STUDIES IN LOGIC
AND
THE FOUNDATIONS OF MATHEMATICS

VOLUME 90

NORTH-HOLLAND PUBLISHING COMPANY—AMSTERDAM · NEW YORK · OXFORD

HANDBOOK OF

MATHEMATICAL LOGIC

EDITED BY

JON BARWISE
University of Wisconsin, Madison

WITH THE COOPERATION OF

H. J. KEISLER
K. KUNEN
Y. N. MOSCHOVAKIS
A. S. TROELSTRA

1977

NORTH-HOLLAND PUBLISHING COMPANY—AMSTERDAM · NEW YORK · OXFORD

Library of Congress Catalog Card Number 76–26032
North-Holland ISBN for this Series 0 7204 2200 0
North-Holland ISBN for this Volume 0 7204 2285 X

PUBLISHERS:
NORTH-HOLLAND PUBLISHING COMPANY
AMSTERDAM · NEW YORK · OXFORD

SOLE DISTRIBUTORS FOR THE U.S.A. AND CANADA:
ELSEVIER NORTH-HOLLAND, INC.
52 VANDERBILT AVENUE, NEW YORK, N.Y. 10017

Library of Congrees Cataloging in Publication Data
Main entry under title:
Handbook of mathematical logic.

(Studies in logic and the foundations of mathematics; 90)
Includes index.
1. Logic, Symbolic and mathematical. I. Barwise, Jon. II. Keisler, H. Jerome. III. Series.
QA9.H32 511'.3 76–26032
ISBN 0–7204–2285–X

PRINTED IN THE NETHERLANDS

Table of Contents

D.2

Proof Theory: Some Applications of Cut-Elimination

HELMUT SCHWICHTENBERG

Contents

HANDBOOK OF MATHEMATICAL LOGIC
Edited by J. Barwise

1. Introduction

1.1. Proof theory began with *Hilbert's Program*, which called for elementary consistency proofs for formalized mathematical theories **S**. Equivalently (under quite general conditions discussed in Chapter D.1) this program can be formulated as follows. Given a formalization in **S** of an abstract proof of an elementary assertion φ (example: proof of $n + m = m + n$, *n, m variables* for natural numbers, in an axiomatic set theory), can one always conclude from this by elementary means that φ is true? Or more precisely, can one give an elementary proof of the schema

$$(*) \qquad \exists x \, \mathrm{Der}_{\mathbf{S}}(x, \ulcorner\varphi\urcorner) \to \varphi,$$

where $\mathrm{Der}_{\mathbf{S}}(\cdot,\cdot)$ is a canonical representation of the derivation predicate for **S** and φ ranges over formulas corresponding to elementary assertions? By the well-known second incompleteness theorem of Gödel, discussed in Chapter D.1, (*) is underivable in **S**, provided **S** is sufficiently strong. Now since one would expect that a strong theory **S** contains at least formalizations of all "elementary" proofs, one may fairly say that this refutes Hilbert's Program in its original form. However, one can also try to extend the (originally quite vague) conception of an elementary proof and then look for such a proof of (*) not formalizable in **S**; in fact, this was Hilbert's reaction to Gödel's result (cf. the introduction to HILBERT and BERNAYS [1934]). We shall not deal here with contributions to Hilbert's Program along these lines (for this, cf. e.g. SCHÜTTE [1960]), but rather concentrate on some less delicate questions which are derived from and closely related to Hilbert's Program.

1.1.1. A theory **S** is called *conservative* over a theory **T** if any formula of L(**T**) (the language of **T**) derivable in **S** is already derivable in **T**. Note that this would be a corollary of the derivability of (*) in **T** (under quite general conditions). There are numerous important and nontrivial examples of theories **S** conservative over a subtheory **T**. Some of these are discussed in Chapters D.4 and D.5. We shall give here a very simple example and show that first-order logic is conservative over its part which uses formulas of a restricted complexity only (cf. Section 2.8).

1.1.2. The schema (*) (now taken with arbitrary φ) provides, generally, a proper extension of **S**. However, (*) has a metamathematical character and its mathematical strength is difficult to judge. So one might ask for an *equivalent formulation of* (*) *having a clear mathematical meaning*. This question has been answered for a wide variety of theories **S**. We shall confine ourselves here to a basic example, namely (classical) arithmetic **Z**, and prove that in this case (a version of) (*) is equivalent to the schema of transfinite induction up to ε_0.

1.2. Our second starting point is a question which only more recently came to the attention of proof theorists (cf. KREISEL [1958]): "*What more do we know if we have proved a theorem by restricted means than if we merely know that it is true*?" Again we shall confine ourselves to the discussion of a basic example, where the "restricted means" are those formalized in arithmetic **Z**. We shall obtain a complete answer to the above question, due to KREISEL [1952]. For some subsystems of analysis one can also get satisfactory answers to questions of the type above; for this we refer the reader to Chapter D.4.

1.3. From a more technical point of view, we survey some elementary applications of a basic technique in proof theory: the method of cut-elimination. This method is due to Gentzen and was later developed particularly by Schütte and Tait (cf. SCHÜTTE [1960] and TAIT [1968]). Other techniques frequently used in proof theory are adequately covered in other chapters in this volume. Especially important is the method of functional interpretation due to GÖDEL [1958], which is treated in Chapter D.5.

1.4. We now give a more detailed account of the content of the present chapter.

In Section 2 we prove the *Cut-Elimination Theorem* for first-order logic; as a corollary we obtain the conservative extension result mentioned above. The proof of this basic Cut-Elimination Theorem is set up in such a way that it can be easily generalized to many other cases where a cut-elimination argument is applied, in particular to those treated here.

In Section 3 we discuss for arithmetic **Z** the provability and unprovability of initial cases of transfinite induction. The result (due to GENTZEN [1943]) is well known: Given a natural well-ordering $<$ of order type ε_0, then with respect to $<$ transfinite induction is provable up to any ordinal $< \varepsilon_0$, but not up to ε_0 itself.

The underivability in **Z** of transfinite induction up to ε_0 will also follow from Gödel's second incompleteness theorem together with the fact that transfinite induction up to ε_0 suffices to prove the reflection principle for **Z** and hence the consistency of **Z** (cf. Section 5). Here we give a direct proof of this underivability result, using a cut-elimination argument. Technically, this provides an easy and convincing example of the usefulness of infinite derivations and the strength of the cut-elimination method when applied to infinite derivations.

In Section 4 we take up the question of Section 1.2. We first consider the special case of $\forall\exists$-formulas. Suppose $\forall n\, \exists m\, \varphi(n, m)$ with $\varphi(n, m)$ quantifier-free is derivable in **Z**. We shall show that then we can find a function F satisfying $\forall n\, \varphi(n, F(n))$ which has a somewhat limited rate of growth: F can be defined by primitive recursive operations and α-recursions for $\alpha < \varepsilon_0$.

We then turn to the general case of arbitrary **Z**-formulas. At first sight a generalization of the result for $\forall\exists$-formulas seems to be impossible, since $\forall n\, \exists m\, \forall k\, (T(n, n, k) \rightarrow T(n, n, m))$ is derivable (in classical logic and hence) in **Z**, but there is no recursive function F satisfying $\forall n\, \forall k\, (T(n, n, k) \rightarrow T(n, n, F(n)))$ (this would contradict the recursive undecidability of $\exists k\, T(n, n, k)$; T is Kleene's T-predicate). However, there is such a generalization, the so-called No-Counterexample-Interpretation due to KREISEL [1952]. To explain it let us first consider a formula of the above form, i.e. $\psi :\equiv \forall n\, \exists m\, \forall k\, \varphi(n, m, k)$ with $\varphi(n, m, k)$ quantifier-free. Its negation is equivalent to $\exists n\, \forall m\, \exists k \neg \varphi(n, m, k)$ and hence (using the axiom of choice) also to $\exists n, f\, \forall m \neg \varphi(n, m, f(m))$; such n, f can be considered as providing a counterexample to the given formula ψ. So a way to express the content of ψ is to say that there is no such counterexample, i.e. that for any n, f we have $\exists m\, \varphi(n, m, f(m))$ (this formula is the Herbrand normal form of ψ), i.e. that there is a functional F such that $\forall n, f\, \varphi(n, F(n, f), f(F(n, f)))$ holds. Now the additional information we obtain from the fact that ψ is derivable in **Z** is that such a functional F can be found which again has a somewhat limited complexity: F can be defined by primitive recursive operations (in the sense of KLEENE [1959]) and α-recursions for some $\alpha < \varepsilon_0$, or — as we shall say — F is $< \varepsilon_0$-recursive.

Generally, let ψ be an arbitrary **Z**-formula and let $\psi_{\mathrm{H}} \equiv \exists \boldsymbol{m}\, \psi^{\mathrm{H}}(\boldsymbol{n}, \boldsymbol{m}, \boldsymbol{f})$ be its Herbrand normal form which is derivable in **Z** iff ψ is. (We use $\boldsymbol{f}$ for finite sequences of function variables and $\boldsymbol{n}, \boldsymbol{m}$ for finite sequences of number variables.) The result then is that from the derivability of ψ in **Z** we can conclude that there are $< \varepsilon_0$-recursive functionals $\boldsymbol{F}$ satisfying $\forall \boldsymbol{n}, \boldsymbol{f}\, \psi^{\mathrm{H}}(\boldsymbol{n}, \boldsymbol{F}(\boldsymbol{n}, \boldsymbol{f}), \boldsymbol{f})$. We also prove that this result is the best possible in the sense that no smaller class of functionals suffices.

The proof involves a new point: it makes use of the fact that the cut-elimination procedure for infinite derivations is an effective operation.

More precisely, we show that for a natural coding of infinite derivations the cut-elimination procedure is given by a primitive recursive function.

In Section 5 we come back to the question asked in Section 1.1.2 and prove the result stated there (which is due to KREISEL and LÉVY [1968]). The proof is a formalization of the argument in Section 4, i.e. cut-elimination for codes of infinite derivations.

Acknowledgements: Parts of the present chapter are based on other sources, in particular TAIT [1968] (for the proof of the Cut-Elimination Theorem in Section 2) and SCHÜTTE [1960] (for the proof in Section 3 of the underivability of transfinite induction up to ε_0 in $\mathbf{Z}$). Also I want to thank S. Feferman, G. Kreisel, R. Statman and A.S. Troelstra for many helpful comments and suggestions; in particular, the idea to prove the No-Counterexample-Interpretation by means of a cut-elimination argument is due to Kreisel.

2. Cut-elimination for first-order logic

We prove this basic Cut-Elimination Theorem by a method due to Gentzen which is central for our later work: nearly all the results mentioned in the introduction will be obtained by generalizations of this method. Technically we shall follow TAIT [1968] quite closely, but with one exeption: we shall avoid infinite formulas throughout (and later use infinite derivations only where they seem to be essential).

2.1. We use the ordinary *language* of first-order logic, for simplicity in the following version: formulas are built up from atomic and negated atomic formulas by means of $\wedge$, $\vee$, $\forall x$, $\exists x$. The negation $\neg\varphi$ of a formula φ is *defined* to be the formula obtained from φ by

(i) putting a $\neg$ in front of any atomic formula,
(ii) replacing $\wedge$, $\vee$, $\forall x$, $\exists x$ by $\vee$, $\wedge$, $\exists x$, $\forall x$, respectively, and
(iii) dropping double negations.

This treatment of negation is possible since we assume classical logic throughout. Note that $\neg\neg\varphi$ is identical with φ, $\neg\neg\varphi\equiv\varphi$. As usual, we define $\varphi\to\psi$ to be $\neg\varphi\vee\psi$ and $\varphi\leftrightarrow\psi$ to be $(\varphi\to\psi)\wedge(\psi\to\varphi)$. Let $|\varphi|$ (the *length* of φ) be defined as follows.

(i) $|\varphi|=|\neg\varphi|=0$, for φ atomic.
(ii) $|\varphi\wedge\psi|=|\varphi\vee\psi|=\sup(|\varphi|,|\psi|)+1$.
(iii) $|\forall x\,\varphi(x)|=|\exists x\,\varphi(x)|=|\varphi(x)|+1$.

Note that $|\neg\varphi|=|\varphi|$.

2.2. Logical rules

We shall derive finite sets of formulas, denoted by $\Gamma, \Delta, \Lambda, \Gamma(a), \ldots$. The intended meaning of Γ is the disjunction of all formulas in Γ. We use the notation

$$\Gamma, \varphi \quad \text{for } \Gamma \cup \{\varphi\},$$
$$\Gamma, \Delta \quad \text{for } \Gamma \cup \Delta.$$

(i) *Normal rules*:

$$\mathrm{A} \qquad \Gamma, \varphi, \neg\varphi \quad \text{if } \varphi \text{ is atomic.}$$

$$\wedge \quad \frac{\Gamma, \varphi \qquad \Gamma, \psi}{\Gamma, \varphi \wedge \psi}.$$

$$\vee_0 \quad \frac{\Gamma, \varphi}{\Gamma, \varphi \vee \psi}, \qquad \vee_1 \quad \frac{\Gamma, \psi}{\Gamma, \varphi \vee \psi}.$$

$$\forall \quad \frac{\Gamma, \varphi(x)}{\Gamma, \forall x\, \varphi(x)} \quad \begin{array}{l}\text{if } x \text{ is not free in } \Gamma \\ (x \text{ is called eigenvariable of } \forall).\end{array}$$

$$\exists \quad \frac{\Gamma, \varphi(s)}{\Gamma, \exists x\, \varphi(x)}.$$

(ii) *Cut-rule*:

$$\text{Cut} \quad \frac{\Gamma, \varphi \qquad \Gamma, \neg\varphi}{\Gamma}.$$

The *principal formulas* (p.f.) in A are φ and $\neg\varphi$. In $\wedge$, $\vee_i$, $\forall$ and $\exists$ the p.f. is $\varphi \wedge \psi$, $\varphi \vee \psi$, $\forall x\, \varphi(x)$ and $\exists x\, \varphi(x)$, respectively. Cut has no p.f. The *minor formula* (m.f.) in the premiss Γ, φ of $\wedge$ is φ, and in the premiss Γ, ψ of $\wedge$ it is ψ. In the premiss of $\vee_0$, $\vee_1$, $\forall$ and $\exists$ the m.f. is φ, ψ, $\varphi(x)$ and $\varphi(s)$, respectively. The m.f. in the premiss Γ, φ of Cut is φ, and in the premiss Γ, $\neg\varphi$ of Cut it is $\neg\varphi$. So any inference has the form

$$(*) \qquad \frac{\Gamma, \varphi_i \quad \text{for all } i < k}{\Gamma, \Delta}$$

$(0 \leq k \leq 2)$, where Δ consists of the p.f. and φ_i is the m.f. in the i-th premiss. The formulas in Γ are called *side formulas* (s.f.) of (*).

Derivations are built up in tree form, as usual. More precisely, they are defined by the following induction. Consider an inference (*) as above and assume that derivations d_i of its premisses Γ, φ_i are given. Then $d = ((d_i)_{i<k}, (\varphi_i)_{i<k}, \Delta, \Gamma)$ is a derivation of the conclusion Γ, Δ of (*). The

inference considered is called the *last inference* of d. The d_i are called *direct subderivations* of d. We write $d \vdash \Gamma$ if d is a derivation of Γ, and $\vdash \Gamma$ if there is a derivation of Γ.

The *length* $|d|$ of a derivation d is inductively defined to be $\sup_{i<k}(|d_i|+1)$ if the d_i, $i<k$, are the direct subderivations of d. Hence $|d|=0$ if d has no direct subderivations. The *cut-rank* $\rho(d)$ of a derivation d is also defined by induction: Let d_i, $i<k$, be the direct subderivations of d. If the last inference of d is a cut with m.f. φ and $\neg\varphi$ let $\rho(d) := \sup(|\varphi|+1, \sup_{i<k}\rho(d_i))$. Otherwise, let $\rho(d) := \sup_{i<k}\rho(d_i)$. Note that $\rho(d)=0$ iff d is cut-free.

It is convenient to use the notions of free and bound occurrences of variables in derivations. A free occurrence of a variable x inside an occurrence of a formula in a derivation d is called *bound in d* if "below" that occurrence x is used as an eigenvariable of an inference $\forall$; otherwise this occurrence of x is called *free in d*. We use the notation $d, d(x), \ldots$ for derivations where it is understood that there may be other free variables different from those actually shown.

2.3. Let d, Γ be obtained from a derivation d by adding Γ to the side formulas of all inferences in d. It is trivial to see that d, Γ is again a derivation provided no variable free in Γ is bound in d. The latter condition can always be assumed to hold if we identify derivations which differ only by a change of bound variables. Hence we have:

2.3.1. Weakening Lemma. *If $d \vdash \Delta$, then $d, \Gamma \vdash \Gamma, \Delta$ with $|d,\Gamma| = |d|$ and $\rho(d,\Gamma)=\rho(d)$.*

2.4. Let $d(s)$ denote the result of substituting s for all free occurrences of x in $d(x)$ (note that some changes of bound variables in $d(x)$ may be necessary). Then we obviously have

2.4.1. Substitution Lemma. *If $d(x) \vdash \Gamma(x)$, then $d(s) \vdash \Gamma(s)$ with $|d(s)| = |d(x)|$ and $\rho(d(s)) = \rho(d(x))$.*

2.5. Inversion Lemma. (i) *If $d \vdash \Gamma, \varphi_0 \wedge \varphi_1$, then we can find $d_i \vdash \Gamma, \varphi_i$ $(i=0,1)$ with $|d_i| \le |d|$ and $\rho(d_i) \le \rho(d)$.*

(ii) *If $d \vdash \Gamma, \forall x\,\psi(x)$, then we can find $d_0 \vdash \Gamma, \psi(x)$ with $|d_0| \le |d|$ and $\rho(d_0) \le \rho(d)$.*

Proof. The proofs of (i) and (ii) are almost identical, both by induction on

$|d|$. We restrict ourselves to (ii). Let φ be $\forall x\,\psi(x)$. We can assume $\varphi \notin \Gamma$, for otherwise the result follows by weakening, taking $d, \psi(x)$.

Case 1: φ is not a p.f. in the last inference of d. Then this inference has the form

$$\frac{\Lambda, \varphi, \psi_j \quad \text{for all } j < k}{\Lambda, \varphi, \Delta}$$

with m.f. ψ_j, p.f. Δ and s.f. Λ, φ, and $\Gamma = \Lambda, \Delta$. By the induction hypothesis $\vdash \Lambda, \psi(x), \psi_j$ for all $j < k$, with length $<|d|$ and cut-rank $\leq \rho(d)$. The result follows by the inference

$$\frac{\Lambda, \psi(x), \psi_j \quad \text{for all } j < k}{\Lambda, \psi(x), \Delta}$$

Case 2: φ is a p.f. in the last inference of d. We can assume that φ is a s.f. in the last inference of d, replacing d by d, φ if necessary. So that inference is of the form

$$\frac{\Gamma, \varphi, \psi(x)}{\Gamma, \varphi}$$

with m.f. $\psi(x)$, p.f. φ and s.f. Γ, φ. By the inductive hypothesis $\vdash \Gamma, \psi(x)$, with length $<|d|$ and cut-rank $\leq \rho(d)$. This completes the proof. □

2.6. Reduction Lemma. *Let $d_0 \vdash \Gamma, \varphi$ and $d_1 \vdash \Delta, \neg\varphi$, both with cut-rank $\rho(d_i) \leq |\varphi|$. Then we can find $d \vdash \Gamma, \Delta$ with $|d| \leq |d_0| + |d_1|$ and $\rho(d) \leq |\varphi|$.*

Of course we could derive Γ, Δ by an application of the cut-rule, but the resulting derivation would then have cut-rank $|\varphi| + 1$.

Proof. The proof is by induction on $|d_0| + |d_1|$. Since $|\varphi| = |\neg\varphi|$ and $\neg\neg\varphi \equiv \varphi$, the lemma is symmetric with respect to the two given derivations.

Case 1: Either φ is not a p.f. in the last inference of d_0 or else $\neg\varphi$ is not a p.f. in the last inference of d_1. By symmetry we can assume the former. Then the last inference of d_0 is of the form

$$\frac{\Lambda, \varphi, \psi_i \quad \text{for all } i < k}{\Lambda, \varphi, \Theta}$$

with m.f. ψ_i, p.f. Θ and s.f. Λ, φ, and $\Gamma = \Lambda, \Theta$. By the induction hypothesis $\vdash \Lambda, \Delta, \psi_i$ for all $i < k$ with length $<|d_0| + |d_1|$ and cut-rank $\leq |\varphi|$. The result then follows by the inference

$$\frac{\Lambda, \Delta, \psi_i \quad \text{for all } i < k}{\Lambda, \Delta, \Theta}$$

Case 2: φ is a p.f. in the last inference of d_0, and $\neg\varphi$ is a p.f. in the last inference of d_1.

Case 2.1.: φ or $\neg\varphi$ is atomic. Then the last (and only) inferences of d_0 and d_1 are instances of the rule A and hence Γ, Δ is also an instance of the rule A.

Case 2.2.: φ or $\neg\varphi$ is a disjunction $\varphi_0 \vee \varphi_1$. By symmetry we can assume the former, so $\neg\varphi$ is $\neg\varphi_0 \wedge \neg\varphi_1$. We can assume that φ is a s.f. of the last inference of d_0, replacing d_0 by d_0, φ if necessary. So that inference is of the form

$$\frac{\Gamma, \varphi, \varphi_i}{\Gamma, \varphi}.$$

By the induction hypothesis $\vdash \Gamma, \Delta, \varphi_i$ with length $< |d_0| + |d_1|$ and cut-rank $\leq |\varphi|$. By the Inversion Lemma $\vdash \Delta, \neg\varphi_i$ with length $\leq |d_1| < |d_0| + |d_1|$ and cut-rank $\leq |\varphi|$. The result follows by an application of the cut rule.

Case 2.3.: φ or $\neg\varphi$ is of the form $\exists x\,\psi(x)$. Again we can assume the former (so $\neg\varphi$ is $\forall x \neg\psi(x)$), and also that φ is a s.f. of the last inference of d_0. So that inference is of the form

$$\frac{\Gamma, \varphi, \psi(s)}{\Gamma, \varphi}.$$

By the induction hypothesis $\vdash \Gamma, \Delta, \psi(s)$ with length $< |d_0| + |d_1|$ and cut-rank $\leq |\varphi|$. By the Inversion Lemma $\vdash \Delta, \neg\psi(a)$ with length $\leq |d_1|$ and cut-rank $\leq |\varphi|$. By the Substitution Lemma $\vdash \Delta, \neg\psi(s)$ also with length $\leq |d_1|$ and cut-rank $\leq |\varphi|$. The result follows by an application of the cut rule. $\square$

2.7. Cut-Elimination Theorem. *If $d \vdash \Gamma$ and $\rho(d) > 0$, then we can find $d' \vdash \Gamma$ with $\rho(d') < \rho(d)$ and $|d'| \leq 2^{|d|}$.*

Proof. The proof is by induction on $|d|$. We may assume that the last inference of d is a cut

$$\frac{\Gamma, \varphi \qquad \Gamma, \neg\varphi}{\Gamma}$$

with $|\varphi| + 1 = \rho(d)$, for otherwise the result follows by the induction hypothesis (making use of the fact that our rules all have finitely many premisses). So assume this. Let $d_0 \vdash \Gamma, \varphi$ and $d_1 \vdash \Gamma, \neg\varphi$ be the direct subderivations of d. By the induction hypothesis we have $d'_0 \vdash \Gamma, \varphi$ and $d'_1 \vdash \Gamma, \neg\varphi$, both with cut-rank $\rho(d'_i) \leq |\varphi|$ and length $|d'_i| \leq 2^{|d_i|}$. The result then follows by the Reduction Lemma, since $|d'_0| + |d'_1| \leq 2^{\sup(|d_0|, |d_1|)+1} = 2^{|d|}$. $\square$

Let $2_0^\xi = \xi$, $2_{k+1}^\xi = 2^{2_k^\xi}$.

2.7.1. COROLLARY. *If $d \vdash \Gamma$, then we can find a cut-free $d^* \vdash \Gamma$ with $|d^*| \leq 2_{\rho(d)}^{|d|}$.*

2.8. In this and the next subsection we prove two important consequences of the Cut-Elimination Theorem.

Define the relation "ψ is a subformula of φ" to be the smallest transitive and reflexive relation with the properties

(i) φ_0, φ_1 are subformulas of $\varphi_0 \wedge \varphi_1$, $\varphi_0 \vee \varphi_1$, and

(ii) $\varphi(s)$ is a subformula of $\forall x\, \varphi(x)$, $\exists x\, \varphi(x)$.

The following is obvious.

2.8.1. SUBFORMULA PROPERTY. *Let d be a cut-free derivation of Γ. Then any formula occurring in d is a subformula of one of the formulas in Γ.*

Hence from the Cut-Elimination Theorem we can conclude that *for any $d \vdash \Gamma$ we can find $d^* \vdash \Gamma$ containing only subformulas of formulas in Γ.*

2.9. HERBRAND'S THEOREM. *Let $d \vdash \exists x\, \varphi(x)$ with $\varphi(x)$ quantifier-free. Then we can find terms $s_0, \ldots, s_{n-1}$ and a derivation $d_0 \vdash \varphi(s_0), \cdots, \varphi(s_{n-1})$.*

PROOF. We can assume that d is cut-free. Hence by the subformula property any instance of the rule $\exists$ in d has the p.f. $\exists x\, \varphi(x)$. Let $s_0, \ldots, s_{n-1}$ be all the terms such that $\varphi(s_i)$ is the m.f. of such an instance of $\exists$. Now add $\varphi(s_0), \ldots, \varphi(s_{n-1})$ to the side formulas of any inference in d, and cancel all occurrences of $\exists x\, \varphi(x)$ in d. It is easy to see that the resulting object is (essentially) the required derivation. $\square$

3. Transfinite induction

In this and the following sections we shall deal with (classical) arithmetic **Z**. We begin with a discussion of transfinite induction, particularly of the question which initial cases of transfinite induction are derivable in **Z**. By an extension of the cut-elimination argument in Section 2 we shall show that transfinite induction up to ε_0 is underivable in **Z**. This provides a precise bound, since it is easy to see that for any $\alpha < \varepsilon_0$ transfinite induction up to α is provable in **Z** (cf. SCHÜTTE [1960] or Chapter D.4).

3.1. To fix notation we first describe our version of *arithmetic* **Z**, which is in fact usual arithmetic plus free set and function variables. So we have number variables, set variables and for any $n > 0$ variables for n-place functions (countably many of each sort). They are denoted by k, m, n, p, by X, Y, Z, and by f, g, h, respectively. The *terms* of **Z** are built up from a constant 0 (for the number 0) and the number variables by means of the function symbols S (for successor), $+, \cdot$ and the function variables. The *atomic formulas* of **Z** are of the form $s = t$, $s < t$ or $s \in X$, where s, t are terms and X is a set variable. The *formulas* are built up from these as usual, using quantification on number variables only.

The *axioms* of **Z** are the usual axioms for $0, S, <$ $(\neg n < 0, m < Sn \leftrightarrow (m < n \vee m = n))$, $+, \cdot$ and equality, and the induction schema

$$\varphi(0) \wedge \forall n\, (\varphi(n) \rightarrow \varphi(Sn)) \rightarrow \forall n\, \varphi(n),$$

where $\varphi(n)$ is an arbitrary formula of the language, possibly containing additional variables. The theorems of **Z** are those derivable from the axioms by classical logic.

The various sets and functions one wants to talk about in arithmetic can be introduced in *definitional* (and hence conservative) *extensions of* **Z**. There is one type of these we are particularly interested in, the so-called recursive extensions of **Z**. Such an extension occurs if

(i) we introduce a new set symbol M with the defining axiom $n \in M \leftrightarrow \varphi(n)$ where $\varphi(n)$ is quantifier-free, or

(ii) if we have derived $\exists m\, \varphi(\boldsymbol{n}, m, \boldsymbol{f})$ with $\varphi(\boldsymbol{n}, m, \boldsymbol{f})$ quantifier-free and then introduce a new functional symbol F with the defining axioms

$$\varphi(\boldsymbol{n}, F(\boldsymbol{n}, \boldsymbol{f}), \boldsymbol{f}), \qquad m < F(\boldsymbol{n}, \boldsymbol{f}) \rightarrow \neg\varphi(\boldsymbol{n}, m, \boldsymbol{f}).$$

Z$'$ is called a *recursive extension* of **Z** if it is obtained from **Z** by a finite sequence of definitional extensions of this sort. Recursive extensions of **Z** will also be denoted by **Z**.

One can show that any primitive recursive function can be introduced in a recursive extension of **Z** (cf. SHOENFIELD [1967]). Conversely, any such function is certainly recursive. We will determine in Section 4 exactly which recursive functionals can be introduced in recursive extensions of **Z**.

Obviously **Z** is a conservative extension of its part without function variables, or without set variables, or without both. These subsystems will also be denoted by **Z**.

3.2. Natural well-orderings of order type ε_0

As is well known, the ordinals $< \varepsilon_0$ can be built up from 0 by means of the ordinal functions $\alpha + \beta$ and ω^α. This build-up is unique if one uses the Cantor normal form (cf. BACHMANN [1955]). Hence ordinals $< \varepsilon_0$ may be considered as finite objects and so they can be coded by natural numbers. It is easy to choose these codes in such a way that

(i) the coding provides a bijective mapping $\alpha \mapsto \ulcorner\alpha\urcorner$ from the ordinals $< \varepsilon_0$ onto the natural numbers,

(ii) the relation $n \prec m$ corresponding to the less-than relation between ordinals $< \varepsilon_0$ is primitive recursive, and

(iii) the number-theoretic functions corresponding to the ordinal functions $\alpha + \beta$, ω^α and their inverses are primitive recursive.

Obviously, any two codings with the properties (i)–(iii) will be primitive recursive isomorphic. Any of the corresponding $\prec$-relations between natural numbers is called a *natural well-ordering of order type* ε_0. We choose one of them, denote it by $\prec$ and fix it for the following. We write $n \preccurlyeq m$ for $n \prec m \vee n = m$.

3.3. Let $\mathrm{Prog}(X)$ ("X is progressive") be the formula $\forall n\, (\forall m\, (m \prec n \to m \in X) \to n \in X)$. The axiom of transfinite induction up to ε_0 is

$$\mathrm{TI}_{\varepsilon_0}(X) \qquad \mathrm{Prog}(X) \to \forall n\, (n \in X).$$

Here $m \prec n$ stands for $\langle m, n\rangle \in M$ where $\langle\cdot,\cdot\rangle$ is one of the usual primitive recursive pairing functions and M is a symbol for the primitive recursive set of pair-numbers $\langle m, n\rangle$ such that $m \prec n$ holds.

3.3.1. THEOREM (GENTZEN [1943]). $\mathrm{TI}_{\varepsilon_0}(X)$ *is underivable in arithmetic* **Z**.

The proof of this theorem will cover the rest of Section 3. In outline, it proceeds as follows. We first embed **Z** in a "semi-formal" system $\mathbf{Z}_\infty$, where induction is replaced by a rule with infinitely many premisses, the so-called *ω-rule*:

$$\frac{\Gamma, \Delta(\bar{\imath}_0, \ldots, \bar{\imath}_{k-1}) \quad \text{for all } i_0, \ldots, i_{k-1} < \omega}{\Gamma, \Delta(n_0, \ldots, n_{k-1})}$$

where $\bar{\imath}$ is the i-th numeral, i.e. $S^i 0$. By a slight extension of the argument in Section 2 we will obtain a Cut-Elimination Theorem for $\mathbf{Z}_\infty$ which gives a bound on the length of the cut-free derivation in terms of length and cut-rank of the derivation we started with. In particular, if we started with (the image in $\mathbf{Z}_\infty$ of) a $\mathbf{Z}$-derivation, then this length will be $< \varepsilon_0$. We will then extend $\mathbf{Z}$ by yet another infinitary rule, the so-called *progression rule* introduced by Schütte:

$$\text{Prog} \qquad \frac{\Gamma, \bar{\imath} \in X \quad \text{for all } i < j}{\Gamma, s \in X}$$

where s is a closed term with numerical value j. It is easy to see that in $\mathbf{Z}_\infty + \text{Prog}$ one can give a derivation of $\text{Prog}(X)$, and that this derivation has a finite length. Again a Cut-Elimination Theorem with the same ordinal bounds holds for $\mathbf{Z}_\infty + \text{Prog}$. Now assume that $\text{TI}_{\varepsilon_0}(X)$ is derivable in $\mathbf{Z}$. Since $\text{Prog}(X)$ is derivable in $\mathbf{Z}_\infty + \text{Prog}$ with finite length, we can conclude that the formula $n \in X$ (with variable n) is cut-free derivable in $\mathbf{Z}_\infty + \text{Prog}$ with a length $\alpha < \varepsilon_0$. Hence also $\overline{\ulcorner \alpha + 1 \urcorner} \in X$ is derivable in $\mathbf{Z}_\infty + \text{Prog}$ with length α. But this is a contradiction, since from the form of the rules of $\mathbf{Z}_\infty + \text{Prog}$ it follows immediately that any cut-free derivation of $\overline{\ulcorner \beta \urcorner} \in X$ has length β.

3.4. Cut-Elimination for $\mathbf{Z}_\infty$

3.4.1. Description of $\mathbf{Z}_\infty$

The *language* of $\mathbf{Z}_\infty$ is the same as for $\mathbf{Z}$; we can assume here that we do not have function variables. For notions connected with derivations we use the same notation as in Section 2.

A finite set Δ of formulas is called a $\mathbf{Z}_\infty$*-axiom* if Δ consists of atomic or negated atomic formulas without number variables such that $\bigvee \Delta$ (the disjunction of the formulas in Δ) is a tautological consequence of substitution instances of the quantifier-free axioms of $\mathbf{Z}$.

The *normal rules* of $\mathbf{Z}_\infty$ are

$$\text{A} \qquad \Gamma, \Delta \quad \text{if } \Delta \text{ is a } \mathbf{Z}_\infty\text{-axiom},$$

the rules $\wedge$, $\vee_0$, $\vee_1$, $\forall$, $\exists$ listed in Section 2 and the ω-rule

$$\omega \qquad \frac{\Gamma, \Delta(\bar{\boldsymbol{\imath}}) \quad \text{for all } \boldsymbol{i}}{\Gamma, \Delta(\boldsymbol{n})}$$

Furthermore, we have in $\mathbf{Z}_\infty$ the *cut-rule* Cut stated in Section 2.

Note that in the ω-rule we allow $\boldsymbol{n}$ to be empty. Also it is allowed that in $\Delta(\boldsymbol{n})$ no variable of $\boldsymbol{n}$ actually has a free occurrence. In these cases the conclusion of the ω-rule is the same as its premiss(es). Such an instance of the ω-rule is called *improper.*

The *prinicipal formulas* (p.f.) in A are all formulas in Δ. In the ω-rule the p.f. are all formulas in $\Delta(\boldsymbol{n})$. The *minor formulas* (m.f.) in the i-th premiss of the ω-rule are all formulas in $\Delta(\bar{\imath})$. So any inference now has the form

$$(*)\qquad \frac{\Gamma, \Delta_i \quad \text{for all } i < \alpha}{\Gamma, \Delta}$$

$(0 \leq \alpha \leq \omega)$, where Δ consists of the p.f. and Δ_i consists of the m.f. in the i-th premiss. The formulas in Γ are again called *side formulas* (s.f.) of $(*)$.

Derivations will now be infinite; they are defined as in Section 2.2. (In the case of the ω-rule we have to add information about the variables $\boldsymbol{n}$.) Also the other notions introduced in Section 2.2, particularly the *length* $|d|$ and the *cut-rank* $\rho(d)$ of a derivation d carry over with the same definitions. Note that $|d|$ is now a countable ordinal, and $\rho(d) \leq \omega$. We restrict ourselves throughout to derivations with only finitely many free and bound variables. The set of variables free in a derivation d is denoted by $\mathrm{Var}(d)$.

3.4.2. EMBEDDING LEMMA. *For any φ derivable in* $\mathbf{Z}$ *we have a* $\mathbf{Z}_\infty$-*derivation $d \vdash \varphi$ of length $|d| < \omega \cdot 2$ and cut-rank $\rho(d) < \omega$.*

This is easy to see for the axioms of $\mathbf{Z}$ (for induction one has to use the ω-rule), and it is trivially preserved by the logical rules.

3.4.3. We now extend the proof given in Section 2 of the Cut-Elimination Theorem for first-order logic to $\mathbf{Z}_\infty$. Obviously we have:

WEAKENING LEMMA. *If $d \vdash \Delta$, then $d, \Gamma \vdash \Gamma, \Delta$ with $|d, \Gamma| = |d|$, $\rho(d, \Gamma) = \rho(d)$ and $\mathrm{Var}(d, \Gamma) = \mathrm{Var}(d) \cup V$, where V is the set of variables free in Γ.*

Note that any closed term s has a numerical value i, and $s = \bar{\imath}$ is a $\mathbf{Z}_\infty$-axiom.

EVALUATION LEMMA. *Let s, t be closed terms, both with the same value i. If $d \vdash \Gamma(s)$, then we can find $d_0 \vdash \Gamma(t)$ with $|d_0| = |d|$, $\rho(d_0) = \rho(d)$ and $\mathrm{Var}(d_0) = \mathrm{Var}(d)$.*

It is easily seen that this holds for instances of the rule A and is preserved by the other rules.

SUBSTITUTION LEMMA. *If* $d(n) \vdash \Gamma(n)$, *then* $d(s) \vdash \Gamma(s)$ *with* $|d(s)| \leq |d(n)|$, $\rho(d(s)) \leq \rho(d(n))$ *and* $\mathrm{Var}(d(s)) \subseteq (\mathrm{Var}(d) - \{n\}) \cup V$, *where* V *is the set of variables free in* s.

The proof is by induction on $|d(n)|$. The only case which requires some argument is that in which the last inference of $d(n)$ is an instance of the ω-rule of the form

$$\frac{\Gamma(n, \boldsymbol{m}, \boldsymbol{p}), \Delta(\bar{\imath}, \bar{\jmath}, \boldsymbol{p}) \text{ for all } i, j}{\Gamma(n, \boldsymbol{m}, \boldsymbol{p}), \Delta(n, \boldsymbol{m}, \boldsymbol{p})}$$

where $\boldsymbol{m}$, $\boldsymbol{p}$ include all variables free in $s = s(\boldsymbol{m}, \boldsymbol{p})$ (but $\Gamma(n, \boldsymbol{m}, \boldsymbol{p})$, $\Delta(n, \boldsymbol{m}, \boldsymbol{p})$ may contain free variables other than those shown). By the induction hypothesis,

$$\vdash \Gamma(\bar{\imath}, \boldsymbol{m}, \bar{\boldsymbol{k}}), \Delta(\bar{\imath}, \bar{\jmath}, \bar{\boldsymbol{k}}) \quad \text{for all } i, j, \boldsymbol{k}$$

with length $< |d(n)|$ and cut-rank $\leq \rho(d(n))$. From some of these derivations we obtain by the Evaluation Lemma,

$$\vdash \Gamma(s(\bar{\jmath}, \bar{\boldsymbol{k}}), \boldsymbol{m}, \bar{\boldsymbol{k}}), \Delta(s(\bar{\jmath}, \bar{\boldsymbol{k}}), \bar{\jmath}, \bar{\boldsymbol{k}}) \quad \text{for all } j, \boldsymbol{k}$$

without raising length or cut-rank. The result follows by an application of the ω-rule.

INVERSION LEMMA. (i) *If* $d \vdash \Gamma, \varphi_0 \wedge \varphi_1$, *then we can find* $d_i \vdash \Gamma, \varphi_i$ $(i = 0, 1)$ *with* $|d_i| \leq |d|$, $\rho(d_i) \leq \rho(d)$ *and* $\mathrm{Var}(d_i) \subseteq \mathrm{Var}(d)$.

(ii) *If* $d \vdash \Gamma, \forall n \psi(n)$, *then we can find* $d_0 \vdash \Gamma, \psi(n)$ *with* $|d_0| \leq |d|$, $\rho(d_0) \leq \rho(d)$ *and* $\mathrm{Var}(d_0) \subseteq \mathrm{Var}(d) \cup \{n\}$.

The proofs of (i) and (ii) are almost identical, both by induction on $|d|$. We restrict ourselves to (ii). The only subcase not similar to 2.5 is where the last inference of d is an instance of the ω-rule. Then that inference is of the form

$$\frac{\Lambda(\boldsymbol{m}), \varphi(\boldsymbol{m}), \Delta(\bar{\imath}), \varphi(\bar{\imath}) \quad \text{for all } \boldsymbol{i}}{\Lambda(\boldsymbol{m}), \Delta(\boldsymbol{m}), \varphi(\boldsymbol{m})}$$

with m.f. $\Delta(\bar{\imath}), \varphi(\bar{\imath})$, p.f. $\Delta(\boldsymbol{m}), \varphi(\boldsymbol{m})$ and s.f. $\Lambda(\boldsymbol{m}), \varphi(\boldsymbol{m})$, and $\Gamma \equiv \Lambda(\boldsymbol{m})$, $\Delta(\boldsymbol{m})$, $\varphi \equiv \varphi(\boldsymbol{m})$. By two applications of the induction hypothesis

$$\vdash \Lambda(\boldsymbol{m}), \psi(n, \boldsymbol{m}), \Delta(\bar{\imath}), \psi(n, \bar{\imath}) \quad \text{for all } \boldsymbol{i}$$

with length $< |d|$ and cut-rank $\leq \rho(d)$. The result follows by an application of the ω-rule.

REDUCTION LEMMA. *Let* $d_0 \vdash \Gamma, \varphi$ *and* $d_1 \vdash \Delta, \neg\varphi$, *both with cut-rank* $\rho(d_i) \leq |\varphi|$. *Then we can find* $d \vdash \Delta, \Gamma$ *with* $\rho(d) \leq |\varphi|$, $|d| \leq |d_0| \# |d_1|$ *and* $\mathrm{Var}(d) \subseteq \mathrm{Var}(d_0) \cup \mathrm{Var}(d_1)$.

Here $\#$ denotes the natural (or Hessenberg) sum of ordinals (cf. BACHMANN [1955]); $\#$ is strictly monotonic in both arguments.

The proof is by induction on $|d_0| \# |d_1|$. Again the only (sub-) case not similar to 2.6 is where φ is a p.f. in the last inference of d_0, and $\neg\varphi$ is a p.f. in the last inference of d_1, and the last inference of d_0 or d_1 is an instance of the ω-rule. By symmetry we can assume the former. We can also assume that φ is a s.f. of the last inference of d_0, replacing d_0 by d_0, φ if necessary. So that inference is of the form

$$\frac{\Lambda(\boldsymbol{m}),\ \varphi(\boldsymbol{m}),\ \Theta(\bar{\imath}),\ \varphi(\bar{\imath}) \quad \text{for all } i}{\Lambda(\boldsymbol{m}),\ \Theta(\boldsymbol{m}),\ \varphi(\boldsymbol{m})}$$

with m.f. $\Theta(\bar{\imath}), \varphi(\bar{\imath})$, p.f. $\Theta(\boldsymbol{m}), \varphi(\boldsymbol{m})$ and s.f. $\Lambda(\boldsymbol{m}), \varphi(\boldsymbol{m})$, and $\Gamma \equiv \Lambda(\boldsymbol{m}), \Theta(\boldsymbol{m})$, $\varphi \equiv \varphi(\boldsymbol{m})$. By the Substitution Lemma $\vdash \Gamma(\bar{\imath}), \varphi(\bar{\imath})$ for all i, with length $< |d_0|$ and cut-rank $\leq |\varphi|$, and also $\vdash \Delta(\bar{\imath}), \neg\varphi(\bar{\imath})$ for all i, with length $\leq |d_1|$ and cut-rank $\leq |\varphi|$. By the induction hypothesis $\vdash \Gamma(\bar{\imath}), \Delta(\bar{\imath})$ for all i with length $< |d_0| \# |d_1|$ and cut-rank $\leq |\varphi|$. The result follows by an application of the ω-rule. This completes the proof of the Reduction Lemma. $\square$

Let $\varepsilon(\alpha)$ be the α-th ε-number.

CUT-ELIMINATION THEOREM. (i) *If* $d \vdash \Gamma$ *with* $\rho(d) = \zeta + 1$, *then we can find* $d' \vdash \Gamma$ *with* $\rho(d') \leq \zeta$, $|d'| \leq 2^{|d|}$ *and* $\mathrm{Var}(d') \subseteq \mathrm{Var}(d)$.

(ii) *If* $d \vdash \Gamma$ *with* $\rho(d) = \omega$, *then we can find* $d' \vdash \Gamma$ *with* $\rho(d') = 0$, $|d'| \leq \varepsilon(|d|)$ *and* $\mathrm{Var}(d') \subseteq \mathrm{Var}(d)$.

PROOF. (i) As in 2.7.

(ii) By induction on $|d|$. We may assume that the last inference of d is a cut

$$\frac{\Gamma, \varphi \qquad \Gamma, \neg\varphi}{\Gamma}$$

for otherwise the result follows by the induction hypothesis. So assume this. By the induction hypothesis we have $d_0 \vdash \Gamma, \varphi$ and $d_1 \vdash \Gamma, \neg\varphi$, both cut-free and with length $|d_i| < \varepsilon(|d|)$. The result then follows by applying (i) $|\varphi|$ times. $\square$

COROLLARY. *If $d \vdash \Gamma$, then we can find a cut-free $d^* \vdash \Gamma$ with $|d^*| \leq 2^{|d|}_{\rho(d)}$ if $\rho(d) < \omega$, and $|d^*| \leq \varepsilon(|d|)$ if $\rho(d) = \omega$.*

3.5. Cut-Elimination for $\mathbf{Z}_\infty$ + Prog

We add to $\mathbf{Z}_\infty$ the following *progression rule*:

$$\text{Prog} \qquad \frac{\Gamma, \bar{\imath} \in X \quad \text{for all } i < j}{\Gamma, s \in X} \qquad \text{for } s \text{ a closed term with value } j.$$

The p.f. in Prog is $s \in X$, and the m.f. in the i-th premiss is $\bar{\imath} \in X$. Now all the definitions, lemmas and proofs of Section 3.4 carry over almost word for word. Only part of the proof of the Reduction Lemma must be extended slightly: So let φ be a p.f. in the last inference of d_0, $\neg\varphi$ be a p.f. in the last inference of d_1 and φ be atomic. Let further the last inference in d_0 be Prog and in d_1 be A. We can assume that φ is a s.f. in the last inference of d_0; hence it has the form

$$\frac{\Gamma, s \in X, \bar{\imath} \in X \quad \text{for all } i < j}{\Gamma, s \in X} \qquad s \text{ a closed term with value } j.$$

The last (and only) inference of d_1 is an instance $\Delta, \neg(s \in X)$ of the rule A. Now it is easy to see that then either

(i) $t \in X$ is in Δ for some closed t with value j, or

(ii) Δ is already an instance of the rule A.

In the latter case the result follows by weakening. In the former case we have by the induction hypothesis $\vdash \Gamma, \Delta, t \in X, \bar{\imath} \in X$ for all $i < j$, with length $< |d_0|$ and cut-rank 0. The result follows by an application of the rule Prog.

3.6. Underivability of $\mathrm{TI}_{\varepsilon_0}(X)$ in Z

3.6.1. LEMMA. *In $\mathbf{Z}_\infty$ + Prog we can derive Prog(X) with finite length and cut-rank.*

We give an informal argument which can be easily transformed into a derivation in $\mathbf{Z}_\infty$ + Prog.

Recall $\mathrm{Prog}(X) \equiv \forall n\, (\forall m\, (m < n \to m \in X) \to n \in X)$. For any $i < j$ we have $\forall m\, (m < \bar{\jmath} \to m \in X) \to \bar{\imath} \in X$. Hence by the progression rule $\forall m\, (m < \bar{\jmath} \to m \in X) \to \bar{\jmath} \in X$. Hence Prog($X$) by the ω-rule.

3.6.2. LEMMA. *Let d be a cut-free derivation in $\mathbf{Z}_\infty$ + Prog of $\overline{\ulcorner\beta_1\urcorner} \in X, \ldots, \overline{\ulcorner\beta_k\urcorner} \in X$. Then d has length $\geq \min(\beta_1, \ldots, \beta_k)$.*

This follows immediately from the form of the rules of $\mathbf{Z}_\infty + \text{Prog}$; use induction on $|d|$. The whole derivation must consist of instances of the rule Prog and of improper instances of the ω-rule.

3.6.3. Now assume $\text{TI}_{\varepsilon_0}(X)$ is derivable in $\mathbf{Z}$. Recall that $\text{TI}_{\varepsilon_0}(X) \equiv \text{Prog}(X) \rightarrow \forall n\,(n \in X)$. By 3.4.2 and 3.6.1 we then have a $\mathbf{Z}_\infty + \text{Prog}$-derivation of $n \in X$ (with variable n) with length $< \omega \cdot 2$ and finite cut-rank. By the Cut-Elimination Theorem for $\mathbf{Z}_\infty + \text{Prog}$ we obtain a cut-free derivation of $n \in X$ in $\mathbf{Z}_\infty + \text{Prog}$ with length $\alpha < \varepsilon_0$. Hence by the Substitution Lemma we should also have a cut-free derivation of $\overline{\ulcorner \alpha + 1 \urcorner} \in X$ in $\mathbf{Z}_\infty + \text{Prog}$ with length α. This contradicts 3.6.2.

4. Bounds from proofs of existential theorems

We now take up the question "What more do we know if we have proved a theorem by restricted means than if we merely know that it is true?" As before, we restrict ourselves to arithmetic $\mathbf{Z}$, where one can get a satisfactory answer; cf. Section 1.4 for a summary of the results. Using the terminology of Section 3.1 we can also summarize the results as follows. We show that a functional F of level ≤ 2 (i.e. with number and function arguments) can be introduced in a recursive extension of $\mathbf{Z}$ iff F is $< \varepsilon_0$-recursive, i.e. F can be defined by the (Kleene) primitive recursive operations and α-recursions for $\alpha < \varepsilon_0$.

4.1. $< \varepsilon_0$-recursive functionals

A functional F of level ≤ 2 is called *primitive recursive in Kleene's sense* iff it can be defined by means of schemata (i)–(v) below. Here $\boldsymbol{n} = n_0, \ldots, n_{p-1}$ is a sequence of number variables and $\boldsymbol{f} = f_0, \ldots, f_{q-1}$ is a sequence of function variables.

(i) (Identity) $F(\boldsymbol{n}, \boldsymbol{f}) = n_i$ (for $i < p$).

(ii) (Function application) $F(\boldsymbol{n}, \boldsymbol{f}) = f_i(n_{j_0}, \ldots, n_{j_{k-1}})$ (for $i < q$ and $j_0, \ldots, j_{k-1} < p$).

(iii) (Successor) $F(\boldsymbol{n}, \boldsymbol{f}) = n_i + 1$ (for $i < p$).

(iv) (Substitution) $F(\boldsymbol{n}, \boldsymbol{f}) = G(H_0(\boldsymbol{n}, \boldsymbol{f}), \ldots, H_{k-1}(\boldsymbol{n}, \boldsymbol{f}),\ K_0(\cdot, \boldsymbol{n}, \boldsymbol{f}), \ldots, K_{l-1}(\cdot, \boldsymbol{n}, \boldsymbol{f}))$.

(v) (Primitive recursion) $F(0, \boldsymbol{m}, \boldsymbol{f}) = G(\boldsymbol{m}, \boldsymbol{f})$, $F(n+1, \boldsymbol{m}, \boldsymbol{f}) = H(F(n, \boldsymbol{m}, \boldsymbol{f}), n, \boldsymbol{m}, \boldsymbol{f})$.

In (iv), $K_j(\cdot, \boldsymbol{n}, \boldsymbol{f})$ means $\lambda x K_j(x, \boldsymbol{n}, \boldsymbol{f})$. Note that $F(\boldsymbol{n}, \boldsymbol{f})$ is always a natural number.

Let α be an ordinal $< \varepsilon_0$ and let $\prec$ be our natural well-ordering of order type ε_0 (cf. Section 3.2). By α-recursion we mean the following definition schema.

(vi) (α-Recursion) For $n \prec \ulcorner \alpha \urcorner$,

$$F(n, m, f) = G(n, m, (F \upharpoonright n)(\cdot, m, f), f)$$

where

$$(F \upharpoonright n)(i, m, f) := \begin{cases} F(i, m, f) & \text{if } i \prec n, \\ 0 & \text{otherwise.} \end{cases}$$

For $\ulcorner \alpha \urcorner \preccurlyeq n$, $F(n, m, f) := 0$.

A functional F of level ≤ 2 is called $< \varepsilon_0$*-recursive* iff F can be defined by the primitive recursive operations (i)–(v) and α-recursions for $\alpha < \varepsilon_0$. The class of $< \varepsilon_0$-recursive functionals of level ≤ 2 is denoted by $\mathrm{Rec}_{<\varepsilon_0}$.

4.2. THEOREM (KREISEL [1952]). *If $\forall n\, \exists m\, \varphi(n, m)$ is derivable in* **Z** *with $\varphi(n, m)$ quantifier-free and without free variables other than those shown, then we can find a function $F \in \mathrm{Rec}_{<\varepsilon_0}$ such that $\forall n\, \varphi(n, F(n))$ holds.*

4.2.1. We first sketch the proof. So let a **Z**-derivation of $\forall n\, \exists m\, \varphi(n, m)$ or equivalently of $\exists m\, \varphi(n, m)$ be given. As in 3.4.2 we can transform this **Z**-derivation into an infinite $\mathbf{Z}_\infty$-derivation $d(n) \vdash \exists m\, \varphi(n, m)$ with length $|d(n)| < \omega \cdot 2$ and finite cut-rank. Furthermore, as in 3.4.3, we can transform $d(n)$ into a cut-free $\mathbf{Z}_\infty$-derivation $d^*(n) \vdash \exists m\, \varphi(n, m)$ with length $|d^*(n)| < \varepsilon_0$. By the Substitution Lemma in 3.4.3 we obtain for any i a $\mathbf{Z}_\infty$-derivation $d^*(\bar{\imath}) \vdash \exists m\, \varphi(\bar{\imath}, m)$ also with length $|d^*(\bar{\imath})| < \varepsilon_0$. Now from the form of the normal rules of $\mathbf{Z}_\infty$ it is clear that $d^*(\bar{\imath})$ contains only subformulas (cf. 2.8) of $\exists m\, \varphi(\bar{\imath}, m)$. We may assume that $d^*(\bar{\imath})$ contains no free variable (otherwise substitute 0 for any variable free in $d^*(\bar{\imath})$). Hence all instances of the ω-rule in $d^*(\bar{\imath})$ must be improper (cf. 3.4.1) and so we may as well cancel them. This yields a cut-free $d^{**} \vdash \exists m\, \varphi(\bar{\imath}, m)$ which does not involve the ω-rule. To d^{**} we can apply the same argument as in the proof of Herbrand's Theorem 2.9 and obtain closed terms $s_0, \dots, s_{k-1}$ and a derivation of $\varphi(\bar{\imath}, s_0), \dots, \varphi(\bar{\imath}, s_{k-1})$. At least one of these formulas must be true. The value at the argument i of the function F we have to construct is to be the (say) least numerical value of some s_j such that $\varphi(\bar{\imath}, s_j)$ is true.

What still remains to be shown is that this F is $< \varepsilon_0$-recursive. For this we use an "effective" counterpart of the above construction, where we work with codes for $\mathbf{Z}_\infty$-derivations instead of using the $\mathbf{Z}_\infty$-derivations themselves.

4.2.2. Codes for $\mathbf{Z}_\infty$-derivations

The codes will be natural numbers. They are defined inductively, corresponding to the inductive build-up of $\mathbf{Z}_\infty$-derivations. The inductive definition is trivial for the finite rules A, $\wedge$, $\vee_0$, $\vee_1$, $\forall$, $\exists$, Cut. However, for the ω-rule there is a difficulty since then we in general have infinitely many premisses. The idea now is to assume that the codes for the premisses can be enumerated by a primitive recursive function, and to use a code (or primitive recursive index) of such an enumeration function to construct a code of the whole derivation. Another essential point is that our codes should contain sufficient information about the coded derivation. In particular, if a number u codes a derivation d, then we want to be able to read off primitive recursively from u

(i) the name of the last inference of d and its p.f., m.f. and s.f. (and hence its conclusion),

(ii) a bound for the length $|d|$,

(iii) a bound for the cut-rank $\rho(d)$, and

(iv) a bound for the (finite) set of variables free in d.

The corresponding primitive recursive functions will be denoted by Rule(u), p.f.(u), m.f.(u), s.f.(u), End(u), $|u|$, Rank(u) and Var(u), respectively.

We do not write out all cases of the inductive definition of the predicate $u \in \text{Code}$(u is a *code* for a $\mathbf{Z}_\infty$-derivation), but rather give two examples corresponding to the rule Cut and the ω-rule.

Cut: If u, $v \in \text{Code}$, $\text{End}(u) = \ulcorner\Gamma, \varphi\urcorner$, $\text{End}(v) = \ulcorner\Gamma, \neg\varphi\urcorner$ and $|u|, |v| < a$, then $\langle\ulcorner\text{Cut}\urcorner, \ulcorner\varphi\urcorner, \ulcorner\Gamma\urcorner, a, u, v\rangle \in \text{Code}$.

ω-rule: If, for any i, $[e](i) =: u_i \in \text{Code}$, $\text{End}(u_i) = \ulcorner\Gamma, \Delta(\bar{\imath})\urcorner$, $|u_i| < a$, $\text{Rank}(u_i) \leq k$ and $\text{Var}(u_i) \subseteq^\# b$, then $\langle\ulcorner\omega\urcorner, \ulcorner\Delta(\boldsymbol{n})\urcorner, \ulcorner\boldsymbol{n}\urcorner, \ulcorner\Gamma\urcorner, a, k, b, e\rangle \in$ Code.

Here $[e]$ denotes the primitive recursive function coded by e. $\ulcorner\cdots\urcorner$ denotes as usual a natural code for the finite object $\cdots$; $\subseteq^\#$ corresponds (under the relevant coding of finite sets of variables) to $\subseteq$; $\langle x_0, \ldots, x_{l-1}\rangle$ is a primitive recursive coding of finite sequences of natural numbers with primitive recursive inverses $(x)_i$, i.e. $(\langle x_0, \ldots, x_{l-1}\rangle)_i = x_i$ for $i < l$. We also skip the (trivial) primitive recursive definitions of the functions Rule(u), ... mentioned above.

4.2.3. It is easy to see that all $\mathbf{Z}_\infty$-derivations obtained by embedding $\mathbf{Z}$ in $\mathbf{Z}_\infty$ (cf. 3.4.2) can be coded, and that any such code has length $|u| < |\omega \cdot 2|$.

4.2.4. We now show that to the operations on $\mathbf{Z}_\infty$-derivations defined in

3.4.3 (weakening, substitution, etc.) there correspond primitive recursive functions on the codes. This will follow by easy applications of the Primitive Recursion Theorem of KLEENE [1958]. The lemmas are stated in the order they can be proved. We shall only sketch the proof for one of them (a typical example).

WEAKENING LEMMA. *We have a primitive recursive function* Weak *such that for any* $u \in \text{Code}$ *and any* Γ *the following holds.*

(i) $\text{Weak}(u, \ulcorner\Gamma\urcorner) =: u_0 \in \text{Code}$,
(ii) $\text{End}(u_0) = \ulcorner\Gamma, \Delta\urcorner$ *if* $\text{End}(u) = \ulcorner\Delta\urcorner$,
(iii) $|u_0| = |u|$,
(iv) $\text{Rank}(u_0) = \text{Rank}(u)$, *and*
(v) $\text{Var}(u_0) = \text{Var}(u) \cup^* V^*$ *with* V *the set of variables free in* Γ.

EVALUATION LEMMA. *We have a primitive recursive function* Eval *such that for any* $u \in \text{Code}$, $\Gamma(n)$, *variable* n *and closed terms* s, t *with the same value the following holds.*

(i) $\text{Eval}(u, \ulcorner\Gamma(n)\urcorner, \ulcorner n\urcorner, \ulcorner s\urcorner, \ulcorner t\urcorner) =: u_0 \in \text{Code}$,
(ii) $\text{End}(u_0) = \ulcorner\Gamma(t)\urcorner$ *if* $\text{End}(u) = \ulcorner\Gamma(s)\urcorner$,
(iii) $|u_0| = |u|$,
(iv) $\text{Rank}(u_0) = \text{Rank}(u)$, *and*
(v) $\text{Var}(u_0) = \text{Var}(u)$.

SUBSTITUTION LEMMA. *We have a primitive recursive function* Sub *such that for any* $u \in \text{Code}$, *variable* n *and term* s *the following holds.*

(i) $\text{Sub}(u, \ulcorner n\urcorner, \ulcorner s\urcorner) =: u_0 \in \text{Code}$,
(ii) $\text{End}(u_0) = \ulcorner\Gamma(s)\urcorner$ *if* $\text{End}(u) = \ulcorner\Gamma(n)\urcorner$,
(iii) $|u_0| \preccurlyeq |u|$,
(iv) $\text{Rank}(u_0) \leq \text{Rank}(u)$, *and*
(v) $\text{Var}(u_0) \subseteq^* (\text{Var}(u) -^* \{n\}^*) \cup^* V^*$ *where* V *is the set of variables free in* s.

For the proof one has to construct a primitive recursive function (also by the Primitive Recursion Theorem) corresponding to the change of bound variables in $\mathbf{Z}_\infty$-derivations.

INVERSION LEMMA. (1) *We have primitive recursive functions* Inv_i $(i = 0, 1)$ *such that for any* $u \in \text{Code}$ *and conjunction* $\varphi_0 \wedge \varphi_1$ *the following holds.*

(i) $\text{Inv}_i(u, \ulcorner\varphi_0 \wedge \varphi_1\urcorner) =: u_i \in \text{Code}$,
(ii) $\text{End}(u_i) = \ulcorner\Gamma, \varphi_i\urcorner$ *if* $\text{End}(u) = \ulcorner\Gamma, \varphi_0 \wedge \varphi_1\urcorner$ *with* $\varphi_0 \wedge \varphi_1$ *not in* Γ,
(iii) $|u_i| \preccurlyeq |u|$,

(iv) $\mathrm{Rank}(u_i) \leq \mathrm{Rank}(u)$, *and*

(v) $\mathrm{Var}(u_i) \subseteq^{\#} \mathrm{Var}(u)$.

(2) *We have a primitive recursive function* Inv *such that for any* $u \in$ Code *and generalization* $\forall n \psi(n)$ *the following holds.*

(i) $\mathrm{Inv}(u, \ulcorner \forall n \psi(n) \urcorner) =: u_0 \in \mathrm{Code}$,

(ii) $\mathrm{End}(u_0) = \ulcorner \Gamma, \psi(n) \urcorner$ *if* $\mathrm{End}(u) = \ulcorner \Gamma, \forall n \psi(n) \urcorner$ *with* $\forall n \psi(n)$ *not in* Γ,

(iii) $|u_0| \preccurlyeq |u|$,

(iv) $\mathrm{Rank}(u_0) \leq \mathrm{Rank}(u)$, *and*

(v) $\mathrm{Var}(u_0) \subseteq^{\#} \mathrm{Var}(u) \cup^{\#} \{n\}^{\#}$.

REDUCTION LEMMA. *We have a primitive recursive function* Red *such that for any* $u_0, u_1 \in$ Code *and formula* φ *with* $\mathrm{Rank}\ (u_i) \leq |\varphi|$ $(i = 0, 1)$ *the following holds.*

(i) $\mathrm{Red}(u_0, u_1, \ulcorner \varphi \urcorner) =: u \in \mathrm{Code}$,

(ii) $\mathrm{End}(u) = \ulcorner \Gamma, \Delta \urcorner$ *if* $\mathrm{End}(u_0) = \ulcorner \Gamma, \varphi \urcorner$ *with* φ *not in* Γ *and* $\mathrm{End}(u_1) = \ulcorner \Delta, \neg \varphi \urcorner$ *with* $\neg \varphi$ *not in* Δ,

(iii) $\mathrm{Rank}(u) \leq |\varphi|$,

(iv) $|u| \preccurlyeq \ulcorner \xi_0 \# \xi_1 \urcorner$ *if* $|u_i| = \ulcorner \xi_i \urcorner$, *and*

(v) $\mathrm{Var}(u) \subseteq^{\#} \mathrm{Var}(u_0) \cup^{\#} \mathrm{Var}(u_1)$.

CUT-ELIMINATION THEOREM. *We have a primitive recursive function* Elim *such that for any* $u \in$ Code *with* $\mathrm{Rank}(u) = k + 1$ *the following holds.*

(i) $\mathrm{Elim}(u) =: u' \in \mathrm{Code}$,

(ii) $\mathrm{End}(u') = \mathrm{End}(u)$,

(iii) $|u'| \preccurlyeq 2^{\ulcorner \xi \urcorner}$ *with* $\ulcorner \xi \urcorner := |u|$,

(iv) $\mathrm{Rank}(u') \leq k$, *and*

(v) $\mathrm{Var}(u') \subseteq^{\#} \mathrm{Var}(u)$.

PROOF. By the Primitive Recursion Theorem we can define a primitive recursive function Elim with code e as follows.

Case 1. $\mathrm{Rule}(u) = \ulcorner \mathrm{Cut} \urcorner$. Let $\mathrm{m.f.}(u) = \{\varphi, \neg \varphi\}^{\#}$.

Subcase 1.1. $|\varphi| + 1 < \mathrm{Rank}(u)$. Define $\mathrm{Elim}(u) = \langle (u)_0, (u)_1, (u)_2, \ulcorner 2^{\xi} \urcorner, \mathrm{Elim}((u)_4), \mathrm{Elim}((u)_5) \rangle$ where $\ulcorner \xi \urcorner = (u)_3$.

Subcase 1.2. $|\varphi| + 1 = \mathrm{Rank}(u)$. Define $\mathrm{Elim}(u) = \mathrm{Red}(\mathrm{Elim}((u)_4), \mathrm{Elim}((u)_5), \ulcorner \varphi \urcorner)$.

Case 2. $\mathrm{Rule}(u) = \ulcorner \omega \urcorner$. Define $\mathrm{Elim}(u) = \langle (u)_0, \ldots, (u)_3, \ulcorner 2^{\xi} \urcorner, k, (u)_6, e' \rangle$ where $\ulcorner \xi \urcorner = (u)_4$ and $e' = e'(e, u)$ is a code of $\mathrm{Elim}([(u)_7](n))$ as a primitive recursive function of n; e' as a function of e and u is primitive recursive. The other cases are treated similarly. By $\prec$-induction on $|u|$ one can prove easily that $\mathrm{Elim}(u)$ has the required properties. $\square$

4.2.5. Now we prove Theorem 4.2, following the sketch in 4.2.1. So let a $\mathbf{Z}$-derivation of $\exists m\, \varphi(n, m)$ be given and let u be a code of the corresponding $\mathbf{Z}_\infty$-derivation (cf. 4.2.3). Hence $|u| = \ulcorner \xi \urcorner < \ulcorner \omega \cdot 2 \urcorner$. By a finite number of applications of the Cut-Elimination Theorem in 4.2.4 we obtain a code u^* of a cut-free $\mathbf{Z}_\infty$-derivation of $\exists m\, \varphi(n, m)$ with $|u^*| \leqslant \ulcorner 2^{\xi}_{\mathrm{Rank}(u)} \urcorner$. Then $\mathrm{Sub}(u^*, \ulcorner n \urcorner, \ulcorner \bar{\imath} \urcorner)$ is a code for a cut-free $\mathbf{Z}_\infty$-derivation of $\exists m\, \varphi(\bar{\imath}, m)$. We may assume $\mathrm{Var}(\mathrm{Sub}(u^*, \ulcorner n \urcorner, \ulcorner \bar{\imath} \urcorner)) = \emptyset^*$ (otherwise apply $\mathrm{Sub}(\cdot, \ulcorner m \urcorner, \ulcorner 0 \urcorner)$ for any $m \in^* \mathrm{Var}(\mathrm{Sub}(u^*, \ulcorner n \urcorner, \ulcorner \bar{\imath} \urcorner)))$. Hence the $\mathbf{Z}_\infty$-derivation coded by $\mathrm{Sub}(u^*, \ulcorner n \urcorner, \ulcorner \bar{\imath} \urcorner)$ contains only improper instances of the ω-rule, which may be cancelled. However, the function F_0 corresponding for codes to this cancellation is not primitive recursive, but only $< \varepsilon_0$-recursive: in case $\mathrm{Rule}(v) = \ulcorner \omega \urcorner$ we have to define $F_0(v) = F_0([(v)_6](0))$ and we only know $|[(v)_6](0)| < |v|$. Now from $F_0(\mathrm{Sub}(u^*, \ulcorner n \urcorner, \ulcorner \bar{\imath} \urcorner))$ we can easily read off primitive recursively all (closed) terms $s_0, \ldots, s_{k-1}$ used in instances of the rule $\exists$ in the corresponding derivation. Since by the same argument as in the proof of Herbrand's Theorem 2.9 we get a derivation of $\varphi(\bar{\imath}, s_0), \ldots, \varphi(\bar{\imath}, s_{k-1})$, we know that at least one $\varphi(\bar{\imath}, s_j)$ must be true. Let $F(i)$ be the least numerical value of some s_j such that $\varphi(\bar{\imath}, s_j)$ is true. This completes the proof of Theorem 4.2. $\square$

4.3. We now turn to a generalization of Theorem 4.2 to arbitrary $\mathbf{Z}$-formulas. For the formulation of the result we need the notion of the *Herbrand normal form* φ_{H} of a formula φ, which we introduce first.

The general definition of φ_{H} is sufficiently explained by the following example. Let $\varphi \equiv \exists n\, \forall m\, \exists k\, \forall p\, \psi(n, m, k, p)$. Then $\varphi_{\mathrm{H}} \equiv \exists n, k\, \psi(n, f(n), k, g(n, k))$ with function variables f, g. One can show easily that $\varphi \to \varphi_{\mathrm{H}}$ is derivable (logically and hence) in $\mathbf{Z}$, and furthermore that if φ_{H} is derivable in $\mathbf{Z}$ then so is φ (cf. SHOENFIELD [1967]).

In general, for an arbitrary prenex formula φ the Herbrand normal form φ_{H} is obtained from φ by (i) dropping all universal quantifiers in the prefix of φ, and (ii) replacing any variable m bound by a universal quantifier in φ by $f(\boldsymbol{n})$, where $\boldsymbol{n}$ are all variables preceding m in the prefix of φ and bound by existential quantifiers, and f is a new function variable. Hence φ_{H} has the form $\exists \boldsymbol{m}\, \varphi^{\mathrm{H}}$ with φ^{H} quantifier-free and generally containing new function variables. Again $\varphi \to \varphi_{\mathrm{H}}$ is derivable (logically and hence) in $\mathbf{Z}$, and if φ_{H} is derivable in $\mathbf{Z}$ then so is φ.

4.4. THEOREM (KREISEL [1952]). *Let φ be a formula without set variables derivable in $\mathbf{Z}$. Let $\varphi_{\mathrm{H}} \equiv \exists \boldsymbol{m}\, \varphi^{\mathrm{H}}(f, \boldsymbol{n}, \boldsymbol{m})$ be its Herbrand normal form. Then* *we can find $<\varepsilon_0$-recursive functionals $\boldsymbol{G}$ such that for all functions $\boldsymbol{F}$ and numbers $\boldsymbol{i}$, $\varphi^{\mathrm{H}}(\boldsymbol{F}, \boldsymbol{i}, \boldsymbol{G}(\boldsymbol{F}, \boldsymbol{i}))$ holds.*

PROOF. For simplicity assume $\varphi_{\mathrm{H}} \equiv \exists m\, \varphi^{\mathrm{H}}(f, n, m)$ with φ^{H} quantifier-free and without free variables other than those shown. Since by assumption φ is derivable in $\mathbf{Z}$, we know that also φ_{H} is derivable in $\mathbf{Z}$. We have to construct a function $G \in \mathrm{Rec}_{<\varepsilon_0}$ such that for any function F and number i, $\varphi^{H}(F, i, G(F, i))$ holds.

The proof is completely parallel to the proof of Theorem 4.2; we only have to relativize it to a given function F.

We first introduce a relativization $\mathbf{Z}_\infty(F)$ of $\mathbf{Z}_\infty$. The language of $\mathbf{Z}_\infty(F)$ is the language of $\mathbf{Z}$ without set variables and with just one distinguished function variable f. A finite set Δ of formulas is called a $\mathbf{Z}_\infty(F)$*-axiom* if Δ consists of atomic or negated atomic formulas without number variables such that $\bigvee \Delta$ is a tautological consequence of substitution instances of the quantifier-free axioms of $\mathbf{Z}$ and the additional axioms $f(\bar{j}) = \bar{k}$ for all j, k such that $F(j) = k$. The rules of $\mathbf{Z}_\infty(F)$ are the same as the rules for $\mathbf{Z}_\infty$.

The treatment of cut-elimination for $\mathbf{Z}_\infty$ in Section 3.4 carries over nearly unchanged to $\mathbf{Z}_\infty(F)$. Just note, for the Evaluation Lemma, that any term $s(f)$ without number variables has a numerical value i under the assignment $f \mapsto F$, and $s(f) = \bar{\imath}$ is a $\mathbf{Z}_\infty(F)$-axiom. Now the proof of Theorem 4.2 can be adapted almost word for word, with the following exceptions.

(1) In the definition of codes for $\mathbf{Z}_\infty(F)$-derivations we replace $[e](\boldsymbol{i})$ by $[e](F, \boldsymbol{i})$; $[e]$ is now the e-th primitive recursive functional (in the sense of Kleene).

(2) The functions Weak, Eval, Sub, Inv_i, Inv, Red, Elim, F_0 are to be replaced by functionals with F as an additional argument. This completes the proof of Theorem 4.4. □

4.5. We now state a converse to Theorem 4.4 (and hence also to Theorem 4.2) and sketch its proof.

THEOREM. *Let F be a $<\varepsilon_0$-recursive functional. Then F can be introduced in a recursive extension of* $\mathbf{Z}$.

4.5.1. For the proof we need an auxiliary notion: the *modulus of continuity* of a functional F. We now introduce this notion.

First note that any $<\varepsilon_0$-recursive functional $F(\boldsymbol{n}, \boldsymbol{f})$ is continuous in the sense that it depends only on a finite part of any of its function arguments. Or equivalently, F is continuous for the discrete topology of $\mathbb{N}$ and the corresponding product topology on product spaces. This can be seen easily by induction over the build-up of $<\varepsilon_0$-recursive functionals. A functional M_F is called a modulus of continuity for F iff for any $\boldsymbol{n}, \boldsymbol{f}$, $M_F(\boldsymbol{n}, \boldsymbol{f})$ codes a finite set S of natural numbers such that for any two tuples of functions $\boldsymbol{f}$ and $\boldsymbol{f}'$ coinciding on $\bigcup_k S^k$ we have $F(\boldsymbol{n}, \boldsymbol{f}) = F(\boldsymbol{n}, \boldsymbol{f}')$.

4.5.2. We shall prove the following extension of Theorem 4.5.

THEOREM. *Let F be a $<\varepsilon_0$-recursive functional. Then we can construct a $<\varepsilon_0$-recursive modulus of continuity M_F for F, and F as well as M_F can be introduced in a recursive extension of* $\mathbf{Z}$.

Remark. The fact that any $<\varepsilon_0$-recursive functional F has a $<\varepsilon_0$-recursive modulus of continuity was first proved by Kreisel in lectures ('71/72); other proofs are in TROELSTRA [1973] and in SCHWICHTENBERG [1973].

The proof is by induction on the build-up of $<\varepsilon_0$-recursive functionals. We only treat the case of α-recursion, the other cases being simpler or trivial. So let

$$F(n, \boldsymbol{m}, \boldsymbol{f}) = G(n, \boldsymbol{m}, (F \restriction n)(\cdot, \boldsymbol{m}, \boldsymbol{f}), \boldsymbol{f}).$$

By the induction hypothesis we can assume that G and a modulus of continuity M_G of G have been introduced (in a recursive extension of $\mathbf{Z}$).

We first show how F can be introduced. The trick is not to introduce F directly, but via another functional which assigns to any argument $n, \boldsymbol{m}, \boldsymbol{f}$ a *computation* u of F at this argument. Here u is called a computation of F at $n, \boldsymbol{m}, \boldsymbol{f}$ iff the following holds.

(i) u is a finite function with domain $\{a_0, a_1, \ldots, a_{k-1}\}$ where $a_0 < a_1 < \cdots < a_{k-1} = n$.

(ii) $u(a_i) = G(a_i, \boldsymbol{m}, (u \restriction a_i), \boldsymbol{f})$ for $i < k$, where $(u \restriction a_i)$ is defined by

$$(u \restriction a_i)(x) = \begin{cases} u(x) & \text{if } x = a_j \quad \text{for some } j < i, \\ 0 & \text{otherwise.} \end{cases}$$

(iii) $M_G(a_i, \boldsymbol{m}, (u \restriction a_i), \boldsymbol{f}) \cap \{x \mid x < a_i\} \subseteq \{a_0, \ldots, a_{i-1}\}$ for $i < k$. Note that any of the conditions (i)–(iii) is quantifier-free and does not involve F. Now one can prove in $\mathbf{Z}$ $\forall n, \boldsymbol{m}, \boldsymbol{f}\, \exists u$ (u is a computation of F at $n, \boldsymbol{m}, \boldsymbol{f}$), by α-induction on n. To see this, observe that adding to $\mathbf{Z}$ the arithmetical axiom of choice and second-order logic (but no second-order instances of the induction schema) gives a conservative extension of **Z**; this can either be proved directly using the method indicated in Chapter D.4, 5.5.1, or else follows from the much stronger result in Chapter D.4, 8.7. Hence the corresponding functional giving u as a functional of $n, \boldsymbol{m}, f$ can be introduced, and from this F can be easily defined explicitly. Furthermore, from the conditions (i)–(iii) and the fact that M_G is a modulus of continuity for G one can prove (in **Z**) the defining equations of F.

Now M_F can be defined from F by the following α-recursion

$$M_F(n, \boldsymbol{m}, f) = S^* \cup^* \bigcup_{\substack{a<n \\ a\in S}}{}^{*} M_F(a, \boldsymbol{m}, f),$$

where

$$S^* = M_G(n, \boldsymbol{m}, (F \restriction n)(\cdot, \boldsymbol{m}, f), f).$$

Hence, by the argument just given, M_F too can be introduced. By α-induction on n one can show in **Z** that M_F is a modulus of continuity for F, using the defining equations for F and the fact that M_G is a modulus of continuity for G.

5. Transfinite induction and the reflection principle

5.1. We now consider **Z** without set and function variables. The (uniform) *reflection principle* for **Z** is the schema

$$\text{RP} \qquad \mathrm{Der}(x, \ulcorner\varphi(\dot{\boldsymbol{n}})\urcorner) \to \varphi(\boldsymbol{n})$$

where $\mathrm{Der}(x, y)$ is the primitive recursive predicate which holds iff x codes a **Z**-derivation $d \vdash \varphi$ and $y = \ulcorner\varphi\urcorner$, and $\ulcorner\varphi(\dot{\boldsymbol{n}})\urcorner$ is a primitive recursive function of $\boldsymbol{n}$ and denotes a code for the formula obtained from $\varphi(\boldsymbol{n})$ by substituting the numerals $\bar{\boldsymbol{n}}$ for the variables $\boldsymbol{n}$, i.e., $\ulcorner\varphi(\dot{\boldsymbol{n}})\urcorner = \mathrm{Subst}(\ulcorner\varphi(\boldsymbol{n})\urcorner, \ulcorner\boldsymbol{n}\urcorner, \mathrm{Num}(\boldsymbol{n}))$ with the obvious primitive recursive functions Subst and Num. Furthermore, we assume that x is not free in $\varphi(\boldsymbol{n})$. Note that RP trivially implies the consistency of **Z**, i.e. the formula $\forall x \neg \mathrm{Der}(x, \ulcorner 0 = 1\urcorner)$. The schema of transfinite induction up to ε_0 for **Z** is

$$\mathrm{TI}_{\varepsilon_0} \qquad \forall n\, (\forall m\, (m < n \to \varphi(m)) \to \varphi(n)) \to \forall n\, \varphi(n).$$

5.2. THEOREM (KREISEL and LÉVY [1968]). ***Z** together with the schema* RP *is equivalent to **Z** together with the schema* $\mathrm{TI}_{\varepsilon_0}$.

PPROOF. We begin with the easy part and show that $\mathrm{TI}_{\varepsilon_0}$ is derivable in $\mathbf{Z} + \mathrm{RP}$. So let $\varphi(n)$ be given and define $\psi(k)$ to be

$$\forall n\,(\forall m\,(m \prec n \to \varphi(m)) \to \varphi(n)) \to \forall n\,(n \prec F(k) \to \varphi(n))$$

where $F(k) = \ulcorner \omega_k \urcorner$, $\omega_0 = 1$, $\omega_{i+1} = \omega^{\omega_i}$. Since $\mathbf{Z} \vdash \forall m\, \exists k\, m \prec F(k)$, it suffices to derive $\psi(k)$ in $\mathbf{Z} + \mathrm{RP}$. Now from the proof of GENTZEN [1943] (or SCHÜTTE [1960]) of transfinite induction up to ω_k in $\mathbf{Z}$ one can extract a primitive recursive function G such that $\mathbf{Z} \vdash \forall k\, \mathrm{Der}(G(k), \ulcorner \psi(\dot{k}) \urcorner)$. From this and RP we obtain $\psi(k)$, as required.

The proof of the converse will cover the rest of this section. We have to show that RP is derivable in $\mathbf{Z} + \mathrm{TI}_{\varepsilon_0}$. So assume $\mathrm{Der}(x, \varphi(\dot{n}))$. Now the following lemma is derivable in $\mathbf{Z}$ (cf. 4.2.3 and 5.2.2):

EMBEDDING LEMMA. *We have a primitive recursive function* Emb *such that for any x, y with* $\mathrm{Der}(x, y)$ *the following holds.*

(i) $\mathrm{Emb}(x) =: u_x \in \mathrm{Code}$,

(ii) $\mathrm{End}(u_x) = y$, *and*

(iii) $|u_x| \prec \ulcorner \omega \cdot 2 \urcorner$.

Also the Cut-Elimination Theorem of 4.2.4 is derivable in $\mathbf{Z} + \mathrm{TI}_{\varepsilon_0}$ (cf. 5.2.2). Hence we can prove in $\mathbf{Z} + \mathrm{TI}_{\varepsilon_0}$ that we have a $u_x^* \in \mathrm{Code}$ (depending primitive recursively on x) with $\mathrm{End}(u_x^*) = \ulcorner \varphi(\dot{n}) \urcorner$ and $\mathrm{Rank}(u_x^*) = 0$. In 5.2.1 we shall give within $\mathbf{Z}$ a *partial truth definition* Tr_q with the following characteristic property: For any formula $\psi(\boldsymbol{n})$ with depth of quantifier-nesting $\mathrm{QD}(\psi(\boldsymbol{n})) \leq q$ one can prove in $\mathbf{Z}$

$$\mathrm{Tr}_q(\ulcorner \psi(\dot{\boldsymbol{n}}) \urcorner) \leftrightarrow \psi(\boldsymbol{n}).$$

Now the following lemma obviously holds (use $\prec$-induction on $|u|$) and is derivable in $\mathbf{Z} + \mathrm{TI}_{\varepsilon_0}$ (cf. 5.2.2):

TRUTH LEMMA. *For any* $u \in \mathrm{Code}$ *with* $\mathrm{Rank}(u) = 0$ *and* $\mathrm{End}(u) = \ulcorner \psi \urcorner$ *where* $\mathrm{QD}(\psi) \leq q$ *we have* $\mathrm{Tr}_q(\ulcorner \psi \urcorner)$.

Specializing this to $u = u_x^*$ we obtain $\mathrm{Tr}_q(\ulcorner \varphi(\dot{\boldsymbol{n}}) \urcorner)$ and hence $\varphi(\boldsymbol{n})$, both in $\mathbf{Z} + \mathrm{TI}_{\varepsilon_0}$.

5.2.1. We define for any $q \geq 0$ a set Tr_q which is intended to give a *partial truth definition* for all $\mathbf{Z}$-formulas φ with depth of quantifier-nesting $\mathrm{QD}(\varphi) \leq q$.

First note that we can easily introduce a function Val (in a recursive extension of $\mathbf{Z}$) such that for any term $s(\boldsymbol{n})$ $\mathrm{Val}(\ulcorner s(\dot{\boldsymbol{n}}) \urcorner) = s(\boldsymbol{n})$ is derivable in $\mathbf{Z}$.

DEFINITION. Tr_q is defined as follows.

(i) $\mathrm{Tr}_q(\ulcorner Ps_0(\dot{n})\cdots s_{p-1}(\dot{n})\urcorner)\leftrightarrow P(\mathrm{Val}(\ulcorner s_0(\dot{n})\urcorner),\ldots,\mathrm{Val}(\ulcorner s_{p-1}(\dot{n})\urcorner))$ for any predicate or set symbol P.

(ii) $\mathrm{Tr}_q(\ulcorner \varphi_0\wedge\varphi_1\urcorner)\leftrightarrow \mathrm{Tr}_q(\ulcorner\varphi_0\urcorner)\wedge\mathrm{Tr}_q(\ulcorner\varphi_1\urcorner)$ if $\mathrm{QD}(\varphi_i)\le q$. Similarly for $\vee$.

(iii) $\mathrm{Tr}_q(\ulcorner\forall n\,\varphi(n)\urcorner)\leftrightarrow\forall n\,\mathrm{Tr}_{q-1}(\ulcorner\varphi(\dot{n})\urcorner)$ if $q\ge 1$ and $\mathrm{QD}(\varphi(n))\le q-1$. Similarly for $\exists$.

LEMMA. *$\mathrm{Tr}_q(\ulcorner\varphi(\dot{n})\urcorner)\leftrightarrow\varphi(n)$ is derivable in $\mathbf{Z}$ if $\mathrm{QD}(\varphi(n))\le q$.*

The proof is obvious, using induction on $|\varphi(n)|$.

5.2.2. We now show that the Embedding Lemma and the Truth Lemma stated in Section 5.2 as well as all the lemmas in 4.2.4 up to and including the Cut-Elimination Theorem are derivable in $\mathbf{Z}+\mathrm{TI}_{\varepsilon_0}$. The only point to verify is that all these lemmas can be formulated in the language of $\mathbf{Z}$; the formalization of the proofs is then routine. Now the only possible obstacle against such a formulation is the occurrence of the inductively defined notion of a code for a $\mathbf{Z}_\infty$-derivation (cf. 4.2.2) in all these lemmas. We now show how this notion can be represented in purely generalized form.

Infinite $\mathbf{Z}_\infty$-derivations may be considered as well-founded trees, where at each node there is either no branching at all (i.e. it is a bottommost node) and an instance of the rule A is affixed, or there is a 1-fold branching (corresponding to the rules $\vee_i$, $\forall$ $\exists$), or a 2-fold branching (corresponding to the rules $\wedge$, Cut), or an ω-fold branching (corresponding to the ω-rule). Then any code u of a $\mathbf{Z}_\infty$-derivation d can be thought of as obtained inductively by affixing to each node of the tree corresponding to d a code of the corresponding subderivation. Hence the property $u\in\mathrm{Code}$ is equivalent to u having such a well-founded genealogic tree. But the latter fact can be easily written in purely generalized form: One has to express that at any node (= sequence number) n the tree is locally correct, i.e. that the code u_n affixed there (u_n can be easily defined by induction on n) and all its predecessors $u_{n*\langle i\rangle}$, $i=0,1,2,\ldots$, fulfill a relation as given in the definition of codes for $\mathbf{Z}_\infty$-derivations. The well-foundedness is then obtained automatically, since in particular $|u_{n*\langle i\rangle}|\prec|u|$ is required and $\prec$ is a well-ordering. $\square$

References

BACHMANN, H.
[1955] *Transfinite Zahlen* (Springer, Berlin).

GENTZEN, G.

[1943] Beweisbarkeit und Unbeweisbarkeit von Anfangsfällen der transfiniten Induktion in der reinen Zahlentheorie, *Math. Ann.*, **119**, 140–161.

GÖDEL, K.

[1958] Über eine bisher noch nicht benützte Erweiterung des finiten Standpunkts, *Dialectica*, **12**, 280–287.

HILBERT, D. and BERNAYS, P.

[1934] *Grundlagen der Mathematik*, I (Springer, Berlin).

KLEENE, S.C.

[1958] Extension of an effectively generated class of functions by enumeration, *Colloq. Math.*, **7**, 67–78.

[1959] Recursive functionals and quantifiers of finite type I, *Trans. Am. Math. Soc.*, **91**, 1–52.

KREISEL, G.

[1952] On the interpretation of non-finitist proofs II, *J. Symbolic Logic*, **17**, 43–58.

[1958] Mathematical significance of consistency proofs, *J. Symbolic Logic*, **23**, 155–182.

[1968] A survey of proof theory, *J. Symbolic Logic*, **33**, 321–388.

KREISEL, G. and LÉVY, A.

[1968] Reflection principles and their use for establishing the complexity of axiomatic systems, *Z. Math. Logik Grundlagen Math.*, **14**, 97–142.

SCHÜTTE, K.

[1960] *Beweistheorie* (Springer, Berlin).

SCHWICHTENBERG, H.

[1973] Einige Anwendungen von unendlichen Termen und Wertfunktionalen (Habilitationsschrift, Münster).

[1975] Elimination of higher type levels in definitions of primitive recursive functionals by means of transfinite recursion, in: *Logic Colloquium '73*, edited by H. E. Rose and J. C. Shepherdson (North-Holland, Amsterdam), pp. 279–303.

SHOENFIELD, J.R.

[1967] *Mathematical Logic* (Addison-Wesley, New York).

TAIT, W.W.

[1968] Normal derivability in classical logic, in: *The Syntax and Semantics of Infinitary Languages*, edited by J. Barwise (Springer, Berlin), pp. 204–236.

TROELSTRA, A.S., editor

[1973] *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis*, Lecture Notes in Mathematics, Vol. 344 (Springer, Berlin).