Gödel's Incompleteness Theorem

Final Degree Thesis In Mathematics

Lorenzo Sauras Altuzarra

2015

Prologue

Gödel's Incompleteness Theorem is one of the greatest landmarks in the history of logic. It shows, by an ingenious arithmetization of the language and an extensive use of the idea of recursiveness, the existence of arithmetical sentences that can be neither proved nor refuted. This work is structured with the help of more or less intuitive questions, which will guide us along the proof of this theorem, and also through some of its fundamental consequences. Moreover, for the sake of clarity, we have highlighted the propositions with a blue stripe in the margin.

The exposition is organized in four chapters:

- The first chapter is a crash course in logic, which intends to present the essential concepts necessary for the understanding of what follows.
- In the second chapter, Peano arithmetic is introduced, a formal system which will provide us with the framework for our discussion.
- The third chapter is the most technical. We introduce in it our main tool, recursiveness. Also, the concept of an expressible relation and that of a representable function (which intuitevely can be described as the relations and functions over the natural numbers such that, when they hold, Peano arithmetic gives account of this fact), and it is proved that recursive relations are expressible and that recursive functions are representable.
- The fourth and final chapter is without doubt the most interesting. Having introduced all the required notions in the previous chapters, we encode sentences about arithmetic as arithmetic sentences themselves by means of Gödel's arithmetization, answering questions raised along the exposition, and allowing us to reach our main goal of proving Gödel's Incompleteness Theorem.

The first two chapters follow the lines of [Hamilton], while the last two follow those of [Mendelson].

I would like to thank professor Carlos Gómez Ambrosi for the direction of this work. His willingness and motivation have allowed to me to learn a lot.

I would also like to give thanks to all the people who have encouraged me during my degree, and specially my mother, Esperanza, for her continuous support. I would like to dedicate this work to her.

Resumen en español (Summary in Spanish)

Este trabajo está estructurado en cuatro capítulos:

- El primer capítulo es un **resumen de lógica**, dividido a su vez en tres secciones:
  - La primera sección trata de **lógica proposicional**. Aunque no es estrictamente necesaria para la posterior exposición, se ha incluido pues permite una aproximación más intuitiva a nociones de mayor generalidad que se definirán a partir de la siguiente sección.
    El resultado más importante que se comenta aquí es el **teorema de completitud** de la lógica proposicional, que nos asegura cómo obtener las «verdades» de la lógica proposicional, llamadas **tautologías**, como **teoremas** formales, es decir, como cadenas de símbolos mecánicamente derivables a partir de ciertas cadenas especiales, los **axiomas**, mediante aplicaciones de **reglas de inferencia**.
    Además, mediante la introducción de las **tablas de verdad**, se evidencia la posibilidad de resolver algorítmicamente los problemas de la lógica proposicional.
  - En la segunda sección se presenta la **lógica de predicados**. Esta lógica supone una generalización de la proposicional, más sofisticada, ya que permite la posibilidad de cuantificar los objetos que intervienen en sus enunciados.
    El concepto esencial para dar una definición de **veracidad** será el concepto de **modelo**, que puede verse como una subteoría de la teoría de conjuntos en la que los teoremas formales de un **sistema formal** son verdaderos.
    Al igual que en la lógica proposicional, se muestra un teorema de completitud, el **teorema de completitud de Gödel**, referente esta vez a las «verdades» de la lógica de predicados, llamadas **fórmulas lógicamente válidas**, y con la certeza de este resultado, se construyen los llamados **sistemas de primer orden**.
    Sin embargo, se adelanta que aceptando la (razonable) definición de algoritmo conocida como **tesis de Church**, es imposible resolver algorítmicamente todos los problemas de la lógica de predicados, dando así respuesta negativa al célebre **problema de la decisión**.
    También se definen los fundamentales conceptos de **consistencia** (imposibilidad de que un enunciado y su negación sean simultáneamente teoremas) y **completitud** (inexistencia de sentencias **indecidibles**, es decir, sentencias que no pueden ser demostradas ni refutadas).
    Es especialmente interesante la **caracterización de la consistencia** que se enuncia, indicando que un sistema de primer orden es consistente si, y sólo si, posee un modelo.
  - En la tercera sección se definen los **sistemas de primer orden con igualdad**, que buscan plasmar formalmente la noción de igualdad.
    El mayor interés de la sección radica en la observación de que no todo modelo de un sistema de primer orden con igualdad interpreta exactamente la igualdad, sino sólo una relación de equivalencia. Los modelos que consiguen expresar la igualdad se denominan **modelos normales**, y se muestra una forma de determinarlos, supuesta la consistencia.
- El segundo capítulo contiene la definición del **sistema formal de la aritmética**, que pretende servir como base para el análisis formal de la teoría de números.

Se comenta aquí la consistencia de dicho sistema formal y se demuestra que cumple una propiedad más fuerte, la **ω-consistencia**. Asegurada ya la consistencia, se define el **modelo estándar**.
Además, se avanza el **teorema de incompletitud de Gödel**, que pone de manifiesto la existencia de sentencias indecidibles en la aritmética, y se demuestra la **existencia de modelos normales para la aritmética esencialmente diferentes**.

- El tercer capítulo es el más técnico. Consta de tres secciones:
  - En la primera sección se definen las **relaciones recursivas** y las **funciones recursivas**, listando bastante de ellas, tanto porque serán herramienta esencial para demostrar los resultados del último capítulo, como porque su conocimiento puede ser útil en diversos campos de las matemáticas.
  - La segunda sección se centra en un tipo especial de recursión, la recursión completa, que también será necesaria para demostrar resultados posteriores.
  - En la tercera sección se definen los conceptos de **relación expresable** y **función representable** (que intuitivamente podemos describir como las relaciones y operaciones sobre números naturales tales que, al verificarse, inducen teoremas formales en el sistema formal de la aritmética), y se demuestra que las **relaciones recursivas son expresables**, así como que las **las funciones recursivas son representables**.
- El cuarto capítulo da respuesta a varios interrogantes planteados durante el trabajo. Se halla segmentado en cuatro secciones:
  - La primera sección muestra la **aritmetización de Gödel**, que permite codificar proposiciones referentes a la consistencia y completitud de la aritmética como enunciados aritméticos.
  - En la segunda sección se procede a demostrar el **teorema del punto fijo**, un resultado técnico aunque muy llamativo, y el **teorema de incompletitud de Gödel**.
  - En la tercera sección se comenta otro resultado especialmente interesante, el **Segundo Teorema de Gödel**, que advierte de **la imposibilidad de que la aritmética**, por medio de la aritmetización de Gödel, **pueda demostrar su propia consistencia**.
  - Finalmente, en la cuarta sección, identificando la idea de «procedimiento algorítmico» con «procedimiento recursivo» (**Tesis de Church**), se evidencia la importancia de la recursividad, definiendo los conceptos de **axiomatizabilidad recursiva** y de **decidibilidad recursiva**, y se demuestra que **la aritmética es recursivamente indecidible**.

Contents

Chapter 1

Preliminaries on logic

It is well-known that set theory is the set of theorems about sets, like arithmetic is the set of theorems about numbers, but...

Is there any mathematical theory which is the set of theorems about theorems?

Yes, such theory is logic. We begin its study by introducing its very beginnings, namely propositional logic.

1.1 Propositional logic

First, we define **statement variables** as letters which stand for arbitrary and unspecified statements, but always under the assumption that they are either true or false.

Given a statement variable p, $\neg p$ stands for the negation of p, and it should be intuitively acceptable that $\neg p$ is true iff p is false. We can describe the situation by a **truth table** (the value T is assigned to a statement variable if the statement it stands for is true, and F otherwise):

p	$\neg p$
F	T
T	F

Other connectives can be considered similarly:

	Conjunction symbol: $\wedge$	**Disjunction symbol**: $\vee$	**Conditional symbol**: $\rightarrow$	**Biconditional symbol**: $\leftrightarrow$
Interpretation	$p \wedge q$ stands for «P and Q»	$p \vee q$ stands for «P or Q»	$p \rightarrow q$ stands for «If P then Q»	$p \leftrightarrow q$ stands for «P if and only if Q»
Truth table	p q $p \wedge q$ F F F F T F T F F T T T	p q $p \vee q$ F F F F T T T F T T T T	p q $p \rightarrow q$ F F T F T T T F F T T T	p q $p \leftrightarrow q$ F F T F T F T F F T T T

Notice that connectives determine **truth functions**, whose graph is determined by the truth table.

A **statement form** is a string of symbols inductively defined by the following rules: [1]

[1] Logic's concepts, in particular inductive definitions, can be re-stated in terms of algebraic structures. An excellent introduction to algebraic logic can be found in [Amor] (in Spanish), and for further reading we refer the reader to [Burris & Sankappanavar] and [Rasiowa].

1. Every statement variable is a statement form.
2. Given statement forms α and β, $\neg\alpha$, $\alpha \wedge \beta$, $\alpha \vee \beta$, $\alpha \to \beta$ and $\alpha \leftrightarrow \beta$ are statement forms.
3. The set of statement forms is generated by rules 1 and 2.

For example, $(p \wedge q) \to \neg(q \vee r)$ is a statement form.

Two statement forms α and β are **logically equivalent**, in whose case we use the notation $\alpha \equiv \beta$, iff they represent the same truth function, i.e. iff the last column of their truth tables is the same. For example:

- *Principle of double negation*: $\neg\neg p \equiv p$.
- *De Morgan's laws*:
  - $\neg(p \wedge q) \equiv \neg p \vee \neg q$.
  - $\neg(p \vee q) \equiv \neg p \wedge \neg q$.
- Every statement form is logically equivalent to one in which only the negation and conditional symbols occur, since:
  - $p \wedge q \equiv \neg(p \to \neg q)$.
  - $p \vee q \equiv \neg p \to q$.
  - $p \leftrightarrow q \equiv \neg((p \to q) \to \neg(q \to p))$.

A statement form is a **tautology** iff its corresponding truth function takes only the value T, i.e. iff the last column of its truth table contains only T's. For example, $q \to (\neg p \to q)$ is a tautology:

p	q	$\neg p$	$p \to q$	$\neg p \to (p \to q)$
F	F	T	T	T
F	T	T	T	T
T	F	F	F	T
T	T	F	T	T

Notice that, given statement forms α and β, $\alpha \equiv \beta$ iff $\alpha \leftrightarrow \beta$ is a tautology. For example, $\neg\neg p \leftrightarrow p$ is a tautology.

«Tautology» is the central notion of propositional logic, since tautologies are the «truths» of propositional logic. For example, the *law of excluded middle* can be stated by saying that $p \vee \neg p$ is a tautology.

Is it possible to find an algorithm that decides if a statement form is a tautology?

Yes, it suffices to write its truth table and check whether the last column contains only T's.

Is it possible to obtain all the «truths» of propositional logic (tautologies) as formal theorems, i.e. as strings of symbols mechanically derivable from some distinghished strings (called axioms) by means of certain rules?

The answer to this question is yes, as it will be made apparent at the end of this section. But first, we need to formalize some of the previous ideas.

Well-formed formulas (**wffs**), inductively defined by the following rules:

1. Every statement variable is a wff.
2. Given wffs α and β, $\neg\alpha$ and $\alpha \to \beta$ are wffs.
3. The set of wffs is generated by rules 1 and 2.

A **formal system**, consists of a non-empty set of wffs, called **axioms**, and a set of partial operations over the set of wffs, called **inference rules**.

Next, we introduce the formal system L in the following way:

- Its axioms are defined by the following rules:
  1. Given wffs α and β, $\alpha \to (\beta \to \alpha)$ is an axiom.

2. Given wffs α, β, γ, $(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$ is an axiom.
3. Given wffs α and β, $(\neg\alpha \to \neg\beta) \to (\beta \to \alpha)$ is an axiom.

- Its only inference rule is **modus ponens** (**MP**): for every $\alpha, \beta \in L$, it associates α and $\alpha \to \beta$ with β.

Given wffs $\alpha_1, ..., \alpha_n$ of L, α_n is a **theorem** of L and $\langle \alpha_1, ..., \alpha_n \rangle$ is a **proof** of α_n in L iff, for every $i \in \{1, ..., n\}$, α_i is an axiom or α_i follows by MP from previous components of the sequence. For example, for every wffs α and β of L, $\neg\alpha \to (\alpha \to \beta)$ is a theorem of L:

(1)	$\neg\alpha \to (\neg\beta \to \neg\alpha)$	(L1)
(2)	$(\neg\beta \to \neg\alpha) \to (\alpha \to \beta)$	(L3)
(3)	$((\neg\beta \to \neg\alpha) \to (\alpha \to \beta)) \to (\neg\alpha \to ((\neg\beta \to \neg\alpha) \to (\alpha \to \beta)))$	(L1)
(4)	$\neg\alpha \to ((\neg\beta \to \neg\alpha) \to (\alpha \to \beta))$	MP(2, 3)
(5)	$(\neg\alpha \to ((\neg\beta \to \neg\alpha) \to (\alpha \to \beta))) \to ((\neg\alpha \to (\neg\beta \to \neg\alpha)) \to (\neg\alpha \to (\alpha \to \beta)))$	(L2)
(6)	$(\neg\alpha \to (\neg\beta \to \neg\alpha)) \to (\neg\alpha \to (\alpha \to \beta))$	MP(4, 5)
(7)	$\neg\alpha \to (\alpha \to \beta)$	MP(1, 6)

We can finally state the **completeness theorem** for propositional logic: the tautologies are precisely the theorems of L (for the proof, see Propositions 2.14 and 2.23 of [Hamilton]).

Is it possible to go deeper in logic, expressing formally the intuitive idea of quantification?

Yes, and this gives rise to a new subtheory, called predicate logic.

1.2 Predicate logic

Now we build a more sophisticated language, one capable of quantifying the objects involved in its statements. In order to do that, we introduce:

- The symbol $\forall$, called the **universal quantifier** and read «for all».
- For any $m \in \mathbb{N}^+$, the symbol c_m, called the m-th **constant**.
- For any $m, n \in \mathbb{N}^+$, the symbol f_m^n, called the m-th n-ary **function letter**.
- For any $m, n \in \mathbb{N}^+$, the symbol A_m^n, called the m-th n-ary **predicate letter**.
- **Terms**, inductively defined by the following rules:
  1. Every constant is a term.
  2. Every variable is a term.
  3. Given terms $t_1, ..., t_n$, $f_m^n(t_1, ..., t_n)$ is a term.
  4. The set of terms is generated by rules 1, 2 and 3.

  For example, $f_1^1(f_2^2(x_1, f_1^3(c_1, c_1, x_5)))$ is a term.
- **Atomic formulas**, which are those of the form $A_m^n(t_1, ..., t_n)$, where $t_1, ..., t_n$ are terms.
- **Well-formed formulas** (**wffs**), inductively defined by the following rules:
  1. Every atomic formula is a wff.
  2. Given wffs α and β, $\forall\, x_m\ \alpha$, $\neg\alpha$ and $\alpha \to \beta$ are wffs.
  3. The set of wffs is generated by rules 1 and 2.

Then, some useful notations are introduced:

- $\neg(\alpha \to \neg\beta)$ is denoted by $\alpha \wedge \beta$.
- $\neg\alpha \to \beta$ is denoted by $\alpha \vee \beta$.
- $\neg((\alpha \to \beta) \to \neg(\beta \to \alpha))$ is denoted by $\alpha \leftrightarrow \beta$.
- $\neg\forall\, x_m\ \neg\alpha$ is denoted by $\exists\, x_m\ \alpha$. $\exists$ is called the **existential quantifier** and read «there is».

Given $\Sigma \subseteq \{c_m, A_m^n, f_m^n\}_{m,n \in \mathbb{N}^+}$ such that there is at least one predicate letter contained in Σ (Σ is called an **alphabet**), $\{\alpha$ wff $\mid$ for every $s \in \{c_m, A_m^n, f_m^n\}_{m,n \in \mathbb{N}^+}$ such that s occurs in $\alpha, s \in \Sigma\}$ is called **first-order language** on Σ, and is denoted by $\mathscr{L}_\Sigma$. Nevertheless, in most of our work we shall not need to specify which alphabet we are using, so we will denote the language simply by $\mathscr{L}$.

Given a wff $a_1 \cdots a_r$ (written as a string of symbols) and $j \in \{1, ..., r\}$, x_m **occurs free** at the j^{th} position of $a_1 \cdots a_r$ iff x_m occurs without quantification in the j-th position, i.e. iff:

- a_j is x_m.
- There are not $i, k \in \{1, ..., r\}$ such that:
  - $i < j < k$.
  - a_i is $\forall$.
  - a_{i+1} is x_m.
  - x_m occurs in $a_i \cdots a_k$.
  - $a_i \cdots a_k$ is a wff.

For example, x_2 occurs free in the 8^{th} position of $\forall\, x_1\ (A_1^2(x_1, x_2) \to \forall\, x_3\ \forall\, x_1\ \forall\, x_2\ A_1^2(x_1, x_2))$ (commas are counted), and in this wff there are no more free occurrences of any variable.

A wff in which no variable occurs free is called a **sentence**. Given $\alpha \in \mathscr{L}$, the **closure** of α is the sentence obtained by prefixing with universal quantifiers those variables, in order of descending subscripts, that occur free in some position of α. For example, the closure of $A_1^2(x_2, x_5) \to \neg\forall\ x_2\ A_1^3(x_1, x_2, x_3)$ is $\forall\, x_5\ \forall\, x_3\ \forall\, x_2\ \forall\, x_1\ (A_1^2(x_2, x_5) \to \neg\forall\ x_2\ A_1^3(x_1, x_2, x_3))$.

Now we proceed to define the concept of truth, «translating» wffs into propositions about sets:

- An **interpretation** I of $\mathscr{L}$ consists of:
  - A nonempty set D_I, called the **domain** of I.
  - A function C_I such that, for every constant c_m of $\mathscr{L}$ [2], $C_I(c_m) \in D_I$.
  - A function F_I such that, for every function letter f_m^n of $\mathscr{L}$, $F_I(f_m^n)$ is an n-ary function over D_I.
  - A function P_I such that, for every predicate letter A_m^n of $\mathscr{L}$, $P_I(A_m^n)$ is an n-ary relation over D_I.
- Given an interpretation I, a **valuation** of I is a function v from the set of terms of $\mathscr{L}$ to the set D_I such that:
  - Given a constant c_m of $\mathscr{L}$, $v(c_m) = C_I(c_m)$.
  - Given a function letter f_m^n of $\mathscr{L}$ and $t_1, ..., t_n$ terms of $\mathscr{L}$, $v(f_m^n(t_1, ..., t_n)) = F_I(f_m^n)(v(t_1), ..., v(t_n))$.

  A valuation assigns to each term in $\mathscr{L}$ the object in D_I which is to be its interpretation, and assigns an element of D_I to each of the variables x_m of $\mathscr{L}$. We can now define inductively what is meant for a wff to be true with respect to a given valuation:
  - Given a predicate letter A_m^n of $\mathscr{L}$, $A_m^n(t_1, ..., t_n)$ is v-true iff $\langle v(t_1), ..., v(t_n)\rangle \in P_I(A_m^n)$.
  - Given $\alpha \in \mathscr{L}$, $\neg\alpha$ is v-true iff α is not v-true.
  - Given $\alpha, \beta \in \mathscr{L}$, $\alpha \to \beta$ is v-true iff $\neg\beta$ or α are v-true.
  - Given $\alpha \in \mathscr{L}$, $\forall\, x_m\ \alpha$ is v-true iff, for every valuation w of I such that, for every $M \in \mathbb{N}^+\backslash\{m\}$, $w(x_M) = v(x_M)$, α is w-true.

  For example, let $\Sigma := \{c_1, A_1^2, f_1^2, f_2^2\}$ and I an interpretation such that $D_I = \mathbb{N}^+$, $C_I(c_1) = 0$, $P_I(A_1^2)$ is equality, $F_I(f_1^2)$ is addition and $F_I(f_2^2)$ is multiplication.
  - If v is a valuation such that $v(x_1) = 2, v(x_2) = 6, v(x_3) = 3$ and $v(x_4) = 4$, $A_1^2(f_1^2(x_1, x_2), f_2^2(x_3, x_4))$ is v-true, since $2 \cdot 6 = 3 \cdot 4$.
  - If v is a valuation such that $v(x_1) = 1, v(x_2) = 5, v(x_3) = 4$ and $v(x_4) = 2$, $A_1^2(f_1^2(x_1, x_2), f_2^2(x_3, x_4))$ is not v-true, since $1 \cdot 5 \neq 4 \cdot 2$.
  - Let v be a valuation such that $v(x_1) = 0$.
    Hence, $A_1^2(x_1, c_1)$ is v-true.
    Let w be a valuation such that, for every $M \in \mathbb{N}^+\backslash\{1\}$, $w(x_M) = v(x_M)$ but $w(x_1) \neq v(x_1)$.
    Hence, $A_1^2(x_1, c_1)$ is not w-true, since $w(x_1) \neq 0$.
    Therefore, $\forall\, x_1\ A_1^2(x_1, c_1)$ is not v-true.
- Finally, given an interpretation I and $\alpha \in \mathscr{L}$, we define:
  - α is **true** in I iff, for every valuation v of I, α is v-true.
  - α is **false** in I iff there is no valuation v of I such that α is v-true.

  For example, let $\Sigma := \{A_1^2, f_1^2\}$, let α be to $\forall\, x_1\ \forall\, x_2\ \exists\, x_3\ A_1^2(f_1^2(x_1, x_3), x_2)$:

[2] That is, more formally, such that $c_m \in \Sigma$.

- If I is an interpretation such that $D_I = \mathbb{Q}^+$, $F_I(f_1^2)$ is multiplication and $P_I(A_1^2)$ is equality, α is true in I, since for every $m, n \in \mathbb{Q}^+$ there is $p \in \mathbb{Q}^+$ such that $m \cdot p = n$.
- If J is an interpretation such that $D_J = \mathbb{N}^+$, $F_J(f_1^2)$ is multiplication and $P_J(A_1^2)$ is equality, α is false in J, since there are $m, n \in \mathbb{N}^+$ such that there is no $p \in \mathbb{N}^+$ such that $m \cdot p = n$.

Notice that:
- To be false is stronger than not to be true.
- A wff is false iff its negation is true.
- Since the domain of an interpretation is non-empty, it is impossible for a wff to be both true and false in a given interpretation.
- Every sentence is true or false. Therefore, it or its negation are true (for the proof, see Corollary 3.34 of [Hamilton]).

Given $\alpha \in \mathscr{L}$, α is **logically valid** iff α is true in every interpretation. For example, given $\alpha \in \mathscr{L}$:
- $\alpha \vee \neg\alpha$ is logically valid (in fact, every wff which is a substitution instance of a tautology of propositional logic is logically valid (for the proof, see Proposition 3.31 of [Hamilton])).
- $\forall\, x_m\ \alpha \to \exists\, x_m\ \alpha$ is logically valid (for the proof, see Example 3.37.b of [Hamilton]).

Logically valid wffs play the same role in predicate logic as tautologies in propositional logic, i.e. logically valid wffs are the «truths» of predicate logic.

(*Entscheidungsproblem*) Like in propositional logic, is it possible to find an algorithm which can decide if a sentence is logically valid?

If we accept the definition of «algorithm» provided by **Church's Thesis**, the answer is negative. We will get back to this question in the last chapter.

Like in propositional logic, is it possible to obtain all the «truths» of predicate logic (logically valid wffs) as formal theorems?

The answer to this question is yes, as it will be made apparent again at the end of this section. But first we need to introducte some concepts.

Given a wff $a_1 \cdots a_r$ (written as a string of symbols) and a term $t_1 \cdots t_s$ (written as a string of symbols), and denoting $a_1 \cdots a_r$ and $u_1 \cdots u_s$ by α and t respectively, t is **free** for x_m in α iff x_m can be replaced by t in its free occurrences in α without new interactions with quantifiers, i.e. iff for every $i \in \{1, ..., r\}$ such that x_m occurs free in the i^{th} position of α, for every $j \in \{1, ..., s\}$ such that there is $M \in \mathbb{N}^+$ such that t_j is x_M, x_M occurs free in the $(i - 1 + j)^{\text{th}}$ position of $a_1 \cdots a_{i-1} u_1 \cdots u_s a_{i+1} \cdots a_r$. For example, in $\forall\, x_1\ A_1^2(x_1, x_2) \to \forall\, x_3\ A_2^2(x_3, x_1)$:
- x_1 is free for x_1 (every variable is free for itself).
- x_2 is free for x_1, but $f_1^2(x_1, x_3)$ is not.
- $f_2^2(x_2, x_3)$ is free for x_2, but $f_3^2(x_1, x_4)$ is not.
- $f_3^2(x_1, x_4)$ is free for x_3 (this is vacuously true, because x_3 does not occur free).

Notice also that every constant is free for every variable in every wff.

Given $\alpha \in \mathscr{L}$ and a term t free for x_m in α, we denote by $\alpha_t^{x_m}$ the wff obtained by replacing in α all the free occurrences (if there are any) of x_m by t.

Now we introduce the formal system $K_{\mathscr{L}}$:
- Its axioms are defined by the following rules:
  1. **(K1)** Given $\alpha, \beta \in \mathscr{L}$, $\alpha \to (\beta \to \alpha)$ is an axiom.
  2. **(K2)** Given $\alpha, \beta, \gamma \in \mathscr{L}$, $(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$ is an axiom.

3. **(K3)** Given $\alpha, \beta \in \mathscr{L}$, $(\neg\alpha \to \neg\beta) \to (\beta \to \alpha)$ is an axiom.
4. **(K4)** Given $\alpha \in \mathscr{L}$ and a term t free for x_m in α, $\forall\, x_m\ \alpha \to \alpha_t^{x_m}$ is an axiom.
5. **(K5)** Given $\alpha, \beta \in \mathscr{L}$ such that there are no free occurrences of x_m in α, $\forall\, x_m\ (\alpha \to \beta) \to (\alpha \to \forall\, x_m\ \beta)$ is an axiom.

- Its inference rules are:
  - **Modus ponens** (**MP**): for every $\alpha, \beta \in \mathscr{L}$, it associates α and $\alpha \to \beta$ with β.
  - **Generalization** with respect to x_m (**Gen**): for every $\alpha \in \mathscr{L}$, it associates α with $\forall\, x_m\ \alpha$.

$K_{\mathscr{L}}$ has some useful inference rules which can be derived from the previous ones and which will be useful in subsequent chapters (see [Mendelson]):

- **Existential Rule E4**: given $\alpha \in \mathscr{L}$ and a term t free for x_m in α, if $\alpha_t^{x_m}$ is a theorem of $K_{\mathscr{L}}$, then $\exists\, x_m\ \alpha$ is also a theorem of $K_{\mathscr{L}}$.
- **Conjunction Introduction**: for every $\alpha_1, ..., \alpha_n$ which are theorems of $K_{\mathscr{L}}$, $\alpha_1 \wedge ... \wedge \alpha_n$ is a theorem of $K_{\mathscr{L}}$.
- **Conjunction Elimination**: for every $\alpha_1, ..., \alpha_n \in \mathscr{L}$ such that $\alpha_1 \wedge ... \wedge \alpha_n$ is a theorem of $K_{\mathscr{L}}$, for every $i \in \{1, ..., n\}$, α_i is a theorem of $K_{\mathscr{L}}$.
- **Biconditional Introduction**: for every $\alpha, \beta \in \mathscr{L}$ such that $\alpha \to \beta$ and $\beta \to \alpha$ are theorems of $K_{\mathscr{L}}$, $\alpha \leftrightarrow \beta$ is a theorem of $K_{\mathscr{L}}$.
- **Biconditional Elimination**: for every $\alpha, \beta \in \mathscr{L}$ such that $\alpha \leftrightarrow \beta$ is a theorem of $K_{\mathscr{L}}$:
  - If α is a theorem of $K_{\mathscr{L}}$, β is a theorem of $K_{\mathscr{L}}$.
  - If $\neg\alpha$ is a theorem of $K_{\mathscr{L}}$, $\neg\beta$ is a theorem of $K_{\mathscr{L}}$.
- **Rule C**: for every $\alpha \in \mathscr{L}$ and $\Gamma \subseteq \mathscr{L}$, α is deducible from Γ by Rule C iff there are $\alpha_1, ..., \alpha_n \in \mathscr{L}$ such that:
  - α_n is α.
  - Given $i \in \{1, ..., n\}$, one of the following conditions holds:
    1. α_i is an axiom of $K_{\mathscr{L}}$.
    2. $\alpha_i \in \Gamma$.
    3. α_i follows by MP or Gen from previous wffs in the sequence.
    4. There is a preceeding wff α_k of $\langle \alpha_1, ..., \alpha_n \rangle$ such that there is $\beta \in \mathscr{L}$ such that α_k is $\exists\, x_m\ \beta$ and there is a new constant c such that $\beta_c^{x_m}$ is α_i (Rule C).
  - As axioms in condition 1, we can also use all axioms that involve the new constants already introduced by applications of condition 4.
  - No application of Gen is made using a variable that is free in some wff of the form $\exists\, x_m\ \beta$ to which Rule C has been previously applied.
  - α contains none of the new constants introduced in any application of Rule C.

  There is no harm in eventually adding new constants with the Rule C, because if α is deducible in $K_{\mathscr{L}}$ from Γ by Rule C, α is deducible in $K_{\mathscr{L}}$ from Γ with no need of such constants (see Proposition 2.9 of [Mendelson]).

We can state the **Gödel's Completeness Theorem**: the logically valid wffs of $\mathscr{L}$ are precisely the theorems of $K_{\mathscr{L}}$ (see Propositions 4.5. and 4.39. of [Hamilton]).

Given a first-order system E:

- Another formal system F is an **extension** of E iff every theorem of E is also a theorem of F.
- An interpretation I is a **model** of a E iff every theorem of E is true in I. In fact, I is a model for E iff every axiom of E is true in I (see Proposition 4.41 of [Hamilton]).

Notice that, since the theorems of $K_{\mathscr{L}}$ are the logically valid wffs, every interpretation is a model of $K_{\mathscr{L}}$. Therefore, the notion of model will get more significance with certain extensions of $K_{\mathscr{L}}$, extensions in which there will appear new and interesting theorems, but in which not every interpretation will be a model.

An extension E of $K_{\mathscr{L}}$ obtained by enlarging the set of axioms of $K_{\mathscr{L}}$ is called a **first-order system**.

Given a first-order system E, $\Gamma \subseteq \mathscr{L}$ and $\alpha_1, ..., \alpha_n \in \mathscr{L}$, α_n is **deducible** in E from Γ and $\langle \alpha_1, ..., \alpha_n \rangle$ is a **deduction** of α_n in E from Γ iff, for every $i \in \{1, ..., n\}$, α_i is an axiom, $\alpha_i \in \Gamma$ or α_i follows by inference rules of E from previous components of the sequence.

We have the **Deduction Theorem** (see Proposition 4.8 of [Hamilton]): given a first-order system E, $\Gamma \subseteq \mathscr{L}$ and $\alpha, \beta \in \mathscr{L}$, $\alpha \to \beta$ is deducible in E from Γ if:

- β is deducible in E from $\Gamma \cup \{\alpha\}$.
- If there is a deduction $\langle \beta_1, ..., \beta_n \rangle$ of β in E from $\Gamma \cup \{\alpha\}$ such that $n > 1$ and such that there is a variable x_m which occurs free at some position of α, there is no $i \in \{1, ..., r-1\}$ such that β_{i+1} is $\forall\, x_m\, \beta_i$.

Thus, it is clear that, if α is a sentence, $\alpha \to \beta$ is deducible in E from Γ iff β is deducible in E from $\Gamma \cup \{\alpha\}$.

Given a first-order system E:

- E is **consistent** iff for no wff are both it and its negation simultaneously theorems of E.

  Notice that the following conditions are equivalent:
  - E is consistent.
  - There is a wff which is not a theorem of E (see Proposition 2.18 of [Hamilton]).
  - E has a model (see Proposition 4.42 of [Hamilton]).

- E is **complete** iff every sentence is **decidable** in E, i.e. iff for every sentence, it or its negation is a theorem of E.

$K_{\mathscr{L}}$ is consistent (see Corollary 4.6 of [Hamilton]).

$K_{\mathscr{L}}$ is incomplete.

Proof

Let $A_i^k \in \Sigma$ (remember that Σ contains at least one predicate letter). Neither $\forall\, x_1\, ...\, \forall\, x_k\, A_i^k(x_1, ..., x_k)$ nor $\neg \forall\, x_1\, ... \forall\, x_k\, A_i^k(x_1, ..., x_k)$ are theorems of $K_{\mathscr{L}}$, since it is always possible to find a non-empty set D such that there are $A \subseteq D^k$ and $d_1, ..., d_k, \widetilde{d}_1, ..., \widetilde{d}_k \in D$ such that $\langle d_1, ..., d_k \rangle \in A$ and $\langle \widetilde{d}_1, ..., \widetilde{d}_k \rangle \notin A$.

□

The following step is to formalize the notion of equality.

1.3 First-order systems with equality

From now on, we will assume that the predicate letter A_1^2 is included in our alphabet. A_1^2 will be denoted by $=$ and, for every t, q terms, $A_1^2(t, u)$ will be denoted by $t = u$.

A first-order system is called a **first-order system with equality** iff the following wffs are included in its set of axioms:

(E1) $x_1 = x_1$. [3]

(E2) $t_i = u \to f_m^n(t_1, ..., t_n) = f_m^n(t_1, ..., t_{i-1}, q, t_{i+1}, ..., t_n)$, with f_m^n a function letter of $\mathscr{L}$, $i \in \{1, ..., n\}$ and $q, t_1, ..., t_n$ terms of $\mathscr{L}$.

(E3) $t_i = u \to (A_m^n(t_1, ..., t_n) \to A_m^n(t_1, ..., t_{i-1}, q, t_{i+1}, ..., t_n))$, with A_m^n a predicate letter of $\mathscr{L}$, $i \in \{1, ..., n\}$ and $q, t_1, ..., t_n$ terms of $\mathscr{L}$.

An axiom of a first-order system with equality is called:

[3] Notice that, for every $m \in \mathbb{N}^+$, $x_m = x_m$ is a theorem of such a first-order system, since a variable can be replaced in a wff by any other variable which does not occur in it, without altering the quality of being a theorem.

- A **logical axiom** iff it is an axiom of $K_{\mathscr{L}}$.
- An **axiom for equality** iff it is one of the axioms (E1), (E2) or (E3).
- A **proper axiom** otherwise.

First-order systems with equality capture the notion of «equivalence relation», since the following wffs are always theorems of those systems (see Proposition 5.4. of [Hamilton]):

- $\forall\ x_1\ x_1 = x_1$.
- $\forall\ x_1\ \forall\ x_2\ (x_1 = x_2 \to x_2 = x_1)$.
- $\forall\ x_1\ \forall\ x_2\ \forall\ x_3\ (x_1 = x_2 \to (x_2 = x_3 \to x_1 = x_3))$.

Therefore, given a model I of a first-order system with equality, $P_I(=)$ is an equivalence relation over D_I.

Nevertheless, in a model of a first-order system with equality the symbol $=$ need not necessarily be interpreted by equality. For example, if $\Sigma = \{f_1^2, =\}$ and I is interpretation such that $D_I = \mathbb{Z}$, $F_I(f_1^2)$ is addition and $P_I(=)$ is congruence modulo 2, I is a model of $K_{\mathscr{L}}$ in which (E1), (E2) and (E3) are true.

Given a model I of a first-order system with equality:

- I is a **normal model** iff $P_I(=)$ is equality.
- It is possible to construct a normal model from I, called the **contraction** of I: a model J is the contraction of I iff:
  - $D_J = \{[x]_{P_I(=)} \mid x \in D_I\}$.
  - Given a constant c_m of $\mathscr{L}$, $C_J(c_m) = [c_m]_{P_I(=)}$.
  - Given a function letter f_m^n of $\mathscr{L}$ and $d_1, ..., d_n \in D_I$, $F_J(f_m^n)(d_1, ..., d_n) = [F_I(f_m^n)(d_1, ..., d_n)]_{P_I(=)}$.
  - Given a predicate letter A_m^n of $\mathscr{L}$ and $d_1, ..., d_n \in D_I$, $\langle [d_1]_{P_I(=)}, ..., [d_n]_{P_I(=)} \rangle \in P_J(A_m^n)$ iff $\langle d_1, ..., d_n \rangle \in P_I(A_m^n)$.

Intuitively, J is obtained from I by reducing everything modulo the equivalence relation $P_I(=)$.

Let $\alpha(x_m)$ a wff of $\mathscr{L}$ in which x_m occurs free, and let x_n be a variable which does not occur at all in $\alpha(x_m)$. Then the wff $\exists\ x_m\ \alpha(x_m) \wedge \forall\ x_m\ \forall\ x_n\ (\alpha(x_m) \wedge (\alpha(x_n) \to x_m = x_n))$ is denoted by $\exists!\ x_m\ \alpha(x_m)$. The symbol $\exists!$ is read «there is one, and only one,».

Chapter 2

Peano arithmetic

From now on, we will denote:

- c_1 by 0.
- f_1^1 by $'$ and, for every term t, $f_1^1(t)$ by t'.
- f_1^2 by $+$ and, for every t, u terms, $f_1^2(t,u)$ by $t+u$.
- f_2^2 by $\cdot$ and, for every t, u terms, $f_2^2(t,u)$ by $t \cdot u$.

Until the end of our work, our alphabet of symbols will be$\Sigma = \{0, +, \cdot, ', =\}$ (and, as usual, we will denote $\mathscr{L}_\Sigma$ simply by $\mathscr{L}$).

Peano arithmetic, denoted by *PA*, is the first-order system with equality whose proper axioms are:

(N1) $\forall\ x_1\ \neg x_1' = 0$.
(N2) $\forall\ x_1\ \forall\ x_2\ (x_1' = x_2' \to x_1 = x_2)$.
(N3) $\forall\ x_1\ x_1 + 0 = x_1$.
(N4) $\forall\ x_1\ \forall\ x_2\ x_1 + (x_2') = (x_1 + x_2)'$.
(N5) $\forall\ x_1\ x_1 \cdot 0 = 0$.
(N6) $\forall\ x_1\ \forall\ x_2\ x_1 \cdot (x_2') = (x_1 \cdot x_2) + x_1$.
(N7) Given a wff $\alpha(x_1)$ of *PA* in which x_1 occurs free, $(\alpha(0) \wedge \forall\ x_1\ (\alpha(x_1) \to \alpha(x_1'))) \to \forall\ x_1\ \alpha(x_1)$, with $\alpha(0)$ and $\alpha(x_1')$ the wffs obtained by replacing in $\alpha(x_1)$ all the free occurrences of x_1 by 0 and x_1' respectively.

Axioms (N1), (N2) and (N7) are based on the classical Peano's axioms, (N7) being a version of the **Principle of Induction**. (N3) and (N4) provide a recursive definition of addition, and (N5) and (N6) a recursive definition of multiplication.

However, (N7) is in fact weaker than the usual Principle of Induction, since the latter refers to the set of all subsets of $\mathbb{N}$, which is uncountable, whereas the former refers to the set of those subsets of $\mathbb{N}$ definable by an arithmetical formula, which is countable.

The interpretation I of *PA* such that $D_I = \mathbb{N}$, $C_I(0) = 0$, $F_I(+)$ is addition, $F_I(\cdot)$ is multiplication, $F_I(')$ is the successor function and $P_I(A_1^2)$ is equality is called the **standard interpretation** of *PA*, and, from now on:

- As usual, we will consider that multiplication prevails over the addition, so for example the wff $(x_1 \cdot x_2) + x_3$ will be simply written as $x_1 \cdot x_2 + x_3$.
- Terms $0, 0', 0'', ..., 0'^{\ldots(n \text{ strokes})\ldots'}, ...$ are called **numerals** and denoted by $\overline{0}, \overline{1}, \overline{2}, ..., \overline{n}, ...$ respectively (except the term 0 which will usually be denoted by 0). Notice that every numeral is free for every variable in every wff.
- Given terms t and s, we will denote the wff $\exists\ x_1\ x_1' + t = s$ by $t < s$.
- Given a wff α of *PA*, we will write $\vdash_{PA}\ \alpha$ iff α is a theorem of *PA*.

If we accept the standard interpretation of *PA* as a model of *PA*, then *PA* is consistent. This model is known as the **standard model** of arithmetic.

PA is strong enough to prove almost every theorem of elementary number theory. For example, Euclidean division (see Proposition 3.11 of [Mendelson]):
$\vdash_{PA} \forall x_1 \forall x_2 (\neg x_2 = 0 \rightarrow \exists! x_3 \exists! x_4 (x_1 = x_2 \cdot x_3 + x_4 \wedge x_4 < x_2))$.

However, is it possible to obtain all «arithmetical truths» as formal theorems, i.e. is *PA* complete?

Unfortunately, this is not the case, since the fact that *PA* is incomplete is precisely the content of **Gödel's Incompleteness Theorem**.

If I is the standard model of *PA*, then the extension $\mathscr{V}$ of *PA* obtained by adding as axioms all wffs which are true in I is consistent and complete.

Proof
- $\mathscr{V}$ is consistent, since I is clearly a model of $\mathscr{V}$.
- $\mathscr{V}$ is complete:
  - Given a sentence α, α or $\neg\alpha$ are true in I, since every sentence is true or false.
  - Then, α or $\neg\alpha$ are theorems of $\mathscr{V}$.
  - So $\mathscr{V}$ is complete.

□

However, $\mathscr{V}$ is useless. The reason for this will be made clear in the last chapter.

Every model for *PA* has an infinite domain, and given a cardinal number $\aleph_\beta$, *PA* has a normal model with domain of cardinality $\aleph_\beta$ (see proposition 3.6 of [Mendelson]).

The incompleteness of *PA* is related to another important deficiency of the system.

Does *PA* characterize $\mathbb{N}$ (up to isomorphism), i.e. is the standard model the «only» (normal) model of *PA*?

Once again, the answer is negative, because there are «essentially different» normal models of *PA*:
- Let α be a sentence of *PA* such that neither α nor $\neg\alpha$ are theorems of *PA* (such α exists by Gödel's Incompleteness Theorem).
- Let PA_α and $PA_{\neg\alpha}$ be the extensions of *PA* obtained by adding as axioms α and $\neg\alpha$ respectively.
- PA_α and $PA_{\neg\alpha}$ are consistent (see Proposition 4.35 of [Hamilton]).
- Let I_α and $I_{\neg\alpha}$ be denumerable models of PA_α and $PA_{\neg\alpha}$ respectively. Such models exists since:
  - A first-order system has a model iff it is consistent.
  - Given a cardinal number $\aleph_\beta$, *PA* has a normal model with domain of cardinality $\aleph_\beta$.
- Let $\widetilde{I}_\alpha$ and $\widetilde{I}_{\neg\alpha}$ be the contractions of I_α and $I_{\neg\alpha}$ respectively.
- $\widetilde{I}_\alpha$ and $\widetilde{I}_{\neg\alpha}$ are two normal models of *PA*, with denumerable domain, since every model for *PA* has an infinite domain.

To finish this section, we introduce an interesting notion which will be needed later: *PA* is **ω-consistent**, i.e. there is no wff α of *PA* such that:
- α contains (at least) one free occurrence of x_1.
- Given $n \in \mathbb{N}$, $\vdash_{PA} \neg\alpha\frac{x_1}{n}$.
- $\vdash_{PA} \exists x_1 \alpha$.

Proof
- Let I be the standard model for *PA*.
- Assume that there is a wff α of *PA* such that:

  - α contains (at least) one free occurrence of x_1.
  - Given $n \in \mathbb{N}$, $\vdash_{PA} \neg\alpha^{x_1}_{\overline{n}}$.
  - $\vdash_{PA} \exists\ x_1\ \alpha$.
- Thus, for every $n \in \mathbb{N}$, $\neg\alpha^{x_1}_{\overline{n}}$ is true in I.
- Hence, $\forall\ x_1\ \neg\alpha$ is true in I.
- But $\exists\ x_1\ \alpha$, i.e. $\neg\forall\ x_1\ \neg\alpha$ is also true in I. Impossible, since a wff is false iff its negation is true.
- So PA is ω-consistent.

□

Chapter 3

Recursiveness

The main purpose of this chapter is to answer a more technical question.

> What relations over the natural numbers are such that, when they hold, there is a theorem of *PA* that gives account of this fact?

Certain relations, called **recursive relations**, are characterized (as we will see in the last section of this chapter) by satisfying this sort of property.

3.1 Definitions and examples

A **number-theoretic relation** of k arguments is a subset of $\mathbb{N}^k$, and a **number-theoretic function** of k arguments is an operation from $\mathbb{N}^k$ to $\mathbb{N}$.

A **recursive function** is a number-theoretic function inductively defined by the following rules:

1. The **zero function**, $\mathcal{Z}(n) := 0$, is recursive.
2. The **successor function**, $\mathcal{S}(n) := n + 1$, is recursive.
3. Given $i \in \{1, ..., k\}$, the i^{th} **projection function** of k arguments, $\mathcal{P}^k_i(n_1, ..., n_k) := n_i$, is recursive.
4. **(Substitution Rule)** Given recursive functions $g(n_1, ..., n_i), h_1(n_1, ..., n_k), ..., h_i(n_1, ..., n_k)$, $g(h_1(n_1, ..., n_k), ..., h_i(n_1, ..., n_k))$ is recursive.
5. **(Recursion Rule)** Given recursive functions $g(n_1, ..., n_k)$ and $h(n_1, ..., n_{k+2})$, is also recursive the function $f : \mathbb{N}^{k+1} \longrightarrow \mathbb{N}$.
   $\langle n_1, ..., n_k, 0\rangle \longmapsto g(n_1, ..., n_k)$
   $\langle n_1, ..., n_k, n + 1\rangle \longmapsto h(n_1, ..., n_k, n, f(n_1, ..., n_k, n))$
   Here, we allow $n = 0$, in which case we have that the function $f : \mathbb{N} \longrightarrow \mathbb{N}$ is recursive.
   $$0 \longmapsto g(0)$$
   $$n + 1 \longmapsto h(n, f(n))$$
6. Given a recursive function $g(n_1, ..., n_{k+1})$ such that, for every $n_1, ..., n_k \in \mathbb{N}$, there is an $m \in \mathbb{N}$ such that $g(n_1, ..., n_k, m) = 0$, the $\boldsymbol{\mu}$**-operator** $\mu_g(n_1, ..., n_k) := \min(\{m \in \mathbb{N} \mid g(n_1, ..., n_k, m) = 0\})$, is recursive.
7. The set of recursive functions is generated by rules 1 to 6.

Notice that, given a recursive function $g(n_1, ..., n_k)$, $g(\mathcal{P}^r_{j_1}(n_1, ..., n_r), ..., \mathcal{P}^r_{j_k}(n_1, ..., n_r))$ is recursive, by the Substitution Rule. This gives certain freedom to define new number-theoretic functions, for example:

- **(Adding dummy variables)** Given a recursive function $g(m, n)$, $f(m, n, p) := g(m, p)$ is recursive.
- **(Permuting variables)** Given a recursive function $g(m, n, p)$, $f(m, n, p) := g(p, m, n)$ is recursive.
- **(Identifying variables)** Given a recursive function $g(m, n, p)$, $f(m, n) := g(n, m, m)$ is recursive.

Now we give a list of recursive functions, that will be needed in the sequel:

1. $m+n$
2. $m \cdot n$
3. $m \dot{-} n := \left\{ \begin{array}{cc} m-n & \text{if} \quad m \geqslant n \\ 0 & \text{if} \quad m < n \end{array} \right\}$
4. $|m-n| := \left\{ \begin{array}{cc} m-n & \text{if} \quad m \geqslant n \\ n-m & \text{if} \quad m < n \end{array} \right\}$
5. $\mathrm{sg}(n) := \left\{ \begin{array}{cc} 1 & \text{if} \quad n > 0 \\ 0 & \text{if} \quad n = 0 \end{array} \right\}$
6. $\overline{\mathrm{sg}}(n) := \left\{ \begin{array}{cc} 0 & \text{if} \quad n > 0 \\ 1 & \text{if} \quad n = 0 \end{array} \right\}$
7. $n!$
8. $\min\{n_1, ..., n_k\}$
9. $\max\{n_1, ..., n_k\}$
10. $\mathrm{qt}(m,n) := \max\{q \in \mathbb{N} \mid n - q \cdot m > 0\}$
11. $\mathrm{rm}(m,n) := n - \mathrm{qt}(m,n) \cdot m$
12. $\tau(n) := \left\{ \begin{array}{cc} 1 & \text{if } n = 0 \\ \#\{m \in \mathbb{N}^+ \mid m|n\} & \text{otherwise} \end{array} \right\}$

Proof

(We only prove some of them, in order to give an idea, for the rest of the proof see Proposition 3.15 of [Mendelson]).

1. $+ : \mathbb{N}^2 \longrightarrow \mathbb{N}$
   $\langle m, 0\rangle \longmapsto \mathcal{P}_1^1(m)$
   $\langle m, n+1\rangle \longmapsto \mathcal{S}(\mathcal{P}_3^3(m,n,m+n))$
2. $\cdot : \mathbb{N}^2 \longrightarrow \mathbb{N}$
   $\langle m, 0\rangle \longmapsto \mathcal{Z}(m)$
   $\langle m, n+1\rangle \longmapsto \mathcal{P}_3^3(m,n,m \cdot n) + \mathcal{P}_1^3(m,n,m \cdot n)$
7. Let $f(n) := n!$
   $f : \mathbb{N} \longrightarrow \mathbb{N}$
   $0 \longmapsto 1$
   $n+1 \longmapsto (n+1) \cdot f(n)$
12. $\tau(n) = \sum\limits_{m<n+1} (\overline{\mathrm{sg}}(\mathrm{rm}(m,n)))$

□

The so-called **bounded sums** and **bounded products** are also recursive:

1. If $k > 1$, for every recursive function $f(n_1, ..., n_k)$ and $p \in \mathbb{N}$:
   (a) $\sum\limits_{m<p} (f(n_1, ..., n_{k-1}, m)) := \left\{ \begin{array}{cc} 0 & \text{if} \quad p = 0 \\ f(n_1, ..., n_{k-1}, 0) + ... + f(n_1, ..., n_{k-1}, p-1) & \text{if} \quad p > 0 \end{array} \right\}$
   (b) $\prod\limits_{m<p} (f(n_1, ..., n_{k-1}, m)) := \left\{ \begin{array}{cc} 0 & \text{if} \quad p = 0 \\ f(n_1, ..., n_{k-1}, 0) \cdot ... \cdot f(n_1, ..., n_{k-1}, p-1) & \text{if} \quad p > 0 \end{array} \right\}$
2. Given a recursive function $f(n)$ and $p \in \mathbb{N}$:
   (a) $\sum\limits_{m<p} (f(m)) := \left\{ \begin{array}{cc} 0 & \text{if} \quad p = 0 \\ f(0) + ... + f(p-1) & \text{if} \quad p > 0 \end{array} \right\}$
   (b) $\prod\limits_{m<p} (f(m)) := \left\{ \begin{array}{cc} 0 & \text{if} \quad p = 0 \\ f(0) \cdot ... \cdot f(p-1) & \text{if} \quad p > 0 \end{array} \right\}$

Proof

(We only prove one of them, in order to give an idea, for the rest of the proof see Proposition 3.16 of [Mendelson]).

Let $g(n_1, ..., n_{k-1}, p) := \sum_{m<p} (f(n_1, ..., n_{k-1}, m))$.

$$\begin{aligned} g : \mathbb{N}^k &\longrightarrow \mathbb{N} \\ \langle n_1, ..., n_{k-1}, 0\rangle &\longmapsto 0 \\ \langle n_1, ..., n_{k-1}, p+1\rangle &\longmapsto g(n_1, ..., n_{k-1}, p) + f(n_1, ..., n_{k-1}, p) \end{aligned}$$

□

The **characteristic function** of a number-theoretic relation $A(n_1, ..., n_k)$ is defined by $C_A(n_1, ..., n_k) := \left\{ \begin{array}{ll} 1 & \text{if } \langle n_1, ..., n_k\rangle \notin A \\ 0 & \text{if } \langle n_1, ..., n_k\rangle \in A \end{array} \right\}$, and we define A to be a **recursive relation** iff C_A is a recursive function.

For example:

- $=$ is recursive, since $C_=(m, n) = \text{sg}(|m - n|)$
- $<$ is recursive, since $C_<(m, n) = \overline{\text{sg}}(|n \dot{-} m|)$
- $|$ is recursive, since $C_|(m, n) = \text{sg}(\text{rm}(m, n))$
- $\text{Pr} := \{m \in \mathbb{N} \mid m \text{ is prime}\}$ is recursive, since $C_{\text{Pr}}(n) = \text{sg}(\tau(n) \dot{-} 2) + \overline{\text{sg}}(|n - 1|) + \overline{\text{sg}}(|n - 0|)$
  Remember that n is prime iff it has exactly two divisors and is not equal to 0 or 1.

Given a recursive relation $A(n_1, ..., n_k)$ (see Proposition 3.17 of [Mendelson]):

- For every recursive relation $B(n_1, ..., n_k)$, $A \cup B$, $A \cap B$, $\mathbb{N}^k \backslash A$ are recursive, so from now on, we denote:
  - $\langle n_1, ..., n_k\rangle \in A \cap B$ by $A(n_1, ..., n_k) \wedge B(n_1, ..., n_k)$.
  - $\langle n_1, ..., n_k\rangle \in A \cup B$ by $A(n_1, ..., n_k) \vee B(n_1, ..., n_k)$.
  - $\langle n_1, ..., n_k\rangle \in \mathbb{N}^k \backslash A$ by $\neg A(n_1, ..., n_k)$.
- If $k > 1$:
  - $\{\langle n_1, ..., n_{k-1}, m\rangle \in \mathbb{N}^k \mid \text{for every } p \in \mathbb{N} \text{ such that } p < m, \langle n_1, ..., n_{k-1}, p\rangle \in A\}$ is recursive, so from now on, we denote that for every $p \in \mathbb{N}$ such that $p < m, \langle n_1, ..., n_{k-1}, p\rangle \in A$ by $\forall\, p_{p<m}\ A(n_1, ..., n_{k-1}, p)$.
  - $\{\langle n_1, ..., n_{k-1}, m\rangle \in \mathbb{N}^k \mid \text{there is } p \in \mathbb{N} \text{ such that, if } p < m\ \langle n_1, ..., n_{k-1}, p\rangle \in A\}$ is recursive, so from now on, we denote that there is $p \in \mathbb{N}$ such that, if $p < m\ \langle n_1, ..., n_{k-1}, p\rangle \in A$ by $\exists\, p_{p<m}\ A(n_1, ..., n_{k-1}, p)$.
- $\{m \in \mathbb{N} \mid \text{for every } p \in \mathbb{N} \text{ such that } p < m, p \in A\}$ is recursive, so from now on, we denote that for every $p \in \mathbb{N}$ such that $p < m, p \in A$ by $\forall\, p_{p<m}\ A(p)$.
- $\{m \in \mathbb{N}^k \mid \text{there is } p \in \mathbb{N} \text{ such that, if } p < m,\ p \in A\}$ is recursive, so from now on, we denote that there is $p \in \mathbb{N}$ such that, if $p < m\ p \in A$ by $\exists\, p_{p<m}\ A(p)$.

The so-called **bounded μ-operators** are also recursive: given a number-theoretic relation $A(n_1, ..., n_k)$ and $p \in \mathbb{N}$, we denote:

- If $k > 1$, $\mu\ m_{m<p}\ A(n_1, ..., n_{k-1}, m) :=$
  $\left\{ \begin{array}{ll} \min(\{m \in \mathbb{N} \mid \langle n_1, ..., n_{k-1}, m\rangle \in A\}) & \text{if there is } m \in \mathbb{N} \text{ such that} \\ & \langle n_1, ..., n_k, m\rangle \in A \text{ and } m < p \\ p & \text{otherwise} \end{array} \right\}$. [1]
- If $k = 1$, $\mu\ m_{m<p}\ A(m) := \left\{ \begin{array}{ll} \min(A) & \text{if there is } m \in A \\ & \text{such that } m < p \\ p & \text{otherwise} \end{array} \right\}$.

[1]

Proof

[1] The value p is chosen in the second cases because it is more convenient in later proofs, but this choice has no intuitive significance.

- $\mu\ m_{m<p}\ A(n_1,...,n_{k-1},m) = \sum_{m<p}\left(\prod_{q<m+1}(C_A(n_1,...,n_{k-1},q))\right)$.
- $\mu\ m_{m<p}\ A(m) = \sum_{m<p}\left(\prod_{q<m+1}(C_A(q))\right)$.

□

Every finite subset of $\mathbb{N}$ is recursive (see Proposition 6.24 and example 6.25.a of [Hamilton]).

Then, we continue listing useful recursive functions:

1. $p(n)$, the n-th prime number.
2. $l(n) := \left\{\begin{array}{ccc} 0 & \text{if} & n=0 \\ 1 & \text{if} & n=1 \\ \max(\{m\in\mathbb{N}\mid p(m)|n\}) & \text{if} & n\geqslant 2 \end{array}\right\}$.
3. Given $i\in\{0,...,l(n)\}$, $(n)_i := \left\{\begin{array}{ccc} 0 & \text{if} & n=0 \\ 0 & \text{if} & n=1 \\ \max(\{m\in\mathbb{N}\mid p(i)^m|n\}) & \text{if} & n\geqslant 2 \end{array}\right\}$.
4. $m*n := m\cdot\prod_{i<l(n)+1}\left(p(l(m)+i+1)^{(n)_i}\right)$.
   Notice that, for every $m,n,p\in\mathbb{N}^+$, $m*(n*p)=(m*n)*p$, so there is no harm in this case in omitting parentheses when writing two of more applications of $*$.

Proof

1. $p:\mathbb{N}\longrightarrow\mathbb{N}$.
   $0\longmapsto 2$
   $n+1\longmapsto \mu\ m_{m<p(n)!+2}\ (p(n)<m\wedge \Pr(m))$[2]
2. $l(n) = n\dot{-}\mu\ m_{m<n+1}\ (p(n\dot{-}m)|n)$.
3. $(n)_i = \mu\ m_{m<n}\ (p(i)^m|n\ \wedge\ p(i)^{m+1}\nmid n)$.
4. Immediate.

□

3.2 Course-of-values recursion

It is often convenient to define functions by a recursion in which the value of $f(n_1,...,n_{k-1},p+1)$ depends not only upon $f(n_1,...,n_{k-1},p)$ but also upon several or all values of $f(n_1,...,n_{k-1},m)$, with $m\leqslant p$. This type of recursion is called a **course-of-values recursion**.

Let $f(n_1,...,n_k)$ be a number-theoretic function, and $f\#(n_1,...,n_{k-1},p) := \prod_{m<p}\left(p(m)^{f(n_1,...,n_{k-1},m)}\right)$. Notice that $f(n_1,...,n_{k-1},p) = (f\#(n_1,...,n_{k-1},p+1))_p$.

Then (see Proposition 3.19 and corollary 3.20 of [Mendelson]):

- For every recursive function $h(n_1,...,n_{k+1})$ and a number-theoretic function $f(n_1,...,n_k)$ such that $f(n_1,...,n_{k-1},p) = h(n_1,...,n_{k-1},p,f\#(n_1,...,n_{k-1},p))$, f is recursive.
- For every number-theoretic relation $A(n_1,...,n_k)$ and recursive function $h(n_1,...,n_{k+1})$ such that, for every $n_1,...,n_{k-1},p\in\mathbb{N}$, $\langle n_1,...,n_k,p\rangle\in A$ iff $h(n_1,...,n_{k-1},p,C_A\#(n_1,...,n_{k-1},p))$, A is recursive.

For example, let f be the Fibonacci sequence.
Then, $f:\mathbb{N}\longrightarrow\mathbb{N}$, i.e. $f:\mathbb{N}\longrightarrow\mathbb{N}$.
$0\longmapsto 1$ $\qquad$ $n\longmapsto \overline{\text{sg}}(n)+\overline{\text{sg}}(|n-1|)+\text{sg}(n\dot{-}1)\cdot((f\#(n))_{n\dot{-}1}+(f\#(n))_{n\dot{-}2})$

[2] The bound is obtained from Euclid's proof of the infinitude of primes.

$$1 \longmapsto 1$$
$$n+2 \longmapsto f(n)+f(n+1)$$

Notice that, considering $h : \mathbb{N}^2 \longrightarrow \mathbb{N}$, $f(n) = h(n, f\#(n))$, so f is recursive.

$$\langle m,n\rangle \longmapsto \overline{\text{sg}}(m) + \overline{\text{sg}}(|m-1|) + \text{sg}(m \dot{-} 1) \cdot ((n)_{m \dot{-} 1} + (n)_{m \dot{-} 2})$$

3.3 Expressibility and representability

A number-theoretic relation A of k arguments is **expressible** in *PA* iff there is a wff $\alpha(x_1, ..., x_k)$ of *PA* with precisely k free variables such that, for any $n_1, ..., n_k \in \mathbb{N}$, if $\alpha(\overline{n}_1, ..., \overline{n}_k)$ is the wff obtained by replacing in $\alpha(x_1, ..., x_k)$, for every $i \in \{1, ..., k\}$, all the free occurrences of x_i by $\overline{n}_i$:

- If $\langle n_1, ..., n_k\rangle \in A$, $\vdash_{PA} \alpha(\overline{n}_1, ..., \overline{n}_k)$.
- If $\langle n_1, ..., n_k\rangle \notin A$, $\vdash_{PA} \neg\alpha(\overline{n}_1, ..., \overline{n}_k)$.

A number-theoretic function f of k arguments is **representable** in *PA* iff there is a wff $\alpha(x_1, ..., x_{k+1})$ of *PA* with precisely $k+1$ free variables such that, for any $n_1, ..., n_{k+1} \in \mathbb{N}$:

- If $\langle n_1, ..., n_{k+1}\rangle \in A$, $\vdash_{PA} \alpha(\overline{n}_1, ..., \overline{n}_{k+1})$.
- $\vdash_{PA} \exists!\, x_{k+1}\ \alpha(\overline{n}_1, ..., \overline{n}_k, x_{k+1})$.

Every recursive function is representable in *PA*. [3]

[3]

Proof

- First, we need the following lemmas:
  - Lemma I **(Gödel's $\boldsymbol{\beta}$-function)** $\boldsymbol{\beta}(m,n,p) := \text{rm}(1+(p+1)\cdot n, m)$ is representable in *PA* by the wff $\text{Bt}(x_1, ..., x_4)$ defined as $\exists\, w\ (x_1 = (\overline{1} + (x_3 + \overline{1}) \cdot x_2) \cdot w + x_4 \wedge x_4 < \overline{1} + (x_3 + \overline{1}) \cdot x_2)$.
    Proof
    * Let $m, n, p, q \in \mathbb{N}$ such that $\boldsymbol{\beta}(m,n,p) = q$.
    * Then, there is $r \in \mathbb{N}$ such that:
      · $m = (1 + (p+1)\cdot n)\cdot r + q$.
      · $q < 1 + (p+1)\cdot n$.
    * Hence, $\vdash_{PA}\ (\overline{m} = (\overline{1} + (\overline{p} + \overline{1}) \cdot \overline{n}) \cdot \overline{r} + \overline{q}) \wedge \overline{q} < \overline{1} + (\overline{p} + \overline{1}) \cdot \overline{n})$.
    * Applying Rule E4, $\vdash_{PA}\ \text{Bt}(\overline{m}, \overline{n}, \overline{p}, \overline{q})$.
    * Finally, notice that $\vdash_{PA}\ \exists!\, x_4\ \text{Bt}(\overline{m}, \overline{n}, \overline{p}, x_4)$, by the «translation» to *PA* of Euclidean division given in Chapter 2.

    □
  - Lemma II For any sequence of natural numbers $n_0, ..., n_k$, there are $b, c \in \mathbb{N}$ such that, for every $i \in \{0, ..., k\}$,
    $\boldsymbol{\beta}(b,c,i) = n_i$.
    Proof
    * Let $j := \max\{k, n_0, ..., n_k\}$ and $c := j!$.
    * Consider, for every $i \in \{0, ..., k\}$, $u_i := 1 + (i+1)\cdot c$.
    * Given $h, i \in \{0, ..., k\}$ such that $h \neq i$, u_h and u_i are relatively prime:
      · Assume $h < i$, and suppose there is a prime number p such that $p \mid u_h$ and $p \mid u_i$.
      · Then, $p \mid u_i - u_h$, i.e. $p \mid (i-h)\cdot c$, hence, $p \mid i - h$ or $p \mid c$.
      · But if $p \mid c$, then $p \mid u_h$ and $p \mid (h+1)\cdot c$, i.e. $p \mid 1 + (h+1)\cdot c$ and $p \mid (h+1)\cdot c$, hence $p \mid 1$, a contradiction.
      · And notice that, if $p \mid i - h$, then $p \mid c$, since $i - h \leqslant h \leqslant j$, and so $i - h \mid j! = c$.
    * Also, for every $i \in \{0, ..., k\}$, $n_i \leqslant j \leqslant j! = c < 1 + (i+1)\cdot c = u_i$.
    * Finally, by the Chinese Remainder Theorem, there is $b \in \mathbb{N}$ such that $b < u_0 \cdot ... \cdot u_k$ and, for every $i \in \{0, ..., k\}$, $\text{rm}(u_i, b) = n_i$, i.e. $\boldsymbol{\beta}(b,c,i) = \text{rm}(1 + (i+1)\cdot c, b) = n_i$.

    □

[3] The converse is also true, see Proposition 3.28 of [Mendelson].

- Lemma III For any wff α of PA and $n \in \mathbb{N}^+$, $\vdash_{PA}\ (\alpha(0) \wedge ... \wedge \alpha(\overline{n-1})) \rightarrow \forall\, x_1\ (x_1 < \overline{n} \rightarrow \alpha(x_1))$ (see Proposition 3.8 of [Mendelson]).

- $\mathcal{Z}$ is representable in PA by $x_1 = x_1 \wedge x_2 = 0$:
  - $\mathcal{Z}(n) = m\ \Rightarrow\ 0 = m\ \Rightarrow \vdash_{PA}\ \overline{n} = \overline{n} \wedge \overline{m} = 0$.
  - Given $n \in \mathbb{N}$, $\vdash_{PA}\ \exists!\ x_2\ \overline{n} = \overline{n} \wedge x_2 = 0$.
- $\mathcal{S}$ is representable in PA by $x_2 = x_1'$:
  - $\mathcal{S}(n) = m\ \Rightarrow\ n+1 = m\ \Rightarrow \vdash_{PA}\ \overline{m} = \overline{n}'$.
  - Given $n \in \mathbb{N}$, $\vdash_{PA}\ \exists!\ x_2\ x_2 = \overline{n}'$.
- $\mathcal{P}_i^k$ is representable in PA by $x_1 = x_1 \wedge ... \wedge x_k = x_k \wedge x_{k+1} = x_i$:
  - $\mathcal{P}_i^k(n_1, ..., n_k) = m\ \Rightarrow\ n_i = m\ \Rightarrow \vdash_{PA}\ \overline{n}_1 = \overline{n}_1 \wedge ... \wedge \overline{n}_k = \overline{n}_k \wedge \overline{m} = \overline{n}_i$.
  - Given $n_1, ..., n_k \in \mathbb{N}$, $\vdash_{PA}\ \exists!\ x_{k+1}\ \overline{n}_1 = \overline{n}_1 \wedge ... \wedge \overline{n}_k = \overline{n}_k \wedge x_{i+1} = \overline{n}_i$.
- The Substitution Rule does not lead out of the set of the representable functions.
  Let $g(n_1, ..., n_i)$ be representable in PA by a wff $\beta(x_1, ..., x_{i+1})$, and $h_1(n_1, ..., n_k), ..., h_i(n_1, ..., n_k)$ be representable in PA by wffs $\alpha_1(x_1, ..., x_{k+1}), ..., \alpha_i(x_1, ..., x_{k+1})$, respectively,
  and let $f(n_1, ..., n_k) := g(h_1(n_1, ..., n_k), ..., h_i(n_1, ..., n_k))$.
  Then f is representable in PA by the wff $\gamma(x_1, ..., x_{k+1})$ defined as
  $\exists\ y_1\ ...\ \exists\ y_i\ (\alpha_1(x_1, ..., x_k, y_1) \wedge ... \wedge \alpha_i(x_1, ..., x_k, y_i) \wedge \beta(y_1, ..., y_i, x_{k+1}))$.
  Indeed (let $n_1, ..., n_k, m \in \mathbb{N}$ such that $f(n_1, ..., n_k) = m$):
  - $f(n_1, ..., n_k) = m \overset{r_j := h_j(n_1, ..., n_k)}{\Rightarrow} g(r_1, ..., r_i) = m \overset{\substack{g, h_1, ..., h_i \text{ are representable in } PA \\ \text{by } \beta, \alpha_1, ..., \alpha_i}}{\Rightarrow}$
    $\left\{ \begin{array}{l} \vdash_{PA}\ \beta(\overline{r}_1, ..., \overline{r}_i, \overline{m}) \\ \vdash_{PA}\ \alpha_j(\overline{n}_1, ..., \overline{n}_k, \overline{r}_j) \end{array} \right\} \overset{\substack{\text{Conjunction} \\ \text{Introduction}}}{\Rightarrow}$
    $\vdash_{PA}\ \alpha_1(\overline{n}_1, ..., \overline{n}_k, \overline{r}_1) \wedge ... \wedge \alpha_i(\overline{n}_1, ..., \overline{n}_k, \overline{r}_i) \wedge \beta(\overline{r}_1, ..., \overline{r}_i, \overline{m}) \overset{\text{Rule E4}}{\Rightarrow}$
    $\vdash_{PA}\ \exists\ y_1\ ...\exists\ y_i\ (\overline{n}_1, ..., \overline{n}_k, y_1) \wedge ... \wedge \alpha_i(\overline{n}_1, ..., \overline{n}_k, y_i) \wedge \beta(y_1, ..., y_i, \overline{m}))\ \Rightarrow \vdash_{PA}\ \gamma(\overline{n}_1, ..., \overline{n}_k, \overline{m})$.
  - $\left\{ \begin{array}{l} \vdash_{PA}\ \gamma(\overline{n}_1, ..., \overline{n}_k, x_{k+1}) \\ \vdash_{PA}\ \gamma(\overline{n}_1, ..., \overline{n}_k, x_{k+2}) \end{array} \right\} \Rightarrow$
    $\left\{ \begin{array}{l} \vdash_{PA}\ \exists\ y_1\ ...\ \exists\ y_i\ (\alpha_1(\overline{n}_1, ..., \overline{n}_k, y_1) \wedge ... \wedge \alpha_i(\overline{n}_1, ..., \overline{n}_k, y_i) \wedge \beta(y_1, ..., y_i, x_{k+1})) \\ \vdash_{PA}\ \exists\ y_1\ ...\ \exists\ y_i\ (\alpha_1(\overline{n}_1, ..., \overline{n}_k, y_1) \wedge ... \wedge \alpha_i(\overline{n}_1, ..., \overline{n}_k, y_i) \wedge \beta(y_1, ..., y_i, x_{k+2})) \end{array} \right\} \overset{\text{Rule C}}{\Rightarrow}$
    For certain new constants $b_1, ..., b_i, c_1, ..., c_i$,
    $\left\{ \begin{array}{l} \vdash_{PA}\ \alpha_1(\overline{n}_1, ..., \overline{n}_k, b_1) \wedge ... \wedge \alpha_i(\overline{n}_1, ..., \overline{n}_k, b_i) \wedge \beta(b_1, ..., b_i, x_{k+1}) \\ \vdash_{PA}\ \alpha_1(\overline{n}_1, ..., \overline{n}_k, c_1) \wedge ... \wedge \alpha_i(\overline{n}_1, ..., \overline{n}_k, c_i) \wedge \beta(c_1, ..., c_i, x_{k+2}) \end{array} \right\} \overset{\substack{\text{Conjunction} \\ \text{Elimination}}}{\Rightarrow}$
    $\left\{ \begin{array}{l} \vdash_{PA}\ \alpha_j(\overline{n}_1, ..., \overline{n}_k, b_j) \\ \vdash_{PA}\ \beta(b_1, ..., b_i, x_{k+1}) \\ \vdash_{PA}\ \alpha_j(\overline{n}_1, ..., \overline{n}_k, c_j) \\ \vdash_{PA}\ \beta(c_1, ..., c_i, x_{k+2}) \end{array} \right\} \overset{\substack{\vdash_{PA}\ \exists!\ x_{k+1}\ \alpha_j(\overline{n}_1, ..., \overline{n}_k, x_{k+1}) \\ \text{(since } h_j \text{ is representable in } PA \text{ by } \alpha_j)}}{\Rightarrow}$
    $b_j = c_j = \overline{r}_j \overset{\left\{ \begin{array}{c} \vdash_{PA}\ \beta(b_1, ..., b_i, x_{i+1}) \\ \text{Axioms for equality} \\ \vdash_{PA}\ \exists!\ x_{i+1}\ \beta(x_1, ..., x_{i+1}) \\ \text{(since } g \text{ is representable in } PA \text{ by } \beta) \end{array} \right\}}{\Rightarrow} x_{k+1} = x_{k+2} \overset{\vdash_{PA}\ \exists\ x_{k+1}\ \gamma(\overline{n}_1, ..., \overline{n}_k, x_{k+1})}{\Rightarrow}$
    $\vdash_{PA}\ \exists!\ x_{k+1}\ \gamma(\overline{n}_1, ..., \overline{n}_k, x_{k+1})$.
- The Recursion Rule does not lead out of the set of representable functions.
  Let $g(n_1, ..., n_k)$ and $h(n_1, ..., n_k, m, p)$ be representable in PA by wffs $\alpha(x_1, ..., x_{k+1})$ and $\beta(x_1, ..., x_{k+3})$, respectively, and let $f : \mathbb{N}^{k+1} \longrightarrow \mathbb{N}$.
  $$\langle n_1, ..., n_k, 0\rangle \longmapsto g(n_1, ..., n_k)$$
  $$\langle n_1, ..., n_k, m+1\rangle \longmapsto h(n_1, ..., n_k, m, f(n_1, ..., n_k, m))$$
  We shall show that f is representable in PA by the following wff $\gamma(x_1, ..., x_{k+2})$:
  $$\exists\ u\ \exists\ v\ (\exists\ w\ (\mathrm{Bt}(u, v, 0, w) \wedge \alpha(x_1, ..., x_k, w)) \wedge \mathrm{Bt}(u, v, x_{k+1}, x_{k+2}) \wedge$$
  $$\forall\ w\ (w < x_{k+1} \rightarrow \exists\ y\ \exists\ z\ (\mathrm{Bt}(u, v, w, y) \wedge \mathrm{Bt}(u, v, w', z) \wedge \beta(x_1, ..., x_k, w, y, z)))).$$
  Indeed (let $n_1, ..., n_k, p, m \in \mathbb{N}$ such that $f(n_1, ..., n_k, p) = m$):

- $\vdash_{PA} \gamma(\overline{n}_1, ..., \overline{n}_k, \overline{p}, \overline{m})$:
  - Case $p = 0$
    - Lemma II $\Rightarrow$ There are $b, c \in \mathbb{N}$ such that $\boldsymbol{\beta}(b, c, 0) = m \overset{\text{Lemma I}}{\Rightarrow} \vdash_{PA} \mathrm{Bt}(\overline{b}, \overline{c}, 0, \overline{m})$. [0]
    - $p = 0 \Rightarrow m = f(n_1, ..., n_k, 0) = g(n_1, ..., n_k) \overset{g \text{ is representable in } PA \text{ by } \alpha}{\Rightarrow}$
      $\vdash_{PA} \alpha(\overline{n}_1, ..., \overline{n}_k, \overline{m}) \overset{\text{[0], Rule E4, Conjunction Introduction}}{\Rightarrow} \vdash_{PA} \exists\, w\, (\mathrm{Bt}(\overline{b}, \overline{c}, 0, w) \wedge \alpha(\overline{n}_1, ..., \overline{n}_k, w))$. [1]
    - $\vdash_{PA} \neg w < 0 \overset{\text{Gen for } w}{\Rightarrow}$
      $\forall\, w\, (w < 0 \rightarrow \exists\, y\, \exists\, z\, (\mathrm{Bt}(\overline{b}, \overline{c}, w, y) \wedge \mathrm{Bt}(\overline{b}, \overline{c}, w', z) \wedge \beta(\overline{n}_1, ..., \overline{n}_k, w, y, z))) \overset{\text{[0], [1], Rule E4, Conjunction Introduction}}{\Rightarrow}$
      $\vdash_{PA} \exists\, u\, \exists\, v\, (\exists\, w\, (\mathrm{Bt}(u, v, 0, w) \wedge \alpha(\overline{n}_1, ..., \overline{n}_k, w)) \wedge \mathrm{Bt}(u, v, 0, \overline{m}) \wedge$
      $\forall\, w\, (w < 0 \rightarrow \exists\, y\, \exists\, z\, (\mathrm{Bt}(u, v, w, y) \wedge \mathrm{Bt}(u, v, w', z) \wedge \beta(\overline{n}_1, ..., \overline{n}_k, w, y, z)))) \Rightarrow$
      $\vdash_{PA} \gamma(\overline{n}_1, ..., \overline{n}_k, 0, \overline{m})$.
  - Case $p > 0$
    - Given $i \in \{0, ..., p\}$, let $r_i := f(n_1, ..., n_k, i)$.
    - Lemma II $\Rightarrow$ there are $b, c \in \mathbb{N}$ such that for every $i \in \{0, ..., p\}$ $\boldsymbol{\beta}(b, c, i) = r_i$. [0]
    - Lemma I $\overset{[0]}{\Rightarrow}$ for every $i \in \{0, ..., p\}$ $\vdash_{PA} \mathrm{Bt}(\overline{b}, \overline{c}, \overline{i}, \overline{r}_i)$. [1]
    - [1] $\Rightarrow$ for every $i \in \{0, ..., p-1\}$ $\vdash_{PA} \mathrm{Bt}(\overline{b}, \overline{c}, \overline{i+1}, \overline{r}_{i+1})$. [2]
    - Given $i \in \{0, ..., p-1\}$, $r_{i+1} = f(n_1, ..., n_k, i+1) =$
      $h(n_1, ..., n_k, i, f(n_1, ..., n_k, i)) = h(n_1, ..., n_k, i, r_i) \overset{h \text{ is representable in } PA \text{ by } \beta}{\Rightarrow}$
      for every $i \in \{0, ..., p-1\}$ $\vdash_{PA} \beta(\overline{n}_1, ..., \overline{n}_k, \overline{i}, \overline{r}_i, \overline{r}_{i+1}) \overset{\text{[1], [2], Rule E4, Conjunction Introduction}}{\Rightarrow}$
      for every $i \in \{0, ..., p-1\}$
      $\vdash_{PA} \exists\, y\, \exists\, z\, (\mathrm{Bt}(\overline{b}, \overline{c}, \overline{i}, y) \wedge \mathrm{Bt}(\overline{b}, \overline{c}, \overline{i+1}, z) \wedge \beta(\overline{n}_1, ..., \overline{n}_k, \overline{i}, y, z)) \overset{\text{Lemma III}}{\Rightarrow}$
      for every $i \in \{0, ..., p-1\}$
      $\vdash_{PA} \forall\, w\, (w < \overline{p} \rightarrow \exists\, y\, \exists\, z\, (\mathrm{Bt}(\overline{b}, \overline{c}, w, y) \wedge \mathrm{Bt}(\overline{b}, \overline{c}, w', z) \wedge \beta(\overline{n}_1, ..., \overline{n}_k, w, y, z)))$. [3]
    - [0] $\Rightarrow \boldsymbol{\beta}(b, c, p) = r_p = f(n_1, ..., n_k, p) = m \overset{\text{Lemma I}}{\Rightarrow} \vdash_{PA} \mathrm{Bt}(\overline{b}, \overline{c}, \overline{p}, \overline{m})$. [4]
    - $r_0 = f(n_1, ..., n_k, 0) = g(n_1, ..., n_k) \overset{g \text{ is representable in } PA \text{ by } \alpha}{\Rightarrow} \vdash_{PA} \alpha(\overline{n}_1, ..., \overline{n}_k, \overline{r}_0) \overset{\text{[1], Rule E4, Conjunction Introduction}}{\Rightarrow}$
      $\vdash_{PA} \exists\, w\, (\mathrm{Bt}(\overline{b}, \overline{c}, 0, w) \wedge \alpha(\overline{n}_1, ..., \overline{n}_k, w)) \overset{\text{[3], [4], Rule E4, Conjunction Introduction}}{\Rightarrow}$
      $\vdash_{PA} \exists\, u\, \exists\, v\, (\exists\, w\, \mathrm{Bt}(u, v, 0, w) \wedge \alpha(\overline{n}_1, ..., \overline{n}_k, w)) \wedge \mathrm{Bt}(u, v, \overline{p}, \overline{m}) \wedge$
      $\forall\, w\, (w < \overline{p} \rightarrow \exists\, y\, \exists\, z\, (\mathrm{Bt}(u, v, w, y) \wedge \mathrm{Bt}(u, v, w', z) \wedge \beta(\overline{n}_1, ..., \overline{n}_k, w, y, z)))) \Rightarrow$
      $\vdash_{PA} \gamma(\overline{n}_1, ..., \overline{n}_k, \overline{p}, \overline{m})$.
- We must show that $\vdash_{PA} \exists!\, x_{k+2}\, \gamma(\overline{n}_1, ..., \overline{n}_k, \overline{p}, x_{k+2})$. Notice that, by what we have proved above, it suffices to prove only uniqueness. We will do it by induction on p.
  - Case 0
    Since $\gamma(\overline{n}_1, ..., \overline{n}_k, 0, x_{k+2})$ is $\exists\, u\, \exists\, v\, (\exists\, w\, (\mathrm{Bt}(u, v, 0, w) \wedge \alpha(\overline{n}_1, ..., \overline{n}_k, w)) \wedge \mathrm{Bt}(u, v, 0, x_{k+2}) \wedge \forall\, w\, (w < 0 \rightarrow \exists\, y\, \exists\, z\, (\mathrm{Bt}(u, v, w, y) \wedge \mathrm{Bt}(u, v, w', z) \wedge \beta(\overline{n}_1, ..., \overline{n}_k, w, y, z))))$, it suffices to prove uniqueness for $\exists!\, x_{k+2}\, \exists\, u\, \exists\, v\, \mathrm{Bt}(u, v, 0, x_{k+2})$, i.e. for $\exists!\, x_{k+2}\, \exists\, u\, \exists\, v\, \exists\, w\, (u = (\overline{1} + v) \cdot w + x_{k+2} \wedge x_{k+2} < \overline{1} + v)$, that can be easily obtained from the «translation» to PA of Euclidean division given in Chapter 2.
  - Case p
    Induction hypothesis. [IH]
  - Case $p+1$
    - $B := f(n_1, ..., n_k, p) \overset{f \text{ is representable in } PA \text{ by } \gamma}{\Rightarrow} \vdash_{PA} \gamma(\overline{n}_1, ..., \overline{n}_k, \overline{p}, \overline{B})$. [0]

· $C := f(n_1, ..., n_k, p+1) \overset{B=f(n_1,...,n_k,p)}{=} h(n_1, ..., n_k, p, B) \overset{h \text{ is representable in } PA \text{ by } \beta}{\Rightarrow}$
$\vdash_{PA} \beta(\overline{n}_1, ..., \overline{n}_k, \overline{p}, \overline{B}, \overline{C})$. [1]
· $C = f(n_1, ..., n_k, p+1) \overset{f \text{ is representable in } PA \text{ by } \gamma}{\Rightarrow} \vdash_{PA} \gamma(\overline{n}_1, ...\overline{n}_k, \overline{p+1}, \overline{C})$.
· Assume $\vdash_{PA} \gamma(\overline{n}_1, ..., \overline{n}_k, \overline{p+1}, x_{k+2})$. We must prove $x_{k+2} = \overline{C}$.
· Applying Rule C and Conjunction Elimination to $\vdash_{PA} \gamma(\overline{n}_1, ..., \overline{n}_k, \overline{p+1}, x_{k+2})$, we have that, for certain new constants b and c:
◇ $\vdash_{PA} \exists\, w\ (\mathrm{Bt}(b, c, 0, w) \wedge \alpha(\overline{n}_1, ..., \overline{n}_k, w))$. [2]
◇ $\vdash_{PA} \mathrm{Bt}(b, c, \overline{p+1}, x_{k+2})$. [3]
◇ $\vdash_{PA} \forall\, w\ (w < \overline{p+1} \to \exists\, y\ \exists\, z\ (\mathrm{Bt}(b, c, w, y) \wedge \mathrm{Bt}(b, c, w', z) \wedge \beta(\overline{n}_1, ..., \overline{n}_k, w, y, z)))$. [4]
· [4] $\overset{\text{(K4), MP}}{\Rightarrow} \vdash_{PA} \exists\, y\ \exists\, z\ (\mathrm{Bt}(b, c, \overline{p}, y) \wedge \mathrm{Bt}(b, c, \overline{p+1}, z) \wedge \beta(\overline{n}_1, ..., \overline{n}_k, \overline{p}, y, z)) \overset{\text{Rule C}}{\Rightarrow}$
For certain new constants d and e,
$\vdash_{PA} \mathrm{Bt}(b, c, \overline{p}, d) \wedge \mathrm{Bt}(b, c, \overline{p+1}, e) \wedge \beta(\overline{n}_1, ..., \overline{n}_k, \overline{p}, d, e)$. [5]
· [4] $\Rightarrow$
$\overset{\text{[2], [5], Rule E4, Conjunction Introduction}}{\Rightarrow}$
$\vdash_{PA} \forall\, w\ (w < \overline{p} \to \exists\, y \exists\, z\ (\mathrm{Bt}(b, c, w, y) \wedge \mathrm{Bt}(b, c, w', z) \wedge \beta(\overline{n}_1, ..., \overline{n}_k, w, y, z)))$
$\vdash_{PA} \exists\, u\ \exists\, v\ (\exists\, w\ (\mathrm{Bt}(u, v, 0, w) \wedge \alpha(\overline{n}_1, ..., \overline{n}_k, w)) \wedge \mathrm{Bt}(u, v, \overline{p}, d)\ \wedge$
$\forall\, w\ (w < \overline{p} \to \exists\, y\ \exists\, z\ (\mathrm{Bt}(u, v, w, y) \wedge \mathrm{Bt}(u, v, w', z) \wedge \beta(\overline{n}_1, ..., \overline{n}_k, w, y, z))))\ \Rightarrow$
$\vdash_{PA} \gamma(\overline{n}_1, ..., \overline{n}_k, \overline{p}, d) \overset{\text{[0], [IH]}}{\Rightarrow} d = \overline{B} \overset{[5]}{\Rightarrow}$
$\vdash_{PA} \mathrm{Bt}(b, c, \overline{p}, \overline{B}) \wedge \mathrm{Bt}(b, c, \overline{p+1}, e) \wedge \beta(\overline{n}_1, ..., \overline{n}_k, \overline{p}, \overline{B}, e) \overset{[1], h \text{ is representable in } PA \text{ by } \beta}{\Rightarrow} e = \overline{C} \overset{[5]}{\Rightarrow}$
$\vdash_{PA} \mathrm{Bt}(b, c, \overline{p+1}, \overline{C}) \overset{\text{[3], Lemma I}}{\Rightarrow} x_{k+2} = \overline{C}\ \Rightarrow \vdash_{PA} \exists!\, x_{k+2}\ \gamma(\overline{n}_1, ..., \overline{n}_k, \overline{p+1}, x_{k+2})$.

- Let $g(n_1, ..., n_{k+1})$ be representable in PA by a wff $\alpha(x_1, ..., x_{k+2})$ and such that, for every $n_1, ..., n_k \in \mathbb{N}$, there is $m \in \mathbb{N}$ such that $g(n_1, ..., n_k, m) = 0$.
Then μ_g is representable in PA by the wff $\alpha(x_1, ..., x_{k+1}, 0) \wedge \forall\, x_{k+2}\ (x_{k+2} < x_{k+1} \to \neg\alpha(x_1, ..., x_k, x_{k+2}, 0))$.
Indeed (let $n_1, ..., n_k, m \in \mathbb{N}$ such that $\mu_g(n_1, ..., n_k) = m$):
  - $\mu_g(n_1, ..., n_k) = m\ \Rightarrow\ \min\{k \in \mathbb{N} \mid g(n_1, ..., n_k, k) = 0\} = m \overset{\text{Lemma III}}{\Rightarrow}$
  $\vdash_{PA} \forall\, x_{k+2}\ (x_{k+2} < \overline{m} \to \neg\alpha(\overline{n}_1, ..., \overline{n}_k, x_{k+2}, 0)) \overset{g \text{ is representable in } PA \text{ by } \alpha}{\Rightarrow}$
  $\vdash_{PA} \alpha(\overline{n}_1, ..., \overline{n}_k, \overline{m}, 0) \wedge \forall\, x_{k+2}\ (x_{k+2} < \overline{m} \to \neg\alpha(\overline{n}_1, ..., \overline{n}_k, x_{k+2}, 0))$.
  - $\vdash_{PA} \exists!\, x_{k+1}\ (\alpha(\overline{n}_1, ..., \overline{n}_k, x_{k+1}, 0) \wedge \forall\, x_{k+2}\ (x_{k+2} < x_{k+1} \to \neg\alpha(\overline{n}_1, ..., \overline{n}_k, x_{k+2}, 0)))$.

□

Every recursive relation is expressible in PA. [4]

[4]

Proof
- Consider a recursive relation A of k arguments, and $n_1, ..., n_{k+1} \in \mathbb{N}$.
- A is recursive $\Rightarrow$ C_A is recursive $\overset{\text{Every recursive function is representable}}{\Rightarrow}$
C_A is representable in PA by a wff $\alpha(x_1, ..., x_{k+1})$, i.e.:
  - If $C_A(n_1, ..., n_k) = n_{k+1}, \vdash_{PA} \alpha(\overline{n}_1, ..., \overline{n}_{k+1})$. [1]
  - $\vdash_{PA} \exists!\, x_{k+1}\ \alpha(\overline{n}_1, ..., \overline{n}_k, x_{k+1})$. [2]
- Then, A is expressible in PA by $\alpha(x_1, ..., x_k, 0)$:
  - $\langle n_1, ..., n_k \rangle \in A\ \Rightarrow\ C_A(n_1, ..., n_k) = 0 \overset{[1]}{\Rightarrow} \vdash_{PA} \alpha(\overline{n}_1, ..., \overline{n}_k, 0)$.
  - $\langle n_1, ..., n_k \rangle \notin A\ \Rightarrow\ C_A(n_1, ..., n_k) = 1 \overset{[1]}{\Rightarrow} \vdash_{PA} \alpha(\overline{n}_1, ..., \overline{n}_k, \overline{1}) \overset{[2]}{\Rightarrow} \vdash_{PA} \neg\alpha(\overline{n}_1, ..., \overline{n}_k, 0)$.

□

[4] The converse is also true, see Corollary 3.29 of [Mendelson].

Chapter 4

Gödel's Incompleteness Theorem

4.1 Gödel numbers

We now pose a clever and seemingly unnatural question.

> Is it possible to «translate» propositions of logic into wffs of *PA*?

Yes, encoding such propositions using a function called **Gödel's arithmetization**. This technique will allow us to prove that *PA* is incomplete.

The function $\mathcal{G} : \{(,), , , \neg, \to, \forall\} \cup \{x_m, c_m, A^n_m, f^n_m\}_{m,n\in\mathbb{N}^+} \longrightarrow \mathbb{N}$ is called **Gödel's arithmetization**.

$$
\begin{aligned}
(,), , &\longmapsto 3, 5, 7\\
\neg, \to, \forall &\longmapsto 9, 11, 13\\
x_m, c_m &\longmapsto 7 + 8 \cdot m, 9 + 8 \cdot m\\
f^n_m, A^n_m &\longmapsto 11 + 8 \cdot 2^n \cdot 3^m, 13 + 8 \cdot 2^n \cdot 3^m
\end{aligned}
$$

And $\mathcal{G}(s)$ is called the **Gödel number** of s.

Notice that $\mathcal{G}$ is injective.

$\mathcal{G}$ can be extended in the following way, remaining injective:

- Given a string os symbols, we define $\mathcal{G}(s_1 \cdots s_r) := p(0)^{\mathcal{G}(a_0)} \cdot ... \cdot p(r)^{\mathcal{G}(a_r)}$.
- Given a sequence of strings of symbols $\alpha_0, ..., \alpha_r$, we define $\mathcal{G}(\alpha_1 \cdots \alpha_r) := p(0)^{\mathcal{G}(\alpha_0)} \cdot ... \cdot p(r)^{\mathcal{G}(\alpha_r)}$.

For example, $\mathcal{G}(x_1 = x_3 \to A^1_1(x_3 \cdot x_2)) = \mathcal{G}(A^2_1(x_1, x_3) \to A^1_1(f^2_2(x_3, x_2))) =$
$p(0)^{\mathcal{G}(()} \cdot p(1)^{\mathcal{G}(A^2_1)} \cdot p(2)^{\mathcal{G}(()} \cdot p(3)^{\mathcal{G}(x_1)} \cdot p(4)^{\mathcal{G}(,)} \cdot p(5)^{\mathcal{G}(x_3)} \cdot p(6)^{\mathcal{G}())} \cdot p(7)^{\mathcal{G}(\to)} \cdot p(8)^{\mathcal{G}(A^1_1)} \cdot p(9)^{\mathcal{G}(()} \cdot p(10)^{\mathcal{G}(f^2_2)} \cdot p(11)^{\mathcal{G}(()} \cdot p(12)^{\mathcal{G}(x_3)} \cdot p(13)^{\mathcal{G}(,)} \cdot p(14)^{\mathcal{G}(x_2)} \cdot p(15)^{\mathcal{G}())} \cdot p(16)^{\mathcal{G}())} \cdot p(17)^{\mathcal{G}())} =$
$2^3 \cdot 3^{13+8\cdot 2^2\cdot 3^1} \cdot 5^3 \cdot 7^{7+8\cdot 1} \cdot 11^7 \cdot 13^{7+8\cdot 3} \cdot 17^5 \cdot 19^{11} \cdot 23^{13+8\cdot 2^1\cdot 3^1} \cdot 29^3 \cdot 31^{11+8\cdot 2^2\cdot 3^2} \cdot 37^3 \cdot 41^{7+8\cdot 3} \cdot 43^7 \cdot 47^{7+8\cdot 2} \cdot 53^5 \cdot 59^5 \cdot 61^5$.

This method of associating numbers with symbols, strings of symbols and sequences of strings of symbols was devised by Gödel in order to arithmetize metamatemathics, i.e. to replace assertions about a formal system by equivalent number-theoretic statements, and then to express these statements within the formal system itself.

The following number-theoretic functions and relations (which are understood to be about *PA*, although many of them are stated in a more general way) are recursive:

1. IC(n), that holds iff n is the Gödel number of a constant.
2. FL(n), that holds iff n is the Gödel number of a function letter.
3. PL(n), that holds iff n is the Gödel number of a predicate letter.

4. EVbl(n), that holds iff n is the Gödel number of a string consisting of a variable.
5. EIC(n), that holds iff n is the Gödel number of a string consisting of a constant.
6. EFL(n), that holds iff n is the Gödel number of a string consisting of a function letter.
7. EPL(n), that holds iff n is the Gödel number of a string consisting of a predicate letter.
8. $\mathrm{Arg_T}(n) := (\mathrm{qt}(8, n \dot{-} 11))_0$ (notice that $\mathrm{Arg_T}(\mathcal{G}(f^n_m)) = n$).
9. $\mathrm{Arg_P}(n) := (\mathrm{qt}(8, n \dot{-} 13))_0$ (notice that $\mathrm{Arg_P}(\mathcal{G}(A^n_m)) = n$).
10. Gd(n), that holds iff n is the Gödel number of a string of symbols of $\{(,), , , \neg, \rightarrow, \forall\} \cup \{x_m, c_m, A^p_m, f^p_m\}_{m,p \in \mathbb{N}^+}$.
11. MP(m, n, p), that holds iff there are strings α and β such that $m = \mathcal{G}(\alpha)$, $n = \mathcal{G}(\alpha \rightarrow \beta)$ and $p = \mathcal{G}(\beta)$.
12. Gen(m, n), that holds iff there is a string α such that there is $i \in \mathbb{N}^+$ such that $m = \mathcal{G}(\alpha)$ and $n = \mathcal{G}(\forall\, x_i\ \alpha)$.
13. Trm(n), that holds iff n is the Gödel number of a term.
14. Atmfl(n), that holds iff n is the Gödel number of an atomic formula.
15. Fml(n), that holds iff n is the Gödel number of a wff.
16. Subst(m, n, p, q), that holds iff m is the Gödel number of $\alpha^{x_r}_t$, with α a wff with Gödel number n, x_r a variable with Gödel number q and t a term with Gödel number p.
17. Sub(n, p, q), the Gödel number of $\alpha^{x_r}_t$, with α a wff with Gödel number n, x_r a variable with Gödel number q and t a term with Gödel number p.
18. FrI(m, n), that holds iff m is the Gödel number of a term that contains (at least) one occurrence of the variable with Gödel number n.
19. FrII(m, n), that holds iff m is the Gödel number of a wff that contains (at least) one free occurrence of the variable with Gödel number n.
20. Ff(m, n, p), that holds iff m is the Gödel number of a term free for the variable with Gödel number n in the wff with Gödel number p.
21. Given $i \in \{1, ..., 5\}$, $\mathrm{Ax}_i(n)$, that holds iff n is the Gödel number of an instance of axiom schema (Ki).
22. LAx(n), that holds iff n is the Gödel number of a logical axiom.
23. EAx(n), that holds iff n is the Gödel number of an axiom for equality.
24. PrAx(n), that holds iff n is the Gödel number of a proper axiom of *PA*.
25. Ax(n), that holds iff n is the Gödel number of an axiom of *PA*.
26. $\mathrm{Neg}(n) := 2^9 * n$ (notice that $\mathrm{Neg}(\mathcal{G}(\alpha)) = \mathcal{G}(\neg\alpha)$).
27. $\mathrm{Cond}(m, n) := 2^3 * m * 2^{11} * n * 2^5$ (notice that $\mathrm{Cond}(\mathcal{G}(\alpha), \mathcal{G}(\beta)) = \mathcal{G}((\alpha \rightarrow \beta))$).
28. Clos(n), the Gödel number of the closure of the wff with Gödel number n.
29. Num(n), the Gödel number of the numeral $\overline{n}$.
30. Nu(n), that holds iff n is the Gödel number of a numeral.
31. **(Diagonal function)** D(n), the Gödel number of $\alpha^{x_1}_{\overline{n}}$, with α a wff with Gödel number n.
32. Prf(n), that holds iff n is the Gödel number of a proof in *PA*.
33. Pf(m, n), that holds iff m is the Gödel number of a proof in *PA* of the wff with Gödel number n.

Proof

(We only prove some of them, in order to give an idea, see Propositions 3.25, 3.26 and 3.27 of [Mendelson]).

1. IC(n) is $\exists\, m_{m<n}\ (1 \leqslant m \wedge n = \mathcal{G}(c_m))$.
2. FL(n) is $\exists\, p_{p<n}\ (1 \leqslant p \wedge \exists\, m_{m<n}\ (1 \leqslant m \wedge n = \mathcal{G}(f^p_m)))$.
3. PL(n) is $\exists\, p_{p<n}\ (1 \leqslant p \wedge \exists\, m_{m<n}\ (1 \leqslant m \wedge n = \mathcal{G}(A^p_m)))$.
4. EVbl(n) is $\exists\, m_{m<n}\ (1 \leqslant m \wedge n = 2^{\mathcal{G}(x_m)})$.
5. EIC(n) is $\exists\, m_{m<n}\ (\mathrm{IC}(m) \wedge n = 2^m)$.
6. EFL(n) is $\exists\, m_{m<n}\ (\mathrm{FL}(m) \wedge n = 2^m)$.
7. EPL(n) is $\exists\, m_{m<n}\ (\mathrm{PL}(m) \wedge n = 2^m)$.
10. Gd(n) is $2^{\mathcal{G}(()} \vee 2^{\mathcal{G}())} \vee 2^{\mathcal{G}(,)} \vee 2^{\mathcal{G}(\neg)} \vee 2^{\mathcal{G}(\rightarrow)} \vee 2^{\mathcal{G}(\forall)} \vee \mathrm{EVbl}(n) \vee \mathrm{EIC}(n) \vee \mathrm{EFL}(n) \vee \mathrm{EPL}(n) \vee$ $\exists\, m_{m<n}\ \exists\, p_{p<n}\ (\mathrm{Gd}(m) \wedge \mathrm{Gd}(p) \wedge m * p = n)$. Notice that here we are using course-of-values recursion.
16. Subst(m, n, p, q) is $\mathrm{Fml}(n) \wedge \mathrm{Trm}(p) \wedge \mathrm{EVbl}(2^q) \wedge ($ $(n = 2^q \wedge m = p) \vee$

$\exists\ w_{w<n}\ (n = 2^w \wedge n \neq 2^q \wedge m = n)\vee$
$\exists\ z_{z<n}\ \exists\ w_{w<n}\ ($
$\quad \mathrm{Fml}(w)\wedge$
$\quad n = 2^{\mathcal{G}(\forall)} * 2^q * w * z\wedge$
$\quad \exists\ a_{a<m}\ (m = 2^{\mathcal{G}(\forall)} * 2^q * w * a \wedge \mathrm{Subst}(a, z, p, q)))\vee$
$(\neg\exists\ z_{z<n}\ \exists\ w_{w<n}\ (\mathrm{Fml}(w) \wedge n = 2^{\mathcal{G}(\forall)} * 2^q * w * z)\wedge$
$\exists\ a_{a<m}\ \exists\ b_{b<m}\ \exists\ z_{z<n}\ ($
$\quad 1 < z\wedge$
$\quad n = 2^{(n)_0} * z\wedge$
$\quad x = a * b\wedge$
$\quad \mathrm{Subst}(a, 2^{(n)_0}, p, q)\wedge$
$\quad \mathrm{Subst}(b, z, p, q))))$.

Notice that we are using course-of-values recursion again.

17. $\mathrm{Sub}(n, p, q)$ is $\mu\ m_{m<(p(n\cdot p)!)^{n\cdot p}}\ \mathrm{Subst}(m, n, p, q)$.
19. $\mathrm{FrII}(m, n) = \mathrm{Fml}(m) \wedge \mathrm{EVbl}(2^n) \wedge \neg\mathrm{Subst}(m, m, 2^{\mathcal{G}(x_n)}, n)$ (that is, substitution in the wff with Gödel number m of a variable different from the variable with Gödel number n yields a different wff).
21. (Case of Ax_4). $\mathrm{Ax}_4(n) = \exists\ m_{m<n}\ \exists\ p_{p<n}\ \exists\ q_{q<n}\ (\mathrm{Fml}(m) \wedge \mathrm{Trm}(p) \wedge \mathrm{EVbl}(2^q) \wedge \mathrm{Ff}(p, q, m)\wedge$ $n = 2^{\mathcal{G}(()} * 2^{\mathcal{G}(\forall)} * 2^{\mathcal{G}(()} * 2^q * m * 2^{\mathcal{G}())} * 2^{\mathcal{G}(\to)} * \mathrm{Sub}(m, p, q) * 2^{\mathcal{G}(()}$).
23. $\mathrm{LAx}(n) = \mathrm{Ax}_1(n) \vee ... \vee \mathrm{Ax}_5(n)$.
30. $\mathrm{Nu}(n) = \exists\ m_{m<n}\ n = \mathrm{Num}(m)$.
31. $\mathrm{D}(n) = \mathrm{Sub}(n, \mathrm{Num}(n), \mathcal{G}(x_1))$.
32. $\mathrm{Prf}(n)$ is $\exists\ m_{m<n}\ \exists\ p_{p<n}\ \exists\ q_{q<n}\ \exists\ r_{r<n}\ ($
$\quad (n = 2^r \wedge \mathrm{Ax}(r))\vee$
$\quad (\mathrm{Prf}(m) \wedge \mathrm{Fml}((m)_r) \wedge n = m * 2^p \wedge \mathrm{Gen}((m)_r, p))\vee$
$\quad (\mathrm{Prf}(m) \wedge \mathrm{Fml}((m)_q) \wedge \mathrm{Fml}((m)_r) \wedge n = m * 2^p \wedge \mathrm{MP}((m)_q, (m)_r, p))\vee$
$\quad (\mathrm{Prf}(m) \wedge n = m * 2^p \wedge \mathrm{Ax}(p)))$.
33. $\mathrm{Pf}(m, n)$ is $\mathrm{Prf}(m) \wedge n = (m)_{l(m)}$.

□

4.2 Gödel's Incompleteness Theorem

The following result is known as the **Fixed Point Theorem**: given a wff α of *PA* which contains (at least) one free occurrence of x_1, and in which x_1 is the only free variable, there is a sentence S such that $\vdash_{PA}\ \alpha(\overline{s}) \leftrightarrow S$, where $s = \mathcal{G}(S)$.

Proof

- D is recursive, so D is representable in *PA* by a wff $D(x_1, x_2)$.
- Let m be the Gödel number of the wff $\forall\ x_2\ (D(x_1, x_2) \rightarrow\ \alpha(x_2))$, S the wff $\forall\ x_2\ (D(\overline{m}, x_2) \rightarrow\ \alpha(x_2))$, and s the Gödel number of S.
- It is clear that $\mathrm{D}(m) = s$.
- Hence, $\vdash_{PA}\ D(\overline{m}, \overline{s})$, since $D(x_1, x_2)$ represents D.
- $\alpha(x_2)$ is deducible in *PA* from $\{\alpha(\overline{s}), D(\overline{m}, x_2)\}$:

(1)	$\alpha(\overline{s})$	Hypothesis
(2)	$D(\overline{m}, x_2)$	Hypothesis
(3)	$\exists!\ x_2\ D(\overline{m}, x_2)$	$D(x_1, x_2)$ represents D
(4)	$x_2 = \overline{s}$	(3), $D(\overline{m}, \overline{s})$, Basic properties of $=$
(5)	$\alpha(x_2)$	(1), (4), Basic properties of $=$

- Applying Gen and Deduction Theorem, $\forall\ x_2\ D(\overline{m}, x_2) \rightarrow \alpha(x_2)$ is deducible in *PA* from $\{\alpha(\overline{s})\}$
- Applying the Deduction Theorem, $\vdash_{PA}\ \alpha(\overline{s}) \rightarrow (\forall\ x_2\ D(\overline{m}, x_2) \rightarrow \alpha(x_2))$, i.e. $\vdash_{PA}\ \alpha(\overline{s}) \rightarrow S$.
- $\alpha(\overline{s})$ is deducible in *PA* from $\{S\}$:

(1)	S (i.e., $\forall\, x_2\ (D(\overline{m}, x_2) \rightarrow\ \alpha(x_2))$)	Hypothesis
(2)	$\forall\, x_2\ (D(\overline{m}, x_2) \rightarrow\ \alpha(x_2)) \rightarrow (D(\overline{m}, \overline{s}) \rightarrow\ \alpha(\overline{s}))$	(K4)
(3)	$D(\overline{m}, \overline{s}) \rightarrow\ \alpha(\overline{s})$	MP$(1, 2)$
(4)	$\alpha(\overline{s})$	MP$(D(\overline{m}, \overline{s}), 3)$

- Applying the Deduction Theorem, $\vdash_{PA}\ S \rightarrow \alpha(\overline{s})$.
- Therefore, applying Biconditional Introduction Rule, $\vdash_{PA}\ \alpha(\overline{s}) \leftrightarrow S$.

□

Now we can finally prove **Gödel's Incompleteness Theorem**: PA is incomplete.

Proof [1]

- Pf is recursive, so Pf is expressible in PA by a wff $Pf(x_1, x_2)$.
- Consider the wff $\forall\, x_2\ \neg Pf(x_2, x_1)$.
- By the Fixed Point Theorem, there is a sentence G, the **Gödel sentence**, with Gödel number q, and such that $\vdash_{PA}\ G \leftrightarrow \forall\, x_2\ \neg Pf(x_2, \overline{q})$.
- $\nvdash_{PA}\ G$:
  - Assume that $\vdash_{PA}\ G$ and let r be the Gödel number of a proof in PA of G.
  - $\vdash_{PA}\ G\ \Rightarrow\ \mathrm{Pf}(r, q)$ holds $\overset{Pf \text{ expresses Pf}}{\Rightarrow} \vdash_{PA}\ Pf(\overline{r}, \overline{q})$. [1]
  - $\left\{ \begin{array}{c} \vdash_{PA}\ G \leftrightarrow \forall\, x_2\ \neg Pf(x_2, \overline{q}) \\ \vdash_{PA}\ G \\ \text{Biconditional Elimination} \end{array} \right\} \Rightarrow \vdash_{PA}\ \forall\, x_2\ \neg Pf(x_2, \overline{q}) \overset{\text{(K4), MP}}{\Rightarrow} \vdash_{PA}\ \neg Pf(\overline{r}, \overline{q}) \overset{[1]}{\Rightarrow}$
    PA is inconsistent, a contradiction.
- $\nvdash_{PA}\ \neg G$:
  - Assume that $\vdash_{PA}\ \neg G$. Since we are assuming that PA is consistent, $\nvdash_{PA}\ G$.
  - $\left\{ \begin{array}{c} \vdash_{PA}\ G \leftrightarrow \forall\, x_2\ \neg Pf(x_2, \overline{q}) \\ \vdash_{PA}\ \neg G \\ \text{Biconditional Elimination} \end{array} \right\} \Rightarrow \vdash_{PA}\ \neg\forall\, x_2\ \neg Pf(x_2, \overline{q})\ \Rightarrow \vdash_{PA}\ \exists\, x_2\ Pf(x_2, \overline{q})$.
  - $\nvdash_{PA}\ G\ \Rightarrow$ There is no proof in PA of $G\ \Rightarrow$ Given $n \in \mathbb{N}, \langle n, q\rangle \notin \mathrm{Pf}\ \Rightarrow$
    Given $n \in \mathbb{N}, \vdash_{PA}\ \neg Pf(\overline{n}, \overline{q})\ \overset{PA \text{ is } \omega\text{-consistent}}{\Rightarrow} \nvdash_{PA}\ \exists\, x_2\ Pf(x_2, \overline{q})$, a contradiction.
    PA is inconsistent. Contradiction.
- Therefore, PA is incomplete.

□

Notice that, in terms of the standard interpretation, $\forall\, x_2\ \neg Pf(x_2, \overline{q})$ says that there is no natural number that is the Gödel number of a proof in PA of the wff G, i.e. that G is unprovable in PA. In other words, G says «I am not provable in PA». This is an analogue of the **Liar Paradox**: «I am lying» (i.e. «I am not true»). However, although the Liar Paradox leads to a contradiction, Gödel showed that G is an undecidable sentence of PA.

4.3 Gödel's Second Theorem

Thanks to Gödel's Incompleteness Theorem, we know that there are unprovable «arithmetical truths». Is consistency of PA one of them?

First, notice that, since Neg and Pf are recursive, Neg is representable in PA by a wff $Neg(x_1, x_2)$ and Pf is expressible in PA by a wff $Pf(x_1, x_2)$. Now let Con(PA) be the sentence $\forall\, x_1\ \forall\, x_2\ \forall\, x_3\ \forall\, x_4\ \neg(Pf(x_1, x_3) \wedge Pf(x_2, x_4) \wedge Neg(x_3, x_4))$, which asserts (in the standard interpretation) that there are no proofs in PA of a wff and its negation, i.e. that PA is consistent.

[1] For this proof, we use consistency and ω-consistency of PA, but there is another proof, due to Rosser, that uses only the consistency of PA. see Proposition 3.36 of [Mendelson].

We have **Gödel's Second Theorem**: $\mathrm{Con}(PA)$ is unprovable in PA, i.e. PA can not prove its own consistency (see Proposition 3.40 of [Mendelson]).

4.4 Church's Thesis

Church's Thesis is a definition of «algorithm», that can be stated as «to solve algorithmically a problem is equivalent to find a recursive relation which models such problem», or simply «'algorithmic' is equivalent to 'recursive'».

Keeping this idea, given an extension E of PA:

- E is a **axiomatic** iff $\{n \in \mathbb{N} \mid \text{there is an axiom } \alpha \text{ of } E \text{ such that } n = \mathcal{G}(\alpha)\}$ is recursive.
  Notice that:
  - Assuming Church's thesis, E is axiomatic iff it is possible to define an algorithm which can decide if a wff is an axiom of E.
  - PA is axiomatic, since PrAx is recursive.
- E is **algorithmically axiomatizable** iff there is an axiomatic extension F of PA such that the theorems of F are exactly the theorems of E.
  It is clear that every axiomatic extension is algorithmically axiomatizable, it suffices to assume $F := E$.
- E is **recursively decidable** iff $\{n \in \mathbb{N} \mid \text{there is a theorem } \alpha \text{ of } E \text{ such that } n = \mathcal{G}(\alpha)\}$ is recursive.
  Notice that:
  - Assuming Church's thesis, E is recursively decidable iff it is possible to find an algorithm which can decide whether a sentence is a theorem of E.
  - It is clear that if E is recursively decidable, E is axiomatic.

Why we said that the answer to the *Entscheidungsproblem* is negative?

The reason is **Church's Theorem**: $K_{\mathscr{L}}$ is not recursively decidable (see Proposition 3.52 of [Mendelson]).

Is PA recursively decidable?

No, PA is not recursively decidable.

Proof

- Let T_{PA} be the set of Gödel numbers of theorems of PA.
- T_{PA} is not expressible in PA. Indeed:
  - Assume that T_{PA} is expressible in PA by a wff $\tau(x_1)$.
  - By the Fixed Point Theorem, there is a sentence S such that $\vdash_{PA} S \leftrightarrow \neg\tau(\overline{\mathcal{G}(S)})$.
    - Case $\vdash_{PA} S$
      - $\vdash_{PA} S \Rightarrow \mathcal{G}(S) \in T_{PA} \overset{\tau \text{ expresses } T_{PA}}{\Rightarrow} \vdash_{PA} \tau(\overline{\mathcal{G}(S)})$. [1]
      - $\left\{ \begin{array}{c} \vdash_{PA} S \leftrightarrow \neg\tau(\overline{\mathcal{G}(S)}) \\ \vdash_{PA} S \\ \text{Biconditional Elimination} \end{array} \right\} \Rightarrow \vdash_{PA} \neg\tau(\overline{\mathcal{G}(S)}) \overset{[1]}{\Rightarrow} PA$ is inconsistent, a contradiction.
    - Case $\nvdash_{PA} S$
      - $\nvdash_{PA} S \Rightarrow \mathcal{G}(S) \notin T_{PA} \overset{\tau \text{ expresses } T_{PA}}{\Rightarrow} \vdash_{PA} \neg\tau(\overline{\mathcal{G}(S)}) \overset{\left\{ \begin{array}{c} \vdash_{PA} S \leftrightarrow \neg\tau(\overline{\mathcal{G}(S)}) \\ \text{Biconditional Elimination} \end{array} \right\}}{\Rightarrow} \vdash_{PA} S$, a contradiction.

- Thus, T_{PA} is not recursive, since every recursive relation is expressible in PA.

□

As we said before, $\mathscr{V}$ is useless, impracticable, since $\mathscr{V}$ is not recursively axiomatizable: if it were, then the same reasoning used in Gödel's Incompleteness Theorem would lead us to the conclusion that $\mathscr{V}$ is incomplete, which is a contradiction.

Therefore, assuming Church Thesis, it is impossible to find an algorithm which can decide whether a given sentence of arithmetic is true or not.

Bibliography

[Amor] José Alfredo Amor Montaño, *Inducción y Recursión* (in Spanish), Miscelánea Matemática, Sociedad Matemática Mexicana, 1997, `http://www.miscelaneamatematica.org/Misc26/amor.pdf`.

[Burris & Sankappanavar] Stanley N. Burris and H.P. Sankappanavar, *A Course in Universal Algebra*, 2012, `http://www.math.uwaterloo.ca/~snburris/htdocs/UALG/univ-algebra2012.pdf`.

[Hamilton] Alan G. Hamilton, *Logic for Mathematicians*, Cambridge University Press, 1978.

[Mendelson] Elliot Mendelson, *Introduction to Mathematical Logic*, Third Edition, Queens College of the City University of New York, 1987.

[Rasiowa] Helena Rasiowa, *An algebraic approach to non-classical logics*. American Elsevier Publishing Company, 1974.