abv
30.	$[\mathbb{q}(\vec{x}, z, j) = (\mu y \le j)\mathbb{P}(\vec{x}, z, y)] \to [\mathbb{q}(\vec{x}, z, Sj) = (\mu y \le Sj)\mathbb{P}(\vec{x}, z, y)]$	9-29 $\to$I
31.	$\forall n([\mathbb{q}(\vec{x}, z, n) = (\mu y \le n)\mathbb{P}(\vec{x}, z, y)] \to [\mathbb{q}(\vec{x}, z, Sn) = (\mu y \le Sn)\mathbb{P}(\vec{x}, z, y)])$	30 $\forall$I
32.	$\mathbb{q}(\vec{x}, z, n) = (\mu y \le n)\mathbb{P}(\vec{x}, z, y)$	1,31 IN

Hints: The zero case (a) is straightforward with T13.20a; for (b) you will be able to show that $b = Sj$; for (c) and (d) you will be able to show $b = a$. And the final result is nearly automatic from this.

T13.39 delivers the equivalences we expect for the bounded quantifiers, bounded minimization, factor and prime.

At this stage, we have defined in PA functions, relations and operators corresponding to all the recursive functions, relations and operators. And in simple cases we have established equivalences to functions, relations and operators already defined. Thus supposing T is a theory including PA, we are in a position simply to write down the following.

T13.40. The following are theorems of PA:

(a) PA $\vdash \mathbb{A}xiomad1(n) \leftrightarrow (\exists p \leq n)(\exists q \leq n)[\mathbb{W}ff(p) \wedge \mathbb{W}ff(q) \wedge n = \mathbb{c}nd(p, \mathbb{c}nd(q, p))]$

and similarly for the other axioms

(b) PA $\vdash \mathbb{A}xiompa(n) \leftrightarrow \mathbb{A}xiomad1(n) \vee \ldots \vee \mathbb{A}xiomq1(n) \vee \ldots \vee \mathbb{A}xiompa7(n)$

(c) PA $\vdash \mathbb{M}p(m, n, o) \leftrightarrow \mathbb{c}nd(n, o) = m$

(d) PA $\vdash \mathbb{G}en(m, n) \leftrightarrow (\exists v \leq n)[\mathbb{V}ar(v) \wedge n = \mathbb{u}nv(v, m)]$

(e) PA $\vdash \mathbb{I}con(m, n, o) \leftrightarrow \mathbb{M}p(m, n, o) \vee (m = n \wedge \mathbb{G}en(n, o))$

(f) PA $\vdash \mathbb{P}rft(m, n) \leftrightarrow \mathbb{e}xp(m, \mathbb{l}en(m) \dot{-} \overline{1}) = n \wedge m > \overline{1} \wedge (\forall k < \mathbb{l}en(m))[\mathbb{A}xiomt(\mathbb{e}xp(m, k)) \vee (\exists i < k)(\exists j < k)\mathbb{I}con(\mathbb{e}xp(m, i), \mathbb{e}xp(m, j), \mathbb{e}xp(m, k))]$

These follow directly from our results with recursive definitions. So for example, the definition MP, with T13.34 gives us, say, PA $\vdash \mathbb{M}p(m, n, o) \leftrightarrow \mathbb{E}q(\mathbb{c}nd(n, o), m)$; then with T13.37f, we arrive at (c). And similarly in other cases.

Where $\mathbb{M}p$, $\mathbb{c}nd$ and the like are defined relative to corresponding recursive functions, it is important that the *operators* in expressions above are the ordinary operators of $\mathcal{L}_{NT}$. Thus we shall be able to manipulate the expressions in the usual ways. We shall find these results useful for the following!

E13.24. Produce derivations to show T13.33a and T13.35e. Hard core: show the remaining cases from T13.35.

E13.25. Show (i) of the condition for *Def*[*pred*] and then T13.36c. Hard core: Show each of the conditions for *Def*[*pred*], *Def*[*sg*] and *Def*[*csg*] and all of the results in T13.36.

*E13.26. Show a, g and j from T13.37. Hard core: Demonstrate each of the results in T13.37.

*E13.27. Show T13.39a. Hard core: show T13.38 along with each of the results in T13.39.

Further results. T13.40 gives us functions in PA corresponding to all the ones from chapter 12. Now we require the ability to manipulate them. Thus we begin with some results for exponentiation, factorial and the like, and continue through to complex notions including $\mathbb{W}\mathit{ff}$ and $\mathit{formsub}$. At this stage, we are acquiring results, not by demonstrating equivalence to expressions already defined (since there are no such expressions already defined), but by showing them directly for symbols defined for the recursive functions.

*T13.41. The following are theorems of PA.

(a) (i) PA $\vdash m^{\emptyset} = \overline{1}$

(ii) PA $\vdash m^{Sn} = m^n \times m$

(b) PA $\vdash m^{\overline{1}} = m$

(c) PA $\vdash \overline{2}^{\overline{2}} = \overline{4}$

(d) PA $\vdash a > \emptyset \to \emptyset^a = \emptyset$

(e) PA $\vdash m^a \times m^b = m^{a+b}$

(f) PA $\vdash m \geq n \to m^a \geq n^a$

(g) PA $\vdash pred(m^b) | m^{a+b}$

(h) PA $\vdash (a > \emptyset \wedge m > \overline{1}) \to pred(m^{a+b}) \nmid m^b$

(i) PA $\vdash m > \emptyset \to m^a > \emptyset$

(j) PA $\vdash (m > \emptyset \wedge a \geq b) \to m^a \geq m^b$

(k) PA $\vdash (m > \overline{1} \wedge a > b) \to m^a > m^b$

(l) PA $\vdash a > \emptyset \to m^a \geq m$

*(m) PA $\vdash m > \overline{1} \to a < m^a$

(n) PA $\vdash m > \overline{1} \rightarrow (m^a = m^b \rightarrow a = b)$

Hints: (a) is from the the definition of power and prior results. For (c) take a look at E6.35e. (e) uses IN on the value of b and (f) uses IN on a. (g) is straightforward with cases for $m^b = \emptyset$ and $m^b > \emptyset$. (i), (j), (k) and (m) are by IN. For (n), $a < b \vee a = b \vee b < a$; but the first and last are impossible.

(a) gives the recursive conditions from which the rest follow. Then (b) - (n) are basic results that should be accessible from ordinary arithmetic.

*T13.42. The following are theorems of PA.

(a) (i) PA $\vdash \mathit{fact}(\emptyset) = \overline{1}$

(ii) PA $\vdash \mathit{fact}(Sn) = \mathit{fact}(n) \times Sn$

(b) PA $\vdash \mathit{fact}(\overline{1}) = \overline{1}$

(c) PA $\vdash \mathit{fact}(n) > \emptyset$

(d) PA $\vdash (\forall y < n) y | \mathit{fact}(n)$

*(e) $(\exists y \leq \mathit{fact}(n) + \overline{1})[n < y \wedge Pr(y)]$

Hints: (a) is from the definition of fact and prior results. (c) and (d) are straightforward by IN. Reasoning for (e) is like (G2) in the arithmetic for Gödel numbering reference once you realize that all the primes less than n are included in $\mathit{fact}(n)$.

These are some basic results for factorial. Again (a) gives the recursive conditions from which the rest follow. (b) is a simple particular fact; and the result from (c) is obvious. (d) is a consequence of the way the factorial includes successors of all the numbers less than it. We will be able to take advantage of (e) immediately below.

*T13.43. The following are theorems of PA.

(a) (i) PA $\vdash \mathit{pi}(\emptyset) = \overline{2}$

(ii) PA $\vdash \mathit{pi}(Sn) = (\mu y \leq \mathit{fact}(\mathit{pi}(n)) + \overline{1})[\mathit{pi}(n) < y \wedge Pr(y)]$

(b) $(\exists y \leq \mathit{fact}(\mathit{pi}(n)) + \overline{1})[\mathit{pi}(n) < y \wedge Pr(y)]$

(c) PA $\vdash \mathit{pi}(Sn) = \mu y[\mathit{pi}(n) < y \wedge Pr(y)]$

(d) PA $\vdash \mathit{pi}(n) < \mathit{pi}(Sn) \wedge Pr(\mathit{pi}(Sn))$

(e) PA $\vdash (\forall w < \mathbb{pi}(Sn))\sim[\mathbb{pi}(n) < w \wedge Pr(w)]$

(f) PA $\vdash Pr(\mathbb{pi}(n))$

(g) PA $\vdash \mathbb{pi}(n) > \overline{1}$

(h) PA $\vdash \mathbb{pi}(n)^a > \emptyset$

(i) PA $\vdash a > \emptyset \rightarrow \mathbb{pi}(n)^a > \overline{1}$

(j) PA $\vdash Spred(\mathbb{pi}(n)^a) = \mathbb{pi}(n)^a$

(k) PA $\vdash (\forall m < n)\mathbb{pi}(m) < \mathbb{pi}(n)$

(l) PA $\vdash (\forall m \leq n)Sm < \mathbb{pi}(n)$

*(m) PA $\vdash \forall y[Pr(y) \rightarrow \exists j\, \mathbb{pi}(j) = y]$

*(n) PA $\vdash m \neq n \rightarrow pred(\mathbb{pi}(m)) \nmid \mathbb{pi}(n)^a$

(o) PA $\vdash m \neq n \rightarrow pred(\mathbb{pi}(m)^{Sb}) \nmid \mathbb{pi}(n)^a$

*(p) PA $\vdash [m \neq n \wedge pred(\mathbb{pi}(m)^b)|(s \times \mathbb{pi}(n)^a)] \rightarrow pred(\mathbb{pi}(m)^b)|s$

Hints: (a) is from definition pi and prior results. (b) is from T13.42e; (c) applies T13.20.b; and then (d) and (e) are by T13.19(b) and (c). (f), (k) and (l) are simple inductions. (m) is by using IN on i to show $(\forall y \leq \mathbb{pi}(i))[Pr(y) \rightarrow \exists j\, \mathbb{pi}(j) = y]$; the result then follows easily with (l). Under the assumption for →I, (n) is by IN on a. For (o) you will be able to show that if $pred(\mathbb{pi}(m)^{Sb})|\mathbb{pi}(n)^a$ then $pred(\mathbb{pi}(m))|\mathbb{pi}(n)^a$ and use (n). For (p) under the assumption for →I you will be able to show $i \leq b \rightarrow pred(\mathbb{pi}(m)^i)|s$ by induction on i; the result then follows easily with $b \leq b$.

These are some basic results from prime sequences. (a) gives the basic recursive conditions. (b) is an existential result; then (c) extracts the successor condition from bounded to unbounded minimization; this allows application of the definition in (d) and (e). (f) - (j) are some simple consequences of the fact that $\mathbb{pi}(n)$ is prime. Then the primes are ordered (k). And (l) each prime is greater than the successor of its index. (m) every prime appears as some $\mathbb{pi}(j)$. And (n) - (p) echo results for factor except combined with primes and exponentiation.

(b) and then (c) - (e) are a first instance of a pattern we shall see repeatedly: Given a bounded condition $\mathbb{a} = (\mu x \leq t)\mathcal{P}(x)$ of the sort that arises from a recursive definition, we show there exists some $\mathcal{P}(x)$ less than or equal to the bound; this allows application of T13.20.b to "extract" the bounded to an unbounded minimization, and then T13.19 to obtain $\mathcal{P}(a)$; this forms the basis for further results.

In order to manipulate *exp*, it will be convenient to introduce a function *ex*, that finds the least exponent x such that $pi(i)^x$ does *not* divide Sn.

Def[*ex*] $ex(n,i) = \mu x[pred(pi(i)^x) \nmid Sn]$

(i) PA ⊢ $\exists x[pred(pi(i)^x) \nmid Sn]$

1.	$pi(i) > \bar{1}$	T13.43g
2.	$Sn < pi(i)^{Sn}$	1 T13.41m
3.	$Spred(pi(i)^{Sn}) = pi(i)^{Sn}$	T13.43j
4.	$Sn < Spred(pi(i)^{Sn})$	2,3 =E
5.	$n < pred(pi(i)^{Sn})$	4 T13.13k
6.	$pred(pi(i)^{Sn}) \nmid Sn$	5 T13.24i
7.	$\exists x[pred(pi(i)^x) \nmid Sn]$	6 ∃I

*T13.44. The following are theorems of PA.

(a) PA ⊢ $exp(n,i) = (\mu x \leq n)[pred(pi(i)^x)|n \wedge pred(pi(i)^{x+\bar{1}}) \nmid n]$

(b) PA ⊢ $exp(\emptyset,i) = \emptyset$

*(c) PA ⊢ $exp(Sn,i) = \mu x[pred(pi(i)^x)|Sn \wedge pred(pi(i)^{x+\bar{1}}) \nmid Sn]$

(d) PA ⊢ $pred(pi(i)^{exp(Sn,i)})|Sn \wedge pred(pi(i)^{exp(Sn,i)+\bar{1}}) \nmid Sn$

(e) PA ⊢ $(\forall w < exp(Sn,i))\sim[pred(pi(i)^w)|Sn \wedge pred(pi(i)^{w+\bar{1}}) \nmid Sn]$

(f) PA ⊢ $[pred(pi(i)^a|Sn \wedge pred(pi(i)^{a+\bar{1}} \nmid Sn] \rightarrow exp(Sn,i) = a$

(g) PA ⊢ $exp(m,j) \leq m$

(h) PA ⊢ $j \geq n \rightarrow exp(Sn,j) = \emptyset$

(i) PA ⊢ $exp(pi(i)^p,i) = p$

(j) PA ⊢ $i \neq j \rightarrow exp(pi(i)^p,j) = \emptyset$

(k) PA ⊢ $pred(pi(i))|Sm \leftrightarrow exp(Sm,i) \geq \bar{1}$

*(l) PA ⊢ $\exists q[pi(i)^{exp(Sn,i)} \times q = Sn \wedge pred(pi(i)) \nmid q \wedge \forall y(y \neq i \rightarrow exp(q,y)$
$= exp(Sn,y))]$

*(m) PA $\vdash$ $\mathbb{exp}(Sm \times Sn, i) = \mathbb{exp}(Sm, i) + \mathbb{exp}(Sn, i)$

Hints: (a) is from definition exp and prior results. (c) is by PA $\vdash$ $(\exists x \leq Sn)[pred(\mathbb{pi}(i)^x)|Sn \wedge pred(\mathbb{pi}(i)^{x+\overline{1}}) \nmid Sn]$ and then T13.20b; $ex(n,i) = \emptyset \vee ex(n,i) > \emptyset$; in the latter case, the trick is to generalize on the number prior to $ex(n,i)$. (f) is by showing that $a = \mu x[pred(\mathbb{pi}(i)^x)|Sn \wedge pred(\mathbb{pi}(i)^{x+\overline{1}}) \nmid Sn]$. (l): from $pred(\mathbb{pi}(i)^{\mathbb{exp}(Sn,i)})|Sn$ there is a j such that $\mathbb{pi}(i)^{\mathbb{exp}(Sn,i)} \times j = Sn$; the hard part is to show $k \neq i \rightarrow \mathbb{exp}(j,k) = \mathbb{exp}(Sn,k)$ — for this, it will be helpful to establish that j is a successor. (m): toward an application of T13.44f it will be easy to establish that $pred(\mathbb{pi}(i)^{\mathbb{exp}(Sm,i)+\mathbb{exp}(Sn,i)})|(Sm \times Sn)$; for the other conjunct, it will be helpful to begin with a couple applications of T13.44l.

(a) is from the definition. (b) is the standard result with bound Ø. (c) extracts the successor case from the bounded to an unbounded minimization; this allows application of the definition in (d) and (e). From (f) the reasoning goes the other way around: not only does the condition apply to the exponent, but if the condition applies to some a, then a is the exponent. Then (g) the exponent of some prime in the factorization of m cannot be greater than m; and (h) a prime whose index is greater than or equal to n does not divide into Sn. (i) and (j) make an obvious connection for the exponent of a prime, and (k) between exponent and factor. According (l) once you divide Sn by $\mathbb{pi}(i)$ $\mathbb{exp}(Sn,i)$ times you are left with a q such that $\mathbb{pi}(i)$ does not divide into it any more, and such that the exponents of all the other primes remain the same as in Sn. From (m) the i^{th} exponent of a product sums the i^{th} exponents of its factors.

*T13.45. The following are theorems of PA.

(a) PA $\vdash$ $\mathbb{len}(n) = (\mu y \leq n)(\forall z \leq n)[z \geq y \rightarrow \mathbb{exp}(n,z) = \emptyset]$

(b) PA $\vdash$ $\mathbb{len}(\emptyset) = \emptyset$

(c) PA $\vdash$ $\mathbb{len}(Sn) = \mu y(\forall z \leq Sn)[z \geq y \rightarrow \mathbb{exp}(Sn,z) = \emptyset]$

(d) PA $\vdash$ $(\forall z \leq Sn)[z \geq \mathbb{len}(Sn) \rightarrow \mathbb{exp}(Sn,z) = \emptyset]$

(e) PA $\vdash$ $(\forall w < \mathbb{len}(Sn)) \sim (\forall z \leq Sn)[z \geq w \rightarrow \mathbb{exp}(Sn,z) = \emptyset]$

(f) PA $\vdash$ $\mathbb{len}(\overline{1}) = \emptyset$

(g) PA $\vdash$ $\mathbb{len}(m) > \emptyset \rightarrow m > \overline{1}$

*(h) PA $\vdash$ $\mathbb{exp}(m,l) > \emptyset \rightarrow \mathbb{len}(m) > l$

(i) PA $\vdash (\forall k > l)exp(Sm, k) = \emptyset \rightarrow len(Sm) \leq Sl$

(j) PA $\vdash m > \overline{1} \rightarrow len(m) > \emptyset$

*(k) PA $\vdash p > \emptyset \rightarrow len(pi(i)^p) = Si$

(l) PA $\vdash (\forall z \geq len(n))exp(n, z) = \emptyset$

*(m) PA $\vdash len(n) = Sl \rightarrow exp(n, l) \geq \overline{1}$

Hints: (a) is from definition length and prior results. (c) follows with T13.44h and existentially generalizing on Sn itself. (f) is by application of (c). Under the assumption for $\rightarrow$I, (h) divides into cases for $m = \emptyset$ and $m > \emptyset$; for the latter, suppose $len(m) \not> i$; then you will be able to make use of (d). (j) is straightforward with T13.25d and ultimately (h) above. For (k), begin with $len(pi(i)^p) < Si \lor len(pi(i)^p) = Si \lor len(pi(i)^p) > Si$ by T13.13p; the first is easily eliminated with T13.45h; then, supposing $len(pi(i)^p) > Si$, you will be able to obtain a contradiction using T13.45e. (l): under the assumption $a \geq len(n)$ for ($\forall$I), either $n = \emptyset$ or $n > \emptyset$; the first case is easy; for the second, there is some m such that $n = Sm$; your main reasoning will be to show $exp(Sm, a) = \emptyset$. (m): under the assumption for $\rightarrow$I, the case when $n = \emptyset$ is impossible; so there is some m such that $n = Sm$; with this, suppose $exp(Sm, l) \not\geq \overline{1}$; then you you will be able to show, contrary to your assumption that $len(Sm) = l$.

Again (a) is from the definition and (b) gives the standard result for bound $\emptyset$. (c) extracts the successor case from bounded to unbounded minimization; (d) and (e) then apply the definition. (f) is a simple particular result; and then (g) is an immediate consequence of (b) and (f). From (h) if an exponent of some prime in the factorization of m is greater than zero, that prime is involved in the factorization of m; (j) gives the biconditional from (g); (k) gives the length for a prime to any power; and from (l) primes $\geq$ the length of n must all have exponent $\emptyset$. Length is set up so that it finds the first prime such that it and all the ones after have exponent zero; so (m) the prime prior to the length has exponent $\geq \overline{1}$.

For the rest of this section including results for concatenation to follow, it will be helpful to introduce a couple of auxiliary notions. First, $exc(m, n, i)$ which (indirectly) takes the value of the i^{th} exponent in the concatenation of m and n.

$$\text{PA} \vdash exc(m, n, i) = (\mu y \leq exp(m, i) + exp(n, i \mathbin{\dot{-}} len(m)))$$
$$([i < len(m) \land y = exp(m, i)] \lor [i \geq len(m) \land y = exp(n, i \mathbin{\dot{-}} len(m))])$$

Since the definition is by bounded minimization, no condition is required. The idea is simply to set y to one or the other of $\mathbb{exp}(m,i)$ or $\mathbb{exp}(n, i \dot{-} \mathbb{len}(m))$ so that y takes the value of the i^{th} exponent in the concatenation of m and n. Then $val(n,i)$ returns the product of the first i primes in the factorization of n.

$\text{PA} \vdash val(n, \emptyset) = \overline{1}$
$\text{PA} \vdash val(n, Sy) = val(n, y) \times \mathbb{pi}(y)^{exp(n,y)}$

Similarly $val^*(m,n,i)$ is defined by recursion as follows.

$\text{PA} \vdash val^*(m,n,\emptyset) = \overline{1}$
$\text{PA} \vdash val^*(m,n,Sy) = val^*(m,n,y) \times \mathbb{pi}(y)^{exc(m,n,y)}$

So $val^*(m,n,i)$ returns the product of the first i primes in the factorization of the concatenation of m and n. Here are some results for these notions. Let $l = \mathbb{len}(m) + \mathbb{len}(n)$.

*T13.46. The following are theorems of PA.

(a) $\text{PA} \vdash exc(m,n,i) = \mu y([i < \mathbb{len}(m) \wedge y = \mathbb{exp}(m,i)] \vee [i \geq \mathbb{len}(m) \wedge y = \mathbb{exp}(n, i \dot{-} \mathbb{len}(m))])$

(b) $\text{PA} \vdash i < \mathbb{len}(m) \rightarrow exc(m,n,i) = \mathbb{exp}(m,i)$

(c) $\text{PA} \vdash i \geq \mathbb{len}(m) \rightarrow exc(m,n,i) = \mathbb{exp}(n, i \dot{-} \mathbb{len}(m))$

(d) $\text{PA} \vdash val^*(m,n,i) > \emptyset$

*(e) $\text{PA} \vdash (\forall i \geq a) pred(\mathbb{pi}(i)) \nmid val^*(m,n,a)$

*(f) $\text{PA} \vdash (\forall j < i) \mathbb{exp}(val^*(m,n,i), j) = exc(m,n,j)$

*(g) $\text{PA} \vdash (\forall i < \mathbb{len}(m))[\mathbb{exp}(val^*(m,n,l), i) = \mathbb{exp}(m,i)] \wedge$
$(\forall i < \mathbb{len}(n))[\mathbb{exp}(val^*(m,n,l), i + \mathbb{len}(m)) = \mathbb{exp}(n,i)]$

*(h) $\text{PA} \vdash [\mathbb{pi}(l)^{m+n}]^l \geq val^*(m,n,l)$

(i) $\text{PA} \vdash val(m,i) > \emptyset$

(j) $\text{PA} \vdash \mathbb{len}(val(a,j)) \leq j$

(k) $\text{PA} \vdash \mathbb{len}(val(a,j)) \leq \mathbb{len}(a)$

(l) $\text{PA} \vdash (\forall i < k) \mathbb{exp}(m,i) = \mathbb{exp}(val(m,k), i)$

(m) $\text{PA} \vdash (\forall i < k) \mathbb{exp}(a,i) = \mathbb{exp}(b,i) \rightarrow val(a,k) = val(b,k)$

*(n) $x \geq \mathbb{len}(Sn) \to \mathit{val}(Sn, x) = Sn$

corollary: PA $\vdash \mathit{val}(Sn, \mathbb{len}(Sn)) = Sn$

*(o) PA $\vdash [\mathbb{len}(n) \leq q \wedge (\forall k < \mathbb{len}(n))\mathbb{exp}(n,k) \leq r] \to [\mathbb{pi}(q)^r]^q \geq \mathit{val}(n, \mathbb{len}(n))$

Hints: (e) is by IN on a. (f) is by IN on i; in the show under $(\forall j < i)\mathbb{exp}(\mathit{val}^*(m,n,i), j) = \mathit{exc}(m,n,j)$ and $a < Si$ you will have separate cases for $a < i$ and $a = i$. (g) is straightforward with applications of (f), (b) and (c). For (h) you may obtain $i \leq l \to [\mathbb{pi}(l)^{m+n}]^i \geq \mathit{val}^*(m,n,i)$ by induction on i; in the show, the main task is to obtain $\mathit{exc}(m,n,i) \leq m+n$; the result then follows with previously established inequalities. (j) is easy with a result like (e). For (n) you will be able to show $\forall x \forall n[\mathbb{len}(Sn) \leq x \to \mathit{val}(Sn,x) = Sn]$ by induction on x: the $\emptyset$-case is straightforward; then under the inductive assumption with $\mathbb{len}(Sa) \leq Sx$ for →I you have $\mathbb{len}(Sa) \leq x \vee \mathbb{len}(Sa) = Sx$; the first case is straightforward; the second is an extended argument — you will be able to apply T13.44l to obtain an Sr whose prime factorization is like that of Sa but without $\mathbb{pi}(x)$; show that $\mathbb{len}(Sr) \leq x$ so that from the assumption, $\mathit{val}(Sr,x) = Sr$; then $\mathit{val}(Sa, Sx) = Sa$ is straightforward. For (o) under the assumption for →I, you will be able to get $i \leq q \to [\mathbb{pi}(q)^r]^i \geq \mathit{val}(n,i)$ by IN.

(a) extracts *exc* from the bounded to unbounded minimization; (b) and (c) apply the definition. (d) is obvious. (e) results because $\mathit{val}^*(m,n,a)$ is a product of primes prior to $\mathbb{pi}(a)$ so that greater primes do not divide it. Then (f) the exponents in in *val** are like the exponents in *exc*. This gives us (g) that the exponents in *val** are like the exponents in m and n. But (h) *val** is constructed so that an induction enables a natural comparison of exponents. Then (m) - (o) are related results for *val*.

In cases to follow, the comparison of exponents from (h) and the closely related (o) will be crucial for finding bounds and so extracting results from bounded minimization.

We are now ready for some results about concatenation. Say $m * n$ is the defined correlate to $\mathsf{m} \star \mathsf{n}$ and as above $l = \mathbb{len}(m) + \mathbb{len}(n)$.

*T13.47. The following are theorems of PA.

(a) (i) PA $\vdash m * n = (\mu x \leq B_{m,n})[x \geq \overline{1} \wedge (\forall i < \mathbb{len}(m))\{\mathbb{exp}(x,i) = \mathbb{exp}(m,i)\} \wedge (\forall i < \mathbb{len}(n))\{\mathbb{exp}(x, i + \mathbb{len}(m)) = \mathbb{exp}(n,i)\}]$

(ii) PA $\vdash B_{m,n} = [\mathbb{pi}(l)^{m+n}]^l$

(b) PA $\vdash m * n = \mu x[x \geq \overline{1} \wedge (\forall i < \mathit{len}(m))\{\mathit{exp}(x, i) = \mathit{exp}(m, i)\} \wedge (\forall i < \mathit{len}(n))\{\mathit{exp}(x, i + \mathit{len}(m)) = \mathit{exp}(n, i)\}]$

(c) PA $\vdash m * n \geq \overline{1} \wedge (\forall i < \mathit{len}(m))\{\mathit{exp}(m * n, i) = \mathit{exp}(m, i)\} \wedge (\forall i < \mathit{len}(n))\{\mathit{exp}(m * n, i + \mathit{len}(m)) = \mathit{exp}(n, i)\}$

(d) PA $\vdash (\forall w < m * n){\sim}[w \geq \overline{1} \wedge (\forall i < \mathit{len}(m))\{\mathit{exp}(w, i) = \mathit{exp}(m, i)\} \wedge (\forall i < \mathit{len}(n))\{\mathit{exp}(w, i + \mathit{len}(m)) = \mathit{exp}(n, i)\}]$

*(e) PA $\vdash \mathit{len}(m * n) \geq l$

*(f) PA $\vdash \mathit{len}(m * n) = l$

(g) PA $\vdash \mathit{exp}(m * n, i + \mathit{len}(m)) = \mathit{exp}(n, i)$

(h) PA $\vdash (a * b) * c = a * (b * c)$

(i) PA $\vdash n \leq \overline{1} \rightarrow Sm * n = Sm$

(j) PA $\vdash n \leq \overline{1} \rightarrow n * Sm = Sm$

(k) PA $\vdash (\mathit{len}(c) = \mathit{len}(d) \wedge Sa * c = Sb * d) \rightarrow Sa = Sb$

corollary: PA $\vdash Sa * c = Sb * c \rightarrow Sa = Sb$

(l) PA $\vdash (\mathit{len}(c) = \mathit{len}(d) \wedge c * Sa = d * Sb) \rightarrow Sa = Sb$

corolary: PA $\vdash c * Sa = c * Sb \rightarrow Sa = Sb$

*(m) PA $\vdash \mathit{val}(Sm * Sn, a) = \mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))$

(n) PA $\vdash (\forall y \leq \mathit{len}(n))[\mathit{val}(m * n, y + \mathit{len}(m)) \geq \mathit{val}(m, \mathit{len}(m))]$

corollary: PA $\vdash m * n \geq m$

(o) PA $\vdash (\forall y \leq \mathit{len}(n))[\mathit{val}(m * n, y + \mathit{len}(m)) \geq \mathit{val}(n, y)]$

corollary: PA $\vdash m * n \geq n$

Hints: (a) is from the definition concatenation with prior results. (b) uses T13.46h. (e) divides into cases for $\mathit{len}(n) = \emptyset$ and $\mathit{len}(n) > \emptyset$; and within the first, again, cases for $\mathit{len}(m) = \emptyset$ and $\mathit{len}(m) > \emptyset$. For (f) show $\mathit{len}(m * n) \leq l$ and apply (e); for the main argument (which will be long!) assume $\mathit{len}(m * n) \not\leq l$; then you will be able to apply T13.44l and show that the q so obtained contradicts T13.47d. (h) where $l = \mathit{len}(a) + \mathit{len}(b) + \mathit{len}(c)$, you will be able to show $(\forall i < l)\mathit{exp}((a * b) * c), i) = \mathit{exp}(a * (b * c), i)$. (k) and (l) are straightforward with T13.47c. For (m) you will be able to show $(\forall i < a)\mathbb{exp}(Sm * Sn, i) = \mathbb{exp}(val(Sm, a) * val(Sn, a \dot{-} \mathbb{len}(Sm)), i)$ and so $val(Sm * Sn, a) = val(val(Sm, a) * val(Sn, a \dot{-} \mathbb{len}(Sm)), a)$; and from this the result you want. (n) and (o) are by induction on y (with the bounded quantifier unabbreviated to the associated conditional).

(a) is from the definition. T13.46h enables us to extract $m * n$ from bounded to unbounded minimization to get (b) and then (c) and (d). (e) and (f) establish that the length of $m * n$ sums the lengths of m and n. (h) is an association result — and with this, we typically ignore parentheses in concatenations much as we have done for association with addition. (k) and (l) enable a sort of cancellation law for concatenation. (n) and (o) apply results from T13.46m and T13.46n for relative values of $m * n$.

The idea for application of T13.46h to get (b) is the same as behind the intuitive account of the bound from chapter 12: $\mathbb{pi}(l)^{m+n}$ is greater than every term in the factorization of $m * n$; so $[\mathbb{pi}(l)^{m+n}]^i$ remains greater than $val^*(m, n, i)$; and $val^*(m, n, l)$ is therefore both under the bound and satisfies the condition for $m * n$ — so that the existential condition is satisfied, and we may extract the bounded to an unbounded minimization. Once this is accomplished, we are most of the way home.

To manipulate $\mathbb{T}ermseq$ it will be convenient to let,

$$
\begin{aligned}
A(s,x) &= \mathbb{exp}(s,x) = \ulcorner \emptyset \urcorner \lor \mathbb{V}ar(\mathbb{exp}(s,x)) \\
B(s,x) &= (\exists j < x)\mathbb{exp}(s,x) = \ulcorner S \urcorner * \mathbb{exp}(s,j) \\
C(s,x) &= (\exists i < x)(\exists j < x)\mathbb{exp}(s,x) = \ulcorner + \urcorner * \mathbb{exp}(s,i) * \mathbb{exp}(s,j) \\
D(s,x) &= (\exists i < x)(\exists j < x)\mathbb{exp}(s,x) = \ulcorner \times \urcorner * \mathbb{exp}(s,i) * \mathbb{exp}(s,j)
\end{aligned}
$$

*T13.48. The following are theorems of PA.

(a) PA $\vdash \mathbb{T}ermseq(m,t) \leftrightarrow \mathbb{exp}(m, \mathbb{len}(m) \dot{-} \overline{1}) = t \land m > \overline{1} \land (\forall k < \mathbb{len}(m))[A(m,k) \lor B(m,k) \lor C(m,k) \lor D(m,k)]$

(b) (i) PA $\vdash \mathbb{T}erm(t) \leftrightarrow (\exists x \leq B_t)\mathbb{T}ermseq(x,t)$

(ii) PA $\vdash B_t = [\mathbb{pi}(\mathbb{len}(t))^t]^{\mathbb{len}(t)}$

(c) PA $\vdash \mathbb{V}ar(t) \leftrightarrow (\exists x \leq t)(t = \overline{2}^{\overline{23}+\overline{2}x})$

(d) PA $\vdash \mathbb{V}ar(t) \rightarrow \mathbb{len}(t) = \overline{1}$

(e) PA $\vdash \mathbb{T}ermseq(m,t) \rightarrow (\forall k < \mathbb{len}(m))\mathbb{exp}(m,k) > \overline{1}$

(f) PA $\vdash \mathbb{T}erm(t) \rightarrow t > \overline{1}$

(g) PA $\vdash t = \ulcorner\emptyset\urcorner \rightarrow \mathbb{T}ermseq(\overline{2}^{t}, t)$

(h) PA $\vdash \mathbb{V}ar(t) \rightarrow \mathbb{T}ermseq(\overline{2}^{t}, t)$

*(i) PA $\vdash \mathbb{T}ermseq(m, t) \rightarrow \mathbb{T}ermseq(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, \ulcorner S \urcorner * t)$

(j) PA $\vdash [\mathbb{T}ermseq(m, t) \wedge \mathbb{T}ermseq(n, q)] \rightarrow \mathbb{T}ermseq(m * n * \overline{2}^{\overline{\ulcorner + \urcorner} * t * q}, \ulcorner + \urcorner * t * q)$

(k) PA $\vdash [\mathbb{T}ermseq(m, t) \wedge \mathbb{T}ermseq(n, q)] \rightarrow \mathbb{T}ermseq(m * n * \overline{2}^{\overline{\ulcorner \times \urcorner} * t * q}, \overline{\ulcorner \times \urcorner} * t * q)$

*(l) PA $\vdash \mathbb{T}ermseq(m, t) \rightarrow \forall x (\forall k < \mathbb{l}en(m))\{\mathbb{l}en(\mathbb{e}xp(m, k)) \leq x \rightarrow \exists n[\mathbb{T}ermseq(n, \mathbb{e}xp(m, k)) \wedge (\forall i < \mathbb{l}en(n))\mathbb{e}xp(n, i) \leq \mathbb{e}xp(m, k) \wedge \mathbb{l}en(n) \leq \mathbb{l}en(\mathbb{e}xp(m, k))]\}$

(m) PA $\vdash \mathbb{T}ermseq(m, t) \rightarrow \mathbb{T}erm(t)$

*(n) PA $\vdash \mathbb{T}ermseq(m, t) \rightarrow (\forall i < \mathbb{l}en(m))\mathbb{T}erm(\mathbb{e}xp(m, i))$

(o) PA $\vdash \mathbb{T}erm(\overline{\ulcorner\emptyset\urcorner})$

(p) PA $\vdash \mathbb{V}ar(v) \rightarrow [\mathbb{T}erm(v) \wedge \mathbb{T}erm(\overline{\ulcorner S \urcorner} * v)]$

Hints: (e) is straightforward by an extended $\vee$E. (g) - (k) are disjunctive but straightforward. (l) is by induction on x: under the assumption $\mathbb{T}ermseq(m, t)$ the basis is straightforward; then, under the inductive assumption along with $a < \mathbb{l}en(m)$ for $(\forall)$I and $\mathbb{l}en(\mathbb{e}xp(m, a)) \leq Sx$ for $\rightarrow$I, apply (a); the derivation is then a (long!) argument by cases where you will be able to apply (g)-(k). (m) follows easily with T13.46o. For (n) under the assumption for $\rightarrow$I, you will be able to show $\forall k[k < \mathbb{l}en(m) \rightarrow \exists x(\mathbb{T}ermseq(x, \mathbb{e}xp(m, k))]$ by strong induction; the result follows easily.

(a), (b) and (c) are from the definitions term sequence and term and variable with prior results. (d), (e) and (f) are simple results. (g) - (k) generate term sequences. (l) yields (m), that anything with a term sequence is a term; the rest follow from that.

From its definition, $\mathbb{T}erm(t)$ does not immediately follow from $\mathbb{T}ermseq(m, t)$ insofar as the sequence might build in extraneous terms not required for t — with the result that m is not less than B_n. The general idea for these theorems is that given a term sequence, there is a *standard* term sequence containing just the elements you would have included in a chapter 4 tree, adequate to yield $\mathbb{T}erm(t)$. Thus we move from the existence of a term sequence through (l) to a term sequence of the right sort, and so to (m). Something new happens in (l) insofar as the induction is not on the length of m but on the length of its *exponents*.

We continue with some results for $\mathbb{F}ormseq$ and $\mathbb{W}ff$ that are closely related to T13.48. Let,

$$
\begin{array}{lcl}
E(s,x) & = & \mathbb{A}tomic(\mathbb{e}xp(s,x)) \\
F(s,x) & = & (\exists j < x)[\mathbb{e}xp(s,x) = \mathbb{n}eg(\mathbb{e}xp(s,j))] \\
G(s,x) & = & (\exists i < x)(\exists j < x)[\mathbb{e}xp(s,x) = \mathbb{c}nd(\mathbb{e}xp(s,i),\mathbb{e}xp(s,j))] \\
H(p,s,x) & = & (\exists i < x)(\exists j < p)[\mathbb{V}ar(j) \wedge \mathbb{e}xp(s,x) = \mathbb{u}nv(j,\mathbb{e}xp(s,i))]
\end{array}
$$

*T13.49. The following are theorems of PA.

(a) PA $\vdash \mathbb{F}ormseq(m,p) \leftrightarrow \mathbb{e}xp(m,\mathbb{l}en(m) \dot{-} \overline{1}) = p \wedge m > \overline{1} \wedge (\forall k < \mathbb{l}en(m))[E(m,k) \vee F(m,k) \vee G(m,k) \vee H(p,m,k)]$

(b) (i) PA $\vdash \mathbb{W}ff(p) \leftrightarrow (\exists x \leq B_p)\mathbb{F}ormseq(x,p)$

(ii) PA $\vdash B_p = [\mathbb{p}i(\mathbb{l}en(p))^p]^{\mathbb{l}en(p)}$

(c) PA $\vdash \mathbb{A}tomic(p) \leftrightarrow (\exists x \leq p)(\exists y \leq p)[\mathbb{T}erm(x) \wedge \mathbb{T}erm(y) \wedge p = \overline{\ulcorner = \urcorner} * x * y$

(d) PA $\vdash \mathbb{F}ormseq(m,p) \rightarrow (\forall k < \mathbb{l}en(m))\mathbb{e}xp(m,k) > \overline{1}$

(e) PA $\vdash \mathbb{W}ff(p) \rightarrow p > \overline{1}$

(f) PA $\vdash \mathbb{A}tomic(p) \rightarrow \mathbb{F}ormseq(\overline{2}^p, p)$

(g) PA $\vdash \mathbb{F}ormseq(m,p) \rightarrow \mathbb{F}ormseq(m * \overline{2}^{\mathbb{n}eg(p)}, \mathbb{n}eg(p))$

(h) PA $\vdash [\mathbb{F}ormseq(m,p) \wedge \mathbb{F}ormseq(n,q)] \rightarrow \mathbb{F}ormseq(m * n * \overline{2}^{\mathbb{c}nd(p,q)})$

(i) PA $\vdash [\mathbb{F}ormseq(m,p) \wedge \mathbb{v}ar(v)] \rightarrow \mathbb{F}ormseq(m * \overline{2}^{\mathbb{u}nv(v,p)}, \mathbb{u}nv(v,p))$

(j) PA $\vdash \mathbb{F}ormseq(m,p) \rightarrow \forall x(\forall k < \mathbb{l}en(m))\{\mathbb{l}en(\mathbb{e}xp(m,k)) \leq x \rightarrow \exists n[\mathbb{F}ormseq(n, \mathbb{e}xp(m,k)) \wedge (\forall i < \mathbb{l}en(n))\mathbb{e}xp(n,i) \leq \mathbb{e}xp(m,k) \wedge \mathbb{l}en(n) \leq \mathbb{l}en(\mathbb{e}xp(m,k))]\}$

(k) PA $\vdash \mathbb{F}ormseq(m,p) \rightarrow \mathbb{W}ff(p)$

(l) PA $\vdash \mathbb{F}ormseq(m,p) \rightarrow (\forall i < \mathbb{l}en(m))\mathbb{W}ff(\mathbb{e}xp(m,i))$

(m) PA $\vdash \mathbb{A}tomic(p) \rightarrow \mathbb{W}ff(p)$

(n) PA $\vdash \mathbb{W}ff(p) \rightarrow \mathbb{W}ff(\mathbb{n}eg(p))$

(o) PA $\vdash [\mathbb{W}\!f\!f(p) \wedge \mathbb{W}\!f\!f(q)] \to \mathbb{W}\!f\!f(\mathbb{c}nd(p,q))$

(p) PA $\vdash [\mathbb{W}\!f\!f(p) \wedge \mathbb{V}ar(v)] \to \mathbb{W}\!f\!f(\mathbb{u}nv(v,p))$

Hints: For each of (a) - (l), see the parallel theorems for T13.48. The others are nearly trivial.

Again, from its definition, $\mathbb{W}\!f\!f(p)$ does not immediately follow from $\mathbb{F}ormseq(m,p)$ insofar as the sequence might build in extraneous elements not required for p — with the result that m is not less than B_p. And again the general idea is that given a formula sequence, there is a *standard* formula sequence containing just the elements you would have included in a chapter 4 tree, adequate to yield $\mathbb{W}\!f\!f(n)$. Thus we move from the existence of a formula sequence through (j) to a formula sequence of the required sort.

Continuing roughly in the order of chapter 12 we move on to some substitution results for terms and atomics. Let,

$$
\begin{array}{lcl}
I(m,n,k) & = & \mathbb{e}xp(m,k) = \overline{\ulcorner \emptyset \urcorner} \wedge \mathbb{e}xp(n,k) = \overline{\ulcorner \emptyset \urcorner} \\
J(v,m,n,k) & = & \mathbb{V}ar(\mathbb{e}xp(m,k)) \wedge \mathbb{e}xp(m,k) \neq v \wedge \mathbb{e}xp(n,k) = \mathbb{e}xp(m,k) \\
K(v,s,m,n,k) & = & \mathbb{V}ar(\mathbb{e}xp(m,k)) \wedge \mathbb{e}xp(m,k) = v \wedge \mathbb{e}xp(n,k) = s \\
L(m,n,k) & = & (\exists i < k)[\mathbb{e}xp(m,k) = \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,i) \wedge \mathbb{e}xp(n,k) = \overline{\ulcorner S \urcorner} * \mathbb{e}xp(n,i)] \\
M(m,n,k) & = & (\exists i < k)(\exists j < k)[\mathbb{e}xp(m,k) = \overline{\ulcorner + \urcorner} * \mathbb{e}xp(m,i) * \mathbb{e}xp(m,j) \wedge \\
 & & \quad \mathbb{e}xp(n,k) = \overline{\ulcorner + \urcorner} * \mathbb{e}xp(n,i) * \mathbb{e}xp(n,j)] \\
N(m,n,k) & = & (\exists i < k)(\exists j < k)[\mathbb{e}xp(m,k) = \overline{\ulcorner \times \urcorner} * \mathbb{e}xp(m,i) * \mathbb{e}xp(m,j) \wedge \\
 & & \quad \mathbb{e}xp(n,k) = \overline{\ulcorner \times \urcorner} * \mathbb{e}xp(n,i) * \mathbb{e}xp(n,j)]
\end{array}
$$

*T13.50. The following are theorems of PA.

(a) PA $\vdash \mathbb{T}subseq(m,n,t,v,s,u) \leftrightarrow \mathbb{T}ermseq(m,t) \wedge \mathbb{l}en(m) = \mathbb{l}en(n) \wedge \mathbb{e}xp(n, \mathbb{l}en(n) \dot{-} \overline{1}) = u \wedge (\forall k < \mathbb{l}en(m))(I(m,n,k) \vee J(v,m,n,k) \vee K(v,s,m,n,k) \vee L(m,n,k) \vee M(m,n,k) \vee N(m,n,k))$

(b) (i) PA $\vdash \mathbb{T}ermsub(t,v,s,u) \leftrightarrow (\exists x \leq X_t)(\exists y \leq Y_{t,u})\mathbb{T}subseq(x,y,t,v,s,u)$

(ii) PA $\vdash X_t = [\mathbb{p}i(\mathbb{l}en(t))^t]^{\mathbb{l}en(t)}$

(iii) PA $\vdash Y_{t,u} = [\mathbb{p}i(\mathbb{l}en(t))^u]^{\mathbb{l}en(t)}$

(c) PA $\vdash \mathbb{A}tomsub(p,v,s,q) \leftrightarrow (\exists a \leq p)(\exists b \leq p)(\exists a' \leq q)(\exists b' \leq q)[\mathbb{T}erm(a) \wedge \mathbb{T}erm(b) \wedge p = \overline{\ulcorner = \urcorner} * a * b \wedge \mathbb{T}ermsub(a,v,s,a') \wedge \mathbb{T}ermsub(b,v,s,b') \wedge q = \overline{\ulcorner = \urcorner} * a' * b']$

(d) PA $\vdash [\mathbb{T}erm(s) \wedge \mathbb{T}subseq(m,n,t,v,s,u)] \to (\forall j < \mathbb{l}en(n))\mathbb{T}erm(\mathbb{e}xp(n,j))$

corollary: PA $\vdash [\mathbb{T}erm(s) \wedge \mathbb{T}ermsub(t,v,s,u)] \to \mathbb{T}erm(u)$

(e) PA $\vdash [\mathbb{T}erm(s) \wedge \mathbb{A}tomsub(p, v, s, q)] \rightarrow \mathbb{A}tomic(q)$

(f) PA $\vdash t = \overline{\ulcorner \emptyset \urcorner} \rightarrow \mathbb{T}subseq(\overline{2}^{t}, \overline{2}^{t}, t, v, s, t)$

(g) PA $\vdash (\mathbb{V}ar(t) \wedge t \neq v) \rightarrow \mathbb{T}subseq(\overline{2}^{t}, \overline{2}^{t}, t, v, s, t)$

(h) PA $\vdash (\mathbb{V}ar(t) \wedge t = v) \rightarrow \mathbb{T}subseq(\overline{2}^{t}, \overline{2}^{s}, t, v, s, s)$

*(i) PA $\vdash \mathbb{T}subseq(m, n, t, v, s, u) \rightarrow \mathbb{T}subseq(m * \overline{2}^{\overline{\ulcorner S \urcorner}*t}, n * \overline{2}^{\overline{\ulcorner S \urcorner}*u}, \overline{\ulcorner S \urcorner} * t, v, s, \overline{\ulcorner S \urcorner} * u)$

(j) PA $\vdash [\mathbb{T}subseq(m, n, t, v, s, u) \wedge \mathbb{T}subseq(m', n', t', v, s, u')] \rightarrow \mathbb{T}subseq(m * m' * \overline{2}^{\overline{\ulcorner + \urcorner}*t*t'}, n * n' * \overline{2}^{\overline{\ulcorner + \urcorner}*u*u'}, \overline{\ulcorner + \urcorner} * t * t', v, s, \overline{\ulcorner + \urcorner} * u * u')$

(k) PA $\vdash [\mathbb{T}subseq(m, n, t, v, s, u) \wedge \mathbb{T}subseq(m', n', t', v, s, u')] \rightarrow \mathbb{T}subseq(m * m' * \overline{2}^{\overline{\ulcorner \times \urcorner}*t*t'}, n * n' * \overline{2}^{\overline{\ulcorner \times \urcorner}*u*u'}, \overline{\ulcorner \times \urcorner} * t * t', v, s, \overline{\ulcorner \times \urcorner} * u * u')$

*(l) PA $\vdash \mathbb{T}subseq(m, n, t, v, s, u) \rightarrow \mathbb{T}ermsub(t, v, s, u)$

*(m) PA $\vdash [\mathbb{T}erm(t) \wedge \mathbb{T}erm(s)] \rightarrow \exists u[\mathbb{T}ermsub(t, v, s, u) \wedge \mathbb{l}en(u) \leq \mathbb{l}en(t) \times \mathbb{l}en(s) \wedge (\forall k < \mathbb{l}en(u))\mathbb{e}xp(u, k) \leq t + s]$

*(n) PA $\vdash [\mathbb{A}tomic(p) \wedge \mathbb{T}erm(s)] \rightarrow \exists q[\mathbb{A}tomsub(p, v, s, q) \wedge \mathbb{l}en(q) \leq \mathbb{l}en(p) \times \mathbb{l}en(s) \wedge (\forall k < \mathbb{l}en(q))\mathbb{e}xp(q, k) \leq p + s]$

Hints: For (l) let $\mathcal{P}(m, n, v, s, k) = \exists a \exists b[\mathbb{T}subseq(a, b, \mathbb{e}xp(m, k), v, s, \mathbb{e}xp(n, k)) \wedge \mathbb{l}en(a) \leq \mathbb{l}en(\mathbb{e}xp(m, k)) \wedge (\forall i < \mathbb{l}en(a))(\mathbb{e}xp(a, i) \leq \mathbb{e}xp(m, k) \wedge \mathbb{e}xp(b, i) \leq \mathbb{e}xp(n, k))]$; then under the assumption for $\rightarrow$I, show $\forall x(\forall k < \mathbb{l}en(m))[\mathbb{l}en(\mathbb{e}xp(m, k) \leq x \rightarrow \mathcal{P}]$ by IN; the result follows from this. Similarly, for (m) let $\mathcal{P}(m, i, v, s) = \exists x \exists y \exists u[\mathbb{T}subseq(x, y, \mathbb{e}xp(m, i), v, s, u) \wedge \mathbb{l}en(u) \leq \mathbb{l}en(\mathbb{e}xp(m, i)) \times \mathbb{l}en(s) \wedge (\forall k < \mathbb{l}en(u))\mathbb{e}xp(u, k) \leq \mathbb{e}xp(m, i) + s]$; under the assumption $\mathbb{T}erm(t) \wedge \mathbb{T}erm(s)$ given $\mathbb{T}ermseq(m, t)$ you will be able to show $\forall i[i < \mathbb{l}en(m) \rightarrow \mathcal{P}]$ by strong induction on i (with extended disjunctions in both the basis and show); the result follows easily from this.

Some substitution results for formulas are closely related to the previous theorem. Let,

$$
\begin{array}{lcl}
O(v,s,m,n,k) & = & \mathbb{A}tomic(\mathbb{e}xp(m,k)) \wedge \mathbb{A}tomsub(\mathbb{e}xp(m,k),v,s,\mathbb{e}xp(n,k)) \\
P(m,n,k) & = & (\exists i < k)[\mathbb{e}xp(m,k) = \mathbb{n}eg(\mathbb{e}xp(m,i)) \wedge \mathbb{e}xp(n,k) = \mathbb{n}eg(\mathbb{e}xp(n,i))] \\
Q(m,n,k) & = & (\exists i < k)(\exists j < k)[\mathbb{e}xp(m,k) = \mathbb{c}nd(\mathbb{e}xp(m,i),\mathbb{e}xp(m,j)) \wedge \\
& & \quad \mathbb{e}xp(n,k) = \mathbb{c}nd(\mathbb{e}xp(n,i),\mathbb{e}xp(n,j))] \\
R(v,p,m,n,k) & = & (\exists i < k)(\exists j < p)[\mathbb{V}ar(j) \wedge j \neq v \wedge \mathbb{e}xp(m,k) = \mathbb{u}nv(j,\mathbb{e}xp(m,i)) \wedge \\
& & \quad \mathbb{e}xp(n,k) = \mathbb{u}nv(j,\mathbb{e}xp(n,i)] \\
S(v,p,m,n,k) & = & (\exists i < k)(\exists j < p)[\mathbb{V}ar(j) \wedge j = v \wedge \mathbb{e}xp(m,k) = \mathbb{u}nv(j,\mathbb{e}xp(m,i)) \wedge \\
& & \quad \mathbb{e}xp(n,k) = \mathbb{e}xp(m,k)]
\end{array}
$$

*T13.51. The following are theorems of PA.

(a) PA $\vdash$ $\mathbb{F}subseq(m,n,p,v,s,q) \leftrightarrow [\mathbb{F}ormseq(m,p) \wedge \mathbb{l}en(m) = \mathbb{l}en(n) \wedge \mathbb{e}xp(n,\mathbb{l}en(n) \dot{-} \overline{1}) = q \wedge (\forall k < \mathbb{l}en(m))(O(v,s,m,n,k) \vee P(m,n,k) \vee Q(m,n,k) \vee R(p,m,n,k) \vee S(p,m,n,k))]$

(b) (i) PA $\vdash$ $\mathbb{F}ormsub(p,v,s,q) \leftrightarrow (\exists x \leq X_p)(\exists y \leq Y_{p,q})\mathbb{F}subseq(x,y,p,v,s,q)$

(ii) PA $\vdash$ $X_p = [\mathbb{p}i(\mathbb{l}en(p))^p]^{\mathbb{l}en(p)}$

(iii) PA $\vdash$ $Y_{p,q} = [\mathbb{p}i(\mathbb{l}en(p))^q]^{\mathbb{l}en(p)}$

(c) (i) PA $\vdash$ $formusb(p,v,s) = (\mu q \leq Z_{p,s})\mathbb{F}ormsub(p,v,s,q)$

(ii) PA $\vdash$ $Z_{p,s} = [\mathbb{p}i(\mathbb{l}en(p) \times \mathbb{l}en(s))^{p+s}]^{\mathbb{l}en(p) \times \mathbb{l}en(s)}$

(d) PA $\vdash$ $[\mathbb{T}erm(s) \wedge \mathbb{F}subseq(m,n,p,v,s,q)] \to (\forall j < \mathbb{l}en(n))\mathbb{W}\!f\!f(\mathbb{e}xp(n,j))$

corollary: PA $\vdash$ $[\mathbb{T}erm(s) \wedge \mathbb{F}ormsub(p,v,s,q)] \to \mathbb{W}\!f\!f(q)$

(e) PA $\vdash$ $[\mathbb{A}tomic(p) \wedge \mathbb{A}tomsub(p,v,s,q)] \to \mathbb{F}subseq(\overline{2}^p, \overline{2}^q, p, v, s, q)$

(f) PA $\vdash$ $\mathbb{F}subseq(m,n,p,v,s,q) \to \mathbb{F}subseq(m*\overline{2}^{\mathbb{n}eg(p)}, n*\overline{2}^{\mathbb{n}eg(q)}, \mathbb{n}eg(p), v, s, \mathbb{n}eg(q))$

(g) PA $\vdash$ $[\mathbb{F}subseq(m,n,p,v,s,q) \wedge \mathbb{F}subseq(m',n',p',v,s,q')] \to \mathbb{F}subseq(m * m' * \overline{2}^{\mathbb{c}nd(p,p')}, n * n' * \overline{2}^{\mathbb{c}nd(q,q')}, \mathbb{c}nd(p,p'), v, s, \mathbb{c}nd(q,q'))$

(h) PA $\vdash$ $[\mathbb{F}subseq(m,n,p,v,s,q) \wedge \mathbb{V}ar(u) \wedge u \neq v] \to \mathbb{F}subseq(m*\overline{2}^{\mathbb{u}nv(u,p)}, n*\overline{2}^{\mathbb{u}nv(u,q)}, \mathbb{u}nv(u,p), v, s, \mathbb{u}nv(u,q))$

(i) PA $\vdash$ $[\mathbb{F}subseq(m,n,p,v,s,q) \wedge \mathbb{V}ar(u) \wedge u = v] \to \mathbb{F}subseq(m*\overline{2}^{\mathbb{u}nv(u,p)}, n*\overline{2}^{\mathbb{u}nv(u,p)}, \mathbb{u}nv(u,p), v, s, \mathbb{u}nv(u,p))$

(j) PA $\vdash$ $\mathbb{F}subseq(m,n,p,v,s,q) \to \mathbb{F}ormsub(p,v,s,q)$

(k) PA $\vdash$ $[\mathbb{W}\!f\!f(p) \wedge \mathbb{T}erm(s)] \to \exists q[\mathbb{F}ormsub(p,v,s,q) \wedge \mathbb{l}en(q) \leq \mathbb{l}en(p) \times \mathbb{l}en(s) \wedge (\forall k < \mathbb{l}en(q))\mathbb{e}xp(q,k) \leq p+s]$

(l) PA $\vdash [\mathbb{W}\mathit{ff}(p) \wedge \mathbb{T}\mathit{erm}(s)] \rightarrow \mathbb{F}\mathit{ormsub}(p, v, s, \mathit{formsub}(p, v, s))$

(m) PA $\vdash [\mathbb{W}\mathit{ff}(p) \wedge \mathbb{T}\mathit{erm}(s)] \rightarrow \mathbb{W}\mathit{ff}(\mathit{formsub}(p, v, s))$

Hints: For (a) - (k) see the parallel results from T13.50. (l) follows easily with (k).

Finally we extend our results by means of a pair of matched theorems whose results are related to unique readability for terms and then formulas (see chapter 11, p. 522).

*T13.52. The following result in PA.

First, as a preliminary to T13.52f and then T13.53g it will be helpful to show the following. We are thinking of $c * a * c_1 * b * c_2$ as for example, $\overline{\ulcorner (\urcorner} * a * \overline{\ulcorner \rightarrow \urcorner} * b * \overline{\ulcorner) \urcorner}$. Let,

$$
\begin{aligned}
l_1 &= \mathbb{l}\mathit{en}(c)\\
l_2 &= \mathbb{l}\mathit{en}(c) + \mathbb{l}\mathit{en}(a)\\
l_3 &= \mathbb{l}\mathit{en}(c) + \mathbb{l}\mathit{en}(a) + \mathbb{l}\mathit{en}(c_1)\\
l_4 &= \mathbb{l}\mathit{en}(c) + \mathbb{l}\mathit{en}(a) + \mathbb{l}\mathit{en}(c_1) + \mathbb{l}\mathit{en}(b)\\
l &= \mathbb{l}\mathit{en}(c) + \mathbb{l}\mathit{en}(a) + \mathbb{l}\mathit{en}(c_1) + \mathbb{l}\mathit{en}(b) + \mathbb{l}\mathit{en}(c_2)
\end{aligned}
$$

*(a)

a.	$\forall u[(\mathcal{P}(u) \wedge \mathbb{l}\mathit{en}(u) \leq x) \rightarrow (\forall k < \mathbb{l}\mathit{en}(u) {\sim}\mathcal{P}(\mathit{val}(u, k))]$	P
b.	$\mathit{val}(c, j) * \mathit{val}(a, j \dot{-} l_1) * \mathit{val}(c_1, j \dot{-} l_2) * \mathit{val}(b, j \dot{-} l_3) * \mathit{val}(c_2, j \dot{-} l_4) = c * d * c_1 * e * c_2$	P
c.	$\mathcal{P}(a) \wedge \mathcal{P}(b) \wedge \mathcal{P}(d) \wedge \mathcal{P}(e)$	P
d.	$\forall v(\mathcal{P}(v) \rightarrow v > \overline{1})$	P
e.	$\mathbb{l}\mathit{en}(c) = 1 \wedge c_1 > \emptyset \wedge c_2 > \emptyset \wedge \mathbb{l}\mathit{en}(c_1) \leq 1 \wedge \mathbb{l}\mathit{en}(c_2) \leq 1$	P
f.	$j < l \wedge Sx \geq l$	P
	$\vdots$	
g.	$\bot$	

So these premises are inconsistent. As a corollary, when $c_1 = c_2 = \overline{1}$ their lengths go to zero and by T13.46n for any x, $\mathit{val}(c_1, x) = \mathit{val}(c_2, x) = \overline{1}$ so that these terms drop out of the concatenations and the theorem reduces to a version where (b) is $\mathit{val}(c, j) * \mathit{val}(a, j \dot{-} l_1) * \mathit{val}(b, j \dot{-} l_3) = c * d * e$, and the only substantive conjunct of (e) is the first.

(b) PA $\vdash [\mathbb{T}\mathit{erm}(a) \wedge \mathbb{T}\mathit{erm}(b)] \rightarrow [\overline{\ulcorner S \urcorner} * a = \overline{\ulcorner S \urcorner} * b \rightarrow a = b]$

(c) PA $\vdash \mathbb{T}\mathit{erm}(\overline{\ulcorner S \urcorner} * a) \rightarrow \exists r[\overline{\ulcorner S \urcorner} * a = \overline{\ulcorner S \urcorner} * r \wedge \mathbb{T}\mathit{erm}(r)]$

(d) PA $\vdash \mathbb{T}\mathit{erm}(\overline{\ulcorner + \urcorner} * a) \rightarrow \exists r \exists s[\overline{\ulcorner + \urcorner} * a = \overline{\ulcorner + \urcorner} * r * s \wedge \mathbb{T}\mathit{erm}(r) \wedge \mathbb{T}\mathit{erm}(s)]$

(e) PA $\vdash \mathbb{T}\mathit{erm}(\overline{\ulcorner \times \urcorner} * a) \rightarrow \exists r \exists s[\overline{\ulcorner \times \urcorner} * a = \overline{\ulcorner \times \urcorner} * r * s \wedge \mathbb{T}\mathit{erm}(r) \wedge \mathbb{T}\mathit{erm}(s)]$

*(f) PA $\vdash \mathbb{T}\mathit{erm}(t) \rightarrow (\forall k < \mathit{len}(t)) {\sim}\mathbb{T}\mathit{erm}(\mathit{val}(t, k))$

(g) PA $\vdash$ $[\mathbb{T}erm(a) \wedge \mathbb{T}erm(b) \wedge \mathbb{T}erm(c) \wedge \mathbb{T}erm(d)] \rightarrow [\overline{\ulcorner + \urcorner} * a * b = \overline{\ulcorner + \urcorner} * c * d \rightarrow (a = c \wedge b = d)]$

(h) PA $\vdash$ $[\mathbb{T}erm(a) \wedge \mathbb{T}erm(b) \wedge \mathbb{T}erm(c) \wedge \mathbb{T}erm(d)] \rightarrow [\overline{\ulcorner \times \urcorner} * a * b = \overline{\ulcorner \times \urcorner} * c * d \rightarrow (a = c \wedge b = d)]$

(i) PA $\vdash$ $[\mathbb{T}erm(a) \wedge \mathbb{T}erm(b) \wedge \mathbb{T}erm(c) \wedge \mathbb{T}erm(d)] \rightarrow [\overline{\ulcorner = \urcorner} * a * b = \overline{\ulcorner = \urcorner} * c * d \rightarrow (a = c \wedge b = d)]$

Hints: For (a) suppose $j \leq l_1$, this leads to contradiction so that $j \geq l_1$ and you can "pick off" the first conjunct from premise (b) to get $val(a, j \dot{-} l_1) * val(c_1, j \dot{-} l_2) * val(b, j \dot{-} l_3) * val(c_2, j \dot{-} l_4) = d * c_1 * e * c_2$; suppose $j < l_2$, again this leads to contradiction so that $j \geq l_2$; either $\mathbb{l}en(d) < \mathbb{l}en(a) \vee \mathbb{l}en(d) = \mathbb{l}en(a) \vee \mathbb{l}en(d) > \mathbb{l}en(a)$; the first and last lead to contradiction and with the other you will be able to pick off another conjunct; continue to $j \geq l$, which contradicts the last premise. For (f) show $\forall t[(\mathbb{T}erm(t) \wedge \mathbb{l}en(t) \leq x) \rightarrow (\forall k < len(t)) \sim \mathbb{T}erm(val(t, k))]$ by induction on x; the zero case is easy; then under the inductive assumption with $\mathbb{T}erm(a) \wedge \mathbb{l}en(a) \leq Sx$ for $\rightarrow$I and $j < len(a)$ for ($\forall$I) you will be able to show $j > \emptyset$; then with $\mathbb{T}ermseq(m, a)$ the argument is an extended disjunction from $A(m, \mathbb{l}en(m) \dot{-} \overline{1}) \vee B(m, \mathbb{l}en(m) \dot{-} \overline{1}) \vee C(m, \mathbb{l}en(m) \dot{-} \overline{1}) \vee D(m, \mathbb{l}en(m) \dot{-} \overline{1})$; you can assume $\mathbb{T}erm(val(a, j))$ and reach contradiction in each case.

Returning to our original results for unique readability, reasoning for (c) - (e) is like that for T11.3 - T11.5. Then (f) is like T11.6. And there are the parallel results for formulas.

*T13.53. The following are theorems of PA.

(a) PA $\vdash [\mathbb{W}\!f\!f(p) \wedge \mathbb{W}\!f\!f(q)] \rightarrow [\mathbb{n}eg(p) = \mathbb{n}eg(q) \rightarrow p = q]$

(b) PA $\vdash [\mathbb{W}\!f\!f(p)) \wedge \mathbb{V}ar(u) \wedge \mathbb{W}\!f\!f(q) \wedge \mathbb{V}ar(v)] \rightarrow [\mathbb{u}nv(u, p) = \mathbb{u}nv(v, q) \rightarrow (u = v \wedge p = q)]$

(c) PA $\vdash \mathbb{W}\!f\!f(\overline{\ulcorner = \urcorner} * a) \rightarrow \exists r \exists s[\overline{\ulcorner = \urcorner} * a = \overline{\ulcorner = \urcorner} * r * s \wedge \mathbb{T}erm(r) \wedge \mathbb{T}erm(s)]$

(d) PA $\vdash \mathbb{W}\!f\!f(\overline{\ulcorner \sim \urcorner} * p) \rightarrow \exists r[\overline{\ulcorner \sim \urcorner} * p = \mathbb{n}eg(r) \wedge \mathbb{W}\!f\!f(r)]$

(e) PA $\vdash \mathbb{W}\!f\!f(\overline{\ulcorner (\urcorner} * p) \rightarrow \exists r \exists s[\overline{\ulcorner (\urcorner} * p = \mathbb{c}nd(r, s) \wedge \mathbb{W}\!f\!f(r) \wedge \mathbb{W}\!f\!f(s)]$

(f) PA $\vdash \mathbb{W}\!f\!f(\overline{\ulcorner \forall \urcorner} * p) \rightarrow \exists w \exists r[\overline{\ulcorner \forall \urcorner} * p = \mathbb{u}nv(w, r) \wedge \mathbb{V}ar(w) \wedge \mathbb{W}\!f\!f(r)]$

(g) PA $\vdash \mathbb{W}\!f\!f(p) \rightarrow (\forall k < len(p)){\sim}\mathbb{W}\!f\!f(val(p,k))$

*(h) PA $\vdash [\mathbb{W}\!f\!f(p)) \wedge \mathbb{W}\!f\!f(q) \wedge \mathbb{W}\!f\!f(a) \wedge \mathbb{W}\!f\!f(b)] \rightarrow [\mathbb{c}nd(p,q) = \mathbb{c}nd(a,b) \rightarrow (p = a \wedge q = b)]$

(i) PA $\vdash [\mathbb{W}\!f\!f(\mathbb{c}nd(p,q)) \wedge \mathbb{W}\!f\!f(p)] \rightarrow \mathbb{W}\!f\!f(q)$

*(j) PA $\vdash \mathbb{A}xiompa(p) \rightarrow \mathbb{W}\!f\!f(p)$

(k) PA $\vdash \mathbb{P}rvpa(p) \rightarrow \mathbb{W}\!f\!f(p)$

Hint: Reasoning for (g) is like T13.52f. Reasoning for (i) is like the final uniqueness part of T11.3; the result is straightforward, starting with (e) — though with $\overline{\ulcorner\rightarrow\urcorner} * q = \overline{\ulcorner\rightarrow\urcorner} * s$, for an application of T13.47l, you will need to worry about the case $q = \emptyset$. Beginning with T13.40, (j) and (k) are not hard.

In the following we shall assume results like (j) - (k) for theories extending PA — though, of course, our prime example just *is* PA. Insofar as theories are recursively defined, some such results should be in the offing.

*E13.28. Show (e) and (j) from T13.41. Hard core: show each of the results from T13.41.

*E13.29. Show (d) and (e) from T13.42. Hard core: show each of the results from T13.42.

*E13.30. Show (k) and (l) from T13.43. Hard core: show each of the results from T13.43.

*E13.31. Show (c) and (f) from T13.44. Hard core: show each of the results from T13.44.

*E13.32. Show (f) and (l) from T13.45. Hard core: show each of the results from T13.45.

*E13.33. Show (a) and (b) from T13.46. Hard core: show each of the results from T13.46.

*E13.34. Show (b) and (e) from T13.47. Hard core: show each of the results from T13.47.

*E13.35. Show (j) and the unfinished cases for the C disjunct in (l) and (n). Hard core: show each of the results from T13.48.

E13.36. Work (g) from T13.49 including at least the A and B cases. Hard core: show each of the results from T13.49.

*E13.37. Work the K and M cases from T13.50l. Hard core: show each of the results from T13.50.

E13.38. Work j from T13.51 including at least the O case. Hard core: show each of the results from T13.51.

*E13.39. Work the case marked "similarly" on line 115 of T13.52a and the D case from T13.52f. Hard core: show each of the results from T13.52.

*E13.40. Show (g) including at least the A case, and (k) from T13.53. Hard core: show each of the results from T13.53.

13.4.2 The result

After all our preparation, we are ready to turn to the second condition, that PA $\vdash \Box(\mathcal{P} \to \mathcal{Q}) \to (\Box\mathcal{P} \to \Box\mathcal{Q})$. Again, given both $\Box(\mathcal{P} \to \mathcal{Q})$ and $\Box\mathcal{P}$ the idea is that there are j and k such that $\textsf{PRFT}(\mathsf{j}, \overline{\ulcorner \mathcal{P} \to \mathcal{Q} \urcorner})$ and $\textsf{PRFT}(\mathsf{k}, \overline{\ulcorner \mathcal{P} \urcorner})$ so that $\mathsf{l} = \mathsf{j} \star \mathsf{k} \star 2^{\ulcorner \mathcal{Q} \urcorner}$ numbers a proof of $\mathcal{Q}$. As it turns out, it will be convenient to have the result in a form with free variables, PA $\vdash Prvt(\mathit{cnd}(p, q)) \to (Prvt(p) \to Prvt(q))$; the second condition then follows as an immediate corollary.

Observe that we have on the table expressions of the sort, $+$, *Plus* and *plus* — where the first is a primitive symbol of $\mathcal{L}_{NT}$, the second the original relation to capture the recursive function plus, and the last a function symbol defined from the recursive function. In view of demonstrated equivalences, we will tend to slide between them without notice. So, for example, given that $\langle\langle 2, 2\rangle, 4\rangle \in$ plus, by capture PA $\vdash Plus(\overline{2}, \overline{2}, \overline{4})$; and by demonstrated equivalences, PA $\vdash \overline{2} + \overline{2} = \overline{4}$ and PA $\vdash \mathit{plus}(\overline{2}, \overline{2}) = \overline{4}$.

*T13.54. PA $\vdash$ $Prvt(\mathit{cnd}(p, q)) \rightarrow (Prvt(p) \rightarrow Prvt(q))$. Corollary: PA $\vdash \Box(\mathcal{P} \rightarrow \mathcal{Q}) \rightarrow (\Box\mathcal{P} \rightarrow \Box\mathcal{Q})$.

1.	$\mathbb{P}rvt(\mathbb{c}nd(p,q))$	A (g →I)
2.	$\mathbb{W}f\!f(\mathbb{c}nd(p,q))$	1 T13.53k
3.	$\mathbb{P}rvt(p)$	A (g →I)
4.	$\mathbb{W}f\!f(p)$	3 T13.53k
5.	$\mathbb{W}f\!f(q)$	2,4 T13.53i
6.	$\mathbb{I}con(\mathbb{c}nd(p,q),p,q)$	T13.40c,e
7.	$\exists v\,\mathbb{P}r\!ft(v,\mathbb{c}nd(p,q))$	1 abv
8.	$\exists v\,\mathbb{P}r\!ft(v,p)$	3 abv
9.	$\mathbb{P}r\!ft(j,\mathbb{c}nd(p,q))$	A (g 7∃E)
10.	$\mathbb{P}r\!ft(k,p)$	A (g 8∃E)
11.	$l = j * k * \overline{2}^q$	def
12.	$\mathbb{e}xp(j,\mathbb{l}en(j) \dot{-} \overline{1}) = \mathbb{c}nd(p,q)$	9 T13.40f
13.	$\mathbb{e}xp(k,\mathbb{l}en(k) \dot{-} \overline{1}) = p$	10 T13.40f
14.	$\mathbb{e}xp(l,\mathbb{l}en(j) + \mathbb{l}en(k)) = q$	11 T13.47c,f
15[a]	$\mathbb{I}con[\mathbb{e}xp(j,\mathbb{l}en(j) \dot{-} \overline{1}),\mathbb{e}xp(k,\mathbb{l}en(k) \dot{-} \overline{1}),\mathbb{e}xp(l,\mathbb{l}en(j) + \mathbb{l}en(k))]$	6,12,13,14 =E
16.	$(\forall i < \mathbb{l}en(j))[\mathbb{e}xp(l,i) = \mathbb{e}xp(j,i)]$	11 T13.47c
17.	$(\forall i < \mathbb{l}en(k))[\mathbb{e}xp(l,\mathbb{l}en(j) + i) = \mathbb{e}xp(k,i)]$	11 T13.47c
18.	$\mathbb{e}xp(l,\mathbb{l}en(j) \dot{-} \overline{1}) = \mathbb{e}xp(j,\mathbb{l}en(j) \dot{-} \overline{1})$	16 T13.45h (∀E)
19.	$\mathbb{e}xp(l,\mathbb{l}en(j) + \mathbb{l}en(k) \dot{-} \overline{1}) = \mathbb{e}xp(k,\mathbb{l}en(k) \dot{-} \overline{1})$	17 T13.45h (∀E)
20[b]	$Icon[\mathbb{e}xp(l,\mathbb{l}en(j) \dot{-} \overline{1}),\mathbb{e}xp(l,\mathbb{l}en(j) + \mathbb{l}en(k) \dot{-} \overline{1}),\mathbb{e}xp(l,\mathbb{l}en(j) + \mathbb{l}en(k))]$	15,18,19 =E
21.	$(\forall i < \mathbb{l}en(j))[\mathbb{A}xiom(\mathbb{e}xp(l,i)) \vee (\exists m < i)(\exists n < i)Icon(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,i))]$	9,16 T13.40f
22.	$(\forall i < \mathbb{l}en(k))[\mathbb{A}xiom(\mathbb{e}xp(l,\mathbb{l}en(j)+i)) \vee$ $(\exists m < i)(\exists n < i)\mathbb{I}con(\mathbb{e}xp(l,\mathbb{l}en(j)+m),\mathbb{e}xp(l,\mathbb{l}en(j)+n),\mathbb{e}xp(l,\mathbb{l}en(j)+i))]$	10,17 T13.40f
23[c]	$(\forall i : \mathbb{l}en(j) \le i < \mathbb{l}en(j) + \mathbb{l}en(k))[\mathbb{A}xiom(\mathbb{e}xp(l,i)) \vee$ $(\exists m < i)(\exists n < i)\mathbb{I}con(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,i))]$	from 22
24.	$x < \mathbb{l}en(l)$	A (g (∀I))
25.	$x < \mathbb{l}en(j) \vee \mathbb{l}en(j) \le x < \mathbb{l}en(j) + \mathbb{l}en(k) \vee x = \mathbb{l}en(j) + \mathbb{l}en(k)$	11,24 T13.47f
26.	$x < \mathbb{l}en(j)$	A (g 25∨E)
27.	$\mathbb{A}xiom(\mathbb{e}xp(l,x)) \vee (\exists m < x)(\exists n < x)\mathbb{I}con(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,x))$	21,26 (∀E)
28.	$\mathbb{l}en(j) \le x < \mathbb{l}en(j) + \mathbb{l}en(k)$	A (g 25∨E)
29.	$\mathbb{A}xiom(\mathbb{e}xp(l,x)) \vee (\exists m < x)(\exists n < x)\mathbb{I}con(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,x))$	23,28 (∀E)
30.	$x = \mathbb{l}en(j) + \mathbb{l}en(k)$	A (g 25∨E)
31.	$(\exists m < x)(\exists n < x)\mathbb{I}con(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,x))$	20,30
32.	$\mathbb{A}xiom(\mathbb{e}xp(l,x)) \vee (\exists m < x)(\exists n < x)\mathbb{I}con(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,x))$	31 ∨I
33.	$\mathbb{A}xiom(\mathbb{e}xp(l,x)) \vee (\exists m < x)(\exists n < x)\mathbb{I}con(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,x))$	25,26-31 ∨E
34[d]	$(\forall x < \mathbb{l}en(l))[\mathbb{A}xiom(\mathbb{e}xp(l,x)) \vee (\exists m < x)(\exists n < x)\mathbb{I}con(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,x))]$	24-33 (∀I)
35.	$q > \emptyset$	5 T13.49e
36.	$\mathbb{l}en(\overline{2}^q) = \overline{1}$	35 T13.45k
37.	$\mathbb{l}en(l) \ge \overline{1}$	11,36 T13.47f
38.	$l > \overline{1}$	37 T13.45g
39.	$\mathbb{e}xp(l,\mathbb{l}en(l) \dot{-} \overline{1}) = q$	14 T13.47f
40.	$\mathbb{e}xp(l,\mathbb{l}en(l) \dot{-} \overline{1}) = q \wedge l > \overline{1} \wedge$ $(\forall x < \mathbb{l}en(l))[\mathbb{A}xiom(\mathbb{e}xp(l,x)) \vee (\exists m < x)(\exists n < x)\mathbb{I}con(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,x))]$	39,38,34 ∧I
41.	$\mathbb{P}r\!ft(l,q)$	40 T13.40f
42.	$\mathbb{P}rvt(q)$	41 ∃I
43.	$\mathbb{P}rvt(q)$	8,10-42 ∃E
44.	$\mathbb{P}rvt(q)$	7,9-43 ∃E
45.	$\mathbb{P}rvt(p) \to \mathbb{P}rvt(q)$	3-44 →I
46[e]	$\mathbb{P}rvt(\mathbb{c}nd(p,q)) \to [\mathbb{P}rvt(p) \to \mathbb{P}rvt(q)]$	1-45 →I

This derivation is long, and skips steps; but it should be enough for you to see how the argument works — and to fill in the details if you choose. First, at (a), under assumptions for $\rightarrow$I, there are derivations numbered j, k and a longer sequence numbered l. And the the last member of this longer sequence is an immediate consequence of last members from the derivations numbered j and k. At (b) the results from (12) are all applied to the sequence numbered l; so the last sentence in the longer sequence is an immediate consequence of its earlier members. At (c), the different fragments of the longer sequence have the character of a proof. And at (d), the whole sequence numbered l has the character of a proof. Finally, at (e) we observe that this longer sequence yields $\mathbb{P}rvt(q)$ and discharge the assumptions for the result that $\mathbb{P}rvt(\mathbb{c}nd(p,q)) \rightarrow [\mathbb{P}rvt(p) \rightarrow \mathbb{P}rvt(q)]$ so that with T13.34 PA $\vdash Prvt(\mathbb{c}nd(p,q)) \rightarrow (Prvt(p) \rightarrow Prvt(q))$.

But then we have $Prvt(\mathbb{c}nd(\overline{\ulcorner \mathcal{P} \urcorner}, \overline{\ulcorner \mathcal{Q} \urcorner})) \rightarrow [Prvt(\overline{\ulcorner \mathcal{P} \urcorner}) \rightarrow Prvt(\overline{\ulcorner \mathcal{Q} \urcorner})]$ as an instance, and by capture, $Prvt(\overline{\ulcorner \mathcal{P} \rightarrow \mathcal{Q} \urcorner}) \rightarrow [Prvt(\overline{\ulcorner \mathcal{P} \urcorner}) \rightarrow Prvt(\overline{\ulcorner \mathcal{Q} \urcorner})]$ so that PA $\vdash \Box(\mathcal{P} \rightarrow \mathcal{Q}) \rightarrow (\Box\mathcal{P} \rightarrow \Box\mathcal{Q})$. Thus the second derivability condition is established.

*E13.41. As a start to a complete demonstration of T13.54, provide a demonstration through part (c) that does not skip any steps. You may find it helpful to divide your demonstration into separate parts for (a), (b) and then for lines (21), (22) and (23). Hard core: complete the entire derivation.

13.5 The Third Condition: $\Box\mathcal{P} \rightarrow \Box\Box\mathcal{P}$

To show the third condition, that PA $\vdash \Box\mathcal{P} \rightarrow \Box\Box\mathcal{P}$, it is sufficient to show PA $\vdash \mathcal{Q} \rightarrow \Box\mathcal{Q}$. For when $\mathcal{Q}$ is $\Box\mathcal{P}$, the result is immediate. Further, $\Box\mathcal{P}$ is $Prvt(\overline{\ulcorner \mathcal{P} \urcorner})$ and $Prvt(\overline{\ulcorner \mathcal{P} \urcorner})$ is Σ_1. So it is sufficient to show that for any Σ_1 sentence $\mathcal{Q}$, PA $\vdash \mathcal{Q} \rightarrow \Box\mathcal{Q}$.

We begin with some additional applications. Then we focus what needs to be shown by an alternate characterization of Σ_1 formulas, along with some results about substitutions. Finally we will be in a position to show the third condition.

13.5.1 More applications

Recall that where $\mathsf{p} = \ulcorner \mathcal{P} \urcorner$, $\mathsf{v} = \ulcorner v \urcorner$, and $\mathsf{s} = \ulcorner s \urcorner$, $\mathsf{formsub}(\mathsf{p}, \mathsf{v}, \mathsf{s})$ returns the Gödel number of $\mathcal{P}^{v}_{s}$. In addition, $\mathsf{num}(\mathsf{n})$ returns the Gödel number of the standard

Second theorems of chapter 13

T13.21. For any friendly recursive function $\mathsf{r}(\vec{\mathsf{x}})$ and original formula $\mathcal{R}(\vec{x}, v)$ by which it is expressed and captured, PA defines a function $r(\vec{x})$ such that PA $\vdash v = r(\vec{x}) \leftrightarrow \mathcal{R}(\vec{x}, v)$. This theorem depends on conditions for the recursion clause and so on T13.22 and T13.31.

T13.22. Where $\mathcal{F}(\vec{x}, y, v)$ is the formula for recursion, PA $\vdash \forall m \forall n[(\mathcal{F}(\vec{x}, y, m) \wedge \mathcal{F}(\vec{x}, y, n)) \rightarrow m = n]$.

T13.23 - T13.26. T13.23 Results for $a \dot{-} b$. T13.24 results for $a|b$. T13.25 results for $Pr(a)$ and $Rp(a)$. T13.26 results for $lcm(a)$.

T13.27. PA $\vdash [(\forall i < k)(m(i) > \emptyset \wedge m(i) > h(i)) \wedge \forall i \forall j(i < j \wedge j < k \rightarrow Rp(Sm(i), Sm(j)))] \rightarrow \exists p(\forall i < k)rm(p, m(i)) = h(i)$ (*CRT*).

T13.28 - T13.30. T13.28 results for *maxp* and *maxs*. T13.29 PA $\vdash \exists p \exists q(\forall i < k)\beta(p, q, i) = h(i)$. T13.30 PA $\vdash \exists p \exists q[(\forall i < k)\beta(p, q, i) = \beta(r, s, i) \wedge \beta(p, q, k) = n]$.

T13.31. PA $\vdash \exists v \exists p \exists q[\beta(p, q, \emptyset) = g(\vec{x}) \wedge (\forall i < y)h(\vec{x}, i, \beta(p, q, i)) = \beta(p, q, Si) \wedge \beta(p, q, y) = v]$.

T13.32. For any friendly recursive relation $\mathsf{R}(\vec{\mathsf{x}})$ with characteristic function $\mathsf{ch_R}(\vec{\mathsf{x}})$, PA $\vdash \mathbb{R}(\vec{x}) \leftrightarrow ch_{\mathsf{R}}(\vec{x}) = \emptyset$. And for a recursive operator $\mathsf{OP}(\mathsf{P}_1(\vec{\mathsf{x}}) \ldots \mathsf{P}_n(\vec{\mathsf{x}}))$ with characteristic function $\mathsf{f}(\mathsf{ch}_{\mathsf{P}_1}(\vec{\mathsf{x}}) \ldots \mathsf{ch}_{\mathsf{P}_n}(\vec{\mathsf{x}}))$, PA $\vdash \mathbb{O}p(\mathbb{P}_1(\vec{x}) \ldots \mathbb{P}_n(\vec{x})) \leftrightarrow f(ch_{\mathsf{P}_1}(\vec{x}) \ldots ch_{\mathsf{P}_n}(\vec{x})) = \emptyset$. Corollary: where $\mathsf{R}(\vec{\mathsf{x}})$ is originally captured by $\mathcal{R}(\vec{x}, \emptyset)$, PA $\vdash \mathbb{R}(\vec{x}) \leftrightarrow \mathcal{R}(\vec{x}, \emptyset)$.

T13.33. Suppose $f(\vec{x}, y)$ is defined by $g(\vec{x})$ and $h(\vec{x}, y, u)$ so that PA $\vdash v = f(\vec{x}, y) \leftrightarrow \mathcal{F}(\vec{x}, y, v)$; then, (i) $f(\vec{x}, \emptyset) = g(\vec{x})$ and (ii) $f(\vec{x}, S(y)) = h(\vec{x}, y, f(\vec{x}, y))$.

T13.34. (a) For any friendly recursive function $\mathsf{r}(\vec{\mathsf{x}})$ and original formula $\mathcal{R}(\vec{x}, v)$ by which it is expressed and captured, PA defines a coordinate function $r(\vec{x})$ such that PA $\vdash v = r(\vec{x}) \leftrightarrow \mathcal{R}(\vec{x}, v)$. And (b) for any friendly recursive relation $\mathsf{R}(\vec{\mathsf{x}})$ with characteristic function $\mathsf{ch_R}(\vec{\mathsf{x}})$, PA defines a coordinate relation $\mathbb{R}(\vec{x})$ such that PA $\vdash \mathbb{R}(\vec{x}) \leftrightarrow ch_{\mathsf{R}}(\vec{x}) = \emptyset$.

T13.35 - T13.37. T13.35 equivalences for *suc*, *zero*, $idnt^j_k$, *plus* and *times*. T13.36 results for *pred*, *sg* and *csg*. T13.37 Equivalences for *pred*, *subc*, *absval*, *sg*, *csg*, *Eq*, *Leq*, *Less*, *Neg*, and *Dsj*.

T13.38. PA proves a characteristic function takes the value $\emptyset$ or $\overline{1}$.

T13.39. Equivalences for $(\exists y \leq z)$, $(\exists y < z)$, $(\forall y \leq z)$, $(\forall y < z)$, $(\mu y \leq z)$, *Fctr*, and *Prime*.

T13.40 - T13.44. T13.40 first applications to recursive functions. T13.41 Results for m^a. T13.42 results for *fact*. T13.43 results for *pi*. T13.44 results for *exp*.

T13.45 - T13.51. T13.45 results for *len*. T13.46 results for *val*. T13.47 results for $m * n$. T13.48 results for *Termseq*. T13.49 results for *Formseq*. T13.50 results for *Tsubseq*. T13.51 results for *Fsubseq*.

T13.52 - T13.53. T13.52 on unique readability. T13.53 results for *Wff* and *Prvpa*.

T13.54. PA $\vdash \Box(\mathcal{P} \rightarrow \mathcal{Q}) \rightarrow (\Box\mathcal{P} \rightarrow \Box\mathcal{Q})$. — D2 numeral for n, and gvar(n) is the Gödel number of variable x_n. So formsub(p, gvar(n), num(y)) is a function which returns the number of the formula that substitutes a numeral for the value (number) assigned to y into the place of x_n. So, for example, if y is assigned the value of 2, then formsub(p, gvar(n), num(y)) returns $\ulcorner \mathcal{P}^{x_n}_{\overline{2}} \urcorner$. And PA defines $\mathbb{f}ormsub(p, \mathbb{g}var(n), \mathbb{n}um(y))$. We require some results for these notions.

First, a pair of theorems with some results for substitutions into terms and then formulas.

T13.55. The following are theorems of PA.

(a) PA $\vdash \mathbb{F}ree_t(t, v) \leftrightarrow \sim\mathbb{T}ermsub(t, v, v \times \overline{4}, t)$

(b) PA $\vdash \mathbb{V}ar(v) \rightarrow \mathbb{T}erm(v \times \overline{4}) \wedge v \times \overline{4} \neq v$

(c) PA $\vdash \mathbb{e}xp(m, k) = \overline{\ulcorner \emptyset \urcorner} \rightarrow \sim[J(v, m, n, k) \vee K(v, s, m, n, k) \vee L(m, n, k) \vee M(m, n, k) \vee N(m, n, k)]$

(d) PA $\vdash [\mathbb{V}ar(\mathbb{e}xp(m, k)) \wedge \mathbb{e}xp(m, k) \neq v] \rightarrow \sim[I(m, n, k) \vee K(v, s, m, n, k) \vee L(m, n, k) \vee M(m, n, k) \vee N(m, n, k)]$

(e) PA $\vdash [\mathbb{V}ar(\mathbb{e}xp(m, k)) \wedge \mathbb{e}xp(m, k) = v] \rightarrow \sim[I(m, n, k) \vee J(v, m, n, k) \vee L(m, n, k) \vee M(m, n, k) \vee N(m, n, k)]$

(f) PA $\vdash \mathbb{e}xp(m, k) = \overline{\ulcorner S \urcorner} * a \rightarrow \sim[I(m, n, k) \vee J(v, m, n, k) \vee K(v, s, m, n, k) \vee M(m, n, k) \vee N(m, n, k)]$

(g) PA $\vdash \mathbb{e}xp(m, k) = \overline{\ulcorner + \urcorner} * a \rightarrow \sim[I(m, n, k) \vee J(v, m, n, k) \vee K(v, s, m, n, k) \vee L(m, n, k) \vee N(m, n, k)]$

(h) PA $\vdash \mathbb{e}xp(m, k) = \overline{\ulcorner \times \urcorner} * a \rightarrow \sim[I(m, n, k) \vee J(v, m, n, k) \vee K(v, s, m, n, k) \vee L(m, n, k) \vee M(m, n, k)]$

*(i) PA $\vdash [\mathbb{T}ermsub(t, v, s, q) \wedge \mathbb{T}ermsub(t, v, s, r)] \rightarrow q = r$

(j) PA $\vdash [\mathbb{A}tomsub(p, v, s, q) \wedge \mathbb{A}tomsub(p, v, s, r)] \rightarrow q = r$

(k) PA $\vdash [\mathbb{T}erm(t) \wedge \mathbb{T}erm(s)] \rightarrow [\sim\mathbb{F}ree_t(t, v) \rightarrow \mathbb{T}ermsub(t, v, s, t)]$

(l) PA $\vdash \mathbb{T}erm(s) \rightarrow [\mathbb{A}tomsub(p, v, v \times \overline{4}, p) \rightarrow \mathbb{A}tomsub(p, v, s, p)]$

(m) PA $\vdash [\mathbb{T}erm(t) \wedge \mathbb{V}ar(v)] \rightarrow [(\mathbb{F}ree_t(t, v) \wedge \mathbb{T}ermsub(t, v, s, u)) \rightarrow s \leq u]$

*(n) PA $\vdash \mathbb{V}ar(v) \rightarrow [(\sim\mathbb{A}tomsub(p, v, v\times\overline{4}, p)\wedge\mathbb{A}tomsub(p, v, s, q)) \rightarrow s \leq q]$

Hints: (i) Under assumptions for →I and (∃E) you have $\mathbb{T}subseq(m, n, t, v, s, q)$ and $\mathbb{T}subseq(m', n', t, v, s, r)$; with this show $\forall k[k < \mathbb{l}en(m) \rightarrow (\forall x < \mathbb{l}en(m'))(\mathbb{e}xp(m, k) = \mathbb{e}xp(m', x) \rightarrow \mathbb{e}xp(n, k) = \mathbb{e}xp(n', x))]$ by strong induction; the result follows easily from this. (k) Under assumptions for →I and then ∃E, you have both $\mathbb{T}subseq(m, n, t, v, v \times \overline{4}, t)$ and $\mathbb{T}subseq(m', n', t, v, s, u)$ with goal $t = u$; by strong induction show $\forall k[k < \mathbb{l}en(m) \rightarrow (\forall x < \mathbb{l}en(m'))(\mathbb{e}xp(m, k) = \mathbb{e}xp(m', k) \rightarrow (\mathbb{e}xp(m, k) = \mathbb{e}xp(n, k) \rightarrow \mathbb{e}xp(m', x) = \mathbb{e}xp(n', x)))]$; then the result follows easily. (m) Under assumptions for →I and ∃E you have $\mathbb{T}ermsub(m, n, t, v, v \times \overline{4}, r)$ and $\mathbb{T}ermsub(m', n', t, v, s, u)$ where $r \neq t$ with goal $s \leq u$; by strong induction show $\forall k(k < \mathbb{l}en(m) \rightarrow (\forall x < \mathbb{l}en(m'))[\mathbb{e}xp(m, k) = \mathbb{e}xp(m', x) \rightarrow (\mathbb{e}xp(m, k) \neq \mathbb{e}xp(n, k) \rightarrow s \leq \mathbb{e}xp(n'x))]$; the result follows.

T13.56. The following are theorems of PA.

(a) PA $\vdash \mathbb{F}ree_f(p, v) \leftrightarrow \sim\mathbb{F}ormsub(p, v, v \times \overline{4}, p)$

(b) PA $\vdash \mathbb{A}tomic(\mathbb{e}xp(m, k) \rightarrow \sim[P(m, n, k) \vee Q(m, n, k) \vee R(v, p, m, n, k) \vee S(v, p, m, n, k)]$

(c) PA $\vdash \mathbb{e}xp(m, k) = \overline{\ulcorner\sim\urcorner} * a \rightarrow \sim[O(v, s, m, n, k) \vee Q(m, n, k) \vee R(v, p, m, n, k) \vee S(v, p, m, n, k)]$

(d) PA $\vdash \mathbb{e}xp(m, k) = \overline{\ulcorner(\urcorner} * a \rightarrow \sim[O(v, s, m, n, k) \vee P(m, n, k) \vee R(v, p, m, n, k) \vee S(v, p, m, n, k)]$

(e) PA $\vdash [\mathbb{V}ar(j) \wedge \mathbb{e}xp(m, k) = \overline{\ulcorner\forall\urcorner} * j * a \wedge j \neq v] \rightarrow \sim[O(v, s, m, n, k) \vee P(m, n, k) \vee Q(m, n, k) \vee S(v, p, m, n, k)]$

(f) PA $\vdash [\mathbb{V}ar(j) \wedge \mathbb{e}xp(m, k) = \overline{\ulcorner\forall\urcorner} * j * a \wedge j = v] \rightarrow \sim[O(v, s, m, n, k) \vee P(m, n, k) \vee Q(m, n, k) \vee R(v, p, m, n, k)]$

(g) PA $\vdash [\mathbb{F}ormsub(p, v, s, q) \wedge \mathbb{F}ormsub(p, v, s, r)] \rightarrow q = r$

(h) PA $\vdash [\mathbb{W}ff(p) \wedge \mathbb{T}erm(s)] \rightarrow [\mathbb{F}ormsub(p, v, s, q) \rightarrow formusb(p, v, s) = q]$

(i) PA $\vdash [\mathbb{W}ff(p) \wedge \mathbb{T}erm(s)] \rightarrow [\sim\mathbb{F}ree_f(p, v) \rightarrow formsub(p, v, s) = p]$

corollary: If x is not free in $\mathcal{P}$, then PA $\vdash formsub(\overline{\ulcorner\mathcal{P}\urcorner}, \overline{\ulcorner x\urcorner}, y) = \overline{\ulcorner\mathcal{P}\urcorner}$

(j) PA $\vdash [\mathbb{W}\!f\!f(p) \wedge \mathbb{T}erm(s) \wedge \mathbb{V}ar(v)] \rightarrow [\mathbb{F}ree_f(p, v) \rightarrow s \leq \mathbb{f}ormsub(p, v, s)]$

Hint: See the corresponding members of T13.55.

We are now positioned for some results related to Gen and A4. Let gvar(n) $=_{\text{def}}$ 2^{23+2n} be the Gödel number of variable x_n, and *numseq*(n) be as follows.

PA $\vdash numseq(\emptyset) = \mathbb{pi}(\emptyset)^{\mathbb{num}(\emptyset)}$
PA $\vdash numseq(Sy) = numseq(y) \times \mathbb{pi}(Sy)^{\mathbb{num}(Sy)}$

We shall be able to show that *numseq*(n) numbers a term sequence for $\mathbb{num}(n)$. In addition let,

$$
\begin{array}{lcl}
T(m,k) & = & \mathbb{A}tomic(\mathbb{e}xp(m,k)) \\
U(m,k) & = & (\exists j < k)[\mathbb{e}xp(m,k) = \mathbb{neg}(\mathbb{e}xp(m,j))] \\
V(m,k) & = & (\exists i < k)(\exists j < k)[\mathbb{e}xp(m,k) = \mathbb{cnd}(\mathbb{e}xp(m,i), \mathbb{e}xp(m,j))] \\
W(u,v,m,k) & = & (\exists p \leq u)[\mathbb{W}\!f\!f(p) \wedge \mathbb{e}xp(m,k) = \mathbb{unv}(v,p)] \\
X(u,v,s,m,k) & = & (\exists i < k)(\exists j \leq u)[\mathbb{V}ar(j) \wedge j \neq v \wedge (\sim\mathbb{F}ree_t(s,j) \vee \sim\mathbb{F}ree_f(\mathbb{e}xp(m,i),v)) \wedge \\
& & \quad \mathbb{e}xp(m,k) = \mathbb{unv}(j, \mathbb{e}xp(m,i))]
\end{array}
$$

T13.57. The following are theorems of PA.

(a) PA $\vdash \mathbb{F}fseq(m,s,v,u) \leftrightarrow [\mathbb{e}xp(m, \mathbb{l}en(m) \mathbin{\dot{-}} 1) = u \wedge m > \overline{1} \wedge (\forall k < \mathbb{l}en(m))(T(m,k) \vee U(m,k) \vee V(m,k) \vee W(u,v,m,k) \vee X(u,v,s,m,k))]$

(b) (i) PA $\vdash \mathbb{F}reefor(s,v,u) \leftrightarrow (\exists x \leq B_u)\mathbb{F}fseq(x,s,v,u)$

(ii) PA $\vdash B_u = [\mathbb{pi}(\mathbb{l}en(u))^u]^{\mathbb{l}en(u)}$

(c) PA $\vdash \mathbb{A}xiomad4(n) \leftrightarrow (\exists p \leq n)(\exists v \leq n)\{\mathbb{W}\!f\!f(p) \wedge \mathbb{V}ar(v) \wedge [$

$(\sim\mathbb{F}ree_f(v,p) \wedge n = \mathbb{cnd}(\mathbb{unv}(v,p),p)) \vee$

$(\exists s \leq n)(\mathbb{F}ree_f(v,p) \wedge \mathbb{T}erm(s) \wedge \mathbb{F}reefor(s,v,p) \wedge n = \mathbb{cnd}(\mathbb{unv}(v,p), \mathbb{f}ormsub(p,v,s))]\}$

(d) (i) PA $\vdash \mathbb{num}(\emptyset) = \overline{\ulcorner \emptyset \urcorner}$

(ii) PA $\vdash \mathbb{num}(Sy) = \overline{\ulcorner S \urcorner} * \mathbb{num}(y)$

(e) PA $\vdash \mathbb{g}var(n) = \overline{2}^{\overline{23}+\overline{2}\times n}$

(f) PA $\vdash \mathbb{V}ar(\mathbb{g}var(n))$

(g) PA $\vdash \mathbb{g}var(m) = \mathbb{g}var(n) \rightarrow m = n$

*(h) PA $\vdash [\mathbb{P}rvt(p) \wedge \mathbb{V}ar(v)] \rightarrow \mathbb{P}rvt(\mathbb{unv}(v,p))$

(i) PA $\vdash \mathbb{A}xiom(n) \rightarrow \mathbb{P}rvt(n)$

*(j) PA $\vdash [\mathbb{W}\!f\!f(p) \wedge \mathbb{V}ar(v)] \rightarrow \mathbb{F}reefor(v, v, p)$

*(k) PA $\vdash \mathbb{A}xiomad4(n) \leftrightarrow \exists s(\exists p \leq n)(\exists v \leq n)[\mathbb{W}\!f\!f(p) \wedge \mathbb{V}ar(v) \wedge$
$\mathbb{T}erm(s) \wedge \mathbb{F}reefor(s, v, p) \wedge n = cnd(unv(v, p), formsub(p, v, s))]$

(l) PA $\vdash num(x) > \emptyset$

(m) PA $\vdash numseq(x) > \overline{1}$

(n) PA $\vdash len(num(x)) = Sx$

*(o) PA $\vdash len(numseq(x)) = Sx$

(p) PA $\vdash \forall y[y \leq x \rightarrow exp(numseq(x), y) = num(y)]$

(q) PA $\vdash \mathbb{V}ar(v) \rightarrow v \neq num(y)$

(r) PA $\vdash \mathbb{T}ermseq(numseq(x), num(x))$
corollary: PA $\vdash \mathbb{T}erm(num(x))$

(s) PA $\vdash \mathbb{T}ermsub(num(n), v, s, num(n))$
corollary: PA $\vdash \sim\mathbb{F}ree_t(num(n), v)$

*(t) PA $\vdash [\mathbb{W}\!f\!f(p) \wedge \mathbb{V}ar(v)] \rightarrow \mathbb{F}reefor(num(x), v, p)$

(u) PA $\vdash \mathbb{W}\!f\!f(p) \rightarrow Prvt(cnd(unv(gvar(n), p), formsub(p, gvar(n), num(x))))$

Hint: (p) is by induction on the value of x. For (q) it may help to think about the length of v and $num(y)$. For (r) to show the bounded quantification for $\mathbb{T}ermseq(numseq(x), num(x))$ you assume $j < len(numseq(x))$; then $j = \emptyset \vee j > \emptyset$ and the cases are easy. (s) again, in the argument for the bounded quantifier, $j = \emptyset \vee j > \emptyset$.

Effectively, (h) is like Gen. (k) is like the intuitive version of A4 from p. 605. And (u) results with A4 when the substituted term is a numeral (so that associated restrictions are automatically met).

Finally, a theorem with results first for substitution into a conditional, and then for substitution into other substitutions. The latter include matched results for $\mathbb{T}ermsub$, $\mathbb{A}tomsub$ and then $\mathbb{F}ormsub$. Suppose $x = x_i$ and $y = x_j$.

T13.58. The following are theorems of PA.

(a) PA $\vdash [\mathbb{W}\!ff(p) \wedge \mathbb{W}\!ff(q) \wedge \mathbb{T}erm(s)] \rightarrow \mathit{formsub}(\mathbb{c}nd(p,q),v,s) =$
$\mathbb{c}nd(\mathit{formsub}(p,v,s), \mathit{formsub}(q,v,s))$

*(b) PA $\vdash [\mathbb{T}erm(p) \wedge v \neq w] \rightarrow \exists q \exists t \exists t'[\mathbb{T}ermsub(p,v,\mathbb{n}um(y),t) \wedge$
$\mathbb{T}ermsub(p,w,\mathbb{n}um(z),t') \wedge \mathbb{T}ermsub(t,w,\mathbb{n}um(z),q) \wedge \mathbb{T}ermsub(t',v,\mathbb{n}um(y),q)]$

(c) PA $\vdash [\mathbb{A}tomic(p) \wedge v \neq w] \rightarrow \exists q \exists t \exists t'[\mathbb{A}tomsub(p,v,\mathbb{n}um(y),t) \wedge \mathbb{A}tomsub(p,w,\mathbb{n}um(z),t') \wedge$
$\mathbb{A}tomsub(t,w,\mathbb{n}um(z),q) \wedge \mathbb{A}tomsub(t',v,\mathbb{n}um(y),q)]$

*(d) PA $\vdash [\mathbb{W}\!ff(p) \wedge v \neq w] \rightarrow \mathit{formsub}(\mathit{formsub}(p,v,\mathbb{n}um(y)),w,\mathbb{n}um(z)) =$
$\mathit{formsub}(\mathit{formsub}(p,w,\mathbb{n}um(z)),v,\mathbb{n}um(y))$

(e) PA $\vdash [\mathbb{T}erm(p) \wedge \mathbb{V}ar(w)] \rightarrow \exists q \exists t \exists t'[\mathbb{T}ermsub(p,v,w,t) \wedge \mathbb{T}ermsub(p,v,\mathbb{n}um(y),t') \wedge$
$\mathbb{T}ermsub(t,w,\mathbb{n}um(y),q) \wedge \mathbb{T}ermsub(t',w,\mathbb{n}um(y),q)]$

(f) PA $\vdash [\mathbb{A}tomic(p) \wedge \mathbb{V}ar(w)] \rightarrow \exists q \exists t \exists t'[\mathbb{A}tomsub(p,v,w,t) \wedge \mathbb{A}tomsub(p,v,\mathbb{n}um(y),t') \wedge$
$\mathbb{A}tomsub(t,w,\mathbb{n}um(y),q) \wedge \mathbb{A}tomsub(t',w,\mathbb{n}um(y),q)]$

(g) PA $\vdash [\mathbb{W}\!ff(p) \wedge \mathbb{V}ar(w)] \rightarrow \mathit{formsub}(\mathit{formsub}(p,v,w),w,\mathbb{n}um(y)) =$
$\mathit{formsub}(\mathit{formsub}(p,v,\mathbb{n}um(y)),w,\mathbb{n}um(y))$

(h) PA $\vdash [\mathbb{T}erm(p) \wedge \mathbb{V}ar(w)] \rightarrow \exists q \exists t \exists t'[\mathbb{T}ermsub(p,v,\overline{\ulcorner S \urcorner} * w,t) \wedge$
$\mathbb{T}ermsub(p,v,\mathbb{n}um(Sy),t') \wedge \mathbb{T}ermsub(t,w,\mathbb{n}um(y),q) \wedge \mathbb{T}ermsub(t',w,\mathbb{n}um(y),q)]$

(i) PA $\vdash [\mathbb{A}tomic(p) \wedge \mathbb{V}ar(w)] \rightarrow \exists q \exists t \exists t'[\mathbb{A}tomsub(p,v,\overline{\ulcorner S \urcorner} * w,t)$
$\wedge\, \mathbb{A}tomsub(p,v,\mathbb{n}um(Sy),t') \wedge \mathbb{A}tomsub(t,w,\mathbb{n}um(y),q) \wedge \mathbb{A}tomsub(t',w,\mathbb{n}um(y),q)]$

(j) PA $\vdash [\mathbb{W}\!ff(p) \wedge \mathbb{V}ar(w)] \rightarrow \mathit{formsub}(\mathit{formsub}(p,v,\overline{\ulcorner S \urcorner} * w),w,\mathbb{n}um(y))$
$= \mathit{formsub}(\mathit{formsub}(p,v,\mathbb{n}um(Sy)),w,\mathbb{n}um(y))$.

Hints: (b) Let $\mathcal{P} = \exists q \exists a \exists b \exists c \exists d[\mathbb{T}subseq(a,b,\mathbb{e}xp(n,k),w,\mathbb{n}um(z),q) \wedge \mathbb{T}subseq(c,d,\mathbb{e}xp(n',k'),v,$ $\mathbb{n}um(y),q)]$; show $\forall x(\forall k < \mathbb{l}en(m))(\forall k' < \mathbb{l}en(m'))[\mathbb{l}en(\mathbb{e}xp(m,k)) \leq x \rightarrow (\mathbb{e}xp(m,k) = \mathbb{e}xp(m',k') \rightarrow$ $\mathcal{P})]$ by IN; the result follows. (c) Under the assumption for $\rightarrow$I, apply T13.49c and then (b). For (e) let $\mathcal{P} = \exists q \exists a \exists b \exists c \exists d[\mathbb{T}subseq(a,b,\mathbb{e}xp(n,k),w,\mathbb{n}um(y),q) \wedge \mathbb{T}subseq(c,d,$ $\mathbb{e}xp(n',k'),w,\mathbb{n}um(y),q)]$; show $\forall x(\forall k < \mathbb{l}en(m))(\forall k' < \mathbb{l}en(m'))[\mathbb{l}en(\mathbb{e}xp(m,k)) \leq x \rightarrow (\mathbb{e}xp(m,k) =$ $\mathbb{e}xp(m',k') \rightarrow \mathcal{P})]$ by IN.

Speaking loosely: From (a), $(\mathcal{P} \to \mathcal{Q})^v_s = \mathcal{P}^v_s \to \mathcal{Q}^v_s$. From theorems leading up to (d), if $v \neq w$ then $(\mathcal{P}^v_{num(y)})^w_{num(z)} = (\mathcal{P}^w_{num(z)})^v_{num(y)}$. From ones leading to (g), $(\mathcal{P}^v_w)^w_{num(y)} = (\mathcal{P}^v_{num(y)})^w_{num(y)}$. And from ones leading to (j), $(\mathcal{P}^v_{Sw})^w_{num(y)} = (\mathcal{P}^v_{num(Sy)})^w_{num(y)}$. For these is important that $num(y)$ is a numeral and so has no variables to be replaced. Arguments combine methods we have seen before; reasoning is straightforward but long.

*E13.42. Set up the argument for T13.55k including assertion of the main proposition to be shown by induction; then set up the show part working just the L case. Hard core: finish T13.55k and the rest of the results in T13.55.

*E13.43. Set up the argument for T13.56i including assertion of the main proposition to be shown by induction; then set up the show part working just the P case. Hard core: finish T13.56c and the rest of the results in T13.56.

*E13.44. Show (s) and (u) from T13.57. Hard core: show the rest of the results from T13.57.

*E13.45. Show T13.58a; then set up the argument for T13.58g including assertion of the main proposition to be shown by induction; then set up the show part working just the P case. Hard core: finish T13.58g and the rest of the results in T13.58.

13.5.2 Sigma star.

Our aim is to show PA $\vdash \mathcal{Q} \to \Box\mathcal{Q}$ for any Σ_1 sentence $\mathcal{Q}$. Given our minimal resources, the task is simplified if we can give a minimal specification of the Σ_1 formulas themselves. Toward this end, we introduce a special class of formulas, the $\Sigma^\star$ formulas; and show that every Σ_1 formula is a $\Sigma^\star$ formula. $\Sigma^\star$ formulas are as follows.

($\Sigma^\star$) For any variables x, y and z,

- (a) $\emptyset = z$, $y = z$, $Sy = z$, $x + y = z$ and $x \times y = z$ are *strictly* $\Sigma^\star$.
- (s) If $\mathcal{P}$ and $\mathcal{Q}$ are strictly $\Sigma^\star$, then so are $(\mathcal{P} \vee \mathcal{Q})$, and $(\mathcal{P} \wedge \mathcal{Q})$.
- (∀) If $\mathcal{P}$ is strictly $\Sigma^\star$, then so is $(\forall x \leq y)\mathcal{P}$ where y does not occur in $\mathcal{P}$.

($\exists$) If $\mathcal{P}$ is strictly $\Sigma^\star$, then so is $\exists x \mathcal{P}$.

(c) Nothing else is strictly $\Sigma^\star$.

A formula is $\Sigma^\star$ iff it is equivalent to a strictly $\Sigma^\star$ formula.

Given that the existential quantifier comes to the front (as for T12.10), it is perhaps obvious that every $\Sigma^\star$ formula is Σ_1. At any rate, we aim to show the other direction: that every Σ_1 formula is provably equivalent a $\Sigma^\star$ formula. Then results which apply to all the $\Sigma^\star$ formulas immediately transfer to the Σ_1 formulas. We begin showing that there are $\Sigma^\star$ formulas equivalent to atomic equalities of the sort $t = x$. Then (depending on an extended notion of *normal* form and a result result according to which Δ_0 formulas always have equivalent normal forms) we show that there are $\Sigma^\star$ formulas equivalent to Δ_0 formulas. From this it is a short step to the result that there are $\Sigma^\star$ formulas equivalent to all the Σ_1 formulas. First, then, the result for atomic equalities,

T13.59. For any $\mathcal{P}$ of the form $t = x$, there is a $\Sigma^\star$ formula $\mathcal{P}^\star$ such that PA $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^\star$.

By induction on the function symbols in t.

Basis: If t has no function symbols, then it is the constant $\emptyset$ or a variable y, so $\mathcal{P}$ is of the form $\emptyset = x$ or $y = x$; but these are already $\Sigma^\star$ formulas. So let $\mathcal{P}^\star$ be the same as $\mathcal{P}$. Then PA $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^\star$.

Assp: For any i, $0 \leq i < k$, if t has i function symbols, there is a $\mathcal{P}^\star$ such that PA $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^\star$.

Show: If t has k function symbols, there is a $\mathcal{P}^\star$ such that PA $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^\star$.

If t has k function symbols, then it is of the form Sr, $r + s$ or $r \times s$ for r and s with $< k$ function symbols.

(S) t is Sr, so that $\mathcal{P}$ is $Sr = x$. Set $\mathcal{P}^\star = \exists z[(r = z)^\star \wedge Sz = x]$; then by assumption, PA $\vdash r = z \leftrightarrow (r = z)^\star$. So reason as follows,

1.	$r = z \leftrightarrow (r = z)^{\star}$	assp
2.	$\quad Sr = x$	A (g $\leftrightarrow$I)
3.	$\quad r = r \wedge Sr = x$	from 2
4.	$\quad \exists z[r = z \wedge Sz = x]$	3 $\exists$I
5.	$\quad \exists z[(r = z)^{\star} \wedge Sz = x]$	1,4 with T9.9
6.	$\quad \exists z[(r = z)^{\star} \wedge Sz = x]$	A (g $\leftrightarrow$I)
7.	$\quad\quad (r = z)^{\star} \wedge Sz = x$	A (g 6$\exists$E)
8.	$\quad\quad r = z$	1,7 $\leftrightarrow$E
9.	$\quad\quad Sr = x$	from 7,8
10.	$\quad Sr = x$	6,7-9 $\exists$E
11.	$Sr = x \leftrightarrow \exists z[(r = z)^{\star} \wedge Sz = x]$	2-5,6-10 $\leftrightarrow$I

So PA $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^{\star}$.

(+) $t = s + r$, so that $\mathcal{P}$ is $s + r = x$. Set $\mathcal{P}^{\star} = \exists u \exists v[(s = u)^{\star} \wedge (r = v)^{\star} \wedge u + v = x]$. Then PA $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^{\star}$.

($\times$) Similarly.

Indct: For any $\mathcal{P}$ of the form $t = x$, there is a $\mathcal{P}^{\star}$ such that PA $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^{\star}$.

Now generalize some operations from T8.1. There we said a formula is in *normal* form iff its only operators are $\vee$, $\wedge$, and $\sim$, and the only instances of $\sim$ are immediately prefixed to atomics. Now a formula is in (*extended*) *normal* form iff its only operators are $\vee$, $\wedge$, $\sim$, or a bounded quantifier, and the only instances of $\sim$ are immediately prefixed to atomics (which may include inequalities). Again, generalizing from before, where $\mathcal{P}$ is a normal form, let $\mathcal{P}'$ be like $\mathcal{P}$ except that $\vee$ and $\wedge$, universal and existential quantifiers and, for an atomic $\mathcal{A}$, $\mathcal{A}$ and $\sim\mathcal{A}$ are interchanged. So, for example, $(\exists x \leq p)(x = p \vee x \not> p)' = (\forall x \leq p)(x \neq p \wedge x > p)$. Still generalizing, for any Δ_0 formula whose operators are $\sim$, $\rightarrow$ and the bounded quantifiers, for atomic $\mathcal{A}$, let $\mathcal{A}^{*} = \mathcal{A}$; and $[\sim\mathcal{P}]^{*} = [\mathcal{P}^{*}]'$; $(\mathcal{P} \rightarrow \mathcal{Q})^{*} = ([\mathcal{P}^{*}]' \vee \mathcal{Q}^{*})$; $[(\exists x \leq t)\mathcal{P}]^{*} = (\exists x \leq t)\mathcal{P}^{*}$ and $[(\forall x \leq t)\mathcal{P}]^{*} = (\forall x \leq t)\mathcal{P}^{*}$ (and similarly for $(\exists x < t)$ and $(\forall x < t)$). Then as a simple extension to the result from E8.10,

T13.60. For any Δ_0 formula $\mathcal{P}$, there is a normal formula $\mathcal{P}^{*}$ such that $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^{*}$.

The demonstration is straightforward extension of the reasoning from E8.9 and E8.10.

We show our result as applied to these normal forms. Thus, *T13.61. For any Δ_0 formula $\mathcal{P}$ there is a $\Sigma^\star$ formula $\mathcal{P}^\star$ such that PA $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^\star$.

From T13.60, for any Δ_0 formula $\mathcal{P}$, there is a normal $\mathcal{P}^*$ such that $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^*$. Now by induction on the number of operators in $\mathcal{P}^*$, we show there is a $\mathcal{P}^\star$ such that PA $\vdash \mathcal{P}^* \leftrightarrow \mathcal{P}^\star$.

Basis: If $\mathcal{P}^*$ has no operators, then it is an atomic of the sort $s = t$, $s \leq t$ or $s < t$.

($=$) $\mathcal{P}^*$ is $s = t$. Set $\mathcal{P}^\star = \exists z[(s = z)^\star \wedge (t = z)^\star]$. By T13.59, PA $\vdash s = z \leftrightarrow (s = z)^\star$ and PA $\vdash t = z \leftrightarrow (t = z)^\star$; so PA $\vdash \mathcal{P}^* \leftrightarrow \mathcal{P}^\star$.

($\leq$) $\mathcal{P}^*$ is $s \leq t$, which is to say $\exists z(z + s = t)$. By the case immediately above, PA $\vdash (z+s = t) \leftrightarrow (z+s = t)^\star$. Set $\mathcal{P}^\star = \exists z(z+s = t)^\star$. Then PA $\vdash \mathcal{P}^* \leftrightarrow \mathcal{P}^\star$. And similarly for $<$.

Assp: For any i, $0 \leq i < k$, if a normal $\mathcal{P}^*$ has i operator symbols, then there is a $\Sigma^\star$ formula $\mathcal{P}^\star$ such that PA $\vdash \mathcal{P}^* \leftrightarrow \mathcal{P}^\star$.

Show: If a normal $\mathcal{P}^*$ has k operator symbols, then there is a $\Sigma^\star$ formula $\mathcal{P}^\star$ such that PA $\vdash \mathcal{P}^* \leftrightarrow \mathcal{P}^\star$.

If $\mathcal{P}^*$ has k operator symbols, then it is of the form $\sim\mathcal{A}$, $\mathcal{B} \wedge \mathcal{C}$, $\mathcal{B} \vee \mathcal{C}$, $(\exists x \leq t)\mathcal{B}$, $(\exists x < t)\mathcal{B}$, $(\forall x \leq t)\mathcal{B}$ or $(\forall x < t)\mathcal{B}$, where $\mathcal{A}$ is atomic and $\mathcal{B}$ and $\mathcal{C}$ are normal with $< k$ operator symbols.

($\sim$) $\mathcal{P}^*$ is $\sim\mathcal{A}$. (i) $\mathcal{P}^*$ is $s \neq t$. Set $\mathcal{P}^\star = (s < t)^\star \vee (t < s)^\star$; then by assumption, PA $\vdash s < t \leftrightarrow (s < t)^\star$ and PA $\vdash t < s \leftrightarrow (t < s)^\star$; and with T13.13p, PA $\vdash \mathcal{P}^* \leftrightarrow \mathcal{P}^\star$.

(ii) $\mathcal{P}^*$ is $s \not< t$; set $\mathcal{P}^\star = (t \leq s)^\star$; then by assumption, PA $\vdash t \leq s \leftrightarrow (t \leq s)^\star$; and with T13.13r, PA $\vdash \mathcal{P}^* \leftrightarrow \mathcal{P}^\star$. And similarly for $\mathcal{P}^\star = s \not\leq t$.

($\wedge$) $\mathcal{P}^*$ is $\mathcal{B} \wedge \mathcal{C}$. Set $\mathcal{P}^\star = \mathcal{B}^\star \wedge \mathcal{C}^\star$; since $\mathcal{B}$ and $\mathcal{C}$ are normal, by assumption PA $\vdash \mathcal{B} \leftrightarrow \mathcal{B}^\star$ and PA $\vdash \mathcal{C} \leftrightarrow \mathcal{C}^\star$; so PA $\vdash \mathcal{P}^* \leftrightarrow \mathcal{P}^\star$. And similarly for $\vee$.

($\forall$) $\mathcal{P}^*$ is $(\forall x \leq t)\mathcal{B}$. Set $\mathcal{P}^\star = \exists z[(t = z)^\star \wedge (\forall x \leq z)\mathcal{B}^\star]$; by T13.59 PA $\vdash t = z \leftrightarrow (t = z)^\star$ and by assumption, PA $\vdash \mathcal{B} \leftrightarrow \mathcal{B}^\star$ so PA $\vdash \mathcal{P}^* \leftrightarrow \mathcal{P}^\star$. And, by a related construction, similarly for $(\forall x < t)\mathcal{B}$.

($\exists$) $\mathcal{P}^*$ is $(\exists x \leq t)\mathcal{B}$. Set $\mathcal{P}^\star = \exists x[(x \leq t)^\star \wedge \mathcal{B}^\star]$; then by assumption PA $\vdash x \leq t \leftrightarrow (x \leq t)^\star$ and PA $\vdash \mathcal{B} \leftrightarrow \mathcal{B}^\star$; so PA $\vdash \mathcal{P}^* \leftrightarrow \mathcal{P}^\star$. And similarly for $(\exists x < t)\mathcal{B}$.

Indct: For any normal $\mathscr{P}^*$ there is a $\mathscr{P}^\star$ such that PA $\vdash \mathscr{P}^* \leftrightarrow \mathscr{P}^\star$.

So from T13.60 for any Δ_0 formula $\mathscr{P}$, there is a $\mathscr{P}^*$ such that $\vdash \mathscr{P} \leftrightarrow \mathscr{P}^*$ and by the above reasoning, PA $\vdash \mathscr{P}^* \leftrightarrow \mathscr{P}^\star$. So PA $\vdash \mathscr{P} \leftrightarrow \mathscr{P}^\star$.

Now it is immediate that for any Σ_1 formula $\mathscr{P}$ there is a $\Sigma^\star$ formula $\mathscr{P}^\star$ such that PA $\vdash \mathscr{P} \leftrightarrow \mathscr{P}^\star$.

T13.62. For any Σ_1 formula $\mathscr{P}$ there is a $\Sigma^\star$ formula $\mathscr{P}^\star$ such that PA $\vdash \mathscr{P} \leftrightarrow \mathscr{P}^\star$.

Consider any Σ_1 formula $\mathscr{P}$. This formula is of the form $\exists x_1 \ldots \exists x_n \mathscr{A}$ for Δ_0 formula $\mathscr{A}$. But by T13.61, there is an $\mathscr{A}^\star$ such that PA $\vdash \mathscr{A} \leftrightarrow \mathscr{A}^\star$. Let $\mathscr{P}^\star$ be $\exists x_1 \ldots \exists x_n \mathscr{A}^\star$. Then PA $\vdash \mathscr{P} \leftrightarrow \mathscr{P}^\star$.

E13.46. Povide a demonstration to show T13.60.

*E13.47. Fill in the parts of T13.59 and T13.61 that are left as "similarly" to to show that PA $\vdash \mathscr{P} \leftrightarrow \mathscr{P}^\star$.

E13.48. Show that for any $\Sigma^\star$ formula $\mathscr{P}^\star$ there is a Σ_1 formula $\mathscr{P}$ such that PA $\vdash \mathscr{P} \leftrightarrow \mathscr{P}^\star$ and so that the $\Sigma^\star$ formulas are the same as the Σ_1 formulas.

13.5.3 Substitutions

We now define a $sub(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{y})$ which substitutes numerals for all the variables free in $\mathscr{P}$. Where $\vec{y}$ is a (possibly empty) sequence of distinct variables, including at least all variables free in $\mathscr{P}$, consider an enumeration $\mathsf{enum(i)}$ of variable subscripts in $\vec{y}$ so that $\mathsf{enum(i)} = \mathsf{y_i}$ is the subscript of the i^{th} variable and $\overline{\mathsf{y}}_\mathsf{i}$ the numeral corresponding to that subscript; so the variables of $\vec{y}$ are $x_{\mathsf{y_1}} \ldots x_{\mathsf{y_n}}$ (perhaps the enumeration is by list where $\mathsf{enum(i)} = \mathsf{enum(n)}$ when $\mathsf{i > n}$). Then,

$$\text{PA} \vdash sub_0(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{y}) = \overline{\ulcorner \mathscr{P} \urcorner}$$

$$\text{PA} \vdash sub_{Si}(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{y}) = formsub(sub_i(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{y}), gvar(\overline{\mathsf{y}}_{\mathsf{Si}}), num(x_{\mathsf{y_{Si}}}))$$

And PA $\vdash$ $sub(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}) = sub_n(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y})$. Observe that enum does not appear in the $\mathcal{L}_{NT}$ expression; rather we use the function to make the specification in which there appears a certain variable $x_{\mathsf{y_{Si}}}$ and numeral $\bar{\mathsf{y}}_{\mathsf{Si}}$. Also, $sub(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y})$ still has as free variables each $x_{\mathsf{y_{Si}}}$ free in $\mathcal{P}$ but returns the Gödel number of a sentence — the sentence which substitutes into places for free variables numerals for the values assigned to those variables.

From a few quick theorems, so long as $\vec{y}$ and $\vec{z}$ include all the free variables of $\mathcal{P}$, $sub(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}) = sub(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{z})$.

T13.63. PA $\vdash$ $\mathbb{W}\!f\!f(sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}))$. Corollary: PA $\vdash$ $\mathbb{W}\!f\!f(sub(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}))$.

By an easy induction.

T13.64. For arbitrary $\vec{u}$, $\vec{v}$, $sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{x_1}} \dots x_{\mathsf{x_i}}, \vec{u}) = sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{x_1}} \dots x_{\mathsf{x_i}}, \vec{v})$

By an easy induction.

*T13.65. For any i, PA $\vdash$ $\mathbb{s}ub_{i+1}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{a}}, x_{\mathsf{y_1}} \dots x_{\mathsf{y_n}}) = \mathbb{s}ub_{i+1}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y_1}} \dots x_{\mathsf{y_i}}, x_{\mathsf{a}}, x_{\mathsf{y_{(i+1)}}} \dots x_{\mathsf{y_n}})$

The argument is an induction on the value of i. For the show, you need PA $\vdash$ $\mathbb{s}ub_{i+2}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{a}}, x_{\mathsf{y_1}} \dots x_{\mathsf{y_n}}) = \mathbb{s}ub_{i+2}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y_1}} \dots x_{\mathsf{y_{i+1}}}, x_{\mathsf{a}}, x_{\mathsf{y_{i+2}}} \dots x_{\mathsf{y_n}})$. The key to this is that $\mathbb{s}ub_{i+2}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y_1}} \dots x_{\mathsf{y_{i+1}}}, x_{\mathsf{a}}, x_{\mathsf{y_{i+2}}} \dots x_{\mathsf{y_n}})$ is,

$$formsub[formsub(sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y_1}} \dots x_{\mathsf{y_{i+1}}}, x_{\mathsf{a}}, x_{\mathsf{y_{i+2}}} \dots x_{\mathsf{yn}}), \mathbb{g}var(\bar{\mathsf{y}}_{\mathsf{i+1}}), \mathbb{n}um(x_{\mathsf{y_{i+1}}})), \mathbb{g}var(\bar{\mathsf{y}}_{\mathsf{a}}), \mathbb{n}um(x_{\mathsf{ya}})]$$

You will be able to use T13.64 and T13.58d. As a preliminary it will be useful to show that if PA $\vdash$ $\mathbb{W}\!f\!f(p)$, then PA $\vdash$ $formsub(formsub(p, \mathbb{g}var(\bar{\mathsf{a}}), \mathbb{n}um(x_{\mathsf{a}})), \mathbb{g}var(\bar{\mathsf{b}}), \mathbb{n}um(x_{\mathsf{b}})) = formsub(formsub(p, \mathbb{g}var(\bar{\mathsf{b}}), \mathbb{n}um(x_{\mathsf{b}})), \mathbb{g}var(\bar{\mathsf{a}}), \mathbb{n}um(x_{\mathsf{a}}))$.

T13.65 effectively gives the ability to sort variables from one order into another. Suppose the variables of $\vec{x}$ are the same as the variables of $\vec{y}$. To convert $\vec{y}$ to $\vec{x}$, a straightforward approach is to switch members into the first position in the reverse of their order in $\vec{x}$ — so for n members, at stage i, the result is $x_{\mathsf{x_{Sn-i}}} \dots x_{\mathsf{x_n}}, \vec{y}'$ where $\vec{y}'$ is like $\vec{y}$ less the members that precede it. So for a vector with 6 members, at stage 0 we begin with some $sub(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y})$; then at stage three PA proves this is equivalent to $sub(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{x_4}}, x_{\mathsf{x_5}}, x_{\mathsf{x_6}}, \vec{y}')$; and at stage 6 that it is equivalent to $sub(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{x})$. This is an induction, but simple enough, so left as an exercise.

T13.66. If x_{a} is not free in $\mathcal{P}$, then PA $\vdash \mathbb{sub}_{i+1}(\overline{\ulcorner \mathcal{P} \urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_i}, x_{\mathsf{a}}, x_{\mathsf{y}_{(i+1)}} \dots x_{\mathsf{y}_n})$ $= \mathbb{sub}_i(\overline{\ulcorner \mathcal{P} \urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_i}, x_{\mathsf{a}}, x_{\mathsf{y}_{(i+1)}} \dots x_{\mathsf{y}_n})$

In light of T13.64 and T13.65 it is sufficient to show PA $\vdash \mathbb{sub}_{i+1}(\overline{\ulcorner \mathcal{P} \urcorner}, x_{\mathsf{a}}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_i}) = \mathbb{sub}_i(\overline{\ulcorner \mathcal{P} \urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_i}, x_{\mathsf{a}})$. The argument is by induction on i, where the basis uses $\mathbb{Wff}(\overline{\ulcorner \mathcal{P} \urcorner}) \wedge \sim\mathbb{Free}_f(\overline{\ulcorner \mathcal{P} \urcorner}, \mathbb{gvar}(\overline{\mathsf{a}})) \wedge \mathbb{Term}(\mathbb{num}(x_{\mathsf{a}}))$ by capture and T13.57r, and then T13.56i to establish that PA $\vdash \mathbb{sub}_1(\overline{\ulcorner \mathcal{P} \urcorner}, x_{\mathsf{a}}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_i}) = \mathbb{sub}_0(\overline{\ulcorner \mathcal{P} \urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_n}, x_{\mathsf{a}})$.

*T13.67. If the variables of $\vec{y}$ and $\vec{z}$ are ordered by their subscripts and $\vec{y}$ and $\vec{z}$ are the same except that $\vec{z}$ includes some variables not in $\vec{y}$ (and so not free in $\mathcal{P}$), then PA $\vdash sub(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{y}) = sub(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{z})$.

Hint: Where the variables of $\vec{y}$ are $x_{\mathsf{y}_1} \dots x_{\mathsf{y}_m}$ and of $\vec{z}$ are $x_{\mathsf{z}_1} \dots x_{\mathsf{z}_n}$, let $S(i.j) = Si.Sj$ when $\mathsf{y}_{\mathsf{Si}} = \mathsf{z}_{\mathsf{Sj}}$ and $S(i.j) = i.Sj$ when $\mathsf{y}_{\mathsf{Si}} \neq \mathsf{z}_{\mathsf{Sj}}$. Then $i.j$ "counts" in the natural way from 0.0 to $m.n$; and you will be able to show that for any member of this $i.j$ sequence, PA $\vdash sub_i(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{y}) = sub_j(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{z})$.

And with T13.65 and T13.67, details of the vectors do not matter: Let $\vec{x}'$ and $\vec{y}'$ be like $\vec{x}$ and $\vec{y}$ except that variables are in standard order, and $\vec{z}$ be just the free variables of $\mathcal{P}$ in standard order. Then by T13.65, $sub(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{x}) = sub(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{x}')$; by T13.67, $sub(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{x}') = sub(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{z})$; by T13.67 again, $sub(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{z}) = sub(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{y}')$; and with T13.65, $sub(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{y}') = sub(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{y})$. So PA $\vdash sub(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{x}) = sub(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{y})$ and we shall not usually worry about details of the vectors.

Then, introducing double brackets as a special notation,

$$Prvt[\![\mathcal{P}(\vec{x})]\!] =_{\text{def}} Prvt(sub(\overline{\ulcorner \mathcal{P} \urcorner}, \vec{x}))$$

Where $\mathcal{P}$ has free variables $\vec{x}$, $Prvt(\overline{\ulcorner \mathcal{P} \urcorner})$ asserts the provability of the open formula $\mathcal{P}(\vec{x})$. But $Prvt[\![\mathcal{P}(\vec{x})]\!]$ itself has all the free variables of $\mathcal{P}$ and asserts the provability of whatever *sentences* have numerals for the variables free in $\mathcal{P}$: so, for example, $\forall x Prvt[\![\mathcal{P}(x)]\!]$ asserts the provability of $\mathcal{P}^x_{\emptyset}$, $\mathcal{P}^x_{S\emptyset}$, and so forth. When $\mathcal{P}$ is a sentence, there are no substitutions to be made, and $Prvt[\![\mathcal{P}]\!]$ is the same as $Prvt(\overline{\ulcorner \mathcal{P} \urcorner})$. Thus we set out to show PA $\vdash \mathcal{P} \rightarrow Prvt[\![\mathcal{P}]\!]$ for $\Sigma^{\star}$ formulas. When $\mathcal{P}$ is a sentence, this gives PA $\vdash \mathcal{P} \rightarrow Prvt(\overline{\ulcorner \mathcal{P} \urcorner})$, which is to be shown.

Finally we shall require also some short theorems in order to manipulate this new notion. There are analogs to D1 and D2, and results for substitution. Each is by a short induction. First, for D1.

T13.68. If PA $\vdash \mathscr{P}$, then PA $\vdash Prvt[\![\mathscr{P}]\!]$

Suppose PA $\vdash \mathscr{P}$. By induction on the value of n, PA $\vdash Prvt(sub_n(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}))$; the case when $i = n$ gives the desired result.

Basis: $sub_0(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}) = \overline{\ulcorner\mathscr{P}\urcorner}$. Since PA $\vdash \mathscr{P}$, by D1, PA $\vdash Prvt(\overline{\ulcorner\mathscr{P}\urcorner})$; so PA $\vdash Prvt(sub_0(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}))$.

Assp: PA $\vdash Prvt(sub_i(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}))$.

Show: PA $\vdash Prvt(sub_{Si}(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}))$.

1. $Prvt(sub_i(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}))$	assp
2. $\mathbb{V}ar(gvar(\overline{\mathsf{x}}_{\mathsf{Si}}))$	T13.57f
3. $\mathbb{W}ff(sub_i(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}))$	T13.63
4. $Prvt[unv(gvar(\overline{\mathsf{x}}_{\mathsf{Si}}), sub_i(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}))]$	1,2 T13.57h
5. $Prvt[cnd(unv(gvar(\overline{\mathsf{x}}_{\mathsf{Si}}), sub_i(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x})),$ $formsub(sub_i(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}), gvar(\overline{\mathsf{x}}_{\mathsf{Si}}), num(x_{\mathsf{x}_{\mathsf{Si}}})))]$	3 T13.57u
6. $Prvt[unv(gvar(\overline{\mathsf{x}}_{\mathsf{Si}}), sub_i(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}))] \rightarrow$ $Prvt[formsub(sub_i(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}), gvar(\overline{\mathsf{x}}_{\mathsf{Si}}), num(x_{\mathsf{x}_{\mathsf{Si}}}))]$	5 D2
7. $Prvt[formsub(sub_i(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}), gvar(\overline{\mathsf{x}}_{\mathsf{Si}}), num(x_{\mathsf{x}_{\mathsf{Si}}}))]$	4,6 →E
8. $Prvt(sub_{Si}(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}))$	7 def

---

Indct: For any n, PA $\vdash Prvt(sub_n(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}))$

And an analog to D2,

T13.69. PA $\vdash Prvt[\![\mathscr{P} \rightarrow \mathscr{Q}]\!] \rightarrow (Prvt[\![\mathscr{P}]\!] \rightarrow Prvt[\![\mathscr{Q}]\!])$

We must show PA $\vdash Prvt(sub(\overline{\ulcorner\mathscr{P} \rightarrow \mathscr{Q}\urcorner}, \vec{x})) \rightarrow (Prvt(sub(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x})) \rightarrow Prvt(sub(\overline{\ulcorner\mathscr{Q}\urcorner}, \vec{x})))$. First, by induction, PA $\vdash sub_i(cnd(\overline{\ulcorner\mathscr{P}\urcorner}, \overline{\ulcorner\mathscr{Q}\urcorner}), \vec{x})) = cnd(sub_i(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}), sub_i(\overline{\ulcorner\mathscr{Q}\urcorner}, \vec{x}))$. This leads immediately to the desired result.

Basis: $sub_0(cnd(\overline{\ulcorner\mathscr{P}\urcorner}, \overline{\ulcorner\mathscr{Q}\urcorner}), \vec{x})) = cnd(sub_0(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}), sub_0(\overline{\ulcorner\mathscr{Q}\urcorner}, \vec{x}))$

1. $sub_0(cnd(\overline{\ulcorner\mathscr{P}\urcorner}, \overline{\ulcorner\mathscr{Q}\urcorner}), \vec{x}) = cnd(\overline{\ulcorner\mathscr{P}\urcorner}, \overline{\ulcorner\mathscr{Q}\urcorner})$	def
2. $sub_0(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}) = \overline{\ulcorner\mathscr{P}\urcorner}$	def
3. $sub_0(\overline{\ulcorner\mathscr{Q}\urcorner}, \vec{x})) = \overline{\ulcorner\mathscr{Q}\urcorner}$	def
4. $sub_0(cnd(\overline{\ulcorner\mathscr{P}\urcorner}, \overline{\ulcorner\mathscr{Q}\urcorner}), \vec{x}) = cnd(sub_0(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}), sub_0(\overline{\ulcorner\mathscr{Q}\urcorner}, \vec{x}))$	1,2,3 =E

Assp: PA $\vdash sub_i(cnd(\overline{\ulcorner\mathscr{P}\urcorner}, \overline{\ulcorner\mathscr{Q}\urcorner}), \vec{x})) = cnd(sub_i(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}), sub_i(\overline{\ulcorner\mathscr{Q}\urcorner}, \vec{x}))$

Show: PA $\vdash sub_{Si}(cnd(\overline{\ulcorner\mathscr{P}\urcorner}, \overline{\ulcorner\mathscr{Q}\urcorner}), \vec{x})) = cnd(sub_{Si}(\overline{\ulcorner\mathscr{P}\urcorner}, \vec{x}), sub_{Si}(\overline{\ulcorner\mathscr{Q}\urcorner}, \vec{x}))$

1. $\mathbb{W}\mathit{ff}(sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{x})) \wedge \mathbb{W}\mathit{ff}(sub_i(\overline{\ulcorner\mathcal{Q}\urcorner}, \vec{x}))$ T13.63
2. $\mathbb{T}erm(num(x_{\mathsf{xSi}}))$ T13.57r
3. $sub_{Si}(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{x}) = formsub(sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{x}), gvar(\overline{\mathsf{x}}_{\mathsf{Si}}), num(x_{\mathsf{xSi}}))$ def
4. $sub_{Si}(\overline{\ulcorner\mathcal{Q}\urcorner}, \vec{x}) = formsub(sub_i(\overline{\ulcorner\mathcal{Q}\urcorner}, \vec{x}), gvar(\overline{\mathsf{x}}_{\mathsf{Si}}), num(x_{\mathsf{xSi}}))$ def
5. $sub_{Si}(cnd(\overline{\ulcorner\mathcal{P}\urcorner}, \overline{\ulcorner\mathcal{Q}\urcorner}), \vec{x})$
6. $\quad = formsub(sub_i(cnd(\overline{\ulcorner\mathcal{P}\urcorner}, \overline{\ulcorner\mathcal{Q}\urcorner}), \vec{x}), gvar(\overline{\mathsf{x}}_{\mathsf{Si}}), num(x_{\mathsf{xSi}}))$ def
7. $\quad = formsub(cnd(sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{x}), sub_i(\overline{\ulcorner\mathcal{Q}\urcorner}, \vec{x})), gvar(\overline{\mathsf{x}}_{\mathsf{Si}}), num(x_{\mathsf{xSi}}))$ assp
8. $\quad = cnd(formsub(sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{x}), gvar(\overline{\mathsf{x}}_{\mathsf{Si}}), num(x_{\mathsf{xSi}})),$
   $\quad formsub(sub_i(\overline{\ulcorner\mathcal{Q}\urcorner}, \vec{x}), gvar(\overline{\mathsf{x}}_{\mathsf{Si}}), num(x_{\mathsf{xSi}})))$ 1,2 T13.58a
9. $\quad = cnd(sub_{Si}(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{x}), sub_{Si}(\overline{\ulcorner\mathcal{Q}\urcorner}, \vec{x}))$ 8,3,4 =E

Indct: For any i, PA $\vdash sub_i(cnd(\overline{\ulcorner\mathcal{P}\urcorner}, \overline{\ulcorner\mathcal{Q}\urcorner}), \vec{x})) = cnd(sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{x}), sub_i(\overline{\ulcorner\mathcal{Q}\urcorner}, \vec{x}))$

So PA $\vdash sub(cnd(\overline{\ulcorner\mathcal{P}\urcorner}, \overline{\ulcorner\mathcal{Q}\urcorner}), \vec{x})) = cnd(sub(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{x}), sub(\overline{\ulcorner\mathcal{Q}\urcorner}, \vec{x}))$. Now,

1. $\quad Prvt(sub(\overline{\ulcorner\mathcal{P} \rightarrow \mathcal{Q}\urcorner}, \vec{x}))$ A (g →I)
2. $\quad Prvt(sub(cnd(\overline{\ulcorner\mathcal{P}\urcorner}, \overline{\ulcorner\mathcal{Q}\urcorner}), \vec{x}))$ 1 cap
3. $\quad Prvt(cnd(sub(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{x}), sub(\overline{\ulcorner\mathcal{Q}\urcorner}, \vec{x})))$ 2 above
4. $\quad Prvt(sub(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{x})) \rightarrow Prvt(sub(\overline{\ulcorner\mathcal{Q}\urcorner}, \vec{x}))$ 3 D2
5. $Prvt(sub(\overline{\ulcorner\mathcal{P} \rightarrow \mathcal{Q}\urcorner}, \vec{x})) \rightarrow [Prvt(sub(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{x})) \rightarrow Prvt(sub(\overline{\ulcorner\mathcal{Q}\urcorner}, \vec{x}))]$ 2-5 →I

Finally a result for substitutions into these expressions. Again, let $x = x_i$ and $y = x_j$.

T13.70. If t is one of $\emptyset$, y or Sy and t is free for x in $\mathcal{P}$, then PA $\vdash Prvt[\![\mathcal{P}^x_t]\!] \leftrightarrow Prvt[\![\mathcal{P}]\!]^x_t$.

Consider the case $t = Sy$ and take the variables in the order $x, y, \vec{z}$ where x and y do not appear in $\vec{z}$. $Prvt[\![\mathcal{P}^x_{Sy}]\!] = Prvt(sub(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, x, y, \vec{z}))$. And $Prvt[\![\mathcal{P}]\!]^x_{Sy} = Prvt[sub(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z})]^x_{Sy} = Prvt[sub(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z})^x_{Sy}]$. Thus it suffices to show PA $\vdash sub(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, x, y, \vec{z}) = sub(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z})^x_{Sy}$. By induction, PA $\vdash sub_n(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, x, y, \vec{z}) = sub_n(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z})^x_{Sy}$.

Basis: PA $\vdash sub_2(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, x, y, \vec{z}) = sub_2(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z})^x_{Sy}$.

1. $\mathbb{W}\!f\!f(\overline{\ulcorner\mathcal{P}\urcorner})$ cap
2. $\mathbb{V}ar(gvar(j))$ T13.57f
3. $sub_1(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, x, y, \vec{z})$
4. $\quad = formsub(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, gvar(\bar{\text{i}}), num(x))$ def
5. $\quad = \overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}$ T13.56i
6. $sub_2(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, x, y, \vec{z})$
7. $\quad = formsub(sub_1(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, x, y, \vec{z}), gvar(\bar{\text{j}}), num(y))$ def
8. $\quad = formsub(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, gvar(\bar{\text{j}}), num(y))$ 3-5 =E
9. $\quad = formsub(formsub(\overline{\ulcorner\mathcal{P}\urcorner}, gvar(\bar{\text{i}}), \overline{\ulcorner S\urcorner} * gvar(\bar{\text{j}})), gvar(\bar{\text{j}}), num(y))$ cap
10. $\quad = formsub[formsub(\overline{\ulcorner\mathcal{P}\urcorner}, gvar(\bar{\text{i}}), num(Sy)), gvar(\bar{\text{j}}), num(y)]$ 1,2 T13.58j
11. $sub_1(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z})$
12. $\quad = formsub(\overline{\ulcorner\mathcal{P}\urcorner}, gvar(\bar{\text{i}}), num(x))$ def
13. $sub_2(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z})^x_{Sy}$
14. $\quad = formsub(sub_1(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z}), gvar(\bar{\text{j}}), num(y))^x_{Sy}$ def
15. $\quad = formsub(formsub(\overline{\ulcorner\mathcal{P}\urcorner}, gvar(\bar{\text{i}}), num(x)), gvar(\bar{\text{j}}), num(y))^x_{Sy}$ 11-12 =E
16. $\quad = formsub(formsub(\overline{\ulcorner\mathcal{P}\urcorner}, gvar(\bar{\text{i}}), num(Sy)), gvar(\bar{\text{j}}), num(y))$ abv
17. $sub_2(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, x, y, \vec{z}) = sub_2(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z})^x_{Sy}$ 6-10,13-16 =E

Assp: For $2 \leq i$, PA $\vdash sub_i(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, x, y, \vec{z}) = sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z})^x_{Sy}$.

Show: PA $\vdash sub_{Si}(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, x, y, \vec{z}) = sub_{Si}(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z})^x_{Sy}$.

1. $sub_{Si}(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, x, y, \vec{z})$
2. $\quad = formsub(sub_i(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, x, y, \vec{z}), gvar(\mathsf{z}_{\mathsf{Si-2}}), num(x_{\mathsf{z}_{\mathsf{Si-2}}}))$ def
3. $\quad = formsub(sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z})^x_{Sy}, gvar(\mathsf{z}_{\mathsf{Si-2}}), num(x_{\mathsf{z}_{\mathsf{Si-2}}}))$ assp
4. $\quad = formsub(sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z}), gvar(\mathsf{z}_{\mathsf{Si-2}}), num(x_{\mathsf{z}_{\mathsf{Si-2}}}))^x_{Sy}$ abv
5. $\quad = sub_{Si}(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z})^x_{Sy}$ def

---

Indct: PA $\vdash sub_n(\overline{\ulcorner\mathcal{P}^x_{Sy}\urcorner}, x, y, \vec{z}) = sub_n(\overline{\ulcorner\mathcal{P}\urcorner}, x, y, \vec{z})^x_{Sy}$

Line (4) of the show is justified insofar as x does not appear in $\vec{z}$.

Other cases are similar and left for homework.

*E13.49. (i) Provide a demonstration for T13.65. (ii) Then provide a demonstration for the sorting result that is "simple enough" and so left as an exercise.

*E13.50. Provide a demonstration for T13.67

E13.51. Complete the demonstration of T13.70 by completing the remaining cases.

13.5.4 The result.

We are finally (!) ready to show that for any $\Sigma^\star$ $\mathcal{P}$, PA $\vdash \mathcal{P} \rightarrow Prvt[\![\mathcal{P}]\!]$. And this is the result we need for D3. The argument is by induction on the number of operators in a $\Sigma^\star$ formula.

Before we launch into the main argument, a word about substitution. From their original statement, the rules $\forall$I and =E result in formulas of the sort $\mathcal{P}^x_t$ or $\mathcal{P}^{t}/_{s}$. So from, say, $\forall$E applied to $\forall x Prvt[\![\mathcal{P}]\!]$ we get something of the sort $Prvt[\![\mathcal{P}]\!]^x_t$. But we need to be careful about what the substitution comes to. In the simplest case, $Prvt[\![\mathcal{P}(x)]\!]$ is of the sort $Prvt(formsub(\overline{\ulcorner \mathcal{P}(x) \urcorner}, gvar(\overline{\mathsf{i}}), num(x)))$, where there is a free x to be replaced by t; but this does not automatically convert to $Prvt[\![\mathcal{P}(t)]\!]$ insofar as $\overline{\ulcorner \mathcal{P}(x) \urcorner}$ is a *numeral* and so lacks any free x. But we do have a theorem, T13.70 which tells us that in certain cases PA $\vdash Prvt[\![\mathcal{P}^x_t]\!] \leftrightarrow Prvt[\![\mathcal{P}]\!]^x_t$, so that the replacements can be moved across the bracket in the natural way. With this said, we turn to our theorem.

T13.71. For any $\Sigma^\star$ formula $\mathcal{P}$, PA $\vdash \mathcal{P} \rightarrow Prvt[\![\mathcal{P}]\!]$.

By induction on the number of operators in $\mathcal{P}$.

Basis: If a $\Sigma^\star$ $\mathcal{P}$ has no operator symbols, then it is an atomic of the sort $\emptyset = z$, $y = z$, $Sy = z$, $x + y = z$ or $x \times y = z$.

(S) Suppose $\mathcal{P}$ is $Sy = z$. Reason as follows,

1.	$Sy = Sy$	=I
2.	$Prvt[\![Sy = Sy]\!]$	1 T13.68
3.	$\quad Sy = z$	A (g →I)
4.	$\quad Prvt[\![(Sy = z)^z_{Sy}]\!]$	2 abv
5.	$\quad Prvt[\![Sy = z]\!]^z_{Sy}$	4 T13.70
6.	$\quad Prvt[\![Sy = z]\!]$	3,5 =E
7.	$Sy = z \rightarrow Prvt[\![Sy = z]\!]$	3-6 →I

Observe that T13.68 applies to theorems, and so not to formulas under the assumption for →I. Thus we take care to restrict its application to formulas against the main scope line. Also, at (5) we use T13.70 to move the substitution across the bracket. With this done, the substitution on line (4) applies only to the free z of $Prvt[\![Sy = z]\!]$ — that is, to the free z of $Prvt(sub(\overline{\ulcorner Sy = z \urcorner}, y, z)$; so that =E applies in a straightforward way to substitute a z back into that place. The argument is similar for $\emptyset = z$ and $y = z$.

(+) Suppose $\mathcal{P}$ is $x + y = z$. The proof in PA requires appeal to IN, with induction on the value of x in $\forall y \forall z(x + y = z \rightarrow Prvt[\![x + y = z]\!])$. For the basis,

1.	$\emptyset + y = y$	T6.51
2.	$Prvt[\![\emptyset + y = y]\!]$	1 T13.68
3.	$(x + y = z)^{x}_{\emptyset}$	A ($g \rightarrow$I)
4.	$\emptyset + y = z$	3 abv
5.	$y = z$	1,4 =E
6.	$Prvt[\![(\emptyset + y = z)^{z}_{y}]\!]$	2 abv
7.	$Prvt[\![\emptyset + y = z]\!]^{z}_{y}$	6 T13.70
8.	$Prvt[\![\emptyset + y = z]\!]$	6,5 =E
9.	$Prvt[\![(x + y = z)^{x}_{\emptyset}]\!]$	8 abv
10.	$Prvt[\![x + y = z]\!]^{x}_{\emptyset}$	9 T13.70
11.	$(x + y = z)^{x}_{\emptyset} \rightarrow Prvt[\![x + y = z]\!]^{x}_{\emptyset}$	3-10 $\rightarrow$I
12.	$(x + y = z \rightarrow Prvt[\![x + y = z]\!])^{x}_{\emptyset}$	11 abv
13.	$\forall y \forall z(x + y = z \rightarrow Prvt[\![x + y = z]\!])^{x}_{\emptyset}$	12 $\forall$I

And the inductive stage,

14.	$x + Sy = z \leftrightarrow Sx + y = z$	T6.42,T6.53
15.	$Prvt[\![x + Sy = z \rightarrow Sx + y = z]\!]$	14 T13.68
16.	$\forall y \forall z(x + y = z \rightarrow Prvt[\![x + y = z]\!])$	A ($g \rightarrow$I)
17.	$(x + y = z)^{x}_{Sx}$	A ($g \rightarrow$I)
18.	$Sx + y = z$	17 abv
19.	$x + Sy = z$	14,18 $\leftrightarrow$E
20.	$x + Sy = z \rightarrow Prvt[\![x + y = z]\!]^{y}_{Sy}$	16 $\forall$E
21.	$Prvt[\![x + y = z]\!]^{y}_{Sy}$	20,19 $\rightarrow$E
22.	$Prvt[\![x + Sy = z]\!]$	21 T13.70
23.	$Prvt[\![x + Sy = z]\!] \rightarrow Prvt[\![Sx + y = z]\!]$	15 T13.69
24.	$Prvt[\![Sx + y = z]\!]$	23,22 $\rightarrow$E
25.	$Prvt[\![x + y = z]\!]^{x}_{Sx}$	24 T13.70
26.	$(x + y = z)^{x}_{Sx} \rightarrow Prvt[\![x + y = z]\!]^{x}_{Sx}$	17-25 $\rightarrow$I
27.	$(x + y = z \rightarrow Prvt[\![x + y = z]\!])^{x}_{Sx}$	26 abv
28.	$\forall y \forall z(x + y = z \rightarrow Prvt[\![x + y = z]\!])^{x}_{Sx}$	27 $\forall$I
29.	$\forall y \forall z(x + y = z \rightarrow Prvt[\![x + y = z]\!]) \rightarrow \forall y \forall z(x + y = z \rightarrow Prvt[\![x + y = z]\!])^{x}_{Sx}$	16-28 $\rightarrow$I
30.	$\forall y \forall z(x + y = z \rightarrow Prvt[\![x + y = z]\!])$	13,29 IN

We are able to apply the assumption at (16) to get $Prvt[\![x + y = z]\!]^{y}_{Sy}$ and convert this into the desired result. So PA $\vdash x + y = z \rightarrow Prvt[\![x + y = z]\!]$.

($\times$) Suppose $\mathscr{P}$ is $x \times y = z$. The proof in PA requires appeal to IN, on the value of x in $\forall y \forall z(x \times y = z \rightarrow Prvt[\![x \times y = z]\!])$. The zero case is straightforward. Then,

1.	$\forall y \forall z(x \times y = z \to Prvt[\![x \times y = z]\!])^x_\emptyset$	zero case
2.	$Sx \times y = z \leftrightarrow x \times y + y = z$	T6.60
3.	$x \times y = v \to (v + y = z \to x \times y + y = z)$	simple ND
4.	$Prvt[\![x \times y + y = z \to Sx \times y = z]\!]$	2 T13.68
5.	$Prvt[\![x \times y = v \to (v + y = z \to x \times y + y = z)]\!]$	3 T13.68
6.	$\quad \forall y \forall z(x \times y = z \to Prvt[\![x \times y = z]\!])$	A (g →I)
7.	$\quad\quad (x \times y = z)^x_{Sx}$	A (g →I)
8.	$\quad\quad Sx \times y = z$	7 abv
9.	$\quad\quad x \times y + y = z$	2,8 ↔E
10.	$\quad\quad \exists v(x \times y = v)$	=I,∃I
11.	$\quad\quad\quad x \times y = v$	A (g 10∃E)
12.	$\quad\quad\quad v + y = z$	9,11 =E
13.	$\quad\quad\quad Prvt[\![v + y = z]\!]$	12 (+) case
14.	$\quad\quad\quad Prvt[\![x \times y = z]\!]^z_v$	6,11 ∀E,→E
15.	$\quad\quad\quad Prvt[\![x \times y = v]\!]$	14 T13.70
16.	$\quad\quad\quad Prvt[\![x \times y = v]\!] \to Prvt[\![v + y = z \to x \times y + y = v]\!]$	5 T13.69
17.	$\quad\quad\quad Prvt[\![v + y = z \to x \times y + y = z]\!]$	15,16 →E
18.	$\quad\quad\quad Prvt[\![v + y = z]\!] \to Prvt[\![x \times y + y = z]\!]$	17 T13.69
19.	$\quad\quad\quad Prvt[\![x \times y + y = z]\!]$	18,13 →E
20.	$\quad\quad\quad Prvt[\![x \times y + y = z]\!] \to Prvt[\![Sx \times y = z]\!]$	4 T13.69
21.	$\quad\quad\quad Prvt[\![Sx \times y = z]\!]$	19,20 →E
22.	$\quad\quad\quad Prvt[\![x \times y = z]\!]^x_{Sx}$	21 T13.70
23.	$\quad\quad Prvt[\![x \times y = z]\!]^x_{Sx}$	10,11-22 ∃E
24.	$\quad (x \times y = z)^x_{Sx} \to Prvt[\![x \times y = z]\!]^x_{Sx}$	7-23 →I
25.	$\quad (x \times y = z \to Prvt[\![x \times y = z]\!])^x_{Sx}$	24 abv
26.	$\quad \forall y \forall z(x \times y = z \to Prvt[\![x \times y = z]\!])^x_{Sx}$	25 ∀I
27.	$\forall y \forall z(x \times y = z \to Prvt[\![x \times y = z]\!]) \to \forall y \forall z(x \times y = z \to Prvt[\![x \times y = z]\!])^x_{Sx}$	6-26 →I
28.	$\forall y \forall z(x \times y = z \to Prvt[\![x \times y = z]\!])$	1,27 IN

The (+) case does not directly apply to $x \times y + y = z$. However, having identified $x \times y$ with variable v we get $Prvt[\![v + y = z]\!]$, and with the inductive assumption $Prvt[\![x \times y = v]\!]$. These then unpack into $Prvt[\![Sx \times y = z]\!]$. So PA $\vdash x \times y = z \to Prvt[\![x \times y = z]\!]$.

Assp: For any i, $0 \leq i < k$ if a $\Sigma^\star$ $\mathcal{P}$ has i operator symbols, then PA $\vdash \mathcal{P} \to Prvt[\![\mathcal{P}]\!]$.

Show: If a $\Sigma^\star$ $\mathcal{P}$ has k operator symbols, then PA $\vdash \mathcal{P} \to Prvt[\![\mathcal{P}]\!]$.

If $\Sigma^\star$ $\mathcal{P}$ has k operator symbols, then it is of the form, $\mathcal{A} \vee \mathcal{B}$, $\mathcal{A} \wedge \mathcal{B}$, $(\forall x \leq y)\mathcal{A}$ (y not in $\mathcal{A}$), or $\exists x \mathcal{A}$ for $\Sigma^\star$ $\mathcal{A}$ and $\mathcal{B}$ with $< k$ operator symbols.

(∧) $\mathcal{P}$ is $\mathcal{A} \wedge \mathcal{B}$. Reason as follows.

1.	$\mathcal{A} \rightarrow Prvt[\![\mathcal{A}]\!]$	by assp
2.	$\mathcal{B} \rightarrow Prvt[\![\mathcal{B}]\!]$	by assp
3.	$\mathcal{A} \rightarrow (\mathcal{B} \rightarrow (\mathcal{A} \wedge \mathcal{B}))$	T9.4
4.	$Prvt[\![\mathcal{A} \rightarrow (\mathcal{B} \rightarrow (\mathcal{A} \wedge \mathcal{B}))]\!]$	3 T13.68
5.	$\quad \mathcal{A} \wedge \mathcal{B}$	A (g →I)
6.	$\quad Prvt[\![\mathcal{A}]\!]$	1,5
7.	$\quad Prvt[\![\mathcal{B}]\!]$	2,5
8.	$\quad Prvt[\![\mathcal{A}]\!] \rightarrow Prvt[\![\mathcal{B} \rightarrow (\mathcal{A} \wedge \mathcal{B})]\!]$	4 T13.69
9.	$\quad Prvt[\![\mathcal{B} \rightarrow (\mathcal{A} \wedge \mathcal{B})]\!]$	6,8 →E
10.	$\quad Prvt[\![\mathcal{B}]\!] \rightarrow Prvt[\![\mathcal{A} \wedge \mathcal{B}]\!]$	9 T13.69
11.	$\quad Prvt[\![\mathcal{A} \wedge \mathcal{B}]\!]$	7,10 →E
12.	$(\mathcal{A} \wedge \mathcal{B}) \rightarrow Prvt[\![\mathcal{A} \wedge \mathcal{B}]\!]$	5-11 →I

And similarly for ∨.

(∃) $\mathcal{P}$ is $\exists x \mathcal{A}$. Reason as follows.

1.	$\mathcal{A} \rightarrow Prvt[\![\mathcal{A}]\!]$	by assp
2.	$\mathcal{A} \rightarrow \exists x \mathcal{A}$	T3.29
3.	$Prvt[\![\mathcal{A} \rightarrow \exists x \mathcal{A}]\!]$	2 T13.68
4.	$\quad \exists x \mathcal{A}$	A (g →I)
5.	$\quad\quad \mathcal{A}$	A (g 4∃E)
6.	$\quad\quad Prvt[\![\mathcal{A}]\!]$	1,5 →E
7.	$\quad\quad Prvt[\![\mathcal{A}]\!] \rightarrow Prvt[\![\exists x \mathcal{A}]\!]$	3 T13.69
8.	$\quad\quad Prvt[\![\exists x \mathcal{A}]\!]$	7,6 →E
9.	$\quad Prvt[\![\exists x \mathcal{A}]\!]$	4,5-8 ∃E
10.	$\exists x \mathcal{A} \rightarrow Prvt[\![\exists x \mathcal{A}]\!]$	5-9 →I

$\mathcal{A}$ has x free. But $\exists x \mathcal{A}$ does not, and $Prvt[\![\exists x \mathcal{A}]\!]$ has the same free variables as $\exists x \mathcal{A}$. So the restriction is met for ∃E at (9).

(∀) $\mathcal{P}$ is $(\forall x \leq y)\mathcal{A}$. The argument in PA requires appeal to IN, for induction on the value of y. For the zero case,

1.	$\mathcal{A}^x_\emptyset \to Prvt[\![\mathcal{A}^x_\emptyset]\!]$	by assp
2.	$(\forall x \le \emptyset)\mathcal{A} \leftrightarrow \mathcal{A}^x_\emptyset$	thrm (with T8.21)
3.	$Prvt[\![\mathcal{A}^x_\emptyset \to (\forall x \le \emptyset)\mathcal{A}]\!]$	2 T13.68
4.	$(\forall x \le y)\mathcal{A}^y_\emptyset$	A (g →I)
5.	$(\forall x \le \emptyset)\mathcal{A}$	4 abv
6.	$\mathcal{A}^x_\emptyset$	2,5 ↔E
7.	$Prvt[\![\mathcal{A}^x_\emptyset]\!]$	1,6 →E
8.	$Prvt[\![\mathcal{A}^x_\emptyset]\!] \to Prvt[\![(\forall x \le \emptyset)\mathcal{A}]\!]$	3 T13.69
9.	$Prvt[\![(\forall x \le \emptyset)\mathcal{A}]\!]$	8,7 →E
10.	$Prvt[\![(\forall x \le y)\mathcal{A}^y_\emptyset]\!]$	9 abv
11.	$Prvt[\![(\forall x \le y)\mathcal{A}]\!]^y_\emptyset$	10 T13.70
12.	$(\forall x \le y)\mathcal{A}^y_\emptyset \to Prvt[\![(\forall x \le y)\mathcal{A}]\!]^y_\emptyset$	5-11 →I
13.	$((\forall x \le y)\mathcal{A} \to Prvt[\![(\forall x \le y)\mathcal{A}]\!])^y_\emptyset$	12 abv

For (5) and (10) it is important that y in a bound quantifier of the $\Sigma^\star$ formula does not appear in $\mathcal{A}$. Now the inductive stage.

14.	$\mathcal{A}^x_{Sy} \to Prvt[\![\mathcal{A}^x_{Sy}]\!]$	by assp
15.	$(\forall x \le Sy)\mathcal{A} \leftrightarrow (\forall x \le y)\mathcal{A} \wedge \mathcal{A}^x_{Sy}$	with T13.13o
16.	$Prvt[\![((\forall x \le y)\mathcal{A} \wedge \mathcal{A}^x_{Sy}) \to (\forall x \le Sy)\mathcal{A}]\!]$	15 T13.68
17.	$(\forall x \le y)\mathcal{A} \to Prvt[\![(\forall x \le y)\mathcal{A}]\!]$	A (g →I)
18.	$((\forall x \le y)\mathcal{A} \wedge \mathcal{A}^x_{Sy}) \to Prvt[\![(\forall x \le y)\mathcal{A} \wedge \mathcal{A}^x_{Sy}]\!]$	14,17 as for ∧
19.	$(\forall x \le Sy)\mathcal{A}$	A (g →I)
20.	$(\forall x \le y)\mathcal{A} \wedge \mathcal{A}^x_{Sy}$	15,19 ↔E
21.	$Prvt[\![(\forall x \le y)\mathcal{A} \wedge \mathcal{A}^x_{Sy}]\!]$	18,20 →E
22.	$Prvt[\![(\forall x \le y)\mathcal{A} \wedge \mathcal{A}^x_{Sy}]\!] \to Prvt[\![(\forall x \le Sy)\mathcal{A}]\!]$	16 T13.69
23.	$Prvt[\![(\forall x \le Sy)\mathcal{A}]\!]$	22,21 →E
24.	$Prvt[\![(\forall x \le y)\mathcal{A}]\!]^y_{Sy}$	23, T13.70
25.	$(\forall x \le Sy)\mathcal{A} \to Prvt[\![(\forall x \le y)\mathcal{A}]\!]^y_{Sy}$	19-24 →I
26.	$((\forall x \le y)\mathcal{A} \to Prvt[\![(\forall x \le y)\mathcal{A}]\!])^y_{Sy}$	25 abv
27.	$((\forall x \le y)\mathcal{A} \to Prvt[\![(\forall x \le y)\mathcal{A}]\!]) \to ((\forall x \le y)\mathcal{A} \to Prvt[\![(\forall x \le y)\mathcal{A}]\!])^y_{Sy}$	17-26 →I
28.	$(\forall x \le y)\mathcal{A} \to Prvt[\![(\forall x \le y)\mathcal{A}]\!]$	13,27 IN

So PA $\vdash (\forall x \le y)\mathcal{A} \to Prvt[\![(\forall x \le y)\mathcal{A}]\!]$.

Indct: For any $\Sigma^\star$ formula $\mathcal{P}$, PA $\vdash \mathcal{P} \to Prvt[\![\mathcal{P}]\!]$.

Now it is a simple matter to pull together our results into the third derivability condition.

T13.72. For any formula $\mathcal{P}$, PA $\vdash \Box\mathcal{P} \to \Box\Box\mathcal{P}$

Consider any formula $\mathcal{P}$ and the Σ_1 sentence $\Box\mathcal{P}$. By T13.62, there is a $(\Box\mathcal{P})^\star$ such that PA $\vdash \Box\mathcal{P} \leftrightarrow (\Box\mathcal{P})^\star$. By T13.71, PA $\vdash (\Box\mathcal{P})^\star \rightarrow$ $Prvt[\![(\Box\mathcal{P})^\star]\!]$. Reason as follows.

1.	$(\Box\mathcal{P})^\star \rightarrow Prvt[\![(\Box\mathcal{P})^\star]\!]$	T13.71
2.	$\Box\mathcal{P} \leftrightarrow (\Box\mathcal{P})^\star$	T13.62
3.	$Prvt[\![(\Box\mathcal{P})^\star \rightarrow \Box\mathcal{P}]\!]$	2 T13.68
4.	$Prvt[\![(\Box\mathcal{P})^\star]\!] \rightarrow Prvt[\![\Box\mathcal{P}]\!]$	3 T13.69
5.	$\Box\mathcal{P} \rightarrow Prvt[\![\Box\mathcal{P}]\!]$	2,1,4 HS

So PA $\vdash \Box\mathcal{P} \rightarrow Prvt[\![\Box\mathcal{P}]\!]$; and since $\Box\mathcal{P}$ is a sentence, this is to say, PA $\vdash \Box\mathcal{P} \rightarrow Prvt(\overline{\ulcorner\Box\mathcal{P}\urcorner})$; which is to say, PA $\vdash \Box\mathcal{P} \rightarrow \Box\Box\mathcal{P}$.

So, at long last, we have a demonstration of D3 and so, given demonstration of the other conditions, of Gödel's second incompleteness theorem.

It is worth reflecting a bit on what we have accomplished. Beginning in section 13.2 we saw how the second theorem follows from the derivability conditions. The first is easy, the others not. In section 13.3 we introduced the idea of definition in PA and demonstrated that PA defines (friendly) recursive functions. 13.4 moves to demonstration of the second condition. The basic idea is straightforward: To show $\Box(\mathcal{P} \rightarrow \mathcal{Q}) \rightarrow (\Box\mathcal{P} \rightarrow \Box\mathcal{Q})$, suppose $\Box(\mathcal{P} \rightarrow \mathcal{Q})$ and $\Box\mathcal{P}$; then there are j and k such that $\textsc{prft}(\mathsf{j}, \ulcorner\mathcal{P} \rightarrow \mathcal{Q}\urcorner)$ and $\textsc{prft}(\mathsf{k}, \ulcorner\mathcal{P}\urcorner)$; so $\mathsf{l} = \mathsf{j} \star \mathsf{k} \star 2^{\ulcorner\mathcal{Q}\urcorner}$ numbers a proof of $\mathcal{Q}$. But considerable effort is expended to show that PA has the resources for the relevant results. And we have just completed discussion of the third condition. If you have gotten this far you have seen the theorem proved — or at least how it is proved. Thus you have progressed considerably beyond the initial argument from the derivability conditions. One reason why it is typical to bypass the details is that there are *so many* details — not all themselves mathematically significant. Still, it is interesting to see *how* reasoning from chapter 12 is reflected in PA for the second theorem.

E13.52. Complete the demonstration of T13.71 by completing the remaining cases.

13.6 Reflections on the theorem

We conclude this chapter with a couple final reflections and consequences on our results.

13.6.1 Consistency sentences

As is typical for demonstrations of Gödel’s second theorem, we have let *Cont* be $\sim Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner})$. But other sentences would do as well. So, where $\mathcal{T}$ is any theorem of T, we might let $Cont_a$ be $\sim Prvt(\overline{\ulcorner \sim\mathcal{T} \urcorner})$. In particular, we might simply consider the case where $\sim\mathcal{T}$ is (equivalent to) $\bot$ and set $Cont_a = \sim Prvt(\overline{\ulcorner \bot \urcorner})$. Then it is easy to see that PA $\vdash$ $Cont \leftrightarrow Cont_a$.

> PA $\vdash \emptyset = S\emptyset \leftrightarrow \bot$; so with D1, PA $\vdash Prvt(\overline{\ulcorner \emptyset = S\emptyset \leftrightarrow \bot \urcorner})$; so with D2, PA $\vdash Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner}) \leftrightarrow Prvt(\overline{\ulcorner \bot \urcorner})$; and contraposing, PA $\vdash Cont \leftrightarrow Cont_a$.

Again, one might let $Cont_b = \sim\exists x(Prvt(x) \wedge \overline{Prvt}(x))$, where $\overline{Prvt}(x))$ just in case there is a proof of the negation of the formula with Gödel number x. Then T is consistent just in case there is no proof of a formula and its negation. Again, PA $\vdash Cont \leftrightarrow Cont_b$. This time the result requires a bit more work.

We show $Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner}) \leftrightarrow \exists x(Prvt(x) \wedge \overline{Prvt}(x))$ and contrapose. First from left to right: Since a contradiction implies anything, PA $\vdash \emptyset = S\emptyset \rightarrow A$ and PA $\vdash \emptyset = S\emptyset \rightarrow \sim A$. Reason as follows.

1.	$\emptyset = S\emptyset \rightarrow A$	thrm
2.	$\emptyset = S\emptyset \rightarrow \sim A$	thrm
3.	$Prvt(\overline{\ulcorner \emptyset = S\emptyset \rightarrow A \urcorner})$	1 D1
4.	$Prvt(\overline{\ulcorner \emptyset = S\emptyset \rightarrow \sim A \urcorner})$	2 D1
5.	$Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner})$	A ($g \rightarrow$I)
6.	$Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner}) \rightarrow Prvt(\overline{\ulcorner A \urcorner})$	3 D2
7.	$Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner}) \rightarrow Prvt(\overline{\ulcorner \sim A \urcorner})$	4 D2
8.	$Prvt(\overline{\ulcorner A \urcorner}) \wedge Prvt(\overline{\ulcorner \sim A \urcorner})$	5,6,7
9.	$\exists x(Prvt(x) \wedge \overline{Prvt}(x))$	8 $\exists$I
10.	$Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner}) \rightarrow \exists x(Prvt(x) \wedge \overline{Prvt}(x))$	7-9 $\rightarrow$I

So PA $\vdash Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner}) \rightarrow \exists x(Prvt(x) \wedge \overline{Prvt}(x))$.

The other direction is not much more difficult. Insofar as the right-hand side is existentially quantified we shall not be able to depend on capture for any particular sentence. However we can reason with free variables. Working up from the bottom of a tree for $\mathcal{P}$ say its *(sententially) basic* subformulas are the first subformulas without a truth functional main operator. Then where where $\mathcal{P}$ has basic subformulas $\mathcal{A}_1 \ldots \mathcal{A}_n$, let $A_1^* \ldots A_n^*$ be some variables $a_1 \ldots a_n$; $\sim\mathcal{P}^*$ is $\mathit{neg}(p)$; and $(\mathcal{P} \rightarrow \mathcal{Q})^*$ is $\mathit{cnd}(p, q)$. Then where $\vdash_{ADs} \mathcal{P}$, we shall be able to show PA $\vdash \mathbb{W}\mathit{ff}(a_1) \wedge \ldots \wedge \mathbb{W}\mathit{ff}(a_n) \rightarrow \mathbb{P}\mathit{rvt}(\mathcal{P}^*)$. Though we shall not go through all the details here, it is simple enough to see how the argument goes: The argument is an induction (of a sort we have seen before). Given an *ADs* derivation of $\mathcal{P}$, under the assumption $\mathbb{W}ff(a) \wedge \ldots \wedge \mathbb{W}ff(b)$, corresponding to any axiom $\mathcal{A}$, we may use the definition to get $\mathbb{A}xiom(\mathcal{A}^*)$ and then T13.57i for $\mathbb{P}rvt(\mathcal{A}^*)$. Corresponding to an application of MP to some $\mathcal{P}$ and $\mathcal{P} \rightarrow \mathcal{Q}$, use T13.54 to convert $\mathbb{P}rvt(\mathbb{c}nd(\mathcal{P}^*, \mathcal{Q}^*))$ to $\mathbb{P}rvt(\mathcal{P}^*) \rightarrow \mathbb{P}rvt(\mathcal{Q}^*)$ and apply MP. As an example, compare the following lines of the sort we might have obtained in chapter 3,

1.	$A \rightarrow (B \rightarrow A)$	A1
2.	$[A \rightarrow (B \rightarrow A)] \rightarrow [(A \rightarrow B) \rightarrow (A \rightarrow A)]$	A2
3.	$(A \rightarrow B) \rightarrow (A \rightarrow A)$	1,2 MP

and the derived version,

0.	$\mathbb{W}ff(a) \wedge \mathbb{W}ff(b)$	A
1.1.	$\mathbb{A}xiom(\mathbb{c}nd(a, \mathbb{c}nd(b, a)))$	0 def
1.	$\mathbb{P}rvt(\mathbb{c}nd(a, \mathbb{c}nd(b, a)))$	1.1 T13.57i
2.1.	$\mathbb{A}xiom(\mathbb{c}nd(\mathbb{c}nd[a, \mathbb{c}nd(b, a)], \mathbb{c}nd[\mathbb{c}nd(a, b), \mathbb{c}nd(a, a)]))$	0 def
2.	$\mathbb{P}rvt(\mathbb{c}nd(\mathbb{c}nd[a, \mathbb{c}nd(b, a)], \mathbb{c}nd[\mathbb{c}nd(a, b), \mathbb{c}nd(a, a)]))$	2.1 T13.57i
3.1.	$\mathbb{P}rvt(\mathbb{c}nd[a, \mathbb{c}nd(b, a)]) \rightarrow \mathbb{P}rvt(\mathbb{c}nd[\mathbb{c}nd(a, b), \mathbb{c}nd(a, a)])$	2 T13.54
3.	$\mathbb{P}rvt(\mathbb{c}nd[\mathbb{c}nd(a, b), \mathbb{c}nd(a, a)])$	1,3.1 MP
4.	$\mathbb{W}ff(a) \wedge \mathbb{W}ff(b) \rightarrow \mathbb{P}rvt(\mathbb{c}nd[\mathbb{c}nd(a, b), \mathbb{c}nd(a, a)])$	0 - 3 DT

And similarly we might show the correlate to T3.9, $\vdash \sim\mathcal{A} \rightarrow (\mathcal{A} \rightarrow \mathcal{B})$, which we record as a theorem.

T13.73. PA $\vdash \mathbb{W}ff(a) \wedge \mathbb{W}ff(b) \rightarrow \mathbb{P}rvt(\mathbb{c}nd[\mathbb{n}eg(a), \mathbb{c}nd(a, b)])$.

But then we may reason as follows.

1.	$\mathbb{W}ff(\ulcorner \emptyset = S\emptyset \urcorner)$	cap
2.	$\exists x[Prvt(x) \wedge \overline{Prvt}(x)]$	A (g →I)
3.	$Prvt(j) \wedge \overline{Prvt}(j)$	A (g 2∃E)
4.	$\mathbb{W}ff(j)$	3 T13.53
5.	$\mathbb{P}rvt(\mathbb{c}nd[\mathbb{n}eg(j), \mathbb{c}nd(j, \overline{\ulcorner \emptyset = S\emptyset \urcorner})])$	1,4 T13.73
6.	$\mathbb{P}rvt(\mathbb{n}eg(j)) \rightarrow \mathbb{P}rvt(\mathbb{c}nd(j, \overline{\ulcorner \emptyset = S\emptyset \urcorner}))$	5 T13.54
7.	$\mathbb{P}rvt(\mathbb{c}nd(j, \overline{\ulcorner \emptyset = S\emptyset \urcorner}))$	3,6 ∧E,→E
8.	$\mathbb{P}rvt(j) \rightarrow \mathbb{P}rvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner})$	7 T13.54
9.	$Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner})$	3,8 ∧E,→E
10.	$Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner})$	2,3-9 ∃E
11.	$\exists x[Prvt(x) \wedge \overline{Prvt}(x)] \rightarrow Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner})$	2-10 →I

So PA $\vdash \exists x[Prvt(x) \wedge \overline{Prvt}(x)] \rightarrow Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner})$. Again note that we reason with free variables under the assumption for ∃E.

Putting the parts together, PA $\vdash Prvt(\overline{\ulcorner \emptyset = S\emptyset \urcorner}) \leftrightarrow \exists x(Prvt(x) \wedge \overline{Prvt}(x))$; and contraposing, PA $\vdash Cont \leftrightarrow Cont_b$. So, to this extent, it does not matter which version of the consistency statement we select. Underlying the point that these different statements are equivalent is that anything follows from a contradiction — so that the one follows from the others.[13]

Having proved PA $\nvdash Cont$, we therefore have PA $\nvdash Cont_a$ and PA $\nvdash Cont_b$. These are particular sentences which, like $\mathscr{G}$, are unprovable. And, now that we have the derivability conditions, with T13.11, neither are their negations provable. They have special interest because because each "says" that PA is consistent.

Still, it is worth asking whether there is some different sentence to express the consistency of PA such that *it* would be provable. Consider, for example a trick related to the Rosser sentence,

$$Prft_c(x, y) =_{\text{def}} Prft(x, y) \wedge (\forall v \leq x){\sim}Prft(v, \overline{\ulcorner \emptyset = S\emptyset \urcorner})$$

So $Prft_c(x, y)$ requires a measure of consistency: it says x numbers a proof of the formula numbered y and no proof numbered less than or equal to x demonstrates inconsistency ($\emptyset = \overline{1}$). Then so long as PA *is* consistent $Prft_c(x, y)$ continues to capture $\textsc{prft}(\mathsf{x}, \mathsf{y})$.

(i) Suppose $\langle \mathsf{m}, \mathsf{n} \rangle \in \textsc{prft}$. (a) By capture, PA $\vdash Prft(\overline{\mathsf{m}}, \overline{\mathsf{n}})$. And (b), since PA is consistent, there is no proof of a contradiction in PA and again by capture, PA $\vdash {\sim}Prft(\overline{0}, \overline{\ulcorner \emptyset = S\emptyset \urcorner})$; PA $\vdash {\sim}Prft(\overline{1}, \overline{\ulcorner \emptyset = S\emptyset \urcorner})$ and ... and PA $\vdash {\sim}Prft(\overline{\mathsf{m}}, \overline{\ulcorner \emptyset = S\emptyset \urcorner})$; so with T8.21, PA $\vdash (\forall v \leq \overline{\mathsf{m}}){\sim}Prft(v, \overline{\ulcorner \emptyset = S\emptyset \urcorner})$; so PA $\vdash Prft_c(\overline{\mathsf{m}}, \overline{\mathsf{n}})$.

(ii) Suppose $\langle \mathsf{m}, \mathsf{n} \rangle \notin \textsc{prft}$; then by capture, PA $\vdash {\sim}Prft(\overline{\mathsf{m}}, \overline{\mathsf{n}})$. So PA $\vdash {\sim}[Prft(\overline{\mathsf{m}}, \overline{\mathsf{n}}) \wedge (\forall v \leq \overline{\mathsf{m}}){\sim}Prft(v, \overline{\ulcorner \emptyset = S\emptyset \urcorner})]$, which is to say PA $\vdash {\sim}Prft_c(\overline{\mathsf{m}}, \overline{\mathsf{n}})$.

And, with T12.6, $Prft_c(x, y)$ expresses $\textsc{prft}(\mathsf{x}, \mathsf{y})$ as well. Given this, set $Prvt_c(y) =_{\text{def}} \exists x Prft_c(x, y)$, and $Cont_c =_{\text{def}} {\sim}Prvt_c(\overline{\ulcorner \emptyset = S\emptyset \urcorner})$. The idea, then is that $Cont_c$ just in case PA is consistent.

But $Prvt_c$ is designed so that $Prvt_c(\overline{\ulcorner \emptyset = S\emptyset \urcorner})$ is impossible — $Prvt_c(\overline{\ulcorner \emptyset = S\emptyset \urcorner})$ requires an x that numbers a proof of $\emptyset = S\emptyset$ such that no $v \leq x$ numbers a proof of $\emptyset = S\emptyset$. This is impossible. So,

[13] This equivalence breaks down in a non-classical logic which blocks *ex falso quodlibet*, the principle that from a contradiction anything follows. So, for example, in relevant logic, it might be that there is some A such that $T \vdash A \wedge {\sim}A$ but $T \nvdash \emptyset = S\emptyset$. See Priest, *Non-Classical Logics* for an introduction to these matters.

1.	$\exists x[Prft(x, \overline{\ulcorner \emptyset = S\emptyset \urcorner}) \wedge (\forall v \leq x)\sim Prft(v, \overline{\ulcorner \emptyset = S\emptyset \urcorner})]$	A (c, $\sim$I)
2.	$Prft(j, \overline{\ulcorner \emptyset = S\emptyset \urcorner}) \wedge (\forall v \leq j)\sim Prft(v, \overline{\ulcorner \emptyset = S\emptyset \urcorner})$	A (c 1$\exists$E)
3.	$Prft(j, \overline{\ulcorner \emptyset = S\emptyset \urcorner})$	2 $\wedge$E
4.	$(\forall v \leq j)\sim Prft(v, \overline{\ulcorner \emptyset = S\emptyset \urcorner})$	2 $\wedge$E
5.	$j \leq j$	with T13.13m
6.	$\sim Prft(j, \overline{\ulcorner \emptyset = S\emptyset \urcorner})$	4,5 ($\forall$E)
7.	$\perp$	3,6 $\perp$I
8.	$\perp$	1,2-7 $\exists$E
9.	$\sim\exists x[Prft(x, \overline{\ulcorner \emptyset = S\emptyset \urcorner}) \wedge (\forall v \leq x)\sim Prft(v, \overline{\ulcorner \emptyset = S\emptyset \urcorner})]$	1-8 $\sim$I

So PA $\vdash \sim\exists x[Prft(x, \overline{\ulcorner \emptyset = S\emptyset \urcorner}) \wedge (\forall v \leq x)\sim Prft(v, \overline{\ulcorner \emptyset = S\emptyset \urcorner})]$ which is to say PA $\vdash Cont_c$. This works because $Prft_c$ builds in from the start that nothing numbers a proof of $\emptyset = S\emptyset$.

Intuitively, so long as PA is consistent, $Prft_c$ works just fine. But if PA is not consistent, then it no longer tracks with proof. Similarly, if PA is consistent, $Cont_c$ plausibly "says" PA is consistent. But if PA is inconsistent then it no longer tracks with consistency. So its provability is, in this sense, uninteresting.

Insofar as $Cont_c$ is provable it must be that $Prvt_c$ fails one or more of the derivability conditions. To see how this might be, suppose PA is inconsistent and proofs are ordered according to their Gödel numbers as follows,

$$\mathcal{A} \rightarrow \mathcal{B} \qquad \mathcal{A} \qquad \emptyset = S\emptyset \qquad \mathcal{B}$$

Then PA $\vdash Prvt(\overline{\ulcorner \mathcal{B} \urcorner})$. However we get PA $\vdash Prvt_c(\overline{\ulcorner \mathcal{A} \rightarrow \mathcal{B} \urcorner})$ and PA $\vdash Prvt_c(\overline{\ulcorner \mathcal{A} \urcorner})$ but, insofar as the proof of $\mathcal{B}$ is numbered greater than the proof of $\emptyset = S\emptyset$, PA $\nvdash Prvt_c(\overline{\ulcorner \mathcal{B} \urcorner})$. In this case, D2 fails, so that our main argument to show PA $\nvdash$ *Cont* does not apply to $Cont_c$.

13.6.2 Löb's Theorem

If T is a recursively axiomatized theory extending Q, by the diagonal lemma there is a sentence $\mathcal{H}$, of which $\mathcal{G}$ is a sample, such that $T \vdash \mathcal{H} \leftrightarrow \sim Prvt(\overline{\ulcorner \mathcal{H} \urcorner})$ — that is, $T \vdash \mathcal{H} \leftrightarrow \sim\Box\mathcal{H}$. We have seen that such a formula $\mathcal{H}$ is not provable. But, of course, by the diagonal lemma, there is another sentence $\mathcal{H}$ such that $T \vdash \mathcal{H} \leftrightarrow \Box\mathcal{H}$. In a brief note, "A Problem Concerning Provability" L. Henkin asks whether this $\mathcal{H}$ is provable. Supposing the first is analogous to the liar, 'this sentence is not true', the latter is like the truth-teller, 'this sentence is true'. An answer to Henkin's question follows immediately from Löb's theorem.

T13.74. Suppose T is a recursively axiomatized theory for which the derivability conditions D1 - D3 hold and $T \vdash \Box\mathscr{P} \to \mathscr{P}$, then $T \vdash \mathscr{P}$. *Löb's Theorem.*

Suppose T is a recursively axiomatized theory for which the derivability conditions hold and $T \vdash \Box\mathscr{P} \to \mathscr{P}$. Then the diagonal lemma obtains as well. Consider $Prvt(y) \to \mathscr{P}$; this is an expression of the sort $\mathscr{F}(y)$ to which the diagonal lemma applies; so by the diagonal lemma there is some $\mathscr{H}$ such that $T \vdash \mathscr{H} \leftrightarrow (Prvt(\overline{\ulcorner \mathscr{H} \urcorner}) \to \mathscr{P})$ — that is, $T \vdash \mathscr{H} \leftrightarrow (\Box\mathscr{H} \to \mathscr{P})$. Now reason as follows.

1.	$\Box\mathscr{P} \to \mathscr{P}$	P
2.	$\mathscr{H} \leftrightarrow (\Box\mathscr{H} \to \mathscr{P})$	diag lemma
3.	$[\mathscr{H} \to (\Box\mathscr{H} \to \mathscr{P})] \wedge [(\Box\mathscr{H} \to \mathscr{P}) \to \mathscr{H}]$	2 abv
4.	$\mathscr{H} \to (\Box\mathscr{H} \to \mathscr{P})$	3 with T3.20
5.	$\Box[\mathscr{H} \to (\Box\mathscr{H} \to \mathscr{P})]$	4 D1
6.	$\Box[\mathscr{H} \to (\Box\mathscr{H} \to \mathscr{P})] \to [\Box\mathscr{H} \to \Box(\Box\mathscr{H} \to \mathscr{P})]$	D2
7.	$\Box\mathscr{H} \to \Box(\Box\mathscr{H} \to \mathscr{P})$	6,5 MP
8.	$\Box(\Box\mathscr{H} \to \mathscr{P}) \to (\Box\Box\mathscr{H} \to \Box\mathscr{P})$	D2
9.	$\Box\mathscr{H} \to (\Box\Box\mathscr{H} \to \Box\mathscr{P})$	7,8 T3.2
10.	$[\Box\mathscr{H} \to (\Box\Box\mathscr{H} \to \Box\mathscr{P})] \to [(\Box\mathscr{H} \to \Box\Box\mathscr{H}) \to (\Box\mathscr{H} \to \Box\mathscr{P})]$	A2
11.	$(\Box\mathscr{H} \to \Box\Box\mathscr{H}) \to (\Box\mathscr{H} \to \Box\mathscr{P})$	10,9 MP
12.	$\Box\mathscr{H} \to \Box\Box\mathscr{H}$	D3
13.	$\Box\mathscr{H} \to \Box\mathscr{P}$	11,12 MP
14.	$\Box\mathscr{H} \to \mathscr{P}$	13,1 T3.2
15.	$(\Box\mathscr{H} \to \mathscr{P}) \to \mathscr{H}$	3 with T3.19
16.	$\mathscr{H}$	15,14 MP
17.	$\Box\mathscr{H}$	16 D1
18.	$\mathscr{P}$	14,17 MP

So $T \vdash \mathscr{P}$. Now return to our original question. Suppose $T \vdash \mathscr{H} \leftrightarrow \Box\mathscr{H}$; then $T \vdash \Box\mathscr{H} \to \mathscr{H}$; so by Löb's theorem, $T \vdash \mathscr{H}$. So if T proves $\mathscr{H} \leftrightarrow \Box\mathscr{H}$, then T proves $\mathscr{H}$.

Löb's theorem is at least surprising! From soundness, if $\mathscr{P}$ is provable then $\mathscr{P}$, so that $\Box\mathscr{P} \to \mathscr{P}$ is true. One might think that PA would "believe" in its soundness so that any such sentence would be provable. But from the theorem, if PA $\nvdash \mathscr{P}$, then PA $\nvdash \Box\mathscr{P} \to \mathscr{P}$. So in any case when PA $\nvdash \mathscr{P}$, PA does not "know" about its own souncness with respect to $\mathscr{P}$. Observe that insofar as $\Box\mathscr{P} \to \mathscr{P}$ is true, for any case where PA $\nvdash \mathscr{P}$ we have here another sentence true but not provable.

Löb's theorem depends upon the derivability conditions. Thus perhaps it is not surprising that Löb's theorem both results in and results from Gödel's second theorem: First, the second theorem follows from Löb's result.

> Suppose PA is consistent and PA $\vdash \sim\Box(\overline{0} = \overline{1})$; then with $\vee$I and Impl, PA $\vdash \Box(\overline{0} = \overline{1}) \to \overline{0} = \overline{1}$; so by Löb's theorem PA $\vdash \overline{0} = \overline{1}$: but PA $\vdash \overline{0} \neq \overline{1}$; so PA is inconsistent. Reject the assumption, PA $\nvdash \sim\Box(\overline{0} = \overline{1})$, which is to say PA $\nvdash$ *Conpa*.

And Löb's theorem follows from the second theorem with consistency.

> Suppose PA is consistent and PA $\vdash \Box\mathcal{P} \to \mathcal{P}$. Let $\sim\mathcal{P}$ be an axiom of an extended theory PA$'$. Then PA$' \vdash \Box\mathcal{P} \to \mathcal{P}$ and PA$' \vdash \sim\mathcal{P}$; so PA$' \vdash \sim\Box\mathcal{P}$; but since it extends PA, PA$' \vdash \emptyset \neq \overline{1}$, so PA$' \vdash \emptyset = \overline{1} \to \mathcal{P}$ and by D1 with D2, PA$' \vdash \Box(\emptyset = \overline{1}) \to \Box\mathcal{P}$, so PA$' \vdash \sim\Box\mathcal{P} \to \sim\Box(\emptyset = \overline{1})$, which is to say PA$' \vdash \sim\Box\mathcal{P} \to$ *Cont*$'$; so PA$' \vdash$ *Cont*$'$. But by the second theorem, if PA$'$ is consistent, then PA$' \nvdash$ *Cont*$'$; so PA$'$ is not consistent. But by T10.6 if PA is consistent and PA $\nvdash \mathcal{P}$ then PA $\cup \{\sim\mathcal{P}\}$ and so PA$'$ is consistent; this is impossible: so PA $\vdash \mathcal{P}$.

And we are in a position to make some applications to the logic of provability. With $\Box\mathcal{P}$ for *Prvt*$(\overline{\ulcorner\mathcal{P}\urcorner})$ by the derivability conditions we have shown that K4 is sound in the sense that if $\vdash_{K4} \mathcal{P}$, then PA $\vdash \mathcal{P}$. It is natural to ask if the converse is true, whether K4 is complete in the sense that if PA $\vdash \mathcal{P}$ then $\vdash_{K4} \mathcal{P}$. But K4 is not so complete. To see this let K4LR be like K4 but with the addition of the *Löb rule*,

LR $\mathcal{P}$ follows from $\Box\mathcal{P} \to \mathcal{P}$

By Löb's theorem, K4LR is sound, so that if $\vdash_{K4LR} \mathcal{P}$, then PA $\vdash \mathcal{P}$. But by its appeal to the diagonal lemma, the proof of Löb's theorem is not entirely contained within K4. And, in fact, K4LR has theorems that that are not theorems of K4. In particular, $\vdash_{K4LR} \Box(\Box\mathcal{P} \to \mathcal{P}) \to \Box\mathcal{P}$,

1.	$\Box[\Box(\Box\mathcal{P} \to \mathcal{P}) \to \Box\mathcal{P}] \to [\Box\Box(\Box\mathcal{P} \to \mathcal{P}) \to \Box\Box\mathcal{P}]$	D2
2.	$\Box(\Box\mathcal{P} \to \mathcal{P}) \to (\Box\Box\mathcal{P} \to \Box\mathcal{P})$	D2
3.	$\Box(\Box\mathcal{P} \to \mathcal{P}) \to \Box\Box(\Box\mathcal{P} \to \mathcal{P})$	D3
4.	$\Box[\Box(\Box\mathcal{P} \to \mathcal{P}) \to \Box\mathcal{P}] \to [\Box(\Box\mathcal{P} \to \mathcal{P}) \to \Box\mathcal{P}]$	1,2,3 T6.4
5.	$\Box(\Box\mathcal{P} \to \mathcal{P}) \to \Box\mathcal{P}$	4 LR

From this, PA $\vdash \Box(\Box\mathcal{P} \to \mathcal{P}) \to \Box\mathcal{P}$. But by E13.55 just below, $\nvDash_{K4} \Box(\Box\mathcal{P} \to \mathcal{P}) \to \Box\mathcal{P}$ so that $\nvdash_{K4} \Box(\Box\mathcal{P} \to \mathcal{P}) \to \Box\mathcal{P}$. So PA proves something that K4 does not. So K4 is not complete in the sense that if PA $\vdash \mathcal{P}$ then $\vdash_{K4} \mathcal{P}$. In fact K4LR is complete — but that is a discussion for another place (see Boolos, *The Logic of Provability*).[14]

E13.53. Provide the argument to show that if $\vdash_{ADs} \mathcal{P}$, then PA $\vdash \mathbb{W}\mathit{ff}(a_1) \wedge \ldots \wedge \mathbb{W}\mathit{ff}(a_n) \rightarrow \mathbb{P}\mathit{rvt}(\mathcal{P}^*)$.

E13.54. In the middle of a restless night dreaming about PA you bolt out of bed. "Eureka!" you cry, "I have discovered a simple means for proving the consistency of arithmetic." Your idea is to show PA $\vdash \Box(\overline{0} = \overline{1}) \rightarrow \overline{0} = \overline{1}$; then from PA $\vdash \overline{0} \neq \overline{1}$ it follows that PA $\vdash \sim\Box(\overline{0} = \overline{1})$ and so that PA $\vdash$ *Conpa*. Explain why this is one of those ideas that seems better at night than in the cold light of day.

E13.55. For those with some knowledge of semantics for modal logic: K4 is the normal modal logic with a transitive access relation. Find a K4 interpretation to show $\nvDash_{K4} \Box(\Box\mathcal{P} \rightarrow \mathcal{P}) \rightarrow \Box\mathcal{P}$. Hint: Your interpretation will have infinitely many worlds.

E13.56. Reasoning for Löb's theorem is closely related to *Curry's paradox*. For this read $\Box\mathcal{P}$ to say that '$\mathcal{P}$' is *true* rather than that it is provable. Consider some false sentence $\mathcal{F}$, as 'I have two heads'. Let $\mathcal{C}$ be the sentence, "If this sentence is true then $\mathcal{F}$" — that is, "If '$\mathcal{C}$' is true then $\mathcal{F}$." Take as given,

D1′.	if $\mathcal{P}$, then $\Box\mathcal{P}$	truth analog to D1
D2′.	$\Box(\mathcal{P} \rightarrow \mathcal{Q}) \rightarrow (\Box\mathcal{P} \rightarrow \Box\mathcal{Q})$	truth analog to D2
D3′.	$\Box\mathcal{P} \rightarrow \Box\Box\mathcal{P}$	truth analog to D3

And as premises,

1′.	$\Box\mathcal{F} \rightarrow \mathcal{F}$	from nature of truth (Tarski's schema T)
2′.	$\mathcal{C} \leftrightarrow (\Box\mathcal{C} \rightarrow \mathcal{F})$	from the definition of $\mathcal{C}$

Use these principles to show that you have two heads. Reflect on this result: When $\Box$ indicates provability, we are in a position to deny (1) that PA $\vdash \Box\mathcal{P} \rightarrow \mathcal{P}$ when PA $\vdash \sim\mathcal{P}$. But it may seem less plausible to deny (1′). Supposing you do not have two heads, what do you think is wrong?

[14] K4LR is equivalent to a logic (GL) like K4 without the Löb rule but with D3 replaced by $\Box(\Box\mathcal{P} \rightarrow \mathcal{P}) \rightarrow \Box\mathcal{P}$. This is the usual form for the logic of provability. We have just seen that K4LR proves anything proved by GL.

E13.57. For each of the following concepts, explain in an essay of about two pages, so that (college freshman) Hannah could understand. In your essay, you should (i) identify the objects to which the concept applies, (ii) give and explain the definition, and give and explicate examples (iii) where the concept applies, and (iv) where it does not. Your essay should exhibit an understanding of methods from the text.

a. The essential elements contributing to the proof (from this chapter) of the incompleteness of arithmetic.

b. The essential elements contributing to the demonstration that PA does not prove its own consistency

Final theorems of chapter 13

T13.55. Further results for $\mathbb{T}ermsub$.

T13.56. Further results for $\mathbb{F}ormsub$.

T13.57. Results for Gen and A4.

T13.58. Results for iterated substitutions.

T13.59. For any $\mathcal{P}$ of the form $t = x$, there is a $\mathcal{P}^\star$ such that PA $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^\star$.

T13.60. For any Δ_0 formula $\mathcal{P}$, there is a normal formula $\mathcal{P}^*$ such that $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^*$.

T13.61. For any Δ_0 formula $\mathcal{P}$ there is a $\Sigma^\star$ formula $\mathcal{P}^\star$ such that PA $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^\star$.

T13.62 For any Σ_1 formula $\mathcal{P}$ there is a $\Sigma^\star$ formula $\mathcal{P}^\star$ such that PA $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^\star$.

T13.63 PA $\vdash \mathbb{W}\!f\!f(sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}))$.

T13.64 For arbitrary $\vec{u}$, $\vec{v}$, $sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{x}_1} \ldots x_{\mathsf{x}_\mathsf{i}}, \vec{u}) = sub_i(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{x}_1} \ldots x_{\mathsf{x}_\mathsf{i}}, \vec{v})$.

T13.65 For any i, PA $\vdash$ $\mathbb{s}ub_{i+1}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{a}}, x_{\mathsf{y}_1} \ldots x_{\mathsf{y}_\mathsf{n}})$ $=$ $\mathbb{s}ub_{i+1}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y}_1} \ldots x_{\mathsf{y}_\mathsf{i}}, x_{\mathsf{a}}, x_{\mathsf{y}_{(\mathsf{i}+1)}} \ldots x_{\mathsf{y}_\mathsf{n}})$.

T13.66 If x_{a} is not free in $\mathcal{P}$, then PA $\vdash \mathbb{s}ub_{i+1}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y}_1} \ldots x_{\mathsf{y}_\mathsf{i}}, x_{\mathsf{a}}, x_{\mathsf{y}_{(\mathsf{i}+1)}} \ldots x_{\mathsf{y}_\mathsf{n}}) = \mathbb{s}ub_i(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y}_1} \ldots x_{\mathsf{y}_\mathsf{i}}, x_{\mathsf{a}}, x_{\mathsf{y}_{(\mathsf{i}+1)}} \ldots x_{\mathsf{y}_\mathsf{n}})$

T13.67 If the variables of $\vec{y}$ and $\vec{z}$ are ordered by their subscripts and $\vec{y}$ and $\vec{z}$ are the same except that $\vec{z}$ includes some variables not in $\vec{y}$ (and so not free in $\mathcal{P}$), then PA $\vdash sub(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}) = sub(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{z})$.

T13.68 If PA $\vdash \mathcal{P}$, then PA $\vdash Prvt[\![\mathcal{P}]\!]$ — analog to D1

T13.69 PA $\vdash Prvt[\![\mathcal{P} \to \mathcal{Q}]\!] \to (Prvt[\![\mathcal{P}]\!] \to Prvt[\![\mathcal{Q}]\!])$ — analog to D2

T13.70 If t is one of $\emptyset$, y or Sy, then PA $\vdash Prvt[\![\mathcal{P}^x_t]\!] \leftrightarrow Prvt[\![\mathcal{P}]\!]^x_t$.

T13.71 For any $\Sigma^\star$ formula $\mathcal{P}$, PA $\vdash \mathcal{P} \to Prvt[\![\mathcal{P}]\!]$.

T13.72 For any formula $\mathcal{P}$, PA $\vdash \Box\mathcal{P} \to \Box\Box\mathcal{P}$ — D3

T13.73 PA $\vdash \mathbb{W}\!f\!f(a) \wedge \mathbb{W}\!f\!f(b) \to \mathbb{P}rvt(\mathbb{c}nd[\mathbb{n}eg(a), \mathbb{c}nd(a,b)])$.

T13.74 Suppose T is a recursively axiomatized theory for which the derivability conditions D1 - D3 hold and $T \vdash \Box\mathcal{P} \to \mathcal{P}$, then $T \vdash \mathcal{P}$. *Löb's Theorem.*

Chapter 14

Logic and Computability

In this chapter, we begin with the notion of a Turing machine, and a Turing computable function. It turns out that the Turing computable functions are the same as the recursive functions. Once we have seen this, it is a short step from a problem about computability — the *halting problem*, to another demonstration of essential results. Further, according to Church's thesis, the Turing computable functions, and so the recursive functions, are *all* the algorithmically computable functions. This converts results like T12.22 according to which no recursive relation is true just of (numbers for) theorems of predicate logic, into ones according to which no algorithmically decidable relation is true just of theorems of predicate logic — where this result is much more than a curiosity about an obscure class of functions.

14.1 Turing Computable Functions

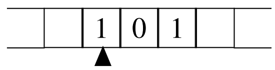
We begin saying what a Turing machine, and the Turing computable functions are. Then we turn to demonstrations that Turing computable functions are recursive, and recursive functions are Turing computable.

14.1.1 Turing Machines

A Turing machine is a simple device which, despite its simplicity, is capable of computing any recursive function — and capable of computing whatever is computable by the more sophisticated computers with which we are familiar.[1]

[1] So called after Alan Turing, who originally proposed them hypothetically, prior to the existence of modern computing devices, for purposes much like our own. Turing went on to develop electro-mechanical machines for code breaking during World War II, and was involved in development of early

We may think of a Turing machine as consisting of a *tape*, *machine head*, and a finite set of *instruction quadruples*.[2]

(A) 

The tape is a sequence of cells, infinite in two directions, where the cells may be empty or filled with 0 or 1. The machine head, indicated by arrow, reads or writes the contents of a given cell, and moves left or right, one cell at a time. The head is capable of five actions: (L) move left one cell; (R) move right one cell; (B) write a blank; (0) write a zero; (1) write a one. When the head is over a cell it is capable of reading or writing the contents of that cell.

Instruction quadruples are of the sort, $\langle q_1, C, A, q_2\rangle$ and constitute a function in the sense that no two quadruples have $\langle q_1, C\rangle$ the same but $\langle A, q_2\rangle$ different. For an instruction quadruple: (q_1) labels the quadruple; (C) is a possible state or content of the scanned cell; (A) is one of the five actions; (q_2) is a label for some (other) quadruples. In effect, an instruction quadruple q_1 says, "if the current cell has content C, perform action A and go to instruction q_2." The machine begins at an instruction with label $q_1 = 1$, and stops after executing an instruction with $q_2 = 0$.

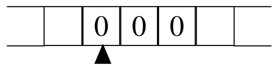
For a simple example, consider the following quadruples, along with the tape (A) from above.

	$\langle 1, 0, R, 1\rangle$	if 0 move right
(B)	$\langle 1, 1, 0, 1\rangle$	if 1 write 0
	$\langle 1, B, L, 2\rangle$	end of word, back up and go to instruction 2
	$\langle 2, 0, L, 2\rangle$	while value is 0, move left
	$\langle 2, B, R, 0\rangle$	end of word, return right and stop

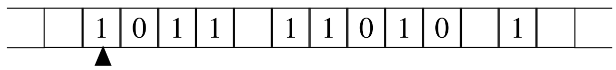
The machine begins at label 1. In this case, the head is over a cell with content 1; so from the second instruction the machine writes 0 in that cell and returns to instruction label 1. Because the cell now contains 0, the machine reads 0; so, from instruction 1, the head moves right one space and returns to instruction 1 again. Now the machine reads 0; so it moves right again and goes returns to instruction 1. Because it reads 1, again the machine writes 0 and goes to instruction 1 where it moves right and goes to 1. Now the head is over a blank; so it moves left one cell, and goes to 2. At instruction 2, the head moves left so long as the tape reads 0. When the head reaches a blank, it moves right one space, back over the word, and stops. So the result is,

stored-program computers after the war.

[2]Specifications of Turing machines differ somewhat. So, for example, some versions allow instruction quintuples, and allow different symbols on the tape. Nothing about what is computable changes on the different accounts.

(C) 

In the standard case, we begin with a blank tape except for one or more binary "words" where the words are separated by single blank cells, and the machine head is over the left-most cell of the left-most block. The above example is a simple case of this sort, but also,

(D) 

And in the usual case the program halts with the head over the leftmost cell of a single word on the tape. A total function $\mathsf{f}(\vec{\mathsf{x}})$ is *Turing computable* when, beginning with $\vec{\mathsf{x}}$ on the tape in binary digits, the result is $\mathsf{f}(\vec{\mathsf{x}})$.[3] Thus our little program computes $\mathsf{zero}(\mathsf{x})$, beginning with any x, and returning the value $\mathsf{0}$.

It will be convenient to require that programs are *dextral* (right-handed), in the sense that (a) in executing a program we never write in a cell to the left of the initial cell, or scan a cell more than one to the left of the initial cell; and (b) when the program halts, the head is over the initial cell and the final result begins in the same cell as the initial scanned cell. This does not affect what can be computed, but aids in predicting results when Turing programs are combined. Our little program is dextral.

A program to compute $\mathsf{suc}(\mathsf{x})$ is not much more difficult. Let us begin by thinking about what we want the program to do. With a three-digit input word, the desired outputs are,

000	$\Longrightarrow$	001	100	$\Longrightarrow$	101
001	$\Longrightarrow$	010	101	$\Longrightarrow$	110
010	$\Longrightarrow$	011	110	$\Longrightarrow$	111
011	$\Longrightarrow$	100	111	$\Longrightarrow$	1000

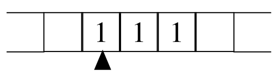
Moving from the right of the input word, we want to turn any one to a zero until we can turn a zero (or a blank) to a one. Here is a way to do that.

[3] A Turing machine might calculate the values a function that is *partial* in the sense that it does not return a value for every input string. We are particularly interested in total functions.

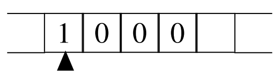
	$\langle 1, 0, R, 1\rangle$	move to end of word
(E)	$\langle 1, 1, R, 1\rangle$	
	$\langle 1, B, L, 5\rangle$	
	$\langle 5, 0, 1, 7\rangle$	flip 1 to 0 then 0 or blank to 1
	$\langle 5, 1, 0, 6\rangle$	
	$\langle 5, B, 1, 7\rangle$	
	$\langle 6, 0, L, 5\rangle$	
	$\langle 7, 0, L, 7\rangle$	return to start
	$\langle 7, 1, L, 7\rangle$	
	$\langle 7, B, R, 0\rangle$	

Do not worry about the gap in instruction labels. Nothing so-far requires instruction labels be sequential. This program moves the head to the right end of the word; from the right, flips one to zero until it finds a zero or blank; once it has acted on a zero or blank, it returns to the start.

So-far, so-good. But there is a problem with this program: In the case when the input is, say,

(F) 

the output is,

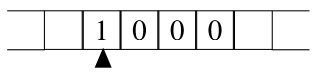


with the first symbol one to the left of the initial position. We turn the first blank to the left of the initial position to a one. So the program is not dextral. The problem is solved by "shifting" the word in the case when it is all ones.

(G)

if solid ones shift right	flip 1 to 0 then 0 to 1
$\langle 1, 0, R, 4\rangle$	$\langle 5, 0, 1, 7\rangle$
$\langle 1, 1, R, 1\rangle$	$\langle 5, 1, 0, 6\rangle$
$\langle 1, B, 1, 2\rangle$	$\langle 5, B, 1, 7\rangle$
$\langle 2, 1, L, 2\rangle$	$\langle 6, 0, L, 5\rangle$
$\langle 2, B, R, 3\rangle$	
	return to start
$\langle 3, 1, B, 3\rangle$	$\langle 7, 0, L, 7\rangle$
$\langle 3, B, R, 4\rangle$	$\langle 7, 1, L, 7\rangle$
	$\langle 7, B, R, 0\rangle$
$\langle 4, 0, R, 4\rangle$	
$\langle 4, 1, R, 4\rangle$	
$\langle 4, B, L, 5\rangle$	

States 5, 6 and 7 are as before. This time we test to see if the word is all ones. If not, the program jumps to 4 where it goes to the end, and to the routine from before. If it gets to the end without encountering a zero, it writes a one, returns to the beginning and deletes the initial symbol — so that the entire word is shifted one to the right. Then it goes to instruction 4 so that it goes to the right and works entirely as before. This time the output from (F) is,



as it should be. It is worthwhile to follow the actual operation of this and the previous program on one of the many Turing simulators available on the web (see E14.1).

More complex is a copy program to take an input x and return x.x. This program has four basic elements.

(1) A sort of control section which says what to do, depending on what sort of character we have in the original word.

(2) A program to copy 0; this will write a blank in the original word to "mark the spot"; move right to the second blank (across the blank between words, and to the blank to be filled); write a 0; move left to the original position, and replace the 0.

(3) Similarly a program to copy 1; this will write a blank in the original word to mark the spot; move right to the second blank; write a 1; move left to the original position, and replace the 1.

(4) And a program to move the head back to the original position when we are done.

Here is a program to do the job.

(H)

(1) *Control*
$\langle 1, 0, B, 10\rangle$
$\langle 1, 1, B, 20\rangle$
$\langle 1, B, L, 30\rangle$

(4) *Finish*
start of word
$\langle 30, 0, L, 30\rangle$
$\langle 30, 1, L, 30\rangle$
$\langle 30, B, R, 0\rangle$

(2) *Copy* 0
move from blank
$\langle 10, B, R, 11\rangle$

right 2 blanks: 0
$\langle 11, 0, R, 11\rangle$
$\langle 11, 1, R, 11\rangle$
$\langle 11, B, R, 12\rangle$

$\langle 12, 0, R, 12\rangle$
$\langle 12, 1, R, 12\rangle$
$\langle 12, B, 0, 13\rangle$

left 2 blanks: 0
$\langle 13, 0, L, 13\rangle$
$\langle 13, 1, L, 13\rangle$
$\langle 13, B, L, 14\rangle$

$\langle 14, 0, L, 14\rangle$
$\langle 14, 1, L, 14\rangle$
$\langle 14, B, 0, 15\rangle$

next char: return
$\langle 15, 0, R, 1\rangle$

(3) *Copy* 1
move from blank
$\langle 20, B, R, 21\rangle$

right 2 blanks: 1
$\langle 21, 0, R, 21\rangle$
$\langle 21, 1, R, 21\rangle$
$\langle 21, B, R, 22\rangle$

$\langle 22, 0, R, 22\rangle$
$\langle 22, 1, R, 22\rangle$
$\langle 22, B, 1, 23\rangle$

left 2 blanks: 1
$\langle 23, 0, L, 23\rangle$
$\langle 23, 1, L, 23\rangle$
$\langle 23, B, L, 24\rangle$

$\langle 24, 0, L, 24\rangle$
$\langle 24, 1, L, 24\rangle$
$\langle 24, B, 1, 25\rangle$

next char: return
$\langle 25, 1, R, 1\rangle$

You should be able to follow each stage.

E14.1. Study the copy program from the text along with the samples `zero` and `suc` from the text website (`http://rocket.csusb.edu/~troy/int-ml.html`). Then, starting with the file `blank.rb`, create Turing programs to compute the following. It will be best to submit your programs electronically.

a. copy(n). Takes input m and returns m.m. This is a simple implementation of the program from the text.

b. Create a Turing program to compute pred(n). Hint: Give your function two separate exit paths: One when the input is a string of 0s, returning with the input. In any other case, the output for input n is the predecessor of n. The method simply flips that for successor: From the right, change 0 to 1 until some 1 can be flipped to 0. There is no need to worry about the addition of a possible leading 0 to your result.

c. Create a Turing program to compute $\text{ident}^3_3(x, y, z)$. For x.y.z observe that z might be longer than x and y put together; but, of course, it is not longer than x, y and z put together. Here is one way to proceed: Move to the start of the third word; use copy to generate x.y.z.z then plug spaces so that you have one long first word, xoyoz.z; you can mark the first position of the long word with a blank (and similarly, each time you write a character, mark the next position to the right with a blank so that you are always writing into the second blank up from the one where the character is read); then it is a simple matter of running a basic copy routine from right-to-left, and erasing junk when you are done.

14.1.2 Turing Computable Functions are Recursive

We turn now to showing that the (dextral) Turing computable functions are the same as the recursive functions. Our first aim is to show that every Turing computable function is recursive. But we begin with the simpler result that there is a recursive enumeration of Turing machines. We shall need this as we go forward, and it will let us compile some important preliminary results along the way.

The method is by now familiar. It will require some work, but we can do it in the same way as we approached recursive functions before. Begin by assigning to each symbol a *Gödel Number*.

a. $g[\mathsf{B}] = 3$	f. $g[\mathsf{L}] = 9$
b. $g[0] = 5$	g. $g[\mathsf{R}] = 11$
c. $g[1] = 7$	h. $g[\mathsf{q_i}] = 13 + 2i$

For a quadruple, say, $\langle \mathsf{q}_1, \mathsf{B}, \mathsf{L}, \mathsf{q}_1 \rangle$, set $g = 2^{15} \times 3^3 \times 5^9 \times 7^{15}$. And for a sequence of quadruples with numbers $g_0, g_1 \ldots g_n$ the super Gödel number $g_s = 2^{g_0} \times 3^{g_1} \times \ldots \times \pi_n^{g_n}$. Again, for convenience we frequently refer to the individual symbol codes with angle quotes around the symbol, so $\langle \mathsf{B} \rangle = 3$ where $\ulcorner \mathsf{B} \urcorner$, the number of the expression is 2^3.

Now we define a recursive function and some simple recursive relations,

$$\mathsf{lb}(v) = 13 + 2v$$

$$\textsc{lb}(n) =_{\text{def}} (\exists v \leq n)(n = \mathsf{lb}(v))$$

$$\textsc{sym}(n) =_{\text{def}} n = \langle \mathsf{B} \rangle \lor n = \langle 0 \rangle \lor n = \langle 1 \rangle$$

$$\textsc{act}(n) =_{\text{def}} \mathsf{sym}(n) \lor n = \langle \mathsf{L} \rangle \lor n = \langle \mathsf{R} \rangle$$

$$\textsc{quad}(n) =_{\text{def}} \mathsf{len}(n) = 4 \land \textsc{lb}(\exp(n, 0)) \land \textsc{sym}(\exp(n, 1)) \land \textsc{act}(\exp(n, 2)) \land \textsc{lb}(\exp(n, 3))$$

$\mathsf{lb}(\mathsf{v})$ is the Gödel number of instruction v. Then the relations are true when n is the number for an instruction label, a symbol, an action and a quadruple. In particular, a code for a quadruple numbers a sequence of four symbols of the appropriate sort.

We are now ready to number the Turing machines. For this, adopt a simple modification of our original specification: We have so-far supposed that a Turing machine might lack any given quadruple, say $\langle 3, 1, x, y\rangle$. In case it lacks this quadruple, if the machine reads 1 and is sent to state 3 it simply "hangs" with no place to go. Where q is the largest label in the machine, we now suppose that for any $p \leq q$, if no $\langle p, C, x, y\rangle$ is a member of the machine, the machine is simply supplemented with $\langle p, C, C, p\rangle$. The effect is as before: In this case, there is a place for the machine to go; but if the machine goes to $\langle p, C, C, p\rangle$, it remains in that state, repeating it over and over. In the case of label 0, the states are added to the machine, but serve no function, as the zero label forces halt. Further, we suppose that the quadruples in a Turing machine are taken in order, $\langle 0, 0, x, y\rangle$, $\langle 0, 1, x, y\rangle$, $\langle 0, B, x, y\rangle$, $\langle 1, 0, x, y\rangle$, $\langle 1, 1, x, y\rangle, \ldots$ $\langle q, 0, x, y\rangle$, $\langle q, 1, x, y\rangle$, $\langle q, B, x, y\rangle$. So each Turing machine has a unique specification. On this account, a Turing machine halts only when it reaches a state of the sort $\langle x, x, x, 0\rangle$. And the ordered specification itself guarantees the functional requirement – that there are no two quadruples with the first inputs the same and the latter different. So for $\textsc{tmach}(n)$,

$$(\exists w < \mathsf{len}(n))(\mathsf{len}(n) = 3 \times (w + 2)) \land (\forall v, 3 \times v + 2 < \mathsf{len}(n))(\forall x \leq n)\{$$
$$[x = \mathsf{exp}(n, 3 \times v) \to (\textsc{quad}(x) \land \mathsf{exp}(x, 0) = \mathsf{lb}(v) \land \mathsf{exp}(x, 1) = \langle 0\rangle)] \land$$
$$[x = \mathsf{exp}(n, 3 \times v + 1) \to (\textsc{quad}(x) \land \mathsf{exp}(x, 0) = \mathsf{lb}(v) \land \mathsf{exp}(x, 1) = \langle 1\rangle)] \land$$
$$[x = \mathsf{exp}(n, 3 \times v + 2) \to (\textsc{quad}(x) \land \mathsf{exp}(x, 0) = \mathsf{lb}(v) \land \mathsf{exp}(x, 1) = \langle B\rangle)]\}$$

Given our modifications, the length of a Turing machine must be a non-zero multiple of three including at least the initial labels zero and one. So for some w, $\mathsf{len}(n) = 3 \times (w + 2)$. Then for each initial label v, there are three quadruples; so there are quadruples $3 \times v$, $3 \times v + 1$ and $3 \times v + 2$, taken in the standard order, and each with initial label v. Since n is a super Gödel number, and each x the number of a quadruple it is the exponents of x that reveal the instruction label and cell content.

But now it is easy to see,

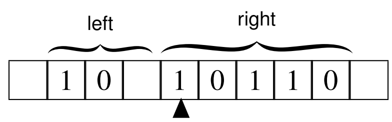
T14.1. There is a recursive enumeration of the Turing machines. Set,

$$\mathsf{mach}(0) = \mu z[\textsc{tmach}(z)]$$
$$\mathsf{mach}(Sn) = \mu z[z > \mathsf{mach}(n) \land \textsc{tmach}(z)]$$

Since $\mathsf{mach}(n)$ is is a recursive function from the natural numbers onto the Turing machines, they are recursively enumerable. While this enumeration is recursive, it is not primitive recursive.

Now, as we work toward a demonstration that Turing computable functions are recursive, let us pause for some key ideas. Consider a tape divided as follows,

(I)



We shall code the tape with a pair of numbers. Where at any stage the head divides the tape into left and right parts, first a standard code for the right hand side, $\ulcorner 10110 \urcorner$, and second, a code for the left side read from the inside out $\ulcorner B01 \urcorner$. Taken as a pair, these numbers record at once contents of the tape, and the position of the head — which is always under the first digit of the coded right number.

Say a dextral Turing machine computes a total function $f(n) = m$. Let us suppose that we have functions $code(n)$ and $decode(m)$ to move between m and n and their codes (where this requires moving from the numbers m and n through their binary representations, and then to the codes). So we concentrate on the machine itself, and wish to track the status of the Turing machine i given input n for each step j of its operation. In order to track the status of the machine, we shall require functions $left(i, n, j)$, $right(i, n, j)$ to record codes of the left and right portions of the tape, and $state(i, n, j)$ for the current quadruple state of the machine.

First, as we have observed, for any Turing machine, there is a unique quadruple for any instruction label and tape value. Thus, $machs(i, m, n)$ numbers a quadruple as a function of the number of the machine in the enumeration, and Gödel numbers for initial label and tape value. Thus $machs(i, m, n)$ is,

$$(\mu y \leq mach(i))(\exists v < len(mach(i)))[y = exp(mach(i), v) \wedge exp(y, 0) = m \wedge exp(y, 1) = n]$$

So $machs(i, m, n)$ returns the number of that quadruple in machine i whose initial label has number m, and initial value number n. Since the machine is a function, there must be a unique state with those initial values.

In addition, where $n = a \star b$, let us adopt a sort of converse to concatenation such that $a \circ n = b$.

$$a \circ n = (\mu x \leq n)(\forall i < len(n) \dot{-} len(a))(exp(x, i) = exp(n, len(a) + i))$$

So we want the least x such that its length is the length of n less the length of a, and the values of x at any position i are the same as those of n at $len(a) + i$. Thus $a \circ n$ "lops off" the portion whose length is that of a from the expression numbered n.

Recall that our Turing machine is to calculate a function $\mathsf{f(n) = m}$. Initial values of $\mathsf{left(i,n,j)}$, $\mathsf{right(i,n,j)}$ and $\mathsf{state(i,n,j)}$ are straightforward.

$$\mathsf{left(i,n,0)} = \ulcorner \mathsf{BB} \urcorner$$
$$\mathsf{right(i,n,0)} = \mathsf{code(n)}$$
$$\mathsf{state(i,n,0)} = \mathsf{machs(i, \langle 1\rangle, exp(right(i,n,0),0))}$$

On a dextral machine, the machine never writes to the left of its initial position, and the head never moves more than one position to the left of its initial position; so we simply set the value of the left portion to a couple of blanks. This ensures that there is enough "space" on the left for the machine to operate (and that, for any position of the machine head, there is always a left portion of the tape). The starting right number is just the code of the input to the function. And the initial state value is determined by the input label $\mathsf{1}$ and the first value on the tape which is coded by the first exponent of $\mathsf{right(i,n,0)}$.

For the successor values,

$$\mathsf{left(i,n,Sj)} = \begin{cases} \mathsf{left(i,n,j)} & \text{if} \quad \textsc{sym}\mathsf{(exp(state(i,n,j),2))} \\ \mathsf{2^{exp(right(i,n,j),0)} \star left(i,n,j)} & \text{if} \quad \mathsf{exp(state(i,n,j),2) = \langle R\rangle} \\ \mathsf{2^{exp(left(i,n,j),0)} \circ left(i,n,j)} & \text{if} \quad \mathsf{exp(state(i,n,j),2) = \langle L\rangle} \end{cases}$$

If a symbol is written in the current cell, there is no change in the left number. If the head moves to the left or the right, the first value is either appended or deleted, depending on direction. And similarly for $\mathsf{right(i,n,Sj)}$ but with separate clauses for each of the symbols that may be written onto the first position. And now the successor value for state is determined by the Turing machine together with the new label and the value under the head after the current action has been performed.

$$\mathsf{state(i,n,Sj) = machs(i, exp(state(i,n,j),3), exp(right(i,n,Sj),0))}$$

The machine jumps to a new state depending on the label and value on the tape. Observe that we are here proceeding by *simultaneous* recursion, defining multiple functions together. It should be clear enough how this works (see E12.25, p. 595).

If the machine enters a zero state then it halts. So set,

$$\mathsf{stop(i,n,j)} =_{\text{def}} (\mu \mathsf{y} \leq \mathsf{len(mach(i))})(\mathsf{exp(state(i,n,j),0) = lb(y)})$$

$\mathsf{exp(state(i,n,j),0)}$ is the number of of the instruction label. So $\mathsf{exp(state(i,n,j),0)} = \mathsf{lb(y)}$ when y is the label. Since there always is some such label, $\mathsf{exp(state(i,n,j),0)} = \mathsf{lb(y)})$ is regular. And $\mathsf{stop(i,n,j)}$ takes the value $\mathsf{0}$ just in case machine i with input n is halted at step j. When the first member of $\mathsf{state(i,n,j)}$ codes zero, the machine is halted, otherwise it is running. So y takes the value zero just in case the machine is halted.

T14.2. Every Turing computable function is a recursive function. Supposing Turing machine i computes a function $f(n)$,

$$f(n) = decode(right(i, n, \mu j[stop(i, n, j) = 0]))$$

When a dextral Turing machine stops, the value of right is just the code of its output value m; so if we decode $right(i, n, j)$ at that stage, we have the value of the function calculated by the Turing machine. Since the Turing computable function is total, there must be some j where the machine is stopped; so the minimization operates on a regular function. Since this function is recursive, the function calculated by Turing machine i is a recursive function.

E14.2. Find a recursive function to calculate $right(i, n, j)$. Hint: You might find a combination of $\star$ and $\circ$ useful for the case when a symbol is written into the first cell.

E14.3. Find a recursive function to calculate $decode(n)$.

E14.4. Suppose a "dual" Turing machine has two tapes, with a machine head for each. Instructions are of the sort $\langle q_i, C_{t_a}, A_{t_b}, q_j\rangle$ where t_a and t_b indicate the relevant tape. Show that every function that is dual Turing computable is recursive.

14.1.3 Recursive Functions are Turing Computable

To show that the recursive functions are identical to the Turing computable functions, we now show that all recursive functions are Turing computable.

T14.3. Every recursive function is Turing computable.

Suppose $f(\vec{x})$ is a recursive function. Then there is a sequence of recursive functions f_0, $f_1 \ldots f_n$ such that $f_n = f$, where each member is either an initial function or arises from previous members by composition, recursion, or regular minimization. The argument is by induction on this sequence.

Basis: We have already seen that the initial functions $\mathsf{zero}(x)$, $\mathsf{suc}(x)$ and idnt^j_k, as illustrated in E14.1, are Turing computable.

Assp: For any i, $0 \le i < k$, $f_i(\vec{x})$ is Turing computable.

Show: $f_k(\vec{x})$ is Turing computable.

f_k is either an initial function or arises from previous members by composition, recursion, or regular minimization. If an initial function, then as in the basis. So suppose f_k arises from previous members.

(c) $f_k(\vec{x}, \vec{y}, \vec{z})$ arises by composition from $g(\vec{y})$ and $h(\vec{x}, w, \vec{z})$. By assumption $g(\vec{y})$ and $h(\vec{x}, w, \vec{z})$ are Turing computable. For the simplest case, consider $h(g(y))$: Chain together Turing programs to calculate $g(y)$ and then $h(w)$ — so the first program operates upon y to calculate $g(y)$ and the second begins where the first leaves off, operating on the result to calculate $h(g(y))$. A case like $h(x, g(y), z)$ is more complex insofar as $g(y)$ may take up a different number of cells from y: it is sufficient to run a copy to get $x.y.z.y$; then $g(y)$ to get $x.y.z.g(y)$; then copy for $x.y.z.g(y).z$ and a copy that replaces the last two numbers to get $x.g(y).z$. Then you can run h. And similarly in other cases.

(r) $f_k(\vec{x}, y)$ arises by recursion from $g(\vec{x})$ and $h(\vec{x}, y, u)$. By assumption $g(\vec{x})$ and $h(\vec{x}, y, u)$ are Turing computable. Recall our little programs from chapter 12 which begin by using $g(\vec{x})$ to find $f(0)$ and then use $h(\vec{x}, y, u)$ repeatedly for y in 0 to $b-1$ to find the value of $f(\vec{x}, b)$ (see, for example, p. 555). For a representative case, consider $f(m, b)$.

a. Produce a sequence,

$$m.b.m.b-1.m.b-2 \ldots m.2.m.1.m.0.m$$

This requires a $\mathsf{copypair}(x, y)$ that takes $m.n$ and returns $m.n.m.n$ and $\mathsf{pred}(x)$. Given $m.b$ on the tape, run copypair to get $m.b.m.b$ (and mark the first m with a blank). Then loop as follows: if the final b is 0, delete it, go to the previous m, and move on to (b); otherwise run pred on the final b, move to previous m, run copypair, and loop.

b. Run g on the last block of digits m. This gives,

$$m.b.m.b-1.m.b-2 \ldots m.2.m.1.m.0.f(m, 0)$$

c. Back up to the previous m and run h on the concluding three blocks $m.0.f(m, 0)$. This gives,

$$m.b.m.b-1.m.b-2 \ldots m.2.m.1.f(m, 1)$$

And so forth. Stop when you reach the m with an extra blank (with two blanks in a row). At that stage, we have, $m^*.b.f(m, b)$. Fill the first blank, run idnt^3_3 and you are done. Observe that the original m.b plays no role in the calculation other to serve as the initial template for the series, and then as an end marker on your way back up — there is never a need to apply h to any value greater than $\mathsf{b} - 1$ in the calculation of $\mathsf{f(m, b)}$.

(m) $\mathsf{f_k}(\vec{\mathsf{x}})$ arises by regular minimization from $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$. By assumption, $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$ is Turing computable. For a representative case, suppose we are given m and want $\mu \mathsf{y}[\mathsf{g(m, y)} = 0]$.

a. Given, m, produce m.0.m.0.

b. From a tape of the form m.y.m.y loop as follows: Move to the second m; run g on m.y; this gives m.y.g(m, y); check to see if the result is zero; if it is, run idnt^3_2 and you are done (this is the same as deleting the last zero and running idnt^2_2); if the result is not zero, delete g(m, y) to get m.y; run suc on y; and then a copier to get $\mathsf{m.y'.m.y'}$, and loop. The loop halts when it reaches the value of y for which g has output 0 — and there must be some such value if g is regular.

Indct: Any recursive function $\mathsf{f}(\vec{\mathsf{x}})$ is Turing computable.

And from T14.2 together with T14.3, the Turing computable functions are identical to the recursive functions. It is perhaps an "amazing" coincidence — that functions independently defined in these ways should turn out to be identical. And we have here the beginnings of an idea behind Church's thesis which we shall explore in section 14.3.

E14.5. From exercise E14.1 you should already have Turing programs for suc(x), pred(x), copy(x) and $\mathsf{idnt}^3_3(\mathsf{x, y, z})$. Now produce each of the following, in order, leading up to the recursive addition function. When you require one as part of another simply copy it into the larger file.

a. The function, h(x, y, u). For addition, h(x, y, u) is $\mathsf{suc}(\mathsf{idnt}^3_3(\mathsf{x, y, u}))$. So this is a simple combination of suc and idnt^3_3. For addition, $\mathsf{g(x)} = \mathsf{idnt}^1_1(\mathsf{x}) = \mathsf{x}$, which requires no action; so we will not worry about that.

b. The function, copypair. Take a.b and return a.b.a.b. One approach is to produce a simple modification of copy that takes a.b and produces a.b.a. Run this program starting at a, and then another copy of it starting at b.

c. The function, cascade. This is the program to produce m.n.m.n − 1.m.n − 2 . . . m.0.m. The key elements are copypair and pred. To prepare for the next stage, you should begin by running copypair and then "damage" the very first m by putting a blank in its first cell. Let the program finish with the head on m at the end.

d. The function, plus(m, n). g is trivial. So from m at the far right of the sequence, back up two words; check to see if there is an extra blank; if so, run idnt^3_3 and you are done; if not, run h(x, y, u). Though m.n is part of the "cascade" series, we never run h on m.n.u. In a program we may make use of m.n as described, but in damaged form — as an end marker for the series.

   There are easier ways to do addition on a Turing machine! The obvious strategy is to put m in a location *x* and n in a location *y*; run pred on the value in location *x* and then suc on the value in location *y*; the result appears in *y* when pred hits zero. The advantage of our approach is that it illustrates (an important case of) the demonstration that a Turing machine can compute any recursive function.

E14.6. Produce each of the following, leading up to a Turing program for the function μy[ch(x = pred(y)) = 0], that is the function which returns the least y such that x equals the predecessor of y — such that the characteristic function of x = pred(y) returns 0.

a. The function idnt^2_2(x, y). This can be a simple modification of idnt^3_3.

b. The function ch(x = y), which returns 0 when x = y and otherwise 1. This is, of course, a recursive function. But you can get it more efficiently and more directly. To compare numbers, you have to worry about leading zeros that might make equivalent numbers physically distinct. Here is one strategy: From x.y check to see if one or both are all zeros; exit with 1 or 0 in the different cases; if neither works, apply pred to x and to y and return to the start; eventually you will come to a stage where the check for zero returns a result.

c. The function ch(x = pred(y)). This is a simple case of composition.

d. The function μy[ch(x = pred(y)) = 0], by the routine discussed in the text.

   Of course, for any number except 0, this is nothing but a long-winded equivalent to suc(x). The point, however, is to apply the algorithm for regular minimization, and so to work through the last stage of the demonstration that recursive functions are Turing computable.

14.2 Essential Results

In chapter 12 essential results were built on the diagonal lemma (T12.19). This time, we depend on a *halting problem* with special application to Turing machines. Once we have established the halting problem, results like ones from before follow in short order.

14.2.1 Halting

A Turing machine is a set of quadruples. Things are arranged so that Turing machines do not “hang” in the sense that they reach a state with no applicable instruction. But a Turing machine may go into a loop or routine from which it never emerges. That is, a Turing machine may or may not *halt* in a finite number of steps. So for example, this machine never stops.

$\langle 1, 0, 0, 1\rangle$
$\langle 1, 1, 1, 1\rangle$
$\langle 1, B, B, 1\rangle$

For any input it simply repeats forever. This raises the question whether there is a general way to *tell* whether Turing machines halt when started on a given input. This is an issue of significance for computing theory. And, as we shall see, the answer has consequences beyond computing.

The problem divides into narrower “self-halting” and broader “general halting” versions. First, the self-halting problem: By T14.1 there is an enumeration of the Turing machines. Consider an enumeration, Π_0, Π_1 ... of Turing machines for functions with a single free variable and an array as follows,

(J)

	0	1	2	...
Π_0	$\boldsymbol{\Pi}_0(0)$	$\Pi_0(1)$	$\Pi_0(2)$	
Π_1	$\Pi_1(0)$	$\boldsymbol{\Pi}_1(1)$	$\Pi_1(2)$	
Π_2	$\Pi_2(0)$	$\Pi_2(1)$	$\boldsymbol{\Pi}_2(2)$	
$\vdots$				

We run Π_0 on inputs $0, 1\ldots$; Π_1 on $0, 1\ldots$; and so forth. Now ask whether there is a Turing program (that is, a recursive function) to decide in general whether Π_i halts when applied to its own number in the enumeration — a program $H(i)$ such that $H(i) = 0$ if $\Pi_i(i)$ halts, and $H(i) = 1$ if $\Pi_i(i)$ does not halt.

T14.4. There is no Turing machine $\mathsf{H}(i)$ such that $\mathsf{H}(i) = 0$ if $\Pi_i(i)$ halts and $\mathsf{H}(i) = 1$ if it does not.

Suppose otherwise. That is, suppose there is a halting machine $\mathsf{H}(i)$ where for any $\Pi_i(i)$, $\mathsf{H}(i) = 0$ if $\Pi_i(i)$ halts and $\mathsf{H}(i) = 1$ if it does not. Chain this program into a simple looping machine $\Lambda(j)$ defined as follows,

$\langle q, 0, 0, q\rangle$
$\langle q, 1, 1, 0\rangle$

So when $j = 0$, Λ goes into an infinite loop, remaining in state q forever; when $j = 1$, Λ halts gracefully with output 1. Let the combination of H and Λ be $\Delta(i)$; so $\Delta(i)$ calculates $\Lambda(\mathsf{H}(i))$. On our assumption that there is a Turing machine $\mathsf{H}(i)$, the machine Δ must appear in the enumeration of Turing machines with some number d.

But this is impossible. Consider $\Delta(d)$ and suppose $\Delta(d)$ halts; since Δ halts on input d, the halting machine, $\mathsf{H}(d) = 0$; and with this input, Λ goes into the infinite loop; so the composition $\Lambda(\mathsf{H}(d))$ does not halt; and this is just to say $\Delta(d)$ does not halt. Reject the assumption, $\Delta(d)$ does not halt. But since $\Delta(d)$ does not halt, the halting machine $\mathsf{H}(d) = 1$; and with this input, Λ halts gracefully with output 1; so the composition $\Lambda(\mathsf{H}(d))$ halts; and this is just to say $\Delta(d)$ halts. Reject the original assumption, there is no machine $\mathsf{H}(i)$ which says whether an arbitrary $\Pi_i(i)$ halts.

For this argument, it is important that H is a component of Δ. Information about whether Δ halts gives information about the behavior of H, and information about the behavior of H, about whether Δ halts.

The more general question is whether there is a machine to decide for any Π_i and n whether $\Pi_i(n)$ halts. But it is immediate that if there is no Turing machine to decide the more narrow self-halting problem, there is no Turing machine to decide this more general version.

T14.5. There is no Turing machine $\mathsf{H}(i, n)$ such that $\mathsf{H}(i, n) = 0$ if $\Pi_i(n)$ halts and $\mathsf{H}(i, n) = 1$ if it does not.

Suppose otherwise. That is, suppose there is a halting machine $\mathsf{H}(i, n)$ where for any $\Pi_i(n)$, $\mathsf{H}(i, n) = 0$ if $\Pi_i(n)$ halts and $\mathsf{H}(i, n) = 1$ if it does not. Chain this program after a copier $\mathsf{K}(n)$ which takes input n and gives $n.n$. The combination $\mathsf{H}(\mathsf{K}(i))$ decides whether $\Pi_i(i)$ halts. This is impossible; reject the assumption: There is no such Turing machine $\mathsf{H}(i, n)$.

And when combined with T14.3 according to which every recursive function is Turing computable, these theorems which tell us that no Turing program is sufficient to solve the halting problem, yield the result that no recursive function solves the halting problem: if a function is recursive, then it is Turing computable; and since it is Turing computable, it does not solve the halting problem. Observe that we may be able to decide in particular cases whether a program halts. No doubt you have been able to do so in particular cases! What we have shown is that there is no perfectly general recursive method to decide whether $\Pi_i(n)$ halts.

E14.7. Say a function is *μ-recursive* just in case it satisfies the conditions for the recursive functions but without the regularity requirement for minimization. So all the recursive functions are μ-recursive, but some μ-recursive functions are not recursive. Where every recursive function $f(\vec{x})$ is *total* in the sense that it returns a value for every $\vec{x}$, some μ-recursive functions are *partial* insofar as there may be values of $\vec{x}$ for which they return no value (as occurs when minimization is applied to a $g(\vec{x}, y)$ that never evaluates to zero). Suppose that the μ-recursive functions can be numbered and that there is a μ-recursive function $emurec(i)$ to enumerate them; so $emurec(i)$ returns the Gödel number of the i^{th} function in the enumeration. (You will have occasion to produce this function in a later exercise.) Show that there is no μ-recursive function $def(i)$ such that $def(i) = 0$ if $f_i(i)$ is defined and $def(i) = 1$ if $f_i(i)$ is undefined. Hint: Let your diagonal function $diag(i) = \mu y[def(i) = y \wedge y = 1]$. We might think of this as the *definition problem*.

14.2.2 The Decision Problem

Recall our demonstration from section 12.5.2 that if Q is consistent then no recursive relation identifies the theorems of predicate logic. With the identity between the recursive functions and the Turing computable functions, this is the same as the result that if Q is consistent then no Turing computable function identifies the theorems of predicate logic. We are now in a position to obtain a related result directly, by means of the halting problem. Recall from chapter 13 (p. 621) that a theory T is *ω-inconsistent* iff for some $\mathcal{P}(x)$, T proves each $\mathcal{P}(\overline{m})$ but also proves $\sim\forall x\mathcal{P}(x)$. Equivalently, T is ω-inconsistent iff T proves each $\sim\mathcal{P}(\overline{m})$ but also proves $\exists x\mathcal{P}(x)$. We show,

T14.6. If Q is ω-consistent, then no Turing computable function $thrmpl(n)$ is such that $thrmpl(n) = 0$ just in case n numbers a theorem of predicate logic.

Suppose Q is ω-consistent, and suppose some Turing computable $\mathsf{thrmpl(n)} = \mathsf{0}$ just in case n numbers a theorem of predicate logic. Consider our recursive function $\mathsf{stop(i, n, j)}$ which takes the value $\mathsf{0}$ iff $\Pi_{\mathsf{i}}(\mathsf{n})$ is halted. Since it is recursive, stop is captured by some $Stop(i, n, j, z)$ so that,

(i) If $\Pi_{\mathsf{i}}(\mathsf{i})$ is halted by step j, $\mathrm{Q} \vdash Stop(\bar{\mathsf{i}}, \bar{\mathsf{i}}, \bar{\mathsf{j}}, \emptyset)$

(ii) If $\Pi_{\mathsf{i}}(\mathsf{i})$ never halts, $\mathrm{Q} \vdash \sim Stop(\bar{\mathsf{i}}, \bar{\mathsf{i}}, \bar{\mathsf{j}}, \emptyset)$ for any j

Let $\mathscr{H}(i) = \exists z Stop(i, i, z, \emptyset)$. Then if $\Pi_{\mathsf{i}}(\mathsf{i})$ halts, there is some j such that $\mathrm{Q} \vdash Stop(\bar{\mathsf{i}}, \bar{\mathsf{i}}, \bar{\mathsf{j}}, \emptyset)$; so $\mathrm{Q} \vdash \mathscr{H}(\bar{\mathsf{i}})$. And if $\Pi_{\mathsf{i}}(\mathsf{i})$ never halts, for every j, $\mathrm{Q} \vdash \sim Stop(\bar{\mathsf{i}}, \bar{\mathsf{i}}, \bar{\mathsf{j}}, \emptyset)$; so since Q is ω-consistent, $\mathrm{Q} \nvdash \mathscr{H}(\bar{\mathsf{i}})$. So where $\mathscr{Q}$ is a conjunction of the axioms of Q, if $\Pi_{\mathsf{i}}(\mathsf{i})$ halts $\vdash \mathscr{Q} \rightarrow \mathscr{H}(\bar{\mathsf{i}})$ and if $\Pi_{\mathsf{i}}(\mathsf{i})$ never halts $\nvdash \mathscr{Q} \rightarrow \mathscr{H}(\bar{\mathsf{i}})$; so,

$$\vdash \mathscr{Q} \rightarrow \mathscr{H}(\bar{\mathsf{i}}) \quad \text{iff} \quad \Pi_{\mathsf{i}}(\mathsf{i}) \text{ halts}$$

Let $\mathsf{q} = \ulcorner \mathscr{Q} \urcorner$ and $\mathsf{h(i)} = \mathsf{formsub}(\ulcorner \mathscr{H}(i) \urcorner, \ulcorner i \urcorner, \mathsf{num(i)})$ — so $\mathsf{h(i)}$ is the number of $\mathscr{H}(\bar{\mathsf{i}})$. Then $\mathsf{thrmpl(cnd(q, h(i)))}$ takes the value $\mathsf{0}$ iff $\mathscr{Q} \rightarrow \mathscr{H}(\bar{\mathsf{i}})$ is a theorem, iff $\Pi_{\mathsf{i}}(\mathsf{i})$ halts. So thrmpl solves the halting problem. This is impossible; reject the assumption: If Q is ω-consistent, then there is no Turing computable function that returns the value zero just for numbers of theorems of predicate logic.

And, of course, this result according to which if Q is ω-consistent no Turing computable function returns zero just for theorems of predicate logic is equivalent to the result that if Q is ω-consistent, then no recursive function returns zero just for theorems of predicate logic.[4]

E14.8. Return again to the μ-recursive functions from E13.7. Suppose that in addition to $\mathsf{emurec(i)}$ to enumerate the functions there is a μ-recursive $\mathsf{umurec(i, n)}$ to return the value of $\mathsf{f_i(n)}$ so that $\mathsf{umurec(i, n)} = \mathsf{f_i(n)}$; say this function is captured in $\mathrm{Q_s}$ by some $Umurec(i, n, y)$ so that if $\mathsf{f_i(n)} = \mathsf{a}$ then $\mathrm{Q} \vdash Umurec(\bar{\mathsf{i}}, \bar{\mathsf{n}}, \bar{\mathsf{a}})$ and if $\mathsf{f_i(n)} \neq \mathsf{a}$ then $\mathrm{Q} \vdash \sim Umurec(\bar{\mathsf{i}}, \bar{\mathsf{n}}, \bar{\mathsf{a}})$. Use your result from the definition problem in E14.7 to show that if $\mathrm{Q_s}$ is ω-consistent, then no μ-recursive function $\mathsf{muthrmpl(n)}$ is such that $\mathsf{muthrmpl(n)} = \mathsf{0}$ just in case n numbers a theorem of predicate logic. Hint: Let $Defined(\bar{\mathsf{i}}) =_{\mathrm{def}} \exists z Umurec(\bar{\mathsf{i}}, \bar{\mathsf{i}}, z)$.

[4] This argument, and the parallel one in chapter 12 have the advantage of simplicity. However, this result that no recursive function is true just of the theorems of predicate logic need not be conditional on the consistency (or ω-consistency) of Q. For an illuminating version of the strengthened result from the halting problem, see chapter 11 of Boolos et al., *Computability and Logic*.

14.2.3 Incompleteness Again

In T12.21 we saw that no consistent, recursively axiomatizable theory extending Q is negation complete. We shall see this again. However, as described in chapter 13, the incompleteness result comes in different forms. In particular, the one as from chapter 12 which depends on consistency and capture, and another which depends on soundness and expression. We are positioned to see the result in both forms.

Semantic Version

A key preliminary to the chapter 12 demonstration of incompleteness is T12.20 which applies the diagonal lemma to show that for no consistent theory T extending Q is a recursive relation true of (numbers for) its theorems. This time, by means of the halting result, we show that the *truths* of $\mathscr{L}_{NT}$ are not recursively enumerable.

T14.7. The set of truths of $\mathscr{L}_{NT}$ is not recursively enumerable.

Consider again our recursive function $\mathsf{stop}(\mathsf{i},\mathsf{n},\mathsf{j})$; since it is recursive, it is expressed by some $Stop(i,n,j,z)$; set $\mathscr{H}(i) = \exists z Stop(i,i,z,\emptyset)$ and $\mathsf{h}(\mathsf{i}) = \mathsf{formsub}(\ulcorner\mathscr{H}(i)\urcorner, \ulcorner i\urcorner, \mathsf{num}(\mathsf{i}))$ — so $\mathsf{h}(\mathsf{i})$ is the number of $\mathscr{H}(\bar{\mathsf{i}})$. Suppose some $\Pi_{\mathsf{e}}(\mathsf{i})$ enumerates the truths of $\mathscr{L}_{NT}$, halting with output $\mathsf{0}$ if $\mathsf{h}(\mathsf{i})$ appears in the enumeration, and with output $\mathsf{1}$ if $\mathsf{neg}(\mathsf{h}(\mathsf{i}))$ appears. Exactly one of $\mathscr{H}(\bar{\mathsf{i}})$ or $\sim\mathscr{H}(\bar{\mathsf{i}})$ is true; so the number for one of them will eventually turn up insofar as Π_{e} enumerates all the truths of $\mathscr{L}_{NT}$.

(i) Suppose $\mathsf{N}[\mathscr{H}(\bar{\mathsf{i}})] = \mathsf{T}$; then for some m, $\mathsf{N}[Stop(\bar{\mathsf{i}},\bar{\mathsf{i}},\bar{\mathsf{m}},\emptyset)] = \mathsf{T}$; so $\mathsf{N}[\sim Stop(\bar{\mathsf{i}},\bar{\mathsf{i}},\bar{\mathsf{m}},\emptyset)] \neq \mathsf{T}$; so by expression, $\langle\langle \mathsf{i},\mathsf{i},\mathsf{m}\rangle,\mathsf{0}\rangle \in \mathsf{stop}$; so $\Pi_{\mathsf{i}}(\mathsf{i})$ stops.

(ii) Suppose $\mathsf{N}[\mathscr{H}(\bar{\mathsf{i}})] \neq \mathsf{T}$; then for any $\mathsf{m} \in \mathsf{U}$, $\mathsf{N}[Stop(\bar{\mathsf{i}},\bar{\mathsf{i}},\bar{\mathsf{m}},\emptyset)] \neq \mathsf{T}$; so by expression, $\langle\langle \mathsf{i},\mathsf{i},\mathsf{m}\rangle,\mathsf{0}\rangle \notin \mathsf{stop}$; so $\Pi_{\mathsf{i}}(\mathsf{i})$ never stops.

$$\text{So} \qquad \mathsf{N}[\mathscr{H}(\bar{\mathsf{i}})] = \mathsf{T} \quad \text{iff} \quad \Pi_{\mathsf{i}}(\mathsf{i}) \text{ halts}$$

Thus by its definition, $\Pi_{\mathsf{e}}(\mathsf{i})$ halts with output $\mathsf{0}$ iff $\mathsf{N}[\mathscr{H}(\bar{\mathsf{i}})] = \mathsf{T}$; iff $\Pi_{\mathsf{i}}(\mathsf{i})$ halts; so $\Pi_{\mathsf{e}}(\mathsf{i})$ solves the halting problem. This is impossible; there is no such Turing machine. And since no Turing machine enumerates the truths of $\mathscr{L}_{NT}$, no recursive function enumerates the truths of $\mathscr{L}_{NT}$.

This theorem, together with T12.17 which tells us that if T is a recursively axiomatized formal theory then the set of theorems of T is recursively enumerable, puts us in a position to obtain an incompleteness result mirroring T13.2.

T14.8. If T is a recursively axiomatized sound theory whose language includes $\mathscr{L}_{\rm NT}$, then T is negation incomplete.

Suppose T is a recursively axiomatized sound theory whose language includes $\mathscr{L}_{\rm NT}$. By T12.17, there is an enumeration of the theorems of T, and since T is sound, all of the theorems in the enumeration are true. But by T14.7, there is no enumeration of all the truths of $\mathscr{L}_{\rm NT}$; so the enumeration of theorems is not an enumeration of all truths; so some true $\mathcal{P}$ is not among the theorems of of T; and since $\mathcal{P}$ is true, $\sim\mathcal{P}$ is not true; and since T is sound, neither is $\sim\mathcal{P}$ among the theorems of T. So $T \nvdash \mathcal{P}$ and $T \nvdash \sim\mathcal{P}$.

This incompleteness result requires the *soundness* of T, where where soundness is more than mere consistency. But it requires only that the language include $\mathscr{L}_{\rm NT}$ and so have the power to *express* recursive functions — where this leaves to the side a requirement that T extends Q, and so be able to capture recursive functions.

Syntactic Version

From the halting problem, we can obtain the other sort of incompleteness result as well. Thus we have a theorem like the combination of T13.4 and T13.5.

T14.9. If T is a recursively axiomatized theory extending Q, then there is a sentence $\mathcal{P}$ such that if T is consistent $T \nvdash \mathcal{P}$, and if T is ω-consistent, $T \nvdash \sim\mathcal{P}$.

Suppose T is a recursively axiomatized theory extending Q. Once again consider $\mathsf{stop}(\mathsf{i},\mathsf{n},\mathsf{j})$; since stop is recursive and T extends Q, stop is captured in T by some $Stop(i,n,j,z)$; let $\mathcal{H}(i) = \exists z Stop(i,i,z,\emptyset)$, and $\mathsf{h}(\mathsf{i}) = \mathsf{formsub}(\ulcorner\mathcal{H}(i)\urcorner,\ulcorner i\urcorner,\mathsf{num}(\mathsf{i}))$. Consider a Turing machine $\Pi_{\mathsf{s}}(\mathsf{i})$ which tests whether successive values of m number a proof of $\sim\mathcal{H}(\bar{\mathsf{i}})$, halting if some m numbers a proof and otherwise continuing forever — so $\Pi_{\mathsf{s}}(\mathsf{i})$ evaluates $\textsc{prft}(\mathsf{m},\mathsf{neg}(\mathsf{h}(\mathsf{i})))$ for successive values of m; since T is a recursively axiomatized theory, this is a recursive relation so that there must be some such Turing machine. We can think of $\Pi_{\mathsf{s}}(\mathsf{i})$ as seeking a proof that $\Pi_{\mathsf{i}}(\mathsf{i})$ does not halt.

Suppose $\Pi_{\mathsf{s}}(\mathsf{s})$ halts. By its definition, $\Pi_{\mathsf{s}}(\mathsf{i})$ halts just in case some m numbers a proof of $\sim\mathcal{H}(\bar{\mathsf{i}})$; since $\Pi_{\mathsf{s}}(\mathsf{s})$ halts, then, there is some m such that $\textsc{prft}(\mathsf{m},\mathsf{neg}(\mathsf{h}(\mathsf{s})))$; so $T \vdash \sim\mathcal{H}(\bar{\mathsf{s}})$. But if $\Pi_{\mathsf{s}}(\mathsf{s})$ halts, for some m, $\langle\langle\mathsf{s},\mathsf{s},\mathsf{m}\rangle,0\rangle \in \mathsf{stop}$; so by capture, $T \vdash Stop(\bar{\mathsf{s}},\bar{\mathsf{s}},\bar{\mathsf{m}},\emptyset)$; so $T \vdash \exists z Stop(\bar{\mathsf{s}},\bar{\mathsf{s}},z,\emptyset)$, which is to say, $T \vdash \mathcal{H}(\bar{\mathsf{s}})$. Reject the assumption: if T is consistent, $\Pi_{\mathsf{s}}(\mathsf{s})$ does not halt.

(i) Suppose T is consistent and $T \vdash \sim\mathscr{H}(\overline{\mathsf{s}})$; then for some m, $\textsc{prft}(\mathsf{m}, \mathsf{neg}(\mathsf{h}(\mathsf{s})))$; so by its definition, $\Pi_{\mathsf{s}}(\mathsf{s})$ halts. But since T is consistent, as we have just seen, $\Pi_{\mathsf{s}}(\mathsf{s})$ does not halt. Reject the assumption: $T \nvdash \sim\mathscr{H}(\overline{\mathsf{s}})$.

(ii) Suppose T is ω-consistent and $T \vdash \sim\sim\mathscr{H}(\overline{\mathsf{s}})$; then $T \vdash \mathscr{H}(\overline{\mathsf{s}})$; so $T \vdash \exists z Stop(\overline{\mathsf{s}}, \overline{\mathsf{s}}, z, \emptyset)$. But since T is ω-consistent, it is consistent so that $\Pi_{\mathsf{s}}(\mathsf{s})$ does not halt; so for any m, $\langle\langle \mathsf{s}, \mathsf{s}, \mathsf{m}\rangle, 0\rangle \notin \mathsf{stop}$; and by capture, for any m, $T \vdash \sim Stop(\overline{\mathsf{s}}, \overline{\mathsf{s}}, \overline{\mathsf{m}}, \emptyset)$; so by ω-consistency, $T \nvdash \exists z Stop(\overline{\mathsf{s}}, \overline{\mathsf{s}}, z, \emptyset)$. This is impossible, $T \nvdash \sim\sim\mathscr{H}(\overline{\mathsf{s}})$

Again, this is roughly the form in which Gödel first proved the incompleteness of arithmetic. However, as we have seen it is possible to strengthen this version of the result to drop the requirement of ω-consistency for the simple result that no consistent, recursively axiomatizable theory extending Q is negation complete.

E14.9. Use the definition problem for μ-recursive functions to show that there is no μ-recursive enumeration of the set of truths of $\mathscr{L}_{NT}$. Hint: Return to $\mathsf{umurec}(\mathsf{i}, \mathsf{n})$, $Umurec(i, n, y)$ and $Defined(\overline{\mathsf{i}})$ — this time supposing that *Umurec* expresses umurec so that if $\mathsf{f_i(n)} = \mathsf{a}$ then $\mathsf{N}[Umurec(\overline{\mathsf{i}}, \overline{\mathsf{n}}, \overline{\mathsf{a}})] = \mathsf{T}$ and if $\mathsf{f_i(n)} \neq \mathsf{a}$ then $\mathsf{N}[\sim Umurec(\overline{\mathsf{i}}, \overline{\mathsf{n}}, \overline{\mathsf{a}})] = \mathsf{T}$. Suppose there is an enumeration $\mathsf{entruth}(\mathsf{n})$ of the truths of $\mathscr{L}_{NT}$; then the characteristic function of $\mathsf{entruth}\{\mu\mathsf{y}[\mathsf{enthrm}(\mathsf{y}) = \ulcorner Defined(\overline{\mathsf{i}})\urcorner \vee \mathsf{enthrm}(\mathsf{y}) = \ulcorner\sim Defined(\overline{\mathsf{i}})\urcorner]\} = \ulcorner Defined(\overline{\mathsf{i}})\urcorner$ is $\mathsf{0}$ when the minimization finds $Defined(\overline{\mathsf{i}})$ in the enumeration, and otherwise $\mathsf{1}$.

E14.10. Use your results for μ-recursive functions from other exercises to show that if T is a recursively axiomatized theory extending Q_s, then there is a sentence $\mathscr{P}$ such that if T is consistent $T \nvdash \mathscr{P}$, and if T is ω-consistent, $T \nvdash \sim\mathscr{P}$.

14.3 Church's Thesis

We have attained a number of negative results, as T14.6 that if Q is ω-consistent then no Turing computable function $\mathsf{thrmpl}(\mathsf{n})$ returns zero just for numbers of theorems of predicate logic, and from T14.7 that no Turing machine enumerates the truths of $\mathscr{L}_{NT}$. These are interesting. But, one might very well think, if no Turing machine computes a function, then we ought simply to compute the function some *other* way. So the significance of our negative results is magnified if the Turing computable functions are, in some sense, the *only* computable functions. If in some important sense the Turing computable functions are the only computable functions, and no Turing machine computes a function, then in the relevant sense the function is not computable. Thus Church's Thesis:

CT The total numerical functions that are effectively computable by some algorithmic method are just the recursive functions.

We want to be clear first, on the *content* of this thesis, and once we know what it says on reasons for thinking that it is true.

14.3.1 The content of Church's thesis

Church's thesis makes a claim about "total numerical functions that are effectively computable by an algorithmic method." Original motivations are from the simple routines we learn in grade school for addition, multiplication, and the like. These effectively compute total numerical functions by an algorithmic method. By themselves, such methods are of interest. However, we mean to include the sorts of methods contemporary computing devices can execute. These are of considerable interest as well. Let us take up the different elements of the proposal in turn.

First, as always, a numerical function is *total* iff it is defined on the entire numerical domain. Arbitrary functions on a finite domain may be finitely specified by listing their members, and then computed by simple lookup. This was our approach with simple, but arbitrary, functions from chapter 4. The question of comuputability becomes interesting when domains are not finite (and from methods like those in the countability reference a function on an infinite domain is always comparable to one that is total). So Church's thesis is a thesis about the computability of total functions.

A function is *effectively computable* iff there is a method for finding its value for any given argument. Correspondingly, a property or relation is *effectively decidable* iff its characteristic function is effectively computable. So methods for addition and multiplication are adequate to calculate the value of the function for any inputs. Or consider a Turing machine programmed to enumerate the theorems of T, stopping with output 0 if it reaches (the number for) $\mathscr{P}$, and output 1 if it reaches $\sim\mathscr{P}$. If T is a consistent recursively axiomatized and negation complete theory, then this is an effective method for deciding the theorems of T. If $\mathscr{P}$ is a theorem, it eventually shows up in the enumeration, and the Turing machine stops with output 0. If $\mathscr{P}$ is not a theorem, $\sim\mathscr{P}$ is a theorem, so $\sim\mathscr{P}$ eventually shows up in the enumeration, and the machine stops with output 1. This was the idea behind T12.18. But if T is not negation complete, this is not an effective method for deciding theorems of T. If $\mathscr{P}$ is a theorem, it eventually shows up in the enumeration, and the machine stops with output 0. But if $\mathscr{P}$ is not a theorem and T is not negation complete, $\sim\mathscr{P}$ might also fail to be a theorem. In this case, the machine continues forever, and does not stop with output 1; so for some arguments, this method does not find the value of the characteristic function, and we have not described an *effective* method for deciding the theorems of this T.

From the start, we may agree that there is some uncertainty about the notion of an *algorithmic* method; so, for example, different texts offer somewhat different definitions. However, as we did for logical validity and soundness in chapter 1, we shall take a particular account as a technical definition — partly as clarified in examples that follow. Difficulties to the side, there does seem to be a relevant core notion: for our purposes an *algorithmic* method is a finitely constrained rule-based procedure (rote, if you will).[5]

There is some vagueness in how much "processing" is allowed in following a rule. So, "write down the value of f(n)" will not do a as a rule for arbitrary f(n); and, less dramatically, an algorithm for multiplication does not typically include instructions for required additions. However, we may take it that if some instructions are sufficient for a computer to calculate a function, then the function is algorithmically computable. Thus that a function is Turing computable is sufficient to show that it is algorithmically computable. Again, standard methods for addition and multiplication are examples of algorithmic procedures. Truth table construction is another example of a method that proceeds by rote in this way. Given the basic tables for the operators, one simply follows the rules to complete the tables and determine validity — and one could program a computer to perform the same task. Thus validity in sentential logic is effectively decidable by an algorithmic method. In contrast, derivations are not an algorithmic method. The strategies are helpful! But, at least in complex cases, there may come a stage where insight or something like lucky guessing is required. And at such a stage, you are not following any rules by rote, and so not following any specific algorithm to reach your result.

And algorithmic methods operate under finite constraints. In general, we shall not worry about how large these constraints may be, so long as they remain finite. Consider first, truth table construction. If this is to be an effective method for determining validity, it should return a result for any sentence. But for any $n > 0$ there are sentences with that many atomic sentences (for example, $A_1 \wedge A_2 \wedge \ldots \wedge A_n$), so the corresponding table requires 2^n rows. This number may be arbitrarily large — and a table may require more paper or memory than are in the entire universe. But, in every case, the limit is finite. So, for our purposes, it qualifies as an effective algo-

[5]We have no intention of engaging Wittgenstenian concerns about following a rule. See, for example, Kripke *Wittgenstein on Rules and Private Language*.

rithmic method. Contrast this case with a device, which we may call "god's mind," that stores all the theorems of predicate logic sorted in order of their Gödel numbers. To calculate whether $\mathcal{P}$ is a theorem, simply search up to the Gödel number of $\mathcal{P}$ to see if that sentence is in the database: if it is, $\mathcal{P}$ is a theorem, if it is not $\mathcal{P}$ is not a theorem. It is not our intent to deny the existence of god, or that one might very well solve mathematical problems by prayer (though this might not go over very well on examinations which require that you show your work)! But, insofar as a device requires infinite memory or the like, it will not for our purposes count as an algorithmic method.

Or consider again a Turing machine programmed to enumerate the theorems of T, stopping with output 0 if it reaches (the number for) $\mathcal{P}$, but continuing forever if $\mathcal{P}$ does not appear. One might suppose the information that $\mathcal{P}$ is not a theorem is contained already in the fact *that the machine never halts*, and that god or some being with an infinite perspective might very well extract this information from the machine. Perhaps so. But this method is not algorithmic just because it requires the infinite perspective. Still, there are interesting attempts to attain the effect of this latter machine without appeals to god. Consider, first, "Zeno's machine." As before, the machine enumerates theorems, this time flashing a light if $\mathcal{P}$ appears in the list. However, for some finite time t (say 60 seconds), this machine takes its first step in $t/2$ seconds, its second step in $t/4$ seconds, and for any n, step n in $t/2^n$ seconds. But the sum of $t/2 + t/4 + \ldots = t$, and the Turing machine runs through all of infinitely many steps in time t. So start the machine. If the light flashes before t seconds elapse, $\mathcal{P}$ is a theorem. If t elapses, the machine has run through all of infinitely many steps, so if the light does not flash, $\mathcal{P}$ is not a theorem.

One might object this proposal reduces to a tautology of the sort, "If such-and-such (impossible) circumstances obtain, then the theorems are decidable." Great, but who cares? However, we should not reject the general strategy out-of-hand. From even a very basic introduction to special relativity, one is exposed to time dilation effects (for a simple case see the time dilation reference). General relativity allows a related effect. Where special relativity applies just to reference frames moving at constant velocity relative to one another, general relativity allows accelerated frames. And it is at least consistent with the laws of general relativity for one frame to have an infinite elapsed time, while another's time is finite.[6] So, for a Malament-Hogarth (MH) machine, put a Turing machine in the one frame and an observer in the other.

[6]Students with the requisite math and physics background might be interested in Hogarth, "Does General Relativity Allow an Observer To View an Eternity In a Finite Time?" See also Earman and Norton, "Forever is a Day," and for the same content, chapter 4 of Earman, *Bangs, Crunches, Whimpers, and Shrieks* (but with additional, though still difficult, setup in earlier chapters of the text).

The Turing machine operates in the usual way in its frame enumerating the theorems forever. If $\mathcal{P}$ is a theorem, it sends a signal back to the observer's frame that is received within the finite interval. From the observer's perspective, this machine runs through infinitely many operations. So if a signal is received in the finite interval, $\mathcal{P}$ is a theorem. If no signal is received in the finite interval, then $\mathcal{P}$ is not a theorem. (And similarly, the MH machine might search for a counterexample to the Goldbach conjecture, or the like.) There is considerable room for debate about whether such a machine is physically possible. But, even if physically realized, it is not *algorithmic*. For we require that an algorithmic method terminates in a finite number of steps.

Church's thesis is thus that the total numerical functions that are effectively computable by some algorithmic method are the the same as the recursive functions. Suppose we obtain a negative result that some function is not algorithmically computable. Even with the finite limits we have placed on memory, number of instructions and the like, the negative result remains of considerable interest: So long as a routine follows definite rules, no (finite) amount of parallel processing, high-speed memory, nanotechnology, and so forth is going to make a difference — the function remains uncomputable.

14.3.2 The basis for Church's thesis

It is widely accepted that Church's thesis is true, but also that it is not susceptible to *proof*. We shall return to the question of proof. There are perhaps three sorts of reasons that have led philosophers, computer scientists and logicians to think it is true. (i) A number of independently defined notions plausibly associated with computability converge on the recursive functions. (ii) No plausible counterexamples — algorithmically computable functions not recursive, have come to light. And (iii) there is a sort of rationale from the nature of an algorithm. This last may verge on, or amount to, demonstration of Church's thesis.

Independent definitions. We have already seen that the Turing computable functions are the same as the recursive functions. And we are in a position to close another loop. From T12.16, any recursive function is captured by a recursively axiomatized consistent theory extending Q. But also,

T14.10. Every (total) function that can be captured by a consistent recursively axiomatized theory is recursive.

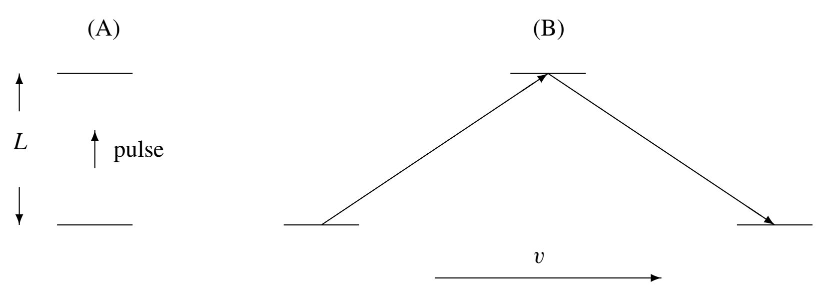
Suppose a function $\mathsf{f(m)} = \mathsf{n}$ can be captured in a consistent recursively axiomatized theory T; then there is some $\mathcal{F}(x, y)$ such that if $\langle \mathsf{m}, \mathsf{n} \rangle \in \mathsf{f}$,

Simple Time Dilation

It is natural to think that, just as a wave in water approaches a boat faster when the boat is moving is moving toward it than when the boat is moving away, so light would approach an observer faster when she is moving toward it, and more slowly whens she is moving away. But this is not so. The 1887 Michelson-Morley experiment (and many others) verify that the speed of light has the *same* value for all observers. Special relativity takes as foundational:

1. The laws of physics may be expressed in equations having the same form in all frames of reference moving at constant velocity with respect to one another.
2. The speed of light in free space has the same value for all observers, regardless of their state of motion.

These principles have many counterintuitive consequences. Here is one: Consider a clock which consists of a pulse of light bouncing between two mirrors separated by distance L as in (A) below. Where c is the constant speed of light, the time between ticks is the distance traveled by the pulse divided by its speed L/c.



Now consider the same clock as observed from a reference frame relative to which it is in motion, as in (B). The speed of light remains c (instead of being increased, as one might expect, by the addition of the horizontal component to its velocity). But the distance traveled between ticks is greater than L, so the time between ticks is greater than L/c — which is to say the clock ticks more slowly from the perspective of the second frame.

One might wonder happens if this clock is rotated 90 degrees so that the pulse is bouncing parallel to the direction of motion, or what would happen if time were measured by a pendulum clock. But within a frame, everything is coordinated according to the usual laws: On special relativity, there are coordinated changes to length, mass and the like so that the effect is robust. As observed from a reference frame relative to which the frame is in motion, time, mass, and length are distorted together. For further discussion, consult any textbook on introductory modern physics.

then $T \vdash \mathcal{F}(\overline{\mathsf{m}},\overline{\mathsf{n}})$ and if $\langle \mathsf{m},\mathsf{n}\rangle \notin \mathsf{f}$ then $T \vdash \sim\mathcal{F}(\overline{\mathsf{m}},\overline{\mathsf{n}})$; and from the latter, since T is consistent, $T \nvdash \mathcal{F}(\overline{\mathsf{m}},\overline{\mathsf{n}})$. But since f is a function, if $\langle \mathsf{m},\mathsf{n}\rangle \in \mathsf{f}$, any $\mathsf{k} \neq \mathsf{n}$ is such that $\langle \mathsf{m},\mathsf{k}\rangle \notin \mathsf{f}$; so that $T \nvdash \mathcal{F}(\overline{\mathsf{m}},\overline{\mathsf{k}})$. Since T is recursively axiomatized there is a recursive PRFT. Suppose $\langle \mathsf{m},\mathsf{n}\rangle \in \mathsf{f}$; then (i) for $\mathsf{b} = \ulcorner\mathcal{F}(\overline{\mathsf{m}},\overline{\mathsf{n}})\urcorner$ there is some a such that PRFT(a, b); and (ii) for $\mathsf{k} \neq \mathsf{n}$, there is no $\mathsf{b}' = \ulcorner\mathcal{F}(\overline{\mathsf{m}},\overline{\mathsf{k}})\urcorner$ such that for some a, PRFT(a, b′).

Intuitively, we can find the value of f(m) by searching the theorems until we find one of the sort $\mathcal{F}(\overline{\mathsf{m}},\overline{\mathsf{n}})$; and from this derive the value n. More formally: First, for the number of $\mathcal{F}(\overline{\mathsf{m}},\overline{\mathsf{n}})$,

$$\mathsf{numf}(\mathsf{m},\mathsf{n}) =_{def} \mathsf{formsub}[\mathsf{formsub}(\ulcorner\mathcal{F}(x,y)\urcorner,\ulcorner x\urcorner,\mathsf{num}(\mathsf{m})),\ulcorner y\urcorner,\mathsf{num}(\mathsf{n})]$$

Recall that formsub(p, v, s) takes the Gödel numbers of a formula $\mathcal{P}$, variable x and term s and returns the number of $\mathcal{P}^x_s$; and num(m) returns the Gödel number of the standard numeral for m. So this gives the Gödel number of $\mathcal{F}(\overline{\mathsf{m}},\overline{\mathsf{n}})$ as a function of m and n. By (loose) analogy with code from chapter 12 (p. 607),

$$\mathsf{codef}(\mathsf{m}) =_{def} \mu \mathsf{z}[\mathsf{len}(\mathsf{z}) = 2 \wedge \textsc{prft}(\mathsf{exp}(\mathsf{z},0),\mathsf{numf}(\mathsf{m},\mathsf{exp}(\mathsf{z},1)))]$$

So codef(m) is of the sort $2^{\mathsf{a}} \times 3^{\mathsf{n}}$, where a numbers a proof of $\mathcal{F}(\overline{\mathsf{m}},\overline{\mathsf{n}})$; that is, exp(z, 0) numbers a proof of numf(m, exp(z, 1)). But there is only one n that could result in a proof of $\mathcal{F}(\overline{\mathsf{m}},\overline{\mathsf{n}})$. So,

$$\mathsf{f}(\mathsf{m}) = \mathsf{exp}(\mathsf{codef}(\mathsf{m}),1)$$

And n is easily recovered from codef. So f(m) is a recursive function.

We use the $\mathcal{F}(x,y)$ that captures f(m) to generate the recursive f(m). So a function is captured in a recursively axiomatized consistent theory iff it is recursive. And increasing the power of a deductive system from Q to PA and beyond does not extend the range of captured functions. So the recursive functions, Turing computable functions and functions captured by a recursively axiomatized consistent theory extending Q are the same.[7]

E14.11. Given that *Plus*(x,y) captures plus(m, n), apply the method of T14.10 to show that plus is recursive.

[7]And there are more. Church himself was originally impressed by an equivalence between his *lambda calculus* and the recursive functions. As additional examples, Markov algorithms are discussed in Mendelson, *Introduction to Mathematical Logic*, §5.5; abacus machines in Boolos et al., *Computability and Logic*, §5; see below for discussion of the Kolmogorov-Uspenskii machine.

Failure of counterexamples. Another reason for accepting Church's thesis is the failure to find counterexamples. This may be very much the same point as before: When we set out to define a notion of computability, or compute a function, what we end up with are recursive functions, rather than something other. Of course, god's mind, Zeno's machine, an MH machine, or the like might compute a non-recursive function. Perhaps there are such devices. However, on our account, they are not algorithmic. What we do not seem to have are algorithmic methods for computing non-recursive functions.

But also in this category of reasons to accept Church's thesis is the failure of a natural strategy for showing that Church's thesis is false. Suppose one were to propose that the *primitive* recursive functions are all the computable functions, and so that regular minimization is redundant (perhaps you have had this very idea). Here is a way to see this hypothesis false:

Observe that the primitive recursive functions are recursively enumerable. For this, we introduce a language $\mathcal{L}_R$ for an alternative representation of the recursive functions. The syntax of this language is developed in the usual way. Symbols are Z^1, S^1, I_i^n, $Comp^n$ and Rec^n with parentheses and comma. Then,

LR (b) If $\mathcal{P}^n$ is Z^1, S^1 or I_i^n then $\mathcal{P}^n$ is a *formula*.

(c) If $\mathcal{P}^m$ and $\mathcal{Q}_1^n \dots \mathcal{Q}_m^n$ are formulas, then $Comp^n(\mathcal{P}^m, \mathcal{Q}_1^n \dots \mathcal{Q}_m^n)$ is a *formula*.

(r) If $\mathcal{G}^n$ and $\mathcal{H}^{n+2}$ are formulas, then $Rec^{n+1}(\mathcal{G}^n, \mathcal{H}^{n+2})$ is a *formula*.

(cl) Any formula can be formed by repeated application of these rules.

These expressions may be exhibited on trees in the usual way. So, for example, $Rec^2(I_1^1, Comp^3(S^1, I_3^3))$ is a formula.

(K)

I_1^1 S^1 I_3^3 by LR(b)

$Comp^3(S^1, I_3^3)$ by LR(c)

$Rec^2(I_1^1, Comp^3(S^1, I_3^3))$ by LR(r)

These expressions may be interpreted so that each $\mathcal{P}^n$ represents a recursive function that applies to n objects. Say $\vec{\mathsf{x}}$ is $\mathsf{x}_1 \dots \mathsf{x}_n$.

IR (z) $\mathsf{I}[Z^1](\mathsf{x}) = \mathsf{zero}(\mathsf{x})$

(s) $\mathsf{I}[S^1](\mathsf{x}) = \mathsf{suc}(\mathsf{x})$

(i) $\mathsf{I}[I_i^n](\vec{\mathsf{x}}) = \mathsf{idnt}_i^n(\vec{\mathsf{x}})$

(c) $\mathsf{I}[Comp^n(\mathcal{P}^m, \mathcal{Q}_1^n \dots \mathcal{Q}_m^n)](\vec{\mathsf{x}}) = \mathsf{I}[\mathcal{P}^m](\mathsf{I}[\mathcal{Q}_1^n](\vec{\mathsf{x}}) \dots \mathsf{I}[\mathcal{Q}_m^n](\vec{\mathsf{x}}))$

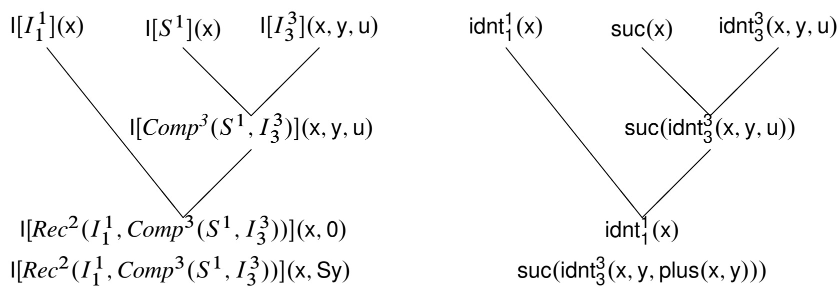
(r) $\mathsf{I}[Rec^{n+1}(\mathcal{G}^n, \mathcal{H}^{n+2})](\vec{\mathsf{x}}, 0) = \mathsf{I}[G^n](\vec{\mathsf{x}})$

$\mathsf{I}[Rec^{n+1}(\mathcal{G}^n, \mathcal{H}^{n+2})](\vec{\mathsf{x}}, \mathsf{Sy}) = \mathsf{I}[H^{n+2}](\vec{\mathsf{x}}, \mathsf{y}, \mathsf{I}[Rec^{n+1}(\mathcal{G}^n, \mathcal{H}^{n+2})](\vec{\mathsf{x}}, \mathsf{y}))$

Observe that we apply a *generalized* version of composition on which $\mathsf{I}[\mathcal{Q}_1^n](\vec{\mathsf{x}}) \dots \mathsf{I}[\mathcal{Q}_m^n](\vec{\mathsf{x}})$ are substituted respectively for the variables of $\mathsf{I}[\mathcal{P}^m]$. Clearly, a generalized composition results from multiple applications of our familiar singular form. And singular composition can be seen as an instance of the generalized form: Say we have $\mathcal{P}(u, v, w)$ and $\mathcal{Q}(u, y, z)$ and want $\mathcal{P}(u, \mathcal{Q}(u, y, z), w)$. Let $\vec{x} = u, w, y, z$ and take $Comp^4(\mathcal{P}^3, I_1^4, Comp^4(\mathcal{Q}^3, I_1^4, I_3^4, I_4^4), I_2^4)$. The result applies generalized compositions, and is equivalent to the composition we want.

As an example for IR, $Rec^2(I_1^1, Comp^3(S^1, I_3^3))$ is plus. Corresponding to the above tree are functions,

(L)



where plus(x, y) is $\mathsf{I}[Rec^2(I_1^1, Comp^3(S^1, I_3^3))](\mathsf{x}, \mathsf{y})$. And the conditions for plus are as we expect.

Now a recursive enumeration of the primitive recursive functions is straightforward. From their interpretation, an enumeration of the formulas is an enumeration of the primitive recursive functions: Assign numbers to the symbols and formulas of $\mathcal{L}_R$; find a recursive PRWFF(n) true of numbers for formulas; and enumerate,

$\mathsf{eprfnc}(0) = \mu \mathsf{z}[\mathsf{PRWFF}(\mathsf{z})]$

$\mathsf{eprfnc}(\mathsf{Sn}) = \mu \mathsf{z}[\mathsf{z} > \mathsf{eprfnc}(\mathsf{n}) \wedge \mathsf{PRWFF}(\mathsf{z})]$

So there is a recursive enumeration of the primitive recursive functions, there is an enumeration of the functions of one free variable, and so forth.

Consider an enumeration of the primitive recursive functions of one free variable and an array as follows.

(M)

	0	1	2	...
f_0	$\mathbf{f_0(0)}$	$f_0(1)$	$f_0(2)$	
f_1	$f_1(0)$	$\mathbf{f_1(1)}$	$f_1(2)$	
f_2	$f_2(0)$	$f_2(1)$	$\mathbf{f_2(2)}$	
$\vdots$				

And consider the function $d(n) = f_n(n) + 1$. This function is *computable*; for any n: (i) run the enumeration to find f_n; (ii) run f_n to find $f_n(n)$; (iii) add one. Since each step is recursive, the whole is computable. But $d(n)$ is not primitive recursive: $d(0) \neq f_0(0)$; $d(1) \neq f_1(1)$; and in general, $d(n) \neq f_n(n)$; so d is not identical to any of the primitive recursive functions. So there are computable functions that are not primitive recursive.

It is natural to think that a related argument would show that not all computable functions are recursive: recursively enumerate the recursive functions; then diagonalize to find a computable function not on the list. But this does not work! It is an entirely "grammatical" matter to identify the primitive recursive functions — the function $\mathsf{eprfnc}(n)$ results purely as a matter of form. But there is no parallel method for the recursive fuctions. This clear already by the halting and definition problems (for the latter see E14.7) — there is no recursive way to say in general whether a function is regular, and so to identify functions as recursive. But we may make the point by another diagonal argument (here applied to Turing machines).

> Suppose there is an enumeration of Turing machines to compute recursive functions (of one free variable) and consider an array as follows.

(N)

	0	1	2	...
Π_0	$\mathbf{\Pi_0(0)}$	$\Pi_0(1)$	$\Pi_0(2)$	
Π_1	$\Pi_1(0)$	$\mathbf{\Pi_1(1)}$	$\Pi_1(2)$	
Π_2	$\Pi_2(0)$	$\Pi_2(1)$	$\mathbf{\Pi_2(2)}$	
$\vdots$				

> Let $\Delta(n)$ be $\Pi_n(n) + 1$. From T14.2 $\Pi_n(n)$ computes the recursive $f(n) = \mathsf{decode}(\mathsf{right}(n, n, \mu j[\mathsf{stop}(n, n, j) = 0]))$; so $f(n) + 1$ computes $\Delta(n)$. And since $f(n) + 1$ is recursive, $\Delta(n)$ is a Turing program of one free variable; so $\Delta(n)$ appears in the enumeration of Turing programs. But this is impossible: $\Delta(0) \neq \Pi_0(0)$; $\Delta(1) \neq \Pi_1(1)$; and in general $\Delta(n) \neq \Pi_n(n)$. Reject the assumption: there is no enumeration of Turing machines to compute recursive functions.

There is an enumeration of Turing machines; but as in the case of a machine that never halts, not every Turing machine computes a total function. Thus the enumeration of Turing machines does not automatically convert to an enumeration of Turing machines to compute recursive functions. And we are in fact blocked from recursively enumerating the recursive functions. So we are blocked from the proposed means of finding a computable function that is not a recursive function. So this attempt to find a counterexample to Church's thesis fails.

E14.12. (i) Write down the $\mathscr{L}_R$ expression that corresponds to times. (ii) Assign numbers to expressions of $\mathscr{L}_R$ and produce the relation PRECWFF to complete the demonstration that there is an enumeration of primitive recursive functions. (iii) Extend the demonstration that there is an enumeration of primitive recursive functions to an enumeration emurec of μ-recursive functions (as from E14.7).

The nature of an algorithm. There are also reasons for Church's thesis from the very nature of an algorithm.[8] Perhaps the "received wisdom" with respect to Church's thesis is as follows.

> The reason why Church's [Thesis] is called a *thesis* is that it has not been rigorously proved and, in this sense, it is something like a "working hypothesis." Its plausibility can be attested inductively — this time not in the sense of mathematical induction, but "on the basis of particular confirming cases." The Thesis is corroborated by the number of intuitively computable functions commonly used by mathematicians, which can be defined within recursion theory. But Church's Thesis is believed by many to be destined to *remain* a thesis. The reason lies, again, in the fact that the notion of effectively computable function is a merely intuitive and somewhat fuzzy one. It is quite difficult to produce a completely rigorous proof of the equivalence between intuitively computable and recursive functions, precisely because one of the sides of the equivalence is not well-defined (Berto, *There's Something About Gödel*, pp. 76-77).

There are a couple of themes in this passage. First, that Church's thesis is typically accepted on grounds of the sort we have already considered. Fair enough. But second that it is not, and perhaps cannot, be proved. The idea seems to be that the recursive functions are a precise mathematically defined class, while the algorithmically

[8]Material in this section is developed from Smith, *An Introduction to Gödel's Theorems*, chapter 45; Smith, "Squeezing Arguments"; along with Kolmogorov and Uspenskii, "On the Definition of an Algorithm." See also Black, "Proving Church's Thesis."

computable functions are not. Thus there is no hope of a demonstrable equivalence between the two.

But we should be careful. Granted: If we start with an inchoate notion of computable function that includes, at once, calculations with pencil and paper, calculations on the latest and greatest supercomputer, and calculations on Zeno's machine, there will be no saying whether the computable functions definitely are, or are not, identical to the Turing computable functions. But this is not the notion with which we are working. We have a relatively refined technical account of algorithmic computability. Of course, it is not yet a *mathematical* definition. But neither are our chapter 1 accounts of logical validity and soundness; yet we have been able to show in T9.1 that any argument that is quantificationally valid (in our mathematical sense) is logically valid. And similarly, the whole translation project of chapter 5 assumes the possibility of moving between ordinary and mathematical notions. It is at least possible that an informally defined predicate might pick out a precise object. The question is whether we can "translate" the notion of an algorithm to formal terms.

So let us turn to the hard work of considering whether there is an argument for accepting Church's thesis. A natural first suggestion is that the step-by-step and finite nature of any algorithm is always within the reach of, or reflected by, some Turing program or recursive function, so that the algorithmically computable functions are inevitably recursively computable.[9] Already, this may amount to a consideration or reason in favor of accepting the Thesis. In chapter 45 of his *An Introduction to Gödel's Theorems*, Peter Smith advances a proposal according to which such considerations amount to proof.

Smith's overall strategy involves "squeezing" algorithmic computability between a pair of mathematically precise notions. Even if a condition C (say, "being a tall person") is vague, it might remain that there is some completely precise sufficient condition S (being over seven feet tall), such that anything that is S is C, and perfectly precise necessary condition N (being over five feet tall) such that anything that is C is N. So,

$$S \implies C \implies N$$

If it should also happen that N implies S, then the loop is closed, so that,

$$S \iff C \iff N$$

And the target condition C is equivalent to (squeezed between) the precise necessary and sufficient conditions. Of course, in our simple example, N does not imply C:

[9]This idea is contained already in the foundational papers of Church, "An Unsolvable Problem," and Turing, "On Computable Numbers."

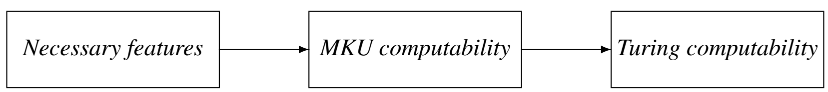
being over five feet tall does not imply being over seven feet tall.

For Church's thesis, we already have that Turing computability is sufficient for algorithmic computability. So what is required is some necessary condition so that,

$$T \quad \Longrightarrow \quad A \quad \Longrightarrow \quad N$$

Turing computability implies algorithmic computability and algorithmic computability implies the necessary condition. Church's thesis follows if, in addition, N implies Turing computability. As it turns out, we shall be able to specify a condition N which (mathematically) implies T. It will be more controversial whether A implies N.

The argument has three stages: The idea is that, (i) there are some necessary features of an algorithm, such that any algorithm has those features; (ii) any routine with those features is embodied in a modified Kolmogorov-Uspenskii (MKU) machine; (iii) every function that is MKU computable is recursive, and so Turing computable.



The result is that MKU computability works as as the precise condition N in the squeezing argument: A implies N, and N implies T. So T iff A iff N, and Church's thesis is established — or no less plausible than is the conclusion of this argument.

Perhaps the following are necessary conditions on any algorithm, so that any algorithm satisfies the conditions. If, additionally, we hold that any routine which satisfies the constraints is an algorithm, then the conditions are necessary and sufficient — so we may see them as an extension or sharpening of our initial more sketchy account. At this stage, though, the important requirement is that any algorithm satisfies the conditions.[10]

AC (1) There is some *dataspace* consisting of a finite array of "cells" which may stand in some relations R_0, $R_1 \dots R_a$ and contain some entities (usually symbols) $s_0, s_1 \dots s_b$.

(2) At every stage in a computation, there is some finite "active" portion of the dataspace upon which the algorithm operates.

[10]Smith seems to grant that some such conditions are necessary, even though some method may satisfy the conditions yet fail to count as an algorithm. Perhaps this is because he is impressed by the initial examples of routines implemented by human agents with relatively limited computing power. This is not a problem for his squeezing argument, since the corresponding recursive function may yet be computable by some other method which satisfies more narrow constraints — for example, by a Turing machine.

(3) The body of the algorithm includes finitely many instructions for modifying the active portion of the dataspace depending on its character, and for jumping to the next set of instructions.

(4) For the calculation of a function $\mathsf{f}(\vec{\mathsf{x}}) = \mathsf{y}$ there is some finite initial representation of $\vec{\mathsf{x}}$ and some way to read off the value of y, after a finite number of steps.

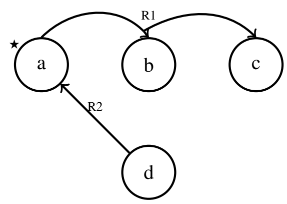
So this sets up an algorithm abstractly described. It is hard to see how an algorithm would not involve some space, portions of which would stand in different relations. At any given stage, the algorithm operates on some portion of the space, where these operations may depend upon, and modify the arrangement of the active space. The algorithm itself consists of some instructions for operating on the dataspace, where these are generically of the sort, "if the active area is of type t, perform action a, and go to new instructions q." The calculation of a function $\mathsf{f}(\vec{\mathsf{x}})$ somehow takes $\vec{\mathsf{x}}$ as an input, and gives a way to read off the value of y as an output. And an algorithm terminates in a finite number of steps.

Observe that the squeezing argument is effective to the extent that we begin with the notion of an algorithm and show that for any algorithm there is a Turing machine equivalent to it. It is cast into doubt if we start with the notion of a Turing machine and force the notion of an algorithm to match. Thus it is important that we are simply spelling out the idea of an algorithm — of what is required of a rote, rule-based based procedure.

Also the finite constraints on the dataspace, relations, symbols and area in (1) and (2) above seem to be consequences of (3) and (4): There is some upper bound to the space modified by instructions from a finite collection, each member of which modifies at most a finite area. Then beginning with a finite initial representation of some $\vec{\mathsf{x}}$, including finitely many cells of the dataspace standing in finitely many relations, filled with finitely many symbols and then modifying finite portions of the space finitely many times, all we are going to get are finitely many cells, standing in finitely many relations, filled with finitely many symbols.

On the face of it, given their extreme simplicity, it is not obvious that Turing machines compute every algorithmically computable function. But a related device, the MKU machine (modified from Kolmogorov and Uspenskii, "On the Definition of an Algorithm") purports to implement conditions along these lines.

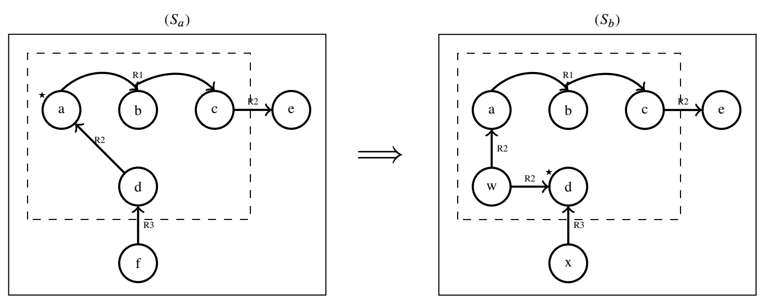
MKU (1) There are some cells c_0, $c_1 \ldots c_a$ which may stand in relations R_0, $R_1 \ldots R_b$ and contain symbols s_0, $s_1 \ldots s_c$. In simple cases, we may think of such arrangements graphically as follows,

(O) 

R2 is a binary relation and R1 tertiary. Each such relation constitutes an *edge*.

(2) Among the one-place relations is an *origin* property such that exactly one cell has it — as indicated by ⋆ above. Then the active area includes all cells on paths $\leq n$ edges from the origin. From (O), cells other than the origin are all one edge from the origin cell.

(3) Instructions are finitely many quadruples of the sort $\langle q_i, S_a, S_b, q_j \rangle$ where q_i and q_j are instruction labels; S_a describes an active area; and S_b a state with which the active area is to be replaced. Associate each cell in S_a with the least number of edges between it and the origin; let n be the greatest such integer in S_a; this n remains the same in every quadruple with label q_i, though the value of n may vary as q_i varies. Again, instructions are a function in the sense that no instruction has $\langle q_i, S_a \rangle$ the same but $\langle S_b, q_j \rangle$ different. We may see S_a and S_b as follows.

(P) 

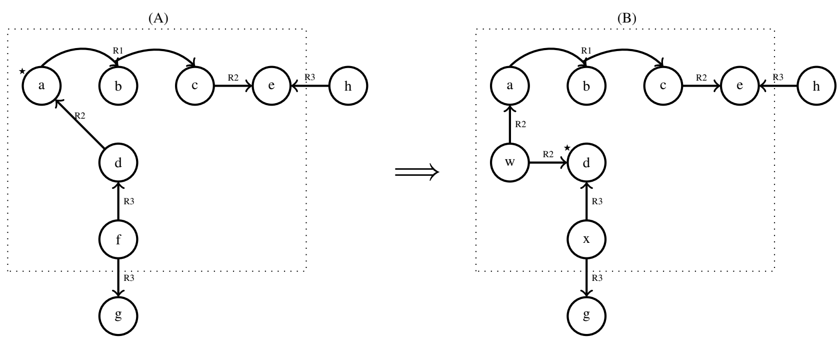
In this case $n = 2$. The active area S_a is replaced by the configuration S_b. The concentric rectangles indicate the "boundary" cells which may themselves be related to cells not part of the active area; the replacing area must have a boundary with cells to match boundary cells of the active area.

(4) There is some finite initial setup, and some means of reading off the final value of the function (for different relation and symbol sets, these may be different). We think of the origin cell as the "machine head," where an

algorithm always begins with an instruction label $q_i = 1$ and terminates when $q_i = 0$.

So an MKU machine is a significant generalization of a Turing machine. We allow arbitrarily many symbols. And the dataspace is no longer a tape with cells in a fixed linear relation, but a space with cells in arbitrary relations which may themselves be modified by the program. Instructions respond to, and modify, not just individual cells, but arbitrarily large areas of the dataspace. Still, it remains that an instruction q_i is of the sort, if S_a perform action A and go to instruction q_j. So, the instruction (P) might be applied to get,

(Q)



As indicated by the dotted line, the dataspace (A) has an active area of the sort required in instruction (P); so the active area is replaced according to the instruction for the resultant space (B). The example is arbitrary. But that is the point: The machine allows arbitrary rote modifications of a dataspace.

Observe that instructions with $S_a \neq S'_a$ might both map onto a given dataspace in case the number n of edges from the origin in S_a is different from S'_a (say an active area with a box for $n = 1$ inside the box in (Q)). But the consistency requirement is satisfied with constant n: for consistency, it is sufficient to require that so long as $n(q_i, S_a)$ is a constant, there is no instruction with $\langle q_i, S_a \rangle$ the same but $\langle S_b, q_j \rangle$ different.

Now every MKU computable function is recursive.

T14.11. Every MKU computable function is a recursive function.

We have been through this sort of thing before. And there are different ways to proceed. I indicate only some natural first steps. Begin assigning numbers to labels, symbols, cells and relations in some reasonable way.

a. $g[q_i] = 3 + 8i$

b. $g[s_i] = 5 + 8i$

c. $g[c_i] = 7 + 8i$

d. $g[r^i_j] = 9 + 8(2^i \times 3^j)$

Then number for a *page* is $\pi_0^{\langle c_i \rangle} \times \pi_1^{\langle s_a \rangle} \times \ldots \times \pi_n^{\langle s_b \rangle}$, and for an *edge* $\pi_0^{\langle r^i_j \rangle} \times \pi_1^{\langle c_{a1} \rangle} \times \ldots \times \pi_i^{\langle c_{ai} \rangle}$. So a page is a cell with some symbols, and an edge is an i-place relation applied to i cells. Some *data* is a sequence of pages with distinct cell numbers, and a *lattice* is a sequence of distinct edges. Cells are (*immediately*) *connected* on an edge when both cells are members of it, and *connected* on a lattice when there is a sequence of cells from the lattice, beginning with the one, ending with the other such that each is immediately connected to the next. A *space* is a lattice with exactly one origin and every cell connected to all the others. A *dataspace* is of the sort $\pi_0^m \times \pi_1^n$ where m numbers some data, n a space, and every cell from m appears in n.

After that, with considerable work, MKUMACH(n) numbers the MKU machines. (Given the potentially vast array of finite spaces, rather than supplementing the machine with repeating commands for every missing instruction, it is simplest to include a single label that loops on the origin, such that the machine defaults to it.) kumachs(i, m, n) numbers an instruction as a function of the number for the machine, initial label, and dataspace. (Where cells are numbered, some S_a matches the active portion of a dataspace when there is a *map* on cells that makes S_a match the active area.) For machine i with input n, mkuspace(i, n, j) and mkustate(i, n, j) give the current number of the dataspace and state. And mkustop(i, n, j) takes the value zero when the machine is stopped. Then,

$$f(n) = \text{mkudecode}(\text{mkuspace}(i, n, \mu j[\text{mkustop}(i, n, j) = 0]))$$

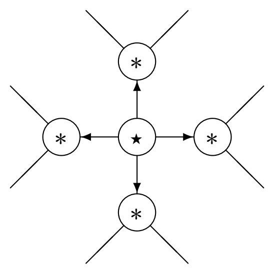
It is a chore to work this out (and you have an opportunity to do so in exercises). But it should be clear that it can be done. Then any MKU computable function is recursive, and therefore every MKU computable function is Turing computable.

Given this, the squeezing argument is complete: Turing computability implies algorithmic computability and algorithmic computability implies MKU and so Turing computability. So the algorithmically computable functions are the same as the Turing computable functions. So Church's thesis! This argument is just as strong as the premise that algorithmic computability implies MKU and so Turing computability. For this, we have *translated* an informal notion into a formal one. Insofar as translation is not itself a formal procedure, the result is not formal proof of Church's thesis. Perhaps it is difficult to imagine an algorithmic method that does not conform to AC and then MKU. But failure of imagination is not the same as proof. This leaves space for different objections:

First, one might worry that the account AC of an algorithm is insufficient in some respect. But AC is offered as a further exposition or sharpening of what it is to be an algorithm. Given this, our version of Church's thesis applies to it. An argument about whether Church's thesis applies to a class C of functions is not undercut by observing that there are classes other than C.

Still, one might worry that the MKU machine does not compute every algorithm from AC. Against this, there are a couple of replies. First, careful about what the MKU machine can do. Say we are interested in parallel computing, whether by persons following instructions or by computing devices. An MKU machine has but a single origin; this might seem to be a problem. Still, an active area might have many "shapes" — and things might be set up as follows,

(R)



with "satellite" centers, to achieve the effect of parallel computing. Similarly, with a bit of thought, one can see how the MKU machine might achieve the effect of absolute addressing or bounded quantifiers other than 'all' and 'some' — as 'most' or the like. So it is important to recognize the generality already built into the MKU machine.

Perhaps, though, the objection goes through and some algorithmic method really is beyond the reach of the MKU machine. So for example some algorithm might require physical actions other than symbol manipulation. Consider a method for truth table construction with the instruction, "whack yourself in the head three times and write a T in the first row of the first column." An MKU machine does not have a head, and so cannot perform this action. More seriously, we might consider actions as applied to, say, a physical abacus — as "move the bead on the second wire to the leftmost available position." The MKU machine does not move physical beads on a wire, so it does not perform addition on an abacus. Still, it should be possible to *number* the states of an abacus, and to represent the successive states so as to calculate any function that can be worked on the physical device. In this case, the claim is not that the MKU machine *effectuates* every algorithm, but rather that it *models* every algorithm. Supposing this is sustained, the argument for Church's thesis stands.

So we are not left with a formal proof of Church's thesis. Rather we have a (powerful) *case* from the independent definitions, the failure of counterexamples and the nature of an algorithm for the result that Church's thesis is true. Plausibly, there is no formal proof that you have a head. Still, there is a strong case to establish that you do! Similarly our case may seem sufficient to establish Church's thesis. To the extent that Church's thesis is either plausible or established, our limiting results become full-fledged *incomputability* results with applications to logic and computing more generally. In addition, from Church's thesis, the *computability* of a function implies that it is recursive. Having attained Church's thesis only at the very end, we have not applied the thesis in this way. But one might move from the observation that some function is computable, through the thesis, to the result that the function is recursive. And this is frequently done!

Theorems of chapter 14

T14.1 There is a recursive enumeration of the Turing machines.

T14.2 Every Turing computable function is a recursive function.

T14.3 Every recursive function is Turing computable.

T14.4 There is no Turing machine $\mathsf{H}(\mathsf{i})$ such that $\mathsf{H}(\mathsf{i}) = 0$ if $\Pi_{\mathsf{i}}(\mathsf{i})$ halts and $\mathsf{H}(\mathsf{i}) = 1$ if it does not.

T14.5 There is no Turing machine $\mathsf{H}(\mathsf{i},\mathsf{n})$ such that $\mathsf{H}(\mathsf{i},\mathsf{n}) = 0$ if $\Pi_{\mathsf{i}}(\mathsf{n})$ halts and $\mathsf{H}(\mathsf{i},\mathsf{n}) = 1$ if it does not.

T14.6 If Q is ω-consistent, then no Turing computable function $\mathsf{f}(\mathsf{n})$ is such that $\mathsf{f}(\mathsf{n}) = 0$ just in case n numbers a theorem of predicate logic.

T14.7 The set of truths of $\mathscr{L}_{NT}$ is not recursively enumerable.

T14.8 If T is a recursively axiomatized sound theory whose language includes $\mathscr{L}_{NT}$, then T is negation incomplete.

T14.9 If T is a recursively axiomatized theory extending Q, then there is a sentence $\mathcal{P}$ such that if T is consistent $T \nvdash \mathcal{P}$, and if T is ω-consistent, $T \nvdash \sim\mathcal{P}$.

T14.10 Every (total) function that can be captured by a recursively axiomatized consistent theory extending Q is recursive.

T14.11 Every MKU computable function is a recursive function.

And we mention,

CT *Church's Thesis*: The total numerical functions that are effectively computable by some algorithmic method are just the recursive functions.

E14.13. Work out codes for the MKU machine through $\mathsf{dataspace}$. Very hard core: Assuming functions $\mathsf{code}(\mathsf{n})$ and $\mathsf{decode}(\mathsf{d})$, complete the demonstration that any MKU computable function $\mathsf{f}(\mathsf{n})$ is recursive.

E14.14. For each of the following concepts, explain in an essay of about two pages, so that (college freshman) Hannah could understand. In your essay, you should (i) identify the objects to which the concept applies, (ii) give and explain the definition, and give and explicate examples (iii) where the concept applies, and (iv) where it does not. Your essay should exhibit an understanding of methods from the text.

a. The Turing computable functions, and their relation to the recursive functions.

b. The essential elements from the chapter contributing to a demonstration of the decision problem, along with the significance of Church's thesis for this result.

c. The essential elements from this chapter contributing to a demonstration of (the semantic version of) the incompleteness of arithmetic.

d. Church's thesis, along with reasons for thinking it is true, including the possibility of demonstrating its truth.

Concluding Remarks

Looking Forward and Back

We began this text in Part I setting up the elements of classical symbolic logic. Thus we began with four notions of validity: logical validity, validity in our derivation systems *AD* and *ND*, along with semantic (sentential and) quantificational validity. After a parenthesis in Part II to think about techniques for reasoning about logic, we began to put those techniques to work. The main burden of Part III was to show soundness and adequacy of our classical logic, that $\Gamma \vdash \mathcal{P}$ iff $\Gamma \vDash \mathcal{P}$. This is the good news. In Part IV we established some limiting results. These include Gödel's first and second theorems, that no consistent, recursively axiomatizable extension of Q is negation complete, and that no consistent recursively axiomatized theory extending PA proves its own consistency. Results about derivations are associated with computations, and the significance of this association extended by means of Church's thesis. This much constitutes a solid introduction to classical logic, and should position you make progress in logic and philosophy, along with related areas of mathematics and computer science.

Excellent texts which mostly overlap the content of one, but extend it in different ways are Mendelson, *Introduction to Mathematical Logic*; Enderton, *Introduction to Mathematical Logic*; and Boolos, Burgess and Jeffrey, *Computability and Logic*; these put increased demands on the reader (and such demands are one motivation for our text), but should be accessible to you now; Schonfield, *Introduction to Mathematical Logic* is excellent yet still more difficult. Smith, *An Introduction to Gödel's Theorems* extends the material of Part IV; Cooper, *Computability Theory* develops it especially from the perspective of chapter 14. Much of what we have done presumes some set theory as Enderton, *Elements of Set Theory*, or model theory as Manzano, *Model Theory* and, more advanced, Hodges, *A Shorter Model Theory*.

In places, we have touched on logics alternative to classical logic, including multi-valued logic, modal logic, and logics with alternative accounts of the conditional. A good place to start is Priest, *Non-Classical Logics*, which is profitably read with Roy, "Natural Derivations for Priest" which introduces derivations in a style much like our own. Our logic is *first-order* insofar as quantifiers bind just variables for objects. Second-order logic lets quantifiers bind variables for predicates as well (so $\forall x \forall y[x = y \rightarrow \forall F(Fx \leftrightarrow Fy)]$ expresses the *indiscernibility of identicals*). Second-order logic has important applications in mathematics, and raises important issues in metalogic. For this, see Shapiro, *Foundations Without Foundationalism*, and Manzano, *Extensions of First Order Logic*.

Philosophy of logic and mathematics is a subject matter of its own. Shapiro, "Philosophy of Mathematics and Its Logic" (along with the rest of the articles in the *Oxford Handbook*, and Shapiro, *Thinking About Mathematics* are a good place to start. Benacerraf and Putnam, *Philosophy of Mathematics* and Marcus and McEvoy, *Philosophy of Mathematics* are collections of classic articles.

Smith's online, "Teach Yourself Logic" is an excellent comprehensive guide to further resources.

Have fun!

Answers to Selected Exercises

Chapter Nine

E9.2. Set up the above induction for T9.2, and complete the unfinished cases to show that if if $\Gamma \vdash_{AD} \mathcal{P}$, then $\Gamma \vdash_{ND} \mathcal{P}$. For cases completed in the text, you may simply refer to the text, as the text refers cases to homework.

Basis: $\mathcal{Q}_1$ in A is a premise or an instance of A1, A2, A3, A4, A5, A6, A7 or A8.

(prem) From text.

(A1) From text.

(A2) From text.

(A3) If $\mathcal{Q}_1$ is an instance of A3, then it is of the form, $(\sim\mathcal{C} \to \sim\mathcal{B}) \to ((\sim\mathcal{C} \to \mathcal{B}) \to \mathcal{C})$, and we continue N as follows,

0.a	$\mathcal{Q}_a$	P
0.b	$\mathcal{Q}_b$	P
⋮		
0.j	$\mathcal{Q}_j$	P
1.1	$\quad\sim\mathcal{C} \to \sim\mathcal{B}$	A (g, $\to$I)
1.2	$\quad\quad\sim\mathcal{C} \to \mathcal{B}$	A (g, $\to$I)
1.3	$\quad\quad\quad\sim\mathcal{C}$	A (c, $\sim$E)
1.4	$\quad\quad\quad\mathcal{B}$	1.2,1.3 $\to$E
1.5	$\quad\quad\quad\sim\mathcal{B}$	1.1,1.3 $\to$E
1.6	$\quad\quad\quad\bot$	1.4,1.5 $\bot$I
1.7	$\quad\quad\mathcal{C}$	1.3-1.6 $\sim$E
1.8	$\quad(\sim\mathcal{C} \to \mathcal{B}) \to \mathcal{C}$	1.2-1.7 $\to$I
1	$(\sim\mathcal{C} \to \sim\mathcal{B}) \to ((\sim\mathcal{C} \to \mathcal{B}) \to \mathcal{C})$	1.1-1.8 $\to$I

So $\mathcal{Q}_1$ appears, under the scope of the premises alone, on the line numbered '1' of N.

(A4) From text.

(A6) If $\mathcal{Q}_1$ is an instance of A6, then it is of the form $x = x$ for some variable x, and we continue N as follows,

0.a	$\mathcal{Q}_a$	P
0.b	$\mathcal{Q}_b$	P
⋮		
0.j	$\mathcal{Q}_j$	P
1	$x = x$	=I

So $\mathcal{Q}_1$ appears, under the scope of the premises alone, on the line numbered '1' of N.

(A7) From text.

(A8) If $\mathcal{Q}_1$ is an instance of A8, then it is of the form $(x_i = y) \rightarrow (\mathcal{R}^n x_1 \ldots x_i \ldots x_n \rightarrow \mathcal{R}^n x_1 \ldots y \ldots x_n)$ for some variables $x_1 \ldots x_n$ and y, and relation symbol $\mathcal{R}^n$; and we continue N as follows,

0.a	$\mathcal{Q}_a$	P
0.b	$\mathcal{Q}_b$	P
⋮		
0.j	$\mathcal{Q}_j$	P
1.1	$x_i = y$	A $(g, \rightarrow\text{I})$
1.2	$\mathcal{R}^n x_1 \ldots x_i \ldots x_n$	A $(g, \rightarrow\text{I})$
1.3	$\mathcal{R}^n x_1 \ldots y \ldots x_n$	1.2,1.1 =E
1.4	$\mathcal{R}^n x_1 \ldots x_i \ldots x_n \rightarrow \mathcal{R}^n x_1 \ldots y \ldots x_n$	1.2-1.3 →I
1	$(x_i = y) \rightarrow (\mathcal{R}^n x_1 \ldots x_i \ldots x_n \rightarrow \mathcal{R}^n x_1 \ldots y \ldots x_n)$	1.1-1.4 →I

So $\mathcal{Q}_1$ appears, under the scope of the premises alone, on the line numbered '1' of N.

Assp: For any i, $1 \leq i < k$, if $\mathcal{Q}_i$ appears on line i of A, then $\mathcal{Q}_i$ appears, under the scope of the premises alone, on the line numbered 'i' of N.

Show: If $\mathcal{Q}_k$ appears on line k of A, then $\mathcal{Q}_k$ appears, under the scope of the premises alone, on the line numbered 'k' of N.

$\mathcal{Q}_k$ in A is a premise, an axiom, or arises from previous lines by MP or Gen. If $\mathcal{Q}_k$ is a premise or an axiom then, by reasoning as in the basis (with line numbers adjusted to $k.n$) if $\mathcal{Q}_k$ appears on line k of A, then $\mathcal{Q}_k$ appears, under the scope of the premises alone, on the line numbered 'k' of A. So suppose $\mathcal{Q}_k$ arises by MP or Gen.

(MP) From text.

(Gen) From text.

In any case then, $\mathcal{Q}_k$ appears under the scope of the premises alone, on the line numbered 'k' of N.

Indct: For any line j of A, $\mathcal{Q}_j$ appears under the scope of the premises alone, on the line numbered 'j' of N.

E9.8. Set up the above demonstration for T9.7 and complete the unfinished case to provide a complete demonstration that for any formula $\mathcal{A}$, and terms r and s,

Exercise 9.8

if $\mathscr{s}$ is free for the replaced instance of $\mathscr{r}$ in $\mathcal{A}$, then $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$.

Consider an arbitrary $\mathscr{r}$, $\mathscr{s}$ and $\mathcal{A}$, and suppose $\mathscr{s}$ is free for the replaced instance of $\mathscr{r}$ in $\mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}}$.

Basis: If $\mathcal{A}$ has no operators and some term in it is replaced, then [from text] $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$.

Assp: For any i, $0 \leq i < k$, if $\mathcal{A}$ has i operator symbols, then $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$.

Show: If $\mathcal{A}$ has k operator symbols, then $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$.

If $\mathcal{A}$ has k operator symbols, then $\mathcal{A}$ is of the form, $\sim\mathcal{P}$, $\mathcal{P} \rightarrow \mathcal{Q}$ or $\forall x \mathcal{P}$ for variable x and formulas $\mathcal{P}$ and $\mathcal{Q}$ with $< k$ operator symbols.

($\sim$) Suppose $\mathcal{A}$ is $\sim\mathcal{P}$. Then [from text] $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$.

($\rightarrow$) Suppose $\mathcal{A}$ is $\mathcal{P} \rightarrow \mathcal{Q}$. Then $\mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}}$ is $\mathcal{P}^{\mathscr{r}}/\!\!/_{\mathscr{s}} \rightarrow \mathcal{Q}$ or $\mathcal{P} \rightarrow \mathcal{Q}^{\mathscr{r}}/\!\!/_{\mathscr{s}}$. (i) In the former case [from text], $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$. (ii) In the latter case, since $\mathscr{s}$ is free for the replaced instance of $\mathscr{r}$ in $\mathcal{A}$, it is free for that instance of $\mathscr{r}$ in $\mathcal{Q}$; so by assumption, $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{Q} \rightarrow \mathcal{Q}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$; so we may reason as follows,

1.	$(\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{Q} \rightarrow \mathcal{Q}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$	prem
2.	$\mid\ \mathscr{r} = \mathscr{s}$	assp (g, DT)
3.	$\mid\ \mid\ \mathcal{P} \rightarrow \mathcal{Q}$	assp (g, DT)
4.	$\mid\ \mid\ \mid\ \mathcal{P}$	assp (g, DT)
5.	$\mid\ \mid\ \mid\ \mathcal{Q}$	3,4 MP
6.	$\mid\ \mid\ \mid\ \mathcal{Q} \rightarrow \mathcal{Q}^{\mathscr{r}}/\!\!/_{\mathscr{s}}$	1,2 MP
7.	$\mid\ \mid\ \mid\ \mathcal{Q}^{\mathscr{r}}/\!\!/_{\mathscr{s}}$	6,5 MP
8.	$\mid\ \mid\ \mathcal{P} \rightarrow \mathcal{Q}^{\mathscr{r}}/\!\!/_{\mathscr{s}}$	4-7 DT
9.	$\mid\ (\mathcal{P} \rightarrow \mathcal{Q}) \rightarrow (\mathcal{P} \rightarrow \mathcal{Q}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$	3-8 DT
10.	$(\mathscr{r} = \mathscr{s}) \rightarrow [(\mathcal{P} \rightarrow \mathcal{Q}) \rightarrow (\mathcal{P} \rightarrow \mathcal{Q}^{\mathscr{r}}/\!\!/_{\mathscr{s}})]$	2-9 DT

So $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow [(\mathcal{P} \rightarrow \mathcal{Q}) \rightarrow (\mathcal{P} \rightarrow \mathcal{Q}^{\mathscr{r}}/\!\!/_{\mathscr{s}})]$; which is to say, $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$. So in either case, $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$.

($\forall$) Suppose $\mathcal{A}$ is $\forall x \mathcal{P}$. Then [from text] $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$.

So for any $\mathcal{A}$ with k operator symbols, $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$.

Indct: For any $\mathcal{A}$, $\vdash_{AD} (\mathscr{r} = \mathscr{s}) \rightarrow (\mathcal{A} \rightarrow \mathcal{A}^{\mathscr{r}}/\!\!/_{\mathscr{s}})$.

E9.10. Prove T9.9, to show that for any formulas $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$, if $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{C}$, then $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$.

Basis: If $\mathcal{A}$ is atomic, then the only formula to be replaced is $\mathcal{A}$ itself, and $\mathcal{B}$ is $\mathcal{A}$; so $\mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$ is $\mathcal{C}$. But then $\mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$ is the same as $\mathcal{B} \leftrightarrow \mathcal{C}$. So if $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{C}$, then $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$.

Assp: For any i, $0 \leq i < k$, if $\mathcal{A}$ has i operator symbols, then if $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{C}$, then $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$.

Show: If $\mathcal{A}$ has k operator symbols, then if $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{C}$, then $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$.

If $\mathcal{A}$ has k operator symbols, then it is of the form $\sim\mathcal{P}$, $\mathcal{P} \to \mathcal{Q}$, or $\forall x\mathcal{P}$, for variable x and formulas $\mathcal{P}$ and $\mathcal{Q}$ with $< k$ operator symbols. If $\mathcal{B}$ is all of $\mathcal{A}$, then as in the basis, if $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{C}$, then $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$. So suppose $\mathcal{B}$ is a proper subformula of $\mathcal{A}$.

($\sim$) Suppose $\mathcal{A}$ is $\sim\mathcal{P}$ and $\mathcal{B}$ is a proper subformula of $\mathcal{A}$. Then $\mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$ is $\sim[\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}}]$. Suppose $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{C}$. By assumption, $\vdash_{AD} \mathcal{P} \leftrightarrow \mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$; so by (abv), $\vdash_{AD} (\mathcal{P} \to \mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}}) \wedge (\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{P})$; so by T3.20 with MP, $\vdash_{AD} \mathcal{P} \to \mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$; and by T3.13 with MP, $\vdash_{AD} \sim\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \sim\mathcal{P}$; similarly, by T3.19 with MP, $\vdash_{AD} \mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{P}$; so by T3.13 with MP, $\vdash_{AD} \sim\mathcal{P} \to \sim\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$; so by T9.4 with two applications of MP, $\vdash_{AD} (\sim\mathcal{P} \to \sim\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}}) \wedge (\sim\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \sim\mathcal{P})$; so by abv, $\vdash_{AD} \sim\mathcal{P} \leftrightarrow \sim\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$; which is just to say, $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$.

($\to$) Suppose $\mathcal{A}$ is $\mathcal{P} \to \mathcal{Q}$ and $\mathcal{B}$ is a proper subformula of $\mathcal{A}$. Then $\mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$ is $\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{Q}$ or $\mathcal{P} \to \mathcal{Q}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$. Suppose $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{C}$.

(i) Say $\mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$ is $\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{Q}$. By assumption, $\vdash_{AD} \mathcal{P} \leftrightarrow \mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$; so by (abv), $\vdash_{AD} (\mathcal{P} \to \mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}}) \wedge (\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{P})$; by T3.19 with MP, $\vdash_{AD} \mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{P}$; but by T3.5, $\vdash_{AD} (\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{P}) \to [(\mathcal{P} \to \mathcal{Q}) \to (\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{Q})]$; so by MP, $\vdash_{AD} (\mathcal{P} \to \mathcal{Q}) \to (\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{Q})$. Similarly, by T3.20 with MP, $\vdash_{AD} \mathcal{P} \to \mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$; and by T3.5, $\vdash_{AD} (\mathcal{P} \to \mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}}) \to [(\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{Q}) \to (\mathcal{P} \to \mathcal{Q})]$; so by MP, $\vdash_{AD} (\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{Q}) \to (\mathcal{P} \to \mathcal{Q})$. So by T9.4 with two applications of MP, $\vdash_{AD} [(\mathcal{P} \to \mathcal{Q}) \to (\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{Q})] \wedge [(\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{Q}) \to (\mathcal{P} \to \mathcal{Q})]$; so by abv, $\vdash_{ND} (\mathcal{P} \to \mathcal{Q}) \leftrightarrow (\mathcal{P}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{Q})$; which is just to say, $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$.

(ii) Say $\mathcal{A}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$ is $\mathcal{P} \to \mathcal{Q}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$. By assumption, $\vdash_{AD} \mathcal{Q} \leftrightarrow \mathcal{Q}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$; so by (abv), $\vdash_{AD} (\mathcal{Q} \to \mathcal{Q}^{\mathcal{B}}/\!\!/_{\mathcal{C}}) \wedge (\mathcal{Q}^{\mathcal{B}}/\!\!/_{\mathcal{C}} \to \mathcal{Q})$; so by T3.20 with MP, $\vdash_{AD} \mathcal{Q} \to \mathcal{Q}^{\mathcal{B}}/\!\!/_{\mathcal{C}}$; but by T3.4, $\vdash_{AD} (\mathcal{Q} \to \mathcal{Q}^{\mathcal{B}}/\!\!/_{\mathcal{C}}) \to [(\mathcal{P} \to \mathcal{Q}) \to$

$(\mathcal{P} \to \mathcal{Q}^{\mathcal{B}}/\!/_{\mathcal{C}})]$; so by MP, $\vdash_{AD} (\mathcal{P} \to \mathcal{Q}) \to (\mathcal{P} \to \mathcal{Q}^{\mathcal{B}}/\!/_{\mathcal{C}})$. Similarly, by T3.19 with MP, $\vdash_{AD} \mathcal{Q}^{\mathcal{B}}/\!/_{\mathcal{C}} \to \mathcal{Q}$; and by T3.4, $\vdash_{AD} (\mathcal{Q}^{\mathcal{B}}/\!/_{\mathcal{C}} \to \mathcal{Q}) \to [(\mathcal{P} \to \mathcal{Q}^{\mathcal{B}}/\!/_{\mathcal{C}}) \to (\mathcal{P} \to \mathcal{Q})]$; so by MP, $\vdash_{AD} (\mathcal{P} \to \mathcal{Q}^{\mathcal{B}}/\!/_{\mathcal{C}}) \to (\mathcal{P} \to \mathcal{Q})$. So by T9.4 with two applications of MP, $\vdash_{AD} [(\mathcal{P} \to \mathcal{Q}) \to (\mathcal{P} \to \mathcal{Q}^{\mathcal{B}}/\!/_{\mathcal{C}})] \wedge [(\mathcal{P} \to \mathcal{Q}^{\mathcal{B}}/\!/_{\mathcal{C}}) \to (\mathcal{P} \to \mathcal{Q})]$; so by abv, $\vdash_{AD} (\mathcal{P} \to \mathcal{Q}) \leftrightarrow (\mathcal{P} \to \mathcal{Q}^{\mathcal{B}}/\!/_{\mathcal{C}})$; and this is just to say, $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!/_{\mathcal{C}}$.

($\forall$) Suppose $\mathcal{A}$ is $\forall x\mathcal{P}$ and $\mathcal{B}$ is a proper subformula of $\mathcal{A}$. Then $\mathcal{A}^{\mathcal{B}}/\!/_{\mathcal{C}}$ is $\forall x[\mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}}]$. Suppose $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{C}$. Then by assumption $\vdash_{AD} \mathcal{P} \leftrightarrow \mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}}$; so by abv, $\vdash_{ND} (\mathcal{P} \to \mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}}) \wedge (\mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}} \to \mathcal{P})$; so by T3.20 with MP, $\vdash_{ND} \mathcal{P} \to \mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}}$. But since x is always free for itself in $\mathcal{P}$, by A4, $\vdash_{AD} \forall x\mathcal{P} \to \mathcal{P}$; so by T3.2, $\vdash_{AD} \forall x\mathcal{P} \to \mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}}$; and since x is not free in $\forall x\mathcal{P}$, by Gen, $\vdash_{AD} \forall x\mathcal{P} \to \forall x\mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}}$. Similarly, by T3.19 with MP, $\vdash_{AD} \mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}} \to \mathcal{P}$; but, since x is free for itself in $\mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}}$, by A4, $\vdash_{AD} \forall x\mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}} \to \mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}}$; so by T3.2, $\vdash_{AD} \forall x\mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}} \to \mathcal{P}$; and since x is not free in $\forall x\mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}}$, by Gen, $\vdash_{AD} \forall x\mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}} \to \forall x\mathcal{P}$. So by T9.4 with two applications of MP, $\vdash_{AD} [\forall x\mathcal{P} \to \forall x\mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}}] \wedge [\forall x\mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}} \to \forall x\mathcal{P}]$; so by abv, $\vdash_{AD} \forall x\mathcal{P} \leftrightarrow \forall x\mathcal{P}^{\mathcal{B}}/\!/_{\mathcal{C}}$; which is to say $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!/_{\mathcal{C}}$.

If $\mathcal{A}$ has k operator symbols, then if $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{C}$, then $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!/_{\mathcal{C}}$.

Indct: For any $\mathcal{A}$, if $\vdash_{AD} \mathcal{B} \leftrightarrow \mathcal{C}$, then $\vdash_{AD} \mathcal{A} \leftrightarrow \mathcal{A}^{\mathcal{B}}/\!/_{\mathcal{C}}$.

E9.12. Set up the above induction for T9.11 and complete the unfinished cases (including the case for $\exists$E) to show that if $\Gamma \vdash_{ND} \mathcal{P}$, then $\Gamma \vdash_{AD} \mathcal{P}$. For cases completed in the text, you may simply refer to the text, as the text refers cases to homework.

Suppose $\Gamma \vdash_{ND} \mathcal{P}$; then there is an *ND* derivation N of $\mathcal{P}$ from premises in Γ. We show that for any i, there is a good *AD* derivation A_i that matches N through line i.

Basis: The first line of N is a premise or an assumption. [From text] A_1 matches N and is good.

Assp: For any i, $0 \leq i < k$, there is a good derivation A_i that matches N through line i.

Show: There is a good derivation A_k that matches N through line k.

Either $\mathcal{Q}_k$ is a premise or assumption, or arises from previous lines by R, $\wedge$E, $\wedge$I, $\rightarrow$E, $\rightarrow$I, $\sim$E, $\sim$I, $\vee$E, $\vee$I, $\leftrightarrow$E, $\leftrightarrow$I, $\forall$E, $\forall$I, $\exists$E, $\exists$I, =E or =I.

(p/a) From text.

(R) From text.

($\wedge$E) From text.

($\wedge$I) From text.

($\rightarrow$E) From text.

($\rightarrow$I) From text.

($\sim$E) From text.

($\sim$I) If $\mathcal{Q}_k$ arises by $\sim$I, then N is something like this,

i	$\quad\mathcal{B}$	
j	$\quad\mathcal{C} \wedge \sim\mathcal{C}$	
k	$\sim\mathcal{B}$	i-j $\sim$I

where $i, j < k$, the subderivation is accessible at line k, and $\mathcal{Q}_k = \sim\mathcal{B}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\mathcal{B}$ and $\mathcal{C} \wedge \sim\mathcal{C}$ appear at the same scope on the lines numbered 'i' and 'j' of A_{k-1}; since they appear at the same scope, the parallel subderivation is accessible in A_{k-1}; since A_{k-1} is good, no application of Gen under the scope of $\mathcal{B}$ is to a variable free in $\mathcal{B}$. So let A_k continue as follows,

i	$\quad\mathcal{B}$	
j	$\quad\mathcal{C} \wedge \sim\mathcal{C}$	
$k.1$	$\mathcal{B} \rightarrow (\mathcal{C} \wedge \sim\mathcal{C})$	i-j DT
$k.2$	$(\mathcal{C} \wedge \sim\mathcal{C}) \rightarrow \mathcal{C}$	T3.20
$k.3$	$(\mathcal{C} \wedge \sim\mathcal{C}) \rightarrow \sim\mathcal{C}$	T3.19
$k.4$	$\mathcal{B} \rightarrow \mathcal{C}$	k.1,k.2 T3.2
$k.5$	$\mathcal{B} \rightarrow \sim\mathcal{C}$	k.1,k.3 T3.2
$k.6$	$\sim\sim\mathcal{B} \rightarrow \mathcal{B}$	T3.10
$k.7$	$\sim\sim\mathcal{B} \rightarrow \mathcal{C}$	k.6,k.4 T3.2
$k.8$	$\sim\sim\mathcal{B} \rightarrow \sim\mathcal{C}$	k.6,k.5 T3.2
$k.9$	$(\sim\sim\mathcal{B} \rightarrow \sim\mathcal{C}) \rightarrow ((\sim\sim\mathcal{B} \rightarrow \mathcal{C}) \rightarrow \sim\mathcal{B})$	A3
$k.10$	$(\sim\sim\mathcal{B} \rightarrow \mathcal{C}) \rightarrow \sim\mathcal{B}$	k.9,k.8 MP
k	$\sim\mathcal{B}$	k.10,k.7 MP

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good.

($\vee$E) From text.

($\vee$I) If $\mathcal{Q}_k$ arises by $\vee$I, then N is something like this,

$$\begin{array}{r|ll} i & \mathcal{B} & \\ & & \\ k & \mathcal{B} \vee \mathcal{C} & i\ \vee\text{I} \end{array} \qquad \text{or} \qquad \begin{array}{r|ll} i & \mathcal{B} & \\ & & \\ k & \mathcal{C} \vee \mathcal{B} & i\ \vee\text{I} \end{array}$$

where $i < k$ and $\mathcal{B}$ is accessible at line k. In the first case, $\mathcal{Q}_k = \mathcal{B} \vee \mathcal{C}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\mathcal{B}$ appears at the same scope on the line numbered 'i' of A_{k-1} and is accessible in A_{k-1}. So let A_k continue as follows,

$$\begin{array}{r|ll} i & \mathcal{B} & \\ & & \\ k.1 & \mathcal{B} \to (\mathcal{B} \vee \mathcal{C}) & \text{T3.17} \\ k & \mathcal{B} \vee \mathcal{C} & k.1,i\ \text{MP} \end{array}$$

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good. And similarly in the other case, by application of T3.18.

($\leftrightarrow$E) If $\mathcal{Q}_k$ arises by $\leftrightarrow$E, then N is something like this,

$$\begin{array}{r|ll} i & \mathcal{B} \leftrightarrow \mathcal{C} & \\ j & \mathcal{B} & \\ & & \\ k & \mathcal{C} & i,j\ \leftrightarrow\text{E} \end{array} \qquad \text{or} \qquad \begin{array}{r|ll} i & \mathcal{B} \leftrightarrow \mathcal{C} & \\ j & \mathcal{C} & \\ & & \\ k & \mathcal{B} & i,j\ \leftrightarrow\text{E} \end{array}$$

where $i, j < k$ and $\mathcal{B} \leftrightarrow \mathcal{C}$ and $\mathcal{B}$ or $\mathcal{C}$ are accessible at line k. In the first case, $\mathcal{Q}_k = \mathcal{C}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\mathcal{B} \leftrightarrow \mathcal{C}$ and $\mathcal{B}$ appear at the same scope on the lines numbered 'i' and 'j' of A_{k-1} and are accessible in A_{k-1}. So let A_k continue as follows,

$$\begin{array}{r|ll} i & \mathcal{B} \leftrightarrow \mathcal{C} & \\ j & \mathcal{B} & \\ & & \\ k.1 & (\mathcal{B} \to \mathcal{C}) \wedge (\mathcal{C} \to \mathcal{B}) & i\ \text{abv} \\ k.2 & [(\mathcal{B} \to \mathcal{C}) \wedge (\mathcal{C} \to \mathcal{B})] \to (\mathcal{B} \to \mathcal{C}) & \text{T3.20} \\ k.3 & \mathcal{B} \to \mathcal{C} & k.2,k.1\ \text{MP} \\ k & \mathcal{C} & k.3,j\ \text{MP} \end{array}$$

Exercise 9.12

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good. And similarly in the other case, by application of T3.19.

(↔I) If $\mathcal{Q}_k$ arises by ↔I, then N is something like this,

g	$\quad\vert\ \mathcal{B}$	
h	$\quad\vert\ \mathcal{C}$	
i	$\quad\vert\ \mathcal{C}$	
j	$\quad\vert\ \mathcal{B}$	
k	$\mathcal{B} \leftrightarrow \mathcal{C}$	g-h,i-j ↔I

where $g, h, i, j < k$, the two subderivations are accessible at line k and $\mathcal{Q}_k = \mathcal{B} \leftrightarrow \mathcal{C}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So the formulas at lines g, h, i, j appear at the same scope on corresponding lines in A_{k-1}; since they appear at the same scope, corresponding subderivations are accessible in A_{k-1}; since A_{k-1} is good, no application of Gen under the scope of $\mathcal{B}$ is to a variable free in $\mathcal{B}$ and no application of Gen under the scope of $\mathcal{C}$ is to a variable free in $\mathcal{C}$. So let A_k continue as follows,

g	$\quad\vert\ \mathcal{B}$	
h	$\quad\vert\ \mathcal{C}$	
i	$\quad\vert\ \mathcal{C}$	
j	$\quad\vert\ \mathcal{B}$	
$k.1$	$\mathcal{B} \rightarrow \mathcal{C}$	g-h DT
$k.2$	$\mathcal{C} \rightarrow \mathcal{B}$	i-j DT
$k.3$	$(\mathcal{B} \rightarrow \mathcal{C}) \rightarrow [(\mathcal{C} \rightarrow \mathcal{B}) \rightarrow ((\mathcal{B} \rightarrow \mathcal{C}) \wedge (\mathcal{C} \rightarrow \mathcal{B}))]$	T9.4
$k.4$	$(\mathcal{C} \rightarrow \mathcal{B}) \rightarrow ((\mathcal{B} \rightarrow \mathcal{C}) \wedge (\mathcal{C} \rightarrow \mathcal{B}))$	$k.3$,$k.1$ MP
$k.5$	$(\mathcal{B} \rightarrow \mathcal{C}) \wedge (\mathcal{C} \rightarrow \mathcal{B})$	$k.4$,$k.2$ MP
k	$\mathcal{B} \leftrightarrow \mathcal{C}$	$k.5$ abv

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good.

(∀E) If $\mathcal{Q}_k$ arises by ∀E, then N looks something like this,

i	$\forall x \mathcal{B}$	
k	$\mathcal{B}^x_t$	i ∀E

where $i < k$, $\forall x\mathcal{B}$ is accessible at line k, term t is free for variable x in $\mathcal{B}$, and $\mathcal{Q}_k = \mathcal{B}^x_t$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\forall x\mathcal{B}$ appears at the same scope on the line numbered 'i' of A_{k-1} and is accessible in A_{k-1}. So let A_k continue as follows,

$$\begin{array}{r|ll}
i & \forall x\mathcal{B} & \\
 & & \\
k.1 & \forall x\mathcal{B} \to \mathcal{B}^x_t & \text{A4} \\
k & \mathcal{B}^x_t & k.1,i\ \text{MP}
\end{array}$$

Since t is free for x in $\mathcal{B}$, $k.1$ is an instance of A4. So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good.

($\forall$I) From text.

($\exists$E) If $\mathcal{Q}_k$ arises by $\exists$E, then N looks something like this,

$$\begin{array}{r|l|ll}
h & \exists x\mathcal{B} & & \\
i & & \mathcal{B}^x_v & \\
 & & & \\
j & & \mathcal{C} & \\
k & \mathcal{C} & & h,i\text{-}j\ \exists\text{E}
\end{array}$$

where $h, i, j < k$, $\exists x\mathcal{B}$ and the subderivation are accessible at line k, and $\mathcal{C}$ is $\mathcal{Q}_k$; further, the *ND* restrictions on $\exists$E are met: (i) v is free for x in $\mathcal{B}$, (ii) v is not free in any undischarged auxiliary assumption, and (iii) v is not free in $\exists x\mathcal{B}$ or in $\mathcal{C}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So the formulas at lines h, i and j appear at the same scope on corresponding lines in A_{k-1}; since they appear at the same scope, $\exists x\mathcal{B}$ and the corresponding subderivation are accessible in A_{k-1}. Since A_{k-1} is good, no application of Gen under the scope of $\mathcal{B}^x_v$ is to a variable free in $\mathcal{B}^x_v$. So let A_k continue as follows,

h	$\exists x\mathcal{B}$	
i	$\quad\mathcal{B}^x_v$	
j	$\quad\mathcal{C}$	
$k.1$	$\mathcal{B}^x_v \to \mathcal{C}$	i-j DT
$k.2$	$\exists v\mathcal{B}^x_v \to \mathcal{C}$	$k.1$ T3.31
$k.3$	$\forall v{\sim}\mathcal{B}^x_v \to \forall x{\sim}\mathcal{B}$	T3.27
$k.4$	$(\forall v{\sim}\mathcal{B}^x_v \to \forall x{\sim}\mathcal{B}) \to ({\sim}\forall x{\sim}\mathcal{B} \to {\sim}\forall v{\sim}\mathcal{B}^x_v)$	T3.13
$k.5$	${\sim}\forall x{\sim}\mathcal{B} \to {\sim}\forall v{\sim}\mathcal{B}^x_v$	$k.4$,$k.3$ MP
$k.6$	$\exists x\mathcal{B} \to \exists v\mathcal{B}^x_v$	$k.5$ abv
$k.7$	$\exists v\mathcal{B}^x_v$	h,$k.6$ MP
k	$\mathcal{C}$	$k.2$,$k.7$ MP

Since from constraint (iii), v is not free in $\mathcal{C}$, $k.2$ meets the restriction on T3.31. If $v = x$ we can go directly from h and $k.2$ to k. So suppose $v \neq x$. To see that $k.3$ is an instance of T3.27, consider first, $\forall v{\sim}\mathcal{B}^x_v \to \forall x[{\sim}\mathcal{B}^x_v]^v_x$; this is an instance of T3.27 so long as x is not free in $\forall v{\sim}\mathcal{B}^x_v$ but free for v in ${\sim}\mathcal{B}^x_v$. First, since ${\sim}\mathcal{B}^x_v$ has all its free instances of x replaced by v, x is not free in $\forall v{\sim}\mathcal{B}^x_v$. Second, since $v \neq x$, with the constraint (iii), that v is not free in $\exists x\mathcal{B}$, v is not free in $\mathcal{B}$, and so ${\sim}\mathcal{B}$; but by (i), v is free for x in $\mathcal{B}$ and so ${\sim}\mathcal{B}$; so v appears free in ${\sim}\mathcal{B}^x_v$ just where x is free in ${\sim}\mathcal{B}$; so x is free for every free instance of v in ${\sim}\mathcal{B}^x_v$. So $\forall v{\sim}\mathcal{B}^x_v \to \forall x[{\sim}\mathcal{B}^x_v]^v_x$ is an instance of T3.27. But since v is not free in ${\sim}\mathcal{B}$, and free for x in ${\sim}\mathcal{B}$, by T8.2, $[{\sim}\mathcal{B}^x_v]^v_x = {\sim}\mathcal{B}$. So $k.3$ is a version of T3.27.

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. There is an application of Gen in T3.31 at $k.2$. But A_{k-1} is good and since A_k matches N and, by (ii), v is free in no undischarged auxiliary assumption of N, v is not free in any undischarged auxiliary assumption of A_k; so A_k is good.

($\exists$I) If $\mathcal{Q}_k$ arises by $\exists$I, then N looks something like this,

i	$\mathcal{B}^x_t$	
k	$\exists x\mathcal{B}$	i $\exists$I

where $i < k$, $\mathcal{B}^x_t$ is accessible at line k, term t is free for variable x in $\mathcal{B}$, and $\mathcal{Q}_k = \exists x\mathcal{B}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\mathcal{B}^x_t$ appears at the same scope on the line numbered 'i' of A_{k-1} and is accessible in A_{k-1}. So let A_k continue as follows,

$$\begin{array}{r|ll} i & \mathcal{B}^x_t & \\ & & \\ k.1 & \mathcal{B}^x_t \to \exists x\mathcal{B} & \text{T3.29} \\ k & \exists x\mathcal{B} & k.1,i \text{ MP} \end{array}$$

Since t is free for x in $\mathcal{B}$, $k.1$ is an instance of T3.29. So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good.

(=E) If $\mathcal{Q}_k$ arises by =E, then N is something like this,

$$\begin{array}{r|ll} i & \mathcal{B} & \\ j & t = s & \\ & & \\ k & \mathcal{B}^t/_s & i,j \text{ =E} \end{array} \quad \text{or} \quad \begin{array}{r|ll} i & \mathcal{B} & \\ j & s = t & \\ & & \\ k & \mathcal{B}^t/_s & i,j \text{ =E} \end{array}$$

where $i, j < k$, s is free for the replaced instances of t in $\mathcal{B}$, $\mathcal{B}$ and the equality are accessible at line k, and $\mathcal{Q}_k = \mathcal{B}^t/_s$. By assumption A_{k-1} matches N through line $k-1$ and is good. So in the first case, $\mathcal{B}$ and $t = s$ appear at the same scope on the lines numbered 'i' and 'j' of A_{k-1} and are accessible in A_{k-1}. So augment A_k as follows,

$$\begin{array}{r|ll} 0.k & (t = s) \to (\mathcal{B} \to \mathcal{B}^t/_s) & \text{T9.8} \\ & & \\ i & \mathcal{B} & \\ j & t = s & \\ & & \\ k.1 & \mathcal{B} \to \mathcal{B}^t/_s & 0.k,j \text{ MP} \\ k & \mathcal{B}^t/_s & k.1,i \text{ MP} \end{array}$$

Since s is free for the replaced instances of t in $\mathcal{B}$, $0.k$ is an instance of T9.8. So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. There may be applications of Gen in the derivation of T9.8; but that derivation is under the scope of no undischarged assumption. And under the scope of any undischarged assumptions, there is no new application of Gen; so A_k is good. And similarly in the other case, with an initial application of T3.33 and MP.

(=I) If $\mathcal{Q}_k$ arises by =I, then N looks something like this,

$$\begin{array}{r|ll} & & \\ k & t = t & \text{=I} \end{array}$$

where $\mathcal{Q}_k$ is $t = t$. By assumption A_{k-1} matches N through line $k-1$ and is good. So let A_k continue as follows,

k | $t = t$ T3.32

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good.

In any case, A_k matches N through line k and is good.

Indct: Derivation A matches N and is good.

E9.15. Set up the above induction and complete the unfinished cases to show that if $\Gamma \vdash_{ND+} \mathcal{P}$, then $\Gamma \vdash_{AD} \mathcal{P}$. For cases completed in the text, you may simply refer to the text, as the text refers cases to homework.

Suppose $\Gamma \vdash_{ND+} \mathcal{P}$; then there is an *ND*+ derivation N of $\mathcal{P}$ from premises in Γ. We show that for any i, there is a good *AD* derivation A_i that matches N through line i.

Basis: The first line of N is a premise or an assumption. Let A_1 be the same. Then A_1 matches N; and since there is no application of Gen, A_1 is good.

Assp: For any i, $0 \leq i < k$, there is a good derivation A_i that matches N through line i.

Show: There is a good derivation of A_k that matches N through line k.

Either $\mathcal{Q}_k$ is a premise or assumption, arises by a rule of *ND*, or by a the *ND*+ derivation rules, MT, HS, DS, NB or a replacement rule. If $\mathcal{Q}_k$ arises by any of the rules other than HS, DS or NB, then by reasoning from the text, there is a good derivation A_k that matches N through line k.

(HS) If $\mathcal{Q}_k$ arises from previous lines by HS then N is something like this,

i | $\mathcal{B} \rightarrow \mathcal{C}$
j | $\mathcal{C} \rightarrow \mathcal{D}$
k | $\mathcal{B} \rightarrow \mathcal{D}$ i,j HS

where $i, j < k$, $\mathcal{B} \rightarrow \mathcal{C}$ and $\mathcal{C} \rightarrow \mathcal{D}$ are accessible at line k, and $\mathcal{Q}_k = \mathcal{B} \rightarrow \mathcal{D}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\mathcal{B} \rightarrow \mathcal{D}$ and $\mathcal{C} \rightarrow \mathcal{D}$ appear at the same scope on the lines numbered 'i' and 'j' of A_{k-1} and are accessible in A_{k-1}. So let A_k continue as follows,

i	$\mathcal{B} \rightarrow \mathcal{C}$	
j	$\mathcal{C} \rightarrow \mathcal{D}$	
k	$\mathcal{B} \rightarrow \mathcal{D}$	i,j T3.2

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good.

(DS) If $\mathcal{Q}_k$ arises by DS, then N is something like this,

i	$\mathcal{B} \vee \mathcal{C}$			i	$\mathcal{B} \vee \mathcal{C}$	
j	$\sim\mathcal{C}$		or	j	$\sim\mathcal{B}$	
k	$\mathcal{B}$	i,j DS		k	$\mathcal{C}$	i,j DS

where $i, j < k$, and the formulas at lines i and j are accessible at line k. In the first case, $\mathcal{Q}_k = \mathcal{B}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\mathcal{B} \vee \mathcal{C}$ and $\sim\mathcal{C}$ appear at the same scope on the lines numbered 'i' and 'j' of A_{k-1} and are accessible in A_{k-1}. So let A_k continue as follows,

i	$\mathcal{B} \vee \mathcal{C}$	
j	$\sim\mathcal{C}$	
$k.1$	$\sim\mathcal{B} \rightarrow \mathcal{C}$	i abv
$k.2$	$(\sim\mathcal{B} \rightarrow \mathcal{C}) \rightarrow (\sim\mathcal{C} \rightarrow \mathcal{B})$	T3.14
$k.3$	$\sim\mathcal{C} \rightarrow \mathcal{B}$	$k.2,k.1$ MP
k	$\mathcal{B}$	$k.3,j$ MP

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good. And similarly in the other case, by application of MP immediately after $k.1$.

(NB) If $\mathcal{Q}_k$ arises by NB, then N is something like this,

i	$\mathcal{B} \leftrightarrow \mathcal{C}$			i	$\mathcal{B} \leftrightarrow \mathcal{C}$	
j	$\sim\mathcal{B}$		or	j	$\sim\mathcal{C}$	
k	$\sim\mathcal{C}$	i,j NB		k	$\sim\mathcal{B}$	i,j NB

where $i, j < k$, and the formulas at lines i and j are accessible at line k. In the first case, $\mathcal{Q}_k = \sim\mathcal{C}$. By assumption A_{k-1} matches N through line $k-1$ and is good. So $\mathcal{B} \leftrightarrow \mathcal{C}$ and $\sim\mathcal{B}$ appear at the same scope on the lines numbered 'i' and 'j' of A_{k-1} and are accessible in A_{k-1}. So let A_k continue as follows,

i	$\mathcal{B} \leftrightarrow \mathcal{C}$	
j	$\sim\mathcal{B}$	
$k.1$	$(\mathcal{B} \to \mathcal{C}) \wedge (\mathcal{C} \to \mathcal{B})$	i abv
$k.2$	$[(\mathcal{B} \to \mathcal{C}) \wedge (\mathcal{C} \to \mathcal{B})] \to (\mathcal{C} \to \mathcal{B})$	T3.19
$k.3$	$\mathcal{C} \to \mathcal{B}$	$k.2$,$k.1$ MP
$k.4$	$(\mathcal{C} \to \mathcal{B}) \to (\sim\mathcal{B} \to \sim\mathcal{C})$	T3.13
$k.5$	$\sim\mathcal{B} \to \sim\mathcal{C}$	$k.4$,$k.3$ MP
k	$\sim\mathcal{C}$	$k.5$,j MP

So $\mathcal{Q}_k$ appears at the same scope on the line numbered 'k' of A_k; so A_k matches N through line k. And since there is no new application of Gen, A_k is good. And similarly in the other case, with application of T3.20 in place of T3.19.

In any case, A_k matches N through line k and is good.

Indct: Derivation A matches N and is good.

Chapter Ten

E10.1. Complete the case for ($\to$) in to complete the demonstration of T10.2. You should set up the complete demonstration, but for cases completed in the text, you may simply refer to the text, as the text refers cases to homework.

For arbitrary formula $\mathcal{Q}$, term r and interpretation I, suppose r is free for x in $\mathcal{Q}$. By induction on the number of operator symbols in $\mathcal{Q}$,

Basis: Suppose $\mathsf{I_d}[r] = \mathsf{o}$. Then [from the text], $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$.

Assp: For any i, $0 \leq i < k$, if $\mathcal{Q}$ has i operator symbols, r is free for x in $\mathcal{Q}$ and $\mathsf{I_d}[r] = \mathsf{o}$, then $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$.

Show: If $\mathcal{Q}$ has k operator symbols, r is free for x in $\mathcal{Q}$ and $\mathsf{I_d}[r] = \mathsf{o}$, then $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$.

Suppose $\mathsf{I_d}[r] = \mathsf{o}$. If $\mathcal{Q}$ has k operator symbols, then $\mathcal{Q}$ is of the form $\sim\mathcal{B}$, $\mathcal{B} \to \mathcal{C}$, or $\forall v\mathcal{B}$ for variable v and formulas $\mathcal{B}$ and $\mathcal{C}$ with $< k$ operator symbols.

($\sim$) Suppose $\mathcal{Q}$ is $\sim\mathcal{B}$. Then [from the text], $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I_{d(x|o)}}[\mathcal{Q}] = \mathsf{S}$.

($\to$) Suppose $\mathcal{Q}$ is $\mathcal{B} \to \mathcal{C}$. Then $\mathcal{Q}^x_r = [\mathcal{B} \to \mathcal{C}]^x_r = [\mathcal{B}^x_r \to \mathcal{C}^x_r]$. Since r is free for x in $\mathcal{Q}$, r is free for x in $\mathcal{B}$ and $\mathcal{C}$; so by assumption,

$\mathsf{I_d}[\mathcal{B}^x_r] = \mathsf{S}$ iff $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{B}] = \mathsf{S}$ and $\mathsf{I_d}[\mathcal{C}^x_r] = \mathsf{S}$ iff $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{C}] = \mathsf{S}$. But by SF($\rightarrow$), $\mathsf{I_d}[\mathcal{B}^x_r \rightarrow \mathcal{C}^x_r] = \mathsf{S}$ iff $\mathsf{I_d}[\mathcal{B}^x_r] \neq \mathsf{S}$ or $\mathsf{I_d}[\mathcal{C}^x_r] = \mathsf{S}$; by assumption, iff $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{B}] \neq \mathsf{S}$ or $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{C}] = \mathsf{S}$; by SF($\rightarrow$), iff $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{B} \rightarrow \mathcal{C}] = \mathsf{S}$. So $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{Q}] = \mathsf{S}$.

($\forall$) Suppose $\mathcal{Q}$ is $\forall v \mathcal{B}$. From the text, by the assumption, for any $\mathsf{m} \in \mathsf{U}$, $\mathsf{I}_{\mathsf{d}(v|\mathsf{m})}[\mathcal{B}^x_r] = \mathsf{S}$ iff $\mathsf{I}_{\mathsf{d}(v|\mathsf{m},x|\mathsf{o})}[\mathcal{B}] = \mathsf{S}$. In addition, if $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{Q}] = \mathsf{S}$ then $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$. Now suppose $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ but $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{Q}] \neq \mathsf{S}$; then $\mathsf{I_d}[\forall v \mathcal{B}^x_r] = \mathsf{S}$ but $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\forall v \mathcal{B}] \neq \mathsf{S}$. From the latter, by SF($\forall$), there is some $\mathsf{m} \in \mathsf{U}$ such that $\mathsf{I}_{\mathsf{d}(v|\mathsf{m},x|\mathsf{o})}[\mathcal{B}] \neq \mathsf{S}$; so by the result from the assumption, $\mathsf{I}_{\mathsf{d}(v|\mathsf{m})}[\mathcal{B}^x_r] \neq \mathsf{S}$; so by SF($\forall$), $\mathsf{I_d}[\forall v \mathcal{B}^x_r] \neq \mathsf{S}$; this is impossible. So $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{Q}] = \mathsf{S}$.

If $\mathcal{Q}$ has k operator symbols, if r is free for x in $\mathcal{Q}$ and $\mathsf{I_d}[r] = \mathsf{o}$, then $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{Q}] = \mathsf{S}$.

Indct: For any $\mathcal{Q}$, if r is free for x in $\mathcal{Q}$ and $\mathsf{I_d}[r] = \mathsf{o}$, then $\mathsf{I_d}[\mathcal{Q}^x_r] = \mathsf{S}$ iff $\mathsf{I}_{\mathsf{d}(x|\mathsf{o})}[\mathcal{Q}] = \mathsf{S}$.

E10.2. Complete the case for (MP) to round out the demonstration that *AD* is sound. You should set up the complete demonstration, but for cases completed in the text, you may simply refer to the text, as the text refers cases to homework.

Suppose $\Gamma \vdash_{AD} \mathcal{P}$. Then there is an *AD* derivation $A = \langle \mathcal{Q}_1 \ldots \mathcal{Q}_n \rangle$ of $\mathcal{P}$ from premises in Γ, with $\mathcal{Q}_n = \mathcal{P}$. By induction on the line numbers in A, for any i, $\Gamma \vDash \mathcal{Q}_i$. The case when $i = n$ is the desired result.

Basis: The first line of A is a premise or an axiom. Then [from the text], $\Gamma \vDash \mathcal{Q}_1$.

Assp: For any i, $1 \leq i < k$, $\Gamma \vDash \mathcal{Q}_i$.

Show: $\Gamma \vDash \mathcal{Q}_k$.

$\mathcal{Q}_k$ is either a premise, an axiom, or arises from previous lines by MP or Gen. If $\mathcal{Q}_k$ is a premise or an axiom then, as in the basis, $\Gamma \vDash \mathcal{Q}_k$. So suppose $\mathcal{Q}_k$ arises by MP or Gen.

(MP) If $\mathcal{Q}_k$ arises by MP, then A is something like this,

i	$\mathcal{B} \rightarrow \mathcal{C}$	
j	$\mathcal{B}$	
	$\vdots$	
k	$\mathcal{C}$	i,j MP

where $i, j < k$ and $\mathcal{Q}_k = \mathcal{C}$. Suppose $\Gamma \not\models \mathcal{Q}_k$; then $\Gamma \not\models \mathcal{C}$; so by QV, there is some I such that $I[\Gamma] = T$ but $I[\mathcal{C}] \neq T$; from the latter, by TI, there is some d such that $I_d[\mathcal{C}] \neq S$. But $I[\Gamma] = T$ and by assumption, $\Gamma \models \mathcal{B} \to \mathcal{C}$ and $\Gamma \models \mathcal{B}$; so by QV, $I[\mathcal{B} \to \mathcal{C}] = T$ and $I[\mathcal{B}] = T$; so by TI, $I_d[\mathcal{B} \to \mathcal{C}] = S$ and $I_d[\mathcal{B}] = S$; from the first of these, by SF($\to$), $I_d[\mathcal{B}] \neq S$ or $I_d[\mathcal{C}] = S$; so $I_d[\mathcal{C}] = S$. This is impossible; reject the assumption: $\Gamma \models \mathcal{Q}_k$.

(Gen) If $\mathcal{Q}_k$ arises by Gen, then [from the text], $\Gamma \models \mathcal{Q}_k$.

$\Gamma \models \mathcal{Q}_k$.

Indct: For any n, $\Gamma \models \mathcal{Q}_n$.

E10.4. Provide an argument to show T10.5.

If there is an interpretation M such that $M[\Gamma \cup \{\sim\mathcal{A}\}] = T$, then $\Gamma \nvdash \mathcal{A}$.

Suppose there is an interpretation M such that $M[\Gamma \cup \{\sim\mathcal{A}\}] = T$ but $\Gamma \vdash \mathcal{A}$. From the former, $M[\Gamma] = T$ and $M[\sim\mathcal{A}] = T$. From the latter, by soundness, $\Gamma \models \mathcal{A}$; but $M[\Gamma] = T$; so by QV, $M[\mathcal{A}] = T$; so by TI, for any d, $M_d[\mathcal{A}] = S$ and since $M[\sim\mathcal{A}] = T$, $M_d[\sim\mathcal{A}] = S$; so by SF($\sim$), $M_d[\mathcal{A}] \neq S$. This is impossible; reject the assumption: if there is an interpretation M such that $M[\Gamma \cup \{\sim\mathcal{A}\}] = T$, then $\Gamma \nvdash \mathcal{A}$.

E10.10. Complete the second half of the conditional case to complete the proof of T10.9_s. You should set up the entire induction, but may refer to the text for parts completed there, as the text refers to homework.

Suppose Σ' is consistent. Then by T10.8_s, Σ'' is maximal and consistent. Now by induction on the number of operators in $\mathcal{B}$,

Basis: If $\mathcal{B}$ has no operators, then it is an atomic of the sort $\mathcal{S}$. But by the construction of M′, $M'[\mathcal{S}] = T$ iff $\Sigma'' \vdash \mathcal{S}$; so $M'[\mathcal{B}] = T$ iff $\Sigma'' \vdash \mathcal{B}$.

Assp: For any i, $0 \leq i < k$, if $\mathcal{B}$ has i operator symbols, then $M'[\mathcal{B}] = T$ iff $\Sigma'' \vdash \mathcal{B}$.

Show: If $\mathcal{B}$ has k operator symbols, then $M'[\mathcal{B}] = T$ iff $\Sigma'' \vdash \mathcal{B}$.

If $\mathcal{B}$ has k operator symbols, then it is of the form $\sim\mathcal{P}$ or $\mathcal{P} \to \mathcal{Q}$ where $\mathcal{P}$ and $\mathcal{Q}$ have $< k$ operator symbols.

($\sim$) Suppose $\mathcal{B}$ is $\sim\mathcal{P}$. [From the text], $M'[\mathcal{B}] = T$ iff $\Sigma'' \vdash \mathcal{B}$.

($\to$) Suppose $\mathcal{B}$ is $\mathcal{P} \to \mathcal{Q}$. (i) Suppose $M'[\mathcal{B}] = T$; then [from the text], $\Sigma'' \vdash \mathcal{B}$. (ii) Suppose $\Sigma'' \vdash \mathcal{B}$ but $M'[\mathcal{B}] \neq T$; then $\Sigma'' \vdash \mathcal{P} \to \mathcal{Q}$ but

$\mathsf{M}'[\mathcal{P} \to \mathcal{Q}] \neq \mathsf{T}$; from the latter, by ST($\to$), $\mathsf{M}'[\mathcal{P}] = \mathsf{T}$ and $\mathsf{M}'[\mathcal{Q}] \neq \mathsf{T}$; so by assumption, $\Sigma'' \vdash \mathcal{P}$ and $\Sigma'' \nvdash \mathcal{Q}$; from the second of these, by maximality, $\Sigma'' \vdash \sim\mathcal{Q}$. But since $\Sigma'' \vdash \mathcal{P}$ and $\Sigma'' \vdash \mathcal{P} \to \mathcal{Q}$, by MP, $\Sigma'' \vdash \mathcal{Q}$; so by consistency, $\Sigma'' \nvdash \sim\mathcal{Q}$. This is impossible; reject the assumption: If $\Sigma'' \vdash \mathcal{B}$, then $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$. So $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

If $\mathcal{B}$ has k operator symbols, then $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

Indct: For any $\mathcal{B}$, $\mathsf{M}'[\mathcal{B}] = \mathsf{T}$ iff $\Sigma'' \vdash \mathcal{B}$.

E10.13. Finish the cases for A2, A3 and MP to complete the proof of T10.12. You should set up the complete demonstration, but may refer to the text for cases completed there, as the text refers cases to homework.

Basis: $\mathcal{B}_1$ is either a member of Σ' or an axiom.

(prem) If $\mathcal{B}_1$ is a member of Σ', then [from text], $\langle \mathcal{B}_1{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

(eq) If $\mathcal{B}_1$ is an equality axiom, A6, A7 or A8, then [from text], $\langle \mathcal{B}_1{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

(A1) If $\mathcal{B}_1$ is an instance of A1, then [from text], $\langle \mathcal{B}_1{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

(A2) If $\mathcal{B}_1$ is an instance of A2, then it is of the form, $[\mathcal{O} \to (\mathcal{P} \to \mathcal{Q})] \to [(\mathcal{O} \to \mathcal{P}) \to (\mathcal{O} \to \mathcal{Q})]$; so $\mathcal{B}_1{}^{a}_{x}$ is $[\mathcal{O}^{a}_{x} \to (\mathcal{P}^{a}_{x} \to \mathcal{Q}^{a}_{x})] \to [(\mathcal{O}^{a}_{x} \to \mathcal{P}^{a}_{x}) \to (\mathcal{O}^{a}_{x} \to \mathcal{Q}^{a}_{x})]$; but this is an instance of A2; so if $\mathcal{B}_1$ is an instance of A2, then $\mathcal{B}_1{}^{a}_{x}$ is an instance of A2, and $\langle \mathcal{B}_1{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

(A3) If $\mathcal{B}_1$ is an instance of A3, then it is of the form, $(\sim\mathcal{Q} \to \sim\mathcal{P}) \to [(\sim\mathcal{Q} \to \mathcal{P}) \to \mathcal{Q}]$; so $\mathcal{B}_1{}^{a}_{x}$ is $(\sim\mathcal{Q}^{a}_{x} \to \sim\mathcal{P}^{a}_{x}) \to [(\sim\mathcal{Q}^{a}_{x} \to \mathcal{P}^{a}_{x}) \to \mathcal{Q}^{a}_{x}]$; but this is an instance of A3; so if $\mathcal{B}_1$ is an instance of A3, then $\mathcal{B}_1{}^{a}_{x}$ is an instance of A3, and $\langle \mathcal{B}_1{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

(A4) If $\mathcal{B}_1$ is an instance of A4, then [from text], $\langle \mathcal{B}_1{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

Assp: For any i, $1 \leq i < k$, $\langle \mathcal{B}_1{}^{a}_{x} \dots \mathcal{B}_i{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

Show: $\langle \mathcal{B}_1{}^{a}_{x} \dots \mathcal{B}_k{}^{a}_{x} \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$.

$\mathcal{B}_k$ is a member of Σ', an axiom, or arises from previous lines by MP or Gen. If $\mathcal{B}_k$ is a member of Σ' or an axiom then, by reasoning as in the basis, $\langle \mathcal{B}_1 \dots \mathcal{B}_k \rangle$ is a derivation from $\Sigma'{}^{a}_{x}$. So two cases remain.

(MP) If $\mathscr{B}_k$ arises by MP, then there are some lines in D,

$$\begin{array}{lll} i & \mathscr{P} \rightarrow \mathscr{Q} & \\ j & \mathscr{P} & \\ & \vdots & \\ k & \mathscr{Q} & i,j \text{ MP} \end{array}$$

where $i, j < k$ and $\mathscr{B}_k = \mathscr{Q}$. By assumption $(\mathscr{P} \rightarrow \mathscr{Q})^a_x$ and $\mathscr{P}^a_x$ are members of the derivation $\langle \mathscr{B}_1{}^a_x \ldots \mathscr{B}_{k-1}{}^a_x \rangle$ from $\Sigma'{}^a_x$; but $(\mathscr{P} \rightarrow \mathscr{Q})^a_x$ is $\mathscr{P}^a_x \rightarrow \mathscr{Q}^a_x$; so by MP, $\mathscr{Q}^a_x$ follows in this new derivation. So $\langle \mathscr{B}_1{}^a_x \ldots \mathscr{B}_k{}^a_x \rangle$ is a derivation from $\Sigma'{}^a_x$.

(Gen) If $\mathscr{B}_k$ arises by Gen, then [from text], $\langle \mathscr{B}_1{}^a_x \ldots \mathscr{B}_k{}^a_x \rangle$ is a derivation from $\Sigma'{}^a_x$.

So $\langle \mathscr{B}_1{}^a_x \ldots \mathscr{B}_k{}^a_x \rangle$ is a derivation from $\Sigma'{}^a_x$.

Indct: For any n, $\langle \mathscr{B}_1{}^a_x \ldots \mathscr{B}_n{}^a_x \rangle$ is a derivation from $\Sigma'{}^a_x$.

E10.21. Complete the proof of T10.14. You should set up the complete induction, but may refer to the text, as the text refers to homework.

The argument is by induction on the number of function symbols in t. Let d be a variable assignment, and t a term in $\mathscr{L}$.

Basis: If t has no function symbols, then it is a variable or a constant in $\mathscr{L}$. If t is a constant, then by construction, $\mathsf{M}[t] = \mathsf{M}'[t]$; so by TA(c), $\mathsf{M_d}[t] = \mathsf{M'_d}[t]$. If t is a variable, by TA(v), $\mathsf{M_d}[t] = \mathsf{d}[t] = \mathsf{M'_d}[t]$. In either case, then, $\mathsf{M_d}[t] = \mathsf{M'_d}[t]$.

Assp: For any i, $0 \leq i < k$, if t has i function symbols, then $\mathsf{M_d}[t] = \mathsf{M'_d}[t]$.

Show: If t has k function symbols, then $\mathsf{M_d}[t] = \mathsf{M'_d}[t]$.

If t has k function symbols, then [from text] $\mathsf{M_d}[t] = \mathsf{M'_d}[t]$.

Indct: For any t in $\mathscr{L}$, $\mathsf{M_d}[t] = \mathsf{M'_d}[t]$.

E10.22. Complete the proof of T10.15. As usual, you should set up the complete induction, but may refer to the text for cases completed there, as the text refers to homework.

The argument is by induction on the number of operator symbols in $\mathscr{P}$. Let d be a variable assignment, and $\mathscr{P}$ a formula in $\mathscr{L}$.

Basis: If $\mathscr{P}$ has no operator symbols, then [from text] $\mathsf{M_d}[\mathscr{P}] = \mathsf{S}$ iff $\mathsf{M'_d}[\mathscr{P}] = \mathsf{S}$.

Assp: For any i, $0 \leq i < k$, and any common variable assignment d, if $\mathcal{P}$ has i operator symbols, $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M'_d}[\mathcal{P}] = \mathsf{S}$.

Show: For any variable assignment d for M, if $\mathcal{P}$ has k operator symbols, $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M'_d}[\mathcal{P}] = \mathsf{S}$.

If $\mathcal{P}$ has k operator symbols, then it is of the form $\sim\mathcal{A}$, $\mathcal{A} \to \mathcal{B}$ or $\forall x\mathcal{A}$ for variable x and formulas $\mathcal{A}$ and $\mathcal{B}$ with $< k$ operator symbols.

($\sim$) Suppose $\mathcal{P}$ is of the form $\sim\mathcal{A}$. Then $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M_d}[\sim\mathcal{A}] = \mathsf{S}$; by SF($\sim$), iff $\mathsf{M_d}[\mathcal{A}] \neq \mathsf{S}$; by assumption, iff $\mathsf{M'_d}[\mathcal{A}] \neq \mathsf{S}$; by SF($\sim$), iff $\mathsf{M'_d}[\sim\mathcal{A}] = \mathsf{S}$; iff $\mathsf{M'_d}[\mathcal{P}] = \mathsf{S}$.

($\to$) Suppose $\mathcal{P}$ is of the form $\mathcal{A} \to \mathcal{B}$. Then $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M_d}[\mathcal{A} \to \mathcal{B}] = \mathsf{S}$; by SF($\to$), iff $\mathsf{M_d}[\mathcal{A}] \neq \mathsf{S}$ or $\mathsf{M_d}[\mathcal{B}] = \mathsf{S}$; by assumption, iff $\mathsf{M'_d}[\mathcal{A}] \neq \mathsf{S}$ or $\mathsf{M'_d}[\mathcal{B}] = \mathsf{S}$; by SF($\to$), iff $\mathsf{M'_d}[\mathcal{A} \to \mathcal{B}] = \mathsf{S}$; iff $\mathsf{M'_d}[\mathcal{P}] = \mathsf{S}$.

($\forall$) Suppose $\mathcal{P}$ is of the form $\forall x\mathcal{A}$. Then $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M_d}[\forall x\mathcal{A}] = \mathsf{S}$; by SF($\forall$), iff for any $\mathsf{m} \in \mathsf{U}$, $\mathsf{M_{d(x|m)}}[\mathcal{A}] = \mathsf{S}$; by assumption, iff for any $\mathsf{m} \in \mathsf{U}$, $\mathsf{M'_{d(x|m)}}[\mathcal{A}] = \mathsf{S}$; by SF($\forall$), iff $\mathsf{M'_d}[\forall x\mathcal{A}] = \mathsf{S}$; iff $\mathsf{M'_d}[\mathcal{P}] = \mathsf{S}$.

If $\mathcal{P}$ has k operator symbols, $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M'_d}[\mathcal{P}] = \mathsf{S}$.

Indct: For any formula $\mathcal{P}$ in $\mathcal{L}$, $\mathsf{M_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{M'_d}[\mathcal{P}] = \mathsf{S}$.

Chapter Eleven

E11.9. Complete the proof of T11.9. You should set up the complete induction, but may refer to the text, as the text refers to homework.

By induction on the number of operators in $\mathcal{P}$. Suppose $\mathsf{D} \cong \mathsf{H}$.

Basis: Suppose $\mathcal{P}$ has no operator symbols and d and h are such that for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$. If $\mathcal{P}$ has no operator symbols, then [from text] $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

Assp: For any i, $0 \leq i < k$, for d and h such that for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$ and $\mathcal{P}$ with i operator symbols, $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

Show: For d and h such that for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$ and $\mathcal{P}$ with k operator symbols, $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

If $\mathcal{P}$ has k operator symbols, then it is of the form $\sim\mathcal{A}$, $\mathcal{A} \to \mathcal{B}$, or $\forall x\mathcal{A}$ for variable x and formulas $\mathcal{A}$ and $\mathcal{B}$ with $< k$ operator symbols. Suppose for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$.

($\sim$) Suppose $\mathcal{P}$ is of the form $\sim\mathcal{A}$. Then [from text] $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

$\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{D_d}[\sim\mathcal{A}] = \mathsf{S}$; by SF($\sim$), iff $\mathsf{D_d}[\mathcal{A}] \neq \mathsf{S}$; by assumption, iff $\mathsf{H_h}[\mathcal{A}] \neq \mathsf{S}$; by SF($\sim$), iff $\mathsf{H_h}[\sim\mathcal{A}] = \mathsf{S}$; iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

($\rightarrow$) $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{D_d}[\mathcal{A} \rightarrow \mathcal{B}] = \mathsf{S}$; by SF($\rightarrow$), iff $\mathsf{D_d}[\mathcal{A}] \neq \mathsf{S}$ or $\mathsf{D_d}[\mathcal{B}] = \mathsf{S}$; by assumption, iff $\mathsf{H_h}[\mathcal{A}] \neq \mathsf{S}$ or $\mathsf{H_h}[\mathcal{B}] = \mathsf{S}$; by SF($\rightarrow$), iff $\mathsf{H_h}[\mathcal{A} \rightarrow \mathcal{B}] = \mathsf{S}$; iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

($\forall$) Suppose $\mathcal{P}$ is of the form $\forall x\mathcal{A}$. Then $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{D_d}[\forall x\mathcal{A}] = \mathsf{S}$; by SF($\forall$), iff for any $\mathsf{m} \in \mathsf{U_D}$, $\mathsf{D_{d(x|m)}}[\mathcal{A}] = \mathsf{S}$. Similarly, $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{H_h}[\forall x\mathcal{A}] = \mathsf{S}$; by SF($\forall$), iff for any $\mathsf{n} \in \mathsf{U_H}$, $\mathsf{H_{h(x|n)}}[\mathcal{A}] = \mathsf{S}$. (i) [From the text], if $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$, then $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$. (ii) Suppose $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ but $\mathsf{H_h}[\mathcal{P}] \neq \mathsf{S}$; then any $\mathsf{m} \in \mathsf{U_D}$ is such that $\mathsf{D_{d(x|m)}}[\mathcal{A}] = \mathsf{S}$, but there is some $\mathsf{n} \in \mathsf{U_H}$ such that $\mathsf{H_{h(x|n)}}[\mathcal{A}] \neq \mathsf{S}$. Since ι is onto $\mathsf{U_H}$, there is some $\mathsf{o} \in \mathsf{U_D}$ such that $\iota(\mathsf{o}) = \mathsf{n}$; so insofar as $\mathsf{d}(x|\mathsf{o})$ and $\mathsf{h}(x|\mathsf{n})$ have each member related by ι, the assumption applies and $\mathsf{D_{d(x|o)}}[\mathcal{A}] \neq \mathsf{S}$; so there is some $\mathsf{m} \in \mathsf{U_D}$ such that $\mathsf{D_{d(x|m)}}[\mathcal{A}] \neq \mathsf{S}$; this is impossible; reject the assumption: if $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$, then $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

For d and h such that for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$ and $\mathcal{P}$ with k operator symbols, $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

Indct: For d and h such that for any x, $\iota(\mathsf{d}[x]) = \mathsf{h}[x]$, and any $\mathcal{P}$, $\mathsf{D_d}[\mathcal{P}] = \mathsf{S}$ iff $\mathsf{H_h}[\mathcal{P}] = \mathsf{S}$.

Chapter Twelve

E12.1. (b) produce functions $\mathsf{gpower(x)}$, and $\mathsf{hpower(x, y, u)}$ and show that they have the same result as conditions (g) and (h).

Set $\mathsf{gpower(x)} = \mathsf{suc(zero(x))}$ and $\mathsf{hpower(x, y, u)} = \mathsf{times(idnt^3_3(x, y, u), x)}$. Then,

$\mathsf{g'}$ $\mathsf{power(x, 0) = S(zero(x)) = S0}$
$\mathsf{h'}$ $\mathsf{power(x, Sy) = idnt^3_3(x, y, power(x, y)) \times x = power(x, y) \times x}$

E12.5. (a) By the method of our core induction, write down formulas to express the following recursive function: $\mathsf{suc(zero(x))}$.

$\mathcal{Z}(x, w)$ is $x = x \wedge w = \emptyset$ and $\mathcal{S}(w, y)$ is $Sw = y$; so their composition $\mathcal{F}(x, y) = \exists w[(x = x \wedge w = \emptyset) \wedge Sw = y]$.

E12.6. Fill out semantic reasoning to demonstrate that proposed (original) formulas satisfy the conditions for expression for the (z), (i), (c) and (m) clauses to T12.3.

(c) $\mathsf{f_k(y)}$ arises by composition from $\mathsf{g(y)}$ and $\mathsf{h(w)}$. By assumption $\mathsf{g(y)}$ is expressed by some $\mathscr{G}(y,w)$ and $\mathsf{h(w)}$ by $\mathscr{H}(w,v)$. And the composition $\mathsf{f(y)}$ is expressed by $\mathscr{F}(y,v) =_{\text{def}} \exists w[\mathscr{G}(y,w) \wedge \mathscr{H}(w,v)]$. Suppose $\langle\mathsf{m,a}\rangle \in \mathsf{f_k}$; then by composition there is some b such that $\langle\mathsf{m,b}\rangle \in \mathsf{g}$ and $\langle\mathsf{b,a}\rangle \in \mathsf{h}$.

(i) Because $\mathscr{G}$ and $\mathscr{H}$ express g and h, $\mathsf{N}[\mathscr{G}(\overline{\mathsf{m}},\overline{\mathsf{b}})] = \mathsf{T}$ and $\mathsf{N}[\mathscr{H}(\overline{\mathsf{b}},\overline{\mathsf{a}})] = \mathsf{T}$. Suppose $\mathsf{N}[\exists w(\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,\overline{\mathsf{a}}))] \neq \mathsf{T}$; then by TI, there is some d such that $\mathsf{N_d}[\exists w(\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,\overline{\mathsf{a}}))] \neq \mathsf{S}$; let h be a particular assignment of this sort; then $\mathsf{N_h}[\exists w(\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,\overline{\mathsf{a}}))] \neq \mathsf{S}$; so by SF($\exists$), for any $\mathsf{o} \in \mathsf{U}$, $\mathsf{N_{h(\mathit{w}|o)}}[\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,\overline{\mathsf{a}})] \neq \mathsf{S}$; so $\mathsf{N_{h(\mathit{w}|b)}}[\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,\overline{\mathsf{a}})] \neq \mathsf{S}$; so since $\mathsf{N_h}[\overline{\mathsf{b}}] = \mathsf{b}$, with T10.2, $\mathsf{N_h}[\mathscr{G}(\overline{\mathsf{m}},\overline{\mathsf{b}}) \wedge \mathscr{H}(\overline{\mathsf{b}},\overline{\mathsf{a}})] \neq \mathsf{S}$; so by SF($\wedge$), $\mathsf{N_h}[\mathscr{G}(\overline{\mathsf{m}},\overline{\mathsf{b}})] \neq \mathsf{S}$ or $\mathsf{N_h}[\mathscr{H}(\overline{\mathsf{b}},\overline{\mathsf{a}})] \neq \mathsf{S}$. But $\mathsf{N}[\mathscr{G}(\overline{\mathsf{m}},\overline{\mathsf{b}})] = \mathsf{T}$; so by TI, for any d, $\mathsf{N_d}[\mathscr{G}(\overline{\mathsf{m}},\overline{\mathsf{b}})] = \mathsf{S}$; so $\mathsf{N_h}[\mathscr{G}(\overline{\mathsf{m}},\overline{\mathsf{b}})] = \mathsf{S}$; so $\mathsf{N_h}[\mathscr{H}(\overline{\mathsf{b}},\overline{\mathsf{a}})] \neq \mathsf{S}$; but $\mathsf{N}[\mathscr{H}(\overline{\mathsf{b}},\overline{\mathsf{a}})] = \mathsf{T}$; so by TI, for any d, $\mathsf{N_d}[\mathscr{H}(\overline{\mathsf{b}},\overline{\mathsf{a}})] = \mathsf{S}$; so $\mathsf{N_h}[\mathscr{H}(\overline{\mathsf{b}},\overline{\mathsf{a}})] = \mathsf{S}$. This is impossible; reject the assumption: $\mathsf{N}[\exists w(\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,\overline{\mathsf{a}}))] = \mathsf{T}$.

(ii) Suppose $\mathsf{N}[\forall z(\exists w(\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,z)) \rightarrow z = \overline{\mathsf{a}})] \neq \mathsf{T}$; then by TI, there is some d such that $\mathsf{N_d}[\forall z(\exists w(\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,z)) \rightarrow z = \overline{\mathsf{a}})] \neq \mathsf{S}$; let h be a particular assignment of this sort; then $\mathsf{N_h}[\forall z(\exists w(\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,z)) \rightarrow z = \overline{\mathsf{a}})] \neq \mathsf{S}$; so by SF($\forall$), for some $\mathsf{o} \in \mathsf{U}$, $\mathsf{N_{h(\mathit{z}|o)}}[\exists w(\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,z)) \rightarrow z = \overline{\mathsf{a}}] \neq \mathsf{S}$; let p be a particular individual of this sort; then $\mathsf{N_{h(\mathit{z}|p)}}[\exists w(\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,z)) \rightarrow z = \overline{\mathsf{a}}] \neq \mathsf{S}$; since $\mathsf{N_h}[\overline{\mathsf{p}}] = \mathsf{p}$, with T10.2, $\mathsf{N_h}[\exists w(\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,\overline{\mathsf{p}})) \rightarrow \overline{\mathsf{p}} = \overline{\mathsf{a}}] \neq \mathsf{S}$; so by SF($\rightarrow$), $\mathsf{N_h}[\exists w(\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,\overline{\mathsf{p}}))] = \mathsf{S}$ and $\mathsf{N_h}[\overline{\mathsf{p}} = \overline{\mathsf{a}}] \neq \mathsf{S}$. From the first of these, by SF($\exists$), there is some $\mathsf{o} \in \mathsf{U}$ such that $\mathsf{N_{h(\mathit{w}|o)}}[\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,\overline{\mathsf{p}})] = \mathsf{S}$; let q be a particular individual of this sort; then $\mathsf{N_{h(\mathit{w}|q)}}[\mathscr{G}(\overline{\mathsf{m}},w) \wedge \mathscr{H}(w,\overline{\mathsf{p}})] = \mathsf{S}$; since $\mathsf{N_h}[\overline{\mathsf{q}}] = \mathsf{q}$, with T10.2, $\mathsf{N_h}[\mathscr{G}(\overline{\mathsf{m}},\overline{\mathsf{q}}) \wedge \mathscr{H}(\overline{\mathsf{q}},\overline{\mathsf{p}})] = \mathsf{S}$; so by SF($\wedge$), $\mathsf{N_h}[\mathscr{G}(\overline{\mathsf{m}},\overline{\mathsf{q}})] = \mathsf{S}$; and $\mathsf{N_h}[\mathscr{H}(\overline{\mathsf{q}},\overline{\mathsf{p}})] = \mathsf{S}$.

Because $\mathscr{G}$ expresses g and $\langle\mathsf{m,b}\rangle \in \mathsf{g}$, $\mathsf{N}[\forall z(\mathscr{G}(\overline{\mathsf{m}},z) \rightarrow z = \overline{\mathsf{b}})] = \mathsf{T}$; so by TI, for any d, $\mathsf{N_d}[\forall z(\mathscr{G}(\overline{\mathsf{m}},z) \rightarrow z = \overline{\mathsf{b}})] = \mathsf{S}$; so $\mathsf{N_h}[\forall z(\mathscr{G}(\overline{\mathsf{m}},z) \rightarrow z = \overline{\mathsf{b}})] = \mathsf{S}$; so by SF($\forall$), for any $\mathsf{o} \in \mathsf{U}$, $\mathsf{N_{h(\mathit{z}|o)}}[\mathscr{G}(\overline{\mathsf{m}},z) \rightarrow z = \overline{\mathsf{b}}] = \mathsf{S}$; so $\mathsf{N_{h(\mathit{z}|q)}}[\mathscr{G}(\overline{\mathsf{m}},z) \rightarrow z = \overline{\mathsf{b}}] = \mathsf{S}$; since $\mathsf{N_h}[\overline{\mathsf{q}}] = \mathsf{q}$, with T10.2, $\mathsf{N_h}[\mathscr{G}(\overline{\mathsf{m}},\overline{\mathsf{q}}) \rightarrow \overline{\mathsf{q}} = \overline{\mathsf{b}}] = \mathsf{S}$; so by SF($\rightarrow$), $\mathsf{N_h}[\mathscr{G}(\overline{\mathsf{m}},\overline{\mathsf{q}})] \neq \mathsf{S}$ or $\mathsf{N_h}[\overline{\mathsf{q}} = \overline{\mathsf{b}}] = \mathsf{S}$; but $\mathsf{N_h}[\mathscr{G}(\overline{\mathsf{m}},\overline{\mathsf{q}})] = \mathsf{S}$; so $\mathsf{N_h}[\overline{\mathsf{q}} = \overline{\mathsf{b}}] = \mathsf{S}$; and since $\mathsf{N_h}[\overline{\mathsf{q}}] = \mathsf{q}$ and $\mathsf{N_h}[\overline{\mathsf{b}}] = \mathsf{b}$, with SF(r), $\mathsf{q} = \mathsf{b}$.

Since $\mathscr{H}$ expresses h, and $\langle\mathsf{b,a}\rangle \in \mathsf{h}$, $\langle\mathsf{q,a}\rangle \in \mathsf{h}$ and $\mathsf{N}[\forall z(\mathscr{H}(\overline{\mathsf{q}},z) \rightarrow z =$

$\overline{\mathsf{a}})] = \mathsf{T}$; so by TI, for any d, $\mathsf{N_d}[\forall z(\mathscr{H}(\overline{\mathsf{q}}, z) \rightarrow z = \overline{\mathsf{a}})] = \mathsf{S}$; so $\mathsf{N_h}[\forall z(\mathscr{H}(\overline{\mathsf{q}}, z) \rightarrow z = \overline{\mathsf{a}})] = \mathsf{S}$; so by SF($\forall$), for any $\mathsf{o} \in \mathsf{U}$, $\mathsf{N_{h(z|o)}}[\mathscr{H}(\overline{\mathsf{q}}, z) \rightarrow z = \overline{\mathsf{a}}] = \mathsf{S}$; so $\mathsf{N_{h(z|p)}}[\mathscr{H}(\overline{\mathsf{q}}, z) \rightarrow z = \overline{\mathsf{a}}] = \mathsf{S}$; since $\mathsf{N_h}[\overline{\mathsf{p}}] = \mathsf{p}$, with T10.2, $\mathsf{N_h}[\mathscr{H}(\overline{\mathsf{q}}, \overline{\mathsf{p}}) \rightarrow \overline{\mathsf{p}} = \overline{\mathsf{a}}] = \mathsf{S}$; so by SF($\rightarrow$), $\mathsf{N_h}[\mathscr{H}(\overline{\mathsf{q}}, \overline{\mathsf{p}})] \neq \mathsf{S}$ or $\mathsf{N_h}[\overline{\mathsf{p}} = \overline{\mathsf{a}}] = \mathsf{S}$; but $\mathsf{N_h}[\mathscr{H}(\overline{\mathsf{q}}, \overline{\mathsf{p}})] = \mathsf{S}$; so $\mathsf{N_h}[\overline{\mathsf{p}} = \overline{\mathsf{a}}] = \mathsf{S}$. This is impossible; reject the assumption: $\mathsf{N}[\forall z(\exists w(\mathscr{G}(\overline{\mathsf{m}}, w) \wedge \mathscr{H}(w, z)) \rightarrow z = \overline{\mathsf{a}})] = \mathsf{T}$.

E12.11. Complete the demonstration of T12.8 by finishing the remaining cases. You should set up the entire argument, but may appeal to the text for parts already completed, as the text appeals to homework.

($\exists \leq$) $\mathscr{P}$ is $(\exists x \leq t)\mathscr{A}(x)$. Since $\mathscr{P}$ is a sentence, x is the only variable free in $\mathscr{A}$; in particular, since x does not appear in t, t is variable free; so $\mathsf{N_d}[t] = \mathsf{N}[t]$ and where $\mathsf{N}[t] = \mathsf{n}$, by T8.13, $\mathsf{Q} \vdash_{ND} t = \overline{\mathsf{n}}$; so $\mathsf{Q} \vdash_{ND} \mathscr{P}$ just in case $\mathsf{Q} \vdash_{ND} (\exists x \leq \overline{\mathsf{n}})\mathscr{A}(x)$.

(i) Suppose $\mathsf{N}[\mathscr{P}] = \mathsf{T}$; then $\mathsf{N}[(\exists x \leq t)\mathscr{A}(x)] = \mathsf{T}$; so by TI, for any d, $\mathsf{N_d}[(\exists x \leq t)\mathscr{A}(x)] = \mathsf{S}$; so by T12.7, for some $\mathsf{m} \leq \mathsf{N_d}[t]$, $\mathsf{N_{d(x|m)}}[\mathscr{A}(x)] = \mathsf{S}$; so where $\mathsf{N_d}[t] = \mathsf{N}[t] = \mathsf{n}$, for some $\mathsf{m} \leq \mathsf{n}$, $\mathsf{N_{d(x|m)}}[\mathscr{A}(x)] = \mathsf{S}$; so with T10.2, for some $\mathsf{m} \leq \mathsf{n}$, $\mathsf{N_d}[\mathscr{A}(\overline{\mathsf{m}})] = \mathsf{S}$; since x is the only variable free in $\mathscr{A}$, $\mathscr{A}(\overline{\mathsf{m}})$ is a sentence; so with T8.5, for some $\mathsf{m} \leq \mathsf{n}$, $\mathsf{N}[\mathscr{A}(\overline{\mathsf{m}})] = \mathsf{T}$; so by assumption for some $\mathsf{m} \leq \mathsf{n}$, $\mathsf{Q} \vdash_{ND} \mathscr{A}(\overline{\mathsf{m}})$; so by T8.20, $\mathsf{Q} \vdash_{ND} (\exists x \leq \overline{\mathsf{n}})\mathscr{A}(x)$; so $\mathsf{Q} \vdash_{ND} \mathscr{P}$.

(ii) Suppose $\mathsf{N}[\mathscr{P}] \neq \mathsf{T}$; then $\mathsf{N}[(\exists x \leq t)\mathscr{A}(x)] \neq \mathsf{T}$; so by TI, for some d, $\mathsf{N_d}[(\exists x \leq t)\mathscr{A}(x)] \neq \mathsf{S}$; so by T12.7, for any $\mathsf{m} \leq \mathsf{N_d}[t]$, $\mathsf{N_{d(x|m)}}[\mathscr{A}(x)] \neq \mathsf{S}$; so where $\mathsf{N_d}[t] = \mathsf{N}[t] = \mathsf{n}$, for any $\mathsf{m} \leq \mathsf{n}$, $\mathsf{N_{d(x|m)}}[\mathscr{A}(x)] \neq \mathsf{S}$; so with T10.2, for any $\mathsf{m} \leq \mathsf{n}$, $\mathsf{N_d}[\mathscr{A}(\overline{\mathsf{m}})] \neq \mathsf{S}$; so by TI, for any $\mathsf{m} \leq \mathsf{n}$, $\mathsf{N}[\mathscr{A}(\overline{\mathsf{m}})] \neq \mathsf{T}$; so $\mathsf{N}[\mathscr{A}(\overline{0})] \neq \mathsf{T}$ and ... and $\mathsf{N}[\mathscr{A}(\overline{\mathsf{n}})] \neq \mathsf{T}$; so by assumption, $\mathsf{Q} \vdash_{ND} \sim\mathscr{A}(\emptyset)$ and ... and $\mathsf{Q} \vdash_{ND} \sim\mathscr{A}(\overline{\mathsf{n}})$; so by T8.21, $\mathsf{Q} \vdash_{ND} (\forall x \leq \overline{\mathsf{n}})\sim\mathscr{A}(x)$; so by BQN, $\mathsf{Q} \vdash_{ND} \sim(\exists x \leq \overline{\mathsf{n}})\mathscr{A}(x)$; so $\mathsf{Q} \vdash_{ND} \sim\mathscr{P}$.

E12.13. Complete the demonstration of T12.11 by completing the remaining cases, including the basis and part (ii) of the case for composition.

Exercise 12.13

1.	$\forall z(\mathscr{G}(\overline{\mathsf{m}}, z) \to z = \overline{\mathsf{b}})$	$\mathscr{G}$ cap g
2.	$\forall z(\mathscr{H}(\overline{\mathsf{b}}, z) \to z = \overline{\mathsf{a}})$	$\mathscr{H}$ cap h
3.	$\quad \exists w[\mathscr{G}(\overline{\mathsf{m}}, w) \wedge \mathscr{H}(w, j)]$	A (g, $\to$I)
4.	$\quad\quad \mathscr{G}(\overline{\mathsf{m}}, k) \wedge \mathscr{H}(k, j)$	A (g, 3 $\exists$E)
5.	$\quad\quad \mathscr{G}(\overline{\mathsf{m}}, k)$	4 $\wedge$E
6.	$\quad\quad \mathscr{G}(\overline{\mathsf{m}}, k) \to k = \overline{\mathsf{b}}$	1 $\forall$E
7.	$\quad\quad k = \overline{\mathsf{b}}$	6,5 $\to$E
8.	$\quad\quad \mathscr{H}(k, j)$	4 $\wedge$E
9.	$\quad\quad \mathscr{H}(\overline{\mathsf{b}}, j)$	8,7 =E
10.	$\quad\quad \mathscr{H}(\overline{\mathsf{b}}, j) \to j = \overline{\mathsf{a}}$	2 $\forall$E
11.	$\quad\quad j = \overline{\mathsf{a}}$	10,9 $\to$E
12.	$\quad j = \overline{\mathsf{a}}$	3,4-11 $\exists$E
13.	$\exists w[\mathscr{G}(\overline{\mathsf{m}}, w) \wedge \mathscr{H}(w, j)] \to j = \overline{\mathsf{a}}$	3-12 $\to$I
14.	$\forall z(\exists w[\mathscr{G}(\overline{\mathsf{m}}, w) \wedge \mathscr{H}(w, z)] \to z = \overline{\mathsf{a}})$	13 $\forall$I

E12.14. Produce a derivation to show the basis in the argument for the uniqueness condition.

1.	$\forall z[\mathscr{G}(\overline{\mathsf{m}}, z) \to z = \overline{\mathsf{k}}_0]$	from capture
2.	$\forall p \forall q \forall y[(\mathscr{B}(p, q, \emptyset, \overline{\mathsf{k}}_0) \wedge \mathscr{B}(p, q, \emptyset, y)) \to \overline{\mathsf{k}}_0 = y]$	from uniqueness
3.	$\quad \exists p \exists q\{\exists v[\mathscr{B}(p, q, \emptyset, v) \wedge \mathscr{G}(\overline{\mathsf{m}}, v)] \wedge \mathscr{Q} \wedge \mathscr{B}(p, q, \emptyset, j)\}$	A (g, $\to$I)
4.	$\quad\quad \exists q\{\exists v[\mathscr{B}(p, q, \emptyset, v) \wedge \mathscr{G}(\overline{\mathsf{m}}, v)] \wedge \mathscr{Q} \wedge \mathscr{B}(p, q, \emptyset, j)\}$	A (g, 3$\exists$E)
5.	$\quad\quad\quad \exists v[\mathscr{B}(p, q, \emptyset, v) \wedge \mathscr{G}(\overline{\mathsf{m}}, v)] \wedge \mathscr{Q} \wedge \mathscr{B}(p, q, \emptyset, j)$	A (g, 4$\exists$E)
6.	$\quad\quad\quad \exists v[\mathscr{B}(p, q, \emptyset, v) \wedge \mathscr{G}(\overline{\mathsf{m}}, v)]$	5 $\wedge$E
7.	$\quad\quad\quad \mathscr{B}(p, q, \emptyset, j)$	5 $\wedge$E
8.	$\quad\quad\quad\quad \mathscr{B}(p, q, \emptyset, k) \wedge \mathscr{G}(\overline{\mathsf{m}}, k)$	A (g, 6$\exists$E)
9.	$\quad\quad\quad\quad \mathscr{B}(p, q, \emptyset, k)$	8 $\wedge$E
10.	$\quad\quad\quad\quad \mathscr{G}(\overline{\mathsf{m}}, k)$	8 $\wedge$E
11.	$\quad\quad\quad\quad \mathscr{G}(\overline{\mathsf{m}}, k) \to k = \overline{\mathsf{k}}_0$	1 $\forall$E
12.	$\quad\quad\quad\quad k = \overline{\mathsf{k}}_0$	11,10 $\to$E
13.	$\quad\quad\quad\quad \mathscr{B}(p, q, \emptyset, \overline{\mathsf{k}}_0)$	9,12 =E
14.	$\quad\quad\quad\quad j = \overline{\mathsf{k}}_0$	2,7,13
15.	$\quad\quad\quad j = \overline{\mathsf{k}}_0$	6,8-14 $\exists$E
16.	$\quad\quad j = \overline{\mathsf{k}}_0$	4,5-15 $\exists$E
17.	$\quad j = \overline{\mathsf{k}}_0$	3,4-16 $\exists$E
18.	$\exists p \exists q\{\exists v[\mathscr{B}(p, q, \emptyset, v) \wedge \mathscr{G}(\vec{x}, v)] \wedge \mathscr{Q} \wedge \mathscr{B}(p, q, \emptyset, j)\} \to j = \overline{\mathsf{k}}_0$	3-17 $\to$I
19.	$\forall w[\exists p \exists q\{\exists v[\mathscr{B}(p, q, \emptyset, v) \wedge \mathscr{G}(\vec{x}, v)] \wedge \mathscr{Q} \wedge \mathscr{B}(p, q, \emptyset, w)\} \to w = \overline{\mathsf{k}}_0]$	18 $\forall$I

E12.19. Work carefully through the demonstration of T12.16 by setting up revised arguments T12.3†, T12.11† and T12.12†.

T12.11†. For any recursive $\mathsf{f}(\vec{x})$ originally expressed by $\mathscr{F}(\vec{x}, v)$, let $\mathscr{F}^{\dagger}(\vec{x}, v)$ be like $\mathscr{F}(\vec{x}, v)$ except that $\mathscr{B}$ is replaced by $\mathscr{B}'$. Then $\mathsf{f}(\vec{x})$ is captured in Q by $\mathscr{F}^{\dagger}(\vec{x}, v)$.

By induction on the sequence of recursive functions.

Basis: f_0 is an initial function. Everything is the same, except that conclusions are for Q rather than Q_s.

Assp: For any i, $0 \leq i < k$, $\mathsf{f}_\mathsf{i}(\vec{\mathsf{x}})$ is captured in Q by $\mathscr{F}^{\dagger}(\vec{x}, v)$.

Show: $\mathsf{f}_\mathsf{k}(\vec{\mathsf{x}})$ is captured in Q by $\mathscr{F}^{\dagger}(\vec{x}, v)$.

f_k is either an initial function or arises from previous members by composition, recursion or regular minimization. If it is an initial function, then as in the basis. So suppose f_k arises from previous members.

(c) $\mathsf{f}_\mathsf{k}(\vec{\mathsf{x}}, \vec{\mathsf{y}}, \vec{\mathsf{z}})$ arises by composition from $\mathsf{g}(\vec{\mathsf{y}})$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{w}, \vec{\mathsf{z}})$. By assumption $\mathsf{g}(\vec{\mathsf{y}})$ is captured by $\mathscr{G}^{\dagger}(\vec{y}, w)$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{w}, \vec{\mathsf{z}})$ by $\mathscr{H}^{\dagger}(\vec{x}, w, \vec{z}, v)$. $\mathscr{F}^{\dagger}(\vec{x}, \vec{y}, \vec{z}, v)$ is $\exists w[\mathscr{G}^{\dagger}(\vec{y}, w) \wedge \mathscr{H}^{\dagger}(\vec{x}, w, \vec{z}, v)]$. Consider the case where $\vec{\mathsf{x}}$ and $\vec{\mathsf{z}}$ drop out and $\vec{\mathsf{y}}$ is a single variable y. Suppose $\langle \mathsf{m}, \mathsf{a} \rangle \in \mathsf{f}_\mathsf{k}$; then by composition there is some b such that $\langle \mathsf{m}, \mathsf{b} \rangle \in \mathsf{g}$ and $\langle \mathsf{b}, \mathsf{a} \rangle \in \mathsf{h}$.

(i) By T12.3†, $\mathscr{F}^{\dagger}(y, v)$ expresses $\mathsf{f}(\mathsf{y})$; thus, since $\langle \mathsf{m}, \mathsf{a} \rangle \in \mathsf{f}_\mathsf{k}$, $\mathsf{N}[\mathscr{F}^{\dagger}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] = \mathsf{T}$; so, since $\mathscr{F}^{\dagger}(y, v)$ is Σ_1, by T12.9, Q $\vdash_{ND}$ $\mathscr{F}^{\dagger}(\overline{\mathsf{m}}, \overline{\mathsf{a}})$.

(ii) Same but with $\mathscr{G}^{\dagger}$, $\mathscr{H}^{\dagger}$ uniformly substituted for $\mathscr{G}$, $\mathscr{H}$.

(r) $\mathsf{f}_\mathsf{k}(\vec{\mathsf{x}}, \mathsf{y})$ arises by recursion from $\mathsf{g}(\vec{\mathsf{x}})$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$. By assumption $\mathsf{g}(\vec{\mathsf{x}})$ is captured by $\mathscr{G}^{\dagger}(\vec{x}, v)$ and $\mathsf{h}(\vec{\mathsf{x}}, \mathsf{y}, \mathsf{u})$ by $\mathscr{H}^{\dagger}(\vec{x}, y, u, v)$. $\mathscr{F}^{\dagger}(\vec{x}, y, z)$ is,

$$\exists p \exists q\{\exists v[\mathscr{B}'(p, q, \emptyset, v) \wedge \mathscr{G}^{\dagger}(\vec{x}, v)] \wedge (\forall i < y)\exists u \exists v[\mathscr{B}'(p, q, i, u) \wedge \mathscr{B}'(p, q, Si, v) \wedge \mathscr{H}^{\dagger}(\vec{x}, i, u, v)] \wedge \mathscr{B}'(p, q, y, z)\}$$

Suppose $\vec{\mathsf{x}}$ reduces to a single variable and $\langle \mathsf{m}, \mathsf{n}, \mathsf{a} \rangle \in \mathsf{f}_\mathsf{k}$. (i) By T12.3†, $\mathscr{F}^{\dagger}(x, y, v)$ expresses $\mathsf{f}(\mathsf{x}, \mathsf{y})$; thus $\mathsf{N}[\mathscr{F}^{\dagger}(\overline{\mathsf{m}}, \overline{\mathsf{n}}, \overline{\mathsf{a}})] = \mathsf{T}$; so, since $\mathscr{F}^{\dagger}(x, y, v)$ is Σ_1, by T12.9, Q $\vdash_{ND}$ $\mathscr{F}^{\dagger}(\overline{\mathsf{m}}, \overline{\mathsf{n}}, \overline{\mathsf{a}})$. And (ii) by T12.12†, Q $\vdash_{ND}$ $\forall w[\mathscr{F}^{\dagger}(\overline{\mathsf{m}}, \overline{\mathsf{n}}, w) \rightarrow w = \overline{\mathsf{a}}]$.

(m) $\mathsf{f}_\mathsf{k}(\vec{\mathsf{x}})$ arises by regular minimization from $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$. By assumption, $\mathsf{g}(\vec{\mathsf{x}}, \mathsf{y})$ is captured by some $\mathscr{G}^{\dagger}(\vec{x}, y, z)$. $\mathscr{F}^{\dagger}(\vec{x}, v)$ is $\mathscr{G}^{\dagger}(\vec{x}, v, \emptyset) \wedge (\forall y < v) \sim \mathscr{G}^{\dagger}(\vec{x}, y, \emptyset)$. Suppose $\vec{x}$ reduces to a single variable and $\langle \mathsf{m}, \mathsf{a} \rangle \in \mathsf{f}_\mathsf{k}$.

(i) By T12.3†, $\mathscr{F}^{\dagger}(x, v)$ expresses $\mathsf{f}(\mathsf{x})$; thus, since $\langle \mathsf{m}, \mathsf{a} \rangle \in \mathsf{f}_\mathsf{k}$, $\mathsf{N}[\mathscr{F}^{\dagger}(\overline{\mathsf{m}}, \overline{\mathsf{a}})] = \mathsf{T}$; so, since $\mathscr{F}^{\dagger}(y, v)$ is Σ_1, by T12.9, Q $\vdash_{ND}$ $\mathscr{F}^{\dagger}(\overline{\mathsf{m}}, \overline{\mathsf{a}})$.

(ii) Same but with $\mathscr{G}^{\dagger}$ uniformly substituted for $\mathscr{G}$.

Exercise 12.19

Indct: Any recursive $\mathsf{f}(\vec{\mathsf{x}})$ is captured in Q by $\mathscr{F}^{\dagger}(\vec{x}, v)$.

E12.24. Provide definitions for the recursive functions $\mathsf{rm}(\mathsf{m},\mathsf{n})$ and $\mathsf{qt}(\mathsf{m},\mathsf{n})$ for the remainder and quotient of $\mathsf{m}/\mathsf{n}+1$. For $\mathsf{rm}(\mathsf{m},\mathsf{n})$,

$$(\mu \mathsf{v} \le \mathsf{n})(\exists \mathsf{w} \le \mathsf{m})[\mathsf{m} = \mathsf{Sn} \times \mathsf{w} + \mathsf{v}]$$

E12.25. Functions $\mathsf{f}_1(\vec{\mathsf{x}},\mathsf{y})$ and $\mathsf{f}_2(\vec{\mathsf{x}},\mathsf{y})$ are defined by *simultaneous* (mutual) recursion just in case,

$\mathsf{f}_1(\vec{\mathsf{x}},0) = \mathsf{g}_1(\vec{\mathsf{x}})$

$\mathsf{f}_2(\vec{\mathsf{x}},0) = \mathsf{g}_2(\vec{\mathsf{x}})$

$\mathsf{f}_1(\vec{\mathsf{x}},\mathsf{Sy}) = \mathsf{h}_1(\vec{\mathsf{x}},\mathsf{y},\mathsf{f}_1(\vec{\mathsf{x}},\mathsf{y}),\mathsf{f}_2(\vec{\mathsf{x}},\mathsf{y}))$

$\mathsf{f}_2(\vec{\mathsf{x}},\mathsf{Sy}) = \mathsf{h}_2(\vec{\mathsf{x}},\mathsf{y},\mathsf{f}_1(\vec{\mathsf{x}},\mathsf{y}),\mathsf{f}_2(\vec{\mathsf{x}},\mathsf{y}))$

Show that f_1 and f_2 so defined are recursive. For $\mathsf{F}(\vec{\mathsf{x}},\mathsf{y}) = \pi_0^{\mathsf{f}_1(\vec{\mathsf{x}},\mathsf{y})} \times \pi_1^{\mathsf{f}_2(\vec{\mathsf{x}},\mathsf{y})}$, set

$\mathsf{G}(\vec{\mathsf{x}}) = \pi_0^{\mathsf{g}_1(\vec{\mathsf{x}})} \times \pi_1^{\mathsf{g}_2(\vec{\mathsf{x}})}$

$\mathsf{H}(\vec{\mathsf{x}},\mathsf{y},\mathsf{u}) = \pi_0^{\mathsf{h}_1(\vec{\mathsf{x}},\mathsf{y},\mathsf{exp}(\mathsf{u},0),\mathsf{exp}(\mathsf{u},1))} \times \pi_1^{\mathsf{h}_2(\mathsf{x},\mathsf{y},\mathsf{exp}(\mathsf{u},0),\mathsf{exp}(\mathsf{u},1))}$

You should explain how these contribute to the desired result.

E12.29. (i) Complete the construction with recursive relations for $\mathsf{AXIOMAD5}(\mathsf{n})$, $\mathsf{GEN}(\mathsf{m},\mathsf{n})$, $\mathsf{AXIOMAD8}(\mathsf{n})$, and so $\mathsf{AXIOMAD}(\mathsf{n})$ and $\mathsf{PRFAD}(\mathsf{m},\mathsf{n})$. (ii) Complete the remaining axioms for Robinson arithmetic, and then $\mathsf{AXIOMQ}(\mathsf{n})$ and $\mathsf{PRFQ}(\mathsf{m},\mathsf{n})$. (iii) Construct also $\mathsf{AXIOMQP}(\mathsf{n})$, like AXIOMQ less $\mathsf{AXIOMQ7}$, and then $\mathsf{AXIOMPA}(\mathsf{n})$ and $\mathsf{PRFPA}(\mathsf{m},\mathsf{n})$.

$\mathsf{AXIOMAD5}(\mathsf{n})$: $(\exists \mathsf{p} \le \mathsf{n})(\exists \mathsf{q} \le \mathsf{n})(\exists \mathsf{v} \le \mathsf{n})[\mathsf{WFF}(\mathsf{p}) \wedge \mathsf{WFF}(\mathsf{q}) \wedge \mathsf{VAR}(\mathsf{v}) \wedge {\sim}\mathsf{FREEf}(\mathsf{p},\mathsf{v}) \wedge \mathsf{n} = \mathsf{cnd}(\mathsf{unv}(\mathsf{v},\mathsf{cnd}(\mathsf{p},\mathsf{q})),\mathsf{cnd}(\mathsf{p},\mathsf{unv}(\mathsf{v},\mathsf{q})))]$

$\mathsf{GEN}(\mathsf{m},\mathsf{n})$: $(\exists \mathsf{v} \le \mathsf{n})[\mathsf{VAR}(\mathsf{v}) \wedge \mathsf{n} = \mathsf{unv}(\mathsf{v},\mathsf{m})]$

$\mathsf{PRFQ}(\mathsf{m},\mathsf{n})$: $\mathsf{exp}(\mathsf{m},\mathsf{len}(\mathsf{m}) \dot{-} \overline{1}) = \mathsf{n} \wedge \mathsf{m} > \overline{1} \wedge (\forall \mathsf{k} < \mathsf{len}(\mathsf{m}))[\mathsf{AXIOMQ}(\mathsf{exp}(\mathsf{m},\mathsf{k})) \vee (\exists \mathsf{i} < \mathsf{k})(\exists \mathsf{j} < \mathsf{k})\mathsf{ICON}(\mathsf{exp}(\mathsf{m},\mathsf{i}),\mathsf{exp}(\mathsf{m},\mathsf{j}),\mathsf{exp}(\mathsf{m},\mathsf{k}))]$

E12.32. Let T be any theory that extends Q. For any formulas $\mathscr{F}_1(y)$ and $\mathscr{F}_2(y)$, generalize the diagonal lemma to find sentences $\mathscr{H}_1$ and $\mathscr{H}_2$ such that,

$$T \vdash \mathscr{H}_1 \leftrightarrow \mathscr{F}_1(\overline{\ulcorner \mathscr{H}_2 \urcorner})$$

$$T \vdash \mathscr{H}_2 \leftrightarrow \mathscr{F}_2(\overline{\ulcorner \mathscr{H}_1 \urcorner})$$

Demonstrate your result.

Let $\mathsf{alt}(\mathsf{p}, \mathsf{f}_1, \mathsf{f}_2) = \ulcorner \exists w \exists x \exists y(w = \urcorner \star \mathsf{num}(\mathsf{p}) \star \ulcorner \wedge \mathsf{x} = \urcorner \star \mathsf{num}(\mathsf{f}_2) \star \ulcorner \wedge y = \urcorner \star \mathsf{num}(\mathsf{f}_1) \star \ulcorner \wedge \exists z(\urcorner \star \mathsf{f}_1 \star \ulcorner \wedge \urcorner \star \mathsf{p} \star \ulcorner))\urcorner$. Then by capture there is a formula $Alt(w, x, y, z)$ that captures alt; let $\mathsf{a} = \ulcorner Alt(w, x, y, z)\urcorner$. Then $\mathscr{H}_1 = \exists w \exists x \exists y(w = \overline{\mathsf{a}} \wedge x = \overline{\mathsf{f}}_2 \wedge y = \overline{\mathsf{f}}_1 \wedge \exists z(\mathscr{F}_1(z) \wedge Alt(w, x, y, z)))$; and $\mathsf{h}_1 = \ulcorner \mathscr{H}_1 \urcorner = \mathsf{alt}(\overline{\mathsf{a}}, \overline{\mathsf{f}}_1, \overline{\mathsf{f}}_2)$. And $\mathscr{H}_2 = \exists w \exists x \exists y(w = \overline{\mathsf{a}} \wedge x = \overline{\mathsf{f}}_1 \wedge y = \overline{\mathsf{f}}_2 \wedge \exists z(\mathscr{F}_2(z) \wedge Alt(w, x, y, z)))$; and $\mathsf{h}_2 = \ulcorner \mathscr{H}_2 \urcorner = \mathsf{alt}(\overline{\mathsf{a}}, \overline{\mathsf{f}}_2, \overline{\mathsf{f}}_1)$. The trick to this is that $\mathscr{H}_1$ says $\mathscr{F}_1(\overline{\mathsf{h}}_2)$ and $\mathscr{H}_2$ says $\mathscr{F}_2(\overline{\mathsf{h}}_1)$. For the first case, argue as follows (broken into separate derivations for the biconditional).

1.	$\mathscr{H}_1 \leftrightarrow \exists w \exists x \exists y(w = \overline{\mathsf{a}} \wedge x = \overline{\mathsf{f}}_2 \wedge y = \overline{\mathsf{f}}_1 \wedge \exists z(\mathscr{F}_1(z) \wedge Alt(w, x, y, z)))$	def $\mathscr{H}_1$
2.	$\forall x[Alt(\overline{\mathsf{a}}, \overline{\mathsf{f}}_2, \overline{\mathsf{f}}_1, x) \rightarrow x = \overline{\mathsf{h}}_2$	from capture
3.	$\mathscr{H}_1$	A ($g \rightarrow$I)
4.	$\exists w \exists x \exists y(w = \overline{\mathsf{a}} \wedge x = \overline{\mathsf{f}}_2 \wedge y = \overline{\mathsf{f}}_1 \wedge \exists z(\mathscr{F}_1(z) \wedge Alt(w, x, y, z)))$	1,3 $\leftrightarrow$E
5.	$\exists x \exists y(j = \overline{\mathsf{a}} \wedge x = \overline{\mathsf{f}}_2 \wedge y = \overline{\mathsf{f}}_1 \wedge \exists z(\mathscr{F}_1(z) \wedge Alt(j, x, y, z)))$	A (g 4$\exists$E)
6.	$\exists y(j = \overline{\mathsf{a}} \wedge k = \overline{\mathsf{f}}_2 \wedge y = \overline{\mathsf{f}}_1 \wedge \exists z(\mathscr{F}_1(z) \wedge Alt(j, k, y, z)))$	A (g 5$\exists$E)
7.	$j = \overline{\mathsf{a}} \wedge k = \overline{\mathsf{f}}_2 \wedge l = \overline{\mathsf{f}}_1 \wedge \exists z(\mathscr{F}_1(z) \wedge Alt(j, k, l, z))$	A (g 6$\exists$E)
8.	$j = \overline{\mathsf{a}}$	7 $\wedge$E
9.	$k = \overline{\mathsf{f}}_2$	7 $\wedge$E
10.	$l = \overline{\mathsf{f}}_1$	7 $\wedge$E
11.	$\exists z(\mathscr{F}_1(z) \wedge Alt(j, k, l, z))$	7 $\wedge$E
12.	$\mathscr{F}_1(m) \wedge Alt(j, k, l, m)$	A (g 11$\exists$E)
13.	$\mathscr{F}_1(m)$	12 $\wedge$E
14.	$Alt(j, k, l, m)$	12 $\wedge$E
15.	$Alt(\overline{\mathsf{a}}, \overline{\mathsf{f}}_2, \overline{\mathsf{f}}_1, m) \rightarrow m = \overline{\mathsf{h}}_2$	2 $\forall$E
16.	$Alt(\overline{\mathsf{a}}, \overline{\mathsf{f}}_2, \overline{\mathsf{f}}_1, m)$	14,8,9,10 =E
17.	$m = \overline{\mathsf{h}}_2$	15,14 $\rightarrow$E
18.	$\mathscr{F}_1(\overline{\mathsf{h}}_2)$	13,17 =E
19.	$\mathscr{F}_1(\overline{\mathsf{h}}_2)$	12,13-18 $\exists$E
20.	$\mathscr{F}_1(\overline{\mathsf{h}}_2)$	6,7-19 $\exists$E
21.	$\mathscr{F}_1(\overline{\mathsf{h}}_2)$	5,6-20 $\exists$E
22.	$\mathscr{F}_1(\overline{\mathsf{h}}_2)$	4,5-21 $\exists$E
23.	$\mathscr{H}_1 \rightarrow \mathscr{F}_1(\overline{\mathsf{h}}_2)$	3-22 $\rightarrow$I

1.	$\mathcal{H}_1 \leftrightarrow \exists w \exists x \exists y(w = \overline{\mathsf{a}} \wedge x = \overline{\mathsf{f}}_2 \wedge y = \overline{\mathsf{f}}_1 \wedge \exists z(\mathcal{F}_1(z) \wedge Alt(w, x, y, z)))$	def $\mathcal{H}_1$
2.	$Alt(\overline{\mathsf{a}}, \overline{\mathsf{f}}_2, \overline{\mathsf{f}}_1, \overline{\mathsf{h}}_2)$	from capture
3.	$\mathcal{F}_1(\overline{\mathsf{h}}_2)$	A ($g \to$I)
4.	$\mathcal{F}_1(\overline{\mathsf{h}}_2) \wedge Alt(\overline{\mathsf{a}}, \overline{\mathsf{f}}_2, \overline{\mathsf{f}}_1, \overline{\mathsf{h}}_2)$	3,2 $\wedge$I
5.	$\exists z(\mathcal{F}_1(z) \wedge Alt(\overline{\mathsf{a}}, \overline{\mathsf{f}}_2, \overline{\mathsf{f}}_1, z))$	4 $\exists$I
6.	$\overline{\mathsf{a}} = \overline{\mathsf{a}} \wedge \overline{\mathsf{f}}_2 = \overline{\mathsf{f}}_2 \wedge \overline{\mathsf{f}}_1 = \overline{\mathsf{f}}_1$	=I, $\wedge$I
7.	$\overline{\mathsf{a}} = \overline{\mathsf{a}} \wedge \overline{\mathsf{f}}_2 = \overline{\mathsf{f}}_2 \wedge \overline{\mathsf{f}}_1 = \overline{\mathsf{f}}_1 \wedge \exists z(\mathcal{F}_1(z) \wedge Alt(\overline{\mathsf{a}}, \overline{\mathsf{f}}_2, \overline{\mathsf{f}}_1, z))$	6,5 $\wedge$I
8.	$\exists y(\overline{\mathsf{a}} = \overline{\mathsf{a}} \wedge \overline{\mathsf{f}}_2 = \overline{\mathsf{f}}_2 \wedge y = \overline{\mathsf{f}}_1 \wedge \exists z(\mathcal{F}_1(z) \wedge Alt(\overline{\mathsf{a}}, \overline{\mathsf{f}}_2, y, z)))$	7 $\exists$I
9.	$\exists x \exists y(\overline{\mathsf{a}} = \overline{\mathsf{a}} \wedge x = \overline{\mathsf{f}}_2 \wedge y = \overline{\mathsf{f}}_1 \wedge \exists z(\mathcal{F}_1(z) \wedge Alt(\overline{\mathsf{a}}, x, y, z)))$	8 $\exists$I
10.	$\exists w \exists x \exists y(w = \overline{\mathsf{a}} \wedge x = \overline{\mathsf{f}}_2 \wedge y = \overline{\mathsf{f}}_1 \wedge \exists z(\mathcal{F}_1(z) \wedge Alt(w, x, y, z)))$	9 $\exists$I
11.	$\mathcal{H}_1$	1,10 $\leftrightarrow$E
12.	$\mathcal{F}_1(\overline{\mathsf{h}}_2) \to \mathcal{H}_1$	3-11 $\to$I

So $T \vdash \mathcal{H}_1 \leftrightarrow \mathcal{F}_1(\overline{\ulcorner \mathcal{H}_2 \urcorner})$.

Chapter Thirteen

E13.2. Complete the demonstration of T13.3 by providing a derivation to show $T \vdash \mathcal{G} \leftrightarrow \sim\exists x Prft(x, \overline{\ulcorner \mathcal{G} \urcorner})$.

1.	$\mathscr{G} \leftrightarrow \exists z(z = \bar{\mathsf{a}} \wedge \sim\exists x\exists y[Prft(x,y) \wedge Diag(z,y)])$	from def $\mathscr{G}$
2.	$Diag(\bar{\mathsf{a}}, \bar{\mathsf{g}})$	from capture
3.	$\forall z(Diag(\bar{\mathsf{a}}, z) \rightarrow z = \bar{\mathsf{g}})$	from capture
4.	$\mathscr{G}$	A (g $\leftrightarrow$I)
5.	$\exists z(z = \bar{\mathsf{a}} \wedge \sim\exists x\exists y[Prft(x,y) \wedge Diag(z,y)])$	1,4 $\leftrightarrow$E
6.	$j = \bar{\mathsf{a}} \wedge \sim\exists x\exists y[Prft(x,y) \wedge Diag(j,y)]$	A (g 5$\exists$E)
7.	$j = \bar{\mathsf{a}}$	6 $\wedge$E
8.	$\sim\exists x\exists y[Prft(x,y) \wedge Diag(j,y)]$	6 $\wedge$E
9.	$\exists x Prft(x, \bar{\mathsf{g}})$	A (c $\sim$I)
10.	$Prft(k, \bar{\mathsf{g}})$	A (c 9$\exists$E)
11.	$Diag(j, \bar{\mathsf{g}})$	2,7 =E
12.	$Prft(k, \bar{\mathsf{g}}) \wedge Diag(j, \bar{\mathsf{g}})$	10,11 $\wedge$I
13.	$\exists y[Prft(k,y) \wedge Diag(j,y)]$	12 $\exists$I
14.	$\exists x\exists y[Prft(x,y) \wedge Diag(j,y)]$	13 $\exists$I
15.	$\bot$	8,14 $\bot$I
16.	$\bot$	9,10-15 $\exists$E
17.	$\sim\exists x Prft(x, \bar{\mathsf{g}})$	9-16 $\sim$I
18.	$\sim\exists x Prft(x, \bar{\mathsf{g}})$	5,6-17 $\exists$E
19.	$\sim\exists x Prft(x, \bar{\mathsf{g}})$	A (g $\leftrightarrow$I)
20.	$\exists x\exists y[Prft(x,y) \wedge Diag(\bar{\mathsf{a}},y)]$	A (c $\sim$I)
21.	$\exists y[Prft(j,y) \wedge Diag(\bar{\mathsf{a}},y)]$	A (c 20$\exists$E)
22.	$Prft(j,k) \wedge Diag(\bar{\mathsf{a}},k)$	A (c 21$\exists$E)
23.	$Diag(\bar{\mathsf{a}},k)$	22 $\wedge$E
24.	$Diag(\bar{\mathsf{a}},k) \rightarrow k = \bar{\mathsf{g}}$	3 $\forall$E
25.	$k = \bar{\mathsf{g}}$	24,23 $\rightarrow$E
26.	$Prft(j,k)$	22 $\wedge$E
27.	$Prft(j, \bar{\mathsf{g}})$	26,25 =E
28.	$\exists x Prft(x, \bar{\mathsf{g}})$	27 $\exists$I
29.	$\bot$	19,28 $\bot$I
30.	$\bot$	21,22-29 $\exists$E
31.	$\bot$	20,21-30 $\exists$E
32.	$\sim\exists x\exists y[Prft(x,y) \wedge Diag(\bar{\mathsf{a}},y)]$	20-31 $\sim$I
33.	$\bar{\mathsf{a}} = \bar{\mathsf{a}}$	=I
34.	$\bar{\mathsf{a}} = \bar{\mathsf{a}} \wedge \sim\exists x\exists y[Prft(x,y) \wedge Diag(\bar{\mathsf{a}},y)]$	33,32 $\wedge$I
35.	$\exists z(z = \bar{\mathsf{a}} \wedge \sim\exists x\exists y[Prft(x,y) \wedge Diag(z,y)])$	34 $\exists$I
36.	$\mathscr{G}$	1,35 $\leftrightarrow$E
37.	$\mathscr{G} \leftrightarrow \sim\exists x Prft(x, \bar{\mathsf{g}})$	4-18,19-36 $\leftrightarrow$I

So $T \vdash \mathscr{G} \leftrightarrow \sim\exists x Prft(x, \bar{\mathsf{g}})$ which is to say, $T \vdash \mathscr{G} \leftrightarrow \sim\exists x Prft(x, \overline{\ulcorner \mathscr{G} \urcorner})$.

E13.7. Complete the unfinished cases to T13.13.

T13.13.

T13.13.a. PA $\vdash (\mathscr{r} \leq \mathscr{s} \wedge \mathscr{s} \leq \mathscr{t}) \rightarrow \mathscr{r} \leq \mathscr{t}$

Hint: This does not require IN. It is not hard and can be worked directly from the definitions.

T13.13.b. $\mathrm{PA} \vdash (r < s \wedge s < t) \rightarrow r < t$

Hint: This does not require IN. It is not hard and can be worked directly from the definitions.

T13.13.c. $\mathrm{PA} \vdash (r \leq s \wedge s < t) \rightarrow r < t$

Hint: This does not require IN. It is not hard and can be worked directly from the definitions.

T13.13.d. $\mathrm{PA} \vdash \emptyset \leq t$

Hint: This is nearly trivial with the definition.

T13.13.e. $\mathrm{PA} \vdash \emptyset < St$

Hint: This is nearly trivial with the definition.

T13.13.f. $\mathrm{PA} \vdash t \neq \emptyset \leftrightarrow \emptyset < t$

Hint: This does not require IN. It is straightforward with the definitions.

T13.13.g. $\mathrm{PA} \vdash t > \emptyset \rightarrow \exists y(t = Sy)$ $\quad$ y not in t.

Hint: This is trivial with (f) and T6.45.

T13.13.h. $\mathrm{PA} \vdash t < St$

Hint: This is easy. It does not require IN.

T13.13.i. $\mathrm{PA} \vdash St = s \rightarrow t < s$

Hint: This does not require IN. It is not hard and can be worked directly from the definitions.

T13.13.j. $\mathrm{PA} \vdash s \leq t \leftrightarrow Ss \leq St$

Hint: This does not require IN. It is not hard and can be worked directly from the definitions. Do not forget about T6.40.

T13.13.k. $\mathrm{PA} \vdash s < t \leftrightarrow Ss < St$.

Hint: This does not require IN. It is not hard and can be worked directly from the definitions.

T13.13.l. PA $\vdash s < t \leftrightarrow Ss \leq t$

Hint: This does not require IN. It is not hard and can be worked directly from the definitions.

T13.13.m. PA $\vdash s \leq t \leftrightarrow s < t \vee s = t$

Hint: This does not require IN. It works as a direct argument from the definitions. Do not forget that you have $j = \emptyset \vee j \neq \emptyset$ with T6.45.

T13.13.n. PA $\vdash s < St \leftrightarrow s < t \vee s = t$

Hint: This does not require IN. It is simplified with (m).

T13.13.o. PA $\vdash s \leq St \leftrightarrow s \leq t \vee s = St$

Hint: This does not require IN. For one direction, it will be helpful to apply (m) and (n).

T13.13.p. PA $\vdash s < t \vee s = t \vee t < s$

Hint: This is a moderately interesting argument by IN where $\mathcal{P}$ is $s < x \vee s = x \vee x < s$. Under the assumption $s < j \vee s = j \vee j < s$, for the third case, you may find (l) and (m) helpful.

T13.13.q. PA $\vdash s \leq t \vee t < s$

Hint: This is a direct consequence of (p) and (m).

T13.13.r. PA $\vdash s \leq t \leftrightarrow t \not< s$

Hint: When $s \leq t$ you will be able to show $t \not< s$ with the definitions. In the other direction, use (p) and (m).

T13.13.s. PA $\vdash t < s \rightarrow t \neq s$

Hint: This does not require IN. It works from the definitions.

T13.13.t. PA $\vdash (s \leq t \wedge t \leq s) \rightarrow s = t$

Hint: Use (r) and (m) with the assumption for $\rightarrow$I.

T13.13.u. PA $\vdash s \leq s + t$

Hint: This is nearly trivial from the definition.

T13.13.v. PA $\vdash r \leq s \rightarrow r + t \leq s + t$

Hint: This does not require IN. It is straightforward from the definition and T6.68.

T13.13.w. PA $\vdash \mathcal{r} < \mathcal{s} \rightarrow \mathcal{r} + \mathcal{t} < \mathcal{s} + \mathcal{t}$

Hint: This does not require IN. It is straightforward from the definition and T6.68.

T13.13.x. PA $\vdash (\mathcal{r} \leq \mathcal{s} \wedge \mathcal{t} \leq \mathcal{u}) \rightarrow \mathcal{r} + \mathcal{t} \leq \mathcal{s} + \mathcal{u}$

Hint: This does not require IN. It is straightforward from the definitions.

T13.13.y. PA $\vdash (\mathcal{r} < \mathcal{s} \wedge \mathcal{t} \leq \mathcal{u}) \rightarrow \mathcal{r} + \mathcal{t} < \mathcal{s} + \mathcal{u}$

Hint: This does not require IN. It is straightforward from the definitions.

T13.13.z. PA $\vdash \emptyset < \mathcal{t} \rightarrow \mathcal{s} \leq \mathcal{s} \times \mathcal{t}$

Hint: This is straightforward with (f) and T6.50.

T13.13.aa. PA $\vdash \mathcal{r} \leq \mathcal{s} \rightarrow \mathcal{r} \times \mathcal{t} \leq \mathcal{s} \times \mathcal{t}$

Hint: This is straightforward with distributivity (T6.64).

T13.13.ab. PA $\vdash \mathcal{r} \times \mathcal{s} > \emptyset \rightarrow \mathcal{s} > \emptyset$

Hint: Under the assumption for $\rightarrow$I, assume the opposite and go for a contradiction.

T13.13.ac. PA $\vdash (\mathcal{r} > \overline{1} \wedge \mathcal{s} > \emptyset) \rightarrow \mathcal{r} \times \mathcal{s} > \mathcal{s}$

Hint: You can apply the definition for $>$ multiple times.

T13.13.ad. PA $\vdash (\mathcal{t} > \emptyset \wedge \mathcal{r} < \mathcal{s}) \rightarrow \mathcal{r} \times \mathcal{t} < \mathcal{s} \times \mathcal{t}$

Hint: This this combines strategies from previous problems.

T13.13.ae. PA $\vdash (\mathcal{r} < \mathcal{s} \wedge \mathcal{t} < \mathcal{u}) \rightarrow \mathcal{r} \times \mathcal{t} < \mathcal{s} \times \mathcal{u}$

Hint: This does not require IN. It is straightforward with T6.65.

T13.13.af. PA $\vdash \forall x[(\forall z < x)\mathcal{P}^x_z \rightarrow \mathcal{P}] \rightarrow \forall x\mathcal{P}$ *strong induction (a)*

Hint: Under the assumption for $\rightarrow$I, you will have a goal like $\mathcal{P}(j)$; you can get $(\forall z < j)\mathcal{P}(z) \rightarrow \mathcal{P}(j)$ from the assumption; go for $(\forall z < j)\mathcal{P}(z)$ by IN (where the induction is on j). Then the goal follows immediately by $\rightarrow$E.

T13.13.ag. PA $\vdash \mathcal{P}^x_\emptyset \wedge \forall x[(\forall z \leq x)\mathcal{P}^x_z \rightarrow \mathcal{P}^x_{Sx}] \rightarrow \forall x\mathcal{P}$ *strong induction (b)*

Again under the assumption for $\rightarrow$I, you will be able to obtain $\forall x\mathcal{P}$, this time by (af).

T13.13.ah. PA $\vdash \exists x \mathcal{P} \rightarrow \exists x[\mathcal{P} \wedge (\forall z < x) \sim \mathcal{P}^{x}_{z}]$ *least number principle*

Hint: This follows immediately from T13.13af applied to $\sim \mathcal{P}$.

E13.9. Produce the quick derivation to show T13.19d.

T13.19.

1.	$(\forall z < m(\vec{x})) \sim \mathcal{Q}(\vec{x}, z)$	T13.19c
2.	$\quad \mathcal{Q}(\vec{x}, v)$	A ($g \rightarrow$I)
3.	$\quad\quad v < m(\vec{x})$	A ($c \sim$I)
4.	$\quad\quad \sim \mathcal{Q}(\vec{x}, v)$	1,3 ($\forall$E)
5.	$\quad\quad \bot$	2,4 $\bot$I
6.	$\quad v \not< m(\vec{x})$	3-5 $\sim$I
7.	$\quad m(\vec{x}) \leq v$	6 T13.13r
8.	$\mathcal{Q}(\vec{x}, v) \rightarrow m(\vec{x}) \leq v$	2-7 $\rightarrow$I

E13.11. Complete the justifications for *Def*[*rm*] and *Def*[*qt*].

Def[*rm*]. (i) PA $\vdash \exists x (\exists w \leq \emptyset)[\emptyset = Sn \times w + x \wedge x < Sn]$.

Supposing the zero case is done,

1.	$\exists x(\exists w \leq \emptyset)[\emptyset = Sn \times w + x \wedge x < Sn]$	zero case
2.	$\exists x(\exists w \leq j)[j = Sn \times w + x \wedge x < Sn]$	A (g →I)
3.	$(\exists w \leq j)[j = Sn \times w + k \wedge k < Sn]$	A (g 2∃E)
4.	$j = Sn \times l + k \wedge k < Sn$	A (g 3 (∃E))
5.	$l \leq j$	
6.	$j = Sn \times l + k$	4 ∧E
7.	$k < Sn$	4 ∧E
8.	$Sj = S[Sn \times l + k]$	from 6
9.	$Sn \times l + Sk = S[Sn \times l + k]$	T6.42
10.	$Sj = Sn \times l + Sk$	8,9 =E
11.	$k < n \vee k = n$	7 T13.13n
12.	$k < n$	A (g 11∨E)
13.	$Sk < Sn$	9 T13.13k
14.	$Sj = Sn \times l + Sk \wedge Sk < Sn$	10,13 ∧I
15.	$l \leq j \vee l = Sj$	5 ∨I
16.	$l \leq Sj$	15 T13.13o
17.	$(\exists w \leq Sj)[Sj = Sn \times w + Sk \wedge Sk < Sn]$	14,16 (∃I)
18.	$\exists x(\exists w \leq Sj)[Sj = Sn \times w + x \wedge x < Sn]$	17 ∃I
19.	$k = n$	A (g 11∨E)
20.	$Sj = Sn \times l + Sn$	10,19 =E
21.	$Sn \times Sl = Sn \times l + Sn$	T6.44
22.	$Sj = Sn \times Sl$	20,21 =E
23.	$Sn \times Sl = Sn \times Sl + \emptyset$	T6.41
24.	$Sj = Sn \times Sl + \emptyset$	22,23 =E
25.	$\emptyset < Sn$	25 T13.13e
26.	$Sj = Sn \times Sl + \emptyset \wedge \emptyset < Sn$	24,25 ∧I
27.	$Sl \leq Sj$	5 T13.13k
28.	$(\exists w \leq Sj)[Sj = Sn \times w + \emptyset \wedge \emptyset < Sn]$	26,27 (∃I)
29.	$\exists x(\exists w \leq Sj)[Sj = Sn \times w + x \wedge x < Sn]$	28 ∃I
30.	$\exists x(\exists w \leq Sj)[Sj = Sn \times w + x \wedge x < Sn]$	11,12-18,19-29 ∨E
31.	$\exists x(\exists w \leq Sj)[Sj = Sn \times w + x \wedge x < Sn]$	3,4-30 (∃E)
32.	$\exists x(\exists w \leq Sj)[Sj = Sn \times w + x \wedge x < Sn]$	2,3-31 ∃E
33.	$\exists x(\exists w \leq j)[j = Sn \times w + x \wedge x < Sn] \to \exists x(\exists w \leq Sj)[Sj = Sn \times w + x \wedge x < Sn]$	2-32 →I
34.	$\forall z(\exists x(\exists w \leq z)[z = Sn \times w + x \wedge x < Sn] \to \exists x(\exists w \leq Sz)[Sz = Sn \times w + x \wedge x < Sn])$	33 ∀I
35.	$\forall z \exists x(\exists w \leq z)[z = Sn \times w + x \wedge x < Sn]$	1,34 IN
36.	$\exists x(\exists w \leq m)[m = Sn \times w + x \wedge x < Sn]$	35 ∀E

(ii) PA $\vdash \forall x \forall y[((\exists w \leq m)[m = Sn \times w + x \wedge x < Sn] \wedge (\exists w \leq m)[m = Sn \times w + y \wedge y < Sn]) \to x = y]$

Exercise 13.11 Def$[rm]$

1.	$(\exists w \leq m)[m = Sn \times w + j \wedge j < Sn] \wedge (\exists w \leq m)[m = Sn \times w + k \wedge k < Sn]$	A (g →I)
2.	$(\exists w \leq m)[m = Sn \times w + j \wedge j < Sn]$	1 ∧E
3.	$(\exists w \leq m)[m = Sn \times w + k \wedge k < Sn]$	1 ∧E
4.	$m = Sn \times p + j \wedge j < Sn$	A (g 2(∃E))
5.	$p \leq m$	
6.	$m = Sn \times q + k \wedge k < Sn$	A (g 3(∃E))
7.	$q \leq m$	
8.	$m = Sn \times p + j$	4 ∧E
9.	$j < Sn$	4 ∧E
10.	$m = Sn \times q + k$	6 ∧E
11.	$k < Sn$	6 ∧E
12.	$Sn \times p + j = Sn \times q + k$	8,10 =E
13.	$p < q \vee p = q \vee q < p$	T13.13p
14.	$p < q$	A (c ∼I)
15.	$\exists v(Sv + p = q)$	14 abv
16.	$Sl + p = q$	A (c 15∃E)
17.	$p + Sl = q$	16, T6.54
18.	$Sn \times p + j = Sn \times (p + Sl) + k$	12,17 =E
19.	$Sn \times p + j = (Sn \times p + Sn \times Sl) + k$	18 T6.63
20.	$Sn \times p + j = Sn \times p + (Sn \times Sl + k)$	19 T6.56
21.	$j = Sn \times Sl + k$	20 T6.68
22.	$\emptyset < Sl$	T13.13e
23.	$Sn \leq Sn \times Sl$	22 T13.13z
24.	$Sn \times Sl \leq Sn \times Sl + k$	T13.13u
25.	$Sn \leq Sn \times Sl + k$	23,24 T13.13a
26.	$Sn \leq j$	21,25 =E
27.	$j \not< Sn$	26 T13.13r
28.	$\perp$	9,27 ⊥I
29.	$\perp$	15,16-28 ∃E
30.	$p \not< q$	14-29 ∼I
31.	$q < p$	A (c ∼I)
32.	$\perp$	similarly
33.	$q \not< p$	31-32 ∼I
34.	$p = q$	13,30,33 DS
35.	$Sn \times p + j = Sn \times p + k$	12,34 =E
36.	$j = k$	35 T6.68
37.	$j = k$	3,6-36 (∃E)
38.	$j = k$	2,4-37 (∃E)
39.	$((\exists w \leq m)[m = Sn \times w + j \wedge j < Sn] \wedge (\exists w \leq m)[m = Sn \times w + k \wedge k < Sn]) \rightarrow j = k$	1-38 →I
40.	$\forall y[((\exists w \leq m)[m = Sn \times w + j \wedge j < Sn] \wedge (\exists w \leq m)[m = Sn \times w + y \wedge y < Sn]) \rightarrow j = y]$	39 ∀I
41.	$\forall x \forall y[((\exists w \leq m)[m = Sn \times w + x \wedge x < Sn] \wedge (\exists w \leq m)[m = Sn \times w + y \wedge y < Sn]) \rightarrow x = y]$	40 ∀I

E13.12. Complete the unfinished cases to T13.21.

For the recursion clause from right to left:

Exercise 13.12

1.	$v = \beta(p,q,i) \leftrightarrow \mathcal{B}(p,q,i,v)$	def β
2.	$v = \mathbbm{g}(\vec{x}) \leftrightarrow \mathcal{G}(\vec{x},v)$	assp
3.	$v = \mathbbm{h}(\vec{x},y,u) \leftrightarrow \mathcal{H}(\vec{x},y,u,v)$	assp
4.	$\mathcal{R}(\vec{x},y,z)$	A ($g \to$I)
5.	$\exists p \exists q\{\exists v[\mathcal{B}(p,q,\emptyset,v) \wedge \mathcal{G}(\vec{x},v)] \wedge$ $(\forall i < y)\exists u \exists v[\mathcal{B}(p,q,i,u) \wedge \mathcal{B}(p,q,Si,v) \wedge \mathcal{H}(\vec{x},i,u,v)] \wedge \mathcal{B}(p,q,y,z)\}$	4 def
6.	$\exists v[\mathcal{B}(a,b,\emptyset,v) \wedge \mathcal{G}(\vec{x},v)] \wedge$ $(\forall i < y)\exists u \exists v[\mathcal{B}(a,b,i,u) \wedge \mathcal{B}(a,b,Si,v) \wedge \mathcal{H}(\vec{x},i,u,v)] \wedge \mathcal{B}(a,b,y,z)$	A (g 5$\exists$E)
7.	$\exists v[\mathcal{B}(a,b,\emptyset,v) \wedge \mathcal{G}(\vec{x},v)]$	6 $\wedge$E
8.	$\mathcal{B}(a,b,\emptyset,k) \wedge \mathcal{G}(\vec{x},k)$	A (g 7$\exists$E)
9.	$\mathcal{B}(a,b,\emptyset,k)$	8 $\wedge$E
10.	$k = \beta(a,b,\emptyset)$	9 with 1
11.	$\mathcal{G}(\vec{x},k)$	8 $\wedge$E
12.	$k = \mathbbm{g}(\vec{x})$	11 with 2
13.	$\beta(a,b,\emptyset) = \mathbbm{g}(\vec{x})$	10,12 =E
14.	$\beta(a,b,\emptyset) = \mathbbm{g}(\vec{x})$	7,8-13 $\exists$E
15.	$(\forall i < y)\exists u \exists v[\mathcal{B}(a,b,i,u) \wedge \mathcal{B}(a,b,Si,v) \wedge \mathcal{H}(\vec{x},i,u,v)]$	6 $\wedge$E
16.	$l < y$	A (g ($\forall$I))
17.	$\exists u \exists v[\mathcal{B}(a,b,l,u) \wedge \mathcal{B}(a,b,Sl,v) \wedge \mathcal{H}(\vec{x},l,u,v)]$	15,16 ($\forall$E)
18.	$\mathcal{B}(a,b,l,r) \wedge \mathcal{B}(a,b,Sl,s) \wedge \mathcal{H}(\vec{x},l,r,s)$	A (g 17$\exists$E)
19.	$\mathcal{B}(a,b,l,r)$	18 $\wedge$E
20.	$r = \beta(a,b,l)$	19, with 1
21.	$\mathcal{B}(a,b,Sl,s)$	18 $\wedge$E
22.	$s = \beta(a,b,Sl)$	21 with 1
23.	$\mathcal{H}(\vec{x},l,r,s)$	18 $\wedge$E
24.	$s = \mathbbm{h}(\vec{x},l,r)$	23 with 3
25.	$\mathbbm{h}(\vec{x},l,\beta(a,b,l)) = \beta(a,b,Sl)$	24,20,22 =E
26.	$\mathbbm{h}(\vec{x},l,\beta(a,b,l)) = \beta(a,b,Sl)$	17,18-25 $\exists$E
27.	$(\forall i < y)\mathbbm{h}(\vec{x},i,\beta(a,b,i)) = \beta(a,b,Si)$	16-26 ($\forall$I)
28.	$\mathcal{B}(a,b,y,z)$	6 $\wedge$E
29.	$\beta(a,b,y) = z$	28 with 1
30.	$\beta(a,b,\emptyset) = \mathbbm{g}(\vec{x}) \wedge (\forall i < y)\mathbbm{h}(\vec{x},i,\beta(a,b,i)) = \beta(a,b,Si) \wedge \beta(a,b,y) = z$	14,27,29 $\wedge$I
31.	$\exists p \exists q[\beta(p,q,\emptyset) = \mathbbm{g}(\vec{x}) \wedge (\forall i < y)\mathbbm{h}(\vec{x},i,\beta(p,q,i)) = \beta(p,q,Si) \wedge \beta(p,q,y) = z]$	30 $\exists$I
32.	$z = \mathbbm{r}(\vec{x},y)$	31 def
33.	$z = \mathbbm{r}(\vec{x},y)$	5,6-32 $\exists$E
34.	$\mathcal{R}(\vec{x},y,z) \to z = \mathbbm{r}(\vec{x},y)$	4-33 $\to$I

E13.13. Complete the justification for T13.22 by demonstrating the zero case.

T13.22. With $\mathcal{F}(\vec{x}, y, v)$ as described in the main text,

1.	$\mathcal{F}(\vec{x}, \emptyset, m) \wedge \mathcal{F}(\vec{x}, \emptyset, n)$	A (g →I)
2.	$\exists p \exists q[\beta(p,q,\emptyset) = g(\vec{x}) \wedge (\forall i < \emptyset)h(\vec{x}, i, \beta(p,q,i)) = \beta(p,q,Si) \wedge \beta(p,q,\emptyset) = m]$	1 ∧E
3.	$\exists p \exists q[\beta(p,q,\emptyset) = g(\vec{x}) \wedge (\forall i < \emptyset)h(\vec{x}, i, \beta(p,q,i)) = \beta(p,q,Si) \wedge \beta(p,q,\emptyset) = n]$	1 ∧E
4.	$\beta(a,b,\emptyset) = g(\vec{x}) \wedge (\forall i < \emptyset)h(\vec{x}, i, \beta(a,b,i)) = \beta(a,b,Si) \wedge \beta(a,b,\emptyset) = m$	A (g 2∃E)
5.	$\beta(a,b,\emptyset) = g(\vec{x})$	4 ∧E
6.	$\beta(a,b,\emptyset) = m$	4 ∧E
7.	$m = g(\vec{x})$	5,6 =E
8.	$\beta(c,d,\emptyset) = g(\vec{x}) \wedge (\forall i < \emptyset)h(\vec{x}, i, \beta(c,d,i)) = \beta(c,d,Si) \wedge \beta(c,d,\emptyset) = n$	A (g 3∃E)
9.	$\beta(c,d,\emptyset) = g(\vec{x})$	8 ∧E
10.	$\beta(c,d,\emptyset) = n$	8 ∧E
11.	$n = g(\vec{x})$	9,10 =E
12.	$m = n$	7,11 =E
13.	$m = n$	3,8-12 ∃E
14.	$m = n$	2,4-13 ∃E
15.	$(\mathcal{F}(\vec{x}, \emptyset, m) \wedge \mathcal{F}(\vec{x}, \emptyset, n)) \rightarrow m = n$	1-14 →I
16.	$\forall m \forall n[(\mathcal{F}(\vec{x}, \emptyset, m) \wedge \mathcal{F}(\vec{x}, \emptyset, n)) \rightarrow m = n]$	15 ∀I

E13.14. Show (i) and (ii) for *Def*[∸]. Then show each of the results in T13.23.

Def[∸].

(i) PA $\vdash \exists v[x = y + v \vee (x < y \wedge v = \emptyset)]$. Beginning with T13.13q, this is is a straightforward derivation.

(ii) PA $\vdash \forall m \forall n[([x = y + m \vee (x < y \wedge m = \emptyset)] \wedge [x = y + n \vee (x < y \wedge n = \emptyset)]) \rightarrow m = n]$

1.	$[x = y + j \lor (x < y \land j = \emptyset)] \land [x = y + k \lor (x < y \land k = \emptyset)]$	A (g →I)
2.	$x = y + j \lor (x < y \land j = \emptyset)$	1 ∧E
3.	$x = y + k \lor (x < y \land k = \emptyset)$	1 ∧E
4.	$y \le x \lor x < y$	T13.13q
5.	$y \le x$	A (g 4∨E)
6.	$x \nless y$	5 T13.13r
7.	$\sim(x < y \land j = \emptyset)$	6 ∨I, DeM
8.	$\sim(x < y \land k = \emptyset)$	6 ∨I, DeM
9.	$x = y + j$	2,7 DS
10.	$x = y + k$	3,8 DS
11.	$y + j = y + k$	9,10 =E
12.	$j = k$	11 T6.68
13.	$x < y$	A (g 4∨E)
14.	$y \le y + j$	T13.13u
15.	$x < y + j$	13,14 T13.13c
16.	$x \ne y + j$	15 T13.13s
17.	$y \le y + k$	T13.13u
18.	$x < y + k$	13,17 T13.13c
19.	$x \ne y + k$	18 T13.13s
20.	$x < y \land j = \emptyset$	2,16 DS
21.	$x < y \land k = \emptyset$	3,19 DS
22.	$j = \emptyset$	20 ∧E
23.	$k = \emptyset$	21 ∧E
24.	$j = k$	22,23 =E
25.	$j = k$	4,5-12,13-24 ∨E
26.	$([x = y + j \lor (x < y \land j = \emptyset)] \land [x = y + k \lor (x < y \land k = \emptyset)]) \to j = k$	1-25→I
27.	$\forall m \forall n[([x = y + m \lor (x < y \land m = \emptyset)] \land [x = y + n \lor (x < y \land n = \emptyset)]) \to m = n]$	26 ∀I

T13.23.

T13.23.a. PA $\vdash a \ge b \to a = b + (a \dot{-} b)$.

This is straightforward with $a = b + (a \dot{-} b) \lor [a < b \land a \dot{-} b = \emptyset]$ from the definition.

T13.23.b. PA $\vdash b \ge a \to a \dot{-} b = \emptyset$.

From your assumption $b \ge a$ you have $a < b \lor a = b$ with T13.13m. In the first case, as in the previous problem, you get the result with the definition. In the second case, $a \ge b$ by T13.13m and you can use (a) with T6.68.

T13.23.c. PA $\vdash a \dot{-} b \le a$.

By T13.13q, $a \ge b \lor a < b$. In the first case apply (a); and in the second you have $a \le b$ so that you can apply (b).

T13.23.f. PA ⊢ $a > b \to a \dot{-} b > \emptyset$.

1.	$a > b$	A (g →I)
2.	$\exists v(Sv + b = a)$	1 def
3.	$Sj + b = a$	A (g 2∃E)
4.	$a \geq b$	1 T13.13m
5.	$a = b + (a \dot{-} b)$	4 T13.23a
6.	$Sj + b = b + (a \dot{-} b)$	3,5 =E
7.	$Sj = a \dot{-} b$	6 T6.68
8.	$\emptyset < Sj$	T13.13e
9.	$\emptyset < a \dot{-} b$	7,8 =E
10.	$\emptyset < a \dot{-} b$	2,3-9 ∃E
11.	$a > b \to \emptyset < a \dot{-} b$	

T13.23.h. PA ⊢ $Sa \dot{-} a = \overline{1}$.

Given T6.68, this is simple once you see from (a) that $Sa = a + (Sa \dot{-} a)$ and from T6.47 that $Sa = a + \overline{1}$.

T13.23.i. PA ⊢ $a > \emptyset \to a \dot{-} \overline{1} < a$

You can do this in just a few lines.

T13.23.l. PA ⊢ $a \geq c \to (a \dot{-} c) + b = (a + b) \dot{-} c$.

1.	$a \geq c$	A (g →I)
2.	$a = c + (a \dot{-} c)$	1 T13.23a
3.	$a + b \geq a$	T13.13u
4.	$a + b \geq c$	1,3 T13.13a
5.	$a + b = c + [(a + b) \dot{-} c]$	4 T13.23a
6.	$[c + (a \dot{-} c)] + b = c + [(a + b) \dot{-} c]$	2,5 =E
7.	$c + [(a \dot{-} c) + b] = c + [(a + b) \dot{-} c]$	6 T6.56
8.	$(a \dot{-} c) + b = (a + b) \dot{-} c$	7 T6.68
9.	$a \geq c \to (a \dot{-} c) + b = (a + b) \dot{-} c$	1-8 →I

T13.23.n. PA ⊢ $(a \dot{-} b) \dot{-} c = a \dot{-} (b + c)$.

1.	$a \geq b + c \vee a < b + c$	T13.13q
2.	$b + c > a$	A (g 1$\vee$E)
3.	$b + c \geq a$	2 T13.13m
4.	$a \dot{-} (b + c) = \emptyset$	3 T13.23b
5.	$a \geq b \vee a < b$	T13.13q
6.	$b > a$	A (g 5$\vee$E)
7.	$b \geq a$	6 T13.13m
8.	$a \dot{-} b = \emptyset$	7 T13.23b
9.	$c \geq \emptyset$	T13.13d
10.	$c \geq a \dot{-} b$	8,9 =E
11.	$(a \dot{-} b) \dot{-} c = \emptyset$	10 T13.23b
12.	$a \geq b$	A (g 5$\vee$E)
13.	$a = b + (a \dot{-} b)$	12 T13.23a
14.	$b + c \geq b + (a \dot{-} b)$	3,13 =E
15.	$c \geq a \dot{-} b$	14 T13.13v
16.	$(a \dot{-} b) \dot{-} c = \emptyset$	15 T13.23b
17.	$(a \dot{-} b) \dot{-} c = \emptyset$	5,6-11,12-16 $\vee$E
18.	$(a \dot{-} b) \dot{-} c = a \dot{-} (b + c)$	17,4 =E
19.	$a \geq b + c$	A (g 1$\vee$E)
20.	$a = (b + c) + [a \dot{-} (b + c)]$	19 T13.23a
21.	$b + c \geq b$	T13.13u
22.	$a \geq b$	19,21 T13.13a
23.	$a = b + (a \dot{-} b)$	22 T13.23a
24.	$b + (a \dot{-} b) \geq b + c$	19,23 =E
25.	$a \dot{-} b \geq c$	24 T13.13v
26.	$a \dot{-} b = c + [(a \dot{-} b) \dot{-} c]$	25 T13.23a
27.	$b + (a \dot{-} b) = (b + c) + [a \dot{-} (b + c)]$	20,23 =E
28.	$b + (c + [(a \dot{-} b) \dot{-} c]) = (b + c) + [a \dot{-} (b + c)]$	26,27 =E
29.	$(b + c) + [(a \dot{-} b) \dot{-} c] = (b + c) + [a \dot{-} (b + c)]$	28 T6.56
30.	$(a \dot{-} b) \dot{-} c = a \dot{-} (b + c)$	29 T6.68
31.	$(a \dot{-} b) \dot{-} c = a \dot{-} (b + c)$	1,2-18,19-30 $\vee$E

T13.23.o. PA $\vdash (a + c) \dot{-} (b + c) = a \dot{-} b$.

Start with $a \geq b \vee a < b$. The second case is easy. For the first, you can apply T13.23a to both $a \geq b$ and to $a + c \geq b + c$.

T13.23.p. PA $\vdash a \times (b \dot{-} c) = a \times b \dot{-} a \times c$.

1.	$a = \emptyset \vee a > \emptyset$	T13.13f
2.	$a = \emptyset$	A (g 1$\vee$E)
3.	$a(b \dot{-} c) = \emptyset$	2 T6.58
4.	$ab = \emptyset$	2 T6.58
5.	$ac \geq \emptyset$	T13.13d
6.	$ac \geq ab$	5,4 =E
7.	$ab \dot{-} ac = \emptyset$	6 T13.23b
8.	$a(b \dot{-} c) = ab \dot{-} ac$	3,7 =E
9.	$a > \emptyset$	A (g 1$\vee$E)
10.	$b \geq c \vee b < c$	T13.13q
11.	$c > b$	A (g 10$\vee$E)
12.	$c \geq b$	11 T13.13m
13.	$b \dot{-} c = \emptyset$	12 T13.23b
14.	$a(b \dot{-} c) = \emptyset$	13 T6.43
15.	$ac \geq ab$	12 T13.13aa
16.	$ab \dot{-} ac = \emptyset$	15 T13.23b
17.	$a(b \dot{-} c) = ab \dot{-} ac$	14,16 =E
18.	$b \geq c$	A (g 10$\vee$E)
19.	$b = c + (b \dot{-} c)$	18 T13.23a
20.	$ab = ab$	=I
21.	$ab = a[c + (b \dot{-} c)]$	20,19 =E
22.	$ab = ac + a(b \dot{-} c)$	21 T6.63
23.	$ab \geq ac$	18 T13.13aa
24.	$ab = ac + (ab \dot{-} ac)$	23 T13.23a
25.	$ac + a(b \dot{-} c) = ac + (ab \dot{-} ac)$	22,24 =E
26.	$a(b \dot{-} c) = ab \dot{-} ac$	25 T6.68
27.	$a(b \dot{-} c) = ab \dot{-} ac$	10,11-17,18-26 $\vee$E
28.	$a(b \dot{-} c) = ab \dot{-} ac$	1,2-8,9-27 $\vee$E

E13.15. Show each of the results in T13.24

T13.24.

T13.24.a. PA $\vdash \emptyset | a$

This is nearly immediate from the definition and T6.57.

T13.24.b. PA $\vdash a | Sa$.

This is nearly immediate from the definition and T6.57.

T13.24.d. PA $\vdash a | b \rightarrow a | (b \times c)$.

With the assumption for $\rightarrow$I, you will be able to get $(Sa \times j)c = bc$; then simple association and the definition give the result.

T13.24.f. PA $\vdash (a|Sb \wedge b|c) \rightarrow a|c$.

This is straightforward once you apply the definition to your assumption for →I, and then make the assumptions for ∃E.

T13.24.g. PA $\vdash a|b \rightarrow [a|(b + c) \leftrightarrow a|c]$.

1.	$a\|b$	A (g →I)
2.	$\exists q(Sa \times q = b)$	1 def
3.	$Sa \times j = b$	A (g 2∃E)
4.	$a\|(b + c)$	A (g ↔I)
5.	$\exists q(Sa \times q = b + c)$	4 def
6.	$Sa \times k = b + c$	A (g 5∃E)
7.	$Sa \times k = (Sa \times j) + c$	3,6 =E
8.	$j \leq k \vee k < j$	T13.13q
9.	$k < j$	A (c ∼I)
10.	$Sa \times j \leq (Sa \times j) + c$	T13.13u
11.	$\emptyset < Sa$	T13.13e
12.	$Sa \times k < Sa \times j$	9,11 T13.13ad
13.	$Sa \times k < (Sa \times j) + c$	10,12 T13.13c
14.	$Sa \times k \neq (Sa \times j) + c$	13 T13.13s
15.	$\bot$	7,14 ⊥I
16.	$k \not< j$	9-15 ∼I
17.	$j \leq k$	8,16 DS
18.	$\exists v(v + j = k)$	17 def
19.	$l + j = k$	A (g 18∃E)
20.	$Sa \times (l + j) = (Sa \times j) + c$	7,19 =E
21.	$(Sa \times l) + (Sa \times j) = (Sa \times j) + c$	20 T6.63
22.	$Sa \times l = c$	21 T6.68
23.	$\exists q(Sa \times q = c)$	22 ∃I
24.	$a\|c$	23 def
25.	$a\|c$	18,19-24 ∃E
26.	$a\|c$	5,6-25 ∃E
27.	$a\|c$	A (g ↔I)
28.	$\exists q(Sa \times q = c)$	27 def
29.	$Sa \times k = c$	A (g 28∃E)
30.	$b + c = b + c$	=I
31.	$(Sa \times j) + (Sa \times k) = b + c$	30,3,29 =E
32.	$Sa \times (j + k) = b + c$	31 T6.63
33.	$\exists q(Sa \times q = b + c)$	32 ∃I
34.	$a\|(b + c)$	33 def
35.	$a\|(b + c)$	28,29-34 ∃E
36.	$a\|(b + c) \leftrightarrow a\|c$	4-26,27-35 ↔I
37.	$a\|(b + c) \leftrightarrow a\|c$	2,3-36 ∃E
38.	$a\|b \rightarrow [a\|(b + c) \leftrightarrow a\|c]$	1-37 →I

Exercise 13.15 T13.24.g

T13.24.h. PA $\vdash (b \geq c \wedge a|b) \rightarrow [a|(b \mathbin{\dot{-}} c) \leftrightarrow a|c]$.

From the assumption for $\rightarrow$I you have $a|(c + (b \mathbin{\dot{-}} c))$; then with each of the assumptions for $\leftrightarrow$I you will be able to apply (g).

T13.24.i. PA $\vdash a < b \rightarrow b \nmid Sa$.

Make the standard assumptions for $\rightarrow$I, $\sim$I and, from the definition, $\exists$E to get $Sb \times j = Sa$; then, using the last strategy for reaching a contradiction, both $j = \emptyset$ and $j \neq \emptyset$ lead to contradiction.

T13.24.j. PA $\vdash a|b \leftrightarrow rm(b,a) = \emptyset$.

This is a matter of connecting the definitions. From $a|b$ you get $Sa \times j = b$ and from $rm(b,a) = \emptyset$, $b = Sa \times j + \emptyset \wedge \emptyset < Sa$; observe also that when $Sa \times j = b$ you have $j \leq b$ for ($\exists$I).

T13.24.k. PA $\vdash rm[a + (y \times Sd), d] = rm(a,d)$.

Let $r = rm(a,d)$

1.	$(\exists w \leq a)[a = Sd \times w + r \wedge r < Sd]$	def rm
2.	$a = (Sd \times j) + r \wedge r < Sd$	A (g 1($\exists$E))
3.	$j \leq a$	
4.	$a = (Sd \times j) + r$	2 $\wedge$E
5.	$a + (y \times Sd) = a + (y \times Sd)$	=I
6.	$a + (y \times Sd) = [(Sd \times j) + r] + (y \times Sd)$	4,5 =E
7.	$a + (y \times Sd) = [(Sd \times j) + (Sd \times y)] + r$	6 with T6.56
8.	$a + (y \times Sd) = Sd \times (j + y) + r$	7 T6.63
9.	$r < Sd$	2 $\wedge$E
10.	$a + (y \times Sd) = Sd \times (j + y) + r \wedge r < Sd$	8,9 $\wedge$I
11.	$a + (y \times Sd) = [d \times (j + y) + (j + y)] + r$	8 T6.60
12.	$a + (y \times Sd) = (j + y) + [d \times (j + y) + r]$	11 with T6.56
13.	$\exists v[v + (j + y) = a + (y \times Sd)]$	12 $\exists$I
14.	$j + y \leq a + (y \times Sd)$	13 def
15.	$(\exists w \leq a + (y \times Sd))[a + (y \times Sd) = Sd \times w + r \wedge r < Sd]$	10,14 ($\exists$I)
16.	$rm(a + (y \times Sd), d) = r$	15 def
17.	$rm(a + (y \times Sd), d) = r$	1,2-16 ($\exists$E)

T13.24.l. PA $\vdash Sd \times z \leq a \rightarrow z \leq qt(a,d)$.

Let $r = rm(a,d)$ and $q = qt(a,d)$

1.	$a = Sd \times q + r \wedge r < Sd$	def qt
2.	$Sd \times z \leq a$	A (g $\rightarrow$I)
3.	$z > q$	A (c $\sim$I)
4.	$z \geq Sq$	3 T13.13l
5.	$a = Sd \times q + r$	1 $\wedge$E
6.	$Sd \times Sq = (Sd \times q) + Sd$	T6.44
7.	$Sd \times z \geq Sd \times Sq$	4 T13.13aa
8.	$Sd \times z \geq (Sd \times q) + Sd$	7,6 =E
9.	$r < Sd$	1 $\wedge$E
10.	$(Sd \times q) + r < (Sd \times q) + Sd$	9 T13.13w
11.	$a < (Sd \times q) + Sd$	5,10 =E
12.	$a < Sd \times z$	8,11 T13.13c
13.	$a \not< Sd \times z$	2 T13.13r
14.	$\bot$	12,13 $\bot$I
15.	$z \not> q$	3-14 $\sim$I
16.	$z \leq q$	15 T13.13r
17.	$Sd \times z \leq a \rightarrow z \leq q$	2-16 $\rightarrow$I
18.	$Sd \times z \leq a \rightarrow z \leq qt(a,d)$	17 abv

T13.24.m. PA $\vdash a \geq y \times Sd \rightarrow rm[a \dot{-} (y \times Sd), d] = rm(a,d)$

Let $r = rm(a,d)$ and $q = qt(a,d)$

1.	$a = Sd \times q + r \wedge r < Sd$	def qt
2.	$a \geq y \times Sd$	A (g $\rightarrow$I)
3.	$a = Sd \times q + r$	1 $\wedge$E
4.	$a = (y \times Sd) + [a \dot{-} (y \times Sd)]$	2 T13.23a
5.	$Sd \times q + r = (y \times Sd) + [a \dot{-} (y \times Sd)]$	3,4 =E
6.	$y \leq q$	2 T13.24l
7.	$Sd \times y \leq Sd \times q$	6 T13.13aa
8.	$Sd \times q = (Sd \times y) + [(Sd \times q) \dot{-} (Sd \times y)]$	7 T13.23a
9.	$(Sd \times q) + r = (Sd \times q) + r$	=I
10.	$[(Sd \times q) \dot{-} (Sd \times y)] + [(Sd \times y) + r] = (Sd \times q) + r$	8,9 =E
11.	$[(Sd \times q) \dot{-} (Sd \times y)] + [(Sd \times y) + r] = (y \times Sd) + [a \dot{-} (y \times Sd)]$	5,10 =E
12.	$[(Sd \times q) \dot{-} (Sd \times y)] + r = a \dot{-} (y \times Sd)$	11 T6.68
13.	$a \dot{-} (y \times Sd) = Sd(q \dot{-} y) + r$	12 T13.23p
14.	$r < Sd$	1 $\wedge$E
15.	$a \dot{-} (y \times Sd) = Sd(q \dot{-} y) + r \wedge r < Sd$	13,14 $\wedge$I
16.	$a \dot{-} (y \times Sd) = [d(q \dot{-} y) + (q \dot{-} y)] + r]$	13 T6.60
17.	$\exists v[v + (q \dot{-} y) = a \dot{-} (y \times Sd)$	16 $\exists$I
18.	$q \dot{-} y \leq a \dot{-} (y \times Sd)$	17 def
19.	$(\exists w < a \dot{-} (y \times Sd))[a \dot{-} (y \times Sd) = Sd \times w + r \wedge r < Sd]$	15,18 ($\exists$I)
20.	$rm(a \dot{-} (y \times Sd), d) = r$	19 def rm
21.	$a \geq y \times Sd \rightarrow rm(a \dot{-} (y \times Sd), d) = r$	2-20 $\rightarrow$I

E13.16. Show each of the the results in T13.25.

T13.25.

Exercise 13.16 T13.25

T13.25.d. PA $\vdash \forall x[x > \bar{1} \rightarrow \exists z(Pr(Sz) \wedge z|x)]$

1.	$\emptyset > \bar{1} \rightarrow \exists z(Pr(Sz) \wedge z\|\emptyset)$	trivial
2.	$(\forall y \leq k)[y > \bar{1} \rightarrow \exists z(Pr(Sz) \wedge z\|y)]$	A (g $\rightarrow$I)
3.	$Sk > \bar{1}$	A (g $\rightarrow$I)
4.	$Pr(Sk) \vee \sim Pr(Sk)$	T3.1
5.	$Pr(Sk)$	A (g 4$\vee$E)
6.	$k\|Sk$	T13.24b
7.	$Pr(Sk) \wedge k\|Sk$	5,6 $\wedge$I
8.	$\exists z(Pr(Sz) \wedge z\|Sk)$	7 $\exists$I
9.	$\sim Pr(Sk)$	A (g 4$\vee$E)
10.	$\sim(\bar{1} < Sk \wedge \forall d[d\|Sk \rightarrow (d = \emptyset \vee Sd = Sk)]$	9 def
11.	$\bar{1} \not< Sk \vee \exists d[d\|Sk \wedge d \neq \emptyset \wedge Sd \neq Sk]$	10 DeM,QN
12.	$\exists d[d\|Sk \wedge d \neq \emptyset \wedge Sd \neq Sk]$	3,11 DS
13.	$j\|Sk \wedge j \neq \emptyset \wedge Sj \neq Sk$	A (g 12$\exists$E)
14.	$j\|Sk$	13 $\wedge$E
15.	$j \neq \emptyset$	13 $\wedge$E
16.	$Sj \neq Sk$	13 $\wedge$E
17.	$Sj \leq k \vee k < Sj$	T13.13q
18.	$k < Sj$	A (c $\sim$I)
19.	$k < j \vee k = j$	18 T13.13n
20.	$k = j$	A (c 19$\vee$E)
21.	$Sk = Sk$	=I
22.	$Sj = Sk$	21,20 =E
23.	$\perp$	16,22 $\perp$I
24.	$k < j$	A (c 19$\vee$E)
25.	$j \nmid Sk$	24 T13.24i
26.	$\perp$	14,25 $\perp$I
27.	$\perp$	19,20-23,24-26 $\vee$E
28.	$k \not< Sj$	18-27 $\sim$I
29.	$Sj \leq k$	17,28 DS
30.	$Sj > \bar{1} \rightarrow \exists z(Pr(Sz) \wedge z\|Sj)$	2,29 ($\forall$E)
31.	$j > \emptyset$	15 T13.13f
32.	$Sj > \bar{1}$	31 T13.13k
33.	$\exists z(Pr(Sz) \wedge z\|Sj)$	30,32 $\rightarrow$E
34.	$Pr(Sl) \wedge l\|Sj$	A (g 33$\exists$E)
35.	$l\|Sj$	34 $\wedge$E
36.	$l\|Sj \wedge j\|Sk$	35,14 $\wedge$I
37.	$l\|Sk$	36 T13.24f
38.	$Pr(Sl)$	34 $\wedge$E
39.	$Pr(Sl) \wedge l\|Sk$	38,37 $\wedge$I
40.	$\exists z(Pr(Sz) \wedge z\|Sk)$	39 $\exists$I
41.	$\exists z(Pr(Sz) \wedge z\|Sk)$	33,34-40 $\exists$E
42.	$\exists z(Pr(Sz) \wedge z\|Sk)$	12,13-41 $\exists$E
43.	$\exists z(Pr(Sz) \wedge z\|Sk)$	4,4-8,9-42 $\vee$E
44.	$Sk > \bar{1} \rightarrow \exists z(Pr(Sz) \wedge z\|Sk)$	3-43 $\rightarrow$I
45.	$(\forall y \leq k)[y > \bar{1} \rightarrow \exists z(Pr(Sz) \wedge z\|y)] \rightarrow [Sk > \bar{1} \rightarrow \exists z(Pr(Sz) \wedge z\|Sk)]$	2-44 $\rightarrow$I
46.	$\forall x\{(\forall y \leq x)[y > \bar{1} \rightarrow \exists z(Pr(Sz) \wedge z\|y)] \rightarrow [Sx > \bar{1} \rightarrow \exists z(Pr(Sz) \wedge z\|Sx)]\}$	45 $\forall$I
47.	$\forall x[x > \bar{1} \rightarrow \exists z(Pr(Sz) \wedge z\|x)]$	1,46 T13.13ag

T13.25.e. PA $\vdash Rp(a,b) \leftrightarrow \sim\exists x[Pr(Sx) \wedge x|a \wedge x|b]$.

Exercise 13.16 T13.25.e

1.	$Rp(a,b)$	A (g $\leftrightarrow$I)
2.	$\forall d[(d \mid a \wedge d \mid b) \rightarrow d = \emptyset]$	1 def
3.	$\exists x[Pr(Sx) \wedge x \mid a \wedge x \mid b]$	A (c $\sim$I)
4.	$Pr(Sj) \wedge j \mid a \wedge j \mid b$	A (c 3$\exists$E)
5.	$j \mid a \wedge j \mid b$	4 $\wedge$E
6.	$j = \emptyset$	2,5 $\forall$E
7.	$\overline{1} \leq \overline{1}$	T13.13m
8.	$Sj \leq \overline{1}$	6,7 =E
9.	$\overline{1} \not< Sj$	8 T13.13r
10.	$Pr(Sj)$	4 $\wedge$E
11.	$\overline{1} < Sj \wedge \forall d[d \mid Sj \rightarrow (d = \emptyset \vee Sd = Sj)]$	10 def
12.	$\overline{1} < Sj$	11 $\wedge$E
13.	$\bot$	9,12 $\bot$I
14.	$\bot$	3,4-13 $\exists$E
15.	$\sim\exists x[Pr(Sx) \wedge x \mid a \wedge x \mid b]$	3-14 $\sim$I
16.	$\sim\exists x[Pr(Sx) \wedge x \mid a \wedge x \mid b]$	A (g $\leftrightarrow$I)
17.	$\forall x[Pr(Sx) \rightarrow \sim(x \mid a \wedge x \mid b)]$	16 QN,DeM
18.	$j \mid a \wedge j \mid b$	A (g $\rightarrow$I)
19.	$j = \emptyset \vee j > \emptyset$	T13.13f
20.	$j > \emptyset$	A (c $\sim$I)
21.	$Sj > \overline{1}$	20 T13.13k
22.	$\exists z(Pr(Sz) \wedge z \mid Sj)$	21 T13.25d
23.	$Pr(Sk) \wedge k \mid Sj$	A (c 22$\exists$E)
24.	$k \mid Sj$	23 $\wedge$E
25.	$j \mid a$	18 $\wedge$E
26.	$k \mid Sj \wedge j \mid a$	24,25 $\wedge$I
27.	$k \mid a$	26 T13.24f
28.	$j \mid b$	18 $\wedge$E
29.	$k \mid Sj \wedge j \mid b$	26,28 $\wedge$E
30.	$k \mid b$	29 T13.24f
31.	$k \mid a \wedge k \mid b$	27,30 $\wedge$I
32.	$Pr(Sk)$	23 $\wedge$E
33.	$\sim(k \mid a \wedge k \mid b)$	17,32 $\forall$E
34.	$\bot$	31,33 $\bot$I
35.	$\bot$	22,23-34 $\exists$E
36.	$j \not> \emptyset$	20-35 $\sim$I
37.	$j = \emptyset$	19,36 DS
38.	$(j \mid a \wedge j \mid b) \rightarrow j = \emptyset$	18-37 $\rightarrow$I
39.	$\forall d[(d \mid a \wedge d \mid b) \rightarrow d = \emptyset]$	38 $\forall$I
40.	$Rp(a,b)$	39 def
41.	$Rp(a,b) \leftrightarrow \sim\exists x[Pr(Sx) \wedge x \mid a \wedge x \mid b]$	1-15,16-40 $\leftrightarrow$I

T13.25.f. PA $\vdash \forall x \forall y[G(a,b,x) \rightarrow G(a,b,x \times y)]$

With the assumptions $G(a,b,j)$ and then $au + j = bv$ for $\rightarrow$I and $\exists$E, you can show $auk + jk = bkv$ and generalize.

T13.25.g. PA $\vdash (a > \emptyset \wedge b > \emptyset) \rightarrow \forall x \forall y[(G(a,b,x) \wedge G(a,b,y) \wedge x \geq y) \rightarrow G(a,b,x \mathbin{\dot{-}} y)]$

1.	$a > \emptyset \wedge b > \emptyset$	A (g →I)
2.	$a > \emptyset$	1 ∧E
3.	$b > \emptyset$	1 ∧E
4.	$G(a,b,i) \wedge G(a,b,j) \wedge i \geq j$	A (g →I)
5.	$G(a,b,i)$	4 ∧E
6.	$\exists x \exists y(ax + i = by)$	5 def
7.	$G(a,b,j)$	4 ∧E
8.	$\exists x \exists y(ax + j = by)$	7 def
9.	$ap + i = bq$	A (g 6∃E)
10.	$ar + j = bs$	A (g 8∃E)
11.	$i \geq j$	4 ∧E
12.	$bar \geq ar$	3 T13.13z
13.	$abs \geq bs$	2 T13.13z
14.	$ap + i \geq i$	T13.13u
15.	$bq \geq i$	9,14 =E
16.	$bq \geq j$	11,15 T13.13a
17.	$bar + bq \geq ar + j$	12,16 T13.13x
18.	$bar + bq \geq bs$	10,17 =E
19.	$(bq + bar) + (bsa \mathbin{\dot{-}} bs) = (bq + bar) + (bsa \mathbin{\dot{-}} bs)$	=I
20.	$[bsa + (bq + bar)] \mathbin{\dot{-}} bs = (bq + bar) + (bsa \mathbin{\dot{-}} bs)$	13,19 T13.23l
21.	$[(bq + bar) \mathbin{\dot{-}} bs] + bsa = (bq + bar) + (bsa \mathbin{\dot{-}} bs)$	18,20 T13.23l
22.	$[(bq + bar) \mathbin{\dot{-}} (ar + j)] + bsa = (bq + bar) + (bsa \mathbin{\dot{-}} bs)$	10,21 =E
23.	$[((bq + bar) \mathbin{\dot{-}} j) \mathbin{\dot{-}} ar] + bsa = (bq + bar) + (bsa \mathbin{\dot{-}} bs)$	22 T13.23n
24.	$[((bq \mathbin{\dot{-}} j) + bar) \mathbin{\dot{-}} ar] + bsa = (bq + bar) + (bsa \mathbin{\dot{-}} bs)$	16,23 T13.23l
25.	$[(bar \mathbin{\dot{-}} ar) + (bq \mathbin{\dot{-}} j)] + bsa = (bq + bar) + (bsa \mathbin{\dot{-}} bs)$	12,24 T13.23l
26.	$[(bar \mathbin{\dot{-}} ar) + ((ap + i) \mathbin{\dot{-}} j)] + bsa = (bq + bar) + (bsa \mathbin{\dot{-}} bs)$	9,25 =E
27.	$[(bar \mathbin{\dot{-}} ar) + ((i \mathbin{\dot{-}} j) + ap] + bsa = (bq + bar) + (bsa \mathbin{\dot{-}} bs)$	11,26 T13.23l
28.	$(ap + abs) + (bar \mathbin{\dot{-}} ar) + (i \mathbin{\dot{-}} j) = (bq + bar) + (bsa \mathbin{\dot{-}} bs)$	27 assoc com
29.	$a(p + bs) + (bar \mathbin{\dot{-}} ar) + (i \mathbin{\dot{-}} j) = b(q + ar) + (bsa \mathbin{\dot{-}} bs)$	28 T6.63
30.	$a(p + bs) + a(br \mathbin{\dot{-}} r) + (i \mathbin{\dot{-}} j) = b(q + ar) + b(sa \mathbin{\dot{-}} s)$	29 T13.23p
31.	$a[(p + bs) + (br \mathbin{\dot{-}} r)] + (i \mathbin{\dot{-}} j) = b[(q + ar) + (sa \mathbin{\dot{-}} s)]$	30 T6.63
32.	$\exists x \exists y[ax + (i \mathbin{\dot{-}} j) = by]$	31 ∃I
33.	$G(a,b,i \mathbin{\dot{-}} j)$	32 def
34.	$G(a,b,i \mathbin{\dot{-}} j)$	8,10-33 ∃E
35.	$G(a,b,i \mathbin{\dot{-}} j)$	6,9-34 ∃E
36.	$[G(a,b,i) \wedge G(a,b,j) \wedge i \geq j] \rightarrow G(a,b,i \mathbin{\dot{-}} j)$	4-35 →I
37.	$\forall x \forall y([G(a,b,x) \wedge G(a,b,y) \wedge x \geq y] \rightarrow G(a,b,x \mathbin{\dot{-}} y))$	36 ∀I
38.	$(a > \emptyset \wedge b > \emptyset) \rightarrow \forall x \forall y([G(a,b,x) \wedge G(a,b,y) \wedge x \geq y] \rightarrow G(a,b,x \mathbin{\dot{-}} y))$	1-37 →I

T13.25.h. PA $\vdash [Rp(a,b) \wedge a > \overline{1} \wedge b > \overline{1}] \rightarrow \exists x \exists y(ax + \overline{1} = by)$

(a) Show $a \times (b \mathbin{\dot{-}} \overline{1}) + a = b \times a$ and generalize.

(b) Show $a \times \emptyset + b = b \times \overline{1}$ and generalize.

(c) Let $q = qt(i, d(a,b))$ and $r = rm(i, d(a,b))$.

c1.	$i = (Sd(a,b) \times q) + r$	def *qt*
c2.	$r < Sd(a,b)$	from def *rm*
c3.	$(\forall y < d(a,b)){\sim}[(a > \emptyset \wedge b > \emptyset) \rightarrow G(a,b,Sy)]$	1 $\wedge$E
c4.	$G(a,b,i)$	A ($g \rightarrow$I)
c5.	$G(a,b,Sd(a,b) \times q)$	7 T13.25f
c6.	$Sd(a,b) \times q \leq (Sd(a,b) \times q) + r$	T13.13u
c7.	$Sd(a,b) \times q \leq i$	c1,c6 =E
c8.	$\forall x \forall y[(G(a,b,x) \wedge G(a,b,y) \wedge x \geq y) \rightarrow G(a,b,x \dot{-} y)]$	6 T13.25g
c9.	$G(a,b,i \dot{-} (Sd(a,b) \times q))$	c4,c5,c7,c8 $\forall$E
c10.	$i = Sd(a,b) \times q + [i \dot{-} (Sd(a,b) \times q)]$	c7 T13.23a
c11.	$Sd(a,b) \times q + [i \dot{-} (Sd(a,b) \times q)] = (Sd(a,b) \times q) + r$	c1,c10 =E
c12.	$i \dot{-} (Sd(a,b) \times q) = r$	c11 T6.68
c13.	$G(a,b,r)$	c9,c11 =E
c14.	$\exists y(r = Sy)$	A (c ${\sim}$I)
c15.	$r = Sk$	A (c c14$\exists$E)
c16.	$Sk < Sd(a,b)$	c2,c16 =E
c17.	$k < d(a,b)$	c16 T13.13k
c18.	${\sim}[(a > \emptyset \wedge b > \emptyset) \rightarrow G(a,b,Sk)]$	c3,c17 ($\forall$E)
c19.	$(a > \emptyset \wedge b > \emptyset) \wedge {\sim}G(a,b,Sk)$	c18 Impl, Dem
c20.	${\sim}G(a,b,Sk)$	c19 $\wedge$E
c21.	${\sim}G(a,b,r)$	c20,c15 =E
c22.	$\bot$	c13,c21 $\bot$I
c23.	$\bot$	c14,c15-c22 $\exists$E
c24.	${\sim}\exists y(r = Sy)$	c14-c23 ${\sim}$I
c25.	$r = \emptyset$	c24 T6.45
c26.	$d(a,b) \mid i$	c25 T13.24j
c27.	$G(a,b,i) \rightarrow d(a,b) \mid i$	c4-c24 $\rightarrow$I
c28.	$\forall x[G(a,b,x) \rightarrow d(a,b) \mid x]$	c27 $\forall$I

T13.25.i. PA $\vdash Pr(Sa) \wedge a \mid (b \times c)] \rightarrow (a \mid b \vee a \mid c)$

1.	$Pr(Sa) \wedge a\vert(b \times c)$	A (g →I)
2.	$Pr(Sa)$	1 ∧E
3.	$\bar{1} < Sa \wedge \forall x[x\vert Sa \rightarrow (x = \emptyset \vee Sx = Sa)]$	2 def
4.	$\forall x[x\vert Sa \rightarrow (x = \emptyset \vee Sx = Sa)]$	3 ∧E
5.	$a\vert(b \times c)$	1 ∧E
6.	$a \nmid b$	A (g →I)
7.	$j\vert b \wedge j\vert Sa$	A (g →I)
8.	$j\vert Sa$	7 ∧E
9.	$j = \emptyset \vee Sj = Sa$	4,8 ∀E
10.	$Sj = Sa$	A (c ∼I)
11.	$j = a$	10 T6.40
12.	$j\vert b$	7 ∧E
13.	$a\vert b$	12,11 =E
14.	$\bot$	6,13 ⊥I
15.	$Sj \neq Sa$	10-14 ∼I
16.	$j = \emptyset$	9,15 DS
17.	$(j\vert b \wedge j\vert Sa) \rightarrow j = \emptyset$	7-16 →I
18.	$\forall x[(x\vert b \wedge x\vert Sa) \rightarrow x = \emptyset]$	17 ∀I
19.	$Rp(b, Sa)$	18 def
20.	$Sa > \emptyset$	T13.13e
21.	$b \not> \emptyset$	A (c ∼E)
22.	$b = \emptyset$	21 T13.13f
23.	$a\vert\emptyset$	T13.24c
24.	$a\vert b$	22,23 =E
25.	$\bot$	6,24 ⊥I
26.	$b > \emptyset$	21-25 ∼E
27.	$\exists x \exists y[bx + \bar{1} = Sa \times y]$	19,20,26 T13.25h
28.	$bp + \bar{1} = Sa \times q$	A (g 27∃E)
29.	$c(Sa \times q) = c(Sa \times q)$	=I
30.	$c(bp + \bar{1}) = c(Sa \times q)$	28,29 =E
31.	$cbp + c = c(Sa \times q)$	30 T6.63
32.	$a\vert cbp$	5 T13.24d
33.	$a\vert Sa$	T13.24b
34.	$a\vert c(Sa \times q)$	33 T13.24d
35.	$a\vert(cbp + c)$	31,34 =E
36.	$a\vert c$	32,35 T13.24g
37.	$a\vert c$	27,28-36 ∃E
38.	$a \nmid b \rightarrow a\vert c$	6-37 →I
39.	$a\vert b \vee a\vert c$	38 Impl
40.	$[Pr(Sa) \wedge a\vert(b \times c)] \rightarrow (a\vert b \vee a\vert c)$	1-39 →I

E13.17. Show the conditions for *Def*[*lcm*] and *Def*[*plm*]. Then show each of the results in T13.26.

Def[*lcm*].

Exercise 13.17 Def[*lcm*]

(i) PA $\vdash \exists x[x > \emptyset \wedge (\forall i < k)m(i)|x]$

Supposing the zero case is done.

1.	$\exists x[x > \emptyset \wedge (\forall i < \emptyset)m(i)\|x]$	zero case
2.	$\exists x[x > \emptyset \wedge (\forall i < j)m(i)\|x]$	A ($g \to$I)
3.	$a > \emptyset \wedge (\forall i < j)m(i)\|a$	A (g 2$\exists$E)
4.	$a > \emptyset$	3 $\wedge$E
5.	$(\forall i < j)m(i)\|a$	3 $\wedge$E
6.	$Sm(j) > \emptyset$	T13.13e
8.	$a \times Sm(j) \geq Sm(j)$	4 T13.13z
9.	$a \times Sm(j) > \emptyset$	6,8 T13.13c
10.	$l < Sj$	A (g ($\forall$I))
11.	$l < j \vee l = j$	10 T13.13n
12.	$l < j$	A (g 11$\vee$E)
13.	$m(l)\|a$	5,12 ($\forall$E)
14.	$m(l)\|(a \times Sm(j))$	13 T13.24d
15.	$l = j$	A (g 11$\vee$E)
16.	$m(j)\|Sm(j)$	T13.24b
17.	$m(l)\|Sm(j)$	16,15 =E
18.	$m(l)\|(a \times Sm(j))$	17 T13.24d
19.	$m(l)\|(a \times Sm(j))$	11,12-14,15-18 $\vee$E
20.	$(\forall i < Sj)m(i)\|(a \times Sm(j))$	10-19 ($\forall$I)
21.	$a \times Sm(j) > \emptyset \wedge (\forall i < Sj)m(i)\|(a \times Sm(j))$	9,20 $\wedge$I
22.	$\exists x[x > \emptyset \wedge (\forall i < Sj)m(i)\|x]$	21 $\exists$I
23.	$\exists x[x > \emptyset \wedge (\forall i < Sj)m(i)\|x]$	2,3-22 $\exists$E
24.	$\exists x[x > \emptyset \wedge (\forall i < j)m(i)\|x] \to \exists x[x > \emptyset \wedge (\forall i < Sj)m(i)\|x]$	2-23$\to$I
25.	$\forall y(\exists x[x > \emptyset \wedge (\forall i < y)m(i)\|x] \to \exists x[x > \emptyset \wedge (\forall i < Sy)m(i)\|x])$	24$\forall$I
26.	$\exists x[x > \emptyset \wedge (\forall i < k)m(i)\|x]$	1,25 IN

Def[*plm*]. These are straightforward.

T13.26.

T13.26.a. Show $\overline{1} > \emptyset \wedge (\forall i < \emptyset)m(i)|\overline{1} \wedge (\forall z < \overline{1}){\sim}[z > \emptyset \wedge (\forall i < \emptyset)m(i)|z]$ and apply the definition.

T13.26.b. This is straightforward.

T13.26.c. PA $\vdash (\forall i < k)m(i)|x \to p_k|x$

Let $q = qt(x, p_k)$ and $r = rm(x, p_k)$.

1.	$(\forall y < l_k)\sim[y > \emptyset \wedge (\forall i < k)m(i)\|y]$	def l_k T13.19c
2.	$Sp_k = l_k$	def p_k
3.	$x = (Sp_k \times q) + r$	def q
4.	$r < Sp_k$	from def r
5.	$(\forall i < k)m(i)\|x$	A (g $\rightarrow$I)
6.	$r < l_k$	4,2 =E
7.	$a < k$	A (g ($\forall$I))
8.	$m(a)\|x$	5,7 ($\forall$E)
9.	$m(a)\|((Sp_k \times q) + r)$	8,3 =E
10.	$m(a)\|l_k$	7 T13.26b
11.	$m(a)\|Sp_k$	2,10 =E
12.	$m(a)\|(Sp_k \times q)$	11 T13.24d
13.	$m(a)\|r$	9,12 T13.24g
14.	$(\forall i < k)m(i)\|r$	7-13 ($\forall$I)
15.	$\sim[r > \emptyset \wedge (\forall i < k)m(i)\|r]$	1,6 ($\forall$E)
16.	$r \not> \emptyset \vee \sim(\forall i < k)m(i)\|r$	15 DeM
17.	$r \not> \emptyset$	14,16 DS
18.	$r = \emptyset$	17 T13.13f
19.	$p_k\|x$	18 T13.24j
20.	$(\forall i < k)m(i)\|x \rightarrow p_k\|x$	5-19 $\rightarrow$I

T13.26.d. PA $\vdash \forall n[(Pr(Sn) \wedge n|l_k) \rightarrow (\exists i < k)n|Sm(i)]$

Supposing the zero case is done.

1.	$\forall n[(Pr(Sn) \wedge n \mid l_{\emptyset}) \rightarrow (\exists i < \emptyset)n \mid Sm(i)]$	zero case
2.	$l_j > \emptyset \wedge (\forall i < j)m(i) \mid l_j$	def l_j T13.19b
3.	$(\forall i < j)m(i) \mid l_j$	2 ∧E
4.	$\forall n[(Pr(Sn) \wedge n \mid l_j) \rightarrow (\exists i < j)n \mid Sm(i)]$	A (g →I)
5.	$Pr(Sa) \wedge a \mid l_{Sj}$	A (g →I)
6.	$Pr(Sa)$	5 ∧E
7.	$b < Sj$	A (g (∀I))
8.	$b < j \vee b = j$	7 T13.13n
9.	$b < j$	A (g 8∨E)
10.	$m(b) \mid l_j$	3,9 (∀E)
11.	$m(b) \mid (l_j \times Sm(j))$	10 T13.24d
12.	$b = j$	A (g 8∨E)
13.	$m(j) \mid Sm(j)$	T13.24b
14.	$m(b) \mid Sm(j)$	12,13 =E
15.	$m(b) \mid (l_j \times Sm(j))$	14 T13.24d
16.	$m(b) \mid (l_j \times Sm(j))$	8,9-11,12-15 ∨E
17.	$(\forall i < Sj)m(i) \mid (l_j \times Sm(j))$	7-16 (∀I)
18.	$p_{Sj} \mid (l_j \times Sm(j))$	17 T13.26c
19.	$Sp_{Sj} = l_{Sj}$	def p_{Sj}
20.	$a \mid l_{Sj}$	5 ∧E
21.	$a \mid Sp_{Sj}$	20,19 =E
22.	$a \mid (l_j \times Sm(j))$	21,18 T13.24f
23.	$a \mid l_j \vee a \mid Sm(j)$	6,22 T13.25i
24.	$j < Sj$	T13.13h
25.	$a \mid l_j$	A (g 23∨E)
26.	$Pr(Sa) \wedge a \mid l_j$	6,25 ∧I
27.	$(\exists i < j)a \mid Sm(i)$	4,26 ∀E
28.	$a \mid Sm(b)$	A (g 27(∃E))
29.	$b < j$	
30.	$b < Sj$	29,24 T13.13b
31.	$(\exists i < Sj)a \mid Sm(i)$	28,30 (∃I)
32.	$(\exists i < Sj)a \mid Sm(i)$	27,28-31 (∃E)
33.	$a \mid Sm(j)$	A (g 23∨E)
34.	$(\exists i < Sj)a \mid Sm(i)$	33,24 (∃I)
35.	$(\exists i < Sj)a \mid Sm(i)$	23,25-32,33-34 ∨E
36.	$(Pr(Sa) \wedge a \mid l_{Sj}) \rightarrow (\exists i < Sj)a \mid Sm(i)$	5-35 →I
37.	$\forall n[(Pr(Sn) \wedge n \mid l_{Sj}) \rightarrow (\exists i < Sj)n \mid Sm(i)]$	36 ∀I
38.	$\forall n[(Pr(Sn) \wedge n \mid l_j) \rightarrow (\exists i < j)n \mid Sm(i)] \rightarrow \forall n[(Pr(Sn) \wedge n \mid l_{Sj}) \rightarrow (\exists i < Sj)n \mid Sm(i)]$	4-37 →I
39.	$\forall y(\forall n[(Pr(Sn) \wedge n \mid l_y) \rightarrow (\exists i < y)n \mid Sm(i)] \rightarrow \forall n[(Pr(Sn) \wedge n \mid l_{Sy}) \rightarrow (\exists i < Sy)n \mid Sm(i)])$	38 ∀I
40.	$\forall n[(Pr(Sn) \wedge n \mid l_k) \rightarrow (\exists i < k)n \mid Sm(i)]$	1,39 IN

E13.18. Provide derivations to show each of [a] - [e] to complete the derivation for T13.27.

Exercise 13.18

T13.27.

a. PA $\vdash \emptyset \leq k \rightarrow (\mathcal{A}(\emptyset) \rightarrow \mathcal{B}(\emptyset))$

Trivially $(\forall i < \emptyset)rm(\emptyset, m(i)) = h(i)$; this gives you $\mathcal{B}(\emptyset)$ and (1) follows easily from this.

b. You will be able to use (10) and (11) to generate the antecedent to (8); (13) then follows by $\rightarrow$E.

c. PA, (11) $\vdash Rp(l_a, Sm(a))$

c1.	$\sim Rp(l_a, Sm(a))$	A (c $\sim$E)
c2.	$\exists x[Pr(Sx) \wedge x \mid l_a \wedge x \mid Sm(a)]$	c1, T13.25e
c3.	$Pr(Su) \wedge u \mid l_a \wedge u \mid Sm(a)$	A (c c2$\exists$E)
c4.	$u \mid Sm(a)$	c3 $\wedge$E
c5.	$Pr(Su)$	c3 $\wedge$E
c6.	$u \mid l_a$	c3 $\wedge$E
c7.	$Pr(Su) \wedge u \mid l_a$	c5,c6 $\wedge$I
c8.	$(\exists i < a)u \mid Sm(i)$	c7 T13.26d
c9.	$u \mid Sm(v)$	A (c c8($\exists$E))
c10.	$v < a$	
c11.	$a < Sa$	T13.13n
c12.	$v < a \wedge a < Sa$	c10,c11 $\wedge$I
c13.	$(v < a \wedge a < Sa) \rightarrow Rp(Sm(v), Sm(a))$	11 $\forall$E
c14.	$Rp(Sm(v), Sm(a))$	c13,c12 $\rightarrow$E
c15.	$Pr(Su) \wedge u \mid Sm(v) \wedge u \mid Sm(a)$	c5,c9,c4 $\wedge$I
c16.	$\exists x[Pr(Sx) \wedge x \mid Sm(v) \wedge x \mid Sm(a)]$	c15 $\exists$I
c17.	$\sim Rp(Sm(v), Sm(a))$	c16 T13.25e
c18.	$\bot$	c14,c17 $\bot$I
c19.	$\bot$	c8,c9-c18 ($\exists$E)
c20.	$\bot$	c2,c3-c19 $\exists$E
c21.	$Rp(l_a, Sm(a))$	c1-c20 $\sim$E

d. PA, (20), (21) $\vdash s = Sm(a) \times c + h(a)$

d1.	$s = (l_a b + r) + h(a)l_a$	21 T6.63
d2.	$l_a > \emptyset$	def l_a
d3.	$h(a)l_a \geq h(a)$	d2 T13.13z
d4.	$h(a)l_a = h(a) + [h(a)l_a \dot{-} h(a)]$	d3 T13.23a
d5.	$h(a)l_a = h(a) + [h(a)l_a \dot{-} h(a)\overline{1}]$	d4 T6.57
d6.	$h(a)l_a = h(a) + h(a)[l_a \dot{-} \overline{1}]$	d5 T13.23p
d7.	$s = (l_a b + r) + (h(a) + h(a)[l_a \dot{-} \overline{1}])$	d1,d6 =E
d8.	$s = [l_a b + (r + [l_a \dot{-} \overline{1}]h(a))] + h(a)$	d7 T6.55
d9.	$s = Sm(a)c + h(a)$	20,d8 =E

e. PA, (10), (13), (21), (22) $\vdash (\forall i < Sa)rm(s, m(i)) = h(i)$

e1.	$u < Sa$	A (g ($\forall$I))
e2.	$u < a \vee u = a$	e1 T13.13n
e3.	$u < a$	A (g e2$\vee$E)
e4.	$m(u) \mid l_a$	e3 T13.26b
e5.	$m(u) \mid l_a(b + h(a))$	e4 T13.24d
e6.	$\exists q[Sm(u)q = l_a(b + h(a))]$	def $\mid$
e7.	$Sm(u)v = l_a(b + h(a))$	A (g e6$\exists$E)
e8.	$rm(s, m(u)) = rm(s, m(u))$	=I
e9.	$rm(s, m(u)) = rm(l_a(b + h(a)) + r, m(u))$	e8,21 =E
e10.	$rm(s, m(u)) = rm(Sm(u)v + r, m(u))$	e9,e7 =E
e11.	$rm(s, m(u)) = rm(r, m(u))$	e10 T13.24k
e12.	$rm(r, (m(u)) = h(u)$	13,e3 ($\forall$E)
e13.	$rm(s, m(u)) = h(u)$	e11,e12 =E
e14.	$rm(s, m(u)) = h(u)$	e6,e7-e13 $\exists$E
e15.	$u = a$	A (g e2$\vee$E)
e16.	$rm(s, m(u)) = rm(s, m(u))$	=I
e17.	$rm(s, m(u)) = rm(Sm(a)c + h(a), m(u))$	e16,22 =E
e18.	$rm(s, m(u)) = rm(Sm(u)c + h(u), m(u))$	e15,e17 =E
e19.	$rm(s, m(u)) = rm(h(u), m(u))$	e18 T13.24k
e20.	$a < Sa$	T13.13h
e21.	$u < Sa$	e20,e15 =E
e22.	$m(u) \geq h(u)$	10,e21 ($\forall$E)
e23.	$h(u) < Sm(u)$	e22 T13.13m,n
e24.	$Sm(u) \times \emptyset = \emptyset$	T6.43
e25.	$\emptyset + h(u) = h(u)$	T6.51
e26.	$h(u) = Sm(u) \times \emptyset + h(u)$	e25,e24 =E
e27.	$h(u) = Sm(u) \times \emptyset + h(u) \wedge h(u) < Sm(u)$	e26,e23 $\wedge$I
e28.	$\exists w[h(u) = Sm(u) \times w + h(u) \wedge h(u) < Sm(u)$	e26 $\exists$I
e29.	$rm(h(u), m(u)) = h(u)$	e28 def rm
e30.	$rm(s, m(u)) = h(u)$	e19,e29 =E
e31.	$rm(s, m(u)) = h(u)$	e2,e3-e14,e15-e30 $\vee$E
e32.	$(\forall i < Sa)rm(s, m(i)) = h(i)$	e1-e31 ($\forall$I)

E13.20. Complete the demonstration for T13.29.

T13.29.

(i)

1.	$j < k$	A (g (∀I))
2.	$Sj > \emptyset$	T13.13e
3.	$q \times Sj \geq q$	2 T13.13z
4.	$q > \emptyset$	def q
5.	$q \times Sj > \emptyset$	3,4 T13.13c
6.	$m(j) > \emptyset$	5 def m
7.	$maxp(k, maxs[h]_k) \geq maxs[h]_k$	T13.28a
8.	$r \geq maxs[h]_k$	7 def r
9.	$(\forall i < k)h(i) \leq maxs[h]_k$	T13.28b
10.	$h(j) \leq maxs[h]_k$	9,1 (∀E)
11.	$h(j) \leq r$	8,10 T13.13a
12.	$r < Sr$	T13.13h
13.	$Sr = s$	def s
14.	$r < s$	12,13 =E
15.	$h(j) < s$	11,14 T13.13c
16.	$r \vert q$	14 T13.26b
17.	$\exists v[Sr \times v = q]$	def |
18.	$Sr \times a = q$	A (g 17∃E)
19.	$s \times a = q$	13,18 =E
20.	$a = \emptyset \vee a > \emptyset$	T13.13f
21.	$a = \emptyset$	A (c ∼I)
22.	$s \times \emptyset = \emptyset$	T6.43
23.	$s \times a = \emptyset$	22,21 =E
24.	$q = \emptyset$	19,23 =E
25.	$q \neq \emptyset$	4 T13.13f
26.	$\bot$	24,25 ⊥I
27.	$a \neq \emptyset$	21-26 ∼I
28.	$a > \emptyset$	20,27 DS
29.	$s \times a \geq s$	28 T13.13z
30.	$s \leq q$	19,29 =E
31.	$q \times Sj \geq s$	30,3 T13.13a
32.	$q \times Sj > h(j)$	15,31 T13.13c
33.	$m(j) > h(j)$	32 def m
34.	$m(j) \geq h(j)$	33 T13.13m
35.	$m(j) \geq h(j)$	17,18-34 ∃E
36.	$m(j) > \emptyset \wedge m(j) \geq h(j)$	6,35 ∧I
37.	$(\forall i < k)(m(i) > \emptyset \wedge m(i) \geq h(i))$	1-36 (∀I)

(ii) (a)

a1.	$i \leq j$	2 T13.13m
a2.	$Si \leq Sj$	a1 T13.13j
a3.	$q \times Si \leq q \times Sj$	a2 T13.13aa
a4.	$S(q \times Si) \leq S(q \times Sj)$	a3 T13.13j
a5.	$a \mid (S(q \times Sj) \dot{-} S(q \times Si))$	a4,8,9 T13.24h
a6.	$S(q \times Sj) \dot{-} S(q \times Si) = S(q \times Sj) \dot{-} S(q \times Si)$	=I
a7.	$S(q \times Sj) = (q \times Sj) + \overline{1}$	T6.47
a8.	$S(q \times Si) = (q \times Si) + \overline{1}$	T6.47
a9.	$S(q \times Sj) \dot{-} S(q \times Si) = [(q \times Sj) + \overline{1}] \dot{-} [(q \times Si) + \overline{1}]$	a6,a7,a8 =E
a10.	$[(q \times Sj) + \overline{1}] \dot{-} [(q \times Si) + \overline{1}] = (q \times Sj) \dot{-} (q \times Si)$	T13.23o
a11.	$(q \times Sj) \dot{-} (q \times Si) = q(Sj \dot{-} Si)$	T13.23p
a12.	$q(Sj \dot{-} Si) = q(Sj \dot{-} Si)$	=I
a13.	$Sj = j + \overline{1}$	T6.47
a14.	$Si = i + \overline{1}$	T6.47
a15.	$q(Sj \dot{-} Si) = q((j + \overline{1}) \dot{-} (i + \overline{1}))$	a12,a13 =E
a16.	$(j + \overline{1}) \dot{-} (i \dot{-} \overline{1}) = j \dot{-} i$	T13.23o
a17.	$q(Sj \dot{-} Si) = q(j \dot{-} i)$	a14,a15 =E
a18.	$S(q \times Sj) \dot{-} S(q \times Si) = q(j \dot{-} i)$	a6,a9,a10,a11,a17 =E
a19.	$a \mid q(j \dot{-} i)$	a5,a18 =E

(b)

b1.	$j \dot{-} i > \emptyset$	2 T13.23f
b2.	$\exists v[j \dot{-} i = Sv]$	b1 T13.13g
b3.	$j \dot{-} i = Sl$	A (g b2∃E)
b4.	$a \mid Sl$	14,b3 =E
b5.	$j \dot{-} i \leq j$	T13.23c
b6.	$j \dot{-} i < k$	b5,3 T13.13c
b7.	$maxp(k, maxs[h]_k) \geq k$	T13.28a
b8.	$Sr > r$	T13.13h
b9.	$k < s$	b7,b8 T13.13c
b10.	$j \dot{-} i < s$	b6,b9 T13.13b
b11.	$Sl < s$	b3,b10 =E
b12.	$l < Sl$	T13.13h
b13.	$l < s$	b11,b12 T13.13b
b14.	$l \mid q$	b13 T13.26b
b15.	$a \mid q$	b4,b14 T13.24f
b16.	$a \mid q$	b2,b3-b15 ∃E

E13.21. Show the conditions for *Def*$[h(i)]$ and then show T13.30.

Def$[h(i)]$. (i) is straightforward under $i < k \vee i \geq k$ from T13.13q. And (ii) is also straightforward.

T13.30.

1.	$(k < k \wedge h(k) = \beta(a,b,k)) \vee (k \geq k \wedge h(k) = n)$	def h
2.	$(l < k \wedge h(l) = \beta(a,b,l)) \vee (l \geq k \wedge h(l) = n)$	def h
3.	$\exists p \exists q(\forall i < Sk)\beta(p,q,i) = h(i)$	T13.29
4.	$(\forall i < Sk)\beta(c,d,i) = h(i)$	A (g 3$\exists$E)
5.	$k < Sk$	T13.13h
6.	$\beta(c,d,k) = h(k)$	4,5 ($\forall$E)
7.	$k \leq k$	T13.13m
8.	$k \not< k$	7 T13.13r
9.	$k \not< k \vee h(k) \neq \beta(a,b,k)$	8 $\vee$I
10.	$\sim(k < k \wedge h(k) = \beta(a,b,k))$	9 DeM
11.	$k \geq k \wedge h(k) = n$	1,10 DS
12.	$h(k) = n$	11 $\wedge$E
13.	$\beta(c,d,k) = n$	6,12 =E
14.	$l < k$	A (g ($\forall$I))
15.	$l < Sk$	14,5 T13.13b
16.	$\beta(c,d,l) = h(l)$	4,15 ($\forall$E)
17.	$l \not\geq k$	14 T13.13r
18.	$l \not\geq k \vee h(l) \neq n$	17 $\vee$I
19.	$\sim(l \geq k \wedge h(l) = n)$	18 DeM
20.	$l < k \wedge h(l) = \beta(a,b,l)$	2,19 DS
21.	$h(l) = \beta(a,b,l)$	20 $\wedge$E
22.	$\beta(c,d,l) = \beta(a,b,l)$	16,21 =E
23.	$(\forall i < k)\beta(c,d,i) = \beta(a,b,i)$	14-22 ($\forall$I)
24.	$(\forall i < k)\beta(c,d,i) = \beta(a,b,i) \wedge \beta(c,d,k) = n$	23,13 $\wedge$I
25.	$\exists p \exists q[(\forall i < k)\beta(p,q,i) = \beta(a,b,i) \wedge \beta(p,q,k) = n]$	24 $\exists$I
26.	$\exists p \exists q[(\forall i < k)\beta(p,q,i) = \beta(a,b,i) \wedge \beta(p,q,k) = n]$	3,4-25 $\exists$E

E13.22. Complete the demonstration of T13.31 by showing the zero case.

T13.31. Apply T13.29 with $h(i) = g(x)$ to get $\exists p \exists q(\forall i < \overline{1})\beta(p,q,i) = g(\vec{x})$; then under an assumption for $\exists$E, with $\emptyset < \overline{1}$ the result easily follows.

E13.26. Demonstrate each of the results in T13.37.

T13.37.

T13.37.b. PA $\vdash$ $subc(x,y) = x \dot{-} y$

1.	$\mathbb{g}subc(x) = \mathbb{i}dnt^1_1(x)$	def from subc, T13.34
2.	$\mathbb{s}ubc(x, \emptyset) = \mathbb{g}subc(x)$	T13.34
3.	$\mathbb{g}subc(x) = x$	1 with T13.35c
4.	$\mathbb{s}ubc(x, \emptyset) = x$	2,3 =E
5.	$x \dot{-} \emptyset = x$	T13.23g
6.	$\mathbb{s}ubc(x, \emptyset) = x \dot{-} \emptyset$	4,5 =E
7.	$\mathbb{s}ubc(x, j) = x \dot{-} j$	A (g (→I)
8.	$\mathbb{s}ubc(x, Sj) = \mathbb{h}subc(x, j, \mathbb{s}ubc(x, j))$	T13.34
9.	$\mathbb{h}subc(x, j, u) = \mathbb{p}red(\mathbb{i}dnt^3_3(x, j, u))$	def from subc, T13.34
10.	$\mathbb{h}subc(x, j, u) = pred(u)$	9 with T13.35c,T13.37a
11.	$\mathbb{h}subc(x, j, \mathbb{s}ubc(x, j)) = pred(\mathbb{s}ubc(x, j))$	10 ∀E
12.	$\mathbb{s}ubc(x, Sj) = pred(\mathbb{s}ubc(x, j))$	8,11 =E
13.	$\mathbb{s}ubc(x, Sj) = pred(x \dot{-} j)$	7,12 =E
14.	$x \leq j \vee x > j$	T13.13q
15.	$x \leq j$	A (g 14∨E)
16.	$x \leq Sj$	15 T13.13o
17.	$x \dot{-} Sj = \emptyset$	16 T13.23b
18.	$x \dot{-} j = \emptyset$	15 T13.23b
19.	$pred(\emptyset) = \emptyset$	T13.36a
20.	$pred(x \dot{-} j) = \emptyset$	18,19 =E
21.	$pred(x \dot{-} j) = x \dot{-} Sj$	20,17 =E
22.	$x > j$	A (g 14∨E)
23.	$x \geq Sj$	T13.13l
24.	$x = Sj + (x \dot{-} Sj)$	23 13.23a
25.	$x \geq j$	22 T13.13m
26.	$x = j + (x \dot{-} j)$	25 13.23a
27.	$Sj + (x \dot{-} Sj) = j + (x \dot{-} j)$	24,26 =E
28.	$j + [S\emptyset + (x \dot{-} Sj)] = j + (x \dot{-} j)$	27 with T6.47
29.	$S\emptyset + (x \dot{-} Sj) = x \dot{-} j$	28 T6.68
30.	$S\emptyset + (x \dot{-} Sj) = S[\emptyset + (x \dot{-} Sj)]$	T6.53
31.	$S[\emptyset + (x \dot{-} Sj)] = x \dot{-} j$	29,30 =E
32.	$\emptyset + (x \dot{-} Sj) = x \dot{-} Sj$	T6.51
33.	$S(x \dot{-} Sj) = x \dot{-} j$	31,32 =E
34.	$x \dot{-} j > \emptyset$	22 T13.23f
35.	$Spred(x \dot{-} j) = x \dot{-} j$	34 T13.36a
36.	$S(x \dot{-} Sj) = Spred(x \dot{-} j)$	33,35 =E
37.	$x \dot{-} Sj = pred(x \dot{-} j)$	36 T6.40
38.	$x \dot{-} Sj = pred(x \dot{-} j)$	14,15-21,22-37 ∨E
39.	$\mathbb{s}ubc(x, Sj) = x \dot{-} Sj$	13,38 =E
40.	$[\mathbb{s}ubc(x, j) = x \dot{-} j] \to [\mathbb{s}ubc(x, Sj) = x \dot{-} Sj]$	7-39 →I
41.	$\forall y([\mathbb{s}ubc(x, y) = x \dot{-} y] \to [\mathbb{s}ubc(x, Sy) = x \dot{-} Sy])$	40 ∀I
42.	$\mathbb{s}ubc(x, y) = x \dot{-} y$	6,41 IN

T13.37.f. PA $\vdash \mathbb{E}q(x, y) \leftrightarrow x = y$

1.	$\mathbb{E}q(x,y) \leftrightarrow \mathbb{s}g(\mathbb{a}bsval(x - y)) = \emptyset$	def from EQ, T13.34
2.	$\mathbb{E}q(x,y) \leftrightarrow sg[(x \dot{-} y) + (y \dot{-} x)] = \emptyset$	1 with T13.37d,c
3.	$\mathbb{E}q(x,y) \leftrightarrow [(x \dot{-} y) + (y \dot{-} x)] = \emptyset$	2 T13.36e
4.	$\mathbb{E}q(x,y)$	A (g ↔I)
5.	$[(x \dot{-} y) + (y \dot{-} x)] = \emptyset$	3,4 ↔E
6.	$x \geq y \vee x < y$	T13.13q
7.	$x \geq y$	A (g 6∨E)
8.	$y \dot{-} x = \emptyset$	7 T13.23b
9.	$(x \dot{-} y) + \emptyset = \emptyset$	5,8 =E
10.	$\emptyset + \emptyset = \emptyset$	T6.41
11.	$(x \dot{-} y) + \emptyset = \emptyset + \emptyset$	9,10 =E
12.	$x \dot{-} y = \emptyset$	11 T6.68
13.	$x = y + (x \dot{-} y)$	7 T13.23a
14.	$x = y + \emptyset$	12,13 =E
15.	$y + \emptyset = y$	T6.41
16.	$x = y$	14,15 =E
17.	$x < y$	A (g 6∨E)
18.	$y \geq x$	17 T13.13m
19.	$x = y$	similarly
20.	$x = y$	6,7-17,18-19 ∨E
21.	$x = y$	A (g ↔I)
22.	$y \geq x$	21 T13.13m
23.	$x \dot{-} y = \emptyset$	22 T13.23b
24.	$x \geq y$	21 T13.13m
25.	$y \dot{-} x = \emptyset$	24 T13.23b
26.	$\emptyset + \emptyset = \emptyset$	T6.41
27.	$[(x \dot{-} y) + (y \dot{-} x)] = \emptyset$	26,23,25 =E
28.	$\mathbb{E}q(x,y)$	3,27 ↔E
29 .	$\mathbb{E}q(x,y) \leftrightarrow x = y$	4-20,21-28 ↔I

T13.37.i. PA $\vdash \mathbb{N}eg(\mathbb{P}(\vec{x})) \leftrightarrow \sim\mathbb{P}(\vec{x})$

1.	$\mathbb{P}(\vec{x}) \leftrightarrow \mathbb{c}h_{\mathsf{P}}(\vec{x}) = \emptyset$	T13.32
2.	$\mathbb{N}eg(\mathbb{P}(\vec{x})) \leftrightarrow \mathbb{c}sg(\mathbb{c}h_{\mathsf{P}}(\vec{x})) = \emptyset$	def from NEG, T13.34
3.	$\mathbb{N}eg(\mathbb{P}(\vec{x})) \leftrightarrow csg(\mathbb{c}h_{\mathsf{P}}(\vec{x})) = \emptyset$	2 T13.37e
4.	$\mathbb{N}eg(\mathbb{P}(\vec{x}))$	A (g ↔I)
5.	$csg(\mathbb{c}h_{\mathsf{P}}(\vec{x})) = \emptyset$	3,4 ↔E
6.	$\mathbb{c}h_{\mathsf{P}}(\vec{x}) > \emptyset$	5 T13.36h
7.	$\mathbb{c}h_{\mathsf{P}}(\vec{x}) \neq \emptyset$	6 T13.13f
8.	$\sim\mathbb{P}(\vec{x})$	1,7 NB
9.	$\sim\mathbb{P}(\vec{x})$	A (g ↔I)
10.	$\mathbb{c}h_{\mathsf{P}}(\vec{x}) \neq \emptyset$	1,9 NB
11.	$\mathbb{c}h_{\mathsf{P}}(\vec{x}) > \emptyset$	10 T13.13f
12.	$csg(\mathbb{c}h_{\mathsf{P}}(\vec{x})) = \emptyset$	11 T13.36h
13.	$\mathbb{N}eg(\mathbb{P}(\vec{x}))$	3,12 ↔E
14.	$\mathbb{N}eg(\mathbb{P}(\vec{x})) \leftrightarrow \sim\mathbb{P}(\vec{x})$	4-8,9-13 ↔I

E13.27. Demonstrate each of the results in T13.39.

T13.39.

T13.39.a. PA $\vdash (\exists y \leq z)\mathbb{P}(\vec{x}, z, y) \leftrightarrow (\exists y \leq z)\mathbb{P}(\vec{x}, y, z)$

1.	$\mathbb{P}(\vec{x}, z, y) \leftrightarrow \mathbb{c}h_{\mathsf{P}}(\vec{x}, z, y) = \emptyset$	T13.32
2.	$\mathbb{c}h_{\mathsf{R}}(\vec{x}, z, \emptyset) = \mathbb{g}ch_{\mathsf{R}}(\vec{x}, z)$	T13.34
3.	$\mathbb{g}ch_{\mathsf{R}}(\vec{x}, z) = \mathbb{c}h_{\mathsf{P}}(\vec{x}, z, \emptyset)$	def from ELEQ, T13.34
4.	$\mathbb{c}h_{\mathsf{R}}(\vec{x}, z, \emptyset) = \mathbb{c}h_{\mathsf{P}}(\vec{x}, z, \emptyset)$	2,3 =E
5.	$\mathbb{c}h_{\mathsf{R}}(\vec{x}, z, \emptyset) = \emptyset$	A (g ↔I)
6.	$\mathbb{c}h_{\mathsf{P}}(\vec{x}, z, \emptyset) = \emptyset$	4,5 =E
7.	$\mathbb{P}(\vec{x}, z, \emptyset)$	1,6 ∀E, ↔E
8.	$\emptyset \leq \emptyset$	T13.13m
9.	$(\exists y \leq \emptyset)\mathbb{P}(\vec{x}, z, y)$	7,8 (∃I)
10.	$(\exists y \leq \emptyset)\mathbb{P}(\vec{x}, z, y)$	A (g ↔I)
11.	$\mathbb{P}(\vec{x}, z, j)$	A (g 10(∃E))
12.	$j \leq \emptyset$	
13.	$j = \emptyset$	12 T13.13m, T6.49
14.	$\mathbb{P}(\vec{x}, z, \emptyset)$	11,13 =E
15.	$\mathbb{c}h_{\mathsf{P}}(\vec{x}, z, \emptyset) = \emptyset$	1,14 ∀E, ↔E
16.	$\mathbb{c}h_{\mathsf{R}}(\vec{x}, z, \emptyset) = \emptyset$	4,15 =E
17.	$\mathbb{c}h_{\mathsf{R}}(\vec{x}, z, \emptyset) = \emptyset$	10,11-16 (∃E)
18.	$\mathbb{c}h_{\mathsf{R}}(\vec{x}, z, \emptyset) = \emptyset \leftrightarrow (\exists y \leq \emptyset)\mathbb{P}(\vec{x}, z, y)$	5-9,10-17 ↔I

1.	$ch_R(\vec{x}, z, \emptyset) = \emptyset \leftrightarrow (\exists y \le \emptyset)\mathbb{P}(\vec{x}, z, y)$	zero case
2.	$\mathbb{P}(\vec{x}, z, y) \leftrightarrow ch_P(\vec{x}, z, y) = \emptyset$	T13.32
3.	$ch_R(\vec{x}, z, Sj) = hch_R(\vec{x}, z, j, ch_R(x, z, j))$	T13.34
4.	$hch_R(\vec{x}, z, j, u) = times[u, ch_P(\vec{x}, z, suc(j))]$	def from ELEQ, T13.34
5.	$hch_R(\vec{x}, z, j, u) = u \times ch_P(\vec{x}, z, Sj)$	4 T13.35a,e
6.	$hch_R(\vec{x}, z, j, ch_R(x, z, j)) = ch_R(x, z, j) \times ch_P(\vec{x}, z, Sj)$	5 ∀E
7.	$ch_R(\vec{x}, z, Sj) = ch_R(x, z, j) \times ch_P(\vec{x}, z, Sj)$	3,6 =E
8.	$ch_R(\vec{x}, z, j) = \emptyset \leftrightarrow (\exists y \le j)\mathbb{P}(\vec{x}, z, y)$	A (g →I)
9.	$ch_R(\vec{x}, z, Sj) = \emptyset$	A (g ↔I)
10.	$ch_R(x, z, j) \times ch_P(\vec{x}, z, Sj) = \emptyset$	7,9 =E
11.	$ch_R(x, z, j) = \emptyset \vee ch_R(x, z, j) > \emptyset$	T13.13f
12.	$ch_R(x, z, j) = \emptyset$	A (g 11∨E)
13.	$(\exists y \le j)\mathbb{P}(\vec{x}, z, y)$	8,12 ↔E
14.	$\mathbb{P}(\vec{x}, z, a)$	A (g 13(∃E))
15.	$a \le j$	
16.	$a \le Sj$	15 T13.13o
17.	$(\exists y \le Sj)\mathbb{P}(\vec{x}, z, y)$	14,16 (∃I)
18.	$(\exists y \le Sj)\mathbb{P}(\vec{x}, z, y)$	13,14-17 (∃E)
19.	$ch_R(x, z, j) > \emptyset$	A (g 11∨E)
20.	$ch_R(x, z, j) \ne \emptyset$	19 T13.13f
22.	$ch_R(x, z, j) \times \emptyset = \emptyset$	T6.43
23.	$ch_R(x, z, j) \times ch_P(\vec{x}, z, Sj) = ch_R(x, z, j) \times \emptyset$	10,22 =E
24.	$ch_P(\vec{x}, z, Sj) = \emptyset$	23,20 T6.69
25.	$\mathbb{P}(\vec{x}, z, Sj)$	2,24 ∀E,↔E
26.	$Sj \le Sj$	T13.13m
27.	$(\exists y \le Sj)\mathbb{P}(\vec{x}, z, y)$	15,26 (∃I)
28.	$(\exists y \le Sj)\mathbb{P}(\vec{x}, z, y)$	11,12-18,19-27 ∨E
29.	$(\exists y \le Sj)\mathbb{P}(\vec{x}, z, y)$	A (g ↔I)
30.	$\mathbb{P}(\vec{x}, z, a)$	A (g 29(∃E))
31.	$a \le Sj$	
32.	$a \le j \vee a = Sj$	31 T13.13o
33.	$a \le j$	A (g 32∨E)
34.	$(\exists y \le j)\mathbb{P}(\vec{x}, z, y)$	30,33 (∃I)
35.	$ch_R(\vec{x}, z, j) = \emptyset$	8,34 ↔E
36.	$ch_R(\vec{x}, z, j) \times ch_P(\vec{x}, z, Sj) = \emptyset$	35 T6.58
37.	$ch_R(\vec{x}, z, Sj) = \emptyset$	7,36 =E
38.	$a = Sj$	A (g 32∨E)
39.	$\mathbb{P}(\vec{x}, z, Sj)$	30,38 =E
40.	$ch_P(\vec{x}, z, Sj) = \emptyset$	2,39 ∀E, ↔E
41.	$ch_R(\vec{x}, z, j) \times ch_P(\vec{x}, z, Sj) = \emptyset$	40 T6.58
42.	$ch_R(\vec{x}, z, Sj) = \emptyset$	7,41 =E
43.	$ch_R(\vec{x}, z, Sj) = \emptyset$	32,33-37,38-42 ∨E
44.	$ch_R(\vec{x}, z, Sj) = \emptyset$	29,30-43 (∃E)
45.	$ch_R(\vec{x}, z, Sj) = \emptyset \leftrightarrow (\exists y \le Sj)\mathbb{P}(\vec{x}, z, y)$	9-28,29-44 ↔I
46.	$[ch_R(\vec{x}, z, j) = \emptyset \leftrightarrow (\exists y \le j)\mathbb{P}(\vec{x}, z, y)] \to [ch_R(\vec{x}, z, Sj) = \emptyset \leftrightarrow (\exists y \le Sj)\mathbb{P}(\vec{x}, z, y)]$	8-45 →I
47.	$\forall w([ch_R(\vec{x}, z, w) = \emptyset \leftrightarrow (\exists y \le w)\mathbb{P}(\vec{x}, z, y)] \to [ch_R(\vec{x}, z, Sw) = \emptyset \leftrightarrow (\exists y \le Sw)\mathbb{P}(\vec{x}, z, y)])$	46 ∀I
48.	$ch_R(\vec{x}, z, n) = \emptyset \leftrightarrow (\exists y \le n)\mathbb{P}(\vec{x}, z, y)$	1,47 IN

Exercise 13.27 T13.39.a

1.	$ch_{R}(\vec{x},z,n)=\emptyset \leftrightarrow (\exists y \le n)\mathbb{P}(\vec{x},z,y)$	from above
2.	$ch_{S}(\vec{x},z)=ch_{R}(\vec{x},z,z)$	def from ELEQ, T13.34
3.	$\mathbb{S}(\vec{x},z) \leftrightarrow ch_{S}(\vec{x},z)=\emptyset$	T13.32
4.	$ch_{R}(\vec{x},z,z)=\emptyset \leftrightarrow (\exists y \le z)\mathbb{P}(\vec{x},z,y)$	1 ∀E
5.	$ch_{S}(\vec{x},z)=\emptyset \leftrightarrow (\exists y \le z)\mathbb{P}(\vec{x},z,y)$	2,4 =E
6.	$\mathbb{S}(\vec{x},z) \leftrightarrow (\exists y \le z)\mathbb{P}(\vec{x},z,y)$	from 3,5
7.	$(\exists y \le z)\mathbb{P}(\vec{x},z,y) \leftrightarrow (\exists y \le z)\mathbb{P}(\vec{x},y,z)$	6 abv

T13.39.e. PA ⊢ $(\mu y \le z)\mathbb{P}(\vec{x},z,y) \leftrightarrow (\mu y \le z)\mathbb{P}(\vec{x},z,y)$

(a)

a1.	$q(\vec{x},z,\emptyset)=gq(\vec{x},z)$	T13.33a
a2.	$gq(\vec{x},z)=zero(ch_{R}(\vec{x},z,\emptyset))$	def from least, T13.34
a3.	$gq(\vec{x},z)=\emptyset$	a2 T13.35b
a4.	$q(\vec{x},z,\emptyset)=\emptyset$	a1,a3 =E
a5.	$(\mu y \le \emptyset)\mathbb{P}(\vec{x},z,y)=\emptyset$	T13.20a
a6.	$q(\vec{x},z,\emptyset)=(\mu y \le \emptyset)\mathbb{P}(\vec{x},z,y)$	a4,a5 =E

(b)

b1.	$k \le j$	A (g (∀I))
b2.	$k < j \vee k = j$	b1 T13.13m
b3.	$k < j$	A (g b2∨E)
b4.	$k < a$	b3,17 =E
b5.	$\sim\mathbb{P}(\vec{x},z,k)$	15,b4 (∀E)
b6.	$k = j$	A (g b2∨E)
b7.	$\sim\mathbb{P}(\vec{x},z,k)$	19,b6 =E
b8.	$\sim\mathbb{P}(\vec{x},z,k)$	b2,b3-b5,b6-b7 ∨E
b9.	$(\forall y \le j)\sim\mathbb{P}(\vec{x},z,y)$	b1-b8 (∀I)
b10.	$\sim(\exists y \le j)\mathbb{P}(\vec{x},z,y)$	b9 (QN)
b11.	$ch_{R}(\vec{x},z,j) \ne \emptyset$	3,b10 NB
b12.	$ch_{R}(\vec{x},z,j)=\bar{1}$	2,b11 DS
b13.	$b = a + \bar{1}$	12,b12 =E
b14.	$b = Sa$	b13 T6.47
b15.	$b = Sj$	b14,17 =E
b16.	$b = Sj \vee P(\vec{x},z,b)$	b15 ∨I
b17.	$k < b$	A (g (∀I))
b18.	$k < Sj$	b17,b15 =E
b19.	$k \ne Sj$	b18 T13.13s
b20.	$k < j \vee k = j$	b18 T13.13.m
b21.	$k < j$	A (g b20∨E)
b22.	$k < a$	b21,17 =E
b23.	$\sim\mathbb{P}(\vec{x},z,k)$	15,b22 (∀E)
b24.	$k = j$	A (g b20∨E)
b25.	$\sim\mathbb{P}(\vec{x},z,k)$	19,b24 =E
b26.	$\sim\mathbb{P}(\vec{x},z,k)$	b20,b21-b23,b24-b25 ∨E
b27.	$k \ne Sj \wedge \sim\mathbb{P}(\vec{x},z,k)$	b19,b26 ∧I
b28.	$(\forall w < b)(w \ne Sj \wedge \sim\mathbb{P}(\vec{x},z,w))$	b17-b27 (∀I)
b29.	$[b = Sj \vee \mathbb{P}(\vec{x},z,b)] \wedge (\forall w < b)(w \ne Sj \wedge \sim\mathbb{P}(\vec{x},z,w))$	b16,b28 ∧I

Exercise 13.27 T13.39.e

(c)

c1.	$j \leq j$	T13.13m
c2.	$(\exists y \leq j)\mathbb{P}(\vec{x}, z, y)$	21,c1 ($\exists$I)
c3.	$\mathit{ch}_{\mathsf{R}}(\vec{x}, z, j) = \emptyset$	3,c2 $\leftrightarrow$E
c4.	$b = a + \emptyset$	12,c3 =E
c5.	$a + \emptyset = a$	t6.41
c6.	$b = a$	c4,c5 =E
c7.	$b = j$	17,c6 =E
c8.	$\mathbb{P}(\vec{x}, z, b)$	21,c7 =E
c9.	$b = Sj \vee \mathbb{P}(\vec{x}, z, b)$	c8 $\vee$I
c10.	$\quad k < b$	A (g ($\forall$I))
c11.	$\quad k < j$	c10,c7 =E
c12.	$\quad k < Sj$	c11 T13.13n
c13.	$\quad k \neq Sj$	c12 T13.13s
c14.	$\quad k < a$	c10,c6 =E
c15.	$\quad \sim\mathbb{P}(\vec{x}, z, k)$	15,c14 ($\forall$E)
c16.	$\quad k \neq Sj \wedge \sim\mathbb{P}(\vec{x}, z, k)$	c13,c15 $\wedge$I
c17.	$(\forall w < b)(w \neq Sj \wedge \sim\mathbb{P}(\vec{x}, z, w))$	c10-c16 ($\forall$I)
c18.	$[b = Sj \vee \mathbb{P}(\vec{x}, z, b)] \wedge (\forall w < b)(w \neq Sj \wedge \sim\mathbb{P}(\vec{x}, z, w))$	c9,c17 $\wedge$I

(d)

d1.	$\quad j < a$	A (c $\sim$I)
d2.	$\quad j \neq j$	15,d1 ($\forall$E)
d3.	$\quad j = j$	=I
d4.	$\quad \bot$	d2,d3 $\bot$I
d5.	$j \not< a$	d1-d4 $\sim$I
d6.	$a \leq j$	d5 T13.13q
d7.	$(\exists y \leq j)\mathbb{P}(\vec{x}, z, y)$	24,d6 ($\exists$I)
d8.	$\mathit{ch}_{\mathsf{R}}(\vec{x}, z, j) = \emptyset$	3,d7 $\leftrightarrow$E
d9.	$b = a + \emptyset$	12,d8 =E
d10.	$a + \emptyset = a$	t6.41
d11.	$b = a$	d9,d10 =E
d12.	$\mathbb{P}(\vec{x}, z, b)$	24,d11 =E
d13.	$b = Sj \vee \mathbb{P}(\vec{x}, z, b)$	d12 $\vee$I
d14.	$\quad k < b$	A (g ($\forall$I))
d15.	$\quad k < a$	d14,d11 =E
d16.	$\quad k < j$	d14,d6 T13.13c
d17.	$\quad k < Sj$	d16 T13.13n
d18.	$\quad k \neq Sj$	d17 T13.13s
d19.	$\quad \sim\mathbb{P}(\vec{x}, z, k)$	15,d15 ($\forall$E)
d20.	$\quad k \neq Sj \wedge \sim\mathbb{P}(\vec{x}, z, k)$	d18,d19 $\wedge$I
d21.	$(\forall w < b)(w \neq Sj \wedge \sim\mathbb{P}(\vec{x}, z, w))$	d14-d20 ($\forall$I)
d22.	$[b = Sj \vee \mathbb{P}(\vec{x}, z, b)] \wedge (\forall w < b)(w \neq Sj \wedge \sim\mathbb{P}(\vec{x}, z, w))$	d13,d21 $\wedge$I

1.	$\mathit{q}(\vec{x}, z, n) = (\mu y \leq n)\mathbb{P}(\vec{x}, z, y)$	from main arg
2.	$\mathit{m}(\vec{x}, z) = \mathit{q}(\vec{x}, z, z)$	def from least, T13.34
3.	$\mathit{q}(\vec{x}, z, z) = (\mu y \leq z)\mathbb{P}(\vec{x}, z, y)$	1 $\forall$E
4.	$\mathit{m}(\vec{x}, z) = (\mu y \leq z)\mathbb{P}(\vec{x}, z, y)$	2,3 =E
5.	$(\mu y \leq z)\mathbb{P}(\vec{x}, z, y) \leftrightarrow (\mu y \leq z)\mathbb{P}(\vec{x}, y, z)$	4 abv

T13.39.g. PA $\vdash$ $\mathbb{P}rime(n) \leftrightarrow Pr(n)$

Exercise 13.27 T13.39.g

1.	$Pr(n)$	A (g $\leftrightarrow$I)
2.	$\overline{1} < n \wedge \forall x[x \mid n \to (x = \emptyset \vee Sx = n)]$	1 *Def*[*Pr*]
3.	$\overline{1} < n$	2 $\wedge$E
4.	$\forall x[x \mid n \to (x = \emptyset \vee Sx = n)]$	2 $\wedge$E
5.	$a < n$	A (g ($\forall$I))
6.	$a \mid n \to (a = \emptyset \vee Sa = n)$	4 $\forall$E
7.	$(\forall j < n)[j \mid n \to (j = \emptyset \vee Sj = n)]$	5-6 ($\forall$I)
8.	$\overline{1} < n \wedge (\forall j < n)[j \mid n \to (j = \emptyset \vee Sj = n)]$	3,7 $\wedge$I
9.	$\mathbb{P}rime(n)$	8 def PRIME and T13.34
10.	$\mathbb{P}rime(n)$	A (g $\leftrightarrow$I)
11.	$\overline{1} < n \wedge (\forall j < n)[j \mid n \to (j = \emptyset \vee Sj = n)]$	10 def PRIME and T13.34
12.	$\overline{1} < n$	11 $\wedge$E
13.	$(\forall j < n)[j \mid n \to (j = \emptyset \vee Sj = n)]$	11 $\wedge$E
14.	$a < n \vee n \leq a$	T13.13q
15.	$a < n$	A (g 14$\vee$E)
16.	$a \mid n \to (a = \emptyset \vee Sa = n)$	13,15 ($\forall$E)
17.	$n \leq a$	A (g 14$\vee$E)
18.	$\emptyset < \overline{1}$	T13.13e
19.	$\emptyset < n$	18,12 T13.13b
20.	$\exists v(n = Sv)$	19 T13.13g
21.	$n = Sb$	A (g 20$\exists$E)
22.	$Sb \leq a$	17,21 =E
23.	$b < a$	22 T13.13l
24.	$a \nmid Sb$	23 T13.24i
25.	$a \nmid n$	24,21 =E
26.	$a \nmid n$	20,21-25 $\exists$E
27.	$a \nmid n \vee (a = \emptyset \vee Sa = n)$	26 $\vee$I
28.	$a \mid n \to (a = \emptyset \vee Sa = n)$	27 Impl
29.	$a \mid n \to (a = \emptyset \vee Sa = n)$	14,15-16,17-28 $\vee$E
30.	$\forall x[x \mid n \to (x = \emptyset \vee Sx = n)]$	29 $\forall$I
31.	$\overline{1} < n \wedge \forall x[x \mid n \to (x = \emptyset \vee Sx = n)]$	12,30 $\wedge$I
32.	$Pr(n)$	31 *Def*[*Pr*]

E13.28. Show each of the results from T13.41.

T13.41.

T13.41.m. PA $\vdash m > \overline{1} \to a < m^a$

1.	$m^{\emptyset} = \overline{1}$	T13.41a
2.	$\emptyset < \overline{1}$	T13.13e
3.	$\emptyset < m^{\emptyset}$	1,2 =E
4.	$m \not> \overline{1} \vee \emptyset < m^{\emptyset}$	3 ∨I
5.	$m > \overline{1} \to \emptyset < m^{\emptyset}$	4 Impl
6.	$m > \overline{1} \to j < m^{j}$	A (g →I)
7.	$m > \overline{1}$	A (g →I)
8.	$j < m^{j}$	6,7 →E
9.	$Sj < Sm^{j}$	8 T13.13k
10.	$m^{Sj} = m^{j} \times m$	T13.41a
11.	$\exists v(Sv + \overline{1} = m)$	7 def
12.	$Sl + \overline{1} = m$	A (g 11∃E)
13.	$Sl + \overline{1} = SSl$	T6.47
14.	$m = SSl$	12,13 =E
15.	$m^{j} \times SSl = m^{j} \times Sl + m^{j}$	T6.44
16.	$m^{j} \times m = m^{j} \times Sl + m^{j}$	15,14 =E
17.	$m^{Sj} = m^{j} \times Sl + m^{j}$	16,10 =E
18.	$Sl > \emptyset$	T13.13e
19.	$m^{j} \times Sl \geq m^{j}$	18 T13.13z
20.	$m > \emptyset$	7,2 T13.13b
21.	$m^{j} > \emptyset$	20 T13.41i
22.	$m^{j} \times Sl > \emptyset$	19,21 T13.13c
23.	$m^{j} \times Sl \geq \overline{1}$	22 T13.13l
24.	$m^{j} \times Sl + m^{j} \geq \overline{1} + m^{j}$	23 T13.13v
25.	$\overline{1} + m^{j} = Sm^{j}$	T6.47
26.	$m^{j} \times Sl + m^{j} \geq Sm^{j}$	24,25 =E
27.	$m^{Sj} \geq Sm^{j}$	17,26 =E
28.	$Sj < m^{Sj}$	9,27 T13.13c
29.	$Sj < m^{Sj}$	11,12-28 ∃E
30.	$m > \overline{1} \to Sj < m^{Sj}$	7-29 →I
31.	$(m > \overline{1} \to j < m^{j}) \to (m > \overline{1} \to Sj < m^{Sj})$	6-30 →I
32.	$\forall y[(m > \overline{1} \to y < m^{y}) \to (m > \overline{1} \to Sy < m^{Sy})]$	31 ∀I
33.	$m > \overline{1} \to a < m^{a}$	5,32 IN

E13.29. Show each of the results from T13.42.

T13.42.

T13.42.e. PA ⊢ $(\exists y \leq fact(n) + \overline{1})[n < y \wedge Pr(y)]$

1.	$fact(n) > 0$	1 T13.42c
2.	$fact(n) + \overline{1} > \overline{1}$	1 with T13.13w
3.	$\exists z[Pr(Sz) \land z \mid (fact(n) + \overline{1})]$	2 T13.25d
4.	$\quad Pr(Sk) \land k \mid (fact(n) + \overline{1})$	A (g 3∃E)
5.	$\quad Pr(Sk)$	4 ∧E
6.	$\quad Sk > \overline{1}$	5 def
7.	$\quad k \mid (fact(n) + \overline{1})$	4 ∧E
8.	$\quad\quad k < n$	A (g ∼I)
9.	$\quad\quad k \mid fact(n)$	8 T13.42d
10.	$\quad\quad k \mid \overline{1}$	7,9 T13.24g
11.	$\quad\quad \emptyset < k$	6 T13.13k
12.	$\quad\quad k \nmid \overline{1}$	11 T13.24i
13.	$\quad\quad \bot$	10,12 ⊥I
14.	$\quad k \not< n$	8-12 ∼I
15.	$\quad n \leq k$	13 T13.13r
16.	$\quad n < Sk$	15 T13.13m,n
17.	$\quad n < Sk \land Pr(Sk)$	5,17 ∧I
18.	$\quad fact(n) + \overline{1} = S\,fact(n)$	T 6.47
19.	$\quad k \mid S\,fact(n)$	7,18 =E
20.	$\quad fact(n) \not< k$	19 T13.24i
21.	$\quad k \leq fact(n)$	20 T13.13r
22.	$\quad Sk \leq S\,fact(n)$	21 T13.13j
23.	$\quad Sk \leq fact(n) + \overline{1}$	22 T6.47
24.	$\quad (\exists y \leq fact(n) + \overline{1})[n < y \land Pr(y)]$	17,23 (∃I)
25.	$(\exists y \leq fact(n) + \overline{1})[n < y \land Pr(y)]$	3,4-24 ∃E

E13.30. Show each of the results from T13.43.

T13.43.

T13.43.m. PA $\vdash \forall y Pr(y) \rightarrow \exists j\, \mathbb{pi}(j) = y$

1.	$a \leq \mathbb{pi}(0)$	A (g ($\forall$I))
2.	$\mathbb{pi}(0) = \overline{2}$	T13.43a
3.	$a \leq \overline{2}$	1,2 =E
4.	$a = \overline{0} \vee a = \overline{1} \vee a = \overline{2}$	3 T8.16
5.	$a = \overline{0}$	A (g 4$\vee$E)
6.	$\sim Pr(\emptyset)$	T13.25a
7.	$\sim Pr(a)$	6,5 =E
8.	$\sim Pr(a) \vee \exists j\, \mathbb{pi}(j) = a$	6 $\vee$I
9.	$a = \overline{1}$	A (g 4$\vee$E)
10.	$\sim Pr(\overline{1})$	T13.25b
11.	$\sim Pr(a)$	10,9 =E
12.	$\sim Pr(a) \vee \exists j\, \mathbb{pi}(j) = a$	11 $\vee$I
13.	$a = \overline{2}$	A (g 4$\vee$E)
14.	$\mathbb{pi}(0) = a$	2,13 =E
15.	$\exists j\, \mathbb{pi}(j) = a$	14 $\exists$I
16.	$\sim Pr(a) \vee \exists j\, \mathbb{pi}(j) = a$	15 $\vee$I
17.	$\sim Pr(a) \vee \exists j\, \mathbb{pi}(j) = a$	4,5-8,9-12,13-16 $\vee$E
18.	$Pr(a) \to \exists j\, \mathbb{pi}(j) = a$	17 Impl
19.	$(\forall y \leq \mathbb{pi}(\emptyset))[Pr(y) \to \exists j\, \mathbb{pi}(j) = y]$	1-17 ($\forall$I)

Exercise 13.30 T13.43.m

20.	$(\forall y \leq \mathbb{pi}(k))[Pr(y) \to \exists j\, \mathbb{pi}(j) = y]$	A (g $\to$I)
21.	$a \leq \mathbb{pi}(Sk)$	A (g ($\forall$I))
22.	$a = \mathbb{pi}(Sk) \vee a < \mathbb{pi}(Sk)$	21 T13.13m
23.	$a = \mathbb{pi}(Sk)$	A (g 22$\vee$E)
24.	$\exists j\, \mathbb{pi}(j) = a$	23 $\exists$I
25.	$\sim Pr(a) \vee \exists j\, \mathbb{pi}(j) = a$	24 $\vee$I
26.	$Pr(a) \to \exists j\, \mathbb{pi}(j) = a$	25 Impl
27.	$a < \mathbb{pi}(Sk)$	A (g 22$\vee$E)
28.	$a \leq \mathbb{pi}(k) \vee a > \mathbb{pi}(k)$	T13.13q
29.	$a \leq \mathbb{pi}(k)$	A (g 28$\vee$E)
30.	$Pr(a) \to \exists j\, \mathbb{pi}(j) = a]$	20,29 ($\forall$E)
31.	$a > \mathbb{pi}(k)$	A (g 28$\vee$E)
32.	$(\forall w < \mathbb{pi}(Sk))\sim[\mathbb{pi}(k) < w \wedge Pr(w)]$	T13.43e
33.	$\sim[\mathbb{pi}(k) < a \wedge Pr(a)]$	32,27 ($\forall$E)
34.	$\mathbb{pi}(k) \not< a \vee \sim Pr(a)$	33 DeM
35.	$\sim Pr(a)$	34,31 DS
36.	$\sim Pr(a) \vee \exists j\, \mathbb{pi}(j) = a$	35 $\vee$I
37.	$Pr(a) \to \exists j\, \mathbb{pi}(j) = a$	36 Impl
38.	$Pr(a) \to \exists j\, \mathbb{pi}(j) = a$	28,29-30,31-37 $\vee$E
39.	$Pr(a) \to \exists j\, \mathbb{pi}(j) = a$	22,23-26,27-38 $\vee$E
40.	$(\forall y \leq \mathbb{pi}(Sk))[Pr(y) \to \exists j\, \mathbb{pi}(j) = y]$	21-39 ($\forall$I)
41.	$(\forall y \leq \mathbb{pi}(k))[Pr(y) \to \exists j\, \mathbb{pi}(j) = y] \to (\forall y \leq \mathbb{pi}(Sk))[Pr(y) \to \exists j\, \mathbb{pi}(j) = y]$	20-40 $\to$I
42.	$\forall z((\forall y \leq \mathbb{pi}(z))[Pr(y) \to \exists j\, \mathbb{pi}(j) = y] \to (\forall y \leq \mathbb{pi}(Sz))[Pr(y) \to \exists j\, \mathbb{pi}(j) = y])$	41 $\forall$I
43.	$(\forall y \leq \mathbb{pi}(i))[Pr(y) \to \exists j\, \mathbb{pi}(j) = y]$	19,42 IN

44.	$Pr(k)$	A (g $\to$I)
45.	$k \leq k$	T13.13m
46.	$Sk < \mathbb{pi}(k)$	45 T13.43l
47.	$k < Sk$	T13.13h
48.	$k < \mathbb{pi}(k)$	46,47 T13.13b
49.	$k \leq \mathbb{pi}(k)$	48 T13.13m
50.	$Pr(k) \to \exists j\, \mathbb{pi}(j) = k$	43,49 ($\forall$E)
51.	$\exists j\, \mathbb{pi}(j) = k$	44,50 $\to$E
52.	$Pr(k) \to \exists j\, \mathbb{pi}(j) = k$	44-51 $\to$I
53.	$\forall y[Pr(y) \to \exists j\, \mathbb{pi}(j) = y]$	52 $\forall$I

T13.43.n. PA $\vdash m \neq n \to pred(\mathbb{pi}(m)) \nmid \mathbb{pi}(n)$[a]

1.	$m \neq n$	A (g $\rightarrow$I)
2.	$\mathbb{pi}(n)^{\emptyset} = \overline{1}$	T13.41a
3.	$Spred(\mathbb{pi}(n)^{\emptyset}) = \mathbb{pi}(n)^{\emptyset}$	T13.43j
4.	$Spred(\mathbb{pi}(n)^{\emptyset}) = \overline{1}$	2,3 =E
5.	$Spred(\mathbb{pi}(m)^{\overline{1}}) = \mathbb{pi}(m)^{\overline{1}}$	T13.43j
6.	$\mathbb{pi}(m)^{\overline{1}} = \mathbb{pi}(m)$	T13.41b
7.	$Spred(\mathbb{pi}(m)) = \mathbb{pi}(m)$	5,6 =E
8.	$\mathbb{pi}(m) > \overline{1}$	T13.43g
9.	$Spred(\mathbb{pi}(m)) > Spred(\mathbb{pi}(n)^{\emptyset})$	8,7,4 =E
10.	$pred(\mathbb{pi}(m)) > pred(\mathbb{pi}(n)^{\emptyset})$	9 T13.13k
11.	$pred(\mathbb{pi}(m)) \nmid Spred(\mathbb{pi}(n)^{\emptyset})$	10 T13.24i
12.	$pred(\mathbb{pi}(m)) \nmid \mathbb{pi}(n)^{\emptyset}$	11,3 =E
13.	$pred(\mathbb{pi}(m)) \nmid \mathbb{pi}(n)^{j}$	A (g $\rightarrow$I)
14.	$pred(\mathbb{pi}(m)) \mid \mathbb{pi}(n)^{Sj}$	A (c $\sim$I)
15.	$\mathbb{pi}(n)^{Sj} = \mathbb{pi}(n)^{j} \times \mathbb{pi}(n)$	T13.41a
16.	$pred(\mathbb{pi}(m)) \mid (\mathbb{pi}(n)^{j} \times \mathbb{pi}(n))$	14,15 =E
17.	$Pr[\mathbb{pi}(m)]$	T13.43f
18.	$Pr[Spred(\mathbb{pi}(m))]$	7,17 =E
19.	$pred(\mathbb{pi}(m)) \mid \mathbb{pi}(n)^{j} \vee pred(\mathbb{pi}(m)) \mid \mathbb{pi}(n)$	16,18 T13.25i
20.	$pred(\mathbb{pi}(m)) \mid \mathbb{pi}(n)$	19,13 DS
21.	$Pr[\mathbb{pi}(n)]$	T13.43f
22.	$pred(\mathbb{pi}(m)) = \emptyset \vee Spred(\mathbb{pi}(m)) = \mathbb{pi}(n)$	20,21 def *Pr*
23.	$Spred(\mathbb{pi}(m)) > S\emptyset$	7,8 =E
24.	$pred(\mathbb{pi}(m)) > \emptyset$	23 T13.13k
25.	$pred(\mathbb{pi}(m)) \neq \emptyset$	24 T13.13f
26.	$Spred(\mathbb{pi}(m)) = \mathbb{pi}(n)$	22,25 DS
27.	$\mathbb{pi}(m) = \mathbb{pi}(n)$	7,26 =E
28.	$m < n \vee n < m$	1 with T13.13p
29.	$m < n$	A (g 28$\vee$E)
30.	$\mathbb{pi}(m) < \mathbb{pi}(n)$	29 T13.43k
31.	$\mathbb{pi}(m) \neq \mathbb{pi}(n)$	30 T13.13f
32.	$n < m$	A (g 28$\vee$E)
33.	$\mathbb{pi}(n) < \mathbb{pi}(m)$	32 T13.43k
34.	$\mathbb{pi}(m) \neq \mathbb{pi}(n)$	33 T13.13f
35.	$\mathbb{pi}(m) \neq \mathbb{pi}(n)$	28,29-31,32-34 $\vee$E
36.	$\bot$	27,35 $\bot$I
37.	$pred(\mathbb{pi}(m)) \nmid \mathbb{pi}(n)^{Sj}$	14-36 $\sim$I
38.	$[\mathbb{pi}(m)) \nmid \mathbb{pi}(n)^{j}] \rightarrow [pred(\mathbb{pi}(m)) \nmid \mathbb{pi}(n)^{Sj}]$	13-37$\rightarrow$I
39.	$\forall y([\mathbb{pi}(m)) \nmid \mathbb{pi}(n)^{y}] \rightarrow [pred(\mathbb{pi}(m)) \nmid \mathbb{pi}(n)^{Sy}])$	38 $\forall$I
40.	$pred(\mathbb{pi}(m)) \nmid \mathbb{pi}(n)^{a}$	12,39 IN
41.	$m \neq n \rightarrow pred(\mathbb{pi}(m)) \nmid \mathbb{pi}(n)^{a}$	1-40 $\rightarrow$I

T13.43.p. PA $\vdash [m \neq n \wedge pred(\mathbb{pi}(m)^{b}) \mid (s \times \mathbb{pi}(n)^{a})] \rightarrow pred(\mathbb{pi}(m)^{b}) \mid s$

1.	$m \neq n \wedge pred(\mathbb{p}i(m)^b) \mid (s \times \mathbb{p}i(n)^a)$	A (g →I)
2.	$m \neq n$	1 ∧E
3.	$pred(\mathbb{p}i(m)^b) \mid (s \times \mathbb{p}i(n)^a)$	1 ∧E
4.	$\mathbb{p}i(m)^{\emptyset} = \overline{1}$	T13.41a
5.	$pred(\overline{1}) = \emptyset$	T13.36b
6.	$\emptyset \mid s$	T13.24a
7.	$pred(\mathbb{p}i(m)^{\emptyset}) \mid s$	6,4,5 =E
8.	$\emptyset \not\leq b \vee pred(\mathbb{p}i(m)^{\emptyset}) \mid s$	7 ∨I
9.	$\emptyset \leq b \rightarrow pred(\mathbb{p}i(m)^{\emptyset}) \mid s$	8 Impl

Exercise 13.30 T13.43.p

10.	$j \le b \to pred(\mathbb{pi}(m)^j)\mid s$	A ($g \to$I)
11.	$Sj \le b$	A ($g \to$I)
12.	$j \le b$	T13.13l,m
13.	$pred(\mathbb{pi}(m)^j)\mid s$	10,12 $\to$E
14.	$Spred(\mathbb{pi}(m)^b) = \mathbb{pi}(m)^b$	T13.43j
15.	$Spred(\mathbb{pi}(m)^j) = \mathbb{pi}(m)^j$	T13.43j
16.	$\exists q[Spred(\mathbb{pi}(m)^b) \times q = s \times \mathbb{pi}(n)^a]$	3 def
17.	$\exists q[Spred(\mathbb{pi}(m)^j) \times q = s]$	13 def
18.	$Spred(\mathbb{pi}(m)^b) \times u = s \times \mathbb{pi}(n)^a$	A (g 16$\exists$E)
19.	$\mathbb{pi}(m)^b \times u = s \times \mathbb{pi}(n)^a$	14,18 =E
20.	$Spred(\mathbb{pi}(m)^j) \times v = s$	A (g 17$\exists$E)
21.	$\mathbb{pi}(m)^j \times v = s$	15,20 =E
22.	$j < b$	11 T13.13l
23.	$\exists v(Sv + j = b)$	22 def
24.	$Sl + j = b$	A (g 23$\exists$E)
25.	$\mathbb{pi}(m)^{Sl+j} = \mathbb{pi}(m)^{Sl} \times \mathbb{pi}(m)^j$	T13.41e
26.	$\mathbb{pi}(m)^b = \mathbb{pi}(m)^{Sl} \times \mathbb{pi}(m)^j$	25,24 =E
27.	$\mathbb{pi}(m)^{Sl} \times \mathbb{pi}(m)^j \times u = s \times \mathbb{pi}(n)^a$	19,26 =E
28.	$\mathbb{pi}(m)^{Sl} \times \mathbb{pi}(m)^j \times u = \mathbb{pi}(m)^j \times v \times \mathbb{pi}(n)^a$	27,21 =E
29.	$\mathbb{pi}(m)^j \ne \emptyset$	with T13.43h
30.	$\mathbb{pi}(m)^{Sl} \times u = v \times \mathbb{pi}(n)^a$	28,29 T6.69
31.	$pred(\mathbb{pi}(m)^{\bar{1}})\mid \mathbb{pi}(m)^{l+\bar{1}}$	T13.41g
32.	$\mathbb{pi}(m)^{\bar{1}} = \mathbb{pi}(m)$	T13.41b
33.	$l + \bar{1} = Sl$	T6.47
34.	$pred(\mathbb{pi}(m))\mid \mathbb{pi}(m)^{Sl}$	31,32,33 =E
35.	$pred(\mathbb{pi}(m))\mid \mathbb{pi}(m)^{Sl} \times u$	34 T13.24d
36.	$pred(\mathbb{pi}(m))\mid v \times \mathbb{pi}(n)^a$	35,30 =E
37.	$Spred(\mathbb{pi}(m)^{\bar{1}}) = \mathbb{pi}(m)^{\bar{1}}$	T13.43j
38.	$\mathbb{pi}(m)^{\bar{1}} = \mathbb{pi}(m)$	T13.41b
39.	$Spred(\mathbb{pi}(m)) = \mathbb{pi}(m)$	37,38 =E
40.	$Pr[\mathbb{pi}(m)]$	T13.43f
41.	$Pr[Spred(\mathbb{pi}(m))]$	40,39 =E
42.	$pred(\mathbb{pi}(m))\mid v \lor pred(\mathbb{pi}(m))\mid \mathbb{pi}(n)^a$	36,41 T13.25i
43.	$pred(\mathbb{pi}(m)) \nmid \mathbb{pi}(n)^a$	2 T13.43n
44.	$pred(\mathbb{pi}(m))\mid v$	42,43 DS
45.	$\exists q[Spred(\mathbb{pi}(m)) \times q = v]$	44 def
46.	$Spred(\mathbb{pi}(m)) \times t = v$	A (g 45$\exists$E)
47.	$\mathbb{pi}(m) \times t = v$	46,39 =E
48.	$\mathbb{pi}(m)^j \times \mathbb{pi}(m) \times t = s$	21,47 =E
49.	$\mathbb{pi}(m)^j \times \mathbb{pi}(m) = \mathbb{pi}(m)^{Sj}$	T13.41a
50.	$\mathbb{pi}(m)^{Sj} \times t = s$	48,49 =E
51.	$Spred(\mathbb{pi}(m)^{Sj}) = \mathbb{pi}(m)^{Sj}$	T13.43j
52.	$Spred(\mathbb{pi}(m)^{Sj}) \times t = s$	50,51 =E
53.	$\exists q[Spred(\mathbb{pi}(m)^{Sj}) \times q = s]$	52 $\exists$I
54.	$pred(\mathbb{pi}(m)^{Sj})\mid s$	53 def
55.	$pred(\mathbb{pi}(m)^{Sj})\mid s$	45,46-54 $\exists$E
56.	$pred(\mathbb{pi}(m)^{Sj})\mid s$	23,24-55 $\exists$E
57.	$pred(\mathbb{pi}(m)^{Sj})\mid s$	17,20-56 $\exists$E
58.	$pred(\mathbb{pi}(m)^{Sj})\mid s$	16,18-57 $\exists$E
59.	$Sj \le b \to pred(\mathbb{pi}(m)^{Sj})\mid s$	11-58 $\to$I
60.	$[j \le b \to pred(\mathbb{pi}(m)^j)\mid s] \to [Sj \le b \to pred(\mathbb{pi}(m)^{Sj})\mid s]$	10-59 $\to$I
61.	$i \le b \to pred(\mathbb{pi}(m)^i)\mid s$	9,60 IN
62.	$b \le b \to pred(\mathbb{pi}(m)^b)\mid s$	61 $\forall$E
63.	$b \le b$	T13.13m
64.	$pred(\mathbb{pi}(m)^b)\mid s$	62,63 $\to$E
65.	$[m \ne n \land pred(\mathbb{pi}(m)^b)\mid (s \times \mathbb{pi}(n)^a)] \to pred(\mathbb{pi}(m)^b)\mid s$	1-64 $\to$I

Exercise 13.30 T13.43.p

E13.31. Show each of the results from T13.44.

T13.44.

T13.44.c. PA $\vdash \mathbb{exp}(Sn, i) = \mu x[pred(\mathbb{pi}(i)^{x})|Sn \wedge pred(\mathbb{pi}(i)^{x+\overline{1}}) \nmid Sn]$

1.	$pred(\mathbb{pi}(i)^{ex(n,i)}) \nmid Sn$	T13.19b
2.	$(\forall z < ex(n,i))pred(\mathbb{pi}(i)^{z})|Sn$	T13.19c
3.	$ex(n,i) = \emptyset \vee ex(n,i) > \emptyset$	T13.13d,m
4.	$\quad ex(n,i) = \emptyset$	A (c ∼I)
5.	$\quad \mathbb{pi}(i)^{\emptyset} = \overline{1}$	T13.41a
6.	$\quad \mathbb{pi}(i)^{ex(n,i)} = \overline{1}$	4,5 =E
7.	$\quad Spred(\mathbb{pi}(i)^{ex(n,i)}) = \mathbb{pi}(i)^{ex(n,i)}$	T13.43j
8.	$\quad Spred(\mathbb{pi}(i)^{ex(n,i)}) = S\emptyset$	6,7 =E
9.	$\quad pred(\mathbb{pi}(i)^{ex(n,i)}) = \emptyset$	8 T6.40
10.	$\quad \emptyset|Sn$	T13.24a
11.	$\quad pred(\mathbb{pi}(i)^{ex(n,i)})|Sn$	9,10 =E
12.	$\quad \bot$	1,11 ⊥I
13.	$ex(n,i) \neq \emptyset$	4-12 ∼I
14.	$ex(n,i) > \emptyset$	3,13 DS
15.	$\exists v[ex(n,i) = Sv]$	14 T13.13g
16.	$\quad ex(n,i) = Sa$	A (g 15∃E)
17.	$\quad a < Sa$	T13.13h
18.	$\quad a < ex(n,i)$	17,16 =E
19.	$\quad pred(\mathbb{pi}(i)^{a})|Sn$	2,18 (∀E)
20.	$\quad pred(\mathbb{pi}(i)^{Sa}) \nmid Sn$	1,16 =E
21.	$\quad Sa = a + \overline{1}$	T6.47
22.	$\quad pred(\mathbb{pi}(i)^{a+\overline{1}}) \nmid Sn$	20,21 =E
23.	$\quad pred(\mathbb{pi}(i)^{a})|Sn \wedge pred(\mathbb{pi}(i)^{a+\overline{1}}) \nmid Sn$	19,22 ∧I
24.	$\quad \mathbb{pi}(i) > \overline{1}$	T13.43g
25.	$\quad a < \mathbb{pi}(i)^{a}$	24 T13.41m
26.	$\quad Spred(\mathbb{pi}(i)^{a}) = \mathbb{pi}(i)^{a}$	T13.43j
27.	$\quad n \not< pred(\mathbb{pi}(i)^{a})$	19 T13.24i
28.	$\quad pred(\mathbb{pi}(i)^{a}) \leq n$	27 T13.13r
29.	$\quad Spred(\mathbb{pi}(i)^{a}) \leq Sn$	28 T13.13j
30.	$\quad \mathbb{pi}(i)^{a} \leq Sn$	26,29 =E
31.	$\quad a < Sn$	25,30 T13.13c
32.	$\quad a \leq Sn$	31 T13.13m
33.	$\quad (\exists x \leq Sn)[pred(\mathbb{pi}(i)^{x})|Sn \wedge pred(\mathbb{pi}(i)^{x+\overline{1}}) \nmid Sn]$	23,32 (∃I)
34.	$(\exists x \leq Sn)[pred(\mathbb{pi}(i)^{x})|Sn \wedge pred(\mathbb{pi}(i)^{x+\overline{1}}) \nmid Sn]$	15,16-33 ∃E
35.	$(\mu x \leq Sn)[pred(\mathbb{pi}(i)^{x})|Sn \wedge pred(\mathbb{pi}(i)^{x+\overline{1}}) \nmid Sn] = \mu x[pred(\mathbb{pi}(i)^{x})|Sn \wedge pred(\mathbb{pi}(i)^{x+\overline{1}}) \nmid Sn]$	34 T13.20b
36.	$\mathbb{exp}(Sn,i) = \mu x[pred(\mathbb{pi}(i)^{x})|Sn \wedge pred(\mathbb{pi}(i)^{x+\overline{1}}) \nmid Sn]$	35 def

T13.44.l. PA $\vdash \exists q[\mathbb{pi}(i)^{\mathbb{exp}(Sn,i)} \times q = Sn \wedge pred(\mathbb{pi}(i)) \nmid q \wedge \forall y(y \neq i \rightarrow \mathbb{exp}(q,y) = \mathbb{exp}(Sn,y))]$

1.	$\mathit{pred}(\mathbb{pi}(i)^{\mathbb{exp}(Sn,i)}) \mid Sn \land \mathit{pred}(\mathbb{pi}(i)^{\mathbb{exp}(Sn,i)+\bar{1}}) \nmid Sn$	T13.44d
2.	$\mathbb{exp}(Sn,i) = a$	abv
3.	$\exists q[S\mathit{pred}(\mathbb{pi}(i)^a) \times q = Sn]$	1,2 with ∧E
4.	$\mathit{pred}(\mathbb{pi}(i)^{a+\bar{1}}) \nmid Sn$	1,2 with ∧E
5.	$S\mathit{pred}(\mathbb{pi}(i)^a) = \mathbb{pi}(i)^a$	T13.43j
6.	$\exists q[\mathbb{pi}(i)^a \times q = Sn]$	3,5 =E
7.	$\mathbb{pi}(i)^a \times j = Sn$	A (g 6∃E)
8.	$\mathit{pred}(\mathbb{pi}(i)) \mid j$	A (c ∼I)
9.	$\exists q[S\mathit{pred}(\mathbb{pi}(i)) \times q = j]$	8 def
10.	$S\mathit{pred}(\mathbb{pi}(i)) \times k = j$	A (g 9∃E)
11.	$\mathbb{pi}(i) \times k = j$	10 T13.43j
12.	$\mathbb{pi}(i)^a \times \mathbb{pi}(i) \times k = Sn$	7,11 =E
13.	$\mathbb{pi}(i)^{a+\bar{1}} \times k = Sn$	12 T13.41a
14.	$S\mathit{pred}(\mathbb{pi}(i)^{a+\bar{1}}) \times k = Sn$	13 T13.43j
15.	$\mathit{pred}(\mathbb{pi}(i)^{a+\bar{1}}) \mid Sn$	14 def
16.	$\bot$	4,15 ⊥I
17.	$\bot$	9,10-16 ∃E
18.	$\mathit{pred}(\mathbb{pi}(i)) \nmid j$	8-17 ∼I
19.	$j = \emptyset \lor j > \emptyset$	T13.13f
20.	$j = \emptyset$	A (c ∼I)
21.	$\mathbb{pi}(i)^a \times \emptyset = \emptyset$	T6.43
22.	$\mathbb{pi}(i)^a \times j = \emptyset$	21,20 =E
23.	$\emptyset = Sn$	7,22 =E
24.	$\emptyset \neq Sn$	with T13.13e
25.	$\bot$	23,24 ⊥I
26.	$j \neq \emptyset$	20-25 ∼I
27.	$j > \emptyset$	19,26 DS
28.	$k \neq i$	A (g →I)
29.	$\exists v(j = Sv)$	27 T13.13g
30.	$j = Sl$	A (g 29∃E)
31.	$\mathbb{pi}(i)^a \times Sl = Sn$	7,30 =E
32.	$\mathbb{exp}(Sn,k) = b$	abv
33.	$\mathit{pred}(\mathbb{pi}(k)^b) \mid Sn$	32 T13.44d
34.	$\mathit{pred}(\mathbb{pi}(k)^b) \mid \mathbb{pi}(i)^a \times Sl$	31,33 =E
35.	$\mathit{pred}(\mathbb{pi}(k)^b) \mid Sl$	28,34 T13.43p
36.	$\mathit{pred}(\mathbb{pi}(k)^{b+\bar{1}}) \nmid Sn$	T13.44d
37.	$\mathit{pred}(\mathbb{pi}(k)^{b+\bar{1}}) \mid Sl$	A (g ∼I)
38.	$\mathit{pred}(\mathbb{pi}(k)^{b+\bar{1}}) \mid \mathbb{pi}(i)^a \times Sl$	37 T13.24d
39.	$\mathit{pred}(\mathbb{pi}(k)^{b+\bar{1}}) \mid Sn$	38,31 =E
40.	$\bot$	36,39 ⊥I
41.	$\mathit{pred}(\mathbb{pi}(k)^{b+\bar{1}}) \nmid Sl$	37-40 ∼I
42.	$\mathit{pred}(\mathbb{pi}(k)^b) \mid Sl \land \mathit{pred}(\mathbb{pi}(k)^{b+\bar{1}}) \nmid Sl$	35,41 ∧I
43.	$\mathbb{exp}(Sl,k) = b$	42 T13.44f
44.	$\mathbb{exp}(j,k) = b$	43,30 =E
45.	$\mathbb{exp}(j,k) = \mathbb{exp}(Sn,k)$	44 abv
46.	$\mathbb{exp}(j,k) = \mathbb{exp}(Sn,k)$	29,30-45 ∃E
47.	$k \neq i \to \mathbb{exp}(j,k) = \mathbb{exp}(Sn,k)$	28-46 →I
48.	$\forall y(y \neq i \to \mathbb{exp}(j,y) = \mathbb{exp}(Sn,y))$	47 ∀I
49.	$\mathbb{pi}(i)^a \times j = Sn \land \mathit{pred}(\mathbb{pi}(i)) \nmid j \land \forall y(y \neq i \to \mathbb{exp}(j,y) = \mathbb{exp}(Sn,y))$	7,18,48 ∧I
50.	$\exists q[\mathbb{pi}(i)^a \times q = Sn \land \mathit{pred}(\mathbb{pi}(i)) \nmid q \land \forall y(y \neq i \to \mathbb{exp}(q,y) = \mathbb{exp}(Sn,y))]$	49 ∃I
51.	$\exists q[\mathbb{pi}(i)^{\mathbb{exp}(Sn,i)} \times q = Sn \land \mathit{pred}(\mathbb{pi}(i)) \nmid q \land \forall y(y \neq i \to \mathbb{exp}(q,y) = \mathbb{exp}(Sn,y))]$	6,7-50 ∃E

T13.44.m. PA $\vdash \mathbb{exp}(Sm \times Sn, i) = \mathbb{exp}(Sm,i) + \mathbb{exp}(Sn,i)$

Exercise 13.31 T13.44.m

1.	$\mathbb{pi}(i)^{a} > \emptyset$	T13.43h
2.	$pred(\mathbb{pi}(i)^{\mathbb{exp}(Sm,i)}) \mid Sm$	T13.44d
3.	$pred(\mathbb{pi}(i)^{\mathbb{exp}(Sn,i)}) \mid Sn$	T13.44d
4.	$pred(\mathbb{pi}(i)^{\mathbb{exp}(Sm,i)} \times \mathbb{pi}(i)^{\mathbb{exp}(Sn,i)}) \mid (Sm \times Sn)$	1,2,3 T13.24e
5.	$pred(\mathbb{pi}(i)^{\mathbb{exp}(Sm,i)+\mathbb{exp}(Sn,i)}) \mid (Sm \times Sn)$	4 T13.41e
6.	$\exists q[\mathbb{pi}(i)^{\mathbb{exp}(Sm,i)} \times q = Sm \wedge pred(\mathbb{pi}(i)) \nmid q]$	T13.44l
7.	$\exists r[\mathbb{pi}(i)^{\mathbb{exp}(Sn,i)} \times r = Sn \wedge pred(\mathbb{pi}(i)) \nmid r]$	T13.44l
8.	$\mathbb{pi}(i)^{\mathbb{exp}(m,i)} \times q = Sm \wedge pred(\mathbb{pi}(i)) \nmid q$	A (g 6,7 ∃E)
9.	$\mathbb{pi}(i)^{\mathbb{exp}(Sn,i)} \times r = Sn \wedge pred(\mathbb{pi}(i)) \nmid r$	
10.	$Sm \times Sn = \mathbb{pi}(i)^{\mathbb{exp}(Sm,i)} \times q \times \mathbb{pi}(i)^{\mathbb{exp}(Sn,i)} \times r$	8,9 ∧E, etc.
11.	$Sm \times Sn = \mathbb{pi}(i)^{\mathbb{exp}(Sm,i)+\mathbb{exp}(Sn,i)} \times q \times r$	10 T13.41e
12.	$pred(\mathbb{pi}(i)^{\mathbb{exp}(Sm,i)+\mathbb{exp}(Sn,i)+1}) \mid (Sm \times Sn)$	A (c ∼I)
13.	$\exists s[Spred(\mathbb{pi}(i)^{\mathbb{exp}(Sm,i)+\mathbb{exp}(Sn,i)+1}) \times s = Sm \times Sn]$	12 def
14.	$Spred(\mathbb{pi}(i)^{\mathbb{exp}(Sm,i)+\mathbb{exp}(Sn,i)+1}) \times s = Sm \times Sn$	A (g 13 ∃E)
15.	$\mathbb{pi}(i)^{\mathbb{exp}(Sm,i)+\mathbb{exp}(Sn,i)+1} \times s = Sm \times Sn$	1,14 T13.36c
16.	$\mathbb{pi}(i)^{\mathbb{exp}(Sm,i)+\mathbb{exp}(Sn,i)} \times \mathbb{pi}(i) \times s = Sm \times Sn$	15 T13.41a
17.	$\mathbb{pi}(i)^{\mathbb{exp}(Sm,i)+\mathbb{exp}(Sn,i)} \times \mathbb{pi}(i) \times s = \mathbb{pi}(i)^{\mathbb{exp}(Sm,i)+\mathbb{exp}(Sn,i)} \times q \times r$	11,16 =E
18.	$\mathbb{pi}(i) \times s = q \times r$	1,17 T6.69
19.	$Spred(\mathbb{pi}(i)) \times s = q \times r$	18 T13.36c
20.	$\exists s[Spred(\mathbb{pi}(i)) \times s = q \times r]$	19 ∃I
21.	$pred(\mathbb{pi}(i)) \mid (q \times r)$	20 def
22.	$pred(\mathbb{pi}(i)) \mid q \vee pred(\mathbb{pi}(i)) \mid r$	T13.43f,13.25i
23.	$\bot$	8,9,22 ⊥I
24.	$\bot$	13,14-23 ∃E
25.	$pred(\mathbb{pi}(i)^{\mathbb{exp}(Sm,i)+\mathbb{exp}(Sn,i)+1}) \nmid (Sm \times Sn)$	12-24 ∼I
26.	$pred(\mathbb{pi}(i)^{\mathbb{exp}(Sm,i)+\mathbb{exp}(Sn,i)}) \mid (Sm \times Sn) \wedge \mathbb{pi}(i)^{\mathbb{exp}(Sm,i)+\mathbb{exp}(Sn,i)+1}) \nmid (Sm \times Sn)$	5,25 ∧I
27.	$\mathbb{exp}(Sm \times Sn, i) = \mathbb{exp}(Sm,i) + \mathbb{exp}(Sn,i)$	26 T13.44f
28.	$\mathbb{exp}(Sm \times Sn, i) = \mathbb{exp}(Sm,i) + \mathbb{exp}(Sn,i)$	6,7,8-27 ∃E

E13.32. Show each of the results from T13.45.

T13.45.

T13.45.h. PA $\vdash \mathbb{exp}(m,i) > \emptyset \rightarrow \mathbb{len}(m) > i$

1.	$\mathbb{exp}(m,i) > \emptyset$	A ($g \rightarrow$I)
2.	$\mathbb{exp}(m,i) \neq \emptyset$	1 T13.13f
3.	$m = \emptyset \vee m > \emptyset$	T13.13f
4.	$m = \emptyset$	A (g 3$\vee$E)
5.	$\mathbb{len}(m) \not> i$	A (c $\sim$E)
6.	$\mathbb{exp}(\emptyset, i) = \emptyset$	T13.44b
7.	$\mathbb{exp}(m,i) = \emptyset$	6,4 =E
8.	$\bot$	2,7 $\bot$I
9.	$\mathbb{len}(m) > i$	5-8 $\sim$E
10.	$m > \emptyset$	A (g 3$\vee$E)
11.	$\mathbb{len}(m) \not> i$	A (c $\sim$E)
12.	$\mathbb{len}(m) \leq i$	11 T13.13r
13.	$\exists v(m = Sv)$	10 T13.13g
14.	$m = Sa$	A (g 13$\exists$E)
15.	$\mathbb{exp}(Sa, i) \neq \emptyset$	2,14 =E
16.	$\mathbb{len}(Sa) \leq i$	12,14 =E
17.	$i > Sa$	A (g $\sim$I)
18.	$i \geq a$	17 T13.13m,n
19.	$\mathbb{exp}(Sa, i) = \emptyset$	18 T13.44h
20.	$\bot$	15,19 $\bot$I
21.	$i \not> Sa$	17-20 $\sim$I
22.	$i \leq Sa$	T13.13r
23.	$(\forall z \leq Sa)[z \geq \mathbb{len}(Sa) \rightarrow \mathbb{exp}(Sa, z) = \emptyset]$	T13.45d
24.	$i \geq \mathbb{len}(Sa) \rightarrow \mathbb{exp}(Sa, i) = \emptyset$	23,22 ($\forall$E)
25.	$\mathbb{exp}(Sa, i) = \emptyset$	24,16 $\rightarrow$E
26.	$\bot$	15,25 $\bot$I
27.	$\bot$	13,14-26 $\exists$E
28.	$\mathbb{len}(m) > i$	11-27 $\sim$E
29.	$\mathbb{len}(m) > i$	3,4-9,10-28 $\vee$E
30.	$\mathbb{exp}(m,i) > \emptyset \rightarrow \mathbb{len}(m) > i$	1-29 $\rightarrow$I

T13.45.k. PA $\vdash p > \emptyset \rightarrow \mathbb{len}(\mathbb{pi}(i)^p) = Si$

1.	$p > \emptyset$	A (g $\rightarrow$I)
2.	$\mathit{len}(\mathit{pi}(i)^p) < Si \vee \mathit{len}(\mathit{pi}(i)^p) = Si \vee \mathit{len}(\mathit{pi}(i)^p) > Si$	T13.13p
3.	$\mathit{exp}(\mathit{pi}(i)^p, i) = p$	T13.44i
4.	$\mathit{exp}(\mathit{pi}(i)^p, i) > \emptyset$	1,3 =E
5.	$\mathit{len}(\mathit{pi}(i)^p) > i$	4 T13.45h
6.	$\mathit{len}(\mathit{pi}(i)^p) \geq Si$	5 T13.13l
7.	$\mathit{len}(\mathit{pi}(i)^p) \not< Si$	6 T13.13r
8.	$\mathit{len}(\mathit{pi}(i)^p) > Si$	A (c $\sim$I)
9.	$\mathit{pi}(i)^p > \emptyset$	T13.43h
10.	$\exists y[\mathit{pi}(i)^p = Sy]$	9 T6.50
11.	$\mathit{pi}(i)^p = Sj$	A (g 10$\exists$E)
12.	$(\forall w < \mathit{len}(Sj))\sim(\forall z < Sj)[z \geq w \rightarrow \mathit{exp}(Sj, z) = \emptyset]$	T13.45e
13.	$\mathit{len}(Sj) > Si$	8,11 =E
14.	$\sim(\forall z < Sj)[z \geq Si \rightarrow \mathit{exp}(Sj, z) = \emptyset]$	12,13 ($\forall$E)
15.	$\sim(\forall z < \mathit{pi}(i)^p)[z \geq Si \rightarrow \mathit{exp}(\mathit{pi}(i)^p, z) = \emptyset]$	11,14 =E
16.	$k < \mathit{pi}(i)^p$	A (g ($\forall$I))
17.	$k \geq Si$	A (g $\rightarrow$I)
18.	$k > i$	17 T13.13h,c
19.	$\mathit{pred}(\mathit{pi}(k)) \nmid \mathit{pi}(i)^p$	18 T13.43n
20.	$\mathit{pred}(\mathit{pi}(k)) \nmid Sj$	11,19 =E
21.	$\mathit{exp}(Sj, k) \not\geq \overline{1}$	20 T13.44k
22.	$\mathit{exp}(Sj, k) < S\emptyset$	21 T13.13r
23.	$\mathit{exp}(Sj, k) < \emptyset \vee \mathit{exp}(Sj, k) = \emptyset$	22 T13.13n
24.	$\mathit{exp}(Sj, k) = \emptyset$	23 with T6.49
25.	$\mathit{exp}(\mathit{pi}(i)^p, k) = \emptyset$	24,11 =E
26.	$k \geq Si \rightarrow \mathit{exp}(\mathit{pi}(i)^p, k) = \emptyset$	17-25 $\rightarrow$I
27.	$(\forall z < \mathit{pi}(i)^p)[z \geq Si \rightarrow \mathit{exp}(\mathit{pi}(i)^p, z) = \emptyset]$	16-26 ($\forall$I)
28.	$\perp$	15,27 $\perp$I
29.	$\perp$	10,11-28 $\exists$E
30.	$\mathit{len}(\mathit{pi}(i)^p) \not> Si$	8-29 $\sim$I
31.	$\mathit{len}(\mathit{pi}(i)^p) = Si$	2,7,30 DS
32.	$p > \emptyset \rightarrow \mathit{len}(\mathit{pi}(i)^p) = Si$	1-31 $\rightarrow$I

T13.45.m. PA $\vdash \mathit{len}(n) = Sl \rightarrow \mathit{exp}(n, l) \geq 1$

1.	$\mathbb{len}(n) = Sl$	A (g $\rightarrow$I)
2.	$n = \emptyset \vee n > \emptyset$	T13.13f
3.	$n = \emptyset$	A (c $\sim$I)
4.	$\mathbb{len}(\emptyset) = \emptyset$	T13.45b
5.	$\mathbb{len}(n) = \emptyset$	3,4 =E
6.	$\emptyset = Sl$	1,5 =E
7.	$\emptyset \neq Sl$	T6.39
8.	$\bot$	6,7 $\bot$I
9.	$n \neq \emptyset$	3-8 $\sim$I
10.	$n > \emptyset$	2,9 DS
11.	$\exists v(n = Sv)$	10 T13.13g
12.	$n = Sm$	A (g 11$\exists$E)
13.	$\mathbb{len}(Sm) = Sl$	1,12 =E
14.	$(\forall z \leq Sm)[z \geq Sl \rightarrow \mathbb{exp}(Sm, z) = \emptyset]$	T13.45d
15.	$(\forall w < Sl)\sim(\forall z \leq Sm)[z \geq w \rightarrow \mathbb{exp}(Sm, z) = \emptyset]$	13 T13.45e
16.	$\mathbb{exp}(Sm, l) \not\geq \overline{1}$	A (c $\sim$E)
17.	$\mathbb{exp}(Sm, l) < \overline{1}$	16 T13.13r
18.	$\mathbb{exp}(Sm, l) = \emptyset$	17 T8.16
19.	$a \leq Sm$	A (g ($\forall$I))
20.	$a \geq l$	A (g $\rightarrow$I)
21.	$l = a \vee l < a$	20 T13.13m
22.	$l = a$	A (g 21$\vee$E)
23.	$\mathbb{exp}(Sm, a) = \emptyset$	18,22 =E
24.	$l < a$	A (g 21$\vee$E)
25.	$Sl \leq a$	24 T13.13l
26.	$\mathbb{len}(Sm) \leq a$	25,13 =E
27.	$\mathbb{exp}(Sm, a) = \emptyset$	26 T13.45l
28.	$\mathbb{exp}(Sm, a) = \emptyset$	21,22-23,24-27 $\vee$E
29.	$a \geq l \rightarrow \mathbb{exp}(Sm, a) = \emptyset$	20-28 $\rightarrow$I
30.	$(\forall z \leq Sm)[z \geq l \rightarrow \mathbb{exp}(Sm, z) = \emptyset]$	19-29 ($\forall$I)
31.	$a < l$	A (g ($\forall$I))
32.	$a < Sl$	31 T13.13n
33.	$\sim(\forall z \leq Sm)[z \geq a \rightarrow \mathbb{exp}(Sm, z) = \emptyset]$	15,32 ($\forall$E)
34.	$(\forall w < l)\sim(\forall z \leq Sm)[z \geq w \rightarrow \mathbb{exp}(Sm, z) = \emptyset]$	31-33 ($\forall$I)
35.	$\mathbb{len}(Sm) = l$	14,34 T13.45c
36.	$Sl = l$	13,35 =E
37.	$Sl \neq l$	T13.13h,s
38.	$\bot$	36,37 $\bot$I
39.	$\mathbb{exp}(Sm, l) \geq 1$	16-38 $\sim$E
40.	$\mathbb{exp}(n, l) \geq 1$	12,39 =E
41.	$\mathbb{exp}(n, l) \geq 1$	11,12-40 $\exists$E
42.	$\mathbb{len}(n) = Sl \rightarrow \mathbb{exp}(n, l) \geq 1$	1-41 $\rightarrow$I

E13.33. Show each of the results from T13.46.

Exercise 13.33

T13.46.

T13.46.e. PA $\vdash (\forall i \geq a)pred(\mathbb{pi}(i)) \nmid val^*(m,n,i)$

1.	$j \geq \emptyset$	A (g ($\forall$I))
2.	$val^*(m,n,\emptyset) = \bar{1}$	def val^*
3.	$\mathbb{pi}(j) > \bar{1}$	T13.43g
4.	$\mathbb{pi}(j) > \emptyset$	3 with T13.13e
5.	$Spred(\mathbb{pi}(j)) = \mathbb{pi}(j)$	4 T13.36c
6.	$Spred(\mathbb{pi}(j)) > S\emptyset$	3,5 =E
7.	$pred(\mathbb{pi}(j)) > \emptyset$	6 T13.13k
8.	$pred(\mathbb{pi}(j)) \nmid \bar{1}$	7 T13.24i
9.	$pred(\mathbb{pi}(j)) \nmid val^*(m,n,\emptyset)$	8,2 =E
10.	$(\forall i \geq \emptyset)pred(\mathbb{pi}(i)) \nmid val^*(m,n,\emptyset)$	1-9 ($\forall$I)
11.	$(\forall i \geq a)pred(\mathbb{pi}(i)) \nmid val^*(m,n,a)$	A (g $\rightarrow$I)
12.	$j \geq Sa$	A (g ($\forall$I))
13.	$j > a$	12 T13.13l
14.	$j \geq a$	13 T13.13m
15.	$pred(\mathbb{pi}(j)) \nmid val^*(m,n,a)$	11,14 ($\forall$E)
16.	$val^*(m,n,Sa) = val^*(m,n,a) \times \mathbb{pi}(a)^{exc(m,n,a)}$	def val^*
17.	$pred(\mathbb{pi}(j)) \mid val^*(m,n,Sa)$	A (c $\sim$I)
18.	$pred(\mathbb{pi}(j)) \mid val^*(m,n,a) \times \mathbb{pi}(a)^{exc(m,n,a)}$	16,17 =E
19.	$j \neq a$	13 T13.13s
20.	$pred(\mathbb{pi}(j)) \mid val^*(m,n,a)$	18,19 T13.43p
21.	$\bot$	15,20 $\bot$I
22.	$pred(\mathbb{pi}(j)) \nmid val^*(m,n,Sa)$	17-21 $\sim$I
23.	$(\forall i \geq Sa)pred(\mathbb{pi}(i)) \nmid val^*(m,n,Sa)$	12-22 ($\forall$I)
24.	$[(\forall i \geq a)pred(\mathbb{pi}(i)) \nmid val^*(m,n,a)] \rightarrow [(\forall i \geq Sa)pred(\mathbb{pi}(i)) \nmid val^*(m,n,Sa)]$	11-23 $\rightarrow$I
25.	$(\forall i \geq a)pred(\mathbb{pi}(i)) \nmid val^*(m,n,a)$	10,24 IN

T13.46.f. PA $\vdash (\forall j < i)\mathbb{exp}(val^*(m,n,i), j) = exc(m,n,j)$

1.	$a < \emptyset$	A (g ($\forall$I))
2.	$\mathbb{exp}(val^*(m,n,\emptyset), a) \neq exc(m,n,a)$	A (c $\sim$E)
3.	$a \nless \emptyset$	T6.49
4.	$\bot$	1,3 $\bot$I
5.	$\mathbb{exp}(val^*(m,n,\emptyset), a) = exc(m,n,a)$	2-4 $\sim$E
6.	$(\forall j < \emptyset)\mathbb{exp}(val^*(m,n,\emptyset), j) = exc(m,n,j)$	1-5 ($\forall$I)

7.	$(\forall j < i)\mathbb{e}xp(val^*(m,n,i), j) = exc(m,n,j)$	A (g $\rightarrow$I)
8.	$a < Si$	A (g ($\forall$I))
9.	$val^*(m,n,i) = Spred(val^*(m,n,i))$	T13.46d, T13.36c
10.	$val^*(m,n,Si) = Spred(val^*(m,n,Si))$	T13.46d, T13.36c
11.	$val^*(m,n,Si) = val^*(m,n,i) \times \mathbb{p}i(i)^{exc(m,n,i)}$	def val^*
12.	$exc(m,n,a) = e$	abv
13.	$a < i \lor a = i$	8 T13.13m
14.	$a < i$	A (g 13$\lor$E)
15.	$\mathbb{e}xp(val^*(m,n,i), a) = exc(m,n,a)$	7,14 ($\forall$E)
16.	$\mathbb{p}red(\mathbb{p}i(a)^{\mathbb{e}xp(val^*(m,n,i),a)}) \mid val^*(m,n,i)$	9 T13.44d
17.	$\mathbb{p}red(\mathbb{p}i(a)^{e}) \mid val^*(m,n,i)$	12,15,16 =E
18.	$\mathbb{p}red(\mathbb{p}i(a)^{e}) \mid val^*(m,n,i) \times \mathbb{p}i(i)^{exc(m,n,i)}$	17 T13.24d
19.	$\mathbb{p}red(\mathbb{p}i(a)^{e}) \mid val^*(m,n,Si)$	18,11 =E
20.	$\mathbb{p}red(\mathbb{p}i(a)^{e+\bar{1}}) \mid val^*(m,n,Si)$	A (c $\sim$I)
21.	$\mathbb{p}red(\mathbb{p}i(a)^{e+\bar{1}}) \mid val^*(m,n,i) \times \mathbb{p}i(i)^{exc(m,n,i)}$	20,11 =E
22.	$a \neq i$	14 T13.13f
23.	$\mathbb{p}red(\mathbb{p}i(a)^{e+\bar{1}}) \mid val^*(m,n,i)$	21,22 T13.43p
24.	$\mathbb{p}red(\mathbb{p}i(a)^{\mathbb{e}xp(val^*(m,n,i),a)+\bar{1}}) \nmid val^*(m,n,i)$	9 T13.44d
25.	$\mathbb{p}red(\mathbb{p}i(a)^{e+\bar{1}}) \nmid val^*(m,n,i)$	12,15,24 =E
26.	$\bot$	23,25 $\bot$I
27.	$\mathbb{p}red(\mathbb{p}i(a)^{e+\bar{1}}) \nmid val^*(m,n,Si)$	20-26 $\sim$I
28.	$\mathbb{p}red(\mathbb{p}i(a)^{e}) \mid val^*(m,n,Si) \land \mathbb{p}red(\mathbb{p}i(a)^{e+\bar{1}}) \nmid val^*(m,n,Si)$	19,27 $\land$I
29.	$\mathbb{e}xp(val^*(m,n,Si), a) = exc(m,n,a)$	28,10 T13.44f
30.	$a = i$	A (g 13$\lor$E)
31.	$val^*(m,n,Si) = val^*(m,n,a) \times \mathbb{p}i(a)^{e}$	11,12,30 =E
32.	$pred(\mathbb{p}i(a)^{e}) \mid Spred(\mathbb{p}i(a)^{e})$	T13.24b
33.	$Spred(\mathbb{p}i(a)^{e}) = \mathbb{p}i(a)^{e}$	T13.43j
34.	$pred(\mathbb{p}i(a)^{e}) \mid \mathbb{p}i(a)^{e}$	32,33 =E
35.	$pred(\mathbb{p}i(a)^{e}) \mid val^*(m,n,a) \times \mathbb{p}i(a)^{e}$	34 T13.24d
36.	$pred(\mathbb{p}i(a)^{e}) \mid val^*(m,n,Si)$	35,31 =E
37.	$pred(\mathbb{p}i(a)^{e+\bar{1}}) \mid val^*(m,n,Si)$	A (c $\sim$I)
38.	$pred(\mathbb{p}i(a)^{e+\bar{1}}) \mid val^*(m,n,a) \times \mathbb{p}i(a)^{e}$	37,31 =E
39.	$\exists q[Spred(\mathbb{p}i(a)^{e+\bar{1}}) \times q = val^*(m,n,a) \times \mathbb{p}i(a)^{e}]$	38 def
40.	$Spred(\mathbb{p}i(a)^{e+\bar{1}}) = \mathbb{p}i(a)^{e+\bar{1}}$	T13.43j
41.	$\exists q[\mathbb{p}i(a)^{e+\bar{1}} \times q = val^*(m,n,a) \times \mathbb{p}i(a)^{e}]$	39,40 =E
42.	$\mathbb{p}i(a)^{e+\bar{1}} \times q = val^*(m,n,a) \times \mathbb{p}i(a)^{e}$	A (c 41$\exists$E)
43.	$e + \bar{1} = Se$	T6.47
44.	$\mathbb{p}i(a)^{Se} \times q = val^*(m,n,a) \times \mathbb{p}i(a)^{e}$	42,43 =E
45.	$\mathbb{p}i(a)^{e} \times \mathbb{p}i(a) \times q = val^*(m,n,a) \times \mathbb{p}i(a)^{e}$	44 T13.41a
46.	$\mathbb{p}i(a)^{e} \neq \emptyset$	with T13.43h
47.	$\mathbb{p}i(a) \times q = val^*(m,n,a)$	45,46 T6.69
48.	$Spred(\mathbb{p}i(a)) = \mathbb{p}i(a)$	with T13.43j
49.	$Spred(\mathbb{p}i(a)) \times q = val^*(m,n,a)$	47,48 =E
50.	$\exists q[Spred(\mathbb{p}i(a)) \times q = val^*(m,n,a)]$	49 $\exists$I
51.	$pred(\mathbb{p}i(a)) \mid val^*(m,n,a)$	50 def
52.	$a \geq a$	T13.13m
53.	$pred(\mathbb{p}i(a)) \nmid val^*(m,n,a)$	52 T13.46e
54.	$\bot$	51,53 $\bot$I
55.	$\bot$	41,42-54 $\exists$E
56.	$pred(\mathbb{p}i(a)^{e+\bar{1}}) \nmid val^*(m,n,Si)$	37-55 $\sim$I
57.	$pred(\mathbb{p}i(a)^{e}) \mid val^*(m,n,Si) \land pred(\mathbb{p}i(a)^{e+\bar{1}}) \nmid val^*(m,n,Si)$	36,56 $\land$I
58.	$\mathbb{e}xp(val^*(m,n,Si), a) = exc(m,n,a)$	57,10 T13.44f
59.	$\mathbb{e}xp(val^*(m,n,Si), a) = exc(m,n,a)$	13,14-29,30-58 $\lor$E
60.	$(\forall j < Si)\mathbb{e}xp(val^*(m,n,Si), j) = exc(m,n,j)$	8-59 ($\forall$I)
61.	$[(\forall j < i)\mathbb{e}xp(val^*(m,n,i), j) = exc(m,n,j)] \rightarrow [(\forall j < Si)\mathbb{e}xp(val^*(m,n,Si), j) = exc(m,n,j)]$	7-60 $\rightarrow$I
62.	$(\forall j < i)\mathbb{e}xp(val^*(m,n,i), j) = exc(m,n,j)$	6,61 IN

Exercise 13.33 T13.46.f

T13.46.g. PA $\vdash (\forall i < \mathbb{l}en(m))[\mathbb{e}xp(val^*(m,n,l),i) = \mathbb{e}xp(m,i)] \wedge (\forall i < \mathbb{l}en(n))[\mathbb{e}xp(val^*(m,n,l),i + \mathbb{l}en(m)) = \mathbb{e}xp(n,i)]$

1.	$l = \mathbb{l}en(m) + \mathbb{l}en(n)$	abv
2.	$(\forall j < l)\mathbb{e}xp(val^*(m,n,l), j) = exc(m,n,j)$	T13.46f
3.	$j < \mathbb{l}en(m) \rightarrow exc(m,n,j) = \mathbb{e}xp(m,j)$	T13.46b
4.	$\quad j < \mathbb{l}en(m)$	A (g ($\forall$I))
5.	$\quad exc(m,n,j) = \mathbb{e}xp(m,j)$	3,4 $\rightarrow$E
6.	$\quad \mathbb{l}en(m) \leq \mathbb{l}en(m) + \mathbb{l}en(n)$	T13.13u
7.	$\quad j < l$	4,6 T13.13c
8.	$\quad \mathbb{e}xp(val^*(m,n,l), j) = exc(m,n,j)$	2,7 ($\forall$E)
9.	$\quad \mathbb{e}xp(val^*(m,n,l), j) = \mathbb{e}xp(m,j)$	5,8 =E
10.	$(\forall i < \mathbb{l}en(m))\mathbb{e}xp(val^*(m,n,l), i) = \mathbb{e}xp(m,i)$	4-9 ($\forall$I)
11.	$j + \mathbb{l}en(m) \geq \mathbb{l}en(m) \rightarrow exc(m,n,j + \mathbb{l}en(m)) = \mathbb{e}xp(n,(j + \mathbb{l}en(m)) \dot{-} \mathbb{l}en(m))$	T13.46c
12.	$\quad j < \mathbb{l}en(n)$	A (g ($\forall$I))
13.	$\quad j + \mathbb{l}en(m) \geq \mathbb{l}en(m)$	T13.13u
14.	$\quad exc(m,n,j + \mathbb{l}en(m)) = \mathbb{e}xp(n,(j + \mathbb{l}en(m)) \dot{-} \mathbb{l}en(m))$	11,12 $\rightarrow$E
15.	$\quad j + \mathbb{l}en(m) = \mathbb{l}en(m) + [(j + \mathbb{l}en(m)) \dot{-} \mathbb{l}en(m)]$	13 T13.23a
16.	$\quad j = (j + \mathbb{l}en(m)) \dot{-} \mathbb{l}en(m)$	15 T6.68
17.	$\quad exc(m,n,j + \mathbb{l}en(m)) = \mathbb{e}xp(n,j)$	14,16 =E
18.	$\quad j + \mathbb{l}en(m) < \mathbb{l}en(n) + \mathbb{l}en(m)$	12 T13.13w
19.	$\quad j + \mathbb{l}en(m) < l$	1,18 =E
20.	$\quad \mathbb{e}xp(val^*(m,n,l), j + \mathbb{l}en(m)) = exc(m,n,j + \mathbb{l}en(m))$	2,19 ($\forall$E)
21.	$\quad \mathbb{e}xp(val^*(m,n,l), j + \mathbb{l}en(m)) = \mathbb{e}xp(n,j)$	20,17 =E
22.	$(\forall i < \mathbb{l}en(n))\mathbb{e}xp(val^*(m,n,l), i + \mathbb{l}en(m)) = \mathbb{e}xp(n,i)$	12-21 ($\forall$I)
23.	$(\forall i < \mathbb{l}en(m))[\mathbb{e}xp(val^*(m,n,l),i) = \mathbb{e}xp(m,i)] \wedge (\forall i < \mathbb{l}en(n))[\mathbb{e}xp(val^*(m,n,l),i + \mathbb{l}en(m)) = \mathbb{e}xp(n,i)]$	10,22 $\wedge$I

T13.46.h. PA $\vdash i \leq l \rightarrow [\mathbb{p}i(l)^{m+n}]^i \geq val^*(m,n,i)$

1.	$l = \mathbb{l}en(m) + \mathbb{l}en(n)$	abv
2.	$\overline{1} \geq \overline{1}$	T8.14
3.	$[\mathbb{p}i(l)^{m+n}]^{\emptyset} = \overline{1}$	T13.41a
4.	$val^*(m,n,\emptyset) = \overline{1}$	def val^*
5.	$[\mathbb{p}i(l)^{m+n}]^{\emptyset} \geq val^*(m,n,\emptyset)$	2,3,4 =E
6.	$\emptyset \not\leq l \vee [\mathbb{p}i(l)^{m+n}]^{\emptyset} \geq val^*(m,n,\emptyset)$	5 ∨I
7.	$\emptyset \leq l \rightarrow [\mathbb{p}i(l)^{m+n}]^{\emptyset} \geq val^*(m,n,\emptyset)$	6 Impl
8.	$i \leq l \rightarrow [\mathbb{p}i(l)^{m+n}]^{i} \geq val^*(m,n,i)$	A (g →I)
9.	$Si \leq l$	A (g →I)
10.	$i < l$	9 T13.13l
11.	$i \leq l$	10 T13.13m
12.	$[\mathbb{p}i(l)^{m+n}]^{i} \geq val^*(m,n,i)$	8,11 →E
13.	$[\mathbb{p}i(l)^{m+n}]^{Si} = [\mathbb{p}i(l)^{m+n}]^{i} \times \mathbb{p}i(l)^{m+n}$	T13.41a
14.	$val^*(m,n,Si) = val^*(m,n,i) \times \mathbb{p}i(i)^{exc(m,n,i)}$	def val^*
15.	$\mathbb{p}i(i) < \mathbb{p}i(l)$	10 T13.43k
16.	$i < \mathbb{l}en(m) \vee i \geq \mathbb{l}en(m)$	T14.13q
17.	$i < \mathbb{l}en(m)$	A (g 16∨E)
18.	$exc(m,n,i) = \mathbb{e}xp(m,i)$	17 T13.46b
19.	$\mathbb{e}xp(m,i) \leq m$	T13.44g
20.	$exc(m,n,i) \leq m$	18,19 =E
21.	$m \leq m+n$	T13.13u
22.	$exc(m,n,i) \leq m+n$	20,21 T13.13a
23.	$i \geq \mathbb{l}en(m)$	A (g 16∨E)
24.	$exc(m,n,i) = \mathbb{e}xp(n, i \dot{-} \mathbb{l}en(m))$	23 T13.46c
25.	$\mathbb{e}xp(n, i \dot{-} \mathbb{l}en(m)) \leq n$	T13.44g
26.	$exc(m,n,i) \leq n$	24,25 =E
27.	$n \leq m+n$	T13.13u
28.	$exc(m,n,i) \leq m+n$	26,27 T13.13a
29.	$exc(m,n,i) \leq m+n$	16,17-22,23-28 ∨E
30.	$\mathbb{p}i(i)^{exc(m,n,i)} \leq \mathbb{p}i(l)^{exc(m,n,i)}$	15 T13.41f
31.	$\mathbb{p}i(l) > \emptyset$	with T13.43g
32.	$\mathbb{p}i(l)^{exc(m,n,i)} \leq \mathbb{p}i(l)^{m+n}$	29,31 T13.41j
33.	$\mathbb{p}i(i)^{exc(m,n,i)} \leq \mathbb{p}i(l)^{m+n}$	30,32 T13.13a
34.	$val^*(m,n,i) \times \mathbb{p}i(i)^{exc(m,n,i)} \leq val^*(m,n,i) \times \mathbb{p}i(l)^{m+n}$	33 T13.13aa
35.	$val^*(m,n,i) \times \mathbb{p}i(l)^{m+n} \leq [\mathbb{p}i(l)^{m+n}]^{i} \times \mathbb{p}i(l)^{m+n}$	12 T13.13aa
36.	$val^*(m,n,i) \times \mathbb{p}i(i)^{exc(m,n,i)} \leq [\mathbb{p}i(l)^{m+n}]^{i} \times \mathbb{p}i(l)^{m+n}$	34,35 T13.13a
37.	$[\mathbb{p}i(l)^{m+n}]^{Si} \geq val^*(m,n,Si)$	13,14,36 =E
38.	$Si \leq l \rightarrow [\mathbb{p}i(l)^{m+n}]^{Si} \geq val^*(m,n,Si)$	9-37 →I
39.	$[i \leq l \rightarrow [\mathbb{p}i(l)^{m+n}]^{i} \geq val^*(m,n,i)] \rightarrow [Si \leq l \rightarrow [\mathbb{p}i(l)^{m+n}]^{Si} \geq val^*(m,n,Si)]$	8-38 →I
40.	$i \leq l \rightarrow [\mathbb{p}i(l)^{m+n}]^{i} \geq val^*(m,n,i)$	7,39 IN
41.	$l \leq l$	T13.13m
42.	$[\mathbb{p}i(l)^{m+n}]^{l} \geq val^*(m,n,l)$	40,41 (∀E)

T13.46.n. PA $\vdash \forall x \forall n[\mathbb{l}en(Sn) \leq x \rightarrow val(Sn,x) = Sn]$

Exercise 13.33 T13.46.n

1.	$\mathbb{l}en(Sa) \leq \emptyset$	A (g →I)
2.	$\mathbb{l}en(Sa) \not> \emptyset$	1 T13.13r
3.	$Sa \not> \bar{1}$	2 T13.45j
4.	$Sa \leq \bar{1}$	3 T13.13r
5.	$a \geq \emptyset$	T13.13d
6.	$Sa \geq \bar{1}$	5 T13.13j
7.	$Sa = \bar{1}$	4,6 T13.13t
8.	$val(\bar{1}, \emptyset) = \bar{1}$	def
9.	$val(Sa, \emptyset) = Sa$	8,7 =E
10.	$\mathbb{l}en(Sa) \leq \emptyset \rightarrow val(Sa, \emptyset) = Sa$	1-9 →I
11.	$\forall n[\mathbb{l}en(Sn) \leq \emptyset \rightarrow val(Sn, \emptyset) = Sn]$	10 ∀I
12.	$\forall n[\mathbb{l}en(Sn) \leq x \rightarrow val(Sn, x) = Sn]$	A (g →I)
13.	$\mathbb{l}en(Sa) \leq x \rightarrow val(Sa, x) = Sa$	12 ∀E
14.	$val(Sa, Sx) = val(Sa, x) \times \mathbb{p}i(x)^{\mathbb{e}xp(Sa,x)}$	def
15.	$\mathbb{l}en(Sa) \leq Sx$	A (g →I)
16.	$\mathbb{l}en(Sa) \leq x \vee \mathbb{l}en(Sa) = Sx$	15 T13.13m
17.	$\mathbb{l}en(Sa) \leq x$	A (g 16∨E)
18.	$val(Sa, x) = Sa$	13,17 →E
19.	$\mathbb{e}xp(Sa, x) = \emptyset$	17 T13.45h
20.	$\mathbb{p}i(x)^{\emptyset} = \bar{1}$	T13.20a
21.	$\mathbb{p}i(x)^{\mathbb{e}xp(Sa,x)} = \bar{1}$	20,19 =E
22.	$val(Sa, Sx) = Sa \times \bar{1}$	14,18,21 =E
23.	$val(Sa, Sx) = Sa$	22 T6.57
24.	$\mathbb{l}en(Sa) = Sx$	A (g 16∨E)
25.	$\exists q[\mathbb{p}i(x)^{\mathbb{e}xp(Sa,x)} \times q = Sa \wedge pred(\mathbb{p}i(x)) \nmid q \wedge \forall y(y \neq x \rightarrow \mathbb{e}xp(q, y) = \mathbb{e}xp(Sa, y))]$	T13.44l
26.	$\mathbb{p}i(x)^{\mathbb{e}xp(Sa,x)} \times q = Sa \wedge pred(\mathbb{p}i(x)) \nmid q \wedge \forall y(y \neq x \rightarrow \mathbb{e}xp(q, y) = \mathbb{e}xp(Sa, y))$	A (g 25∃E)
27.	$\mathbb{p}i(x)^{\mathbb{e}xp(Sa,x)} \times q = Sa$	26 ∧E
28.	$pred(\mathbb{p}i(x)) \nmid q$	26 ∧E
29.	$\forall y(y \neq x \rightarrow \mathbb{e}xp(q, y) = \mathbb{e}xp(Sa, y))$	26 ∧E
30.	$q > \emptyset$	27 T13.13ab
31.	$\exists r(q = Sr)$	30 T6.50
32.	$q = Sr$	A (g 31∃E)
33.	$\forall y(y \neq x \rightarrow \mathbb{e}xp(Sr, y) = \mathbb{e}xp(Sa, y))$	29,32 =E
34.	$\mathbb{l}en(Sr) > x$	A (c ∼I)
35.	$\sim(\forall z \leq Sr)[z \geq x \rightarrow \mathbb{e}xp(Sr, z) = \emptyset]$	34 T13.45e
36.	$l \leq Sr$	A (g (∀I))
37.	$l \geq x$	A (g →I)
38.	$l > x \vee l = x$	37 T13.13
39.	$l > x$	A (g 38∨E)
40.	$l \neq x$	39 T13.13s
41.	$\mathbb{e}xp(Sr, l) = \mathbb{e}xp(Sa, l)$	33,40 ∀E
42.	$l \geq Sx$	39 T13.13l
43.	$l \geq \mathbb{l}en(Sa)$	42,24 =E
44.	$\mathbb{e}xp(Sa, l) = \emptyset$	43 T13.45l
45.	$\mathbb{e}xp(Sr, l) = \emptyset$	44,41 =E
46.	$l = x$	A (g 38∨E)
47.	$pred(\mathbb{p}i(x)) \nmid Sr$	28,32 =E
48.	$\mathbb{e}xp(Sr, x) = \emptyset$	47 T13.44k
49.	$\mathbb{e}xp(Sr, l) = \emptyset$	48,46 =E
50.	$\mathbb{e}xp(Sr, l) = \emptyset$	38,39-45,46-49 ∨E
51.	$l \geq x \rightarrow \mathbb{e}xp(Sr, l) = \emptyset$	37-50 →I
52.	$(\forall z \leq Sr)[z \geq x \rightarrow \mathbb{e}xp(Sr, z) = \emptyset]$	36-51 (∀I)
53.	$\perp$	35,52 ⊥I
54.	$\mathbb{l}en(Sr) \not> x$	34-53 ∼I
55.	$\mathbb{l}en(Sr) \leq x$	54 T13.13r

Exercise 13.33 T13.46.n

56.	$val(Sr, x) = Sr$	12,55 ∀E
57.	$l < x$	A (g (∀I))
58.	$l \neq x$	57 T13.13s
59.	$exp(Sr, l) = exp(Sa, l)$	33,58 ∀E
60.	$(\forall i < x)exp(Sr, i) = exp(Sa, i)$	57-59 (∀I)
61.	$val(Sr, x) = val(Sa, x)$	60 T13.46m
62.	$pi(x)^{exp(Sa,x)} \times Sr = Sa$	27,32 =E
63.	$val(Sa, x) \times pi(x)^{exp(Sa,x)} = Sa$	62,56,61 =E
64.	$val(Sa, Sx) = Sa$	14,63 =E
65.	$val(Sa, Sx) = Sa$	31,32-64 ∃E
66.	$val(Sa, Sx) = Sa$	25,26-65 ∃E
67.	$val(Sa, Sx) = Sa$	16,17-23,24-66 ∨E
68.	$len(Sa) \leq Sx \rightarrow val(Sa, Sx) = Sa$	15-67 →I
69.	$\forall n[len(Sn) \leq Sx \rightarrow val(Sn, Sx) = Sn]$	68 ∀I
70.	$\forall n[len(Sn) \leq x \rightarrow val(Sn, x) = Sn)] \rightarrow \forall n[len(Sn) \leq Sx \rightarrow val(Sn, Sx) = Sn]$	12-69 →I
71.	$\forall x \forall n[len(Sn) \leq x \rightarrow val(Sn, x) = Sn]$	11,70 IN

T13.46.o. $[len(n) \leq q \wedge (\forall k < len(n))exp(n, k) \leq r] \rightarrow [pi(q)^r]^q \geq val(n, len(n))$

1.	$\mathbb{l}en(n) \leq q \wedge (\forall k < len(n))\mathbb{e}xp(n,k) \leq r$	A (g →I)
2.	$\mathbb{l}en(n) \leq q$	1 ∧E
3.	$(\forall k < len(n))\mathbb{e}xp(n,k) \leq r$	1 ∧E
4.	$[\mathbb{p}i(q)^r]^{\emptyset} = \bar{1}$	T13.41a
5.	$val(n,\emptyset) = \bar{1}$	def
6.	$[\mathbb{p}i(q)^r]^{\emptyset} \geq val(n,\emptyset)$	4,5 T13.13m
7.	$\emptyset \leq q \rightarrow [\mathbb{p}i(q)^r]^{\emptyset} \geq val(n,\emptyset)$	6 ∨I
8.	$i \leq q \rightarrow [\mathbb{p}i(q)^r]^i \geq val(n,i)$	A (g →I)
9.	$Si \leq q$	A (g →I)
10.	$i \leq q$	9 T13.13l,m
11.	$val(n,Si) = val(n,i) \times \mathbb{p}i(i)^{\mathbb{e}xp(n,i)}$	def
12.	$[\mathbb{p}i(q)^r]^{Si} = [\mathbb{p}i(q)^r]^i \times \mathbb{p}i(q)^r$	T13.41a
13.	$[\mathbb{p}i(q)^r]^i \geq val(n,i)$	8,10 →E
14.	$\mathbb{p}i(i) \leq \mathbb{p}i(q)$	10 T13.43k
15.	$i < \mathbb{l}en(n) \vee i \geq \mathbb{l}en(n)$	T13.13q
16.	$i < \mathbb{l}en(n)$	A (g 15∨E)
17.	$\mathbb{e}xp(n,i) \leq r$	3,16 (∀E)
18.	$i \geq \mathbb{l}en(n)$	A (g 15∨E)
19.	$\mathbb{e}xp(n,i) = \emptyset$	18 T13.45l
20.	$\emptyset \leq r$	T13.13d
21.	$\mathbb{e}xp(n,i) \leq r$	20,19 =E
22.	$\mathbb{e}xp(n,i) \leq r$	15,16-17,18-21 ∨E
23.	$\mathbb{p}i(i) > \bar{1}$	T13.43g
24.	$\mathbb{p}i(i)^{\mathbb{e}xp(n,i)} \leq \mathbb{p}i(i)^r$	22,23 T13.41j
25.	$\mathbb{p}i(i)^r \leq \mathbb{p}i(q)^r$	14 T13.41f
26.	$\mathbb{p}i(i)^{\mathbb{e}xr(n,i)} \leq \mathbb{p}i(q)^r$	24,25 T13.13a
27.	$val(n,i) \times \mathbb{p}i(i)^{\mathbb{e}xp(n,i)} \leq val(n,i) \times \mathbb{p}i(q)^r$	26 T13.13aa
28.	$val(n,i) \times \mathbb{p}i(q)^r \leq [\mathbb{p}i(q)^r]^i \times \mathbb{p}i(q)^r$	13 T13.13aa
29.	$val(n,i) \times \mathbb{p}i(i)^{\mathbb{e}xp(n,i)} \leq [\mathbb{p}i(q)^r]^i \times \mathbb{p}i(q)^r$	27,28 T13.13a
30.	$[\mathbb{p}i(q)^r]^{Si} \geq val(n,Si)$	29,11,12 =E
31.	$Si \leq q \rightarrow [\mathbb{p}i(q)^r]^{Si} \geq val(n,Si)$	9-30 →I
32.	$\{i \leq q \rightarrow [\mathbb{p}i(q)^r]^i \geq val(n,i)\} \rightarrow \{Si \leq q \rightarrow [\mathbb{p}i(q)^r]^{Si} \geq val(n,Si)\}$	8-31 →I
33.	$i \leq q \rightarrow [\mathbb{p}i(q)^r]^i \geq val(n,i)$	7,32 IN
34.	$[\mathbb{p}i(q)^r]^{\mathbb{l}en(n)} \geq val(n,\mathbb{l}en(n))$	2,33 →E
35.	$\mathbb{p}i(q)^r > \emptyset$	T13.43h
36.	$[\mathbb{p}i(q)^r]^{\mathbb{l}en(n)} \leq [\mathbb{p}i(q)^r]^q$	35,2 T13.41j
37.	$[\mathbb{p}i(q)^r]^q \geq val(n,\mathbb{l}en(n))$	34,36 T13.13a
38.	$[\mathbb{l}en(n) \leq q \wedge (\forall k < len(n))\mathbb{e}xp(n,k) \leq r] \rightarrow [\mathbb{p}i(q)^r]^q \geq val(n,\mathbb{l}en(n))$	1-37 →I

E13.34. Show each of the results from T13.47.

T13.47.

T13.47.e. PA ⊢ $\mathbb{l}en(m * n) \geq l$

1.	$l = \mathbb{l}en(m) + \mathbb{l}en(n)$	abv
2.	$\mathbb{l}en(n) = \emptyset \vee \mathbb{l}en(n) > \emptyset$	T13.13f
3.	$\mathbb{l}en(n) = \emptyset$	A (g 2$\vee$E)
4.	$\mathbb{l}en(m) = \emptyset \vee \mathbb{l}en(m) > \emptyset$	T13.13f
5.	$\mathbb{l}en(m) = \emptyset$	A (g 4 $\vee$E)
6.	$\emptyset + \emptyset = \emptyset$	T6.41
7.	$\mathbb{l}en(m * n) \geq \emptyset$	T13.13d
8.	$\mathbb{l}en(m * n) \geq \emptyset + \emptyset$	6,7 =E
9.	$\mathbb{l}en(m * n) \geq l$	8,5,3 =E
10.	$\mathbb{l}en(m) > \emptyset$	A (g 4$\vee$E)
11.	$\exists v[\mathbb{l}en(m) = Sv]$	10 T13.13g
12.	$\mathbb{l}en(m) = Sa$	A (g 11$\exists$E)
13.	$\mathbb{e}xp(m, a) > \emptyset$	12 with T13.45m
14.	$a < \mathbb{l}en(m)$	12 T13.13i
15.	$(\forall i < \mathbb{l}en(m))\mathbb{e}xp(m * n, i) = \mathbb{e}xp(m, i)$	T13.47c
16.	$\mathbb{e}xp(m * n, a) = \mathbb{e}xp(m, a)$	15,14 ($\forall$E)
17.	$\mathbb{e}xp(m * n, a) > \emptyset$	13,16 =E
18.	$\mathbb{l}en(m * n) > a$	17 T13.45h
19.	$\mathbb{l}en(m * n) \geq Sa$	18 T13.13l
20.	$\mathbb{l}en(m * n) \geq \mathbb{l}en(m)$	19,12 =E
21.	$\mathbb{l}en(m) + \emptyset = \mathbb{l}en(m)$	T6.41
22.	$l = \mathbb{l}en(m)$	21,3 =E
23.	$\mathbb{l}en(m * n) \geq l$	20,22 =E
24.	$\mathbb{l}en(m * n) \geq l$	11,12-23 $\exists$E
25.	$\mathbb{l}en(m * n) \geq l$	4,5-9,10-24 $\vee$E
26.	$\mathbb{l}en(n) > \emptyset$	A (g 2$\vee$E)
27.	$\exists v[\mathbb{l}en(n) = Sv]$	26 T13.13g
28.	$\mathbb{l}en(n) = Sa$	A (g 27$\exists$E)
29.	$\mathbb{e}xp(n, a) > \emptyset$	28 with T13.45m
30.	$a < \mathbb{l}en(n)$	28 T13.13i
31.	$(\forall i < \mathbb{l}en(n))\mathbb{e}xp(m * n, i + \mathbb{l}en(m)) = \mathbb{e}xp(n, i)$	T13.47c
32.	$\mathbb{e}xp(m * n, a + \mathbb{l}en(m)) = \mathbb{e}xp(n, a)$	31,30 ($\forall$E)
33.	$\mathbb{e}xp(m * n, a + \mathbb{l}en(m)) > \emptyset$	29,32 =E
34.	$\mathbb{l}en(m * n) > a + \mathbb{l}en(m)$	33 T13.45h
35.	$\mathbb{l}en(m * n) \geq S(a + \mathbb{l}en(m))$	34 T13.13l
36.	$S(a + \mathbb{l}en(m)) = Sa + \mathbb{l}en(m)$	T6.53
37.	$S(a + \mathbb{l}en(m)) = l$	36,28 =E
38.	$\mathbb{l}en(m * n) \geq l$	35,37 =E
39.	$\mathbb{l}en(m * n) \geq l$	27,28-38 $\exists$E
40.	$\mathbb{l}en(m * n) \geq l$	2,3-25,26-39 $\vee$E

T13.47.f. PA $\vdash \mathbb{l}en(m * n) = l$

1.	$l = \mathbb{l}en(m) + \mathbb{l}en(n)$	abv
2.	$\mathbb{l}en(m * n) \geq l$	T13.47e
3.	$\mathbb{l}en(m * n) \not\leq l$	A (c ∼E)
4.	$\mathbb{l}en(m * n) > l$	3 T13.13r
5.	$l \geq \emptyset$	T13.13d
6.	$\mathbb{l}en(m * n) > \emptyset$	4,5 T13.13c
7.	$m * n > \overline{1}$	6 T13.45g
8.	$\overline{1} > \emptyset$	T8.14
9.	$m * n > \emptyset$	7,8 T13.13b
10.	$\exists v[m * n = Sv]$	9 T13.13g
11.	$m * n = Sp$	A (c 10∃E)
12.	$\mathbb{l}en(Sp) > l$	4,11 =E
13.	$\exists v[Sv + l = \mathbb{l}en(Sp)]$	12 def
14.	$Sa + l = \mathbb{l}en(Sp)$	A (c 13∃E)
15.	$S(a + l) = Sa + l$	T6.53
16.	$S(a + l) = \mathbb{l}en(Sp)$	14,15 =E
17.	$\mathbb{e}xp(Sp, a + l) \geq \overline{1}$	16 T13.45m
18.	$\exists q[\mathbb{p}i(a + l)^{\mathbb{e}xp(Sp,a+l)} \times q = Sp \wedge \forall y(y \neq a + l \rightarrow \mathbb{e}xp(q, y) = \mathbb{e}xp(Sp, y))]$	T13.44l
19.	$\mathbb{p}i(a + l)^{\mathbb{e}xp(Sp,a+l)} \times j = Sp \wedge \forall y(y \neq a + l \rightarrow \mathbb{e}xp(j, y) = \mathbb{e}xp(Sp, y))$	A (c 18∃E)
20.	$\mathbb{p}i(a + l)^{\mathbb{e}xp(Sp,a+l)} \times j = Sp$	19 ∧E
21.	$\mathbb{p}i(a + l)^{\mathbb{e}xp(Sp,a+l)} \geq \mathbb{p}i(a + l)$	17 with T13.41l
22.	$\mathbb{p}i(a + l) > \overline{1}$	T13.43g
23.	$\mathbb{p}i(a + l)^{\mathbb{e}xp(Sp,a+l)} > \overline{1}$	21,22 T13.13c
24.	$Sp > \emptyset$	T13.13e
25.	$\mathbb{p}i(a + l)^{\mathbb{e}xp(Sp,a+l)} \times j > \emptyset$	24,20 =E
26.	$j > \emptyset$	25 T13.13ab
27.	$\mathbb{p}i(a + l)^{\mathbb{e}xp(Sp,a+l)} \times j > j$	23,26 T13.13ac
28.	$j < Sp$	20,27 =E

29.	$\forall y(y \neq a + l \rightarrow \mathit{exp}(j, y) = \mathit{exp}(Sp, y))$	19 ∧E
30.	$b < \mathit{len}(m)$	A (g (∀I))
31.	$(\forall i < \mathit{len}(m))\mathit{exp}(m * n, i) = \mathit{exp}(m, i)$	T13.47c
32.	$\mathit{exp}(m * n, b) = \mathit{exp}(m, b)$	31,30 (∀E)
33.	$\mathit{exp}(Sp, b) = \mathit{exp}(m, b)$	11,32 =E
34.	$\mathit{len}(m) \leq a + l$	T13.13u
35.	$b < a + l$	30,34 T13.13c
36.	$b \neq a + l$	35 T13.13s
37.	$b \neq a + l \rightarrow \mathit{exp}(j, b) = \mathit{exp}(Sp, b)$	29 ∀E
38.	$\mathit{exp}(j, b) = \mathit{exp}(Sp, b)$	37,36 →E
39.	$\mathit{exp}(j, b) = \mathit{exp}(m, b)$	33,38 =E
40.	$(\forall i < \mathit{len}(m))\mathit{exp}(j, i) = \mathit{exp}(m, i)$	30-39 (∀I)
41.	$b < \mathit{len}(n)$	A (g (∀I))
42.	$(\forall i < \mathit{len}(n))\mathit{exp}(m * n, i + \mathit{len}(m)) = \mathit{exp}(n, i)$	T13.47c
43.	$\mathit{exp}(m * n, b + \mathit{len}(m)) = \mathit{exp}(n, b)$	42,41 (∀E)
44.	$\mathit{exp}(Sp, b + \mathit{len}(m)) = \mathit{exp}(n, b)$	43,11 =E
45.	$\mathit{len}(m) \leq a + \mathit{len}(m)$	T13.13u
46.	$b + \mathit{len}(m) < a + l$	41,45 T13.13y
47.	$b + \mathit{len}(m) \neq a + l$	46 T13.13s
48.	$b + \mathit{len}(m) \neq a + l \rightarrow \mathit{exp}(j, b + \mathit{len}(m)) = \mathit{exp}(Sp, b + \mathit{len}(m))$	29 ∀E
49.	$\mathit{exp}(j, b + \mathit{len}(m)) = \mathit{exp}(Sp, b + \mathit{len}(m))$	48,47 →E
50.	$\mathit{exp}(j, b + \mathit{len}(m)) = \mathit{exp}(n, b)$	44,49 =E
51.	$(\forall i < \mathit{len}(n))\mathit{exp}(j, i + \mathit{len}(m)) = \mathit{exp}(n, i)$	41-50 (∀I)
52.	$(\forall i < \mathit{len}(m))\mathit{exp}(j, i) = \mathit{exp}(m, i) \wedge (\forall i < \mathit{len}(n))\mathit{exp}(j, i + \mathit{len}(m)) = \mathit{exp}(n, i)$	40,51 ∧I
53.	$(\forall w < m * n)\sim[(\forall i < \mathit{len}(m))\mathit{exp}(w, i) = \mathit{exp}(m, i) \wedge (\forall i < \mathit{len}(n))\mathit{exp}(w, i + \mathit{len}(m)) = \mathit{exp}(n, i)]$	T13.47d
54.	$(\forall w < Sp)\sim[(\forall i < \mathit{len}(m))\mathit{exp}(w, i) = \mathit{exp}(m, i) \wedge (\forall i < \mathit{len}(n))\mathit{exp}(w, i + \mathit{len}(m)) = \mathit{exp}(n, i)]$	53,11 =E
55.	$\sim[(\forall i < \mathit{len}(m))\mathit{exp}(j, i) = \mathit{exp}(m, i) \wedge (\forall i < \mathit{len}(n))\mathit{exp}(j, i + \mathit{len}(m)) = \mathit{exp}(n, i)]$	54,28 (∀E)
56.	$\bot$	52,55 ⊥I
57.	$\bot$	18,19-56 ∃E
58.	$\bot$	13,14-57 ∃E
59.	$\bot$	10,11-58 ∃E
60.	$\mathit{len}(m * n) \leq l$	3-59 ∼E
61.	$\mathit{len}(m * n) = l$	2,60 T13.13t

T13.47.m. PA $\vdash \mathit{val}(Sm * Sn, a) = \mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))$

Exercise 13.34 T13.47.m

1.	$i < a$	A (g ($\forall$I))
2.	$a < \mathit{len}(Sm) \vee a \geq \mathit{len}(Sm)$	T13.13q
3.	$a < \mathit{len}(Sm)$	A (g 2$\vee$E)
4.	$i < \mathit{len}(Sm)$	1,3 T13.13b
5.	$\mathit{exp}(Sm * Sn, i) = \mathit{exp}(Sm, i)$	4 T13.47c
6.	$a \dot{-} \mathit{len}(Sm) = \emptyset$	3 T13.23b
7.	$\mathit{val}(Sn, a \dot{-} \mathit{len}(m)) = \overline{1}$	6 def
8.	$\mathit{val}(Sm, a) > \emptyset$	T13.46i
9.	$\mathit{val}(Sm, a) = \mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))$	7,8 T13.47i
10.	$\mathit{exp}(\mathit{val}(Sm, a), i) = \mathit{exp}(Sm, i)$	1 T13.46l
11.	$\mathit{exp}(Sm * Sn, i) = \mathit{exp}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), i)$	5,10,9 =E
12.	$a \geq \mathit{len}(Sm)$	A (g 2$\vee$E)
13.	$\mathit{val}(Sm, a) = Sm$	12 T13.46n
14.	$\mathit{len}(\mathit{val}(Sm, a)) = \mathit{len}(Sm)$	13 =E
15.	$i < \mathit{len}(Sm) \vee i \geq \mathit{len}(Sm)$	T13.13q
16.	$i < \mathit{len}(Sm)$	A (g 15$\vee$E)
17.	$\mathit{exp}(Sm * Sn, i) = \mathit{exp}(Sm, i)$	16 T13.47c
18.	$i < \mathit{len}(\mathit{val}(Sm, a))$	16,14 =E
19.	$\mathit{exp}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), i) = \mathit{exp}(\mathit{val}(Sm, a), i)$	18 T13.47c
20.	$\mathit{exp}(\mathit{val}(Sm, a), i) = \mathit{exp}(Sm, i)$	1 T13.46l
21.	$\mathit{exp}(Sm * Sn, i) = \mathit{exp}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), i)$	17,20,19 =E
22.	$i \geq \mathit{len}(Sm)$	A (g 15$\vee$E)
23.	$\mathit{exp}(Sm * Sn, (i \dot{-} \mathit{len}(Sm)) + \mathit{len}(Sm)) = \mathit{exp}(Sn, i \dot{-} \mathit{len}(Sm))$	T13.47g
24.	$i = \mathit{len}(Sm) + (i \dot{-} \mathit{len}(Sm))$	22 T13.23a
25.	$\mathit{exp}(Sm * Sn, i) = \mathit{exp}(Sn, i \dot{-} \mathit{len}(Sm))$	23,24 =E
26.	$\mathit{exp}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), (i \dot{-} \mathit{len}(Sm)) + \mathit{len}(\mathit{val}(Sm, a))) =$ $\mathit{exp}(\mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), i \dot{-} \mathit{len}(Sm))$	T13.47g
27.	$\mathit{exp}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), i) = \mathit{exp}(\mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), i \dot{-} \mathit{len}(Sm))$	26,24,14 =E
28.	$a \dot{-} \mathit{len}(Sm) > i \dot{-} \mathit{len}(Sm)$	22,1 T13.23e
29.	$\mathit{exp}(\mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), i \dot{-} \mathit{len}(Sm)) = \mathit{exp}(Sn, i \dot{-} \mathit{len}(Sm))$	28 T13.46l
30.	$\mathit{exp}(Sm * Sn, i) = \mathit{exp}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), i)$	25,29,27 =E
31.	$\mathit{exp}(Sm * Sn, i) = \mathit{exp}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), i)$	15,16-21,22-30 $\vee$E
32.	$\mathit{exp}(Sm * Sn, i) = \mathit{exp}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), i)$	2,3-11,12-31 $\vee$E
33.	$(\forall i < a)\mathit{exp}(Sm * Sn, i) = \mathit{exp}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), i)$	1-32 ($\forall$I)
34.	$\mathit{val}(Sm * Sn, a) = \mathit{val}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), a)$	33 T13.46m
35.	$\mathit{len}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))) = \mathit{len}(\mathit{val}(Sm, a)) + \mathit{len}(\mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)))$	T13.47f
36.	$a < \mathit{len}(Sm) \vee a \geq \mathit{len}(Sm)$	T13.13q
37.	$a < \mathit{len}(Sm)$	A (g 36$\vee$E)
38.	$\mathit{len}(\mathit{val}(Sm, a)) \leq a$	T13.46j
39.	$a \dot{-} \mathit{len}(Sm) = \emptyset$	37 T13.23b
40.	$\mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)) = \overline{1}$	39 def
41.	$\mathit{len}(\mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))) = \emptyset$	40 T13.45f
42.	$\mathit{len}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))) = \mathit{len}(\mathit{val}(Sm, a))$	35,41 =E
43.	$\mathit{len}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))) \leq a$	38,42 =E
44.	$a \geq \mathit{len}(Sm)$	A (g 36$\vee$E)
45.	$\mathit{len}(\mathit{val}(Sm, a)) \leq \mathit{len}(Sm)$	T13.46k
46.	$\mathit{len}(\mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))) \leq a \dot{-} \mathit{len}(Sm)$	T13.46j
47.	$\mathit{len}(\mathit{val}(Sm, a)) + \mathit{len}(\mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))) \leq \mathit{len}(Sm) + (a \dot{-} \mathit{len}(Sm))$	45,46 T13.13v
48.	$a = \mathit{len}(Sm) + (a \dot{-} \mathit{len}(Sm))$	44 T13.23a
49.	$\mathit{len}(\mathit{val}(Sm, a)) + \mathit{len}(\mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))) \leq a$	47,48 =E
50.	$\mathit{len}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))) \leq a$	35,49 =E
51.	$\mathit{len}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))) \leq a$	36,37-43,44-50 $\vee$E
52.	$\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)) \geq \overline{1}$	T13.47c
53.	$\mathit{val}(\mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm)), a) = \mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))$	51 T13.46n
54.	$\mathit{val}(Sm * Sn, a) = \mathit{val}(Sm, a) * \mathit{val}(Sn, a \dot{-} \mathit{len}(Sm))$	34,53 =E

Exercise 13.34 T13.47.m

E13.35. Show (j) and the unfinished cases for the C disjunct in (l) and (n). Hard core: show each of the results from T13.48.

T13.48.

T13.48.i. PA $\vdash \mathbb{T}ermseq(m, t) \rightarrow \mathbb{T}ermseq(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, \overline{\ulcorner S \urcorner} * t)$

1.	$\mathbb{T}ermseq(m,t)$	A (g $\rightarrow$I)
2.	$\mathbb{e}xp(m,\mathbb{l}en(m) \dot{-} \overline{1}) = t$	1 T13.48a
3.	$m > \overline{1}$	1 T13.48a
4.	$(\forall k < \mathbb{l}en(m))[A(m,k) \vee B(m,k) \vee C(m,k) \vee D(m,k)]$	1 T13.48a
5.	$\mathbb{l}en(\overline{2}^{\ulcorner S\urcorner * t}) = \overline{1}$	T13.45k
6.	$\mathbb{e}xp(\overline{2}^{\ulcorner S\urcorner * t}, \emptyset) = \overline{\ulcorner S\urcorner} * t$	T13.44i
7.	$\mathbb{l}en(m * \overline{2}^{\ulcorner S\urcorner * t}) = \mathbb{l}en(m) + \overline{1}$	5 T13.47f
8.	$\mathbb{l}en(m) + \overline{1} = S\mathbb{l}en(m)$	T6.47
9.	$\mathbb{l}en(m) = S\mathbb{l}en(m) \dot{-} \overline{1}$	T13.23k
10.	$\mathbb{l}en(m) = \mathbb{l}en(m * \overline{2}^{\ulcorner S\urcorner * t}) \dot{-} \overline{1}$	9,7,8 =E
11.	$\mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, \mathbb{l}en(m)) = \overline{\ulcorner S\urcorner} * t$	6 T13.47c
12.	$\mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, \mathbb{l}en(m * \overline{2}^{\ulcorner S\urcorner * t}) \dot{-} \overline{1}) = \overline{\ulcorner S\urcorner} * t$	11,10 =E
13.	$\mathbb{l}en(m * \overline{2}^{\ulcorner S\urcorner * t}) > \emptyset$	7 T13.13u
14.	$m * \overline{2}^{\ulcorner S\urcorner * t} > \overline{1}$	13 T13.45g
15.	$a < \mathbb{l}en(m * \overline{2}^{\ulcorner S\urcorner * t})$	A (g ($\forall$I))
16.	$a < \mathbb{l}en(m) \vee a = \mathbb{l}en(m)$	15,7 T13.13n
17.	$a < \mathbb{l}en(m)$	A (g 16$\vee$E)
18.	$\mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, a) = \mathbb{e}xp(m,a))$	17 T13.47c
19.	$A(m,a) \vee B(m,a) \vee C(m,a) \vee D(m,a)$	4,17 ($\forall$E)
20.	$A(m,a)$	A (g 19$\vee$E)
21.	$\mathbb{e}xp(m,a) = \overline{\ulcorner \emptyset\urcorner} \vee \mathbb{V}ar(\mathbb{e}xp(m,a))$	20 abv
22.	$\mathbb{e}xp(m,a) = \overline{\ulcorner \emptyset\urcorner}$	A (g 21$\vee$E)
23.	$\mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, a) = \overline{\ulcorner \emptyset\urcorner}$	18,22 =E
24.	$\mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, a) = \overline{\ulcorner \emptyset\urcorner} \vee \mathbb{V}ar(\mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, a))$	23 $\vee$I
25.	$A(m * \overline{2}^{\ulcorner S\urcorner * t}, a)$	24 abv
26.	$\mathbb{V}ar(\mathbb{e}xp(m,a))$	A (g 21$\vee$E)
27.	$\mathbb{V}ar(\mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, a))$	18,26 =E
28.	$\mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, a) = \overline{\ulcorner \emptyset\urcorner} \vee \mathbb{V}ar(\mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, a))$	27 $\vee$I
29.	$A(m * \overline{2}^{\ulcorner S\urcorner * t}, a)$	28 abv
30.	$A(m * \overline{2}^{\ulcorner S\urcorner * t}, a)$	21,22-25,26-29$\vee$E
31.	$A(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee B(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee C(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee D(m * \overline{2}^{\ulcorner S\urcorner * t}, a)$	30 $\vee$I
32.	$B(m,a)$	A (g 19$\vee$E)
33.	$(\exists j < a)[\mathbb{e}xp(m,a) = \overline{\ulcorner S\urcorner} * \mathbb{e}xp(m,j)]$	32 abv
34.	$\mathbb{e}xp(m,a) = \overline{\ulcorner S\urcorner} * \mathbb{e}xp(m,j)$	A (g 33($\exists$E))
35.	$j < a$	
36.	$j < \mathbb{l}en(m)$	17,35 T13.13b
37.	$\mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, j) = \mathbb{e}xp(m,j))$	36 T13.47c
38.	$\mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, a) = \overline{\ulcorner S\urcorner} * \mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, j)$	34,18,37 =E
39.	$(\exists j < a)[\mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, a) = \overline{\ulcorner S\urcorner} * \mathbb{e}xp(m * \overline{2}^{\ulcorner S\urcorner * t}, j)]$	38,35 ($\exists$I)
40.	$B(m * \overline{2}^{\ulcorner S\urcorner * t}, a)$	39 abv
41.	$B(m * \overline{2}^{\ulcorner S\urcorner * t}, a)$	33,34-40 ($\exists$E)
42.	$A(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee B(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee C(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee D(m * \overline{2}^{\ulcorner S\urcorner * t}, a)$	41 $\vee$I
43.	$C(m,a)$	A (g 19$\vee$E)
44.	$A(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee B(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee C(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee D(m * \overline{2}^{\ulcorner S\urcorner * t}, a)$	similarly
45.	$m,a)$	A (g 19$\vee$E)
46.	$A(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee B(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee C(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee D(m * \overline{2}^{\ulcorner S\urcorner * t}, a)$	similarly
47.	$A(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee B(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee C(m * \overline{2}^{\ulcorner S\urcorner * t}, a) \vee D(m * \overline{2}^{\ulcorner S\urcorner * t}, a)$	19,20-46 $\vee$E

Exercise 13.35 T13.48.i

48. $a = \mathbb{len}(m)$ — A (g 16∨E)
49. $\mathbb{len}(m) > \emptyset$ — 3 T13.45j
50. $\mathbb{len}(m) \dot{-} \overline{1} < \mathbb{len}(m)$ — 49 T13.23i
51. $\mathbb{exp}(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, \mathbb{len}(m) \dot{-} \overline{1}) = \mathbb{exp}(m, \mathbb{len}(m) \dot{-} \overline{1})$ — 50 T13.47c
52. $\mathbb{exp}(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, \mathbb{len}(m) \dot{-} \overline{1}) = t$ — 51,2 =E
53. $\mathbb{exp}(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, a) = \overline{\ulcorner S \urcorner} * t$ — 11,48 =E
54. $\mathbb{exp}(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, a) = \overline{\ulcorner S \urcorner} * \mathbb{exp}(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, \mathbb{len}(m) \dot{-} \overline{1})$ — 52,53 =E
55. $(\exists j < a)[\mathbb{exp}(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, a) = \overline{\ulcorner S \urcorner} * \mathbb{exp}(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, j)]$ — 50,54 (∃I)
56. $B(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, a)$ — 55 abv
57. $A(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, a) \vee B(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, a) \vee C(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, a) \vee D(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, a)$ — 56 ∨I
58. $A(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, a) \vee B(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, a) \vee C(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, a) \vee D(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, a)$ — 16,17-47,48-57 ∨E
59. $(\forall k < \mathbb{len}(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}))[A(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, k) \vee B(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, k) \vee C(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, k) \vee D(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, k)]$ — 15-58 (∀I)
60. $\mathbb{T}ermseq(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, \overline{\ulcorner S \urcorner} * t)$ — 12,14,59 T13.48a
61. $\mathbb{T}ermseq(m, t) \to \mathbb{T}ermseq(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, \overline{\ulcorner S \urcorner} * t)$ — 1-60 →I

T13.48.l. PA $\vdash \mathbb{T}ermseq(m,t) \to \forall x(\forall k < \mathbb{len}(m))\{\mathbb{len}(\mathbb{exp}(m,k)) \leq x \to \exists n[Termseq(n, \mathbb{exp}(m,k)) \wedge (\forall i < \mathbb{len}(n))\mathbb{exp}(n,i) \leq \mathbb{exp}(m,k) \wedge \mathbb{len}(n) \leq \mathbb{len}(\mathbb{exp}(m,k)]\}$

Let $\mathscr{P}$ be the formula, $(\forall k < \mathbb{len}(m))\{\mathbb{len}(\mathbb{exp}(m,k)) \leq x \to \exists n[Termseq(n, \mathbb{exp}(m,k)) \wedge (\forall i < \mathbb{len}(n))\mathbb{exp}(n,i) \leq \mathbb{exp}(m,k) \wedge \mathbb{len}(n) \leq \mathbb{len}(\mathbb{exp}(m,k)]\}$

1. $\mathbb{T}ermseq(m,t)$ — A (g →I)
2. $\mathscr{P}^x_\emptyset$ — basis
3. $(\forall k < \mathbb{len}(m))\mathbb{exp}(m,k) > \overline{1}$ — 1 T13.48e
4. $\mathscr{P}$ — A g →I
5. $(\forall k < \mathbb{len}(m))\{\mathbb{len}(\mathbb{exp}(m,k)) \leq x \to \exists n[Termseq(n, \mathbb{exp}(m,k)) \wedge$
   $(\forall i < \mathbb{len}(n))\mathbb{exp}(n,i) \leq \mathbb{exp}(m,k) \wedge \mathbb{len}(n) \leq \mathbb{len}(\mathbb{exp}(m,k)]\}$ — 4 abv
6. $a < \mathbb{len}(m)$ — A (g (∀I))
7. $\mathbb{exp}(m,a) > \overline{1}$ — 3,6 (∀E)
8. $\mathbb{len}(\overline{2}^{\mathbb{exp}(m,a)}) = \overline{1}$ — 7 with T13.45k
9. $\mathbb{exp}(\overline{2}^{\mathbb{exp}(m,a)}, \emptyset) = \mathbb{exp}(m,a)$ — T13.44i
10. $\mathbb{len}(\mathbb{exp}(m,a)) \leq Sx$ — A (g →I)
11. $(\forall k < \mathbb{len}(m)[A(m,k) \vee B(m,k) \vee C(m,k) \vee D(m,k)]$ — 1 T13.48a
12. $A(m,a) \vee B(m,a) \vee C(m,a) \vee D(m,a)$ — 11,6 (∀E)
13. $A(m,a)$ — A (g 12 ∨E)
14. $\mathbb{exp}(m,a) = \overline{\ulcorner \emptyset \urcorner} \vee \mathbb{V}ar(\mathbb{exp}(m,a))$ — 13 abv
15. $\mathbb{T}ermseq(\overline{2}^{\mathbb{exp}(m,a)}, \mathbb{exp}(m,a))$ — 14 T13.48g,h
16. $b < \overline{1}$ — A (g (∀I))
17. $b = \emptyset$ — 16 with T8.16
18. $\mathbb{exp}(\overline{2}^{\mathbb{exp}(m,a)}, b) \leq \mathbb{exp}(m,a)$ — 9 T13.13m
19. $(\forall i < \mathbb{len}(\overline{2}^{\mathbb{exp}(m,a)}))\mathbb{exp}(\overline{2}^{\mathbb{exp}(m,a)}, i) \leq \mathbb{exp}(m,a)$ — 8,16-18 (∀I)
20. $\mathbb{len}(\mathbb{exp}(m,a)) \geq \overline{1}$ — 7 T13.45j
21. $\mathbb{len}(\overline{2}^{\mathbb{exp}(m,a)}) \leq \mathbb{len}(\mathbb{exp}(m,a)$ — 8,20 =E
22. $\exists n[Termseq(n, \mathbb{exp}(m,a)) \wedge (\forall i < \mathbb{len}(n))\mathbb{exp}(n,i) \leq \mathbb{exp}(m,a) \wedge \mathbb{len}(n) \leq \mathbb{len}(\mathbb{exp}(m,a)]$ — 15,19,21 ∃I

23.	$B(m,a)$	A (g 12 ∨E)
24.	$(\exists j < a)\mathit{exp}(m,a) = \overline{\ulcorner S \urcorner} * \mathit{exp}(m,j)$	23 abv
25.	$b < a$	A (g 24 ∃E)
26.	$\mathit{exp}(m,a) = \overline{\ulcorner S \urcorner} * \mathit{exp}(m,b)$	
27.	$b < \mathit{len}(m)$	6,25 T13.13b
28.	$\mathit{exp}(m,b) \leq \mathit{exp}(m,a)$	26 T13.47n
29.	$\mathit{len}(\overline{\ulcorner S \urcorner}) = \overline{1}$	cap
30.	$\mathit{len}(\overline{\ulcorner S \urcorner} * \mathit{exp}(m,b))) = \overline{1} + \mathit{len}(\mathit{exp}(m,b))$	29 T13.47f
31.	$\mathit{len}(\mathit{exp}(m,b)) < \mathit{len}(\mathit{exp}(m,a))$	26,30 def
32.	$\mathit{len}(\mathit{exp}(m,b)) < Sx$	10,31 T13.13d
33.	$\mathit{len}(\mathit{exp}(m,b)) \leq x$	32 T13.13n
34.	$\exists n[\mathit{Termseq}(n,\mathit{exp}(m,b)) \wedge (\forall i < \mathit{len}(n))\mathit{exp}(n,i) \leq \mathit{exp}(m,b) \wedge \mathit{len}(n) \leq \mathit{len}(\mathit{exp}(m,b))]$	5,27,33 (∀E)
35.	$\mathit{Termseq}(l,\mathit{exp}(m,b)) \wedge (\forall i < \mathit{len}(l))\mathit{exp}(l,i) \leq \mathit{exp}(m,b) \wedge \mathit{len}(l) \leq \mathit{len}(\mathit{exp}(m,b))$	A (g 34 ∃E)
36.	$\mathit{len}(l * \overline{2}^{\mathit{exp}(m,a)}) = \mathit{len}(l) + \mathit{len}(\overline{2}^{\mathit{exp}(m,a)})$	T13.47f
37.	$\mathit{len}(l * \overline{2}^{\mathit{exp}(m,a)}) = \mathit{len}(l) + \overline{1}$	36,8 =E
38.	$\mathit{Termseq}(l,\mathit{exp}(m,b))$	35 ∧E
39.	$\mathbb{T}\mathit{ermseq}(l * \overline{2}^{\overline{\ulcorner S \urcorner} * \mathit{exp}(m,b)}, \overline{\ulcorner S \urcorner} * \mathit{exp}(m,b))$	38 T13.48i
40.	$\mathbb{T}\mathit{ermseq}(l * \overline{2}^{\mathit{exp}(m,a)}, \mathit{exp}(m,a))$	26,39 =E
41.	$j < \mathit{len}(l * \overline{2}^{\mathit{exp}(m,a)})$	A (g (∀I))
42.	$j < S\mathit{len}(l)$	41,37 =E
43.	$j < \mathit{len}(l) \vee j = \mathit{len}(l)$	42 T13.13n
44.	$j < \mathit{len}(l)$	A (g 43 ∨E)
45.	$(\forall i < \mathit{len}(l))\mathit{exp}(l,i) \leq \mathit{exp}(m,b)$	35 ∧E
46.	$\mathit{exp}(l,j) \leq \mathit{exp}(m,b)$	45,44 (∀E)
47.	$\mathit{exp}(l,j) \leq \mathit{exp}(m,a)$	46,28 T13.13a
48.	$\mathit{exp}(l,j) = \mathit{exp}(l * \overline{2}^{\mathit{exp}(m,a)}, j)$	44 T13.47c
49.	$\mathit{exp}(l * \overline{2}^{\mathit{exp}(m,a)}, j) \leq \mathit{exp}(m,a)$	47,48 =E
50.	$j = \mathit{len}(l)$	A (g 43 ∨E)
51.	$\mathit{exp}(\overline{2}^{\mathit{exp}(m,a)}, \emptyset) = \mathit{exp}(l * \overline{2}^{\mathit{exp}(m,a)}, \mathit{len}(l))$	T13.47c
52.	$\mathit{exp}(m,a) = \mathit{exp}(l * \overline{2}^{\mathit{exp}(m,a)}, \mathit{len}(l))$	51,9 =E
53.	$\mathit{exp}(l * \overline{2}^{\mathit{exp}(m,a)}, j) \leq \mathit{exp}(m,a)$	52 T13.13m
54.	$\mathit{exp}(l * \overline{2}^{\mathit{exp}(m,a)}, j) \leq \mathit{exp}(m,a)$	43,44-49,50-53 ∨E
55.	$(\forall i < \mathit{len}(l * \overline{2}^{\mathit{exp}(m,a)}))\mathit{exp}(l * \overline{2}^{\mathit{exp}(m,a)}, i) \leq \mathit{exp}(m,a)$	41-54 (∀I)
56.	$\mathit{len}(l) \leq \mathit{len}(\mathit{exp}(m,b))$	35 ∧E
57.	$\mathit{len}(l) < \mathit{len}(\mathit{exp}(m,a)$	56,31 T13.13c
58.	$S\mathit{len}(l) \leq \mathit{len}(\mathit{exp}(m,a)$	57 T13.13l
59.	$\mathit{len}(l * \overline{2}^{\mathit{exp}(m,a)}) \leq \mathit{len}(\mathit{exp}(m,a)$	58,37 =E
60.	$\exists n[\mathit{Termseq}(n,\mathit{exp}(m,a)) \wedge (\forall i < \mathit{len}(n))\mathit{exp}(n,i) \leq \mathit{exp}(m,a) \wedge \mathit{len}(n) \leq \mathit{len}(\mathit{exp}(m,a)]$	40,55,59 ∃I
61.	$\exists n[\mathit{Termseq}(n,\mathit{exp}(m,a)) \wedge (\forall i < \mathit{len}(n))\mathit{exp}(n,i) \leq \mathit{exp}(m,a) \wedge \mathit{len}(n) \leq \mathit{len}(\mathit{exp}(m,a)]$	34,35-60 ∃E
62.	$\exists n[\mathit{Termseq}(n,\mathit{exp}(m,a)) \wedge (\forall i < \mathit{len}(n))\mathit{exp}(n,i) \leq \mathit{exp}(m,a) \wedge \mathit{len}(n) \leq \mathit{len}(\mathit{exp}(m,a)]$	24,25-61 (∃E)
63.	$C(m,a)$	A (g 12 ∨E)
64.	$\exists n[\mathit{Termseq}(n,\mathit{exp}(m,a)) \wedge (\forall i < \mathit{len}(n))\mathit{exp}(n,i) \leq \mathit{exp}(m,a) \wedge \mathit{len}(n) \leq \mathit{len}(\mathit{exp}(m,a)]$	similarly
65.	$D(m,a)$	A (g 12 ∨E)
66.	$\exists n[\mathit{Termseq}(n,\mathit{exp}(m,a)) \wedge (\forall i < \mathit{len}(n))\mathit{exp}(n,i) \leq \mathit{exp}(m,a) \wedge \mathit{len}(n) \leq \mathit{len}(\mathit{exp}(m,a)]$	similarly
67.	$\exists n[\mathit{Termseq}(n,\mathit{exp}(m,a)) \wedge (\forall i < \mathit{len}(n))\mathit{exp}(n,i) \leq \mathit{exp}(m,a) \wedge \mathit{len}(n) \leq \mathit{len}(\mathit{exp}(m,a)]$	12,13-66 ∨E
68.	$\mathit{len}(\mathit{exp}(m,a)) \leq Sx \to \exists n[\mathit{Termseq}(n,\mathit{exp}(m,a)) \wedge (\forall i < \mathit{len}(n))\mathit{exp}(n,i) \leq \mathit{exp}(m,a) \wedge$ $\mathit{len}(n) \leq \mathit{len}(\mathit{exp}(m,a)]$	10-67 →I
69.	$(\forall k < \mathit{len}(m))\{\mathit{len}(\mathit{exp}(m,k)) \leq Sx \to \exists n[\mathit{Termseq}(n,\mathit{exp}(m,k)) \wedge$ $(\forall i < \mathit{len}(n))\mathit{exp}(n,i) \leq \mathit{exp}(m,k) \wedge \mathit{len}(n) \leq \mathit{len}(\mathit{exp}(m,k)]\}$	6-68 (∀I)
70.	$\mathcal{P}^x_{Sx}$	69 abv
71.	$\mathcal{P} \to \mathcal{P}^x_{Sx}$	4-70 →I
72.	$\forall x(\forall k < \mathit{len}(m))\{\mathit{len}(\mathit{exp}(m,k)) \leq x \to \exists n[\mathit{Termseq}(n,\mathit{exp}(m,k)) \wedge (\forall i < \mathit{len}(n))\mathit{exp}(n,i) \leq \mathit{exp}(m,k) \wedge$ $\mathit{len}(n) \leq \mathit{len}(\mathit{exp}(m,k)]\}$	2, 71 IN
73.	$\mathbb{T}\mathit{ermseq}(m,t) \to \forall x(\forall k < \mathit{len}(m))\{\mathit{len}(\mathit{exp}(m,k)) \leq x \to \exists n[\mathit{Termseq}(n,\mathit{exp}(m,k)) \wedge$ $(\forall i < \mathit{len}(n))\mathit{exp}(n,i) \leq \mathit{exp}(m,k) \wedge \mathit{len}(n) \leq \mathit{len}(\mathit{exp}(m,k)]\}$	1-72 →I

Exercise 13.35 T13.48.1

T13.48.n. PA $\vdash \mathbb{T}ermseq(m, t) \rightarrow (\forall i < \mathbb{l}en(m))\mathbb{T}erm(\mathbb{e}xp(m, i))$

Exercise 13.35 T13.48.n

1.	$\mathbb{T}ermseq(m,t)$	A (g →I)
2.	$\mathbb{e}xp(m, \mathbb{l}en(m) \dot{-} \overline{1}) = t$	1 T13.48a
3.	$m > \overline{1}$	1 T13.48a
4.	$(\forall k < \mathbb{l}en(m))[A(m,k) \vee B(m,k) \vee C(m,k) \vee D(m,k)]$	1 T13.48a
5.	$\emptyset < \mathbb{l}en(m)$	3 T13.45j
6.	$A(m,\emptyset) \vee B(m,\emptyset) \vee C(m,\emptyset) \vee D(m,\emptyset)$	4,5 (∀E)
7.	$A(m,\emptyset)$	A (g 6∨E)
8.	$\mathbb{e}xp(m,\emptyset) = \overline{\ulcorner \emptyset \urcorner} \vee \mathbb{V}ar(\mathbb{e}xp(m,\emptyset))$	7 abv
9.	$\mathbb{T}ermseq(\overline{2}^{\mathbb{e}xp(m,\emptyset)}, \mathbb{e}xp(m,\emptyset))$	8 T13.48g,h
10.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,\emptyset))$	9 ∃I
11.	$B(m,\emptyset)$	A (g 6∨E)
12.	$\sim\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,\emptyset))$	A (c ∼E)
13.	$(\exists j < \emptyset)\mathbb{e}xp(m,\emptyset) = \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j)$	11 abv
14.	$\mathbb{e}xp(m,\emptyset) = \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j)$	A (c 13 (∃E))
15.	$j < \emptyset$	
16.	$j \not< \emptyset$	T13.13d,r
17.	$\bot$	15,16 ⊥I
18.	$\bot$	13,14-17 (∃E)
19.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,\emptyset))$	12-18 ∼E
20.	$C(m,\emptyset)$	A (g 6∨E)
21.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,\emptyset))$	similarly
22.	$D(m,\emptyset)$	A (g 6∨E)
23.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,\emptyset))$	similarly
24.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,\emptyset))$	6,7-23 ∨E
25.	$\emptyset < \mathbb{l}en(m) \to \exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,\emptyset))$	24 ∨I
26.	$(\forall z \leq k)[z < \mathbb{l}en(m) \to \exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,z))]$	A (g →I)
27.	$Sk < \mathbb{l}en(m)$	A (g →I)
28.	$k < \mathbb{l}en(m)$	27 T13.13l
29.	$A(m,Sk) \vee B(m,Sk) \vee C(m,Sk) \vee D(m,Sk)$	4,27 (∀E)
30.	$A(m,Sk)$	A (g 29∨E)
31.	$\mathbb{e}xp(m,Sk) = \overline{\ulcorner \emptyset \urcorner} \vee \mathbb{V}ar(\mathbb{e}xp(m,Sk))$	30 abv
32.	$\mathbb{T}ermseq(\overline{2}^{\mathbb{e}xp(m,Sk)}, \mathbb{e}xp(m,Sk))$	31 T13.48g,h
33.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,Sk))$	32 ∃I
34.	$B(m,Sk)$	A (g 29∨E)
35.	$(\exists j < Sk)\mathbb{e}xp(m,Sk) = \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j)$	34 abv
36.	$\mathbb{e}xp(m,Sk) = \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,a)$	A (g 35 (∃E))
37.	$a < Sk$	
38.	$a \leq k$	37 T13.13n
39.	$a < \mathbb{l}en(m)$	38,28 T13.13c
40.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,a))$	26,38,39 (∀E)
41.	$\mathbb{T}ermseq(n, \mathbb{e}xp(m,a))$	A (g 40∃E)
42.	$\mathbb{T}ermseq(n * \overline{2}^{\overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,a)}, \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,a))$	41 T13.48i
43.	$\exists x \mathbb{T}ermseq(x, \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,a))$	42 ∃I
44.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,Sk))$	43,36 =E
45.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,Sk))$	40,41-44 ∃E
46.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,Sk))$	35,36-45 (∃E)
47.	$C(m,Sk)$	A (g 29∨E)
48.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,Sk))$	similarly
49.	$D(m,Sk)$	A (g 29∨E)
50.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,Sk))$	similarly
51.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,Sk))$	29,30-50 ∨E
52.	$Sk < \mathbb{l}en(m) \to \exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,Sk))$	27-51 →I
53.	$(\forall z \leq k)[z < \mathbb{l}en(m) \to \exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,z))] \to [Sk < \mathbb{l}en(m) \to \exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,Sk))]$	26-52 →I
54.	$\forall k[k < \mathbb{l}en(m) \to \exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,k))]$	25,53 T13.13ag
55.	$a < \mathbb{l}en(m)$	A (g (∀I))
56.	$\exists x \mathbb{T}ermseq(x, \mathbb{e}xp(m,a))$	55 (∀E)
57.	$\mathbb{T}erm(\mathbb{e}xp(m,a))$	56 T13.48m
58.	$(\forall i < \mathbb{l}en(m))\mathbb{T}erm(\mathbb{e}xp(m,i))$	55-57 (∀I)
59.	$\mathbb{T}ermseq(m,t) \to (\forall i < \mathbb{l}en(m))\mathbb{T}erm(\mathbb{e}xp(m,i))$	1-59 →I

Exercise 13.35 T13.48.n

E13.37. Work the K and M cases from T13.50l. Hard core: show each of the results from T13.50.

T13.50.

T13.50.i. PA $\vdash \mathbb{T}subseq(m, n, t, v, s, u) \rightarrow \mathbb{T}subseq(m * \overline{2}^{\overline{\ulcorner S \urcorner} * t}, n * \overline{2}^{\overline{\ulcorner S \urcorner} * u}, \overline{\ulcorner S \urcorner} * t, v, s, \overline{\ulcorner S \urcorner} * u)$

1.	$\mathbb{T}subseq(m,n,t,v,s,u)$	A (g $\rightarrow$I)
2.	$\mathbb{T}ermseq(m,t)$	1 T13.50a
3.	$\mathbb{l}en(m) = \mathbb{l}en(n)$	1 T13.50a
4.	$\mathbb{e}xp(n, \mathbb{l}en(n) \dot{-} \overline{1}) = u$	1 T13.50a
5.	$(\forall k < \mathbb{l}en(m))(I(m,n,k) \vee J(v,m,n,k) \vee K(v,s,m,n,k) \vee L(m,n,k) \vee M(m,n,k) \vee N(m,n,k))$	1 T13.50a
6.	$\mathbb{T}ermseq(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, \overline{\ulcorner S\urcorner} * t)$	2 T13.48i
7.	$\overline{\ulcorner S\urcorner} > \emptyset$	cap
8.	$\overline{\ulcorner S\urcorner} * t > \emptyset \wedge \overline{\ulcorner S\urcorner} * u > \emptyset$	7 T13.47n
9.	$\mathbb{l}en(\overline{2}^{\overline{\ulcorner S\urcorner}*t}) = \overline{1} \wedge \mathbb{l}en(\overline{2}^{\overline{\ulcorner S\urcorner}*u}) = \overline{1}$	8 T13.45k
10.	$\mathbb{l}en(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}) = \mathbb{l}en(m) + \overline{1} \wedge \mathbb{l}en(n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}) = \mathbb{l}en(n) + \overline{1}$	9 T13.47f
11.	$\mathbb{l}en(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}) = \mathbb{l}en(n * \overline{2}^{\overline{\ulcorner S\urcorner}*u})$	10,3 =E
12.	$\mathbb{l}en(n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}) \dot{-} \overline{1} = \mathbb{l}en(n)$	10 T13.23k
13.	$\mathbb{e}xp(n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, \mathbb{l}en(n)) = \mathbb{e}xp(\overline{2}^{\overline{\ulcorner S\urcorner}*u}, \emptyset)$	T13.47g
14.	$\mathbb{e}xp(\overline{2}^{\overline{\ulcorner S\urcorner}*u}, \emptyset) = \overline{\ulcorner S\urcorner} * u$	T13.44i
15.	$\mathbb{e}xp(n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, \mathbb{l}en(n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}) \dot{-} \overline{1}) = \overline{\ulcorner S\urcorner} * u$	12,13,14 =E
16.	$l < \mathbb{l}en(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t})$	A (g ($\forall$I))
17.	$l < S\mathbb{l}en(m)$	10,16 =E
18.	$l < \mathbb{l}en(m) \vee l = \mathbb{l}en(m)$	17 T13.13n
19.	$l < \mathbb{l}en(m)$	A (g 18$\vee$E)
20.	$\mathbb{e}xp(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, l) = \mathbb{e}xp(m,l) \wedge \mathbb{e}xp(n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, l) = \mathbb{e}xp(n,l)$	19,3 T13.47c
21.	$I(m,n,l) \vee J(v,m,n,l) \vee K(v,s,m,n,l) \vee L(m,n,l) \vee M(m,n,l) \vee N(m,n,l)$	5,19 ($\forall$E)
22.	$I(m,n,l)$	A (g 21$\vee$E)
23.	$\mathbb{e}xp(m,l) = \overline{\ulcorner\emptyset\urcorner} \wedge \mathbb{e}xp(n,l) = \overline{\ulcorner\emptyset\urcorner}$	22 abv
24.	$\mathbb{e}xp(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, l) = \overline{\ulcorner\emptyset\urcorner} \wedge \mathbb{e}xp(n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, l) = \overline{\ulcorner\emptyset\urcorner}$	20,23 =E
25.	$I(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, l)$	24 abv
26.	$I \vee J \vee K \vee L \vee M \vee N(v,s,m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, l)$	25 $\vee$I
27.	$J(v,m,n,l) \vee K(v,s,m,n,l)$	A (g 21$\vee$E)
28.	$I \vee J \vee K \vee L \vee M \vee N(v,s,m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, l)$	similarly
29.	$L(m,n,l)$	A (g 21$\vee$E)
30.	$(\exists i < l)[\mathbb{e}xp(m,l) = \overline{\ulcorner S\urcorner} * \mathbb{e}xp(m,i) \wedge \mathbb{e}xp(n,l) = \overline{\ulcorner S\urcorner} * \mathbb{e}xp(n,i)]$	29 abv
31.	$i < l$	A (g 30 ($\exists$E))
32.	$\mathbb{e}xp(m,l) = \overline{\ulcorner S\urcorner} * \mathbb{e}xp(m,i) \wedge \mathbb{e}xp(n,l) = \overline{\ulcorner S\urcorner} * \mathbb{e}xp(n,i)$	
33.	$i < \mathbb{l}en(m) \wedge i < \mathbb{l}en(n)$	31,19,3 T13.13b
34.	$\mathbb{e}xp(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, i) = \mathbb{e}xp(m,i) \wedge \mathbb{e}xp(n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, i) = \mathbb{e}xp(n,i)$	33 T13.47c
35.	$\mathbb{e}xp(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, l) = \overline{\ulcorner S\urcorner} * \mathbb{e}xp(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, i) \wedge \mathbb{e}xp(n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, l) = \overline{\ulcorner S\urcorner} * \mathbb{e}xp(n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, i)]$	32,20,34 =E
36.	$(\exists i < l)[\mathbb{e}xp(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, l) = \overline{\ulcorner S\urcorner} * \mathbb{e}xp(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, i) \wedge \mathbb{e}xp(n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, l) = \overline{\ulcorner S\urcorner} * \mathbb{e}xp(n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, i)]$	31,35 ($\exists$I)
37.	$L(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, l)$	36 abv
38.	$L(m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, l)$	30,31-37 ($\exists$E)
39.	$I \vee J \vee K \vee L \vee M \vee N(v,s,m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, l)$	38 $\vee$I
40.	$M(m,n,l) \vee N(m,n,l)$	A (g 21$\vee$E)
41.	$I \vee J \vee K \vee L \vee M \vee N(v,s,m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, l)$	similarly
42.	$I \vee J \vee K \vee L \vee M \vee N(v,s,m * \overline{2}^{\overline{\ulcorner S\urcorner}*t}, n * \overline{2}^{\overline{\ulcorner S\urcorner}*u}, l)$	21,22-41 $\vee$E

43.	$l = \mathbb{len}(m)$	A (g 18$\vee$E)
44.	$l = \mathbb{len}(n)$	43,3 =E
45.	$m > \overline{1}$	2 T13.48a
46.	$\mathbb{len}(m) > \emptyset$	45 T13.45j
47.	$\mathbb{len}(m) \dot{-} \overline{1} < \mathbb{len}(m)$	46 T13.23i
48.	$\mathbb{len}(m) \dot{-} \overline{1} < \mathbb{len}(n)$	47,3 =E
49.	$\mathbb{len}(m) \dot{-} \overline{1} < l$	47,43 =E
50.	$\mathbb{exp}(m * \overline{2}^{\ulcorner S \urcorner * t}, \mathbb{len}(m) \dot{-} \overline{1}) = \mathbb{exp}(m, \mathbb{len}(m) \dot{-} \overline{1})$	47 T13.47c
51.	$\mathbb{exp}(m, \mathbb{len}(m) \dot{-} \overline{1}) = t$	2 T13.48a
52.	$\mathbb{exp}(m * \overline{2}^{\ulcorner S \urcorner * t}, \mathbb{len}(m) \dot{-} \overline{1}) = t$	50,51 =E
53.	$\mathbb{exp}(m * \overline{2}^{\ulcorner S \urcorner * t}, \mathbb{len}(m)) = \mathbb{exp}(\overline{2}^{\ulcorner S \urcorner * t}, \emptyset)$	T13.47g
54.	$\mathbb{exp}(\overline{2}^{\ulcorner S \urcorner * t}, \emptyset) = \overline{\ulcorner S \urcorner} * t$	T13.44i
55.	$\mathbb{exp}(m * \overline{2}^{\ulcorner S \urcorner * t}, \mathbb{len}(m)) = \overline{\ulcorner S \urcorner} * t$	53,54 =E
56.	$\mathbb{exp}(m * \overline{2}^{\ulcorner S \urcorner * t}, l) = \overline{\ulcorner S \urcorner} * \mathbb{exp}(m * \overline{2}^{\ulcorner S \urcorner * t}, \mathbb{len}(m) \dot{-} \overline{1})$	55,43,52 =E
57.	$\mathbb{exp}(n * \overline{2}^{\ulcorner S \urcorner * u}, \mathbb{len}(m) \dot{-} \overline{1}) = \mathbb{exp}(n, \mathbb{len}(m) \dot{-} \overline{1})$	48 T13.47c
58.	$\mathbb{exp}(n, \mathbb{len}(m) \dot{-} \overline{1}) = u$	3,4 =E
59.	$\mathbb{exp}(n * \overline{2}^{\ulcorner S \urcorner * u}, \mathbb{len}(m) \dot{-} \overline{1}) = u$	57,58 =E
60.	$\mathbb{exp}(n * \overline{2}^{\ulcorner S \urcorner * u}, \mathbb{len}(n)) = \mathbb{exp}(\overline{2}^{\ulcorner S \urcorner * u}, \emptyset)$	T13.47g
61.	$\mathbb{exp}(\overline{2}^{\ulcorner S \urcorner * u}, \emptyset) = \overline{\ulcorner S \urcorner} * u$	T13.44i
62.	$\mathbb{exp}(n * \overline{2}^{\ulcorner S \urcorner * t}, \mathbb{len}(m)) = \overline{\ulcorner S \urcorner} * u$	3,60,61 =E
63.	$\mathbb{exp}(n * \overline{2}^{\ulcorner S \urcorner * u}, l) = \overline{\ulcorner S \urcorner} * \mathbb{exp}(n * \overline{2}^{\ulcorner S \urcorner * u}, \mathbb{len}(m) \dot{-} \overline{1})$	62,43,59 =E
64.	$(\exists i < l)[\mathbb{exp}(m * \overline{2}^{\ulcorner S \urcorner * t}, l) = \overline{\ulcorner S \urcorner} * \mathbb{exp}(m * \overline{2}^{\ulcorner S \urcorner * t}, i) \wedge \mathbb{exp}(n * \overline{2}^{\ulcorner S \urcorner * u}, l) = \overline{\ulcorner S \urcorner} * \mathbb{exp}(n * \overline{2}^{\ulcorner S \urcorner * u}, i)]$	56,63,49 ($\exists$I)
65.	$L(m * \overline{2}^{\ulcorner S \urcorner * t}, n * \overline{2}^{\ulcorner S \urcorner * u}, l)$	64 abv
66.	$I \vee J \vee K \vee L \vee M \vee N(v, s, m * \overline{2}^{\ulcorner S \urcorner * t}, n * \overline{2}^{\ulcorner S \urcorner * u}, l)$	65 $\vee$I
67.	$I \vee J \vee K \vee L \vee M \vee N(v, s, m * \overline{2}^{\ulcorner S \urcorner * t}, n * \overline{2}^{\ulcorner S \urcorner * u}, l)$	18,19-66 $\vee$E
68.	$(\forall k < \mathbb{len}(m * \overline{2}^{\ulcorner S \urcorner * t}))I \vee J \vee K \vee L \vee M \vee N(v, s, m * \overline{2}^{\ulcorner S \urcorner * t}, n * \overline{2}^{\ulcorner S \urcorner * u}, k)$	16-67 ($\forall$I)
69.	$\mathbb{T}subseq(m * \overline{2}^{\ulcorner S \urcorner * t}, n * \overline{2}^{\ulcorner S \urcorner * u}, \overline{\ulcorner S \urcorner} * t, v, s, \overline{\ulcorner S \urcorner} * u)$	6,11,15,68 T13.50a
70.	$\mathbb{T}subseq(m, n, t, v, s, u) \rightarrow \mathbb{T}subseq(m * \overline{2}^{\ulcorner S \urcorner * t}, n * \overline{2}^{\ulcorner S \urcorner * u}, \overline{\ulcorner S \urcorner} * t, v, s, \overline{\ulcorner S \urcorner} * u)$	1-69 $\rightarrow$I

T13.50.l. PA $\vdash \mathbb{T}subseq(m, n, t, v, s, u) \rightarrow \mathbb{T}ermsub(t, v, s, u)$

Let $\mathcal{P}(m, n, v, s, k) = \exists a \exists b[\mathbb{T}subseq(a, b, \mathbb{exp}(m, k), v, s, \mathbb{exp}(n, k)) \wedge \mathbb{len}(a) \leq \mathbb{len}(\mathbb{exp}(m, k)) \wedge (\forall i < \mathbb{len}(a))(\mathbb{exp}(a, i) \leq \mathbb{exp}(m, k) \wedge \mathbb{exp}(b, i) \leq \mathbb{exp}(n, k))]$

1.	$\mathbb{T}subseq(m,n,t,v,s,u)$	A (g →I)
2.	$\mathbb{T}ermseq(m,t)$	1 T13.50a
3.	$\mathbb{l}en(m) = \mathbb{l}en(n)$	1 T13.50a
4.	$\mathbb{e}xp(n, \mathbb{l}en(n) \dot{-} \overline{1}) = u$	1 T13.50a
5.	$(\forall k < \mathbb{l}en(m))(I(m,n,k) \vee J(v,m,n,k) \vee K(v,s,m,n,k) \vee L(m,n,k) \vee M(m,n,k) \vee N(m,n,k))$	1 T13.50a
6.	$\mathbb{e}xp(m, \mathbb{l}en(m) \dot{-} \overline{1}) = t$	2 T13.48a
7.	$m > \overline{1}$	2 T13.48a
8.	$(\forall k < \mathbb{l}en(m))[A(m,k) \vee B(m,k) \vee C(m,k) \vee D(m,k)]$	2 T13.48a
9.	$k < \mathbb{l}en(m)$	A (g (∀I))
10.	$\mathbb{l}en(\mathbb{e}xp(m,k)) \leq \emptyset$	A (g →I)
11.	$\sim\mathcal{P}$	A (g ∼E)
12.	$\mathbb{e}xp(m,k) > \overline{1}$	2,9 T13.48e
13.	$\mathbb{e}xp(m,k) \not> \overline{1}$	10 T13.45j
14.	$\bot$	12,13 ⊥I
15.	$\mathcal{P}$	11-14 ∼E
16.	$\mathbb{l}en(\mathbb{e}xp(m,k)) \leq \emptyset \to \mathcal{P}$	10-15 →I
17.	$(\forall k < \mathbb{l}en(m))[\mathbb{l}en(\mathbb{e}xp(m,k)) \leq \emptyset \to \mathcal{P}]$	9-16 (∀I)
18.	$(\forall k < \mathbb{l}en(m))[\mathbb{l}en(\mathbb{e}xp(m,k)) \leq x \to \mathcal{P}]$	A (g →I)
19.	$j < \mathbb{l}en(m)$	A (g (∀I))
20.	$\mathbb{l}en(\mathbb{e}xp(m,j)) \leq Sx$	A (g →I)
21.	$\mathbb{e}xp(m,j) > \overline{1}$	2,19 T13.48e
22.	$\mathbb{l}en(\mathbb{e}xp(m,j)) \geq \overline{1}$	21 T13.45j
23.	$I(m,n,j) \vee J(v,m,n,j) \vee K(v,s,m,n,j) \vee L(m,n,j) \vee M(m,n,j) \vee N(m,n,j)$	5,19 (∀E)
24.	$I(m,n,j)$	A (g 23∨E)
25.	$\mathbb{e}xp(m,j) = \overline{\ulcorner\emptyset\urcorner} \wedge \mathbb{e}xp(n,j) = \overline{\ulcorner\emptyset\urcorner}$	24 abv
26.	$\mathbb{T}subseq(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, \overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, \mathbb{e}xp(m,j), v, s, \mathbb{e}xp(n,j))$	25 T13.50f
27.	$\mathbb{l}en(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}) = \overline{1}$	cap
28.	$\mathbb{l}en(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}) \leq \mathbb{l}en(\mathbb{e}xp(m,j))$	22,27 =E
29.	$l < \mathbb{l}en(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}})$	A (g (∀I))
30.	$l = \emptyset$	27,29 T8.16
31.	$\mathbb{e}xp(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, \emptyset) = \overline{\ulcorner\emptyset\urcorner}$	T13.44i
32.	$\mathbb{e}xp(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, l) \leq \mathbb{e}xp(m,j)$	25,31 =E
33.	$\mathbb{e}xp(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, l) \leq \mathbb{e}xp(n,j)$	25,31 =E
34.	$\mathbb{e}xp(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, l) \leq \mathbb{e}xp(m,j) \wedge \mathbb{e}xp(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, l) \leq \mathbb{e}xp(n,j)$	32,33 ∧I
35.	$(\forall i < \mathbb{l}en(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}))(\mathbb{e}xp(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, i) \leq \mathbb{e}xp(m,j) \wedge \mathbb{e}xp(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, i) \leq \mathbb{e}xp(n,j)$	29-34 (∀I)
36.	$\mathcal{P}^k_j$	26,28,35 ∃I

Exercise 13.37 T13.50.l

37.	$J(v,m,n,j)$	A (g 23∨E)
38.	$\mathbb{V}ar(\mathbb{exp}(m,j)) \wedge \mathbb{exp}(m,j) \neq v \wedge \mathbb{exp}(n,j) = \mathbb{exp}(m,j)$	37 abv
39.	$\mathbb{T}subseq(\overline{2}^{\mathbb{exp}(m,j)}, \overline{2}^{\mathbb{exp}(n,j)}, \mathbb{exp}(m,j), v, s, \mathbb{exp}(n,j))$	38 T13.50g
40.	$\mathbb{len}(\overline{2}^{\mathbb{exp}(m,j)}) = \overline{1}$	21 T13.45k
41.	$\mathbb{len}(\overline{2}^{\mathbb{exp}(m,j)}) \leq \mathbb{len}(\mathbb{exp}(m,j))$	22,40 =E
42.	$l < \mathbb{len}(\overline{2}^{\mathbb{exp}(m,j)})$	A (g (∀I))
43.	$l = \emptyset$	40,42 T8.16
44.	$\mathbb{exp}(\overline{2}^{\mathbb{exp}(m,j)}, \emptyset) = \mathbb{exp}(m,j) \wedge \mathbb{exp}(\overline{2}^{\mathbb{exp}(n,j)}, \emptyset) = \mathbb{exp}(n,j)$	T13.44i
45.	$\mathbb{exp}(\overline{2}^{\mathbb{exp}(m,j)}, \emptyset) \leq \mathbb{exp}(m,j) \wedge \mathbb{exp}(\overline{2}^{\mathbb{exp}(n,j)}, \emptyset) \leq \mathbb{exp}(n,j)$	44 T13.13m
46.	$\mathbb{exp}(\overline{2}^{\mathbb{exp}(m,j)}, l) \leq \mathbb{exp}(m,j) \wedge \mathbb{exp}(\overline{2}^{\mathbb{exp}(n,j)}, l) \leq \mathbb{exp}(n,j)$	43,45 =E
47.	$(\forall i < \mathbb{len}(\overline{2}^{\mathbb{exp}(m,j)}))(\mathbb{exp}(\overline{2}^{\mathbb{exp}(m,j)}, i) \leq \mathbb{exp}(m,j) \wedge \mathbb{exp}(\overline{2}^{\mathbb{exp}(n,j)}, i) \leq \mathbb{exp}(n,j))$	42-46 (∀I)
48.	$\mathcal{P}^k_j$	39,41,47 ∃I
49.	$K(v,s,m,n,j)$	A (g 23∨E)
50.	$\mathcal{P}^k_j$	similarly
51.	$L(m,n,j)$	A (g 23∨E)
52.	$(\exists i < j)[\mathbb{exp}(m,j) = \overline{\ulcorner S \urcorner} * \mathbb{exp}(m,i) \wedge \mathbb{exp}(n,j) = \overline{\ulcorner S \urcorner} * \mathbb{exp}(n,i)]$	51 abv
53.	$l < j$	A (g 52 (∃E))
54.	$\mathbb{exp}(m,j) = \overline{\ulcorner S \urcorner} * \mathbb{exp}(m,l)$	
55.	$\mathbb{exp}(n,j) = \overline{\ulcorner S \urcorner} * \mathbb{exp}(n,l)$	
56.	$l < \mathbb{len}(m)$	19,53 T13.13b
57.	$\mathbb{len}(\overline{\ulcorner S \urcorner}) = \overline{1}$	cap
58.	$\mathbb{len}(\overline{\ulcorner S \urcorner} * \mathbb{exp}(m,l)) = \overline{1} + \mathbb{len}(\mathbb{exp}(m,l))$	57 T13.47f
59.	$\mathbb{len}(\mathbb{exp}(m,l)) < \mathbb{len}(\mathbb{exp}(m,j))$	54,58 def
60.	$\mathbb{len}(\mathbb{exp}(m,l)) \leq x$	20,59 T13.13n
61.	$\mathcal{P}^k_l$	18,56,60 (∀E)
62.	$\mathbb{T}subseq(c, d, \mathbb{exp}(m,l), v, s, \mathbb{exp}(n,l))$	A (g 61∃E)
63.	$\mathbb{len}(c) \leq \mathbb{len}(\mathbb{exp}(m,l))$	
64.	$(\forall i < \mathbb{len}(c))(\mathbb{exp}(c,i) \leq \mathbb{exp}(m,l) \wedge \mathbb{exp}(d,i) \leq \mathbb{exp}(n,l))$	
65.	$\mathbb{len}(c) = \mathbb{len}(d)$	62 T13.50a
66.	$\mathbb{T}subseq(c * \overline{2}^{\mathbb{exp}(m,j)}, d * \overline{2}^{\mathbb{exp}(n,j)}, \mathbb{exp}(m,j), v, s, \mathbb{exp}(n,j))$	54,55,62 T13.50i
67.	$\mathbb{len}(\overline{\ulcorner S \urcorner} * \mathbb{exp}(n,l)) = \overline{1} + \mathbb{len}(\mathbb{exp}(n,l))$	57 T13.47f
68.	$\mathbb{len}(\overline{\ulcorner S \urcorner} * \mathbb{exp}(n,l)) \geq \overline{1}$	67 T13.13u
69.	$\overline{\ulcorner S \urcorner} * \mathbb{exp}(n,l) > \overline{1}$	68 T13.45g
70.	$\mathbb{exp}(n,j) > \overline{1}$	55,69 =E
71.	$\mathbb{len}(\overline{2}^{\mathbb{exp}(m,j)}) = \overline{1} \wedge \mathbb{len}(\overline{2}^{\mathbb{exp}(n,j)} = \overline{1})$	21,70 T13.45k
72.	$\mathbb{len}(c * \overline{2}^{\mathbb{exp}(m,j)}) = \mathbb{len}(c) + 1 \wedge \mathbb{len}(d * \overline{2}^{\mathbb{exp}(n,j)}) = \mathbb{len}(d) + 1$	71 T13.47f
73.	$\mathbb{len}(c * \overline{2}^{\mathbb{exp}(m,j)}) = \mathbb{len}(d * \overline{2}^{\mathbb{exp}(n,j)})$	65,72 =E
74.	$\mathbb{len}(\mathbb{exp}(m,j)) = \overline{1} + \mathbb{len}(\mathbb{exp}(m,l))$	54,58 =E
75.	$\mathbb{len}(c) + \overline{1} \leq \mathbb{len}(\mathbb{exp}(m,l)) + \overline{1}$	63 T13.13v
76.	$\mathbb{len}(c * \overline{2}^{\mathbb{exp}(m,j)}) \leq \mathbb{len}(\mathbb{exp}(m,j))$	72,74,75 =E
77.	$q < \mathbb{len}(c * \overline{2}^{\mathbb{exp}(m,j)})$	A (g (∀I))
78.	$q < S\,\mathbb{len}(c)$	72,77 =E
79.	$q < \mathbb{len}(c) \vee q = \mathbb{len}(c)$	78 T13.13n
80.	$q < \mathbb{len}(c)$	A (g 79∨E)
81.	$q < \mathbb{len}(d)$	80,65 =E
82.	$\mathbb{exp}(c,q) \leq \mathbb{exp}(m,l) \wedge \mathbb{exp}(d,q) \leq \mathbb{exp}(n,l))$	64,80 (∀E)
83.	$\mathbb{exp}(c,q) \leq \mathbb{exp}(m,j) \wedge \mathbb{exp}(d,q) \leq \mathbb{exp}(n,j)$	54,55,82 T13.47o
84.	$\mathbb{exp}(c * \overline{2}^{\mathbb{exp}(m,j)}, q) = \mathbb{exp}(c,q) \wedge \mathbb{exp}(d * \overline{2}^{\mathbb{exp}(n,j)}, q) = \mathbb{exp}(d,q)$	80,81 T13.47c
85.	$\mathbb{exp}(c * \overline{2}^{\mathbb{exp}(m,j)}, q) \leq \mathbb{exp}(m,j) \wedge \mathbb{exp}(d * \overline{2}^{\mathbb{exp}(n,j)}, q) \leq \mathbb{exp}(n,j)$	83,84 =E
86.	$q = \mathbb{len}(c)$	A (g 79∨E)
87.	$\mathbb{exp}(c * \overline{2}^{\mathbb{exp}(m,j)}, q) = \mathbb{exp}(\overline{2}^{\mathbb{exp}(m,j)}, \emptyset) \wedge \mathbb{exp}(d * \overline{2}^{\mathbb{exp}(n,j)}, q) = \mathbb{exp}(\overline{2}^{\mathbb{exp}(n,j)}, \emptyset)$	86,65 T13.47g
88.	$\mathbb{exp}(\overline{2}^{\mathbb{exp}(m,j)}, \emptyset) = \mathbb{exp}(m,j) \wedge \mathbb{exp}(\overline{2}^{\mathbb{exp}(n,j)}, \emptyset) = \mathbb{exp}(n,j)$	T13.44i
89.	$\mathbb{exp}(c * \overline{2}^{\mathbb{exp}(m,j)}, q) \leq \mathbb{exp}(m,j) \wedge \mathbb{exp}(d * \overline{2}^{\mathbb{exp}(n,j)}, q) \leq \mathbb{exp}(n,j)$	87,86 =E
90.	$\mathbb{exp}(c * \overline{2}^{\mathbb{exp}(m,j)}, q) \leq \mathbb{exp}(m,j) \wedge \mathbb{exp}(d * \overline{2}^{\mathbb{exp}(n,j)}, q) \leq \mathbb{exp}(n,j)$ *Exercise 13.37 T13.50.l*	79,80-89 ∨E
91.	$(\forall i < \mathbb{len}(c * \overline{2}^{\mathbb{exp}(m,j)}))(\mathbb{exp}(c * \overline{2}^{\mathbb{exp}(m,j)}, i) \leq \mathbb{exp}(m,j) \wedge \mathbb{exp}(d * \overline{2}^{\mathbb{exp}(n,j)}, i) \leq \mathbb{exp}(n,j))$	77-90 (∀I)
92.	$\mathcal{P}^k_j$	66,73,76,91 ∃I
93.	$\mathcal{P}^k_j$	61,62-92 ∃E
94.	$\mathcal{P}^k_j$	52,53-93 (∃E)

95.	$M(m,n,j)$	A (g 23∨E)
96.	$\mathcal{P}^k_j$	similarly
97.	$N(m,n,j)$	A (g 23∨E)
98.	$\mathcal{P}^k_j$	similarly
99.	$\mathcal{P}^k_j$	23,24-98 ∨E
100.	$\mathbb{len}(\mathbb{exp}(m,j)) \leq Sx \to \mathcal{P}^k_j$	20-99 →I
101.	$(\forall k < \mathbb{len}(m))[\mathbb{len}(\mathbb{exp}(m,k)) \leq Sx \to \mathcal{P}]$	19-100 (∀I)
102.	$(\forall k < \mathbb{len}(m))[\mathbb{len}(\mathbb{exp}(m,k)) \leq x \to \mathcal{P}] \to (\forall k < \mathbb{len}(m))[\mathbb{len}(\mathbb{exp}(m,k)) \leq Sx \to \mathcal{P}]$	18-101 →I
103.	$\forall x(\forall k < \mathbb{len}(m))[\mathbb{len}(\mathbb{exp}(m,k)) \leq x \to \mathcal{P}]$	17,102 IN
104.	$\mathbb{len}(m) > \emptyset$	7 T13.45j
105.	$\mathbb{len}(m) \dot{-} \overline{1} < \mathbb{len}(m)$	104 T13.23i
106.	$\mathcal{P}^k_{\mathbb{len}(m)\dot{-}\overline{1}}$	103,105 (∀E)
107.	$\mathbb{Tsubseq}(a,b,t,v,s,u)$	A (g 106,4,6 ∃E)
108.	$\mathbb{len}(a) \leq \mathbb{len}(t)$	
109.	$(\forall i < \mathbb{len}(a))(\mathbb{exp}(a,i) \leq t \wedge \mathbb{exp}(b,i) \leq u]$	
110.	$\mathbb{len}(a) = \mathbb{len}(b)$	107 T13.50a
111.	$[\mathbb{pi}(\mathbb{len}(t))^t]^{\mathbb{len}(t)} \geq val(a,\mathbb{len}(a))$	108,109 T13.46o
112.	$[\mathbb{pi}(\mathbb{len}(t))^u]^{\mathbb{len}(t)} \geq val(b,\mathbb{len}(b))$	110,108,109 T13.46o
113.	$\mathbb{Termseq}(a,t)$	107 T13.50a
114.	$a > \overline{1}$	113 T13.48a
115.	$\mathbb{len}(a) > \emptyset$	114 T13.45j
116.	$\mathbb{len}(b) > \emptyset$	115,110 =E
117.	$b > \overline{1}$	116 T13.45g
118.	$a \leq [\mathbb{pi}(\mathbb{len}(t))^t]^{\mathbb{len}(t)} \wedge b \leq [\mathbb{pi}(\mathbb{len}(t))^u]^{\mathbb{len}(t)}$	111,112,114,117 T13.46n
119.	$(\exists x \leq X_t)(\exists y \leq Y_{t,u})\mathbb{Tsubseq}(x,y,t,v,s,u)$	107,118 (∃I)
120.	$\mathbb{Termsub}(t,v,s,u)$	119 T13.50b
121.	$\mathbb{Termsub}(t,v,s,u)$	106,107-120 ∃E
122.	$\mathbb{Tsubseq}(m,n,t,v,s,u) \to \mathbb{Termsub}(t,v,s,u)$	1-121 →I

T13.50.m. PA $\vdash [\mathbb{Term}(t) \wedge \mathbb{Term}(s)] \to \exists u[\mathbb{Termsub}(t,v,s,u) \wedge \mathbb{len}(u) \leq \mathbb{len}(t) \times \mathbb{len}(s) \wedge (\forall k < \mathbb{len}(u))\mathbb{exp}(u,k) \leq t + s]$

Let $\mathcal{P}(m,i,v,s) = \exists x \exists y \exists u[\mathbb{Tsubseq}(x,y,\mathbb{exp}(m,i),v,s,u) \wedge \mathbb{len}(u) \leq \mathbb{len}(\mathbb{exp}(m,i)) \times \mathbb{len}(s) \wedge (\forall k < \mathbb{len}(u))\mathbb{exp}(u,k) \leq \mathbb{exp}(m,i) + s]$

1.	$\mathbb{T}erm(t) \wedge \mathbb{T}erm(s)$	A (g →I)
2.	$\mathbb{T}ermseq(m,t)$	1 T13.48b, ∃E
3.	$\mathbb{e}xp(m,\mathbb{l}en(m) \dot{-} \overline{1}) = t \wedge m > \overline{1} \wedge (\forall k < \mathbb{l}en(m))[A(m,k) \vee B(m,k) \vee C(m,k) \vee D(m,k)]$	2 T13.48a
4.	$\mathbb{l}en(m) > \emptyset$	3 T13.45j
5.	$\mathbb{l}en(m) \dot{-} \overline{1} \leq \mathbb{l}en(m)$	4 T13.23i
6.	$s > \overline{1}$	1 T13.48f
7.	$\mathbb{l}en(s) > \emptyset$	6 T13.45j
8.	$\emptyset < \mathbb{l}en(m)$	A (g →I)
9.	$\mathbb{T}erm(\mathbb{e}xp(m,\emptyset))$	2,8 T13.48n
10.	$\mathbb{e}xp(m,\emptyset) > \overline{1}$	T13.48f
11.	$\mathbb{l}en(\mathbb{e}xp(m,\emptyset)) > \emptyset$	T13.45j
12.	$A(m,\emptyset) \vee B(m,\emptyset) \vee C(m,\emptyset) \vee D(m,\emptyset)$	3,8 (∀E)
13.	$A(m,\emptyset)$	A (g 12∨E)
14.	$\mathbb{e}xp(m,\emptyset) = \overline{\ulcorner\emptyset\urcorner} \vee \mathbb{V}ar(\mathbb{e}xp(m,\emptyset))$	13 abv
15.	$\mathbb{e}xp(m,\emptyset) = \overline{\ulcorner\emptyset\urcorner}$	A (g 14∨E)
16.	$\mathbb{l}en(\overline{\ulcorner\emptyset\urcorner}) = \overline{1}$	cap
17.	$\mathbb{T}subseq(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, \overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, \mathbb{e}xp(m,\emptyset), v, s, \overline{\ulcorner\emptyset\urcorner})$	15 T13.50f
18.	$\mathbb{l}en(\overline{\ulcorner\emptyset\urcorner}) \leq \mathbb{l}en(\overline{\ulcorner\emptyset\urcorner}) \times \mathbb{l}en(s)$	7 T13.13z
19.	$\mathbb{l}en(\overline{\ulcorner\emptyset\urcorner}) \leq \mathbb{l}en(\mathbb{e}xp(m,\emptyset)) \times \mathbb{l}en(s)$	15,18 =E
20.	$k < \mathbb{l}en(\overline{\ulcorner\emptyset\urcorner})$	A (g (∀I))
21.	$\mathbb{e}xp(\overline{\ulcorner\emptyset\urcorner}, k) \leq \overline{\ulcorner\emptyset\urcorner}$	T13.44g
22.	$\overline{\ulcorner\emptyset\urcorner} \leq \overline{\ulcorner\emptyset\urcorner} + s$	T13.13u
23.	$\mathbb{e}xp(\overline{\ulcorner\emptyset\urcorner}, k) \leq \mathbb{e}xp(m,\emptyset) + s$	15,21,22 T13.13a
24.	$(\forall k < \mathbb{l}en(\overline{\ulcorner\emptyset\urcorner}))\mathbb{e}xp(\overline{\ulcorner\emptyset\urcorner}, k) \leq \mathbb{e}xp(m,\emptyset) + s$	20-23 (∀I)
25.	$\mathcal{P}^i_\emptyset$	17,19,24 ∃I
26.	$\mathbb{V}ar(\mathbb{e}xp(m,\emptyset))$	A (g 14∨E)
27.	$\mathbb{e}xp(m,\emptyset) = v \vee \mathbb{e}xp(m,\emptyset) \neq v$	T3.1
28.	$\mathbb{e}xp(m,\emptyset) = v$	A (g 27∨E)
29.	$\mathbb{T}subseq(\overline{2}^{\mathbb{e}xp(m,\emptyset)}, \overline{2}^{\mathbb{e}xp(m,\emptyset)}, \mathbb{e}xp(m,\emptyset), v, s, s)$	26 T13.50h
30.	$\mathbb{l}en(\mathbb{e}xp(m,\emptyset)) > \emptyset$	26 T13.48d
31.	$\mathbb{l}en(s) \leq \mathbb{l}en(\mathbb{e}xp(m,\emptyset)) \times \mathbb{l}en(s)$	30 T13.13z
32.	$k < \mathbb{l}en(s)$	A (g (∀I))
33.	$\mathbb{e}xp(s,k) \leq s$	T13.44g
34.	$s \leq \mathbb{e}xp(m,\emptyset) + s$	T13.13u
35.	$\mathbb{e}xp(s,k) \leq \mathbb{e}xp(m,\emptyset) + s$	33,34 T13.13a
36.	$(\forall k < \mathbb{l}en(s))\mathbb{e}xp(s,k) \leq \mathbb{e}xp(m,\emptyset) + s$	32-35 (∀I)
37.	$\mathcal{P}^i_\emptyset$	29,31,36 ∃I
38.	$\mathbb{e}xp(m,\emptyset) \neq v$	A (g 27∨E)
39.	$\mathbb{T}subseq(\overline{2}^{\mathbb{e}xp(m,\emptyset)}, \overline{2}^{\mathbb{e}xp(m,\emptyset)}, \mathbb{e}xp(m,\emptyset), v, s, \mathbb{e}xp(m,\emptyset))$	38 T13.50g
40.	$\mathbb{l}en(\mathbb{e}xp(m,\emptyset)) \leq \mathbb{l}en(\mathbb{e}xp(m,\emptyset)) \times \mathbb{l}en(s)$	7 T13.13z
41.	$k < \mathbb{l}en(\mathbb{e}xp(m,\emptyset))$	A (g (∀I))
42.	$\mathbb{e}xp(\mathbb{e}xp(m,\emptyset), k) \leq \mathbb{e}xp(m,\emptyset)$	T13.44g
43.	$\mathbb{e}xp(m,\emptyset) \leq \mathbb{e}xp(m,\emptyset) + s$	T13.13u
44.	$\mathbb{e}xp(\mathbb{e}xp(m,\emptyset), k) \leq \mathbb{e}xp(m,\emptyset) + s$	42,43 T13.13a
45.	$(\forall k < \mathbb{l}en(\mathbb{e}xp(m,\emptyset)))\mathbb{e}xp(m,\emptyset), k) \leq \mathbb{e}xp(m,\emptyset) + s$	41-44 (∀I)
46.	$\mathcal{P}^i_\emptyset$	39,40,45 ∃I
47.	$\mathcal{P}^i_\emptyset$	27,28-46∨E
48.	$\mathcal{P}^i_\emptyset$	14,15-47 ∨E
49.	$B(m,\emptyset) \vee C(m,\emptyset) \vee D(m,\emptyset)$	A (g 12∨E)
50.	$\mathcal{P}^i_\emptyset$	trivial
51.	$\mathcal{P}^i_\emptyset$	12,13-50 ∨E
52.	$\emptyset < \mathbb{l}en(m) \rightarrow \mathcal{P}^i_\emptyset$	8-51 →I

Exercise 13.37 T13.50.m

53.	$(\forall z \leq i)(z < \mathbb{l}en(m) \rightarrow \mathcal{P}^i_z)$	A ($g \rightarrow$I)
54.	$Si < \mathbb{l}en(m)$	A ($g \rightarrow$I)
55.	$A(m,Si) \vee B(m,Si) \vee C(m,Si) \vee D(m,Si)$	3,54 ($\forall$E)
56.	$A(m,Si)$	A (g 55$\vee$E)
57.	$\mathcal{P}^i_{Si}$	as above
58.	$B(m,Si)$	A (g 55$\vee$E)
59.	$(\exists j < Si)\mathbb{e}xp(m,Si) = \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j)$	58 abv
60.	$\mathbb{e}xp(m,Si) = \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j)$	A (g 59 ($\exists$E))
61.	$j < Si$	
62.	$j \leq i$	61 T13.13n
63.	$j < \mathbb{l}en(m)$	54,61 T13.13b
64.	$\mathcal{P}^i_j$	53,62,63 ($\forall$E)
65.	$\mathbb{T}subseq(a,b,\mathbb{e}xp(m,j),v,s,r)$	A (g 64 $\exists$E)
66.	$\mathbb{l}en(r) \leq \mathbb{l}en(\mathbb{e}xp(m,j)) \times \mathbb{l}en(s)$	
67.	$(\forall k < \mathbb{l}en(r))\mathbb{e}xp(r,k) \leq \mathbb{e}xp(m,j) + s$	
68.	$\mathbb{T}subseq(a * \overline{2}^{\overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j)}, b * \overline{2}^{\overline{\ulcorner S \urcorner} * r}, \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j), v, s, \overline{\ulcorner S \urcorner} * r)$	65 T13.50i
69.	$\mathbb{l}en(\overline{\ulcorner S \urcorner}) = \overline{1}$	cap
70.	$\mathbb{l}en(\overline{\ulcorner S \urcorner} * r) = \overline{1} + \mathbb{l}en(r)$	69 T13.47f
71.	$\mathbb{l}en(\overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j)) = \overline{1} + \mathbb{l}en(\mathbb{e}xp(m,j))$	69 T13.47f
72.	$\overline{1} + \mathbb{l}en(r) \leq \overline{1} + \mathbb{l}en(\mathbb{e}xp(m,j)) \times \mathbb{l}en(s)$	66 T13.13v
73.	$\mathbb{l}en(\overline{\ulcorner S \urcorner} * r) \leq \overline{1} + \mathbb{l}en(\mathbb{e}xp(m,j)) \times \mathbb{l}en(s)$	72,70 =E
74.	$\overline{1} + \mathbb{l}en(\mathbb{e}xp(m,j)) \times \mathbb{l}en(s) \leq \mathbb{l}en(s) + \mathbb{l}en(\mathbb{e}xp(m,j)) \times \mathbb{l}en(s)$	7 T13.13v
75.	$\mathbb{l}en(\overline{\ulcorner S \urcorner} * r) \leq \mathbb{l}en(s) + \mathbb{l}en(\mathbb{e}xp(m,j)) \times \mathbb{l}en(s)$	73,74 T13.13a
76.	$\mathbb{l}en(\overline{\ulcorner S \urcorner} * r) \leq [\overline{1} + \mathbb{l}en(\mathbb{e}xp(m,j))] \times \mathbb{l}en(s)$	75 T6.64
77.	$\mathbb{l}en(\overline{\ulcorner S \urcorner} * r) \leq \mathbb{l}en(\mathbb{e}xp(m,Si)) \times \mathbb{l}en(s)$	60,71,76 =E
78.	$k < \mathbb{l}en(\overline{\ulcorner S \urcorner} * r)$	A (g ($\forall$I))
79.	$k < \mathbb{l}en(\overline{\ulcorner S \urcorner}) + \mathbb{l}en(r)$	78 T13.47f
80.	$k < \mathbb{l}en(\overline{\ulcorner S \urcorner}) \vee k \geq \mathbb{l}en(\overline{\ulcorner S \urcorner})$	T13.13q
81.	$k < \mathbb{l}en(\overline{\ulcorner S \urcorner})$	A (g 80$\vee$E)
82.	$\mathbb{e}xp(\overline{\ulcorner S \urcorner} * r, k) = \mathbb{e}xp(\overline{\ulcorner S \urcorner}, k)$	81 T13.47c
83.	$\mathbb{e}xp(\overline{\ulcorner S \urcorner}, k) \leq \overline{\ulcorner S \urcorner}$	T13.44g
84.	$\mathbb{e}xp(\overline{\ulcorner S \urcorner} * r, k) \leq \overline{\ulcorner S \urcorner}$	82,83 =E
85.	$\overline{\ulcorner S \urcorner} \leq \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j)$	T13.47n
86.	$\overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j) \leq \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j) + s$	T13.13u
87.	$\overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j) \leq \mathbb{e}xp(m,Si) + s$	60,85 =E
88.	$\mathbb{e}xp(\overline{\ulcorner S \urcorner} * r, k) \leq \mathbb{e}xp(m,Si) + s$	84,85,87 T13.13a
89.	$k \geq \mathbb{l}en(\overline{\ulcorner S \urcorner})$	A (g 80$\vee$E)
90.	$k = \mathbb{l}en(\overline{\ulcorner S \urcorner}) + (k \dot{-} \mathbb{l}en(\overline{\ulcorner S \urcorner}))$	89 T13.23a
91.	$\mathbb{e}xp(\overline{\ulcorner S \urcorner} * r, k) = \mathbb{e}xp(r, k \dot{-} \mathbb{l}en(\overline{\ulcorner S \urcorner}))$	90 T13.47g
92.	$k \dot{-} \mathbb{l}en(\overline{\ulcorner S \urcorner}) < (\mathbb{l}en(\overline{\ulcorner S \urcorner}) + \mathbb{l}en(r)) \dot{-} \mathbb{l}en(\overline{\ulcorner S \urcorner})$	89,79 T13.23e
93.	$k \dot{-} \mathbb{l}en(\overline{\ulcorner S \urcorner}) < \mathbb{l}en(r)$	92 T13.23l,b
94.	$\mathbb{e}xp(r, k \dot{-} \mathbb{l}en(\overline{\ulcorner S \urcorner})) \leq \mathbb{e}xp(m,j) + s$	93,67 ($\forall$E)
95.	$\mathbb{e}xp(\overline{\ulcorner S \urcorner} * r, k) \leq \mathbb{e}xp(m,j) + s$	91,94 =E
96.	$\mathbb{e}xp(m,j) \leq \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j)$	T13.47o
97.	$\mathbb{e}xp(m,j) \leq \mathbb{e}xp(m,Si)$	60,96 =E
98.	$\mathbb{e}xp(\overline{\ulcorner S \urcorner} * r, k) \leq \mathbb{e}xp(m,Si) + s$	95,97 T13.13v
99.	$\mathbb{e}xp(\overline{\ulcorner S \urcorner} * r, k) \leq \mathbb{e}xp(m,Si) + s$	80,81-98 $\vee$E
100.	$(\forall k < \mathbb{l}en(\overline{\ulcorner S \urcorner} * r))\mathbb{e}xp(\overline{\ulcorner S \urcorner} * r, k) \leq \mathbb{e}xp(m,Si) + s$	78-99 ($\forall$I)
101.	$\mathcal{P}^i_{Si}$	68,77,100 $\exists$I
102.	$\mathcal{P}^i_{Si}$	64,65-101 $\exists$E
103.	$\mathcal{P}^i_{Si}$	59,60-102 ($\exists$E)

Exercise 13.37 T13.50.m

104.	$C(m, Si)$	A (g 55$\vee$E)
105.	$\mathcal{P}^i_{Si}$	similarly
106.	$D(m, Si)$	A (g 55$\vee$E)
107.	$\mathcal{P}^i_{Si}$	similarly
108.	$\mathcal{P}^i_{Si}$	55,56-107 $\vee$E
109.	$Si < \mathbb{l}en(m) \rightarrow \mathcal{P}^i_{Si}$	54-108 $\rightarrow$I
110.	$[(\forall z \le i)(z < \mathbb{l}en(m) \rightarrow \mathcal{P}^i_z)] \rightarrow [Si < \mathbb{l}en(m) \rightarrow \mathcal{P}^i_{Si}]$	53-109 $\rightarrow$I
111.	$\forall i[i < \mathbb{l}en(m) \rightarrow \mathcal{P}]$	52,110 T13.13ag
112.	$\exists x \exists y \exists u[\mathbb{T}subseq(x, y, t, v, s, u) \wedge \mathbb{l}en(u) \le \mathbb{l}en(t) \times \mathbb{l}en(s) \wedge (\forall k < \mathbb{l}en(u))\mathbb{e}xp(u, k) \le t + s]$	3,5,111 $\forall$E
113.	$\mathbb{T}subseq(x, y, t, v, s, u) \wedge \mathbb{l}en(u) \le \mathbb{l}en(t) \times \mathbb{l}en(s) \wedge (\forall k < \mathbb{l}en(u))\mathbb{e}xp(u, k) \le t + s$	A (g 112 $\exists$E)
114.	$\mathbb{T}ermsub(t, v, s, u) \wedge \mathbb{l}en(u) \le \mathbb{l}en(t) \times \mathbb{l}en(s) \wedge (\forall k < \mathbb{l}en(u))\mathbb{e}xp(u, k) \le t + s$	113 T13.50l
115.	$\exists u[\mathbb{T}ermsub(t, v, s, u) \wedge \mathbb{l}en(u) \le \mathbb{l}en(t) \times \mathbb{l}en(s) \wedge (\forall k < \mathbb{l}en(u))\mathbb{e}xp(u, k) \le t + s]$	114 $\exists$I
116.	$\exists u[\mathbb{T}ermsub(t, v, s, u) \wedge \mathbb{l}en(u) \le \mathbb{l}en(t) \times \mathbb{l}en(s) \wedge (\forall k < \mathbb{l}en(u))\mathbb{e}xp(u, k) \le t + s]$	112,113-115 $\exists$E
117.	$[\mathbb{T}erm(t) \wedge \mathbb{T}erm(s)] \rightarrow \exists u[\mathbb{T}ermsub(t, v, s, u) \wedge \mathbb{l}en(u) \le \mathbb{l}en(t) \times \mathbb{l}en(s) \wedge (\forall k < \mathbb{l}en(u))\mathbb{e}xp(u, k) \le t + s]$	1-116 $\rightarrow$I

T13.50.n. PA $\vdash$ $[\mathbb{A}tomic(p) \wedge \mathbb{T}erm(s)] \rightarrow \exists q[\mathbb{A}tomsub(p, v, s, q) \wedge \mathbb{l}en(q) \le \mathbb{l}en(p) \times \mathbb{l}en(s) \wedge (\forall k < \mathbb{l}en(q))\mathbb{e}xp(q, k) \le p + s]$

1.	$\mathbb{A}tomic(p) \wedge \mathbb{T}erm(s)$	A (g →I)
2.	$s > \overline{1}$	1 T13.48f
3.	$\mathbb{l}en(s) > \emptyset$	2 T13.45j
4.	$(\exists x \leq p)(\exists y \leq p)[\mathbb{T}erm(x) \wedge \mathbb{T}erm(y) \wedge p = \overline{\ulcorner = \urcorner} * x * y]$	1 T13.49c
5.	$\mathbb{T}erm(a) \wedge \mathbb{T}erm(b)$	A (g 4 (∃E))
6.	$p = \overline{\ulcorner = \urcorner} * a * b$	
7.	$a \leq p \wedge b \leq p$	
8.	$\exists a'[\mathbb{T}ermsub(a, v, s, a') \wedge \mathbb{l}en(a') \leq \mathbb{l}en(a) \times \mathbb{l}en(s) \wedge (\forall k < \mathbb{l}en(a'))\mathbb{e}xp(a', k) \leq a + s]$	1,5 T13.50m
9.	$\exists b'[\mathbb{T}ermsub(b, v, s, b') \wedge \mathbb{l}en(b') \leq \mathbb{l}en(b) \times \mathbb{l}en(s) \wedge (\forall k < \mathbb{l}en(b'))\mathbb{e}xp(b', k) \leq b + s]$	1,5 T13.50m
10.	$\mathbb{T}ermsub(a, v, s, a')$	A (g 8∃E)
11.	$\mathbb{l}en(a') \leq \mathbb{l}en(a) \times \mathbb{l}en(s)$	
12.	$(\forall k < \mathbb{l}en(a'))\mathbb{e}xp(a', k) \leq a + s$	
13.	$\mathbb{T}ermsub(b, v, s, b')$	A (g 9∃E)
14.	$\mathbb{l}en(b') \leq \mathbb{l}en(b) \times \mathbb{l}en(s)$	
15.	$(\forall k < \mathbb{l}en(b'))\mathbb{e}xp(b', k) \leq b + s$	
16.	$b' \leq \overline{\ulcorner = \urcorner} * a' * b'$	T13.47o
17.	$a' \leq \overline{\ulcorner = \urcorner} * a'$	T13.47o
18.	$\overline{\ulcorner = \urcorner} * a' \leq \overline{\ulcorner = \urcorner} * a' * b'$	T13.47n
19.	$a' \leq \overline{\ulcorner = \urcorner} * a' * b'$	17,18 T13.13a
20.	$a' \leq \overline{\ulcorner = \urcorner} * a' * b' \wedge b' \leq \overline{\ulcorner = \urcorner} * a' * b'$	19,16 ∧I
21.	$\mathbb{T}erm(a) \wedge \mathbb{T}erm(b) \wedge p = \overline{\ulcorner = \urcorner} * a * b \wedge \mathbb{T}ermsub(a, v, s, a') \wedge \mathbb{T}ermsub(b, v, s, b') \wedge$ $\overline{\ulcorner = \urcorner} * a' * b' = \overline{\ulcorner = \urcorner} * a' * b'$	5,6,10,13 ∧I
22.	$\mathbb{A}tomsub(p, v, s, \overline{\ulcorner = \urcorner} * a' * b')$	7,20,21 (∃I)
23.	$\mathbb{l}en(\overline{\ulcorner = \urcorner}) \leq \mathbb{l}en(\overline{\ulcorner = \urcorner}) \times \mathbb{l}en(s)$	3 T13.13z
24.	$\mathbb{l}en(\overline{\ulcorner = \urcorner} * a * b) = \mathbb{l}en(\overline{\ulcorner = \urcorner}) + \mathbb{l}en(a) + \mathbb{l}en(b)$	T13.47f
25.	$\mathbb{l}en(\overline{\ulcorner = \urcorner} * a' * b') = \mathbb{l}en(\overline{\ulcorner = \urcorner}) + \mathbb{l}en(a') + \mathbb{l}en(b')$	T13.47f
26.	$\mathbb{l}en(\overline{\ulcorner = \urcorner}) + \mathbb{l}en(a') + \mathbb{l}en(b') \leq \mathbb{l}en(\overline{\ulcorner = \urcorner}) \times \mathbb{l}en(s) + \mathbb{l}en(a) \times \mathbb{l}en(s) + \mathbb{l}en(b) \times \mathbb{l}en(s)$	23,11,14 T13.13v
27.	$\mathbb{l}en(\overline{\ulcorner = \urcorner}) \times \mathbb{l}en(s) + \mathbb{l}en(a) \times \mathbb{l}en(s) + \mathbb{l}en(b) \times \mathbb{l}en(s) = [\mathbb{l}en(\overline{\ulcorner = \urcorner}) + \mathbb{l}en(a) + \mathbb{l}en(b)] \times \mathbb{l}en(s)$	T6.64
28.	$\mathbb{l}en(\overline{\ulcorner = \urcorner}) + \mathbb{l}en(a') + \mathbb{l}en(b') \leq [\mathbb{l}en(\overline{\ulcorner = \urcorner}) + \mathbb{l}en(a) + \mathbb{l}en(b)] \times \mathbb{l}en(s)$	26,27 =E
29.	$\mathbb{l}en(\overline{\ulcorner = \urcorner} * a' * b') \leq \mathbb{l}en(\overline{\ulcorner = \urcorner} * a * b) \times \mathbb{l}en(s)$	28,25,24 =E
30.	$\mathbb{l}en(\overline{\ulcorner = \urcorner} * a' * b') \leq \mathbb{l}en(p) \times \mathbb{l}en(s)$	29,6 =E
31.	$j < \mathbb{l}en(\overline{\ulcorner = \urcorner} * a' * b')$	A (g (∀I))
32.	$j < \mathbb{l}en(\overline{\ulcorner = \urcorner}) \vee j \geq \mathbb{l}en(\overline{\ulcorner = \urcorner})$	T13.13q
33.	$j < \mathbb{l}en(\overline{\ulcorner = \urcorner})$	A (g 32∨E)
34.	$\mathbb{e}xp(\overline{\ulcorner = \urcorner} * a' * b', j) = \mathbb{e}xp(\overline{\ulcorner = \urcorner}, j)$	33 T13.47c
35.	$\mathbb{e}xp(\overline{\ulcorner = \urcorner}, j) \leq \overline{\ulcorner = \urcorner}$	T13.44g
36.	$\overline{\ulcorner = \urcorner} \leq \overline{\ulcorner = \urcorner} * a * b$	T13.47n
37.	$\overline{\ulcorner = \urcorner} * a * b \leq \overline{\ulcorner = \urcorner} * a * b + s$	T13.13u
38.	$\mathbb{e}xp(\overline{\ulcorner = \urcorner}, j) \leq \overline{\ulcorner = \urcorner} * a * b + s$	35,36,37 T13.13a
39.	$\mathbb{e}xp(\overline{\ulcorner = \urcorner} * a' * b', j) \leq \overline{\ulcorner = \urcorner} * a * b + s$	34,38 =E

40.	$j \geq \mathbb{len}(\overline{\ulcorner = \urcorner})$	A (g 32∨E)
41.	$\mathbb{len}(\overline{\ulcorner = \urcorner}) = l_e$	def
42.	$j = l_e + (j \dot{-} l_e)$	40 T13.23a
43.	$\mathbb{exp}(\overline{\ulcorner = \urcorner} * a' * b', j) = \mathbb{exp}(a' * b', j \dot{-} l_e)$	42 T13.47g
44.	$j \dot{-} l_e < \mathbb{len}(a') \vee j \dot{-} l_e \geq \mathbb{len}(a')$	T13.13q
45.	$j \dot{-} l_e < \mathbb{len}(a')$	A (g 44 ∨E)
46.	$\mathbb{exp}(a' * b', j \dot{-} l_e) = \mathbb{exp}(a', j \dot{-} l_e)$	45 T13.47c
47.	$\mathbb{exp}(\overline{\ulcorner = \urcorner} * a' * b', j) = \mathbb{exp}(a', j \dot{-} l_e)$	43,46 =E
48.	$\mathbb{exp}(a', j \dot{-} l_e) \leq a + s$	12,45 (∀E)
49.	$\mathbb{exp}(\overline{\ulcorner = \urcorner} * a' * b', j) \leq a + s$	47,48 =E
50.	$a \leq \overline{\ulcorner = \urcorner} * a$	T13.47o
51.	$\overline{\ulcorner = \urcorner} * a \leq \overline{\ulcorner = \urcorner} * a * b$	T13.47n
52.	$a \leq \overline{\ulcorner = \urcorner} * a * b$	50,51 T13.13a
53.	$\mathbb{exp}(\overline{\ulcorner = \urcorner} * a' * b', j) \leq \overline{\ulcorner = \urcorner} * a * b + s$	49,52 T13.13v
54.	$j \dot{-} l_e \geq \mathbb{len}(a')$	A (g 44∨E)
55.	$(j \dot{-} l_e) + l_e \geq l_e + \mathbb{len}(a')$	54 T13.13v
56.	$j \geq l_e + \mathbb{len}(a')$	42,55 =E
57.	$l_e + \mathbb{len}(a') = l_a$	def
58.	$j = l_a + (j \dot{-} l_a)$	56 T13.23a
59.	$\mathbb{len}(\overline{\ulcorner = \urcorner} * a') = l_a$	T13.47f
60.	$\mathbb{exp}(\overline{\ulcorner = \urcorner} * a' * b', j) = \mathbb{exp}(b', j \dot{-} l_a)$	58,59 T13.47g
61.	$\mathbb{len}(\overline{\ulcorner = \urcorner} * a' * b') = l_a + \mathbb{len}(b')$	T13.47f
62.	$j < l_a + \mathbb{len}(b')$	31,61 =E
63.	$l_a + (j \dot{-} l_a) < l_a + \mathbb{len}(b')$	58,62=E
64.	$j \dot{-} l_a < \mathbb{len}(b')$	63 T13.13w
65.	$\mathbb{exp}(b', j \dot{-} l_a) \leq b + s$	15,64 (∀E)
66.	$b \leq \overline{\ulcorner = \urcorner} * a * b$	T13.47o
67.	$b + s \leq \overline{\ulcorner = \urcorner} * a * b + s$	66 T13.13v
68.	$\mathbb{exp}(b', j \dot{-} l_a) \leq \overline{\ulcorner = \urcorner} * a * b + s$	65,67 T13.13a
69.	$\mathbb{exp}(\overline{\ulcorner = \urcorner} * a' * b', j) \leq \overline{\ulcorner = \urcorner} * a * b + s$	60,68 =E
70.	$\mathbb{exp}(\overline{\ulcorner = \urcorner} * a' * b', j) \leq \overline{\ulcorner = \urcorner} * a * b + s$	44,45-69 ∨E
71.	$\mathbb{exp}(\overline{\ulcorner = \urcorner} * a' * b', j) \leq \overline{\ulcorner = \urcorner} * a * b + s$	32,33-70 ∨E
72.	$\mathbb{exp}(\overline{\ulcorner = \urcorner} * a' * b', j) \leq p + s$	71,6 =E
73.	$(\forall k < \mathbb{len}(\overline{\ulcorner = \urcorner} * a' * b'))\mathbb{exp}(\overline{\ulcorner = \urcorner} * a' * b', k) \leq p + s$	31-72 (∀I)
74.	$\exists q[\mathbb{A}tomsub(p, v, s, q) \wedge \mathbb{len}(q) \leq \mathbb{len}(p) \times \mathbb{len}(s) \wedge (\forall k < \mathbb{len}(q))\mathbb{exp}(q, k) \leq p + s]$	22,30,73 ∃I
75.	$\exists q[\mathbb{A}tomsub(p, v, s, q) \wedge \mathbb{len}(q) \leq \mathbb{len}(p) \times \mathbb{len}(s) \wedge (\forall k < \mathbb{len}(q))\mathbb{exp}(q, k) \leq p + s]$	9,13-74 ∃E
76.	$\exists q[\mathbb{A}tomsub(p, v, s, q) \wedge \mathbb{len}(q) \leq \mathbb{len}(p) \times \mathbb{len}(s) \wedge (\forall k < \mathbb{len}(q))\mathbb{exp}(q, k) \leq p + s]$	8,10-75 ∃E
77.	$\exists q[\mathbb{A}tomsub(p, v, s, q) \wedge \mathbb{len}(q) \leq \mathbb{len}(p) \times \mathbb{len}(s) \wedge (\forall k < \mathbb{len}(q))\mathbb{exp}(q, k) \leq p + s]$	4,5-76 (∃E)
78.	$[\mathbb{A}tomic(p) \wedge \mathbb{T}erm(s)] \rightarrow \exists q[\mathbb{A}tomsub(p, v, s, q) \wedge \mathbb{len}(q) \leq \mathbb{len}(p) \times \mathbb{len}(s) \wedge (\forall k < \mathbb{len}(q))\mathbb{exp}(q, k) \leq p + s]$	1-77 →I

E13.39. Work the case marked “similarly” on line 115 of T13.52a and the D case from T13.52f. Hard core: show each of the results from T13.52.

T13.52.

T13.52.a.

1.	$\forall u[(\mathcal{P}(u) \wedge \mathit{len}(u) \leq x) \to (\forall k < \mathit{len}(u) \sim \mathcal{P}(\mathit{val}(u,k)]$	P
2.	$\mathit{val}(c,j) * \mathit{val}(a, j \dot{-} l_1) * \mathit{val}(c_1, j \dot{-} l_2) * \mathit{val}(b, j \dot{-} l_3) * \mathit{val}(c_2, j \dot{-} l_4) = c * d * c_1 * e * c_2$	P
3.	$\mathcal{P}(a) \wedge \mathcal{P}(b) \wedge \mathcal{P}(d) \wedge \mathcal{P}(e)$	P
4.	$\forall v(\mathcal{P}(v) \to v > \overline{1})$	P
5.	$\mathit{len}(c) = 1 \wedge c_1 > \emptyset \wedge c_2 > \emptyset \wedge \mathit{len}(c_1) \leq 1 \wedge \mathit{len}(c_2) \leq 1$	P
6.	$j < l \wedge Sx \geq l$	P
7.	$a > \overline{1} \wedge b > \overline{1} \wedge d > \overline{1} \wedge e > \overline{1}$	3,4 ∀E
8.	$\mathit{val}(a, \mathit{len}(a)) = a \wedge \mathit{val}(b, \mathit{len}(b)) = b \wedge \mathit{val}(d, \mathit{len}(d)) = d \wedge \mathit{val}(e, \mathit{len}(e)) = e$	7 T13.46n
9.	$c > \emptyset$	5 T13.45g
10.	$\mathit{val}(c, \mathit{len}(c)) = c \wedge \mathit{val}(c_1, \mathit{len}(c_1)) = c_1 \wedge \mathit{val}(c_2, \mathit{len}(c_2)) = c_2$	5,9 T13.46n
11.	$l = S(\mathit{len}(a) + \mathit{len}(c_1) + \mathit{len}(b) + \mathit{len}(c_2))$	5 T6.47
12.	$Sx \geq S(\mathit{len}(a) + \mathit{len}(c_1) + \mathit{len}(b) + \mathit{len}(c_2))$	6,11 =E
13.	$x \geq \mathit{len}(a) + \mathit{len}(c_1) + \mathit{len}(b) + \mathit{len}(c_2)$	12 T13.13j
14.	$\mathit{len}(a) \leq x \wedge \mathit{len}(b) \leq x$	13 T13.13u
15.	$\mathit{len}(\mathit{val}(c,j) * \mathit{val}(a, j \dot{-} l_1) * \mathit{val}(c_1, j \dot{-} l_2) * \mathit{val}(b, j \dot{-} l_3) * \mathit{val}(c_2, j \dot{-} l_4)) =$ $\mathit{len}(\mathit{val}(c,j)) + \mathit{len}(\mathit{val}(a, j \dot{-} l_1)) + \mathit{len}(\mathit{val}(c_1, j \dot{-} l_2)) + \mathit{len}(\mathit{val}(b, j \dot{-} l_3)) + \mathit{len}(\mathit{val}(c_2, j \dot{-} l_4))$	T13.47f
16.	$\mathit{len}(\mathit{val}(c,j)) + \mathit{len}(\mathit{val}(a, j \dot{-} l_1)) + \mathit{len}(\mathit{val}(c_1, j \dot{-} l_2)) + \mathit{len}(\mathit{val}(b, j \dot{-} l_3) + \mathit{len}(\mathit{val}(c_2, j \dot{-} l_4)) \leq l$	T13.46k,T13.13v
17.	$\mathit{len}(c * d * c_1 * e * c_2) \leq l$	2,15,16 =E
18.	$\mathit{len}(c * d * c_1 * e * c_2) = S(\mathit{len}(d) + \mathit{len}(c_1) + \mathit{len}(e) + \mathit{len}(c_2))$	5 T13.47f
19.	$S(\mathit{len}(d) + \mathit{len}(c_1) + \mathit{len}(e) + \mathit{len}(c_2)) \leq Sx$	17,18,6 T13.13a
20.	$\mathit{len}(d) + \mathit{len}(c_1) + \mathit{len}(e) + \mathit{len}(c_2) \leq x$	19 T13.13j
21.	$\mathit{len}(d) \leq x \wedge \mathit{len}(e) \leq x$	20 T13.13u
22.	$j < l_1$	A (c ∼I)
23.	$j = \emptyset$	5,22 T8.16
24.	$j \dot{-} l_1 = \emptyset \wedge j \dot{-} l_2 = \emptyset \wedge j \dot{-} l_3 = \emptyset \wedge j \dot{-} l_4 = \emptyset$	23 T13.23b
25.	$\mathit{val}(c,j) = \overline{1} \wedge \mathit{val}(a, j \dot{-} l_1) = \overline{1} \wedge \mathit{val}(c_1, j \dot{-} l_2) = \overline{1} \wedge \mathit{val}(b, j \dot{-} l_3) = \overline{1} \wedge \mathit{val}(c_2, j \dot{-} l_4) = \overline{1}$	23,24 def
26.	$\mathit{val}(c,j) * \mathit{val}(a, j \dot{-} l_1) * \mathit{val}(c_1, j \dot{-} l_2) * \mathit{val}(b, j \dot{-} l_3) * \mathit{val}(c_2, j \dot{-} l_4) = \overline{1}$	25 T13.47i
27.	$c * d * c_1 * e * c_2 = \overline{1}$	2, 26 =E
28.	$\mathit{len}(c * d * c_1 * e * c_2) \geq \overline{1}$	5 T13.47f
29.	$c * d * c_1 * e * c_2 > \overline{1}$	T13.45g
30.	$\overline{1} > \overline{1}$	27,29 =E
31.	$\overline{1} \not> \overline{1}$	T13.13s
32.	$\bot$	30,31 ⊥I
33.	$j \not< l_1$	22-32 ∼I
34.	$j \geq l_1$	33 T13.13r
35.	$\mathit{val}(c,j) = c$	9,34 T13.46n
36.	$\mathit{val}(a, j \dot{-} l_1) * \mathit{val}(c_1, j \dot{-} l_2) * \mathit{val}(b, j \dot{-} l_3) * \mathit{val}(c_2, j \dot{-} l_4) > \emptyset$	T13.47c
37.	$d * c_1 * e * c_2 > \emptyset$	T13.47c
38.	$\mathit{val}(a, j \dot{-} l_1) * \mathit{val}(c_1, j \dot{-} l_2) * \mathit{val}(b, j \dot{-} l_3) * \mathit{val}(c_2, j \dot{-} l_4) = d * c_1 * e * c_2$	2,35,36,37 T13.47l
39.	$j < l_2$	A (c ∼I)
40.	$j \dot{-} l_2 = \emptyset \wedge j \dot{-} l_3 = \emptyset \wedge j \dot{-} l_4 = \emptyset$	39 T13.23b
41.	$\mathit{val}(c_1, j \dot{-} l_2) = \overline{1} \wedge \mathit{val}(b, j \dot{-} l_3) = \overline{1} \wedge \mathit{val}(c_2, j \dot{-} l_4) = \overline{1}$	40 def
42.	$\mathit{val}(a, j \dot{-} l_1) > \emptyset$	41 T13.46i
43.	$\mathit{val}(a, j \dot{-} l_1) * \mathit{val}(c_1, j \dot{-} l_2) * \mathit{val}(b, j \dot{-} l_3) * \mathit{val}(c_2, j \dot{-} l_4) = \mathit{val}(a, j \dot{-} l_1)$	42,41 T13.47i
44.	$\mathit{val}(a, j \dot{-} l_1) = d * c_1 * e * c_2$	38,43 =E
45.	$\mathit{len}(d * c_1 * e * c_2) = \mathit{len}(d) + \mathit{len}(c_1) + \mathit{len}(e) + \mathit{len}(c_2)$	T13.47f
46.	$\mathit{len}(d) \leq \mathit{len}(d * c_1 * e * c_2)$	45 T13.13u
47.	$\mathit{len}(d) \leq \mathit{len}(\mathit{val}(a, j \dot{-} l_1))$	46,44 =E
48.	$\mathit{len}(\mathit{val}(a, j \dot{-} l_1)) \leq j \dot{-} l_1$	T13.46j
49.	$\mathit{len}(d) \leq j \dot{-} l_1$	47,48 T13.13a
50.	$z < \mathit{len}(d)$	A (g (∀I))
51.	$\mathit{exp}(d * c_1 * e * c_2, z) = \mathit{exp}(d, z)$	50 T13.47c
52.	$z < \mathit{len}(\mathit{val}(a, j \dot{-} l_1))$	47,50 T13.13c
53.	$\mathit{exp}(\mathit{val}(a, j \dot{-} l_1) * \mathit{val}(c_1, j \dot{-} l_2) * \mathit{val}(b, j \dot{-} l_3) * \mathit{val}(c_2, j \dot{-} l_4, z) = \mathit{exp}(\mathit{val}(a, j \dot{-} l_1), z)$	52 T13.47c
54.	$z < j \dot{-} l_1$	50,49 T13.13c
55.	$\mathit{exp}(\mathit{val}(a, j \dot{-} l_1), z) = \mathit{exp}(a, z)$	54 T13.46l
56.	$\mathit{exp}(a, z) = \mathit{exp}(d, z)$	38,51,53,55 =E
57.	$(\forall z < \mathit{len}(d))\mathit{exp}(a, z) = \mathit{exp}(d, z)$	50-56 (∀I)
58.	$\mathit{val}(a, \mathit{len}(d)) = \mathit{val}(d, \mathit{len}(d))$	57 T13.46m
59.	$d = \mathit{val}(a, \mathit{len}(d))$	58,8 =E
60.	$\mathcal{P}(\mathit{val}(a, \mathit{len}(d)))$	3,59 =E
61.	$j \dot{-} l_1 < l_2 \dot{-} l_1$	34,39 T13.23e
62.	$l_2 \dot{-} l_1 = \mathit{len}(a)$	T13.23l
63.	$\mathit{len}(d) < \mathit{len}(a)$	49,61,62 T13.13c
64.	$\sim\mathcal{P}(\mathit{val}(a, \mathit{len}(d)))$	1,3,14,63 ∀E
65.	$\bot$	60,64 ⊥I
66.	$j \not< l_2$	39-65 ∼I

Exercise 13.39 T13.52.a

66.	$j \geq l_2$	66 T13.13r
67.	$l_2 \geq l_1$	T13.13u
68.	$j \dot{-} l_1 \geq l_2 \dot{-} l_1$	66,67 T13.23d
69.	$l_2 \dot{-} l_1 = \mathbb{l}en(a)$	T13.23l
70.	$j \dot{-} l_1 \geq \mathbb{l}en(a)$	68,69 =E
71.	$val(a, j \dot{-} l_1) = a$	7,70 T13.46n
72.	$\mathbb{l}en(d) < \mathbb{l}en(a) \vee \mathbb{l}en(d) = \mathbb{l}en(a) \vee \mathbb{l}en(d) > \mathbb{l}en(a)$	T13.13p
73.	$\mathbb{l}en(d) < \mathbb{l}en(a)$	A (c 72∨E)
74.	$z < \mathbb{l}en(d)$	A (g (∀I))
75.	$\mathbb{e}xp(d * c_1 * e * c_2, z) = \mathbb{e}xp(d, z)$	74 T13.47c
76.	$z < \mathbb{l}en(val(a, j \dot{-} l_1))$	71,73,74 T13.13c
77.	$\mathbb{e}xp(val(a, j \dot{-} l_1) * val(c_1, j \dot{-} l_2) * val(b, j \dot{-} l_3) * val(c_2, l \dot{-} l_4), z) = \mathbb{e}xp(val(a, j \dot{-} l_1), z)$	76 T13.47c
78.	$\mathbb{e}xp(a, z) = \mathbb{e}xp(d, z)$	71,77,75,38 =E
79.	$(\forall z < \mathbb{l}en(d))\mathbb{e}xp(a, z) = \mathbb{e}xp(d, z)$	74-78 (∀I)
80.	$val(a, \mathbb{l}en(d)) = val(d, \mathbb{l}en(d))$	79 T13.46m
81.	$val(a, \mathbb{l}en(d)) = d$	80,8 =E
82.	$\mathcal{P}(val(a, \mathbb{l}en(d)))$	3,81 =E
83.	$\sim\mathcal{P}(val(a, \mathbb{l}en(d)))$	1,3,14,73 ∀E
84.	$\bot$	82,83 ⊥I
85.	$\mathbb{l}en(d) > \mathbb{l}en(a)$	A (c 72∨E)
86.	$\bot$	similarly (72)
87.	$\mathbb{l}en(d) = \mathbb{l}en(a)$	A (c 72∨E)
88.	$z < \mathbb{l}en(d)$	A (g (∀I))
89.	$z < \mathbb{l}en(a)$	88,87 =E
90.	$z < \mathbb{l}en(val(a, j \dot{-} l_1))$	71,89 =E
91.	$\mathbb{e}xp(d * c_1 * e * c_2, z) = \mathbb{e}xp(d, z)$	88 T13.47c
92.	$\mathbb{e}xp(val(a, j \dot{-} l_1) * val(c_1, j \dot{-} l_2) * val(b, j \dot{-} l_3) * val(c_2, j \dot{-} l_4), z) = \mathbb{e}xp(val(a, j \dot{-} l_1), z)$	90 T13.47c
93.	$\mathbb{e}xp(val(a, j \dot{-} l_1), z) = \mathbb{e}xp(d, z)$	92,91,38 =E
94.	$(\forall z < \mathbb{l}en(d))\mathbb{e}xp(val(a, j \dot{-} l_1), z) = \mathbb{e}xp(d, z)$	88-93 (∀I)
95.	$val(val(a, j \dot{-} l_1), \mathbb{l}en(val(a, j \dot{-} l_1))) = val(d, \mathbb{l}en(d))$	94,71,87 T13.46m
96.	$val(a, j \dot{-} l_1) > \emptyset$	T13.46i
97.	$val(val(a, j \dot{-} l_1), \mathbb{l}en(val(a, j \dot{-} l_1))) = val(a, j \dot{-} l_1)$	96 T13.46n
98.	$val(a, j \dot{-} l_1) = d$	95,97,8 =E
99.	$val(c_1, j \dot{-} l_2) * val(b, j \dot{-} l_3) * val(c_2, j \dot{-} l_4)) > \emptyset$	T13.47c
100.	$c_1 * e * c_2 > \emptyset$	T13.47c
101.	$val(c_1, j \dot{-} l_2) * val(b, j \dot{-} l_3) * val(c_2, j \dot{-} l_4) = c_1 * e * c_2$	98,38,99,100 T13.47l
102.	$j < l_3$	A (c ∼I)
103.	$\bot$	similarly (22)
104.	$j \not< l_3$	102-103 ∼I
105.	$j \geq l_3$	104 T13.13r
106.	$l_3 \geq l_2$	T13.13u
107.	$j \dot{-} l_2 \geq l_3 \dot{-} l_2$	105,106 T13.23d
108.	$l_3 \dot{-} l_2 = \mathbb{l}en(c_1)$	T13.23l
109.	$j \dot{-} l_2 \geq \mathbb{l}en(c_1)$	107,108 =E
110.	$val(c_1, j \dot{-} l_2) = c_1$	5,105 T13.46n
111.	$val(b, j \dot{-} l_3) * val(c_2, j \dot{-} l_4) > \emptyset$	T13.47c
112.	$e * c_2 > \emptyset$	T13.47c
113.	$val(b, j \dot{-} l_3) * val(c_2, j \dot{-} l_4) = e * c_2$	101,110,111,112 T13.47l
114.	$j < l_4$	A (c ∼I)
115.	$\bot$	similarly (39)
116.	$j \not< l_4$	114-115 ∼I

Exercise 13.39 T13.52.a

117.	$j \geq l_4$	116 T13.13r
118.	$l_4 \geq l_3$	T13.13u
119.	$j \dot{-} l_3 \geq l_4 \dot{-} l_3$	117,118 T13.23d
120.	$l_4 \dot{-} l_3 = \mathbb{l}en(b)$	T13.23l
121.	$j \dot{-} l_3 \geq \mathbb{l}en(b)$	119,120 =E
122.	$val(b, j \dot{-} l_3) = b$	121,7 T13.46n
123.	$\mathbb{l}en(e) < \mathbb{l}en(b) \vee \mathbb{l}en(e) = \mathbb{l}en(b) \vee \mathbb{l}en(e) > \mathbb{l}en(b)$	
124.	$\mathbb{l}en(e) < \mathbb{l}en(b)$	A (c 123$\vee$E)
125.	$\bot$	similarly (72)
126.	$\mathbb{l}en(e) > \mathbb{l}en(b)$	A (c 123$\vee$E)
127.	$\bot$	similarly (72)
128.	$\mathbb{l}en(e) = \mathbb{l}en(b)$	A (c 123$\vee$E)
129.	$val(b, j \dot{-} l_3) = e$	similarly
130.	$val(c_2, j \dot{-} l_4) > \emptyset$	T13.46i
131.	$val(c_2, j \dot{-} l_4) = c_2$	113,130,5 T13.47l
132.	$\mathbb{l}en(val(c_2, j \dot{-} l_4)) = \mathbb{l}en(c_2)$	131 =E
133.	$\mathbb{l}en(val(c_2, j \dot{-} l_4)) \leq j \dot{-} l_4$	T13.46j
134.	$j \dot{-} l_4 \geq \mathbb{l}en(c_2)$	133,134 =E
135.	$(j \dot{-} l_4) + l_4 \geq \mathbb{l}en(c_2) + l_4$	134 T13.13v
136.	$j = l_4 + (j \dot{-} l_4)$	117 T13.23a
137.	$j \geq l$	135,136 =E
138.	$j \not< l$	137 T13.13r
139.	$\bot$	138,6 $\bot$I
140.	$\bot$	123,124-139 $\vee$E
141.	$\bot$	72,73-140 $\vee$E

T13.52.f. PA $\vdash \mathbb{T}erm(t) \rightarrow (\forall k < len(t)) {\sim} \mathbb{T}erm(val(t, k))$

1.	$\mathbb{T}erm(t) \wedge \mathbb{l}en(t) \leq \emptyset$	A ($g \to$I)
2.	$k < \mathbb{l}en(t)$	A (g ($\forall$I))
3.	$\mathbb{T}erm(val(t,k))$	A ($c \sim$I)
4.	$k < \emptyset$	1,2 T13.13c
5.	$k \not< \emptyset$	T13.13d,r
6.	$\bot$	4,5 $\bot$I
7.	$\sim\mathbb{T}erm(val(t,k))$	3-6 $\sim$I
8.	$(\forall k < len(t))\sim\mathbb{T}erm(val(t,k))$	2-7 ($\forall$I)
9.	$(\mathbb{T}erm(t) \wedge \mathbb{l}en(t) \leq \emptyset) \to (\forall k < len(t))\sim\mathbb{T}erm(val(t,k))$	1-8 $\to$ I
10.	$\forall t[(\mathbb{T}erm(t) \wedge \mathbb{l}en(t) \leq \emptyset) \to (\forall k < len(t))\sim\mathbb{T}erm(val(t,k))]$	9 $\forall$I
11.	$\forall t[(\mathbb{T}erm(t) \wedge \mathbb{l}en(t) \leq x) \to (\forall k < len(t))\sim\mathbb{T}erm(val(t,k))]$	A ($g \to$I)
12.	$\mathbb{T}erm(a) \wedge \mathbb{l}en(a) \leq Sx$	A ($g \to$I)
13.	$\mathbb{T}erm(a)$	12 $\wedge$E
14.	$\mathbb{l}en(a) \leq Sx$	12 $\wedge$E
15.	$j < len(a)$	A (g ($\forall$I))
16.	$j = \emptyset \vee j > \emptyset$	T13.13d,m
17.	$j = \emptyset$	A (g 16$\vee$E)
18.	$val(a,j) = \overline{1}$	17 def
19.	$val(a,j) \not> \overline{1}$	18 T13.13m,r
20.	$\sim\mathbb{T}erm(val(a,j))$	19 T13.48f
21.	$j > \emptyset$	A (g 16$\vee$E)
22.	$j = S(j \dot{-} \overline{1})$	21 T13.23j
23.	$S(j \dot{-} \overline{1}) < \mathbb{l}en(a)$	15,22 =E
24.	$\mathbb{T}ermseq(m,a)$	13 T13.48b
25.	$\mathbb{e}xp(m, \mathbb{l}en(m) \dot{-} \overline{1}) = a$	24 T13.48a
26.	$m > \overline{1}$	24 T13.48a
27.	$(\forall k < \mathbb{l}en(m))[A(m,k) \vee B(m,k) \vee C(m,k) \vee D(m,k)]$	24 T13.48a
28.	$\mathbb{l}en(m) > \emptyset$	26 T13.45j
29.	$\mathbb{l}en(m) \dot{-} \overline{1} < \mathbb{l}en(m)$	28 T13.23i
30.	$A(m, \mathbb{l}en(m) \dot{-} \overline{1}) \vee B(m, \mathbb{l}en(m) \dot{-} \overline{1}) \vee C(m, \mathbb{l}en(m) \dot{-} \overline{1}) \vee D(m, \mathbb{l}en(m) \dot{-} \overline{1})$	27,29 ($\forall$E)
31.	$\mathbb{T}erm(val(a,j))$	A ($c \sim$I)
32.	$A(m, \mathbb{l}en(m) \dot{-} \overline{1})$	A (c 30 $\vee$E)
33.	$a = \overline{\ulcorner \emptyset \urcorner} \vee \mathbb{V}ar(a)$	32,25 abv
34.	$a = \overline{\ulcorner \emptyset \urcorner}$	A (g 33$\vee$E)
35.	$\mathbb{l}en(a) = \overline{1}$	34 cap
36.	$\mathbb{V}ar(a)$	A (g 33$\vee$E)
37.	$(\exists x \leq a)a = \overline{2}^{\overline{23}+\overline{2}x}$	36 def
38.	$a = \overline{2}^{\overline{23}+\overline{2}x}$	A (g 37 ($\exists$E))
39.	$\mathbb{l}en(a) = \overline{1}$	38 T13.45k
40.	$\mathbb{l}en(a) = \overline{1}$	37,38-39 ($\exists$E)
41.	$\mathbb{l}en(a) = \overline{1}$	33,34-35,36-40 $\vee$E
42.	$j < \emptyset \vee j = \emptyset$	15,41 T13.13n
43.	$j = \emptyset$	42 T13.13d,r
44.	$\bot$	21,43 $\bot$I
45.	$B(m, \mathbb{l}en(m) \dot{-} \overline{1})$	A (c 30 $\vee$E)
46.	$(\exists j < \mathbb{l}en(m) \dot{-} \overline{1})a = \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,j)$	45,25 abv
47.	$l < \mathbb{l}en(m) \dot{-} \overline{1}$	A (c 46 ($\exists$E))
48.	$a = \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,l)$	
49.	$l < \mathbb{l}en(m)$	29,47 T13.13b
50.	$\mathbb{T}erm(\mathbb{e}xp(m,l))$	24,49 T13.48n
51.	$\mathbb{l}en(\overline{\ulcorner S \urcorner}) = \overline{1}$	cap
52.	$\overline{\ulcorner S \urcorner} > \emptyset$	51 T13.45g
53.	$\mathbb{e}xp(m,l) > \emptyset$	49,24 T13.48e
54.	$val(\overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,l), j) = val(\overline{\ulcorner S \urcorner}, j) * val(\mathbb{e}xp(m,l), j \dot{-} \overline{1})$	51,52,53 T13.47m
55.	$val(\overline{\ulcorner S \urcorner}, j) = \overline{\ulcorner S \urcorner}$	21,51 T13.46n
56.	$val(a,j) = \overline{\ulcorner S \urcorner} * val(\mathbb{e}xp(m,l), j \dot{-} \overline{1})$	54,48,55 =E
57.	$\exists r[\overline{\ulcorner S \urcorner} * val(\mathbb{e}xp(m,l), j \dot{-} \overline{1}) = \overline{\ulcorner S \urcorner} * r \wedge \mathbb{T}erm(r)]$	31,56 T13.52c

Exercise 13.39 T13.32.f

58.	$\overline{\ulcorner S\urcorner} * val(exp(m,l), j \dot{-} \overline{1}) = \overline{\ulcorner S\urcorner} * r$	A (*c* 57∃E)
59.	$\mathbb{T}erm(r)$	
60.	$val(exp(m,l), j \dot{-} \overline{1}) > \emptyset$	T13.46i
61.	$r > \emptyset$	59 T13.48f
62.	$val(exp(m,l), j \dot{-} \overline{1}) = r$	58,60,61 T13.47l
63.	$\mathbb{T}erm(val(exp(m,l), j \dot{-} \overline{1}))$	59,62 =E
64.	$len(a) = len(\overline{\ulcorner S\urcorner}) + len(exp(m,l))$	48 T13.47f
65.	$len(a) = \overline{1} + len(exp(m,l))$	64,51 =E
66.	$len(a) = S\,len(exp(m,l))$	65 T6.47
67.	$S\,len(exp(m,l)) \leq Sx$	14,66 =E
68.	$len(exp(m,l)) \leq x$	67 T13.13j
69.	$S(j \dot{-} \overline{1}) < S\,len(exp(m,l))$	66,23 =E
70.	$j \dot{-} \overline{1} < len(exp(m,l))$	69 T13.13k
71.	$\sim\mathbb{T}erm(val(exp(m,l), j \dot{-} \overline{1}))$	11,50,68,70 (∀E)
72.	$\bot$	63,71 ⊥I
73.	$\bot$	57,58-72 ∃E
74.	$\bot$	46,47-73 (∃E)
75.	$C(m, len(m) \dot{-} \overline{1})$	A (*c* 30 ∨E)
76.	$(\exists i < len(m) \dot{-} \overline{1})(\exists j < len(m) \dot{-} \overline{1})a = \overline{\ulcorner + \urcorner} * exp(m,i) * exp(m,j)$	75 abv
77.	$k < len(m) \dot{-} \overline{1}$	A (*c* 76(∃E))
78.	$l < len(m) \dot{-} \overline{1}$	
79.	$a = \overline{\ulcorner + \urcorner} * exp(m,k) * exp(m,l)$	
80.	$k < len(m)$	29,77 T13.13b
81.	$l < len(m)$	29,78 T13.13b
82.	$\mathbb{T}erm(exp(m,k))$	24,80 T13.48n
83.	$\mathbb{T}erm(exp(m,l))$	24,81 T13.48n
84.	$len(\overline{\ulcorner + \urcorner}) = \overline{1}$	cap
85.	$\overline{\ulcorner + \urcorner} > \emptyset$	84 T13.45g
86.	$exp(m,k) > \emptyset$	77,24 T13.48e
87.	$exp(m,l) > \emptyset$	78,24 T13.48e
88.	$val(\overline{\ulcorner + \urcorner} * exp(m,k) * exp(m,l), j) =$ $val(\overline{\ulcorner + \urcorner}, j) * val(exp(m,k), j \dot{-} \overline{1}) * val(exp(m,l), j \dot{-} (\overline{1} + len(exp(m,k))))$	84,85,86,87 T13.47m
89.	$val(\overline{\ulcorner + \urcorner}, j) = \overline{\ulcorner + \urcorner}$	21,84 T13.46n
90.	$val(a, j) = \overline{\ulcorner + \urcorner} * val(exp(m,k), j \dot{-} \overline{1}) * val(exp(m,l), j \dot{-} (\overline{1} + len(exp(m,k))))$	88,79,89 =E
91.	$\exists r \exists s[\overline{\ulcorner + \urcorner} * val(exp(m,k), j \dot{-} \overline{1}) * val(exp(m,l), j \dot{-} (\overline{1} + len(exp(m,k)))) =$ $\overline{\ulcorner + \urcorner} * r * s \wedge \mathbb{T}erm(r) \wedge \mathbb{T}erm(s)$	31,90 T13.52d
92.	$\overline{\ulcorner + \urcorner} * val(exp(m,k), j \dot{-} \overline{1}) * val(exp(m,l), j \dot{-} (\overline{1} + len(exp(m,k)))) = \overline{\ulcorner + \urcorner} * r * s$	A (*c* 91∃E)
93.	$\mathbb{T}erm(r)$	
94.	$\mathbb{T}erm(s)$	
95.	$val(\overline{\ulcorner + \urcorner}, j) * val(exp(m,k), j \dot{-} \overline{1}) * val(exp(m,l), j \dot{-} (\overline{1} + len(exp(m,k)))) = \overline{\ulcorner + \urcorner} * r * s$	92,89 =E
96.	$\mathbb{T}erm(exp(m,k)) \wedge \mathbb{T}erm(exp(m,l)) \wedge \mathbb{T}erm(r) \wedge \mathbb{T}erm(s)$	82,83,93,94 ∧I
97.	$\forall v(\mathbb{T}erm(v) \rightarrow v > \overline{1})$	T13.48f
98.	$len(a) \leq Sx \wedge j < len(a)$	14,15 ∧I
99.	$\bot$	11,95,96,97,84,98 T13.52a
100.	$\bot$	91,92-99 ∃E
101.	$\bot$	76,77-100 (∃E)
102.	$D(m, len(m) \dot{-} \overline{1})$	A (*c* 30 ∨E)
103.	$\bot$	similarly
104.	$\bot$	30,32-103 ∨E
105.	$\sim\mathbb{T}erm(val(a, j))$	31-104 ∼I
106.	$\sim\mathbb{T}erm(val(a, j))$	16,17-20,21-105 ∨E
107.	$(\forall k < len(a))\sim\mathbb{T}erm(val(a,k))$	15-106 (∀I)
108.	$(\mathbb{T}erm(a) \wedge len(a) \leq Sx) \rightarrow (\forall k < len(a))\sim\mathbb{T}erm(val(a,k))$	12-108 →I
109.	$\forall t[(\mathbb{T}erm(t) \wedge len(t) \leq Sx) \rightarrow (\forall k < len(t))\sim\mathbb{T}erm(val(t,k))]$	108 ∀I
110.	$\forall t[(\mathbb{T}erm(t) \wedge len(t) \leq x) \rightarrow (\forall k < len(t))\sim\mathbb{T}erm(val(t,k))] \rightarrow$ $\forall t[(\mathbb{T}erm(t) \wedge len(t) \leq Sx) \rightarrow (\forall k < len(t))\sim\mathbb{T}erm(val(t,k))]$	11-109 →I
111.	$\forall t[(\mathbb{T}erm(t) \wedge len(t) \leq x) \rightarrow (\forall k < len(t))\sim\mathbb{T}erm(val(t,k))]$	10,110 IN

Exercise 13.39 T13.52.f

E13.40. Show (g) including at least the A case, and (k) from T13.53. Hard core: show each of the results from T13.53.

T13.53.

T13.53.h. PA $\vdash [\mathbb{Wff}(p)) \wedge \mathbb{Wff}(q) \wedge \mathbb{Wff}(a) \wedge \mathbb{Wff}(b)] \to [\mathbb{cnd}(p,q) = \mathbb{cnd}(a,b) \to (p = a \wedge q = b)]$

1.	$\mathbb{Wff}(p)) \wedge \mathbb{Wff}(q) \wedge \mathbb{Wff}(a) \wedge \mathbb{Wff}(b)$	A ($g \to$I)
2.	$\mathbb{cnd}(p,q) = \mathbb{cnd}(a,b)$	A ($g \to$I)
3.	$\overline{\ulcorner(\urcorner} * p * \overline{\ulcorner\to\urcorner} * q * \overline{\ulcorner)\urcorner} = \overline{\ulcorner(\urcorner} * a * \overline{\ulcorner\to\urcorner} * b * \overline{\ulcorner)\urcorner}$	2 def
4.	$p > \overline{1} \wedge q > \overline{1} \wedge a > \overline{1} \wedge b > \overline{1}$	1 T13.49e
5.	$p * \overline{\ulcorner\to\urcorner} * q * \overline{\ulcorner)\urcorner} > \overline{1} \wedge a * \overline{\ulcorner\to\urcorner} * b * \overline{\ulcorner)\urcorner} > \overline{1}$	4 T13.47n
6.	$p * \overline{\ulcorner\to\urcorner} * q * \overline{\ulcorner)\urcorner} = p * \overline{\ulcorner\to\urcorner} * q * \overline{\ulcorner)\urcorner}$	3,5 T13.47l
7.	$p * \overline{\ulcorner\to\urcorner} * q > \overline{1} \wedge a * \overline{\ulcorner\to\urcorner} * b > \overline{1}$	4 T13.47n
8.	$p * \overline{\ulcorner\to\urcorner} * q = a * \overline{\ulcorner\to\urcorner} * b$	6,7 T13.47k
9.	$\mathbb{len}(p) < \mathbb{len}(a) \vee \mathbb{len}(p) = \mathbb{len}(a) \vee \mathbb{len}(p) > \mathbb{len}(a)$	T13.13p
10.	$\mathbb{len}(p) < \mathbb{len}(a)$	A (g ∼I)
11.	$i < \mathbb{len}(p)$	A g (∀I))
12.	$i < \mathbb{len}(a)$	11,10 T13.13b
13.	$\mathbb{exp}(p * \overline{\ulcorner\to\urcorner} * q, i) = \mathbb{exp}(p,i) \wedge \mathbb{exp}(a * \overline{\ulcorner\to\urcorner} * b, i) = \mathbb{exp}(a,i)$	11,12 T13.47c
14.	$\mathbb{exp}(p,i) = \mathbb{exp}(a,i)$	8,13 =E
15.	$(\forall i < \mathbb{len}(p))\mathbb{exp}(p,i) = \mathbb{exp}(a,i)$	11-14 (∀I)
16.	$\mathbb{val}(p, \mathbb{len}(p)) = \mathbb{val}(a, \mathbb{len}(p))$	15 T13.46m
17.	$p = \mathbb{val}(a, \mathbb{len}(p))$	16,4 T13.46n
18.	$\mathbb{Wff}(\mathbb{val}(a, \mathbb{len}(p)))$	17,1 =E
19.	$\sim\mathbb{Wff}(\mathbb{val}(a, \mathbb{len}(p)))$	1,10 T13.52g
20.	$\bot$	18,19 ⊥I
21.	$\mathbb{len}(p) \not< \mathbb{len}(a)$	10-20 ∼I
22.	$\mathbb{len}(p) > \mathbb{len}(a)$	A (g ∼I)
23.	$\bot$	similarly
24.	$\mathbb{len}(p) \not> \mathbb{len}(a)$	22-23 ∼I
25.	$\mathbb{len}(p) = \mathbb{len}(a)$	9,21,24 DS
26.	$\overline{\ulcorner\to\urcorner} * q > 1 \wedge \overline{\ulcorner\to\urcorner} * b > 1$	4 T13.47o
27.	$\overline{\ulcorner\to\urcorner} * q = \overline{\ulcorner\to\urcorner} * b$	8,25,26 T13.47l
28.	$q = b$	27,4 T13.47l
29.	$p * \overline{\ulcorner\to\urcorner} > 1 \wedge a * \overline{\ulcorner\to\urcorner} > \overline{1}$	4 T13.47n
30.	$p * \overline{\ulcorner\to\urcorner} = a * \overline{\ulcorner\to\urcorner}$	8,28,29 T13.47k
31.	$p = a$	30,4 T13.47k
32.	$p = a \wedge q = b$	31,28 ∧I
33.	$\mathbb{cnd}(p,q) = \mathbb{cnd}(a,b) \to (p = a \wedge q = b)$	2-32 →I
34.	$[\mathbb{Wff}(p)) \wedge \mathbb{Wff}(q) \wedge \mathbb{Wff}(a) \wedge \mathbb{Wff}(b)] \to [\mathbb{cnd}(p,q) = \mathbb{cnd}(a,b) \to (p = a \wedge q = b)]$	1-33 →I

T13.53.j. PA $\vdash \mathbb{Axiompa}(p) \to \mathbb{Wff}(p)$

The cases for axioms of Q are immediate by capture. The following should be sufficient to see how other cases will go.

PA $\vdash \mathbb{Axiomad6}(n) \to \mathbb{Wff}(n)$

1.	$\mathbb{A}xiomad6(n)$	A (g →I)
2.	$(\exists v \leq n)[\mathbb{V}ar(v) \wedge n = \overline{\ulcorner = \urcorner} * v * v]$	1 T13.40a
3.	$v \leq n$	A (g 2 (∃E))
4.	$\mathbb{V}ar(v) \wedge n = \overline{\ulcorner = \urcorner} * v * v$	
5.	$\mathbb{T}erm(v)$	4 T13.48p
6.	$\mathbb{T}erm(v) \wedge \mathbb{T}erm(v) \wedge n = \overline{\ulcorner = \urcorner} * v * v$	5,4 ∧I
7.	$(\exists x \leq n)(\exists y \leq n)[\mathbb{T}erm(x) \wedge \mathbb{T}erm(y) \wedge n = \overline{\ulcorner = \urcorner} * x * y]$	6,3 (∃I)
8.	$\mathbb{A}tomic(n)$	7 T13.49c
9.	$\mathbb{W}f\!f(n)$	8 T13.49m
10.	$\mathbb{W}f\!f(n)$	2,3-9 (∃E)
11.	$\mathbb{A}xiomad6(n) \rightarrow \mathbb{W}f\!f(n)$	1-10 →I

PA $\vdash \mathbb{A}xiompa7(n) \rightarrow \mathbb{W}f\!f(n)$

1.	$\mathbb{A}xiompa7(p)$	A (g →I)
2.	$(\exists p \leq n)(\exists v \leq n)[\mathbb{W}f\!f(p) \wedge \mathbb{V}ar(v) \wedge n = \mathbb{c}nd(\mathbb{n}eg(\mathbb{c}nd(formsub(p, v, \overline{\ulcorner \emptyset \urcorner}),$ $\mathbb{n}eg(\mathbb{u}nv(v, \mathbb{c}nd(p, formsub(p, v, \overline{\ulcorner S \urcorner} * v)))))), \mathbb{u}nv(v, p))]$	1 T13.40a
3.	$\mathbb{W}f\!f(p) \wedge \mathbb{V}ar(v)$	A (g 2 (∃E))
4.	$n = \mathbb{c}nd(\mathbb{n}eg(\mathbb{c}nd(formsub(p, v, \overline{\ulcorner \emptyset \urcorner}), \mathbb{n}eg(\mathbb{u}nv(v, \mathbb{c}nd(p, formsub(p, v, \overline{\ulcorner S \urcorner} * v)))))), \mathbb{u}nv(v, p))$	
5.	$\mathbb{T}erm(\overline{\ulcorner \emptyset \urcorner}) \wedge \mathbb{T}erm(\overline{\ulcorner S \urcorner} * v)$	3 T13.48o,p
6.	$\mathbb{W}f\!f(formsub(p, v, \overline{\ulcorner \emptyset \urcorner}))$	3,5 T13.51m
7.	$\mathbb{W}f\!f(formsub(p, v, \overline{\ulcorner S \urcorner} * v))$	3,5 T13.51m
8.	$\mathbb{W}f\!f(\mathbb{c}nd(p, formsub(p, v, \overline{\ulcorner S \urcorner} * v)))$	3,7 T13.49o
9.	$\mathbb{W}f\!f(\mathbb{u}nv(v, \mathbb{c}nd(p, formsub(p, v, \overline{\ulcorner S \urcorner} * v))))$	3,8 T13.49p
10.	$\mathbb{W}f\!f(\mathbb{n}eg(\mathbb{u}nv(v, \mathbb{c}nd(p, formsub(p, v, \overline{\ulcorner S \urcorner} * v)))))$	9 T13.49c
11.	$\mathbb{W}f\!f(\mathbb{c}nd(formsub(p, v, \overline{\ulcorner \emptyset \urcorner}), \mathbb{n}eg(\mathbb{u}nv(v, \mathbb{c}nd(p, formsub(p, v, \overline{\ulcorner S \urcorner} * v))))))$	6,10 T13.49o
12.	$\mathbb{W}f\!f(\mathbb{n}eg(\mathbb{c}nd(formsub(p, v, \overline{\ulcorner \emptyset \urcorner}), \mathbb{n}eg(\mathbb{u}nv(v, \mathbb{c}nd(p, formsub(p, v, \overline{\ulcorner S \urcorner} * v)))))))$	11 T13.49c
13.	$\mathbb{W}f\!f(\mathbb{u}nv(v, p))$	3 T13.49p
14.	$\mathbb{W}f\!f(\mathbb{c}nd(\mathbb{n}eg(\mathbb{c}nd(formsub(p, v, \overline{\ulcorner \emptyset \urcorner}), \mathbb{n}eg(\mathbb{u}nv(v, \mathbb{c}nd(p, formsub(p, v, \overline{\ulcorner S \urcorner} * v)))))), \mathbb{u}nv(v, p)))$	12,13 T13.49o
15.	$\mathbb{W}f\!f(n)$	4,14 =E
16.	$\mathbb{W}f\!f(n)$	2,3-15 (∃E)
17.	$\mathbb{A}xiompa7(n) \rightarrow \mathbb{W}f\!f(n)$	1-16 →I

E13.41. As a start to a complete demonstration of T13.54, provide a demonstration through part (C) that does not skip any steps.

T13.54. PA $\vdash Prvt(\mathbb{c}nd(p, q)) \rightarrow (Prvt(p) \rightarrow Prvt(q))$.

(a)

1.	$\mathbb{P}rvt(\mathbb{c}nd(p,q))$	A (g $\rightarrow$I)
2.	$\mathbb{W}\!f\!f(\mathbb{c}nd(p,q))$	1 T13.53k
3.	$\mathbb{P}rvt(p)$	A (g $\rightarrow$I)
4.	$\mathbb{W}\!f\!f(p)$	3 T13.53k
5.	$\mathbb{W}\!f\!f(q)$	2,4 T13.53i
6.	$\mathbb{M}p(\mathbb{c}nd(p,q),p,q)$	T13.40c
7.	$\mathbb{M}p(\mathbb{c}nd(p,q),p,q) \vee (\mathbb{c}nd(p,q) = p \wedge \mathbb{G}en(p,q))$	6 $\vee$I
8.	$\mathbb{I}con(\mathbb{c}nd(p,q),p,q)$	7 T13.40e
9.	$\exists v\, \mathbb{P}rft(v,\mathbb{c}nd(p,q))$	1 abv
10.	$\exists v\, \mathbb{P}rft(v,p)$	3 abv
11.	$\mathbb{P}rft(j,\mathbb{c}nd(p,q))$	A (g 9$\exists$E)
12.	$\mathbb{P}rft(k,p)$	A (g 10$\exists$E)
13.	$l =_{\text{def}} j * k * \bar{2}^q$	def
14.	$\mathbb{e}xp(j,\mathbb{l}en(j) \dot{-} \bar{1}) = \mathbb{c}nd(p,q)$	11 T13.40f
15.	$\mathbb{e}xp(k,\mathbb{l}en(k) \dot{-} \bar{1}) = p$	12 T13.40f
16.	$\mathbb{l}en(j * k) = \mathbb{l}en(j) + \mathbb{l}en(k)$	T13.47f
17.	$q > \emptyset$	5 T13.49e
18.	$\mathbb{l}en(\bar{2}^q) = \bar{1}$	17 T13.45k
19.	$(\forall i < \bar{1})[\mathbb{e}xp(l,i + \mathbb{l}en(j * k)) = \mathbb{e}xp(\bar{2}^q,i)$	13,18 T13.47c
20.	$\emptyset < \bar{1}$	T13.13e
21.	$\mathbb{e}xp(l,\mathbb{l}en(j * k)) = \mathbb{e}xp(\bar{2}^q,\emptyset)$	19,20 ($\forall$E)
22.	$\mathbb{e}xp(\bar{2}^q,\emptyset) = q$	T13.44i
23.	$\mathbb{e}xp(l,\mathbb{l}en(j * k)) = q$	21,22 =E
24.	$\mathbb{e}xp(l,\mathbb{l}en(j) + \mathbb{l}en(k)) = q$	23,16 =E
25.	$\mathbb{I}con[\mathbb{e}xp(j,\mathbb{l}en(j) \dot{-} 1),\mathbb{e}xp(k,\mathbb{l}en(k) \dot{-} 1),\mathbb{e}xp(l,\mathbb{l}en(j) + \mathbb{l}en(k))]$	8,14,15,24 =E

(b)

26.	$(\forall i < \mathbb{l}en(j))\mathbb{e}xp(l,i) = \mathbb{e}xp(j,i)$	13 T13.47c
27.	$(\forall i < \mathbb{l}en(j * k))\mathbb{e}xp(l,i) = \mathbb{e}xp(j * k,i)$	13 T13.47c
28.	$(\forall i < \mathbb{l}en(k))\mathbb{e}xp(j * k,i + \mathbb{l}en(j)) = \mathbb{e}xp(k,i)$	T13.47c
29.	$a < \mathbb{l}en(k)$	A (g ($\forall$I))
30.	$\mathbb{e}xp(j * k,a + \mathbb{l}en(j)) = \mathbb{e}xp(k,a)$	28,29 ($\forall$E)
31.	$\mathbb{l}en(j) + a < \mathbb{l}en(j) + \mathbb{l}en(k)$	29 T13.13w
32.	$\mathbb{l}en(j) + a < \mathbb{l}en(j * k)$	31,16 =E
33.	$\mathbb{e}xp(l,\mathbb{l}en(j) + a) = \mathbb{e}xp(j * k,\mathbb{l}en(j) + a)$	27,32 ($\forall$E)
34.	$\mathbb{e}xp(l,\mathbb{l}en(j) + a) = \mathbb{e}xp(k,a)$	33,30 =E
35.	$(\forall i < \mathbb{l}en(k))\mathbb{e}xp(l,\mathbb{l}en(j) + i) = \mathbb{e}xp(k,i)$	29-34 ($\forall$I)
36.	$\mathbb{c}nd(p,q) > \emptyset$	2 T13.49e
37.	$\mathbb{e}xp(j,\mathbb{l}en(j) \dot{-} \bar{1}) > \emptyset$	14,36 =E
38.	$\mathbb{l}en(j) \dot{-} \bar{1} < \mathbb{l}en(j)$	37 T13.45h
39.	$\mathbb{e}xp(l,\mathbb{l}en(j) \dot{-} \bar{1}) = \mathbb{e}xp(j,\mathbb{l}en(j) \dot{-} \bar{1})$	26,38 ($\forall$E)
40.	$p > \emptyset$	4 T13.49e
41.	$\mathbb{e}xp(k,\mathbb{l}en(k) \dot{-} \bar{1}) > \emptyset$	40,15 =E
42.	$\mathbb{l}en(k) \dot{-} \bar{1} < \mathbb{l}en(k)$	41 T13.45h
43.	$\mathbb{e}xp(l,\mathbb{l}en(j) + \mathbb{l}en(k) \dot{-} \bar{1}) = \mathbb{e}xp(k,\mathbb{l}en(k) \dot{-} \bar{1})$	35,42 ($\forall$E)
44.	$\mathbb{I}con[\mathbb{e}xp(l,\mathbb{l}en(j) \dot{-} \bar{1}),\mathbb{e}xp(l,\mathbb{l}en(j) + \mathbb{l}en(k) \dot{-} \bar{1}),\mathbb{e}xp(l,\mathbb{l}en(j) + \mathbb{l}en(k))]$	25,39,43 =E

Exercise 13.41 T13.54

(c1)

45.	$(\forall i < \mathbb{l}en(j))[\mathbb{A}xiomt(\mathbb{e}xp(j,i)) \vee (\exists m < i)(\exists n < i)\mathbb{I}con(\mathbb{e}xp(j,m),\mathbb{e}xp(j,n),\mathbb{e}xp(j,i))]$	T13.40f
46.	$a < \mathbb{l}en(j)$	A (g ($\forall$I))
47.	$\mathbb{A}xiomt(\mathbb{e}xp(j,a)) \vee (\exists m < a)(\exists n < a)\mathbb{I}con(\mathbb{e}xp(j,m),\mathbb{e}xp(j,n),\mathbb{e}xp(j,a))$	45,46 ($\forall$E)
48.	$\mathbb{e}xp(l,a) = \mathbb{e}xp(j,a)$	26,46 ($\forall$E)
49.	$\mathbb{A}xiomt(\mathbb{e}xp(j,a))$	A (g 47$\vee$E)
50.	$\mathbb{A}xiomt(\mathbb{e}xp(l,a))$	49,48 =E
51.	$\mathbb{A}xiomt(\mathbb{e}xp(l,a)) \vee (\exists m < a)(\exists n < a)\mathbb{I}con(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,a))$	50 $\vee$I
52.	$(\exists m < a)(\exists n < a)\mathbb{I}con(\mathbb{e}xp(j,m),\mathbb{e}xp(j,n),\mathbb{e}xp(j,a))$	A (g 47$\vee$E)
53.	$\mathbb{I}con(\mathbb{e}xp(j,m'),\mathbb{e}xp(j,n'),\mathbb{e}xp(j,a))$	A (g 52$\exists$E)
54.	$m' < a$	
55.	$n' < a$	
56.	$m' < \mathbb{l}en(j)$	46,54 T13.13b
57.	$n' < \mathbb{l}en(j)$	46,55 T13.13b
58.	$\mathbb{e}xp(l,m') = \mathbb{e}xp(j,m')$	26,56 ($\forall$E)
59.	$\mathbb{e}xp(l,n') = \mathbb{e}xp(j,n')$	26,57 ($\forall$E)
60.	$\mathbb{I}con(\mathbb{e}xp(l,m'),\mathbb{e}xp(l,n'),\mathbb{e}xp(l,a))$	53,58,59,48 =E
61.	$(\exists m < a)(\exists n < a)\mathbb{I}con(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,a))$	60,54,55 ($\exists$I)
62.	$(\exists m < a)(\exists n < a)\mathbb{I}con(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,a))$	52,53-61 ($\exists$E)
63.	$\mathbb{A}xiomt(\mathbb{e}xp(l,a)) \vee (\exists m < a)(\exists n < a)\mathbb{I}con(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,a))$	62 $\vee$I
64.	$\mathbb{A}xiomt(\mathbb{e}xp(l,a)) \vee (\exists m < a)(\exists n < a)\mathbb{I}con(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,a))$	47,49-51,52-63 $\vee$E
65.	$(\forall i < \mathbb{l}en(j))[\mathbb{A}xiom(\mathbb{e}xp(l,i)) \vee (\exists m < i)(\exists n < i)Icon(\mathbb{e}xp(l,m),\mathbb{e}xp(l,n),\mathbb{e}xp(l,i))]$	46-64 ($\forall$I)

(c2) The argument is similar for,

$(\forall i < \mathbb{l}en(k))[\mathbb{A}xiom(\mathbb{e}xp(l,\mathbb{l}en(j)+i)) \vee (\exists m<i)(\exists n<i)\mathbb{I}con(\mathbb{e}xp(l,\mathbb{l}en(j)+m),\mathbb{e}xp(l,\mathbb{l}en(j)+n),\mathbb{e}xp(l,\mathbb{l}en(j)+i))]$

(c3) Here is a schematic argument (or theorem) you can apply.

1.	$(\forall i < \mathscr{s})[\mathscr{P}(\mathscr{t}+i) \vee (\exists m < i)(\exists n < i)\mathscr{Q}(\mathscr{t}+m, \mathscr{t}+n, \mathscr{t}+i)]$	prem
2.	$\mathscr{t} \leq a \wedge a < \mathscr{t}+\mathscr{s}$	A ($g \to$I)
3.	$\mathscr{t} \leq a$	2 $\wedge$E
4.	$a < \mathscr{t}+\mathscr{s}$	2 $\wedge$E
5.	$\exists v(v+\mathscr{t} = a)$	3 def
6.	$l + \mathscr{t} = a$	A (g 5$\exists$E)
7.	$\mathscr{t} + l < \mathscr{t}+\mathscr{s}$	4,6 =E
8.	$l < \mathscr{s}$	7 T13.13w
9.	$\mathscr{P}(\mathscr{t}+l) \vee (\exists m < l)(\exists n < l)\mathscr{Q}(\mathscr{t}+m, \mathscr{t}+n, \mathscr{t}+l)$	1,8 ($\forall$E)
10.	$\mathscr{P}(\mathscr{t}+l)$	A (g 9$\vee$E)
11.	$\mathscr{P}(a)$	10,6 =E
12.	$\mathscr{P}(a) \vee (\exists m < a)(\exists n < a)\mathscr{Q}(m, n, a)$	11 $\vee$I
13.	$(\exists m < l)(\exists n < l)\mathscr{Q}(\mathscr{t}+m, \mathscr{t}+n, \mathscr{t}+l)$	A (g 9$\vee$E)
14.	$\mathscr{Q}(\mathscr{t}+m', \mathscr{t}+n', \mathscr{t}+l)$	A (g 13($\exists$E))
15.	$m' < l$	
16.	$n' < l$	
17.	$\mathscr{t}+m' < \mathscr{t}+l$	15 T13.13w
18.	$\mathscr{t}+m' < a$	17,6 =E
19.	$\mathscr{t}+n' < \mathscr{t}+l$	16 T13.13w
20.	$\mathscr{t}+n' < a$	19,6 =E
21.	$(\exists m < a)(\exists n < a)\mathscr{Q}(m, n, \mathscr{t}+l)$	14,18,20 ($\exists$I)
22.	$(\exists m < a)(\exists n < a)\mathscr{Q}(m, n, a)$	21,6 =E
23.	$(\exists m < a)(\exists n < a)\mathscr{Q}(m, n, a)$	13,14-22 ($\exists$E)
24.	$\mathscr{P}(a) \vee (\exists m < a)(\exists n < a)\mathscr{Q}(m, n, a)$	23 $\vee$I
25.	$\mathscr{P}(a) \vee (\exists m < a)(\exists n < a)\mathscr{Q}(m, n, a)$	9,10-12,13-24 $\vee$E
26.	$\mathscr{P}(a) \vee (\exists m < a)(\exists n < a)\mathscr{Q}(m, n, a)$	5,6-25 $\exists$E
27.	$(\mathscr{t} \leq a \wedge a < \mathscr{t}+\mathscr{s}) \to [\mathscr{P}(a) \vee (\exists m < a)(\exists n < a)\mathscr{Q}(m, n, a)]$	2-26 $\to$I
28.	$\forall i[(\mathscr{t} \leq i \wedge i < \mathscr{t}+\mathscr{s}) \to [\mathscr{P}(i) \vee (\exists m < i)(\exists n < i)\mathscr{Q}(m, n, i)]]$	27$\forall$I
29.	$(\forall i : \mathscr{t} \leq i < \mathscr{t}+\mathscr{s})[\mathscr{P}(i) \vee (\exists m < i)(\exists n < i)\mathscr{Q}(m, n, i)]$	28 abv

E13.42. Show

T13.55.

T13.55.i. PA $\vdash [\mathbb{T}ermsub(t, v, s, q) \wedge \mathbb{T}ermsub(t, v, s, r)] \to q = r$

1.	$\mathbb{T}ermsub(t,v,s,q) \wedge \mathbb{T}ermsub(t,v,s,r)$	A (g →I)
2.	$(\exists x \leq X)(\exists y \leq Y)\mathbb{T}subseq(x,y,t,v,s,q) \wedge (\exists x \leq X)(\exists y \leq Y)\mathbb{T}subseq(x,y,t,v,s,r)$	1 T13.50b
3.	$\mathbb{T}subseq(m,n,t,v,s,q) \wedge \mathbb{T}subseq(m',n',t,v,s,r)$	A (g 2 (∃E))
4.	$\mathbb{T}ermseq(m,t) \wedge \mathbb{T}ermseq(m',t)$	3 T13.50a
5.	$\mathbb{l}en(m) = \mathbb{l}en(n) \wedge \mathbb{l}en(m') = \mathbb{l}en(n')$	3 T13.50a
6.	$\mathbb{e}xp(n,\mathbb{l}en(n) \dot{-} \overline{1}) = q \wedge \mathbb{e}xp(n',\mathbb{l}en(n') \dot{-} \overline{1}) = r$	3 T13.50a
7.	$\mathbb{e}xp(m,\mathbb{l}en(m) \dot{-} \overline{1}) = t \wedge \mathbb{e}xp(m',\mathbb{l}en(m') \dot{-} \overline{1}) = t$	4 T13.48a
8.	$m > \overline{1} \wedge m' > \overline{1}$	4 T13.48a
9.	$\mathbb{l}en(m) > \emptyset \wedge \mathbb{l}en(m') > \emptyset$	8 T13.45j
10.	$\mathbb{l}en(m) \dot{-} \overline{1} < \mathbb{l}en(m) \wedge \mathbb{l}en(m') \dot{-} \overline{1} < \mathbb{l}en(m')$	9 T13.23i
11.	$\emptyset < \mathbb{l}en(m)$	A (g →I)
12.	$a < \mathbb{l}en(m')$	A (g (∀I))
13.	$\mathbb{e}xp(m,\emptyset) = \mathbb{e}xp(m',a)$	A (g →I)
14.	$I(m,n,\emptyset) \vee J(v,m,n,\emptyset) \vee K(v,s,m,n,\emptyset) \vee L(m,n,\emptyset) \vee M(m,n,\emptyset) \vee N(m,n,\emptyset)$	3,11 T13.50a
15.	$I(m',n',a) \vee J(v,m',n',a) \vee K(v,s,m',n',a) \vee L(m',n',a) \vee M(m',n',a) \vee N(m',n',a)$	3,12, T13.50a
16.	$I(m,n,\emptyset)$	A (g 14∨E)
17.	$\mathbb{e}xp(m,\emptyset) = \overline{\ulcorner \emptyset \urcorner} \wedge \mathbb{e}xp(n,\emptyset) = \overline{\ulcorner \emptyset \urcorner}$	16 abv
18.	$I(m',n',a)$	A (g 15∨E)
19.	$\mathbb{e}xp(n',a) = \overline{\ulcorner \emptyset \urcorner}$	18 abv
20.	$\mathbb{e}xp(n,\emptyset) = \mathbb{e}xp(n',a)$	17,19 =E
21.	$J(v,m',n',a) \vee K(v,s,m',n',a) \vee L(m',n',a) \vee M(m',n',a) \vee N(m',n',a)$	A (g 15∨E)
22.	$\mathbb{e}xp(n,\emptyset) \neq \mathbb{e}xp(n',a)$	A (c ∼E)
23.	$\mathbb{e}xp(m',a) = \overline{\ulcorner \emptyset \urcorner}$	13,17 =E
24.	$\sim[J(v,m',n',a) \vee K(v,s,m',n',a) \vee L(m',n',a) \vee M(m',n',a) \vee N(m',n',a)]$	23 T13.55c
25.	$\bot$	21,24 ⊥I
26.	$\mathbb{e}xp(n,\emptyset) = \mathbb{e}xp(n',a)$	22-25 ∼E
27.	$\mathbb{e}xp(n,\emptyset) = \mathbb{e}xp(n',a)$	15,18-26 ∨E
28.	$J(v,m,n,\emptyset) \vee K(v,s,m,n,\emptyset)$	A (g 14∨E)
29.	$\mathbb{e}xp(n,\emptyset) = \mathbb{e}xp(n',a)$	similarly
30.	$L(m,n,\emptyset)$	A (g 14∨E)
31.	$(\exists i < \emptyset)[\mathbb{e}xp(m,\emptyset) = \overline{\ulcorner S \urcorner} * \mathbb{e}xp(m,i) \wedge \mathbb{e}xp(n,\emptyset) = \mathbb{e}xp(n,i)$	30 abv
32.	$i < \emptyset$	A (g 31 (∃E))
33.	$\mathbb{e}xp(n,\emptyset) \neq \mathbb{e}xp(n',a)$	A (c ∼E)
34.	$i \nless \emptyset$	T13.13d,r
35.	$\bot$	32,34 ⊥I
36.	$\mathbb{e}xp(n,\emptyset) = \mathbb{e}xp(n',a)$	33-35 ∼E
37.	$\mathbb{e}xp(n,\emptyset) = \mathbb{e}xp(n',a)$	31,32-36 (∃E)
38.	$M(m,n,\emptyset) \vee N(m,n,\emptyset)$	A (g 14∨E)
39.	$\mathbb{e}xp(n,\emptyset) = \mathbb{e}xp(n',a)$	similarly
40.	$\mathbb{e}xp(n,\emptyset) = \mathbb{e}xp(n',a)$	14,16-39 ∨E
41.	$\mathbb{e}xp(m,\emptyset) = \mathbb{e}xp(m',a) \rightarrow \mathbb{e}xp(n,\emptyset) = \mathbb{e}xp(n',a)$	13-40 →I
42.	$(\forall x < \mathbb{l}en(m'))(\mathbb{e}xp(m,\emptyset) = \mathbb{e}xp(m',x) \rightarrow \mathbb{e}xp(n,\emptyset) = \mathbb{e}xp(n',x))$	12-41 (∀I)
43.	$\emptyset < \mathbb{l}en(m) \rightarrow (\forall x < \mathbb{l}en(m'))(\mathbb{e}xp(m,\emptyset) = \mathbb{e}xp(m',x) \rightarrow \mathbb{e}xp(n,\emptyset) = \mathbb{e}xp(n',x))$	11-42 →I

44.	$(\forall z \leq k)[z < \mathit{len}(m) \to (\forall x < \mathit{len}(m'))(\mathit{exp}(m,z) = \mathit{exp}(m',x) \to \mathit{exp}(n,z) = \mathit{exp}(n',x))]$	A (g →I)
45.	$Sk < \mathit{len}(m)$	A (g →I)
46.	$a < \mathit{len}(m')$	A (g (∀I))
47.	$\mathit{exp}(m,Sk) = \mathit{exp}(m',a)$	A (g →I)
48.	$I(m,n,Sk) \vee J(v,m,n,Sk) \vee K(v,s,m,n,Sk) \vee L(m,n,Sk) \vee M(m,n,Sk) \vee N(m,n,Sk)$	3,45 T13.50a
49.	$I(m',n',a) \vee J(v,m',n',a) \vee K(v,s,m',n',a) \vee L(m',n',a) \vee M(m',n',a) \vee N(m',n',a)$	3,46 T13.50a
50.	$I(m,n,Sk) \vee J(v,m,n,Sk) \vee K(v,s,m,n,Sk)$	A (g 48∨E)
51.	$\mathit{exp}(n,Sk) = \mathit{exp}(n',a)$	as from basis
52.	$L(m,n,Sk)$	A (g 48∨E)
53.	$(\exists i < Sk)[\mathit{exp}(m,Sk) = \overline{\ulcorner S \urcorner} * \mathit{exp}(m,i) \wedge \mathit{exp}(n,Sk) = \overline{\ulcorner S \urcorner} * \mathit{exp}(n,i)]$	52 abv
54.	$b < Sk$	A (g 53 (∃E))
55.	$\mathit{exp}(m,Sk) = \overline{\ulcorner S \urcorner} * \mathit{exp}(m,b) \wedge \mathit{exp}(n,Sk) = \overline{\ulcorner S \urcorner} * \mathit{exp}(n,b)$	
56.	$L(m',n',a)$	A (g 49∨E)
57.	$(\exists i < a)[\mathit{exp}(m',a) = \overline{\ulcorner S \urcorner} * \mathit{exp}(m',i) \wedge \mathit{exp}(n',a) = \overline{\ulcorner S \urcorner} * \mathit{exp}(n',i)]$	56 abv
58.	$c < a$	A (g 57 (∃E))
59.	$\mathit{exp}(m',a) = \overline{\ulcorner S \urcorner} * \mathit{exp}(m',c) \wedge \mathit{exp}(n',a) = \overline{\ulcorner S \urcorner} * \mathit{exp}(n',c)$	
60.	$\overline{\ulcorner S \urcorner} * \mathit{exp}(m,b) = \overline{\ulcorner S \urcorner} * \mathit{exp}(m',c)$	47,55,59 =E
61.	$b < \mathit{len}(m) \wedge c < \mathit{len}(m')$	45,46,54,58 T13.13b
62.	$\mathit{Term}(\mathit{exp}(m,b)) \wedge \mathit{Term}(\mathit{exp}(m',c))$	4,61 T13.48n
63.	$\mathit{exp}(m,b) = \mathit{exp}(m',c)$	60,62 T13.52b
64.	$b \leq k$	54 T13.13n,m
65.	$\mathit{exp}(m,b) = \mathit{exp}(m',c) \to \mathit{exp}(n,b) = \mathit{exp}(n',c)$	44,64,61 (∀E)
66.	$\mathit{exp}(n,b) = \mathit{exp}(n',c)$	65,63 →E
67.	$\overline{\ulcorner S \urcorner} * \mathit{exp}(n,b) = \overline{\ulcorner S \urcorner} * \mathit{exp}(n',c)$	66 =E
68.	$\mathit{exp}(n,Sk) = \mathit{exp}(n',a)$	67,55,59 =E
69.	$\mathit{exp}(n,Sk) = \mathit{exp}(n',a)$	57,58-68 (∃E)
70.	$I(m',n',a) \vee J(v,m',n',a) \vee K(v,s,m',n',a) \vee M(m',n',a) \vee N(m',n',a)$	A (g 49∨E)
71.	$\mathit{exp}(n,Sk) = \mathit{exp}(n',a)$	as before
72.	$\mathit{exp}(n,Sk) = \mathit{exp}(n',a)$	49,56-71 ∨E
73.	$\mathit{exp}(n,Sk) = \mathit{exp}(n',a)$	53,54-72 (∃E)
74.	$M(m,n,Sk) \vee N(m,n,Sk)$	A (g 48∨E)
75.	$\mathit{exp}(n,Sk) = \mathit{exp}(n',a)$	similarly
76.	$\mathit{exp}(n,Sk) = \mathit{exp}(n',a)$	48,50-75 ∨E
77.	$\mathit{exp}(m,Sk) = \mathit{exp}(m',a) \to \mathit{exp}(n,Sk) = \mathit{exp}(n',a)$	47-76 →I
78.	$(\forall x < \mathit{len}(m'))(\mathit{exp}(m,Sk) = \mathit{exp}(m',x) \to \mathit{exp}(n,Sk) = \mathit{exp}(n',x))$	46-77 (∀I)
79.	$Sk < \mathit{len}(m) \to (\forall x < \mathit{len}(m'))(\mathit{exp}(m,Sk) = \mathit{exp}(m',x) \to \mathit{exp}(n,Sk) = \mathit{exp}(n',x))$	45-78 →I
80.	$(\forall z \leq k)[z < \mathit{len}(m) \to (\forall x < \mathit{len}(m'))(\mathit{exp}(m,z) = \mathit{exp}(m',x) \to \mathit{exp}(n,z) = \mathit{exp}(n',x))] \to$ $[Sk < \mathit{len}(m) \to (\forall x < \mathit{len}(m'))(\mathit{exp}(m,Sk) = \mathit{exp}(m',x) \to \mathit{exp}(n,Sk) = \mathit{exp}(n',x))]$	44-79 →I
81.	$\forall k[k < \mathit{len}(m) \to (\forall x < \mathit{len}(m'))(\mathit{exp}(m,k) = \mathit{exp}(m',x) \to \mathit{exp}(n,k) = \mathit{exp}(n',x))]$	43,80 T13.13ag
82.	$\mathit{exp}(m,\mathit{len}(m) \dot{-} \overline{1}) = \mathit{exp}(m',\mathit{len}(m') \dot{-} \overline{1}) \to \mathit{exp}(n,\mathit{len}(n) \dot{-} \overline{1}) = \mathit{exp}(n',\mathit{len}(n') \dot{-} \overline{1})$	81,5,10 (∀E)
83.	$\mathit{exp}(m,\mathit{len}(m) \dot{-} 1) = \mathit{exp}(m',\mathit{len}(m') \dot{-} 1)$	7 =E
84.	$\mathit{exp}(n,\mathit{len}(n) \dot{-} \overline{1}) = \mathit{exp}(n',\mathit{len}(n') \dot{-} \overline{1})$	82,83 →E
85.	$q = r$	6,84 =E
86.	$q = r$	2,3-85 (∃E)
87.	$[\mathit{Termsub}(t,v,s,q) \wedge \mathit{Termsub}(t,v,s,r)] \to q = r$	3-85 →I

T13.55.n. PA $\vdash \mathit{Var}(v) \to [(\sim\mathit{Atomsub}(p,v,v \times \overline{4},p) \wedge \mathit{Atomsub}(p,v,s,q)) \to s \leq q]$

Exercise 13.42 T13.55.n

1.	$\mathbb{V}ar(v)$	A (g →I)
2.	$\sim\mathbb{A}tomsub(p, v, v \times \overline{4}, p) \wedge \mathbb{A}tomsub(p, v, s, q)$	A (g →I)
3.	$w = v \times \overline{4}$	def
4.	$\mathbb{T}erm(w) \wedge w \neq v$	1,3 T13.55b
5.	$(\exists a \leq p)(\exists b \leq p)(\exists a' \leq q)(\exists b' \leq q)[\mathbb{T}erm(a) \wedge \mathbb{T}erm(b) \wedge p = \overline{\ulcorner = \urcorner} * a * b \wedge$ $\mathbb{T}ermsub(a, v, s, a') \wedge \mathbb{T}ermsub(b, v, s, b') \wedge q = \overline{\ulcorner = \urcorner} * a' * b']$	2 T13.50c
6.	$\mathbb{T}erm(c) \wedge \mathbb{T}erm(d) \wedge p = \overline{\ulcorner = \urcorner} * c * d$	A (g 5 (∃E)
7.	$\mathbb{T}ermsub(c, v, s, c') \wedge \mathbb{T}ermsub(d, v, s, d') \wedge q = \overline{\ulcorner = \urcorner} * c' * d'$	
8.	$\mathbb{A}tomic(p)$	6 T13.49c
9.	$\exists q\, \mathbb{A}tomsub(p, v, w, q)$	4,8 T13.50n
10.	$\mathbb{A}tomsub(p, v, w, r)$	A (g 9∃E)
11.	$r \neq p$	2,10 ∼I
12.	$(\exists a \leq p)(\exists b \leq p)(\exists a' \leq r)(\exists b' \leq r)[\mathbb{T}erm(a) \wedge \mathbb{T}erm(b) \wedge p = \overline{\ulcorner = \urcorner} * a * b \wedge$ $\mathbb{T}ermsub(a, v, w, a') \wedge \mathbb{T}ermsub(b, v, w, b') \wedge r = \overline{\ulcorner = \urcorner} * a' * b']$	10 T13.50c
13.	$\mathbb{T}erm(e) \wedge \mathbb{T}erm(f) \wedge p = \overline{\ulcorner = \urcorner} * e * f$	A (g 12 (∃E)
14.	$\mathbb{T}ermsub(e, v, w, e') \wedge \mathbb{T}ermsub(f, v, w, f') \wedge r = \overline{\ulcorner = \urcorner} * e' * f'$	
15.	$\overline{\ulcorner = \urcorner} * c * d = \overline{\ulcorner = \urcorner} * e * f$	6,13 =E
16.	$c = e \wedge d = f$	6,13,15 T13.52i
17.	$\overline{\ulcorner = \urcorner} * e * f \neq \overline{\ulcorner = \urcorner} * e' * f'$	11,13,14 =E
18.	$e \neq e' \vee f \neq f'$	17 ∼I
19.	$\sim\mathbb{T}ermsub(e, v, w, e) \vee \sim\mathbb{T}ermsub(f, v, w, f)$	14,18 T13.55i
20.	$\mathbb{F}ree_t(e, v) \vee \mathbb{F}ree_t(f, v)$	19 T13.55a
21.	$\mathbb{F}ree_t(e, v)$	A (g 20∨E)
22.	$\mathbb{T}ermsub(e, v, s, c')$	7,16 =E
23.	$s \leq c'$	13,1,21,22 T13.55m
24.	$c' \leq \overline{\ulcorner = \urcorner} * c' * d'$	T13.47n,o
25.	$s \leq q$	23,24,7 T13.13a
26.	$\mathbb{F}ree_t(f, v)$	A (g 20∨E)
27.	$s \leq q$	similarly
28.	$s \leq q$	20,21-27 ∨E
29.	$s \leq q$	12,13-28 (∃E)
30.	$s \leq q$	9,10-29 ∃E
31.	$s \leq q$	5,6-30 (∃E)
32.	$(\sim\mathbb{A}tomsub(p, v, v \times \overline{4}, p) \wedge \mathbb{A}tomsub(p, v, s, q)) \rightarrow s \leq q$	2-31 →I
33.	$\mathbb{V}ar(v) \rightarrow [(\sim\mathbb{A}tomsub(p, v, v \times \overline{4}, p) \wedge \mathbb{A}tomsub(p, v, s, q)) \rightarrow s \leq q]$	1-32 →I

E13.44. Show (s) and (u) from T13.57. Hard core: show the rest of the results from T13.57.

T13.57.

T13.57.h. PA ⊢ $[\mathbb{P}rvt(p) \wedge \mathbb{V}ar(v)] \rightarrow \mathbb{P}rvt(\mathbb{unv}(v, p))$

Exercise 13.44 T13.57h

1.	$\mathbb{P}rvt(p) \wedge \mathbb{V}ar(v)$	A (g →I)
2.	$\mathbb{P}rvt(p)$	1 ∧E
3.	$\exists v\, \mathbb{P}rft(v, p)$	2 abv
4.	$\mathbb{P}rft(m, p)$	A (g 3∃E)
5.	$\mathbb{e}xp(m, \mathbb{l}en(m) \dot{-} \overline{1}) = p$	4 T13.40f
6.	$m > \overline{1}$	4 T13.40f
7.	$(\forall k < \mathbb{l}en(m))[\mathbb{A}xiomt(\mathbb{e}xp(m, k)) \vee (\exists i < k)(\exists j < k)\mathbb{I}con(\mathbb{e}xp(m, i), \mathbb{e}xp(m, j), \mathbb{e}xp(m, k))]$	4 T13.40f
8.	$\mathbb{l}en(\overline{\ulcorner\forall\urcorner}) = \overline{1}$	cap
9.	$\mathbb{l}en(\mathbb{u}nv(v, p)) = \mathbb{l}en(\overline{\ulcorner\forall\urcorner}) + \mathbb{l}en(v) + \mathbb{l}en(p)$	T13.47f def
10.	$\mathbb{l}en(\mathbb{u}nv(v, p)) \geq \overline{1}$	8,9 T13.13u
11.	$\mathbb{u}nv(v, p) > \overline{1}$	10 T13.45g
12.	$\mathbb{l}en(\overline{2}^{\mathbb{u}nv(v,p)}) = \overline{1}$	11 T13.45k
13.	$\mathbb{l}en(m * \overline{2}^{\mathbb{u}nv(v,p)}) = \mathbb{l}en(m) + \overline{1}$	12 T13.47f
14.	$\mathbb{l}en(m * \overline{2}^{\mathbb{u}nv(v,p)}) \dot{-} \overline{1} = \mathbb{l}en(m)$	13 T13.23k
15.	$\mathbb{e}xp(m * \overline{2}^{\mathbb{u}nv(v,p)}, \mathbb{l}en(m)) = \mathbb{e}xp(\overline{2}^{\mathbb{u}nv(v,p)}, \emptyset)$	14 T13.47g
16.	$\mathbb{e}xp(\overline{2}^{\mathbb{u}nv(v,p)}, \emptyset) = \mathbb{u}nv(v, p)$	T13.44i
17.	$\mathbb{e}xp(m * \overline{2}^{\mathbb{u}nv(v,p)}, \mathbb{l}en(m)) = \mathbb{u}nv(v, p)$	15,16 =E
18.	$\mathbb{e}xp(m * \overline{2}^{\mathbb{u}nv(v,p)}, \mathbb{l}en(m * \overline{2}^{\mathbb{u}nv(v,p)}) \dot{-} \overline{1}) = \mathbb{u}nv(v, p)$	17,14 =E
19.	$\mathbb{l}en(m * \overline{2}^{\mathbb{u}nv(v,p)}) \geq \overline{1}$	13 T13.13u
20.	$m * \overline{2}^{\mathbb{u}nv(v,p)} > \overline{1}$	19 T13.45g
21.	$\mathbb{u}nv(v, p) = u$	abv
22.	$a < \mathbb{l}en(m) * \overline{2}^{u}$	A (g (∀I))
23.	$a < \mathbb{l}en(m) \vee a = \mathbb{l}en(m)$	13 T13.13n
24.	$a < \mathbb{l}en(m)$	A (g 23∨E)
25.	$\mathbb{e}xp(m * \overline{2}^{u}, a) = \mathbb{e}xp(m, a)$	24 T13.47c
26.	$\mathbb{A}xiomt(\mathbb{e}xp(m, a)) \vee (\exists i < a)(\exists j < a)\mathbb{I}con(\mathbb{e}xp(m, i), \mathbb{e}xp(m, j), \mathbb{e}xp(m, a))$	7,24 (∀E)
27.	$\mathbb{A}xiomt(\mathbb{e}xp(m, a))$	A (g 26∨E)
28.	$\mathbb{A}xiomt(\mathbb{e}xp(m * \overline{2}^{u}, a))$	27,25 =E
29.	$\mathbb{A}xiomt(\mathbb{e}xp(m * \overline{2}^{u}, a)) \vee (\exists i < a)(\exists j < a)\mathbb{I}con(\mathbb{e}xp(m * \overline{2}^{u}, i), \mathbb{e}xp(m * \overline{2}^{u}, j), \mathbb{e}xp(m * \overline{2}^{u}, a))$	28 ∨I
30.	$(\exists i < a)(\exists j < a)\mathbb{I}con(\mathbb{e}xp(m, i), \mathbb{e}xp(m, j), \mathbb{e}xp(m, a))$	A (g 26∨E)
31.	$r < a \wedge s < a$	A (g 30 (∃E))
32.	$\mathbb{I}con(\mathbb{e}xp(m, r), \mathbb{e}xp(m, s), \mathbb{e}xp(m, a))$	
33.	$r < \mathbb{l}en(m) \wedge s < \mathbb{l}en(m)$	24,31 T13.13b
34.	$\mathbb{e}xp(m * \overline{2}^{u}, r) = \mathbb{e}xp(m, r) \wedge \mathbb{e}xp(m * \overline{2}^{u}, s) = \mathbb{e}xp(m, s)$	33 T13.47c
35.	$\mathbb{I}con(\mathbb{e}xp(m * \overline{2}^{u}, r), \mathbb{e}xp(m * \overline{2}^{u}, s), \mathbb{e}xp(m * \overline{2}^{u}, a))$	32,34,25 =E
36.	$(\exists i < a)(\exists j < a)\mathbb{I}con(\mathbb{e}xp(m * \overline{2}^{u}, i), \mathbb{e}xp(m * \overline{2}^{u}, j), \mathbb{e}xp(m * \overline{2}^{u}, a))$	31,35 (∃I)
37.	$\mathbb{A}xiomt(\mathbb{e}xp(m * \overline{2}^{u}, a)) \vee (\exists i < a)(\exists j < a)\mathbb{I}con(\mathbb{e}xp(m * \overline{2}^{u}, i), \mathbb{e}xp(m * \overline{2}^{u}, j), \mathbb{e}xp(m * \overline{2}^{u}, a))$	36 ∨I
38.	$\mathbb{A}xiomt(\mathbb{e}xp(m * \overline{2}^{u}, a)) \vee (\exists i < a)(\exists j < a)\mathbb{I}con(\mathbb{e}xp(m * \overline{2}^{u}, i), \mathbb{e}xp(m * \overline{2}^{u}, j), \mathbb{e}xp(m * \overline{2}^{u}, a))$	30,31-37 (∃E)
39.	$\mathbb{A}xiomt(\mathbb{e}xp(m * \overline{2}^{u}, a)) \vee (\exists i < a)(\exists j < a)\mathbb{I}con(\mathbb{e}xp(m * \overline{2}^{u}, i), \mathbb{e}xp(m * \overline{2}^{u}, j), \mathbb{e}xp(m * \overline{2}^{u}, a))$	26,27-38 ∨E
40.	$a = \mathbb{l}en(m)$	A (g 23∨E)
41.	$\mathbb{l}en(m) > \emptyset$	6 T13.45j
42.	$\mathbb{l}en(m) \dot{-} \overline{1} < \mathbb{l}en(m)$	41 T13.23i
43.	$\mathbb{e}xp(m * \overline{2}^{u}, \mathbb{l}en(m) \dot{-} \overline{1}) = \mathbb{e}xp(m, \mathbb{l}en(m) \dot{-} \overline{1})$	42 T13.47c
44.	$\mathbb{e}xp(m * \overline{2}^{u}, \mathbb{l}en(m) \dot{-} \overline{1}) = p$	43,5 =E
45.	$v \leq \mathbb{u}nv(v, p)$	T13.47n,o
46.	$(\exists v \leq u)(\mathbb{V}ar(v) \wedge u = \mathbb{u}nv(v, \mathbb{e}xp(m * \overline{2}^{u}, \mathbb{l}en(m) \dot{-} \overline{1})))$	1,44,45 (∃I)
47.	$\mathbb{G}en(\mathbb{e}xp(m * \overline{2}^{u}, \mathbb{l}en(m) \dot{-} \overline{1}), u)$	46 T13.40d
48.	$\mathbb{MP}(\mathbb{e}xp(m * \overline{2}^{u}, \mathbb{l}en(m) \dot{-} \overline{1}), \mathbb{e}xp(m * \overline{2}^{u}, \mathbb{l}en(m) \dot{-} \overline{1}), u) \vee$ $(\mathbb{e}xp(m * \overline{2}^{u}, \mathbb{l}en(m) \dot{-} \overline{1}) = \mathbb{e}xp(m * \overline{2}^{u}, \mathbb{l}en(m) \dot{-} \overline{1}) \wedge \mathbb{G}en(\mathbb{e}xp(m * \overline{2}^{u}, \mathbb{l}en(m) \dot{-} \overline{1}), u)$	47 ∨I
49.	$\mathbb{I}con(\mathbb{e}xp(m * \overline{2}^{u}, \mathbb{l}en(m) \dot{-} \overline{1}), \mathbb{e}xp(m * \overline{2}^{u}, \mathbb{l}en(m) \dot{-} \overline{1}), u)$	48 T13.40e
50.	$\mathbb{l}en(m) \dot{-} \overline{1} < a$	42,40 =E
51.	$(\exists i < a)(\exists j < a)\mathbb{I}con(\mathbb{e}xp(m * \overline{2}^{u}, i), \mathbb{e}xp(m * \overline{2}^{u}, j), \mathbb{e}xp(m * \overline{2}^{u}, a))$	50,17 (∃I)
52.	$\mathbb{A}xiomt(\mathbb{e}xp(m * \overline{2}^{u}, a)) \vee (\exists i < a)(\exists j < a)\mathbb{I}con(\mathbb{e}xp(m * \overline{2}^{u}, i), \mathbb{e}xp(m * \overline{2}^{u}, j), \mathbb{e}xp(m * \overline{2}^{u}, a))$	51 ∨I
53.	$\mathbb{A}xiomt(\mathbb{e}xp(m * \overline{2}^{u}, a)) \vee (\exists i < a)(\exists j < a)\mathbb{I}con(\mathbb{e}xp(m * \overline{2}^{u}, i), \mathbb{e}xp(m * \overline{2}^{u}, j), \mathbb{e}xp(m * \overline{2}^{u}, a))$	23,24-52 ∨E
54.	$(\forall k < \mathbb{l}en(m) * \overline{2}^{\mathbb{u}nv(v,p)})[\mathbb{A}xiomt(\mathbb{e}xp(m * \overline{2}^{\mathbb{u}nv(v,p)}, k)) \vee$ $(\exists i < k)(\exists j < k)\mathbb{I}con(\mathbb{e}xp(m * \overline{2}^{\mathbb{u}nv(v,p)}, i), \mathbb{e}xp(m * \overline{2}^{\mathbb{u}nv(v,p)}, j), \mathbb{e}xp(m * \overline{2}^{\mathbb{u}nv(v,p)}, k))]$	22-53 (∀I)
55.	$\mathbb{P}rft(m * \overline{2}^{\mathbb{u}nv(v,p)}, \mathbb{u}nv(v, p))$	18,20,54 T13.40f
56.	$\mathbb{P}rvt(\mathbb{u}nv(v, p))$	55 ∃I
57.	$\mathbb{P}rvt(\mathbb{u}nv(v, p))$	3,4-56 ∃E
58.	$[\mathbb{P}rvt(p) \wedge \mathbb{V}ar(v)] \rightarrow \mathbb{P}rvt(\mathbb{u}nv(v, p))$	1-57 →I

T13.57.j. PA $\vdash [\mathbb{W}ff(p) \wedge \mathbb{V}ar(v)] \rightarrow \mathbb{F}reefor(v, v, p)$

1.	$\mathbb{W}ff(p) \wedge \mathbb{V}ar(v)$	A (g →I)
2.	$\mathbb{F}ormseq(m, p)$	1 T13.49b
3.	$\mathbb{e}xp(m, \mathbb{l}en(m) \dot{-} \overline{1}) = p$	2 T13.49a
4.	$m > \overline{1}$	2 T13.49a
5.	$\mathbb{l}en(m) > \emptyset$	4 T13.45j
6.	$\mathbb{l}en(m) \dot{-} \overline{1} < \mathbb{l}en(m)$	5 T13.23i
7.	$\mathbb{F}ormseq(n, p) \wedge (\forall i < \mathbb{l}en(n))\mathbb{e}xp(n, i) \leq p \wedge \mathbb{l}en(n) \leq \mathbb{l}en(p)$	2,3,6 T13.49j
8.	$[\mathbb{p}i(\mathbb{l}en(p))^p]^{\mathbb{l}en(p)} \geq val(n, \mathbb{l}en(n))$	7 T13.46o
9.	$n > \overline{1}$	7 T13.49a
10.	$n \leq [\mathbb{p}i(\mathbb{l}en(p))^p]^{\mathbb{l}en(p)}$	8,9 T13.46n
11.	$n \leq B_p$	10 T13.57b
12.	$\mathbb{e}xp(n, \mathbb{l}en(n) \dot{-} \overline{1}) = p$	7 T13.49a
13.	$a < \mathbb{l}en(n)$	A (g (∀I))
14.	$E(n,a) \vee F(n,a) \vee G(n,a) \vee H(p,n,a)$	7,13 T13.49a
15.	$E(n,a)$	A (g 14∨E)
16.	$\mathbb{A}tomic(\mathbb{e}xp(n,a))$	15 abv
17.	$T(n,a)$	16 abv
18.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,v,n,a)$	17∨I
19.	$F(n,a) \vee G(n,a)$	A (g 14∨E)
20.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,v,n,a)$	similarly
21.	$H(p,n,a)$	A (g 14∨E)
22.	$(\exists i < a)(\exists j < p)[\mathbb{V}ar(j) \wedge \mathbb{e}xp(n,a) = \mathbb{u}nv(j, \mathbb{e}xp(n,i))$	21 abv
23.	$l < a \wedge u < p$	A (g 22 (∃E))
24.	$\mathbb{V}ar(u) \wedge \mathbb{e}xp(n,a) = \mathbb{u}nv(u, \mathbb{e}xp(n,l))$	
25.	$u = v \vee u \neq v$	T3.1
26.	$u = v$	A (g 25∨E)
27.	$l < \mathbb{l}en(n)$	13,23 T13.13b
28.	$\mathbb{W}ff(\mathbb{e}xp(n,l))$	7,27 T13.49l
29.	$\mathbb{e}xp(n,l) \leq p$	7,27 (∀E)
30.	$\mathbb{e}xp(n,a) = \mathbb{u}nv(v, \mathbb{e}xp(n,l))$	24,26 =E
31.	$(\exists q < p)[\mathbb{W}ff(q) \wedge \mathbb{e}xp(n,a) = \mathbb{u}nv(v,q)]$	29,28,30 (∃I)
32.	$W(p,v,n,a)$	31 abv
33.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,v,n,a)$	32 ∨I
34.	$u \neq v$	A (g 25∨E)
35.	$\mathbb{T}subseq(\overline{2}^v, \overline{2}^v, v, u, u \times \overline{4}, v)$	1,34 T13.50g
36.	$\mathbb{T}ermsub(v, u, u \times \overline{4}, v)$	35 T13.50l
37.	$\sim\mathbb{F}ree_t(v,u)$	36 T13.55a
38.	$\sim\mathbb{F}ree_t(v,u) \vee \sim\mathbb{F}ree_f(\mathbb{e}xp(n,l), v)$	37 ∨I
39.	$(\exists i < a)(\exists j \leq p)[\mathbb{V}ar(j) \wedge j \neq v \wedge (\sim\mathbb{F}ree_t(v,j) \vee \sim\mathbb{F}ree_f(\mathbb{e}xp(n,i),v)) \wedge \mathbb{e}xp(n,a) = \mathbb{u}nv(j, \mathbb{e}xp(n,i))$	23,24,34,38 (∃I)
40.	$X(p,v,v,n,a)$	39 abv
41.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,v,n,a)$	40 ∨I
42.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,v,n,a)$	25,26-41 ∨E
43.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,v,n,a)$	22,23-42 (∃E)
44.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,v,n,a)$	14,15-43 ∨E
45.	$(\forall k < \mathbb{l}en(n))[T(n,k) \vee U(n,k) \vee V(n,k) \vee W(p,v,n,k) \vee X(p,v,v,n,k)]$	13-44 (∀I)
46.	$\mathbb{F}fseq(n, v, v, p)$	12,9,45 T13.57a
47.	$(\exists x \leq B_p)\mathbb{F}fseq(x, v, v, p)$	11,46 (∃I)
48.	$\mathbb{F}reefor(v, v, p)$	47 T13.57b
49.	$[\mathbb{W}ff(p) \wedge \mathbb{V}ar(v)] \rightarrow \mathbb{F}reefor(v, v, p)$	1-48 →I

Exercise 13.44 T13.57.j

T13.57.k. PA $\vdash$ $\mathbb{A}xiomad4(n) \leftrightarrow \exists s(\exists p \leq n)(\exists v \leq n)[\mathbb{W}ff(p) \wedge \mathbb{V}ar(v) \wedge \mathbb{T}erm(s) \wedge \mathbb{F}reefor(s, v, p) \wedge n = \mathbb{c}nd(\mathbb{u}nv(v, p), \mathbb{f}ormsub(p, v, s))]$

Let $\mathcal{A} = \sim\mathbb{F}ree_f(v, p) \wedge n = \mathbb{c}nd(\mathbb{u}nv(v, p), p)$ and $\mathcal{B} = (\exists s \leq n)(\mathbb{F}ree_f(v, p) \wedge \mathbb{T}erm(s) \wedge \mathbb{F}reefor(s, v, p) \wedge n = \mathbb{c}nd(\mathbb{u}nv(v, p), \mathbb{f}ormsub(p, v, s))$

1.	$\mathbb{A}\mathit{xiomad4}(n)$	A (g ↔I)
2.	$(\exists p \le n)(\exists v \le n)[\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land (\mathcal{A} \lor \mathcal{B})]$	1 T13.57c
3.	$p \le n \land v \le n$	A (g 2 (∃E))
4.	$\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v)$	
5.	$\mathcal{A} \lor \mathcal{B}$	
6.	$\mathcal{A}$	A (g 5∨E)
7.	$\sim\mathbb{F}\mathit{ree}_f(v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), p)$	6 abv
8.	$v \le \mathbb{u}\mathit{nv}(v,p)$	T13.47n,o
9.	$v \le n$	7,8 T13.47n,o
10.	$\mathbb{T}\mathit{erm}(v)$	4 T13.48i,m
11.	$\mathbb{F}\mathit{reefor}(v,v,p)$	4 T13.57j
12.	$\mathit{formsub}(p,v,v) = p$	4,10,7 T13.56i
13.	$n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), \mathit{formsub}(p,v,v))$	7,12 =E
14.	$\exists s(\exists p \le n)(\exists v \le n)[\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land \mathbb{T}\mathit{erm}(s) \land \mathbb{F}\mathit{reefor}(s,v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), \mathit{formsub}(p,v,s))]$	3,4,10,11,13 (∃I)
15.	$\mathcal{B}$	A (g 5 (∃E)
16.	$(\exists s \le n)(\mathbb{F}\mathit{ree}_f(v,p) \land \mathbb{T}\mathit{erm}(s) \land \mathbb{F}\mathit{reefor}(s,v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), \mathit{formsub}(p,v,s)))$	15 abv
17.	$s \le n$	A (g 16 (∃E))
18.	$\mathbb{F}\mathit{ree}_f(v,p) \land \mathbb{T}\mathit{erm}(s) \land \mathbb{F}\mathit{reefor}(s,v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), \mathit{formsub}(p,v,s)))$	
19.	$\exists s(\exists p \le n)(\exists v \le n)[\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land \mathbb{T}\mathit{erm}(s) \land \mathbb{F}\mathit{reefor}(s,v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), \mathit{formsub}(p,v,s))]$	3,4,18 (∃I)
20.	$\exists s(\exists p \le n)(\exists v \le n)[\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land \mathbb{T}\mathit{erm}(s) \land \mathbb{F}\mathit{reefor}(s,v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), \mathit{formsub}(p,v,s))]$	16,17-19 (∃E)
21.	$\exists s(\exists p \le n)(\exists v \le n)[\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land \mathbb{T}\mathit{erm}(s) \land \mathbb{F}\mathit{reefor}(s,v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), \mathit{formsub}(p,v,s))]$	5,6-20 ∨E
22.	$\exists s(\exists p \le n)(\exists v \le n)[\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land \mathbb{T}\mathit{erm}(s) \land \mathbb{F}\mathit{reefor}(s,v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), \mathit{formsub}(p,v,s))]$	2,3-21 (∃E)
23.	$\exists s(\exists p \le n)(\exists v \le n)[\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land \mathbb{T}\mathit{erm}(s) \land \mathbb{F}\mathit{reefor}(s,v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), \mathit{formsub}(p,v,s))]$	A (g ↔I)
24.	$p \le n \land v \le n$	A (g 23 (∃E))
25.	$\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land \mathbb{T}\mathit{erm}(s) \land \mathbb{F}\mathit{reefor}(s,v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), \mathit{formsub}(p,v,s))$	
26.	$\mathbb{F}\mathit{ree}_f(v,p) \lor \sim\mathbb{F}\mathit{ree}_f(v,p)$	T3.1
27.	$\mathbb{F}\mathit{ree}_f(v,p)$	A (g 26∨E)
28.	$s \le \mathit{formsub}(p,v,s)$	25,27 T13.56j
29.	$s \le n$	28,25 T13.47n,o
30.	$\mathbb{F}\mathit{ree}_f(v,p) \land \mathbb{T}\mathit{erm}(s) \land \mathbb{F}\mathit{reefor}(s,v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), \mathit{formsub}(p,v,s))$	27,25 ∧I
31.	$(\exists s \le n)[\mathbb{F}\mathit{ree}_f(v,p) \land \mathbb{T}\mathit{erm}(s) \land \mathbb{F}\mathit{reefor}(s,v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), \mathit{formsub}(p,v,s))]$	29,30 (∃I)
32.	$\mathcal{B}$	31 abv
33.	$\mathcal{A} \lor \mathcal{B}$	32 ∨I
34.	$(\exists p \le n)(\exists v \le n)[\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land (\mathcal{A} \lor \mathcal{B})]$	24,25,33 (∃I)
35.	$\sim\mathbb{F}\mathit{ree}_f(v,p)$	A (g 26∨E)
36.	$\mathit{formsub}(p,v,s) = p$	25,35 T13.56i
37.	$n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), p)$	25,36 =E
38.	$\sim\mathbb{F}\mathit{ree}_f(v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), p)$	35,37 ∧I
39.	$\mathcal{A}$	38 abv
40.	$\mathcal{A} \lor \mathcal{B}$	39 ∨I
41.	$\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land (\mathcal{A} \lor \mathcal{B})$	25,40 ∧I
42.	$(\exists p \le n)(\exists v \le n)[\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land (\mathcal{A} \lor \mathcal{B})]$	24,42 (∃I)
43.	$(\exists p \le n)(\exists v \le n)[\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land (\mathcal{A} \lor \mathcal{B})]$	26,27-42 ∨E
44.	$(\exists p \le n)(\exists v \le n)[\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land (\mathcal{A} \lor \mathcal{B})]$	23,24-43 (∃E)
45.	$\mathbb{A}\mathit{xiomad4}(n)$	44 T13.57c
46.	$\mathbb{A}\mathit{xiomad4}(n) \leftrightarrow \exists s(\exists p \le n)(\exists v \le n)[\mathbb{W}\mathit{ff}(p) \land \mathbb{V}\mathit{ar}(v) \land \mathbb{T}\mathit{erm}(s) \land \mathbb{F}\mathit{reefor}(s,v,p) \land n = \mathbb{c}\mathit{nd}(\mathbb{u}\mathit{nv}(v,p), \mathit{formsub}(p,v,s))]$	1-22,23-45 ↔I

T13.57.o. PA ⊢ $\mathbb{l}\mathit{en}(\mathit{numseq}(x)) = Sx$

1.	$numseq(\emptyset) = \mathbb{p}i(\emptyset)^{\mathbb{n}um(\emptyset)}$	def
2.	$\mathbb{n}um(\emptyset) > \emptyset$	T13.57l
3.	$\mathbb{l}en(\mathbb{p}i(\emptyset)^{\mathbb{n}um(\emptyset)}) = S\emptyset$	2 T13.45k
4.	$\mathbb{l}en(numseq(\emptyset)) = S\emptyset$	3,1 =E
5.	$\quad \mathbb{l}en(numseq(x)) = Sx$	A (g →I)
6.	$\quad numseq(Sx) = numseq(x) \times \mathbb{p}i(Sx)^{\mathbb{n}um(Sx)}$	def
7.	$\quad \mathbb{n}um(Sx) > \emptyset$	T13.57l
8.	$\quad numseq(x) > \emptyset$	T13.57m
9.	$\quad \mathbb{p}i(Sx)^{\mathbb{n}um(Sx)} > \emptyset$	T13.43h
10.	$\quad \forall j[\mathbb{e}xp(numseq(Sx), j) = \mathbb{e}xp(numseq(x), j) + \mathbb{e}xp(\mathbb{p}i(Sx)^{\mathbb{n}um(Sx)}, j)]$	6,8,9 T13.44m
11.	$\quad \mathbb{e}xp(\mathbb{p}i(Sx)^{\mathbb{n}um(Sx)}, Sx) = \mathbb{n}um(Sx)$	T13.44i
12.	$\quad \mathbb{e}xp(\mathbb{p}i(Sx)^{\mathbb{n}um(Sx)}, Sx) > \emptyset$	7,11 =E
13.	$\quad \mathbb{e}xp(numseq(Sx), Sx) \geq \mathbb{e}xp(\mathbb{p}i(Sx)^{\mathbb{n}um(Sx)}, Sx)$	10 T13.13u
14.	$\quad \mathbb{e}xp(numseq(Sx), Sx) > \emptyset$	12,13 T13.13c
15.	$\quad \mathbb{l}en(numseq(Sx)) > Sx$	14 T13.45h
16.	$\quad \mathbb{l}en(numseq(Sx)) \geq SSx$	15 T13.13l
17.	$\quad\quad k > Sx$	A (g (∀I))
18.	$\quad\quad \mathbb{e}xp(numseq(x), k) = \emptyset$	5,17 T13.45l
19.	$\quad\quad \mathbb{e}xp(\mathbb{p}i(Sx)^{\mathbb{n}um(Sx)}, k) = \emptyset$	17 T13.44j
20.	$\quad\quad \mathbb{e}xp(numseq(Sx), k) = \emptyset$	10,18,19 =E
21.	$\quad (\forall k > Sx)\mathbb{e}xp(numseq(Sx), k) = \emptyset$	17-20 (∀I)
22.	$\quad \mathbb{l}en(\mathbb{n}umseq(Sx)) \leq SSx$	21 T13.45i
23.	$\quad \mathbb{l}en(\mathbb{n}umseq(Sx)) = SSx$	16,22 T13.20
24.	$\mathbb{l}en(numseq(x)) = Sx \rightarrow \mathbb{l}en(numseq(Sx)) = SSx$	5-23 →I
25.	$\mathbb{l}en(numseq(x)) = Sx$	4,24 IN

T13.57.t. PA $\vdash [\mathbb{W}ff(p) \wedge \mathbb{V}ar(v)] \rightarrow \mathbb{F}reefor(\mathbb{n}um(x), v, p)$

1.	$\mathbb{W}ff(p) \wedge \mathbb{V}ar(v)$	A (g →I)
2.	$\mathbb{F}ormseq(m, p)$	1 T13.49b
3.	$\mathbb{e}xp(m, \mathbb{l}en(m) \dot{-} \bar{1}) = p$	2 T13.49a
4.	$Formseq(n, p)$	2,3 T13.49j
5.	$(\forall i < \mathbb{l}en(n))\mathbb{e}xp(n, i) \leq p \wedge \mathbb{l}en(n) \leq \mathbb{l}en(p)$	2,3 T13.49j
6.	$[\mathbb{p}i(\mathbb{l}en(p))^p]^{\mathbb{l}en(p)} \geq val(n, \mathbb{l}en(n))$	5 T13.46o
7.	$n > \bar{1}$	4 T13.49a
8.	$val(n, \mathbb{l}en(n)) = n$	7 T13.46n
9.	$n \leq B_p$	6,8 T13.57b
10.	$\mathbb{e}xp(n, \mathbb{l}en(n) \dot{-} \bar{1}) = p$	4 T13.49a
11.	$a < \mathbb{l}en(n)$	A (g (∀I))
12.	$E(n,a) \vee F(n,a) \vee G(n,a) \vee H(p,n,a)$	4,11 T13.49a
13.	$E(n,a)$	A (g 12∨E)
14.	$\mathbb{A}tomic(\mathbb{e}xp(n,a))$	13 abv
15.	$T(n,a)$	14 abv
16.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,\mathbb{n}um(x),n,a)$	15 ∨I
17.	$F(n,a) \vee G(n,a)$	A (g 12∨E)
18.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,\mathbb{n}um(x),n,a)$	similarly
19.	$H(p,n,a)$	A (g 12∨E)
20.	$(\exists i < a)(\exists j < p)[\mathbb{V}ar(j) \wedge \mathbb{e}xp(n,a) = \mathbb{u}nv(j, \mathbb{e}xp(n,i))]$	19 abv
21.	$i < a \wedge j < p$	A (g 20 (∃E))
22.	$\mathbb{V}ar(j)$	
23.	$\mathbb{e}xp(n,a) = \mathbb{u}nv(j, \mathbb{e}xp(n,i))$	
24.	$j = v \vee j \neq v$	T3.1
25.	$j = v$	A (g 24∨E)
26.	$i < \mathbb{l}en(n)$	11,21 T13.13b
27.	$\mathbb{W}ff(\mathbb{e}xp(n,i))$	4,26 T13.49l
28.	$\mathbb{e}xp(n,a) = \mathbb{u}nv(v, \mathbb{e}xp(n,i))$	23,25 =E
29.	$\mathbb{W}ff(\mathbb{e}xp(n,i)) \wedge \mathbb{e}xp(n,a) = \mathbb{u}nv(v, \mathbb{e}xp(n,i))$	27,28 ∧I
30.	$\mathbb{e}xp(n,i) \leq p$	5,26 (∀E)
31.	$(\exists b \leq p)[\mathbb{W}ff(b) \wedge \mathbb{e}xp(n,a) = \mathbb{u}nv(v,b)]$	29,30 (∃I)
32.	$W(p,v,n,a)$	31 abv
33.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,\mathbb{n}um(x),n,a)$	32 ∨I
34.	$j \neq v$	A (g 24∨E)
35.	$\sim\mathbb{F}ree_t(\mathbb{n}um(x), j)$	T13.57s
36.	$\sim\mathbb{F}ree_t(\mathbb{n}um(x), j) \vee \sim\mathbb{F}ree_f(\mathbb{e}xp(n,i), v)$	35 ∨I
37.	$(\exists i < a)(\exists j < p)[\mathbb{V}ar(j) \wedge j \neq v \wedge (\sim\mathbb{F}ree_t(\mathbb{n}um(x), j) \vee \sim\mathbb{F}ree_f(\mathbb{e}xp(n,i), v)) \wedge \mathbb{e}xp(n,a) = \mathbb{u}nv(j, \mathbb{e}xp(n,i))]$	21,22,34,36,23 (∃I)
38.	$X(p,v,\mathbb{n}um(x),n,a)$	37 abv
39.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,\mathbb{n}um(x),n,a)$	38 ∨I
40.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,\mathbb{n}um(x),n,a)$	24,25-39 ∨E
41.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,\mathbb{n}um(x),n,a)$	20,21-40 (∃E)
42.	$T(n,a) \vee U(n,a) \vee V(n,a) \vee W(p,v,n,a) \vee X(p,v,\mathbb{n}um(x),n,a)$	12,13-41 ∨E
43.	$(\forall k < \mathbb{l}en(n))[T(n,k) \vee U(n,k) \vee V(n,k) \vee W(p,v,n,k) \vee X(p,v,\mathbb{n}um(x),n,k)]$	11-42 (∀I)
44.	$\mathbb{F}fseq(n, \mathbb{n}um(x), v, p)$	10,7,43 T13.57a
45.	$(\exists y \leq B_p)(\mathbb{F}fseq(y, \mathbb{n}um(x), v, p)$	9,44 (∃I)
46.	$\mathbb{F}reefor(\mathbb{n}um(x), v, p)$	45 T13.57b
47.	$[\mathbb{W}ff(p) \wedge \mathbb{V}ar(v)] \rightarrow \mathbb{F}reefor(\mathbb{n}um(x), v, p)$	1-46 →I

E13.45. Show T13.58a; then set up the argument for T13.58g including assertion of the main proposition to be shown by induction; then set up the show part working just the P case. Hard core: finish T13.58g and the rest of the results in T13.58.

T13.58.

T13.58.b. PA $\vdash [\mathbb{T}erm(p) \wedge v \neq w] \rightarrow \exists q \exists t \exists t'[\mathbb{T}ermsub(p, v, \mathbb{n}um(y), t) \wedge \mathbb{T}ermsub(p, w, \mathbb{n}um(z), t') \wedge \mathbb{T}ermsub(t, w, \mathbb{n}um(z), q) \wedge \mathbb{T}ermsub(t', v, \mathbb{n}um(y), q)]$

Let $\mathcal{P} = \exists q \exists a \exists b \exists c \exists d[\mathbb{T}subseq(a, b, \mathbb{e}xp(n, k), w, \mathbb{n}um(z), q) \wedge \mathbb{T}subseq(c, d, \mathbb{e}xp(n', k'), v, \mathbb{n}um(y), q)]$

1.	$\mathbb{T}erm(p) \wedge v \neq w$	A (g $\rightarrow$I)
2.	$\mathbb{T}erm(\mathbb{n}um(y)) \wedge \mathbb{T}erm(\mathbb{n}um(z))$	T13.57r
3.	$\exists t\, \mathbb{T}ermsub(p, v, \mathbb{n}um(y), t) \wedge \exists t'\, \mathbb{T}ermsub(p, w, \mathbb{n}um(z), t')$	1,2 T13.50m
4.	$\mathbb{T}ermsub(p, v, \mathbb{n}um(y), t) \wedge \mathbb{T}ermsub(p, w, \mathbb{n}um(z), t')$	A (g 3$\exists$E)
5.	$(\exists x \leq X)(\exists y \leq Y)\mathbb{T}subseq(x, y, p, v, \mathbb{n}um(y), t) \wedge (\exists x \leq X)(\exists y \leq Y)\mathbb{T}subseq(x, y, p, w, \mathbb{n}um(z), t')$	4 T13.50b
6.	$\mathbb{T}subseq(m, n, p, v, \mathbb{n}um(y), t) \wedge \mathbb{T}subseq(m', n', p, w, \mathbb{n}um(z), t')$	A (g 5 ($\exists$E))
7.	$\mathbb{T}ermseq(m, p) \wedge \mathbb{T}ermseq(m', t')$	6 T13.50a
8.	$\mathbb{e}xp(m, \mathbb{l}en(m) \dot{-} \overline{1}) = p \wedge \mathbb{e}xp(m', \mathbb{l}en(m') \dot{-} \overline{1}) = p$	7 T13.48a
9.	$m > \overline{1} \wedge m' > \overline{1}$	7 T13.48a
10.	$\mathbb{l}en(m) > \emptyset \wedge \mathbb{l}en(m') > \emptyset$	9 T13.45j
11.	$\mathbb{e}xp(n, \mathbb{l}en(n) \dot{-} \overline{1}) = t \wedge \mathbb{e}xp(n', \mathbb{l}en(n') \dot{-} \overline{1}) = t'$	6 T13.50a
12.	$\mathbb{l}en(m) = \mathbb{l}en(n) \wedge \mathbb{l}en(m') = \mathbb{l}en(n')$	6 T13.50a
13.	$(\forall k < \mathbb{l}en(m))[I(m, n, k) \vee J(v, m, n, k) \vee K(v, \mathbb{n}um(y), m, n, k) \vee L(m, n, k) \vee M(m, n, k) \vee N(m, n, k)]$	6 T13.50a
14.	$(\forall k < \mathbb{l}en(m'))[I(m', n', k) \vee J(w, m', n', k) \vee K(w, \mathbb{n}um(z), m', n', k) \vee L(m', n', k) \vee M(m', n', k) \vee N(m', n', k)]$	6 T13.50a
15.	$l < \mathbb{l}en(m) \wedge l' < \mathbb{l}en(m')$	A (g ($\forall$I))
16.	$\mathbb{l}en(\mathbb{e}xp(m, l)) \leq \emptyset$	A (g $\rightarrow$I)
17.	$\sim[\mathbb{e}xp(m, l) = \mathbb{e}xp(m', l') \rightarrow \mathcal{P}^{k,k'}_{l,l'}]$	A (c $\sim$E)
18.	$\mathbb{e}xp(m, l) > \overline{1}$	7,15 T13.48f
19.	$\mathbb{e}xp(m, l) \not> \overline{1}$	16 T13.45j
20.	$\bot$	18,19 $\bot$I
21.	$\mathbb{e}xp(m, l) = \mathbb{e}xp(m', l') \rightarrow \mathcal{P}^{k,k'}_{l,l'}$	17-20 $\sim$E
22.	$\mathbb{l}en(\mathbb{e}xp(m, l)) \leq \emptyset \rightarrow (\mathbb{e}xp(m, l) = \mathbb{e}xp(m', l') \rightarrow \mathcal{P}^{k,k'}_{l,l'})$	16-21 $\rightarrow$I
23.	$(\forall k < \mathbb{l}en(m))(\forall k' < \mathbb{l}en(m'))[\mathbb{l}en(\mathbb{e}xp(m, k)) \leq \emptyset \rightarrow (\mathbb{e}xp(m, k) = \mathbb{e}xp(m', k') \rightarrow \mathcal{P})]$	15-22 ($\forall$I)
24.	$(\forall k < \mathbb{l}en(m))(\forall k' < \mathbb{l}en(m'))[\mathbb{l}en(\mathbb{e}xp(m, k)) \leq x \rightarrow (\mathbb{e}xp(m, k) = \mathbb{e}xp(m', k') \rightarrow \mathcal{P})]$	A (g $\rightarrow$I)
25.	$l < \mathbb{l}en(m) \wedge l' < \mathbb{l}en(m')$	A (g ($\forall$I))
26.	$\mathbb{l}en(\mathbb{e}xp(m, l)) \leq Sx \wedge \mathbb{e}xp(m, l) = \mathbb{e}xp(m', l')$	A (g $\rightarrow$I)
27.	$I(m, n, l) \vee J(v, m, n, l) \vee K(v, \mathbb{n}um(y), m, n, l) \vee L(m, n, l) \vee M(m, n, l) \vee N(m, n, l)$	13,25 ($\forall$E)
28.	$I(m', n', l') \vee J(w, m', n', l') \vee K(w, \mathbb{n}um(z), m', n', l') \vee L(m', n', l') \vee M(m', n', l') \vee N(m', n', l')$	14,25 ($\forall$E)
29.	$I(m, n, l)$	A (g 27$\vee$E)
30.	$\mathbb{e}xp(m, l) = \overline{\ulcorner\emptyset\urcorner} \wedge \mathbb{e}xp(n, l) = \overline{\ulcorner\emptyset\urcorner}$	29 abv
31.	$I(m', n', l')$	A (g 28$\vee$E)
32.	$\mathbb{e}xp(m', l') = \overline{\ulcorner\emptyset\urcorner} \wedge \mathbb{e}xp(n', l') = \overline{\ulcorner\emptyset\urcorner}$	31 abv
33.	$\mathbb{T}subseq(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, \overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, \mathbb{e}xp(n, l), w, \mathbb{n}um(z), \overline{\ulcorner\emptyset\urcorner})$	30 T13.50f
34.	$\mathbb{T}subseq(\overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, \overline{2}^{\overline{\ulcorner\emptyset\urcorner}}, \mathbb{e}xp(n', l'), v, \mathbb{n}um(y), \overline{\ulcorner\emptyset\urcorner})$	32 T13.50f
35.	$\mathcal{P}^{k,k'}_{l,l'}$	33,34 $\exists$I
36.	$J(w, m', n', l') \vee K(w, \mathbb{n}um(z), m', n', l') \vee L(m', n', l') \vee M(m', n', l') \vee N(m', n', l')$	A (g 28$\vee$E)
37.	$\sim\mathcal{P}^{k,k'}_{l,l'}$	A (c $\sim$E)
38.	$\mathbb{e}xp(m', l') = \overline{\ulcorner\emptyset\urcorner}$	30,26 =E
39.	$\sim[J(w, m', n', l') \vee K(w, \mathbb{n}um(z), m', n', l') \vee L(m', n', l') \vee M(m', n', l') \vee N(m', n', l')]$	38 T13.55c
40.	$\bot$	36,39 $\bot$I
41.	$\mathcal{P}^{k,k'}_{l,l'}$	37-40 $\sim$E

Exercise 13.45 T13.58.b

42.	$J(v,m,n,l)$	A (g 27 $\vee$E)
43.	$\mathbb{V}ar(exp(m,l)) \wedge exp(m,l) \neq v \wedge exp(n,l) = exp(m,l)$	42 abv
44.	$J(w,m',n',l')$	A (g 28$\vee$E)
45.	$\mathbb{V}ar(exp(m',l')) \wedge exp(m',l') \neq w \wedge exp(n',l') = exp(m',l')$	43 abv
46.	$exp(n,l) \neq w \wedge exp(n',l') \neq v \wedge exp(n,l) = exp(n',l')$	26,43,45 =E
47.	$\mathbb{T}subseq(\overline{2}^{exp(n,l)}, \overline{2}^{exp(n,l)}, exp(n,l), w, num(z), exp(n,l))$	43,46 T13.50g
48.	$\mathbb{T}subseq(\overline{2}^{exp(n',l')}, \overline{2}^{exp(n',l')}, exp(n',l'), v, num(y), exp(n',l'))$	45,46 T13.50g
49.	$\mathcal{P}^{k,k'}_{l,l'}$	47,48,46 $\exists$I
50.	$K(w, num(z), m', n', l')$	A (g 28$\vee$E)
51.	$\mathbb{V}ar(exp(m',l')) \wedge exp(m',l') = w \wedge exp(n',l') = num(z)$	50 abv
52.	$\mathbb{V}ar(exp(n,l)) \wedge exp(n,l) = w$	26,43,51 =E
53.	$\mathbb{T}subseq(\overline{2}^{exp(n,l)}, \overline{2}^{num(z)}, exp(n,l), w, num(z), num(z))$	52 T13.50h
54.	$\mathbb{T}ermsub(exp(n',l'), v, num(y), num(z))$	51 T13.57s
55.	$(\exists x \leq X)(\exists y \leq Y)\mathbb{T}subseq(x, y, exp(n',l'), v, num(y), num(z))$	54 T13.50b
56.	$\mathbb{T}subseq(e, f, exp(n',l'), v, num(y), num(z))$	A (g 55 ($\exists$E))
57.	$\mathcal{P}^{k,k'}_{l,l'}$	53,56 $\exists$I
58.	$\mathcal{P}^{k,k'}_{l,l'}$	55,56-57 ($\exists$E)
59.	$I(m',n',l') \vee L(m',n',l') \vee M(m',n',l') \vee N(m',n',l')$	A (g 28$\vee$E)
60.	$\mathbb{V}ar(exp(m',l'))$	43,26 =E
61.	$\sim\mathcal{P}^{k,k'}_{l,l'}$	A (c $\sim$E)
62.	$exp(m',l') = w$	A (c $\sim$I)
63.	$\sim[I(m',n',l') \vee J(w,m',n',l') \vee L(m',n',l') \vee M(m',n',l') \vee N(m',n',l')]$	60,62 T13.55e
64.	$\bot$	with 59,63
65.	$exp(m',l') \neq w$	62-64 $\sim$I
66.	$\sim[I(m',n',l') \vee K(w,num(z),m',n',l') \vee L(m',n',l') \vee M(m',n',l') \vee N(m',n',l')]$	60,65 T13.55d
67.	$\bot$	with 59,66
68.	$\mathcal{P}^{k,k'}_{l,l'}$	61-67 $\sim$E
69.	$\mathcal{P}^{k,k'}_{l,l'}$	28,44-68 $\vee$E

Exercise 13.45 T13.58.b

70.	$K(v, \mathbb{num}(y), m, n, l)$	A (g 27∨E)
71.	$\mathbb{V}ar(\mathbb{exp}(m,l) \wedge \mathbb{exp}(m,l) = v \wedge \mathbb{exp}(n,l) = \mathbb{num}(y)$	70 abv
72.	$K(w, \mathbb{num}(z), m', n', l')$	A (g 28∨E)
73.	$\mathbb{V}ar(\mathbb{exp}(m',l') \wedge \mathbb{exp}(m',l') = w \wedge \mathbb{exp}(n',l') = \mathbb{num}(z)$	72 abv
74.	$\sim\mathcal{P}^{k,k'}_{l,l'}$	A (c ∼E)
75.	$v = w$	26,71,73
76.	$\bot$	1,75 ⊥I
77.	$\mathcal{P}^{k,k'}_{l,l'}$	74-76 ∼E
78.	$J(w, m', n', l')$	A (g 28∨E)
79.	$\mathbb{V}ar(\mathbb{exp}(m',l')) \wedge \mathbb{exp}(m',l') \neq w \wedge \mathbb{exp}(n',l') = \mathbb{exp}(m',l')$	78 abv
80.	$\mathbb{V}ar(\mathbb{exp}(n',l')) \wedge \mathbb{exp}(n',l') = v$	26,71,79 =E
81.	$\mathbb{T}subseq(\overline{2}^{\mathbb{exp}(n',l')}, \overline{2}^{\mathbb{num}(y)}, \mathbb{exp}(n',l'), v, \mathbb{num}(y), \mathbb{num}(y))$	80 T13.50h
82.	$\mathbb{T}ermsub(\mathbb{exp}(n,l), w, \mathbb{num}(z), \mathbb{num}(y))$	71 T13.57s
83.	$\mathbb{T}subseq(e, f, \mathbb{exp}(n,l), w, \mathbb{num}(z), \mathbb{num}(y))$	82 T13.50b
84.	$\mathcal{P}^{k,k'}_{l,l'}$	81,83 ∃I
85.	$I(m',n',l') \vee L(m',n',l') \vee M(m',n',l') \vee N(m',n',l')$	A (g 28∨E)
86.	$\mathbb{V}ar(\mathbb{exp}(m',l'))$	26,71 =E
87.	$\sim\mathcal{P}^{k,k'}_{l,l'}$	A (c ∼E)
88.	$\mathbb{exp}(m',l') = w$	A (c ∼I)
89.	$\sim[I(m',n',l') \vee J(w,m',n',l') \vee L(m',n',l') \vee M(m',n',l') \vee N(m',n',l')]$	86,88 T13.55e
90.	$\bot$	with 85,89
91.	$\mathbb{exp}(m',l') \neq w$	62-64 ∼I
92.	$\sim[I(m',n',l') \vee K(w,\mathbb{num}(z),m',n',l') \vee L(m',n',l') \vee M(m',n',l') \vee N(m',n',l')]$	86,91 T13.55d
93.	$\bot$	with 85,92
94.	$\mathcal{P}^{k,k'}_{l,l'}$	87-93 ∼E
95.	$\mathcal{P}^{k,k'}_{l,l'}$	28,72-94 ∨E

96.	$L(m,n,l)$	A (g 27∨E)
97.	$(\exists i < l)[exp(m,l) = \overline{\ulcorner S \urcorner} * exp(m,i) \wedge exp(n,l) = \overline{\ulcorner S \urcorner} * exp(n,i)]$	96 abv
98.	$h < l$	A (g 97 (∃E))
99.	$exp(m,l) = \overline{\ulcorner S \urcorner} * exp(m,h) \wedge exp(n,l) = \overline{\ulcorner S \urcorner} * exp(n,h)$	
100.	$L(m',n',l')$	A (g 28∨E)
101.	$(\exists i < l')[exp(m',l') = \overline{\ulcorner S \urcorner} * exp(m',i) \wedge exp(n',l') = \overline{\ulcorner S \urcorner} * exp(n',i)]$	100 abv
102.	$h' < l'$	A (g 101 (∃E))
103.	$exp(m',l') = \overline{\ulcorner S \urcorner} * exp(m',h') \wedge exp(n',l') = \overline{\ulcorner S \urcorner} * exp(n',h')$	
104.	$\overline{\ulcorner S \urcorner} * exp(m,h) = \overline{\ulcorner S \urcorner} * exp(m',h')$	26,99,103 =E
105.	$h < len(m) \wedge h' < len(m')$	25,98,102 T13.13b
106.	$Term(exp(m,h)) \wedge Term(exp(m',h'))$	7,105 T13.48n
107.	$exp(m,h) = exp(m',h')$	106,104 T13.52b
108.	$len(exp(m,l)) = \overline{1} + len(exp(m,h))$	99 T13.47f
109.	$len(exp(m,l)) > len(exp(m,h))$	108 T13.13l
110.	$len(exp(m,h)) < Sx$	26,109 T13.13c
111.	$len(exp(m,h)) \leq x$	110 T13.13n
112.	$exp(m,h) = exp(m',h') \rightarrow \mathcal{P}^{k,k'}_{h,h'}$	24,105,111 (∀E)
113.	$\mathcal{P}^{k,k'}_{h,h'}$	112,107 →E
114.	$\exists q \exists a \exists b \exists c \exists d[Tsubseq(a,b,exp(n,h),w,num(z),q) \wedge Tsubseq(c,d,exp(n',h'),v,num(y),q)]$	113 abv
115.	$Tsubseq(a,b,exp(n,h),w,num(z),q) \wedge Tsubseq(c,d,exp(n',h'),v,num(y),q)$	A (g 114∃E)
116.	$Tsubseq(a * \overline{2}^{\overline{\ulcorner S \urcorner} * exp(n,h)}, b * \overline{2}^{\overline{\ulcorner S \urcorner} * q}, \overline{\ulcorner S \urcorner} * exp(n,h), w, num(z), \overline{\ulcorner S \urcorner} * q)$	115 T13.50i
117.	$Tsubseq(c * \overline{2}^{\overline{\ulcorner S \urcorner} * exp(n',h')}, d * \overline{2}^{\overline{\ulcorner S \urcorner} * q}, \overline{\ulcorner S \urcorner} * exp(n',h'), v, num(y), \overline{\ulcorner S \urcorner} * q)$	115 T13.50i
118.	$Tsubseq(a * \overline{2}^{exp(n,l)}, b * \overline{2}^{\overline{\ulcorner S \urcorner} * q}, exp(n,l), w, num(z), \overline{\ulcorner S \urcorner} * q)$	99,116 =E
119.	$Tsubseq(c * \overline{2}^{exp(n',l')}, b * \overline{2}^{\overline{\ulcorner S \urcorner} * q}, exp(n',l'), v, num(y), \overline{\ulcorner S \urcorner} * q)$	103,117 =E
120.	$\mathcal{P}^{k,k'}_{l,l'}$	118,119 ∃I
121.	$\mathcal{P}^{k,k'}_{l,l'}$	114,115-120 ∃E
122.	$\mathcal{P}^{k,k'}_{l,l'}$	101,102-121 (∃E)
123.	$I(m',n',l') \vee J(w,m',n',l') \vee K(w,num(z),m',n',l') \vee M(m',n',l') \vee N(m',n',l')$	A (g 28∨E)
124.	$exp(m',l') = \overline{\ulcorner S \urcorner} * exp(m,h)$	26,99 =E
125.	$\sim\mathcal{P}^{k,k'}_{l,l'}$	A (c ∼E)
126.	$\sim[I(m',n',l') \vee J(w,m',n',l') \vee K(w,num(z),m',n',l') \vee M(m',n',l') \vee N(m',n',l')]$	124 T13.55f
127.	$\bot$	123,126 ⊥I
128.	$\mathcal{P}^{k,k'}_{l,l'}$	125-127 ∼E
129.	$\mathcal{P}^{k,k'}_{l,l'}$	28,100-128 ∨E
130.	$\mathcal{P}^{k,k'}_{l,l'}$	97,98-129 (∃E)
131.	$M(m,n,l) \vee N(m,n,l)$	A (g 27∨E)
132.	$\mathcal{P}^{k,k'}_{l,l'}$	similarly
133.	$\mathcal{P}^{k,k'}_{l,l'}$	27,29-132 ∨E

134. $\mathbb{len}(\mathbb{exp}(m,l)) \leq Sx \rightarrow (\mathbb{exp}(m,l) = \mathbb{exp}(m',l') \rightarrow \mathcal{P}^{k,k'}_{l,l'})$ 26-133 →I

135. $(\forall k < \mathbb{len}(m))(\forall k' < \mathbb{len}(m'))[\mathbb{len}(\mathbb{exp}(m,k)) \leq Sx \rightarrow (\mathbb{exp}(m,k) = \mathbb{exp}(m',k') \rightarrow \mathcal{P})]$ 25-134 (∀I)

136. $(\forall k < \mathbb{len}(m))(\forall k' < \mathbb{len}(m'))[\mathbb{len}(\mathbb{exp}(m,k)) \leq x \rightarrow (\mathbb{exp}(m,k) = \mathbb{exp}(m',k') \rightarrow \mathcal{P})] \rightarrow$
$(\forall k < \mathbb{len}(m))(\forall k' < \mathbb{len}(m'))[\mathbb{len}(\mathbb{exp}(m,k)) \leq Sx \rightarrow (\mathbb{exp}(m,k) = \mathbb{exp}(m',k') \rightarrow \mathcal{P})]$ 24-135 →I

137. $\forall x(\forall k < \mathbb{len}(m))(\forall k' < \mathbb{len}(m'))[\mathbb{len}(\mathbb{exp}(m,k)) \leq x \rightarrow (\mathbb{exp}(m,k) = \mathbb{exp}(m',k') \rightarrow \mathcal{P})]$ 23,136 IN

138. $\mathbb{len}(m) \dot{-} \bar{1} < \mathbb{len}(m) \wedge \mathbb{len}(m') \dot{-} \bar{1} < \mathbb{len}(m')$ 10 T13.23i

139. $\mathbb{len}(\mathbb{exp}(m, \mathbb{len}(m) \dot{-} \bar{1})) \leq \mathbb{len}(p) \rightarrow (\mathbb{exp}(m, \mathbb{len}(m) \dot{-} \bar{1}) = \mathbb{exp}(m', \mathbb{len}(m') \dot{-} \bar{1}) \rightarrow \mathcal{P}^{k,k'}_{\mathbb{len}(m)\dot{-}\bar{1},\mathbb{len}(m')\dot{-}\bar{1}})$ 137,138 (∀E)

140. $\mathcal{P}^{k,k'}_{\mathbb{len}(m)\dot{-}\bar{1},\mathbb{len}(m')\dot{-}\bar{1}}$ 139,8 →E

141. $\exists q\exists a\exists b\exists c\exists d[\mathbb{T}subseq(a,b,\mathbb{exp}(n,\mathbb{len}(m) \dot{-} \bar{1}), w, \mathbb{num}(z), q) \wedge \mathbb{T}subseq(c,d,\mathbb{exp}(n',\mathbb{len}(m') \dot{-} \bar{1}), v, \mathbb{num}(y), q)]$ 140 abv

142. $\exists q\exists a\exists b\exists c\exists d[\mathbb{T}subseq(a,b,t,w,\mathbb{num}(z),q) \wedge \mathbb{T}subseq(c,d,t',v,\mathbb{num}(y),q)]$ 141,11,12 =E

143. $\mathbb{T}subseq(a,b,t,w,\mathbb{num}(z),q) \wedge \mathbb{T}subseq(c,d,t',v,\mathbb{num}(y),q)$ A (g 142∃E)

144. $\mathbb{T}ermsub(t,w,\mathbb{num}(z),q) \wedge \mathbb{T}ermsub(t',v,\mathbb{num}(y),q)$ 143 T13.50l

145. $\exists q\exists t\exists t'[\mathbb{T}ermsub(p,v,\mathbb{num}(y),t) \wedge \mathbb{T}ermsub(p,w,\mathbb{num}(z),t') \wedge$
$\mathbb{T}ermsub(t,w,\mathbb{num}(z),q) \wedge \mathbb{T}ermsub(t',v,\mathbb{num}(y),q)]$ 4,144 ∃I

146. $\exists q\exists t\exists t'[\mathbb{T}ermsub(p,v,\mathbb{num}(y),t) \wedge \mathbb{T}ermsub(p,w,\mathbb{num}(z),t') \wedge$
$\mathbb{T}ermsub(t,w,\mathbb{num}(z),q) \wedge \mathbb{T}ermsub(t',v,\mathbb{num}(y),q)]$ 142,143-145 ∃E

147. $\exists q\exists t\exists t'[\mathbb{T}ermsub(p,v,\mathbb{num}(y),t) \wedge \mathbb{T}ermsub(p,w,\mathbb{num}(z),t') \wedge$
$\mathbb{T}ermsub(t,w,\mathbb{num}(z),q) \wedge \mathbb{T}ermsub(t',v,\mathbb{num}(y),q)]$ 5,6-146 (∃E)

148. $\exists q\exists t\exists t'[\mathbb{T}ermsub(p,v,\mathbb{num}(y),t) \wedge \mathbb{T}ermsub(p,w,\mathbb{num}(z),t') \wedge$
$\mathbb{T}ermsub(t,w,\mathbb{num}(z),q) \wedge \mathbb{T}ermsub(t',v,\mathbb{num}(y),q)]$ 3,4-147 ∃E

149. $[\mathbb{T}erm(p) \wedge v \neq w] \rightarrow \exists q\exists t\exists t'[\mathbb{T}ermsub(p,v,\mathbb{num}(y),t) \wedge \mathbb{T}ermsub(p,w,\mathbb{num}(z),t') \wedge$
$\mathbb{T}ermsub(t,w,\mathbb{num}(z),q) \wedge \mathbb{T}ermsub(t',v,\mathbb{num}(y),q)]$ 1-148 →I

T13.58.d. PA $\vdash [\mathbb{W}ff(p) \wedge v \neq w] \rightarrow \mathbb{f}ormsub(\mathbb{f}ormsub(p,v,\mathbb{num}(y)),w,\mathbb{num}(z)) =$
$\mathbb{f}ormsub(\mathbb{f}ormsub(p,w,\mathbb{num}(z)),v,\mathbb{num}(y))$

Let $\mathcal{P} = \exists q\exists a\exists b\exists c\exists d[\mathbb{F}subseq(a,b,\mathbb{exp}(n,k),w,\mathbb{num}(z),q) \wedge \mathbb{F}subseq(c,d,\mathbb{exp}(n',k'),v,\mathbb{num}(y),q)]$

1.	$\mathbb{W}ff(p) \wedge v \neq w$	A (g →I)
2.	$\mathbb{T}erm(\mathbb{n}um(y)) \wedge \mathbb{T}erm(\mathbb{n}um(z))$	T13.57r
3.	$\exists q \mathbb{F}ormsub(p, v, \mathbb{n}um(y), q) \wedge \exists q \mathbb{F}ormsub(p, w, \mathbb{n}um(z), q)$	1,2 T13.51k
4.	$\mathbb{F}ormsub(p, v, \mathbb{n}um(y), t) \wedge \mathbb{F}ormsub(p, w, \mathbb{n}um(z), t')$	A (g 3∃E)
5.	$formsub(p, v, \mathbb{n}um(y)) = t \wedge formsub(p, w, \mathbb{n}um(z)) = t'$	1,2,4 T13.56h
6.	$\mathbb{W}ff(t) \wedge \mathbb{W}ff(t')$	4,2 T13.51d
7.	$(\exists x \leq X)(\exists y \leq Y)\mathbb{F}subseq(x, y, p, v, \mathbb{n}um(y), t) \wedge (\exists x \leq X)(\exists y \leq Y)\mathbb{F}subseq(x, y, p, w, \mathbb{n}um(z), t')$	4 T13.51b
8.	$\mathbb{F}subseq(m, n, p, v, \mathbb{n}um(y), t) \wedge \mathbb{F}subseq(m', n', p, w, \mathbb{n}um(z), t')$	A (g 7 (∃E))
9.	$\mathbb{F}ormseq(m, p) \wedge \mathbb{F}ormseq(m', p)$	8 T13.51a
10.	$\mathbb{e}xp(m, \mathbb{l}en(m) \dot{-} \overline{1}) = p \wedge \mathbb{e}xp(m', \mathbb{l}en(m') \dot{-} \overline{1}) = p$	9 T13.49a
11.	$m > \overline{1} \wedge m' > \overline{1}$	9 T13.49a
12.	$\mathbb{l}en(m) > \emptyset \wedge \mathbb{l}en(m') > \emptyset$	11 T13.45j
13.	$\mathbb{e}xp(n, \mathbb{l}en(n) \dot{-} \overline{1}) = t \wedge \mathbb{e}xp(n', \mathbb{l}en(n') \dot{-} \overline{1}) = t'$	8 T13.51a
14.	$\mathbb{l}en(m) = \mathbb{l}en(n) \wedge \mathbb{l}en(m') = \mathbb{l}en(n')$	8 T13.51a
15.	$(\forall k < \mathbb{l}en(m))[O(v, \mathbb{n}um(y), m, n, k) \vee P(m, n, k) \vee Q(m, n, k) \vee R(v, p, m, n, k) \vee S(v, p, m, n, k)$	8 T13.51a
16.	$(\forall k < \mathbb{l}en(m'))[O(w, \mathbb{n}um(z), m', n', k) \vee P(m', n', k) \vee Q(m', n', k) \vee R(w, p, m', n', k) \vee S(w, p, m', n', k)$	8 T13.51a
17.	$l < \mathbb{l}en(m) \wedge l' < \mathbb{l}en(m')$	A (g (∀I))
18.	$\mathbb{l}en(\mathbb{e}xp(m, l)) \leq \emptyset$	A (g →I)
19.	$\sim[\mathbb{e}xp(m, l) = \mathbb{e}xp(m', l') \to \mathcal{P}^{k,k'}_{l,l'}]$	A (c ∼E)
20.	$\mathbb{e}xp(m, l) > \overline{1}$	9,17 T13.49d
21.	$\mathbb{e}xp(m, l) \not> \overline{1}$	18 T13.45j
22.	$\bot$	20,21 ⊥I
23.	$\mathbb{e}xp(m, l) = \mathbb{e}xp(m', l') \to \mathcal{P}^{k,k'}_{l,l'}$	19-22 ∼E
24.	$\mathbb{l}en(\mathbb{e}xp(m, l)) \leq \emptyset \to (\mathbb{e}xp(m, l) = \mathbb{e}xp(m', l') \to \mathcal{P}^{k,k'}_{l,l'})$	18-23 →I
25.	$(\forall k < \mathbb{l}en(m))(\forall k' < \mathbb{l}en(m'))[\mathbb{l}en(\mathbb{e}xp(m, k)) \leq \emptyset \to (\mathbb{e}xp(m, k) = \mathbb{e}xp(m', k') \to \mathcal{P})]$	17-24 (∀I)
26.	$(\forall k < \mathbb{l}en(m))(\forall k' < \mathbb{l}en(m'))[\mathbb{l}en(\mathbb{e}xp(m, k)) \leq x \to (\mathbb{e}xp(m, k) = \mathbb{e}xp(m', k') \to \mathcal{P})]$	A (g →I)
27.	$l < \mathbb{l}en(m) \wedge l' < \mathbb{l}en(m')$	A (g (∀I))
28.	$\mathbb{l}en(\mathbb{e}xp(m, l) \leq Sx \wedge \mathbb{e}xp(m, l) = \mathbb{e}xp(m', l')$	A (g →I)
29.	$O(v, \mathbb{n}um(y), m, n, l) \vee P(m, n, l) \vee Q(m, n, l) \vee R(v, p, m, n, l) \vee S(v, p, m, n, l)$	15,27 (∀E)
30.	$O(w, \mathbb{n}um(z), m', n', l') \vee P(m', n', l') \vee Q(m', n', l') \vee R(w, p, m', n', l') \vee S(w, p, m', n', l')$	16,27 (∀E)
31.	$O(v, \mathbb{n}um(y), m, n, l)$	A (g 29∨E)
32.	$\mathbb{A}tomic(\mathbb{e}xp(m, l)) \wedge \mathbb{A}tomsub(\mathbb{e}xp(m, l), v, \mathbb{n}um(y), \mathbb{e}xp(n, l))$	31 abv
33.	$O(w, \mathbb{n}um(z), m', n', l')$	A (g 30∨E)
34.	$\mathbb{A}tomic(\mathbb{e}xp(m', l')) \wedge \mathbb{A}tomsub(\mathbb{e}xp(m', l'), w, \mathbb{n}um(z), \mathbb{e}xp(n', l'))$	33 abv
35.	$\mathbb{A}tomsub(\mathbb{e}xp(m, l), w, \mathbb{n}um(z), \mathbb{e}xp(n', l'))$	34,28 =E
36.	$\mathbb{A}tomic(\mathbb{e}xp(n, l)) \wedge \mathbb{A}tomic(\mathbb{e}xp(n', l'))$	2,32,34 T13.50e
37.	$\exists q \exists t \exists t'[\mathbb{A}tomsub(\mathbb{e}xp(m, l), v, \mathbb{n}um(y), t) \wedge \mathbb{A}tomsub(\mathbb{e}xp(m, l), w, \mathbb{n}um(z), t') \wedge$ $\mathbb{A}tomsub(t, w, \mathbb{n}um(z), q) \wedge \mathbb{A}tomsub(t', v, \mathbb{n}um(y), q)]$	1,32 T13.58c
38.	$\mathbb{A}tomsub(\mathbb{e}xp(m, l), v, \mathbb{n}um(y), u) \wedge \mathbb{A}tomsub(\mathbb{e}xp(m, l), w, \mathbb{n}um(z), u')$	A (g 37∃E)
39.	$\mathbb{A}tomsub(u, w, \mathbb{n}um(z), r) \wedge \mathbb{A}tomsub(u', v, \mathbb{n}um(y), r)$	
40.	$\mathbb{e}xp(n, l) = u \wedge \mathbb{e}xp(n', l') = u'$	32,35,38, T13.55j
41.	$\mathbb{A}tomsub(\mathbb{e}xp(n, l), w, \mathbb{n}um(z), r) \wedge \mathbb{A}tomsub(\mathbb{e}xp(n', l'), v, \mathbb{n}um(y), r)$	39,40 =E
42.	$\mathbb{F}subseq(\overline{2}^{\mathbb{e}xp(n,l)}, \overline{2}^{r}, \mathbb{e}xp(n, l), w, \mathbb{n}um(z), r) \wedge \mathbb{F}subseq(\overline{2}^{\mathbb{e}xp(n',l')}, \overline{2}^{r}, \mathbb{e}xp(n', l'), v, \mathbb{n}um(y), r)$	36,41 T13.51e
43.	$\mathcal{P}^{k,k'}_{l,l'}$	42 ∃I
44.	$\mathcal{P}^{k,k'}_{l,l'}$	37,38-43 ∃E
45.	$P(m', n', l') \vee Q(m', n', l') \vee R(w, p, m', n', l') \vee S(w, p, m', n', l')$	A (g 30∨E)
46.	$\sim\mathcal{P}^{k,k'}_{l,l'}$	A (c ∼E)
47.	$\mathbb{A}tomic(\mathbb{e}xp(m', l'))$	32,28 =E
48.	$\sim[P(m', n', l') \vee Q(m', n', l') \vee R(w, p, m', n', l') \vee S(w, p, m', n', l')]$	47 T13.56b
49.	$\bot$	45,48 ⊥I
50.	$\mathcal{P}^{k,k'}_{l,l'}$	46-49 ∼E
51.	$\mathcal{P}^{k,k'}_{l,l'}$	30,33-50 ∨E

Exercise 13.45 T13.58.d

52.	$P(m,n,l)$	A (g 29∨E)
53.	$(\exists i < l)[\mathbb{exp}(m,l) = \mathbb{neg}(\mathbb{exp}(m,i)) \wedge \mathbb{exp}(n,l) = \mathbb{neg}(\mathbb{exp}(n,i))$	52 abv
54.	$h < l$	A (g 53 (∃E))
55.	$\mathbb{exp}(m,l) = \mathbb{neg}(\mathbb{exp}(m,h)) \wedge \mathbb{exp}(n,l) = \mathbb{neg}(\mathbb{exp}(n,h))$	
56.	$P(m',n',l')$	A (g 30∨E)
57.	$(\exists i < l')[\mathbb{exp}(m',l') = \mathbb{neg}(\mathbb{exp}(m',i)) \wedge \mathbb{exp}(n',l') = \mathbb{neg}(\mathbb{exp}(n',i))$	56 abv
58.	$h' < l'$	A (g 57 (∃E))
59.	$\mathbb{exp}(m',l') = \mathbb{neg}(\mathbb{exp}(m',h')) \wedge \mathbb{exp}(n',l') = \mathbb{neg}(\mathbb{exp}(n',h'))$	
60.	$\mathbb{neg}(\mathbb{exp}(m,h)) = \mathbb{neg}(\mathbb{exp}(m',h'))$	28,55,59 =E
61.	$h < \mathbb{len}(m) \wedge h' < \mathbb{len}(m')$	27,54,58 T13.13b
62.	$\mathbb{Wff}(\mathbb{exp}(m,h)) \wedge \mathbb{Wff}(\mathbb{exp}(m',h'))$	9,61 T13.49l
63.	$\mathbb{exp}(m,h) = \mathbb{exp}(m',h')$	60,62 T13.53a
64.	$\mathbb{len}(\mathbb{exp}(m,l)) = \overline{1} + \mathbb{len}(\mathbb{exp}(m,h))$	55 T13.47f
65.	$\mathbb{len}(\mathbb{exp}(m,h)) < \mathbb{len}(\mathbb{exp}(m,l))$	64 T13.13h
66.	$\mathbb{len}(\mathbb{exp}(m,h)) < Sx$	28,65 T13.13c
67.	$\mathbb{len}(\mathbb{exp}(m,h)) \leq x$	66 T13.13n
68.	$\mathbb{exp}(m,h) = \mathbb{exp}(m',h') \to \mathcal{P}^{k,k'}_{h,h'}$	26,61,67 (∀E)
69.	$\mathcal{P}^{k,k'}_{h,h'}$	68,63 →E
70.	$\exists q \exists a \exists b \exists c \exists d[\mathbb{Fsubseq}(a,b,\mathbb{exp}(n,h),w,\mathbb{num}(z),q) \wedge \mathbb{Fsubseq}(c,d,\mathbb{exp}(n',h'),v,\mathbb{num}(y),q)]$	69 abv
71.	$\mathbb{Fsubseq}(a,b,\mathbb{exp}(n,h),w,\mathbb{num}(z),q) \wedge \mathbb{Fsubseq}(c,d,\mathbb{exp}(n',h'),v,\mathbb{num}(y),q)$	A (g 70∃E)
72.	$\mathbb{Fsubseq}(a * \overline{2}^{\mathbb{neg}(\mathbb{exp}(n,h))}, \overline{2}^{\mathbb{neg}(q)}, \mathbb{neg}(\mathbb{exp}(n,h)), w, \mathbb{num}(z), \mathbb{neg}(q)) \wedge$	
	$\mathbb{Fsubseq}(c * \overline{2}^{\mathbb{neg}(\mathbb{exp}(n',h'))}, \overline{2}^{\mathbb{neg}(q)}, \mathbb{neg}(\mathbb{exp}(n',h')), v, \mathbb{num}(y), \mathbb{neg}(q))$	71 T13.51f
73.	$\mathbb{Fsubseq}(a * \overline{2}^{\mathbb{exp}(n,l)}, \overline{2}^{\mathbb{neg}(q)}, \mathbb{exp}(n,l)), w, \mathbb{num}(z), \mathbb{neg}(q)) \wedge$	
	$\mathbb{Fsubseq}(c * \overline{2}^{\mathbb{exp}(n',l')}, \overline{2}^{\mathbb{neg}(q)}, \mathbb{exp}(n',l')), v, \mathbb{num}(y), \mathbb{neg}(q))$	72,55,59 =E
74.	$\mathcal{P}^{k,k'}_{l,l'}$	73 ∃I
75.	$\mathcal{P}^{k,k'}_{l,l'}$	70,71-74 ∃E
76.	$\mathcal{P}^{k,k'}_{l,l'}$	57,58-75 (∃E)
77.	$O(w,\mathbb{num}(z),m',n',l') \vee Q(m',n',l') \vee R(w,p,m',n',l') \vee S(w,p,m',n',l')$	A (g 30∨E)
78.	$\sim\mathcal{P}^{k,k'}_{l,l'}$	A (c ∼E)
79.	$\mathbb{exp}(m',l') = \mathbb{neg}(\mathbb{exp}(m,h))$	55,28 =E
80.	$\sim[O(w,\mathbb{num}(z),m',n',l') \vee Q(m',n',l') \vee R(w,p,m',n',l') \vee S(w,p,m',n',l')]$	79 T13.56c
81.	$\bot$	77,80 ⊥I
82.	$\mathcal{P}^{k,k'}_{l,l'}$	78-81 ∼E
83.	$\mathcal{P}^{k,k'}_{l,l'}$	30,56-82 ∨E
84.	$\mathcal{P}^{k,k'}_{l,l'}$	53,54-83 (∃E)
85.	$Q(m,n,l) \vee R(v,p,m,n,l)$	A (g 29∨E)
86.	$\mathcal{P}^{k,k'}_{l,l'}$	similarly

87.	$S(v,p,m,n,l)$	A (g 29∨E)
88.	$(\exists i<l)(\exists j<p)[\mathbb{V}ar(j)\wedge j=v\wedge \mathbb{exp}(m,l)=\mathbb{unv}(j,\mathbb{exp}(m,i))\wedge \mathbb{exp}(n,l)=\mathbb{exp}(m,l)$	87 abv
89.	$h<l\wedge u<p$	A (g 88 (∃E))
90.	$\mathbb{V}ar(u)\wedge u=v\wedge \mathbb{exp}(m,l)=\mathbb{unv}(u,\mathbb{exp}(m,h))\wedge \mathbb{exp}(n,l)=\mathbb{exp}(m,l)$	
91.	$S(w,p,m',n',l')$	A (g 30∨E)
92.	$(\exists i<l')(\exists j<p)[\mathbb{V}ar(j)\wedge j=w\wedge \mathbb{exp}(m',l')=\mathbb{unv}(j,\mathbb{exp}(m',i))\wedge \mathbb{exp}(n',l')=\mathbb{exp}(m',l')$	91 abv
93.	$h'<l'\wedge u'<p$	A (g 92 (∃E))
94.	$\mathbb{V}ar(u')\wedge u'=w\wedge \mathbb{exp}(m',l')=\mathbb{unv}(u',\mathbb{exp}(m',h'))\wedge \mathbb{exp}(n',l')=\mathbb{exp}(m',l')$	
95.	$h<\mathbb{len}(m)\wedge h'<\mathbb{len}(m')$	27,89,93 T13.13b
96.	$\mathbb{Wff}(\mathbb{exp}(m,h))\wedge \mathbb{Wff}(\mathbb{exp}(m',h')$	9,95 T13.49l
97.	$\exists q\,\mathbb{Formsub}(\mathbb{exp}(m,h),w,\mathbb{num}(z),q)\wedge \exists q\,\mathbb{Formsub}(\mathbb{exp}(m',h'),v,\mathbb{num}(y),q)$	2,96 T13.51k
98.	$\mathbb{Formsub}(\mathbb{exp}(m,h),w,\mathbb{num}(z),q)\wedge \mathbb{Formsub}(\mathbb{exp}(m',h'),v,\mathbb{num}(y),q')$	A (g 97∃E)
99.	$(\exists x\leq X)(\exists y\leq Y)\mathbb{Fsubseq}(x,y,\mathbb{exp}(m,h),w,\mathbb{num}(z),q)\wedge$ $(\exists x\leq X)(\exists y\leq Y)\mathbb{Fsubseq}(x,y,\mathbb{exp}(m',h'),v,\mathbb{num}(y),q')$	98 T13.51b
100.	$\mathbb{Fsubseq}(a,b,\mathbb{exp}(m,h),w,\mathbb{num}(z),q)\wedge \mathbb{Fsubseq}(c,d,\mathbb{exp}(m',h'),v,\mathbb{num}(y),q')$	A (g 99 (∃E))
101.	$\mathbb{unv}(u,\mathbb{exp}(m,h))=\mathbb{unv}(u',\mathbb{exp}(m',h'))$	28,90,94 =E
102.	$\mathbb{exp}(m,h)=\mathbb{exp}(m',h')\wedge u=u'$	101,96,90,94 T13.53b
103.	$u=w\wedge u'=v$	90,94,102 =E
104.	$\mathbb{exp}(n,l)=\mathbb{exp}(n',l')$	28,90,94 =E
105.	$\mathbb{Fsubseq}(a*\bar{2}^{\mathbb{unv}(u,\mathbb{exp}(m,h))},b*\bar{2}^{\mathbb{unv}(u,\mathbb{exp}(m,h))},\mathbb{unv}(u,\mathbb{exp}(m,h)),w,\mathbb{num}(z),\mathbb{unv}(u,\mathbb{exp}(m,h)))$	100,90,103 T13.51i
106.	$\mathbb{Fsubseq}(a*\bar{2}^{\mathbb{exp}(n,l)},b*\bar{2}^{\mathbb{exp}(n,l)},\mathbb{exp}(n,l),w,\mathbb{num}(z),\mathbb{exp}(n,l))$	105,90 =E
107.	$\mathbb{Fsubseq}(c*\bar{2}^{\mathbb{unv}(u',\mathbb{exp}(m',h'))},d*\bar{2}^{\mathbb{unv}(u',\mathbb{exp}(m',h'))},$ $\mathbb{unv}(u',\mathbb{exp}(m',h')),v,\mathbb{num}(y),\mathbb{unv}(u',\mathbb{exp}(m',h')))$	100,94,103 T13.51i
108.	$\mathbb{Fsubseq}(c*\bar{2}^{\mathbb{exp}(n',l')},b*\bar{2}^{\mathbb{exp}(n',l')},\mathbb{exp}(n',l'),v,\mathbb{num}(y),\mathbb{exp}(n',l'))$	107,94 =E
109.	$\mathbb{Fsubseq}(c*\bar{2}^{\mathbb{exp}(n',l')},b*\bar{2}^{\mathbb{exp}(n',l')},\mathbb{exp}(n',l'),v,\mathbb{num}(y),\mathbb{exp}(n,l))$	108,104 =E
110.	$\mathcal{P}^{k,k'}_{l,l'}$	106,109 ∃I
111.	$\mathcal{P}^{k,k'}_{l,l'}$	99,100-110 (∃E)
112.	$\mathcal{P}^{k,k'}_{l,l'}$	97,98-111 ∃E
113.	$\mathcal{P}^{k,k'}_{l,l'}$	92,93-112 (∃E)
114.	$O(w,\mathbb{num}(z),m',n',l')\vee P(m',n',l')\vee Q(m',n',l')\vee R(w,p,m',n',l')$	A (g 30∨E)
115.	$\mathcal{P}^{k,k'}_{l,l'}$	as above
116.	$\mathcal{P}^{k,k'}_{l,l'}$	30,91-115 ∨E
117.	$\mathcal{P}^{k,k'}_{l,l'}$	88,89-116 (∃E)
118.	$\mathcal{P}^{k,k'}_{l,l'}$	29,31-117 ∨E
119.	$\mathbb{len}(\mathbb{exp}(m,l))\leq Sx\rightarrow(\mathbb{exp}(m,l)=\mathbb{exp}(m',l')\rightarrow \mathcal{P}^{k,k'}_{l,l'})$	28-118 →I
120.	$(\forall k<\mathbb{len}(m))(\forall k'<\mathbb{len}(m'))[\mathbb{len}(\mathbb{exp}(m,k))\leq Sx\rightarrow(\mathbb{exp}(m,k)=\mathbb{exp}(m',k')\rightarrow \mathcal{P})]$	27-119 (∀I)
121.	$(\forall k<\mathbb{len}(m))(\forall k'<\mathbb{len}(m'))[\mathbb{len}(\mathbb{exp}(m,k))\leq x\rightarrow(\mathbb{exp}(m,k)=\mathbb{exp}(m',k')\rightarrow \mathcal{P})]\rightarrow$ $(\forall k<\mathbb{len}(m))(\forall k'<\mathbb{len}(m'))[\mathbb{len}(\mathbb{exp}(m,k))\leq Sx\rightarrow(\mathbb{exp}(m,k)=\mathbb{exp}(m',k')\rightarrow \mathcal{P})]$	26-120 →I
122.	$\forall x(\forall k<\mathbb{len}(m))(\forall k'<\mathbb{len}(m'))[\mathbb{len}(\mathbb{exp}(m,k))\leq x\rightarrow(\mathbb{exp}(m,k)=\mathbb{exp}(m',k')\rightarrow \mathcal{P})]$	25,121 IN
123.	$\mathbb{len}(m)\dot{-}\bar{1}<\mathbb{len}(m)\wedge \mathbb{len}(m')\dot{-}\bar{1}<\mathbb{len}(m')$	12 T13.23i
124.	$\mathbb{len}(\mathbb{exp}(m,\mathbb{len}(m)\dot{-}\bar{1}))\leq \mathbb{len}(p)\rightarrow(\mathbb{exp}(m,\mathbb{len}(m)\dot{-}\bar{1})=\mathbb{exp}(m',\mathbb{len}(m')\dot{-}\bar{1})\rightarrow \mathcal{P}^{k,k'}_{\mathbb{len}(m)\dot{-}\bar{1},\mathbb{len}(m')\dot{-}\bar{1}})$	122,123 (∀E)
125.	$\mathbb{len}(p)\leq \mathbb{len}(p)\rightarrow(p=p\rightarrow \mathcal{P}^{k,k'}_{\mathbb{len}(m)\dot{-}\bar{1},\mathbb{len}(m')\dot{-}\bar{1}})$	124,10 =E
126.	$\mathcal{P}^{k,k'}_{\mathbb{len}(m)\dot{-}\bar{1},\mathbb{len}(m')\dot{-}\bar{1}}$	125 =I,→E
127.	$\mathcal{P}^{k,k'}_{\mathbb{len}(n)\dot{-}\bar{1},\mathbb{len}(n')\dot{-}\bar{1}}$	126,14 =E
128.	$\exists q\exists a\exists b\exists c\exists d[\mathbb{Fsubseq}(a,b,t,w,\mathbb{num}(z),q)\wedge \mathbb{Fsubseq}(c,d,t',v,\mathbb{num}(y),q)]$	127,13 =E
129.	$\mathbb{Fsubseq}(a,b,t,w,\mathbb{num}(z),q)\wedge \mathbb{Fsubseq}(c,d,t',v,\mathbb{num}(y),q)$	A (g 128∃E)
130.	$\mathbb{Formsub}(t,w,\mathbb{num}(z),q)\wedge \mathbb{Formsub}(t',v,\mathbb{num}(y),q)$	129 T13.51j
131.	$\mathit{formsub}(t,w,\mathbb{num}(z))=q\wedge \mathit{formsub}(t',v,\mathbb{num}(y))=q$	130,6,2 T13.56h
132.	$\mathit{formsub}(t,w,\mathbb{num}(z))=\mathit{formsub}(t',v,\mathbb{num}(y))$	131 =E
133.	$\mathit{formsub}(\mathit{formsub}(p,v,\mathbb{num}(y)),w,\mathbb{num}(z))=\mathit{formsub}(\mathit{formsub}(p,w,\mathbb{num}(z)),v,\mathbb{num}(y))$	5,132 =E
134.	$\mathit{formsub}(\mathit{formsub}(p,v,\mathbb{num}(y)),w,\mathbb{num}(z))=\mathit{formsub}(\mathit{formsub}(p,w,\mathbb{num}(z)),v,\mathbb{num}(y))$	128,129-133 ∃E
135.	$\mathit{formsub}(\mathit{formsub}(p,v,\mathbb{num}(y)),w,\mathbb{num}(z))=\mathit{formsub}(\mathit{formsub}(p,w,\mathbb{num}(z)),v,\mathbb{num}(y))$	7,8-134 (∃E)
136.	$\mathit{formsub}(\mathit{formsub}(p,v,\mathbb{num}(y)),w,\mathbb{num}(z))=\mathit{formsub}(\mathit{formsub}(p,w,\mathbb{num}(z)),v,\mathbb{num}(y))$	3,4-135 ∃E
137.	$[\mathbb{Wff}(p)\wedge v\neq w]\rightarrow \mathit{formsub}(\mathit{formsub}(p,v,\mathbb{num}(y)),w,\mathbb{num}(z))=\mathit{formsub}(\mathit{formsub}(p,w,\mathbb{num}(z)),v,\mathbb{num}(y))$	1-136 →I

Exercise 13.45 T13.58.d

E13.47. Fill in the parts of T13.61 that are left as "similarly" to to show that PA $\vdash$ $\mathcal{P} \leftrightarrow \mathcal{P}^{\star}$.

T13.61. For any Δ_0 formula $\mathcal{P}$ there is a $\Sigma^{\star}$ formula $\mathcal{P}^{\star}$ such that PA $\vdash \mathcal{P} \leftrightarrow \mathcal{P}^{\star}$.

$\mathcal{P}^{*}$ is $(\forall x < t)\mathcal{B}$. Set $\mathcal{P}^{\star} = \exists z[(t = z)^{\star} \wedge (\forall x \leq z)((x \neq z)^{\star} \rightarrow \mathcal{B}^{\star}]$.

1.	$t = z \leftrightarrow (t = z)^{\star}$	T13.59
2.	$x \neq z \leftrightarrow (x \neq z)^{\star}$	($\sim$) case
3.	$\mathcal{B} \leftrightarrow \mathcal{B}^{\star}$	by assp
4.	$\mathcal{P}^{\star}$	A (g $\leftrightarrow$I)
5.	$\exists z[(t = z)^{\star} \wedge (\forall x \leq z)((x \neq z)^{\star} \rightarrow \mathcal{B}^{\star}(x))]$	4 abv
6.	$\exists z[t = z \wedge (\forall x \leq z)(x \neq z \rightarrow \mathcal{B}(x))]$	5 with 1,2,3
7.	$t = a \wedge (\forall x \leq a)(x \neq a \rightarrow \mathcal{B}(x))$	A (g 6$\exists$E)
8.	$l < t$	A (g ($\forall$I)
9.	$t = a$	7 $\wedge$E
10.	$(\forall x \leq a)(x \neq a \rightarrow \mathcal{B}(x))$	7 $\wedge$E
11.	$(\forall x \leq t)(x \neq t \rightarrow \mathcal{B}(x))$	10,9 =E
12.	$l \leq t$	8 T13.13m
13.	$l \neq t \rightarrow \mathcal{B}(l)$	11,12 ($\forall$E)
14.	$l \neq t$	8 T13.13s
15.	$\mathcal{B}(l)$	13,14 $\rightarrow$E
16.	$(\forall x < t)\mathcal{B}(x)$	8-15 ($\forall$I)
17.	$(\forall x < t)\mathcal{B}(x)$	6,7-16 $\exists$E
18.	$\mathcal{P}^{*}$	abv
19.	$\mathcal{P}^{*}$	A (g $\leftrightarrow$I)
20.	$(\forall x < t)\mathcal{B}(x)$	19 abv
21.	$t = t$	=I
22.	$a \leq t$	A (g ($\forall$I))
23.	$a < t \vee a = t$	22 T13.13m
24.	$a < t$	A (g 23$\vee$E)
25.	$\mathcal{B}(a)$	20,24 ($\forall$E)
26.	$a = t \vee \mathcal{B}(a)$	25 $\vee$I
27.	$a \neq t \rightarrow \mathcal{B}(a)$	26 Impl
28.	$a = t$	A (g 23$\vee$E)
29.	$a = t \vee \mathcal{B}(a)$	28 $\vee$I
30.	$a \neq t \rightarrow \mathcal{B}(a)$	29 Impl
31.	$a \neq t \rightarrow \mathcal{B}(a)$	23,24-27,28-30 $\vee$E
32.	$(\forall x \leq t)(x \neq t \rightarrow \mathcal{B}(x))$	22-31 ($\forall$I)
33.	$t = t \wedge (\forall x \leq t)(x \neq t \rightarrow \mathcal{B}(x))]$	21,32 $\wedge$I
34.	$\exists z[t = z \wedge (\forall x \leq z)(x \neq z \rightarrow \mathcal{B}(x))]$	33 $\exists$I
35.	$\exists z[(t = z)^{\star} \wedge (\forall x \leq z)((x \neq z)^{\star} \rightarrow \mathcal{B}^{\star}(x))]$	34 with 1,2,3
36.	$\mathcal{P}^{\star}$	35 abv
37.	$\mathcal{P}^{\star} \leftrightarrow \mathcal{P}^{*}$	4-18,19-36 $\leftrightarrow$I

E13.49. Provide a demonstration for T13.65.

T13.65. For any i, PA $\vdash$ $\mathbb{sub}_{i+1}(\overline{\ulcorner \mathcal{P} \urcorner}, x_{\mathsf{a}}, x_{\mathsf{y}_1} \ldots x_{\mathsf{y}_n}) = \mathbb{sub}_{i+1}(\overline{\ulcorner \mathcal{P} \urcorner}, x_{\mathsf{y}_1} \ldots x_{\mathsf{y}_i}, x_{\mathsf{a}}, x_{\mathsf{y}_{(i+1)}} \ldots x_{\mathsf{y}_n})$.

Preliminary: If PA $\vdash$ $\mathit{Wff}(p)$, then PA $\vdash$ $\mathit{formsub}(\mathit{formsub}(p, \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}})), \mathit{gvar}(\bar{\mathsf{b}}), \mathit{num}(x_{\mathsf{b}})) = \mathit{formsub}(\mathit{formsub}(p, \mathit{gvar}(\bar{\mathsf{b}}), \mathit{num}(x_{\mathsf{b}})), \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}}))$.

Suppose PA $\vdash$ $\mathit{Wff}(p)$.

(i) Suppose $\mathsf{a} = \mathsf{b}$; then trivially PA $\vdash$ $\mathit{formsub}(\mathit{formsub}(p, \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}})), \mathit{gvar}(\bar{\mathsf{b}}), \mathit{num}(x_{\mathsf{b}})) = \mathit{formsub}(\mathit{formsub}(p, \mathit{gvar}(\bar{\mathsf{b}}), \mathit{num}(x_{\mathsf{b}})), \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}}))$.

(ii) Suppose $\mathsf{a} \neq \mathsf{b}$; then by capture PA $\vdash \bar{\mathsf{a}} \neq \bar{\mathsf{b}}$; so by T13.57g, PA $\vdash \mathit{gvar}(\bar{\mathsf{a}}) \neq \mathit{gvar}(\bar{\mathsf{b}})$; so by T13.58d, PA $\vdash$ $\mathit{formsub}(\mathit{formsub}(p, \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}})), \mathit{gvar}(\bar{\mathsf{b}}), \mathit{num}(x_{\mathsf{b}})) = \mathit{formsub}(\mathit{formsub}(p, \mathit{gvar}(\bar{\mathsf{b}}), \mathit{num}(x_{\mathsf{b}})), \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}}))$.

In either case, then, PA $\vdash$ $\mathit{formsub}(\mathit{formsub}(p, \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}})), \mathit{gvar}(\bar{\mathsf{b}}), \mathit{num}(x_{\mathsf{b}})) = \mathit{formsub}(\mathit{formsub}(p, \mathit{gvar}(\bar{\mathsf{b}}), \mathit{num}(x_{\mathsf{b}})), \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}}))$.

Basis: PA $\vdash \mathit{sub}_1(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{a}}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_n}) = \mathit{sub}_1(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{a}}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_n})$.

Assp: For any i, PA $\vdash \mathit{sub}_{i+1}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{a}}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_n}) = \mathit{sub}_{i+1}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_i}, x_{\mathsf{a}}, x_{\mathsf{y}_{i+1}} \dots x_{\mathsf{y}_n})$

Show: PA $\vdash \mathit{sub}_{i+2}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{a}}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_n}) = \mathit{sub}_{i+2}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_{i+1}}, x_{\mathsf{a}}, x_{\mathsf{y}_{i+2}} \dots x_{\mathsf{y}_n})$

1.	$\mathit{Wff}(\mathit{sub}_i(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_i}, x_{\mathsf{a}}, x_{\mathsf{y}_{i+1}} \dots x_{\mathsf{y}_n}))$	T13.63
2.	$\mathit{sub}_{i+2}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_{i+1}}, x_{\mathsf{a}}, x_{\mathsf{y}_{i+2}} \dots x_{\mathsf{y}_n})$	
3.	$= \mathit{formsub}[\mathit{sub}_{i+1}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_{i+1}}, x_{\mathsf{a}}, x_{\mathsf{y}_{i+2}} \dots x_{\mathsf{y}_n}), \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}})]$	def
4.	$= \mathit{formsub}[\mathit{formsub}(\mathit{sub}_i(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_i}, x_{\mathsf{y}_{i+1}}, x_{\mathsf{a}}, x_{\mathsf{y}_{i+2}} \dots x_{\mathsf{y}_n}), \mathit{gvar}(\bar{\mathsf{y}}_{i+1}), \mathit{num}(x_{\mathsf{y}_{i+1}})), \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}})]$	def
5.	$= \mathit{formsub}[\mathit{formsub}(\mathit{sub}_i(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_i}, x_{\mathsf{a}}, x_{\mathsf{y}_{i+1}} \dots x_{\mathsf{y}_n}), \mathit{gvar}(\bar{\mathsf{y}}_{i+1}), \mathit{num}(x_{\mathsf{y}_{i+1}})), \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}})]$	T13.64
6.	$= \mathit{formsub}[\mathit{formsub}(\mathit{sub}_i(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_i}, x_{\mathsf{a}}, x_{\mathsf{y}_{i+1}} \dots x_{\mathsf{y}_n}), \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}})), \mathit{gvar}(\bar{\mathsf{y}}_{i+1}), \mathit{num}(x_{\mathsf{y}_{i+1}})]$	1,5 prelm
7.	$= \mathit{formsub}[\mathit{formsub}(\mathit{sub}_{i+1}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_i}, x_{\mathsf{a}}, x_{\mathsf{y}_{i+1}} \dots x_{\mathsf{y}_n}), \mathit{gvar}(\bar{\mathsf{y}}_{i+1}), \mathit{num}(x_{\mathsf{y}_{i+1}})]$	def
8.	$= \mathit{formsub}[\mathit{formsub}(\mathit{sub}_{i+1}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{a}}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_n})), \mathit{gvar}(\bar{\mathsf{y}}_{i+1}), \mathit{num}(x_{i+1})]$	assp
9.	$= \mathit{sub}_{i+2}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{a}}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_n})$	def

Indct: For any i, PA $\vdash \mathit{sub}_{i+1}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{a}}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_n}) = \mathit{sub}_{i+1}(\overline{\ulcorner\mathcal{P}\urcorner}, x_{\mathsf{y}_1} \dots x_{\mathsf{y}_i}, x_{\mathsf{a}}, x_{\mathsf{y}_{i+1}} \dots x_{\mathsf{y}_n})$

E13.50. Provide a demonstration for T13.67

T13.67. If the variables of $\vec{y}$ and $\vec{z}$ are ordered by their subscripts and $\vec{y}$ and $\vec{z}$ are the same except that $\vec{z}$ includes some variables not in $\vec{y}$ (and so not free in $\mathcal{P}$), then PA $\vdash \mathit{sub}(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}) = \mathit{sub}(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{z})$.

Suppose $S(i.j)$ is as in the hint to T13.67.

Basis: PA $\vdash \mathit{sub}_0(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}) = \overline{\ulcorner\mathcal{P}\urcorner} = \mathit{sub}_0(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{z})$.

Assp: For any $i.j$ in the sequence, PA $\vdash \mathit{sub}_i(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}) = \mathit{sub}_j(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{z})$

Show: For $S(i.j) = k.l$, PA $\vdash \mathit{sub}_k(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}) = \mathit{sub}_l(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{z})$. Either (i) $\mathsf{y}_{\mathsf{S}i} = \mathsf{z}_{\mathsf{S}j}$ or (ii) $\mathsf{y}_{\mathsf{S}i} \neq \mathsf{z}_{\mathsf{S}j}$.

(i) $\mathsf{y}_{\mathsf{S}i} = \mathsf{z}_{\mathsf{S}j}$ so that $k.l = Si.Sj$. Let $\mathsf{a} = \mathsf{y}_{\mathsf{S}i} = \mathsf{z}_{\mathsf{S}j}$.

1.	$\mathit{sub}_{Si}(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}) = \mathit{formsub}(\mathit{sub}_i(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}), \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}}))$	by def
2.	$\mathit{formsub}(\mathit{sub}_i(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}), \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}})) = \mathit{formsub}(\mathit{sub}_j(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{z}), \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}}))$	by assp
3.	$\mathit{formsub}(\mathit{sub}_j(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{z}), \mathit{gvar}(\bar{\mathsf{a}}), \mathit{num}(x_{\mathsf{a}})) = \mathit{sub}_{Sj}(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{z})$	by def
4.	$\mathit{sub}_{Si}(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{y}) = \mathit{sub}_{Sj}(\overline{\ulcorner\mathcal{P}\urcorner}, \vec{z})$	1,2,3 =E

So PA $\vdash sub_k(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{y}) = sub_l(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{z})$.

(ii) $\mathsf{y}_{\mathsf{Si}} \neq \mathsf{z}_{\mathsf{Sj}}$ so that $k.l = i.Sj$. Let $\mathsf{a} = \mathsf{z}_{\mathsf{Sj}}$; in this case, x_{a} is not in $\vec{y}$ and so not free in $\mathscr{P}$.

1.	$sub_{Sj}(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{z}) = sub_j(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{z})$	T13.66
2.	$sub_j(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{z}) = sub_i(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{y})$	by assp
3.	$sub_i(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{y}) = sub_{Sj}(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{z})$	1,2 =E

So PA $\vdash sub_k(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{y}) = sub_l(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{z})$.

Indct: For any $i.j$ in the sequence PA $\vdash sub_i(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{y}) = sub_j(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{z})$; and PA $\vdash sub_n(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{y}) = sub_m(\overline{\ulcorner \mathscr{P} \urcorner}, \vec{z})$.

Chapter Fourteen

You are ready to do these on your own!

Bibliography

Benacerraf, P., and H. Putnam. *Philosophy of Mathematics: Selected Readings*. Cambridge: Cambridge University Press, 1983, 2nd edition.

Bergmann, M., J. Moor, and J. Nelson. *The Logic Book*. New York: McGraw-Hill, 2004, 4th edition.

Berto, Francesco. *There's Something About Gödel: The Complete Guide to the Incompleteness Theorem*. Oxford: Wiley-Blackwell, 2009.

Black, Robert. "Proving Church's Thesis." *Philosophia Mathematica* 8 (2000): 244–258.

Boolos, G., J. Burgess, and R. Jeffrey. *Computability and Logic*. Cambridge: Cambridge University Press, 2002, 4th edition.

Boolos, George. *The Logic of Provability*. Cambridge: Cambridge University Press, 1993.

Cederblom, J, and D Paulsen. *Critical Reasoning*. Belmont: Wadsworth, 2005, 6th edition.

Church, Alonzo. "An Unsolvable Problem of Elementary Number Theory." *American Journal of Mathematics* 58 (1936): 345–363.

Cooper, B. *Computability Theory*. Boca Raton: Chapman & Hall/CRC Mathematics, 2004.

Dennett, Daniel, editor. *The Philosopher's Lexicon*. 1987. URL http://www.blackwellpublishing.com/lexicon/.

Drake, F., and Singh D. *Intermediate Set Theory*. Chichester, England: John Wiley & Sons, 1996.

Earman, J, and J. Norton. “Forever is a Day: Supertasks in Pitowsky and Malament-Hogarth Spacetimes.” *Philosophy of Science* 60 (1993): 22–42.

Earman, John. *Bangs, Crunches, Whimpers, and Shrieks: Singularities and Acausalities in Relativistic Spacetimes*. New York: Oxford University Press, 1995.

Enderton, H. *Elements of Set Theory*. Boston: Academic Press, Inc., 1977.

Feferman, et al., editors. *Gödel’s Collected Works: Vol I*. New York: Oxford University Press, 1986.

Fisher, A. *Formal Number Theory and Computability*. Oxford: Clarendon Press, 1982.

George, A, and D. Velleman. *Philosophies of Mathematics*. Blackwell Publishers, 2002.

Gödel, K. “On Formally Undecidable Propositions of *Principia Mathematica* and Related Systems I.” In *Collected Works, Vol. I: Publications 1929-1936*, Oxford: Oxford University Press, 1986, 144–95.

Gödel, Kurt. “Die Vollständigkeit der Axiome des Logischen Funktionenkalküls.” *Monatshefte für Mathematik und Physik* 37 (1930): 349–360.

von Heijenoort, editor. *From Frege to Gödel*. Cambridge: Harvard University Press, 1967.

Henkin, Leon. “The Completeness of the First-Order Functional Calculus.” *Journal of Symbolic Logic* 14 (1949): 159–166.

———. “A Problem Concerning Provability.” *Journal of Symbolic Logic* 17 (1952): 160.

Hodges, W. *A Shorter Model Theory*. Cambridge: Cambridge University Press, 1997.

Hogarth, Mark. “Does General Relativity Allow an Observer To View an Eternity In a Finite Time?” *Foundations of Physics Letters* 173–181.

Kolmogorov, and Uspenskii. “On the Definition of an Algorithm.” *American Mathematical Society Translations* 29 (1963): 217–245.

Kripke, Saul. *Wittgenstein on Rules and Private Language: An Elementary Exposition*. Cambridge, Mass.: Harvard University Press, 1982.

Manzano, María. *Extensions of First Order Logic*. Cambridge: Cambridge University Press, 1996.

———. *Model Theory*. Oxford: Clarendon Press, 1999.

Marcus, and McEvoy. *An Historical Introduction to the Philosophy of Mathematics*. London: Bloomsbury Publishing, 2016.

Mendelson, Elliott. *Introduction to Mathematical Logic*. New York: Chapman and Hall, 1997, 4th edition.

Pietroski, Paul. "Logical Form." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, 2009. Fall, 2009 edition. URL http://plato.stanford.edu/archives/fall2009/entries/logical-form/.

Plantinga, Alvin. *God, Freedom, and Evil*. Grand Rapids: Eerdmans, 1977.

Pohlers, W. *Proof Theory*. Berlin: Springer-Verlag, 1989.

Priest, Graham. *Non-Classical Logics*. Cambridge: Cambridge University Press, 2001.

Putnam, Hilary. *Reason, Truth and History*. Cambridge: Cambridge University Pres, 1981.

Raatikainen, Panu. "Gödel's Incompleteness Theorems." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, 2015. Spring 2015 edition. URL http://plato.stanford.edu/archives/spr2015/entries/goedel-incompleteness/.

Robinson, R. "An Essentially Undecidable Axiom System." *Proceedings of the International Congress of Mathematics* 1 (1950): 729–730.

Rosser, Barkley. "Extensions of Some Theorems of Gödel and Church." *Journal of Symbolic Logic* 1 (1936): 230–235.

Rowling, J.K. *Harry Potter and the Prisoner of Azkaban*. New York: Scholastic Inc., 1999.

Roy, Tony. "Natural Derivations for Priest, *An Introduction to Non-Classical Logic*." *The Australasian Journal of Logic* 47–192. URL http://ojs.victoria.ac.nz/ajl/article/view/1779.

———. "Modality." In *The Continuum Companion to Metaphysics*, London: Continuum Publishing Group, 2012, 46–66.

Russell, B. "On Denoting." *Mind* 14.

Shapiro, S. *Foundations Without Foundationalism: A Case for Second Order Logic*. Oxford: Clarendon Press, 1991.

———. *Thinking About Mathematics: The Philosophy of Mathematics*. Oxford: Oxford University Press, 2000.

———. "Philosophy of Mathematics and Its Logic: Introduction." In *The Oxford Handbook of Philosophy of Mathematics and Logic*, edited by S. Shapiro, Oxford: Oxford University Press, 2005, 3–28.

Smith, Peter. "Squeezing Arguments." *Analysis* 71 (2011): 22–30.

———. *An Introduction to Gödel's Theorems*. Cambridge: Cambridge University Press, 2013a, second edition.

———. "Teach Yourself Logic: A Study Guide.", 2013b. URL http://www.logicmatters.net/tyl/.

Szabo, M., editor. *The Collected Papers of Gerhard Gentzen*. Amsterdam: North-Holland, 1969.

Takeuti, G. *Proof Theory*. Amsterdam: North-Holland, 1975.

Tourlakis, George. *Lectures in Logic and Set Theory, Volume I: Mathematical Logic*. Cambridge: Cambridge University Press, 2003.

Turing, Alan. "On Computable Numbers, With an Application to the *Entscheidungsproblem*." *Proceedings of the London Mathematical Society* 42 (1936): 230–265.

Wang, Hao. "The axiomatization of Arithmetic." *Journal of Symbolic Logic* 22 (1957): 145–158.

Index

expressive completeness, 428