University of Zürich
Institute of Mathematics

Master Thesis

# A Complete Proof of Incompleteness

*Author:*
Regula Krapf

*Supervisor:*
Dr. Lorenz Halbeisen

December 3, 2014

# Acknowledgement

Several People have made it possible for me to complete this thesis. On general, I would like to acknowledge the support which has been offered to me from the Institute of Mathematics, University of Zürich. In particular, I would like to express my gratitude to my supervisor Dr. Lorenz Halbeisen for his advice and the inspiring discussions about logic and philosophy.

Furthermore, I would like to thank my friends and fellow students Noam Arnold, Patrik Lengacher, Andreas Scheuss and Yannick Widmer for looking closely at my thesis and offering suggestions for improvement.

Last but not least, I would like show gratitude to my family and friends for their patience and moral support.

# Contents

# Chapter 1

# Introduction

## Peano Arithmetic and its Consistency

Peano Arithmetic (PA) is intended to be an axiomatization of the natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$. However, the Incompleteness Theorems proved by Kurt Gödel state that PA is incomplete and unable to prove its own consistency. More concretely, the First Incompleteness Theorem states that there is a sentence in the language of PA which can neither be proven nor disproven and the meaning of the Second Incompleteness Theorem is that within PA it is impossible to show that no contradiction can be derived from the Peano Axioms. In fact, the same statements still hold for any extension of PA which can be axiomatized using a finite number of axioms or axiom schemas. In order to prove this, however, it is necessary to formalize the concepts of "proofs" and "consistency"within PA which requires much work; for example, it includes the introduction of a function which allows the encoding of finite sequences.

There are numerous proofs or hints for proofs to be found in the literature. However, often many crucial details are omitted. Furthermore, the proofs of the Incompleteness Theorems, and in particular that of the Second Incompleteness Theorem, are commonly based on the theory of primitive recursive functions. The aim of this thesis is to present a detailed and complete proof of both Incompleteness Theorems that does not make use of recursion theory.

The fundamental question which arises in conjunction with the Incompleteness Theorems is that of the consistency of Peano Arithmetic. The basic number theoretical results which are shown in the first chapter, do not presuppose the consistency of PA. Nonetheless, the encoding of terms, formulas and proofs within PA (the so-called gödelization) which is the topic of the second chapter, requires the existence of a model of PA consisting only of finite numbers, i.e. a set of natural numbers which is considered the standard model of Peano Arithmetic.

However, the mere concept of models requires some naive mathematical background in which a notion of "sets" is given. Therefore, the desired standard model of Peano Arithmetic is to be a naive set in this mathematical background. The question that arises in this context is what exactly is a naive set of natural numbers. A possible solution of this problem is the following:

We consider our set to be the set of strings $\mathbb{S} = \{\varepsilon, |, ||, |||, \dots\}$ where $\varepsilon$ is the empty string, and each element is thus either the empty string or a string containing only the symbol $|$. This naive set allows a natural definition of

- a successor function which adds simply another $|$ to the string,
- an operation representing addition which simply concatenates both strings,
- an operation representing multiplication in the following way: Given $s, s' \in \mathbb{S}$, a new string $s''$ is constructed which is at first the empty string and for each occurrence of $|$ in the string $s$, the string $s'$ is added to the string $s''$ (while eliminating the symbol $|$ in the string $s$). This is repeated until the string $s$ becomes the empty string and the result is thus $s''$.

It is obvious that these naive operations are equivalent to our intuitive conception of addition and multiplication of natural numbers. However, the operations on the string set $\mathbb{S}$ describe simply a recipe of how to draw a new strings from given ones and thus do not actually presuppose a mathematical notion of arithmetic.

Moreover, the operations on $\mathbb{S}$ allow the definition of new functions and relations just in the same way as in the set of natural numbers, e.g. for $s, s' \in \mathbb{S}$ we can say that $s < s'$, if for each occurrence of $|$ in the string $s$ we can eliminate a copy of $|$ in $s'$ and the result is not the empty string. The result can then be defined as $s' - s$.

On the other hand, the solution presented above can immediately be identified with the set $\mathbb{N}$ by considering the numbers $1, 2$ and so on to be names of strings and in particular the empty string can be identified with 0. As we are more acquainted with arithmetic in the naive set $\mathbb{N}$ equipped with the "usual" addition $+$, multiplication $\cdot$ and successor function given by $\mathrm{s}(n) = n + 1$ for any $n \in \mathbb{N}$, we will henceforth work with $\mathbb{N}$ rather than $\mathbb{S}$. In $\mathbb{N}$ we can define functions and relations such as $\leq$, prime, $-$ (where $-$ is the subtraction that rounds up to zero).

To sum up, the problem of naive set theory remains. However, the following paper is neither able nor intended to tackle this rather philosophical question. From now on, we will accept the existence of a naive standard model.

# Outline

The first chapter is devoted to the proof of basic results of number theory in Peano Arithmetic. The intuition behind these formalized proofs corresponds to the "usual"proofs commonly known from the natural numbers. Therefore, in order to understand the Incompleteness Theorems, it is possible to start with Chapter 2 whose goal is to define new functions and relations in PA which, for example, formalize the concept of formulas and provabilty. The next chapter encompasses the actual proof of the First and Second Imcompleteness Theorems, and in particular the so-called Derivability Conditions which state e.g. that if a formula is provable, then one can prove its provability within PA. Last but not least, we will study Presburger Arithmetic which is similar to Peano Arithmetic but is only concerned with addition and the successor function. This theory, in contrast to PA, will be shown to be complete.

## Conventions and Notations

Basic concepts of mathematical logic such as presented in [Rau08] are presumed. The logical axioms and the inference rules as well as the tautologies that this thesis is based upon, can be found in the Appendices. The tautologies are numbered by the alphabet, while equations are represented by numbers. Numbering is always done on the right hand side, while on the left hand side the previous results, which are applied, are cited.

For the sake of simplicity, we will use the notation $\varphi_1, \ldots, \varphi_n \vdash \psi$ instead of $\{\varphi_1, \ldots, \varphi_n\} \vdash \psi$ for any formulas $\varphi_1, \ldots, \varphi_n, \psi$. Moreover, for a set of formulas $T$ and a formula $\varphi$ the notation $\vdash_T \varphi$ is an abbreviation for $T \vdash \varphi$.

If $\varphi$ is a formula with $n$ free variables $x_1, \ldots, x_n$ we write $\varphi(\vec{x})$ instead of $\varphi(x_1, \ldots, x_n)$. Furthermore, $\mathrm{var}(\varphi)$ denotes the set of all variables occurring in $\varphi$ and likewise $\mathrm{free}(\varphi)$ is the set of the free variables of $\varphi$.

For functions $f$ and relations $R$ which are defined in PA, we generally denote the corresponding symbols in $\mathbb{N}$ by $f^{\mathbb{N}}$ respectively $R^{\mathbb{N}}$. If it is clear whether the symbol forms part of the formal language or not, this distinction will be given up.

# Chapter 2

# Basic number theory in Peano Arithmetic

In this first chapter, we will derive basic number theoretical results in Peano Arithmetic which are necessary to prove the Incompleteness Theorems. These include for example Bézout's Lemma and the Chinese Remainder Theorem.

## 2.1 Peano Arithmetic

**Definition 2.1.** The language of Peano Arithmetic is given by $\mathcal{L}_{\mathrm{PA}} = \{\mathbf{0}, \mathbf{S}, +, \cdot\}$, where $\mathbf{0}$ is a symbol for a constant, $\mathbf{S}$ a unary function symbol and $+$ and $\cdot$ are binary function symbols. We abbreviate the term $\mathbf{S0}$ as $\underline{1}$.

**Definition 2.2.** Peano Arithmetic consists of the following axioms and axiom schema:

($\mathrm{PA}_1$) $\forall x \neg(\mathbf{S}x = \mathbf{0})$,

($\mathrm{PA}_2$) $\forall x \forall y(\mathbf{S}x = \mathbf{S}y \to x = y)$,

($\mathrm{PA}_3$) $\forall x(x + \mathbf{0} = x)$,

($\mathrm{PA}_4$) $\forall x \forall y(x + \mathbf{S}y = \mathbf{S}(x + y))$,

($\mathrm{PA}_5$) $\forall x(x \cdot \mathbf{0} = \mathbf{0})$,

($\mathrm{PA}_6$) $\forall x \forall y(x \cdot \mathbf{S}y = (x \cdot y) + x)$.

If $\varphi = \varphi(x, \vec{y})$ is a formula with $\mathrm{free}(\varphi) = \{x, y_0, \ldots, y_n\}$, we denote by ($\mathrm{I}_\varphi$) the following axiom schema, called the induction schema:

$$(\mathrm{I}_\varphi) \quad \forall \vec{y}\big[\varphi(\mathbf{0}, \vec{y}) \wedge \forall x\big(\varphi(x, \vec{y}) \to \varphi(\mathbf{S}x, \vec{y})\big) \to \forall x \varphi(x, \vec{y})\big].$$

Now we are able to verify standard rules of arithmetic such as commutativity and associativity of addition and multiplication.

While proving, we will make use of ($\mathrm{L}_{12}$), ($\mathrm{L}_{16}$) – ($\mathrm{L}_{18}$) without explicitly mentioning them every time.

**Lemma 2.3.** $\vdash_{\mathrm{PA}} \forall x \forall y (x + y = y + x)$.

*Proof.* We will use induction on $x$ to show $\vdash_{\mathrm{PA}} \forall y (x + y = y + x)$; then the claim follows from $(\forall)$.

For this, we need to prove first

(1) $\vdash_{\mathrm{PA}} \forall x (\mathbf{0} + x = x)$

(2) $\vdash_{\mathrm{PA}} \forall x \forall y (\mathbf{S}(x + y) = \mathbf{S}x + y)$.

We show both assertions by induction; the first one by induction on $x$, the second one by induction on $y$. The base case of (1) follows directly from $(\mathrm{PA}_3)$. The induction step is a consequence of

$$\mathbf{0} + x = x \vdash_{\mathrm{PA}} \mathbf{0} + \mathbf{S}x \overset{(\mathrm{PA}_4)}{=} \mathbf{S}(\mathbf{0} + x) = \mathbf{S}x$$

and (DT). Now we prove (2). For $y = \mathbf{0}$ we have $\vdash_{\mathrm{PA}} \mathbf{S}(x + \mathbf{0}) \overset{(\mathrm{PA}_3)}{=} \mathbf{S}x \overset{(\mathrm{PA}_3)}{=} \mathbf{S}x + \mathbf{0}$. The induction step follows from

$$\mathbf{S}(x + y) = \mathbf{S}x + y \vdash_{\mathrm{PA}} \mathbf{S}(x + \mathbf{S}y) \overset{(\mathrm{PA}_4)}{=} \mathbf{S}(\mathbf{S}(x + y)) = \mathbf{S}(\mathbf{S}x + y) \overset{(\mathrm{PA}_4)}{=} \mathbf{S}x + \mathbf{S}y$$

using (DT) and $(\forall)$. Finally, we are able to show the claim. We get the base case using (1), $(\mathrm{PA}_1)$ and generalization: $\vdash_{\mathrm{PA}} \mathbf{0} + y = y = y + \mathbf{0}$. The induction step is a consequence of

$$x + y = y + x \vdash_{\mathrm{PA}} \mathbf{S}x + y \overset{(2)}{=} \mathbf{S}(x + y) = \mathbf{S}(y + x) \overset{(\mathrm{PA}_4)}{=} y + \mathbf{S}x$$

and (DT) and $(\forall)$. ⊣

In a similar way we can derive associativity of $+$ and $\cdot$, commutativity of $\cdot$ as well as distributivity.

**Lemma 2.4.** *The following rules hold in Peano Arithmetic:*

1. $\vdash_{\mathrm{PA}} \forall x \forall y \forall z ((x + y) + z = x + (y + z))$,
2. $\vdash_{\mathrm{PA}} \forall x \forall y \forall z ((x \cdot y) \cdot z = x \cdot (y \cdot z))$,
3. $\vdash_{\mathrm{PA}} \forall x \forall y (x \cdot y = y \cdot x)$,
4. $\vdash_{\mathrm{PA}} \forall x \forall y \forall z (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$.

From now on, we will make use of these rules without explicitly mentioning them anymore.

**Lemma 2.5.** $\vdash_{\mathrm{PA}} \forall x \forall y \forall z (x + y = x + z \to y = z)$.

*Proof.* We will show $\vdash_{\mathrm{PA}} \forall x\varphi(x)$, where $\varphi(x) = (\forall y \forall z(x+y = x+z \to y = z))$. The base case is a consequence of ($\mathrm{PA}_3$) using generalization. The induction step follows from

$$\begin{aligned} \varphi(x), \mathbf{S}x + y = \mathbf{S}x + z &\vdash_{\mathrm{PA}} \mathbf{S}(x+y) = \mathbf{S}x + y = \mathbf{S}x + z = \mathbf{S}(x+z) && \text{(Proof 2.3)} \\ &\vdash_{\mathrm{PA}} x + y = x + z && (\mathrm{PA}_3) \\ &\vdash_{\mathrm{PA}} y = z \end{aligned}$$

using (DT) and (∀). ⊣

We can also show that each number is either $\mathbf{0}$ or it has an antecessor.

**Lemma 2.6.** $\vdash_{\mathrm{PA}} \forall x(x = \mathbf{0} \vee \exists y(x = \mathbf{S}y))$.

*Proof.* We proof $\vdash_{\mathrm{PA}} \forall x\varphi(x)$ for $\varphi(x) = (x = \mathbf{0} \vee \exists y(x = \mathbf{S}y))$ using induction on $x$. The case $x = \mathbf{0}$ is clear by the axiom ($\mathrm{L}_6$). It remains to verify the induction step. Here we use (∨2):

$$\begin{aligned} x = \mathbf{0} \vee \exists y(x = \mathbf{S}y), \neg x = \mathbf{0} &\vdash_{\mathrm{PA}} \exists y(x = \mathbf{S}y) && (\vee 2) \\ x = \mathbf{S}y &\vdash_{\mathrm{PA}} \mathbf{S}x = \mathbf{S}(\mathbf{S}y) && (\mathrm{L}_{18}) \\ x = \mathbf{S}y &\vdash_{\mathrm{PA}} \exists y(\mathbf{S}x = \mathbf{S}y). && (\mathrm{L}_{13}) \end{aligned}$$

Hence by (∃) and ($\mathrm{L}_6$) we have shown $\varphi(x), \exists y(x = \mathbf{S}y) \vdash_{\mathrm{PA}} \varphi(\mathbf{S}x)$. The other case is easy as well:

$$\begin{aligned} x = \mathbf{0} &\vdash_{\mathrm{PA}} \mathbf{S}x = \mathbf{S0} && (\mathrm{L}_{18}) \\ &\vdash_{\mathrm{PA}} \exists y(\mathbf{S}x = \mathbf{S}y). && (\mathrm{L}_{13}) \end{aligned}$$

Therefore we obtain again using (∃) and ($\mathrm{L}_6$): $\varphi(x), x = \mathbf{0} \vdash_{\mathrm{PA}} \varphi(\mathbf{S}x)$. The induction step follows then from (∨4). ⊣

From now on, we will use the convention that $\cdot$ binds stronger than $+$ and omit the multplication sign. Furthermore, by the associativity, we obtain that it is not necessary to write the brackets while adding or multiplying various terms.

**Definition 2.7.** We will now define the binary relations $\leq$ and $<$ in PA by

$$\begin{aligned} x \leq y &:\leftrightarrow \exists r(x + r = y), \\ x < y &:\leftrightarrow x \leq y \wedge x \neq y, \end{aligned}$$

where $x \neq y$ is an abbreviation for $\neg(x = y)$. Furthermore, we can define $x \geq y \leftrightarrow y \leq x$ and $x > y \leftrightarrow y < x$. We obviously have the equivalences $\vdash_{\mathrm{PA}} \forall x \forall y(x < y \leftrightarrow \exists r(r \neq \mathbf{0} \wedge x + r = y))$ and $\vdash_{\mathrm{PA}} \forall x \forall y(x \leq y \leftrightarrow x < y \vee x = y)$.

The following three lemmas will show the reflexivity, antisymmetry and transitivity of $\leq$ as well as some elementary arithmetical rules concerning the above defined relations.

**Lemma 2.8.** *The following rules hold in PA:*

1. $\vdash_{\mathrm{PA}} \forall x \neg(x < \mathbf{0})$,
2. $\vdash_{\mathrm{PA}} \forall x \forall y (x < \mathbf{S}y \leftrightarrow x \leq y)$ *and* $\vdash_{\mathrm{PA}} \forall x \forall y (x < y \leftrightarrow \mathbf{S}x \leq y)$.

*Proof.*

1. We show the claim using $(\vee 1)$ and Lemma 2.6. The case $x = \mathbf{0}$ is trivial. For the case $x = \mathbf{S}y$ we note

$$x = \mathbf{S}y, x + r = \mathbf{0} \vdash_{\mathrm{PA}} \mathbf{S}(y + r) = \mathbf{S}y + r = x + r = \mathbf{0} \tag{2}$$

   which contradicts $(\mathrm{PA}_1)$. Applying $(\exists)$ twice leads to $\exists y(\mathbf{S}y = x) \vdash_{\mathrm{PA}} \neg(x < \mathbf{0})$. The claim follows from $(\vee 1)$.

2. We will only show the first claim. By $(\leftrightarrow)$ it is enough to verify each direction separately. Firstly, we note

$$\begin{aligned} x < \mathbf{S}y, x + r = \mathbf{S}y &\vdash_{\mathrm{PA}} \neg(r = \mathbf{0}) && (\lightning) \\ &\vdash_{\mathrm{PA}} \exists z (r = \mathbf{S}z). && (\vee 3,\ 2.6) \end{aligned}$$

   Using $(\exists)$ twice, the first direction follows then from

$$\begin{aligned} x + r = \mathbf{S}y, r = \mathbf{S}z &\vdash_{\mathrm{PA}} \mathbf{S}(x + z) = x + \mathbf{S}z = x + r = \mathbf{S}y && (\mathrm{PA}_4) \\ &\vdash_{\mathrm{PA}} x + z = y && (\mathrm{PA}_2) \\ &\vdash_{\mathrm{PA}} x \leq y. \end{aligned}$$

   Secondly, we have

$$\begin{aligned} x + r = y &\vdash_{\mathrm{PA}} \mathbf{S}x + r = \mathbf{S}(x + r) = \mathbf{S}y && (\text{Proof 2.3}) \\ &\vdash_{\mathrm{PA}} \mathbf{S}x \leq \mathbf{S}y \end{aligned}$$

   as well as

$$\begin{aligned} x + r = y, x = \mathbf{S}y &\vdash_{\mathrm{PA}} \mathbf{S}r = \mathbf{0} && (2.5) \\ &\vdash_{\mathrm{PA}} x \neq \mathbf{S}y. && (\mathrm{PA}_1,\ \lightning) \end{aligned}$$

   To sum up, $(\exists)$ implies $x \leq y \vdash_{\mathrm{PA}} x < \mathbf{S}y$ and hence $\vdash_{\mathrm{PA}} x \leq y \to x < \mathbf{S}y$ by (DT).

⊣

**Lemma 2.9.** *The relations* $\leq$ *and* $<$ *satisfy the properties*

1. $\vdash_{\mathrm{PA}} \forall x \forall y (x < y \vee x = y \vee x > y)$.
2. $\vdash_{\mathrm{PA}} \forall x (x \leq x)$,
3. $\vdash_{\mathrm{PA}} \forall x \forall y (x \leq y \wedge y \leq x \to x = y)$,

*4.* $\vdash_{\mathrm{PA}} \forall x\forall y\forall z(x \leq y \wedge y \leq z \to x \leq z)$ *and* $\vdash_{\mathrm{PA}} \forall x\forall y\forall z(x \prec_1 y \wedge y \prec_2 z \to x < z)$ *where* $\prec_1, \prec_2 \in \{\leq, <\}$ *and at least one of them is* $<$*.*

*Proof.*

1. We use induction on $x$ in order to prove the claim. If $x = \mathbf{0}$, we distinguish between two cases according to Lemma 2.6. Firstly, $x = \mathbf{0}, y = \mathbf{0} \vdash_{\mathrm{PA}} x = y$ is clear. Secondly, we have

$$\begin{aligned} x = \mathbf{0}, y = \mathbf{S}z &\vdash_{\mathrm{PA}} y = \mathbf{S}z \neq \mathbf{0} && (\mathrm{PA}_1)\\ &\vdash_{\mathrm{PA}} y = \mathbf{S}z = \mathbf{S}z + \mathbf{0} && (\mathrm{PA}_3)\\ &\vdash_{\mathrm{PA}} y > \mathbf{0}. && (\wedge,\mathrm{L}_{13}) \end{aligned}$$

   We show the induction step by proving each of the three cases $x < y \vee x = y \vee x > y$ separately.

$$\begin{aligned} x < y, x + r = y &\vdash_{\mathrm{PA}} \exists t(\mathbf{S}t = r) && (2.6,\ \vee 4)\\ x < y, x + r = y, r = \mathbf{S}t, t = \mathbf{0} &\vdash_{\mathrm{PA}} \mathbf{S}x = \mathbf{S}(x + \mathbf{0}) = x + \mathbf{S0} = y && (\mathrm{PA}_3,\ \mathrm{PA}_4)\\ x < y, x + r = y, r = \mathbf{S}t, t = \mathbf{S}u &\vdash_{\mathrm{PA}} \mathbf{S}x + t = \mathbf{S}(x + t) = x + \mathbf{S}t = y && (2,\ \mathrm{PA}_4)\\ &\vdash_{\mathrm{PA}} \mathbf{S}x < y && (\mathrm{PA}_1,\ \wedge)\\ x < y &\vdash_{\mathrm{PA}} \mathbf{S}x < y \vee \mathbf{S}x = y. && (\exists,\ \vee 1,\ 2.6) \end{aligned}$$

$$\begin{aligned} x = y &\vdash_{\mathrm{PA}} \mathbf{S}x = \mathbf{S}(x + \mathbf{0}) = x + \mathbf{S0} = y + \mathbf{S0} && (\mathrm{PA}_3,\ \mathrm{PA}_4)\\ &\vdash_{\mathrm{PA}} \mathbf{S}x > y. \end{aligned}$$

$$\begin{aligned} x > y, y + r = x &\vdash_{\mathrm{PA}} y + \mathbf{S}r = \mathbf{S}(y + r) = \mathbf{S}x && (\mathrm{PA}_4)\\ &\vdash_{\mathrm{PA}} \mathbf{S}x > y. \end{aligned}$$

   Combining all three cases and using $(\mathrm{L}_6)$ and $(\mathrm{L}_7)$, we obtain $x < y \vee x = y \vee x > y \vdash_{\mathrm{PA}} \mathbf{S}x < y \vee \mathbf{S}x = y \vee \mathbf{S}x > y$ which proves the induction step.

2. Follows directly from the definition of $\leq$ since $\vdash_{\mathrm{PA}} x + \mathbf{0} = x$.

3. We will prove the assertion using each $(\exists)$ and $(\forall)$ twice.

$$\begin{aligned} x + r = y, y + s = x &\vdash_{\mathrm{PA}} y + (s + r) = (y + s) + r = x + r = y = y + \mathbf{0} && (2.4.1,\ \mathrm{PA}_3)\\ &\vdash_{\mathrm{PA}} s + r = \mathbf{0} && (2.5)\\ &\vdash_{\mathrm{PA}} s \leq \mathbf{0}\\ &\vdash_{\mathrm{PA}} s = \mathbf{0} && (2.8.1)\\ &\vdash_{\mathrm{PA}} x = y + s = y + \mathbf{0} = y. && (\mathrm{PA}_3) \end{aligned}$$

4. We will only prove the first case, since the others can be shown in a similar way. It is a direct consequence of $x+r = y, y+s = z \vdash_{\mathrm{PA}} x+(r+s) = (x+r)+s = y+s = z$ using $(\exists)$ twice and (DT).

⊣

In particular, the fourth statement allows us to handle inequalities in PA in the "usual" way. We will use these results constantly without mentioning them. We state two more lemmas whose proofs are omitted.

**Lemma 2.10.** $\vdash_{\mathrm{PA}} \forall x \forall y \forall z (x \neq \mathbf{0} \to (x \cdot y = x \cdot z \to y = z))$.

**Lemma 2.11.** *The following rules hold:*

1. $\vdash_{\mathrm{PA}} \forall x \forall y \forall z (x \leq y \leftrightarrow x + z \leq y + z)$,
2. $\vdash_{\mathrm{PA}} \forall x \forall y \forall z (x \leq y \to x \cdot z \leq y \cdot z)$ *and* $\vdash_{\mathrm{PA}} \forall x \forall y \forall z (z \neq \mathbf{0} \to (x \cdot z \leq y \cdot z \to x \leq y))$.

The next lemma will allow us to define subtraction in PA, where negative numbers are rounded up to zero.

**Lemma 2.12.** $\vdash_{\mathrm{PA}} \forall x \forall y (x \leq y \to \exists! r (x + r = y))$.

*Proof.* By (DT) and (∀) it suffices to show $x \leq y \vdash_{\mathrm{PA}} \exists! r (x + r = y)$. The existence follows directly from the definition of $\leq$. The uniqueness is a consequence of Lemma 2.5. ⊣

**Definition 2.13.** We define the two-place function $-$ in PA as follows:

$$x - y = z :\leftrightarrow (y \leq x \wedge y + z = x) \vee (x < y \wedge z = \mathbf{0}).$$

The previous lemma legitimizes this definition.

**Lemma 2.14.** *The function* $-$ *has the properties*

1. $\vdash_{\mathrm{PA}} \forall x \forall y (x + y) - y = x$ *and* $\vdash_{\mathrm{PA}} \forall x \forall y (x \geq y \to ((x - y) + y = x))$,
2. $\vdash_{\mathrm{PA}} \forall x \forall y \forall z ((x - y) - z = x - (y + z))$ *as well as*
   $\vdash_{\mathrm{PA}} \forall x \forall y \forall z ((x \geq y \wedge y \geq z) \to (x - (y - z) = (x - y) + z))$,
3. $\vdash_{\mathrm{PA}} \forall x \forall y \forall z (y \geq z((x + y) - z = x + (y - z)))$,
4. $\vdash_{\mathrm{PA}} \forall x \forall y \forall z (x(y - z) = xy - xz)$,
5. $\vdash_{\mathrm{PA}} \forall x \forall y \forall z (x \leq y \to x - z \leq y - z)$.

In this section we have derived the basic arithmetical rules in PA concerning $+, \cdot, -$ and the order relations $\leq$ and $<$ which we will use from now on without mentioning explicitly the corresponding lemma.

## 2.2 Alternative induction schemas

In this section, which is based on [Kay91], we will describe a few variants of the induction scheme ($\mathrm{I}_\varphi$) which will be very useful for proving theorem such as Bézout's Lemma in Peano Arithmetic.

**Proposition 2.15** (Induction with Upper Bound)**.** *For each formula $\varphi = \varphi(x, \vec{y})$ in $\mathcal{L}_{\mathrm{PA}}$ with $\mathrm{free}(\varphi) = \{x, y_0, \ldots, y_n\}$ and for any $\mathcal{L}_{\mathrm{PA}}$-term $t$ the following schema holds:*

$$(\mathrm{I}_{\varphi_{\leq t}}) \quad \vdash_{\mathrm{PA}} \forall \vec{y}\big[\varphi(\mathbf{0}, \vec{y}) \wedge \forall x < t(\varphi(x, \vec{y}) \to \varphi(\mathbf{S}x, \vec{y})) \to \forall x \leq t\varphi(x, \vec{y})\big].$$

*Proof.* We set $\psi(x, \vec{y}) = (x \leq t \to \varphi(x, \vec{y}))$ and we would like to apply ($\mathrm{I}_\psi$) with respect to the variable $x$. The base case follows directly from the definition of $\psi$:

$$\begin{aligned} \varphi(\mathbf{0}, \vec{y}) &\vdash_{\mathrm{PA}} \mathbf{0} \leq t \to \varphi(\mathbf{0}, \vec{y}) \\ &\vdash_{\mathrm{PA}} \psi(\mathbf{0}, \vec{y}). \end{aligned}$$

For the induction step we set $T = \{\varphi(\mathbf{0}, \vec{y}) \wedge x < t \to (\varphi(x, \vec{y}) \to \varphi(\mathbf{S}x, \vec{y})), \psi(x, \vec{y})\}$.

$$\begin{aligned} T &\vdash_{\mathrm{PA}} (x < t \to \varphi(x, \vec{y})) \to (x < t \to \varphi(\mathbf{S}x, \vec{y})) && (\mathrm{L}_2) \\ &\vdash_{\mathrm{PA}} x < t \to \varphi(\mathbf{S}x, \vec{y}) && (\mathrm{MP}) \\ &\vdash_{\mathrm{PA}} \mathbf{S}x \leq t \to \varphi(\mathbf{S}x, \vec{y}) && (2.8.2,\ \mathrm{B}.14) \\ &\vdash_{\mathrm{PA}} \psi(\mathbf{S}x, \vec{y}). \end{aligned}$$

Using ($\mathrm{I}_\psi$) we obtain

$$\varphi(\mathbf{0}, \vec{y}) \wedge x < t \to (\varphi(x, \vec{y}) \to \varphi(\mathbf{S}x, \vec{y})) \vdash_{\mathrm{PA}} \forall x \psi(x, \vec{y})$$

which proves the assertion. ⊣

**Proposition 2.16** (Induction with Lower Bound)**.** *For any $\mathcal{L}_{\mathrm{PA}}$−formula $\varphi = \varphi(x, \vec{y})$ with $\mathrm{free}(\varphi) = \{x, y_0, \ldots, y_n\}$ und for any $\mathcal{L}_{\mathrm{PA}}$-term $t$ the following schema holds:*

$$(\mathrm{I}_{\varphi_{\geq t}}) \quad \vdash_{\mathrm{PA}} \forall \vec{y}\big[\varphi(t, \vec{y}) \wedge \forall x \geq t(\varphi(x, \vec{y}) \to \varphi(\mathbf{S}x, \vec{y})) \to \forall x \geq t(\varphi(x, \vec{y}))\big].$$

*Proof.* We set $\psi(x, \vec{y}) = (x \geq t \to \varphi(x, \vec{y}))$ and we will prove the assertion using induction on $x$. Let $T = \{\varphi(t, \vec{y}) \wedge \forall x \geq t(\varphi(x, \vec{y}) \to \varphi(\mathbf{S}x, \vec{y}))\}$. We show $T \vdash_{\mathrm{PA}} \forall x \psi(x, \vec{y})$. The base case holds because of $\mathbf{0} \geq t \vdash_{\mathrm{PA}} \mathbf{0} = t$. For the induction step we consider two cases using $T \cup \{\psi(x, \vec{y}), \mathbf{S}x \geq z\} \vdash_{\mathrm{PA}} \mathbf{S}x = t \vee x \geq t$ and ($\vee 1$). The first case is clear.

$$\begin{aligned} T \cup \{\psi(x, \vec{y}), x \geq t\} &\vdash_{\mathrm{PA}} \varphi(x, \vec{y}) && (\mathrm{MP}) \\ &\vdash_{\mathrm{PA}} \varphi(\mathbf{S}x, \vec{y}). && (\mathrm{L}_{12},\ \mathrm{MP}) \end{aligned}$$

By (DT) we obtain the second case and hence the assertion. ⊣

**Proposition 2.17** (Strong Induction)**.** *Let $\varphi(x, \vec{y})$ be an $\mathcal{L}_{\mathrm{PA}}$-formula with $\mathrm{free}(\varphi) = \{x, y_0, \ldots, y_n\}$. Then $\varphi$ fulfills the principle of strong induction:*

$$(\mathrm{I}_{\varphi_+}) \quad \vdash_{\mathrm{PA}} \forall \vec{y}(\forall x(\forall z < x \varphi(z, \vec{y}) \to \varphi(x, \vec{y})) \to \forall x \varphi(x, \vec{y})).$$

*Proof.* We define $\psi(x,\vec{y}) = (\forall z < x\varphi(z,\vec{y}) \wedge \varphi(x,\vec{y}))$ und we apply $(\mathrm{I}_\psi)$ to prove

$$\forall x(\forall z < x\varphi(z,\vec{y}) \to \varphi(x,\vec{y})) \vdash_{\mathrm{PA}} \forall x\psi(x,\vec{y}). \tag{3}$$

This implies $\forall x(\forall z < x\varphi(z,\vec{y}) \to \varphi(x,\vec{y})) \vdash_{\mathrm{PA}} \forall x\varphi(x,\vec{y})$ and hence the assertion. The base case is fulfilled because of

$$\begin{aligned}
\forall x(\forall z < x\varphi(z,\vec{y}) \to \varphi(x,\vec{y})) &\vdash_{\mathrm{PA}} z < \mathbf{0} \to \varphi(z,\vec{y}) && (\mathrm{L}_{10})\\
&\vdash_{\mathrm{PA}} \forall z < \mathbf{0}\varphi(z,\vec{y}) && \\
&\vdash_{\mathrm{PA}} \varphi(\mathbf{0},\vec{y}) && (\mathrm{L}_{12},\ \mathrm{MP})\\
&\vdash_{\mathrm{PA}} \psi(\mathbf{0},\vec{y}). && (\wedge)
\end{aligned}$$

Now we verify the induction step:

$$\begin{aligned}
\forall x(\forall z < x\varphi(z,\vec{y}) \to \varphi(x,\vec{y})), \psi(x,\vec{y}), z < \mathbf{S}x &\vdash_{\mathrm{PA}} z < x \vee z = x\\
&\vdash_{\mathrm{PA}} \varphi(z,\vec{y}). && (\vee 1)
\end{aligned}$$

Thus we obtain

$$\begin{aligned}
\forall x(\forall z < x\varphi(z,\vec{y}) \to \varphi(x,\vec{y})), \psi(x,\vec{y}) &\vdash_{\mathrm{PA}} \forall z < \mathbf{S}x\varphi(z,\vec{y})\\
&\vdash_{\mathrm{PA}} \varphi(\mathbf{S}x,\vec{y}) && (\mathrm{L}_{12},\ \mathrm{MP})\\
&\vdash_{\mathrm{PA}} (\forall z < \mathbf{S}x\varphi(z,\vec{y}) \wedge \varphi(\mathbf{S}x,\vec{y})) = \psi(\mathbf{S}x,\vec{y})
\end{aligned}$$

which implies (3).

⊣

**Proposition 2.18** (Least Number Principle)**.** *Let $\varphi(x,\vec{y})$ be an $\mathcal{L}_{\mathrm{PA}}$-formula with* $\mathrm{free}(\varphi) = \{x, y_0, \ldots, y_n\}$*. Then the Least Number Principle holds:*

$$(\mathrm{I}_{\varphi\_}) \quad \vdash_{\mathrm{PA}} \forall\vec{y}\big[\exists x\varphi(x,\vec{y}) \to \exists z(\varphi(z,\vec{y}) \wedge \forall w < z\neg\varphi(w,\vec{y}))\big].$$

Intuitively, this principle corresponds to the well-ordering principle which says that any subset of the set of natural numbers has a least element.

*Proof.* We obtain the claim using strong induction for the formula $\neg\varphi(x,\vec{y})$:

$$\vdash_{\mathrm{PA}} \forall\vec{y}(\forall x(\forall z < x\neg\varphi(z,\vec{y}) \to \neg\varphi(x,\vec{y})) \to \forall x\neg\varphi(x,\vec{y})). \tag{4}$$

Using the substitution theorem, we obtain equivalences

$$\begin{aligned}
\forall x(\forall z < x\neg\varphi(x,\vec{y}) \to \neg\varphi(x,\vec{y})) &\equiv_{PA} \forall x(\neg\forall z < x\neg\varphi(x,\vec{y}) \vee \neg\varphi(x,\vec{y})) && (\mathrm{E})\\
&\equiv_{PA} \forall x\neg(\forall z < x\neg\varphi(z,\vec{y}) \wedge \varphi(x,\vec{y})) && (\mathrm{F}.1)\\
&\equiv_{PA} \neg\exists x(\varphi(x,\vec{y}) \wedge \forall z < x\neg\varphi(z,\vec{y})). && (\mathrm{K}.1)
\end{aligned}$$

This leads to

$$\begin{aligned}
&\forall x(\forall z < x\neg\varphi(x,\vec{y}) \to \neg\varphi(x,\vec{y})) \to \forall x\neg\varphi(x,\vec{y})) \\
&\quad \equiv_{PA} \neg\exists x(\varphi(x,\vec{y}) \wedge \forall z < x\neg\varphi(z,\vec{y})) \to \forall x\neg\varphi(x,\vec{y})) \\
&\quad \equiv_{PA} \exists x(\varphi(x,\vec{y}) \wedge \forall z < x\neg\varphi(z,\vec{y})) \vee \forall x\neg\varphi(x,\vec{y})) && \text{(E, A)} \\
&\quad \equiv_{PA} \neg\exists x\varphi(x,\vec{y}) \vee \exists x(\varphi(x,\vec{y}) \wedge \forall z < x\neg\varphi(z,\vec{y})) && \text{(K.1, D.1)} \\
&\quad \equiv_{PA} \exists x\varphi(x,\vec{y}) \to \exists x(\varphi(x,\vec{y}) \wedge \forall z < x\neg\varphi(z,\vec{y})). && \text{(E)}
\end{aligned}$$

Hence it is clear that (4) and ($\mathrm{I}_{\varphi^-}$) are equivalent. ⊣

*Remark* 2.19. The Least Number Principle does not only prove the existence of a least number which fulfills some formula, but also its uniqueness. Thus for a formula $\varphi$ as above we have

$$\vdash_{\mathrm{PA}} \forall\vec{y}\big[\exists x\varphi(x,\vec{y}) \to \exists! z(\varphi(z,\vec{y}) \wedge \forall w < z\neg\varphi(w,\vec{y}))\big].$$

## 2.3 The Chinese Remainder Theorem

The goal of the following section is to prove the Chinese Remainder Theorem in Peano Arithmetic which is necessary for the construction of Gödel's $\beta$-function. In order to achieve this, we need to show first some basic number theoretic results, such as division with remainder and Bézout's Lemma. Contrary to the last sections, we will not state all details of the formal proofs, but rather mention all important steps and the axioms and results which are applied. For less formalized proofs, see [Boo95].

**Proposition 2.20** (Division with Remainder)**.**

$$\vdash_{\mathrm{PA}} \forall x\forall y \neq \mathbf{0}\exists! r\exists! s(x = ys + r \wedge r < y).$$

*Proof.* For the existence we show $y > \mathbf{0} \vdash_{\mathrm{PA}} \exists r\exists s\varphi$ with $\varphi = (x = ys + r \wedge r < y)$ using induction on $x$. We consider first the base case

$$\begin{aligned}
&y > \mathbf{0} \vdash_{\mathrm{PA}} \mathbf{0} < y \\
&\quad \vdash_{\mathrm{PA}} \mathbf{0} = y \cdot \mathbf{0} = y \cdot \mathbf{0} + \mathbf{0} && (\mathrm{PA}_3,\mathrm{PA}_5) \\
&\quad \vdash_{\mathrm{PA}} \mathbf{0} = y \cdot \mathbf{0} = y \cdot \mathbf{0} + \mathbf{0} \wedge \mathbf{0} < y. && (\wedge)
\end{aligned}$$

We will now prove the induction step; ($\mathrm{PA}_4$) and ($\mathrm{L}_{18}$) imply

$$y > \mathbf{0}, x = ys + r \wedge r < y \vdash_{\mathrm{PA}} \mathbf{S}x = \mathbf{S}(ys + r) = ys + \mathbf{S}r. \tag{5}$$

Now we can apply ($\vee$1) by distinguishing between the two cases in $r < y \vdash_{\mathrm{PA}} \mathbf{S}r < y \vee \mathbf{S}r = y$ which is a consequence of 2.8.

$$\begin{aligned}
y > \mathbf{0}, x = ys + r \wedge r < y, \mathbf{S}r < y &\vdash_{\mathrm{PA}} \mathbf{S}x = ys + \mathbf{S}r \wedge \mathbf{S}r < y \\
&\vdash_{\mathrm{PA}} \varphi(x/\mathbf{S}x, r/\mathbf{S}r).
\end{aligned}$$

$$y > \mathbf{0}, x = ys + r \wedge r < y, \mathbf{S}r = y \vdash_{\mathrm{PA}} \mathbf{S}x \overset{(5)}{=} ys + y \overset{(\mathrm{PA6})}{=} y \cdot \mathbf{S}s \overset{(\mathrm{PA4})}{=} y \cdot \mathbf{S}s + \mathbf{0} \vdash_{\mathrm{PA}} \varphi(x/\mathbf{S}x, r/\mathbf{0}, s/\mathbf{S}s).$$

Hence ($\vee 1$) and ($\mathrm{L}_{13}$) imply

$$y > \mathbf{0}, x = ys + r \wedge r < y \vdash_{\mathrm{PA}} \exists r \exists s \varphi(\mathbf{S}x, r, s)$$

from which in turn we can conclude the induction step using (DT) and ($\exists$).
In order to prove uniqueness we need to show

$$y > \mathbf{0} \vdash_{\mathrm{PA}} \forall r \forall r' \forall s \forall s' (x = ys + r \wedge r < y \wedge x = ys' + r' \wedge r' < y \to r = r' \wedge s = s').$$

We set $T = \{y \neq \mathbf{0}, x = ys + r \wedge r < y, x = ys' + r' \wedge r' < y\}$ and we distinguish between three cases due to $T \vdash_{\mathrm{PA}} s < s' \vee s = s' \vee s' < s$. The third case is omitted, as its proof is analogous to the first case. Firstly, we have

$$\begin{aligned} T, s < s' &\vdash_{\mathrm{PA}} \mathbf{S}s \leq s' && (2.8)\\ &\vdash_{\mathrm{PA}} x = ys + r < ys + y = y \cdot \mathbf{S}s \leq ys' \leq ys' + r' = x && (\mathrm{PA}_6,\ 2.11)\\ &\vdash_{\mathrm{PA}} x < x\\ &\vdash_{\mathrm{PA}} \bot. \end{aligned}$$

Now we consider the second case

$$\begin{aligned} T, s = s' &\vdash_{\mathrm{PA}} ys = ys' && (\mathrm{L}_{18})\\ &\vdash_{\mathrm{PA}} ys + r = ys + r' && (\mathrm{L}_{18},\ \mathrm{B}.17)\\ &\vdash_{\mathrm{PA}} r = r'. && (2.5) \end{aligned}$$

Therefore, with (DT) and the generalization rule we can conclude the uniqueness. $\dashv$

Thus we have shown that we can define in Peano Arithmetic a function that computes the integer value after division as well as one that calculates the remainder of the division of two numbers.

**Definition 2.21.** We define the binary functions

$$\begin{aligned} \mathrm{int\_div}(x, y) = z &:\leftrightarrow (y = \mathbf{0} \wedge z = \mathbf{0}) \vee (y > \mathbf{0} \wedge \exists r(x = yz + r \wedge r < y)),\\ \mathrm{rest}(x, y) = z &:\leftrightarrow (y = \mathbf{0} \wedge z = \mathbf{0}) \vee (y > \mathbf{0} \wedge z < y \wedge \exists s(x = ys + z)). \end{aligned}$$

The previous proposition legitimizes both definitions.

**Definition 2.22.** We define the binary divisibility relation as follows

$$y \mid x :\leftrightarrow \exists z(x = yz).$$

Furthermore, we introduce the abbreviation $y \nmid x \leftrightarrow \neg(y \mid x)$. We can also introduce the quotient of two divisible numbers as

$$\frac{x}{y} = z :\leftrightarrow (y > \mathbf{0} \wedge x = yz) \vee ((y = \mathbf{0} \vee x \neq yz) \wedge z = \mathbf{0}).$$

Lemma 2.11.2 legitimizes this definition.

Without effort, one can verify reflexivity, antisymmetry and transitivity of the divisibility relation in PA. Thus we will omit the proof of the next lemma.

**Lemma 2.23.** *The divisibility relation has the properties*

1. $\vdash_{\mathrm{PA}} \forall x(x \mid x)$,
2. $\vdash_{\mathrm{PA}} \forall x \forall y(x \mid y \wedge y \mid x \to x = y)$,
3. $\vdash_{\mathrm{PA}} \forall x \forall y \forall z(x \mid y \wedge y \mid z \to x \mid z)$.

**Lemma 2.24.** *The following statements hold:*

1. $\vdash_{\mathrm{PA}} \forall x \forall y \forall z(x \mid y \wedge x \mid z \to x \mid y+z)$ *and* $\vdash_{\mathrm{PA}} \forall x \forall y \forall z(x \mid y \wedge x \mid z \wedge z \leq y \to x \mid y-z)$,
2. $\vdash_{\mathrm{PA}} \forall x \forall y \forall z(x \mid y \to x \mid yz)$.

*Proof.*

1. Since both proofs can be realized in a similar fashion, we will only consider the first statement.

$$\begin{aligned} x > \mathbf{0}, y = xu, z = xv &\vdash_{\mathrm{PA}} x(u+v) = xu + xv = y + z \\ &\vdash_{\mathrm{PA}} x \mid y + z. \end{aligned}$$

   The assertion is then a consequence of $(\exists)$ and the deduction theorem.

2. Follows directly from the definition of the divisibility relation.

⊣

**Lemma 2.25.** *The following statements concerning the remainder function hold:*

1. $\vdash_{\mathrm{PA}} x \mid y \leftrightarrow \mathrm{rest}(y, x) = \mathbf{0}$,
2. $\vdash_{\mathrm{PA}} z \mid y \to \mathrm{rest}(x + y, z) = \mathrm{rest}(x, z)$,
3. $\vdash_{\mathrm{PA}} x < y \to \mathrm{rest}(x, y) = x$.

*Proof.*

1. The implication ″⇒‶ is a consequence of

$$\begin{aligned} x > \mathbf{0}, xz = y &\vdash_{\mathrm{PA}} y = xz + \mathbf{0} \wedge \mathbf{0} < x \qquad (\mathrm{PA}_3, \wedge) \\ &\vdash_{\mathrm{PA}} \mathrm{rest}(y, x) = \mathbf{0} \end{aligned}$$

   using $(\exists)$ and $x = \mathbf{0} \vdash_{\mathrm{PA}} x \nmid y$. The second direction follows by definition from $\mathrm{rest}(y, x) = \mathbf{0} \vdash_{\mathrm{PA}} y = x \cdot \mathrm{int\_div}(y, x) + \mathbf{0} = x \cdot \mathrm{int\_div}(y, x)$.

2. Once again, we make use of (∃) and (DT):

$$\begin{aligned} z > \mathbf{0}, uz = y &\vdash_{\mathrm{PA}} x = z \cdot \mathrm{int\_div}(x,z) + \mathrm{rest}(x,z) \\ &\vdash_{\mathrm{PA}} x + y = (z \cdot \mathrm{int\_div}(x,z) + \mathrm{rest}(x,z)) + uz \\ &\qquad = (\mathrm{int\_div}(x,z) + u)z + \mathrm{rest}(x,z) \\ &\vdash_{\mathrm{PA}} x + y = (\mathrm{int\_div}(x,z) + u)z + \mathrm{rest}(x,z) \wedge \mathrm{rest}(x,z) < z \qquad (\wedge) \\ &\vdash_{\mathrm{PA}} \mathrm{rest}(x+y,z) = \mathrm{rest}(x,z). \end{aligned}$$

   Again, the case $z = \mathbf{0}$ is trivial.

3. The last property is a direct consequence of the definition of rest.

⊣

**Definition 2.26.** We define the unary predicate prime and the binary predicate coprime to express that a number is prime respectively that two numbers are coprime.

$$\begin{aligned} \mathrm{prime}(x) &:\leftrightarrow x > \underline{1} \wedge \forall y \forall z (x \mid (y \cdot z) \to (x \mid y \vee x \mid z)), \\ \mathrm{coprime}(x,y) &:\leftrightarrow x \geq \underline{1} \wedge y \geq \underline{1} \wedge \forall z (z \mid x \wedge z \mid y \to z = \underline{1}). \end{aligned}$$

We can now state and prove Bézout's Lemma in Peano Arithmetic. We note that since the "usual" subtraction is impossible in PA, the standard proof used for the integers cannot be transfered to PA.

**Proposition 2.27** (Bézout's Lemma)**.** $\vdash_{\mathrm{PA}} \forall x \forall y (\mathrm{coprime}(x,y) \to \exists u \exists v (ux + \underline{1} = vy))$.

*Proof.* The cases $x = \mathbf{0}$ or $y = \mathbf{0}$ are obvious. We consider the cases $x = \underline{1}$ as well as $y = \underline{1}$ separately. We have $y = \underline{1} \vdash_{\mathrm{PA}} \mathbf{0} \cdot x + \underline{1} = \underline{1} \cdot \underline{1}$ and $x = \underline{1}, y = \mathbf{S}z \vdash_{\mathrm{PA}} zx + \underline{1} = z + \underline{1} = \mathbf{S}z = y$ and thus we obtain the claim by 2.6 and (∃). Thus the claim can be reduced to

$$x > \underline{1}, y > \underline{1}, \mathrm{coprime}(x,y) \vdash_{\mathrm{PA}} \varphi(\underline{1}), \tag{6}$$

where $\varphi(z) = (z \neq \mathbf{0}) \wedge (\exists u \exists v (ux + z = vy))$. We set $T = \{x > \underline{1}, y > \underline{1}, \mathrm{coprime}(x,y)\}$ and show first the statements

$$T \vdash_{\mathrm{PA}} \varphi(x), \tag{7}$$

$$T \vdash_{\mathrm{PA}} \varphi(y), \tag{8}$$

$$T \vdash_{\mathrm{PA}} \varphi(z) \to \forall w > \mathbf{0}\, \varphi(wz), \tag{9}$$

$$T, z' < z \vdash_{\mathrm{PA}} \varphi(z) \wedge \varphi(z') \to \varphi(z - z'). \tag{10}$$

Statement (7) follows from $T \vdash_{\mathrm{PA}} (y - \underline{1})x + x = (y - \underline{1})x + \underline{1} \cdot x = ((y - \underline{1}) + \underline{1})x = yx = xy$. Claim (8) is a consequence of $T \vdash_{\mathrm{PA}} \mathbf{0} \cdot x + y = y = \underline{1} \cdot y$.

Using (DT), (∀) and (∃) we obtain (9) from

$$\begin{aligned} T, ux + z = vy, w \neq \mathbf{0} &\vdash_{\mathrm{PA}} w(ux + z) = w(vy) = (wv)y \\ &\vdash_{\mathrm{PA}} w(ux + z) = w(ux) + (wz) = (wu)x + (wz) \\ &\vdash_{\mathrm{PA}} (wu)x + (wz) = (wv)y \\ &\vdash_{\mathrm{PA}} \varphi(wz). \qquad (\mathrm{L}_{13}) \end{aligned}$$

The last statement requires the greatest effort. We define $T' = T \cup \{z' < z, ux + z = vy, u'x + z' = v'y\}$. Then,

$$\begin{aligned}
T' &\vdash_{\mathrm{PA}} z = vy - ux \\
&\vdash_{\mathrm{PA}} z' = v'y - u'x \\
&\vdash_{\mathrm{PA}} z - z' = (vy - ux) - (v'y - u'x) = ((vy - ux) - v'y) + u'x && (\mathrm{L}_{18}) \\
&\qquad = (vy - (ux + v'y)) + u'x = u'x + (vy - (ux + v'y)) \\
&\qquad = (u'x + vy) - (ux + v'y). && (11)
\end{aligned}$$

Now we want to show that if $z' < z$ and if $z$ and $z'$ fulfil the desired condition, then so does $z - z'$. Since similar arguments as in (11) are used, the details are left out.

$$\begin{aligned}
T' \vdash_{\mathrm{PA}} (u + v'y + u'(y - \underline{1}))x + (z - z') &= (ux + (v'x)y + u'y - u'x) && (8) \\
&\quad + ((u'x + vy) - (ux + v'y)) \\
&= (u'y + vy + v'(x - \underline{1})y \\
&= (u' + v + v'(x - \underline{1}))y.
\end{aligned}$$

As a result of $z < z' \vdash_{\mathrm{PA}} z - z' \neq \mathbf{0}$, we can conclude $T, z' < z, ux + z = vy, u'x + z' = v'y \vdash_{\mathrm{PA}} \varphi(z - z')$ and due to $(\exists)$ and the deduction theorem also (10) is proved.
Now we apply the Least Number Principle in order to find a smallest $z$ which fulfills $\varphi(z)$:

$$T \vdash_{\mathrm{PA}} \exists z(\varphi(z) \wedge \forall z'(z' < z \to \neg\varphi(z'))) \qquad (12)$$

Furthermore, we need to show that every $w$ with $\varphi(w)$ satisfies $z \mid w$. Firstly, we have

$$\begin{aligned}
T, \varphi(z) \wedge \forall z'(z' < z \to \neg\varphi(z')), \varphi(w) &\vdash_{\mathrm{PA}} w < z \to \neg\varphi(w) && (\mathrm{L}_{12}) \\
&\vdash_{\mathrm{PA}} \neg(w < z) && (\mathrm{CP}) \\
&\vdash_{\mathrm{PA}} w \geq z && (\vee 2) \\
&\vdash_{\mathrm{PA}} \mathrm{int_div}(w, z) \neq \mathbf{0} && (2.21) \\
&\vdash_{\mathrm{PA}} \varphi(\mathrm{int_div}(w, z) \cdot z). && (9) \quad (13)
\end{aligned}$$

The penultimate step holds by contradiction due to

$$w \geq z, \mathrm{int\_div}(w, z) = \mathbf{0} \vdash_{\mathrm{PA}} w = \mathrm{int\_div}(w, z) \cdot z + \mathrm{rest}(w, z) = \mathrm{rest}(w, z) < z \leq w.$$

Because of (13) and $\vdash_{\mathrm{PA}} w - \mathrm{int\_div}(w, z) \cdot z = \mathrm{rest}(w, z)$ we can conclude

$$T, \varphi(z) \wedge \forall z'(z' < z \to \neg\varphi(z')), \varphi(w), \mathrm{rest}(w, z) \neq \mathbf{0} \vdash_{\mathrm{PA}} \varphi(\mathrm{rest}(w, z)), \qquad (10)$$

but as a consequence of $\vdash_{\mathrm{PA}} \mathrm{rest}(w, z) < z$, we also have

$$T, \varphi(z) \wedge \forall z'(z' < z \to \neg\varphi(z')), \varphi(w), \mathrm{rest}(w, z) \neq \mathbf{0} \vdash_{\mathrm{PA}} \neg\varphi(z)$$

which leads to a contradiction. Therefore, we obtain

$$\begin{aligned}
T, \varphi(z) \wedge \forall z'(z' < z \to \neg\varphi(z')), \varphi(w) &\vdash_{\mathrm{PA}} \mathrm{rest}(w, z) = \mathbf{0} \\
&\vdash_{\mathrm{PA}} z \mid w. && (2.25.1) \quad (14)
\end{aligned}$$

The deduction theorem and the generalization rule then imply

$$T, \varphi(z) \wedge \forall z'(z' < z \to \neg\varphi(z')) \vdash_{\mathrm{PA}} \forall w(\varphi(w) \to z \mid w) \tag{14}$$
$$\vdash_{\mathrm{PA}} z \mid x \tag{7}$$
$$\vdash_{\mathrm{PA}} z \mid y \tag{8}$$
$$\vdash_{\mathrm{PA}} z \mid x \wedge z \mid y \tag{$\wedge$}$$
$$\vdash_{\mathrm{PA}} z = \underline{1}, \tag{15}$$

because $x$ and $y$ are coprime by definition of $T$. Bézout's Lemma is then a consequence of (12) and (15). ⊣

Using Bézout's Lemma we can show the equivalence of primality and irreducibility. In order to achieve this, we need to define irreducibility in Peano Arithmetic.

**Definition 2.28.** We define the relation

$$\mathrm{irreducible}(x) :\leftrightarrow \forall y(y \mid x \to (y = \underline{1} \vee y = x)).$$

*Remark* 2.29. We can easily show that $\underline{1}$ is irreducible, i.e. $\vdash_{\mathrm{PA}} \mathrm{irreducible}(\underline{1})$. This follows from

$$xy = \underline{1}, x < \underline{1} \vdash_{\mathrm{PA}} x = \mathbf{0}$$
$$\vdash_{\mathrm{PA}} \underline{1} = xy = \mathbf{0} \cdot y = \mathbf{0} \tag{$\mathrm{PA}_5$}$$

and

$$xy = \underline{1}, x > \underline{1}, y \geq \underline{1} \vdash_{\mathrm{PA}} xy = \underline{1} < x = \underline{1} \cdot x \leq yx = xy \tag{2.11}$$

which are both contradictions and prove the result since the case $y = \mathbf{0}$ can be excluded in the same way as the case $x = \mathbf{0}$.

**Corollary 2.30.** $\vdash_{\mathrm{PA}} \forall x(\mathrm{prime}(x) \leftrightarrow \mathrm{irreducible}(x) \wedge x > \underline{1})$.

*Proof.* By ($\leftrightarrow$), the generalization rule and the deduction theorem, it is enough to show

$$\mathrm{prime}(x), y \mid x \vdash_{\mathrm{PA}} y = \underline{1} \vee y = x, \tag{16}$$
$$\mathrm{irreducible}(x), x > \underline{1}, x \mid yz \vdash_{\mathrm{PA}} x \mid y \vee x \mid z. \tag{17}$$

Firstly, we consider (16).

$$\mathrm{prime}(x), yz = x \vdash_{\mathrm{PA}} x \mid yz \tag{2.23}$$
$$\vdash_{\mathrm{PA}} x \mid y \vee x \mid z. \tag{2.26}$$

By ($\vee$1), it is sufficient to prove $yz = x, x \mid y \vdash_{\mathrm{PA}} x = y$ as well as $yz = x, x \mid z \vdash_{\mathrm{PA}} y = \underline{1}$. Both cases follow from elementary rules of arithmetic and divisibility as follows:

$$yz = x, x \mid y \vdash_{\mathrm{PA}} y \mid x$$
$$\vdash_{\mathrm{PA}} x \mid y \wedge y \mid x \tag{$\wedge$}$$
$$\vdash_{\mathrm{PA}} x = y \tag{2.9.3}$$

$$yz = x, x \mid z \vdash_{\mathrm{PA}} yz \mid z \tag{2.9.4}$$
$$yz = x, (yz)w = z \vdash_{\mathrm{PA}} z \cdot \underline{1} = z = (yz)w = (zy)w = z(yw)$$
$$\vdash_{\mathrm{PA}} yw = \underline{1} \tag{2.10}$$
$$\vdash_{\mathrm{PA}} y \mid \underline{1} \tag{2.22}$$
$$\vdash_{\mathrm{PA}} y = \underline{1}. \tag{2.29}$$

By applying $(\exists)$, we obtain (16). For (17), by $(\vee 1)$ and $(\mathrm{L}_6)$ it is enough to verify only the case $x > \underline{1}, \mathrm{irreducible}(x), x \mid yz, x \nmid y \vdash_{\mathrm{PA}} x \mid z$, since both cases can be shown in a similar way. Bézout's Lemma implies

$$x > \underline{1}, \mathrm{irreducible}(x), x \mid yz, x \nmid y \vdash_{\mathrm{PA}} y \neq x \tag{2.9.2}$$
$$\vdash_{\mathrm{PA}} \mathrm{coprime}(x, y) \tag{2.26}$$
$$\vdash_{\mathrm{PA}} \exists u \exists v (ux + \underline{1} = vy). \tag{2.27}$$

Hence we have

$$\mathrm{irreducible}(x), x \mid yz, x \nmid y, ux + \underline{1} = vy \vdash_{\mathrm{PA}} (ux + \underline{1})z = (vy)z$$
$$\vdash_{\mathrm{PA}} uxz + z = vyz$$
$$\vdash_{\mathrm{PA}} x \mid uxz \tag{2.24.2}$$
$$\vdash_{\mathrm{PA}} x \mid vyz \tag{2.24.2}$$
$$\vdash_{\mathrm{PA}} x \mid vyz - uxz = z, \tag{2.24.1}$$

and thus (b) holds. ⊣

In the following, we will introduce the least common multiple of a bounded number of values in Peano Arithmetic which will be significant for the proof of the Chinese Remainder Theorem.

**Lemma 2.31.** *Let $f$ be a unary function. Then the following statement holds:*

$$\vdash_{\mathrm{PA}} \forall i < k (f(i) > \mathbf{0}) \to \exists! x \big[ x > \mathbf{0} \wedge \forall i < k (f(i) \mid x)) \wedge \forall y < x \neg (y > \mathbf{0} \wedge \forall i < k (f(i) \mid y)) \big].$$

*Proof.* We set $\varphi(x, k) = (\forall i < k (f(i) \mid x))$. By remark 2.19 and the deduction theorem, it is sufficient to show

$$\forall i < k (f(i) > \mathbf{0}) \vdash_{\mathrm{PA}} \exists x \varphi(x, k). \tag{18}$$

We prove (18) by induction on $k$. The base case $\vdash_{\mathrm{PA}} \exists x \varphi(x, \mathbf{0})$ follows directly from $\vdash_{\mathrm{PA}} \forall i \neg (i < \mathbf{0})$. For the induction step we note

$$\forall i < k (f(i) > \mathbf{0}) \to \exists x \varphi(x, k), \forall i < \mathbf{S}k (f(i) > \mathbf{0}) \vdash_{\mathrm{PA}} \exists x \varphi(x, k).$$

We have

$$\forall i < k (f(i) \mid x), i < k \ \vdash_{\mathrm{PA}} f(i) \mid x \wedge x \mid f(k) \cdot x$$
$$\vdash_{\mathrm{PA}} f(i) \mid f(k) \cdot x, \tag{2.23.3}$$

as well as $\vdash_{\mathrm{PA}} f(k) \mid f(k) \cdot x$. This implies

$$\forall i < \mathbf{S}k(f(i) > \mathbf{0}), \forall i < k(f(i) \mid x), i < \mathbf{S}k \vdash_{\mathrm{PA}} i < k \vee i = k \\ \vdash_{\mathrm{PA}} f(i) \mid f(k) \cdot x, \tag{$\vee$1}$$

from which we can conclude the induction step using (DT), ($\forall$) and ($\mathrm{L}_{18}$). ⊣

Lemma 2.31 indicates that the following definition schema of the least common multiple is legitimate.

**Definition 2.32.** For an arbitrary unary function $f$ we define

$$\begin{aligned}\mathrm{lcm}[f(i), i < k] = x \leftrightarrow \big[&k > \mathbf{0} \wedge \forall i < k(f(i) > \mathbf{0}) \wedge x > \mathbf{0} \wedge \forall i < k(f(i) \mid x) \wedge \forall y < x \\ &\neg(y > \mathbf{0} \wedge \forall i < k(f(i) \mid y))\big] \vee (k > \mathbf{0} \wedge \exists i < k(f(i) = \mathbf{0}) \wedge x = \mathbf{0}) \\ &\vee (k = \mathbf{0} \wedge x = \underline{1}).\end{aligned}$$

Before we can proceed to the proof of the Chinese Remainder Theorem, we need some basic results concerning the least common multilple.

**Lemma 2.33.** *Let $f$ be a unary function. Then the following statements hold:*

1. $\forall i < k(f(i) > \mathbf{0}) \vdash_{\mathrm{PA}} j < k \to f(j) \mid \mathrm{lcm}[f(i), i < k]$,
2. $\forall i < k(f(i) > \mathbf{0}) \vdash_{\mathrm{PA}} \forall i < k(f(i) \mid y) \to \mathrm{lcm}[f(i), i < k] \mid y$,
3. $\vdash_{\mathrm{PA}} \mathrm{prime}(p) \wedge p \mid \mathrm{lcm}[f(i), i < k] \to \exists i < k(p \mid f(i))$.

*Proof.*

1. Holds by definition.
2. The case $k = \mathbf{0}$ is obvious and can thus be omitted. We set $T = \{x = \mathrm{lcm}[f(i), i < k], \forall i < k(f(i) > \mathbf{0}), \forall i < k(f(i) \mid y)\}$. Then we have

$$\begin{aligned}T, i < k &\vdash_{\mathrm{PA}} y = \mathrm{int\_div}(y, x) \cdot x + \mathrm{rest}(y, x) \\ &\vdash_{\mathrm{PA}} f(i) \mid x && (1.) \\ &\vdash_{\mathrm{PA}} f(i) \mid \mathrm{int\_div}(y, x) \cdot x && (2.24.2) \\ &\vdash_{\mathrm{PA}} f(i) \mid y \wedge f(i) \mid \mathrm{int\_div}(y, x) \cdot x && (\wedge) \\ &\vdash_{\mathrm{PA}} f(i) \mid y - \mathrm{int\_div}(y, x) \cdot x = \mathrm{rest}(y, x). && (2.24.1)\end{aligned}$$

   Therefore, the assertion follows from

$$\begin{aligned}T &\vdash_{\mathrm{PA}} \forall i < k(f(i) \mid \mathrm{rest}(y, x)) \wedge \mathrm{rest}(y, x) < x \\ &\vdash_{\mathrm{PA}} \neg(\mathrm{rest}(y, x) > \mathbf{0} \wedge \forall i < k(f(i) \mid \mathrm{rest}(y, x)) \\ &\vdash_{\mathrm{PA}} \mathrm{rest}(y, x) = \mathbf{0} \vee \neg(\forall i < k(f(i) \mid \mathrm{rest}(y, x))) && (\mathrm{F}.1) \\ &\vdash_{\mathrm{PA}} \mathrm{rest}(y, x) = \mathbf{0} && (\vee 4) \\ &\vdash_{\mathrm{PA}} \mathrm{lcm}[f(i), i < k] = x \mid y. && (2.25.1)\end{aligned}$$

3. The cases $k = \mathbf{0}$ and $\exists i < k(f(i) = \mathbf{0})$ are obvious. Thus by $(\vee 1)$ it is enough to consider the case $k > \mathbf{0} \wedge \forall i < k(f(i) > \mathbf{0})$. We show the claim by induction on $k$ with lower bound $\underline{1}$. For the base case, one has to show $\vdash_{\mathrm{PA}} \mathrm{lcm}[f(i), i < \underline{1}] = f(\mathbf{0})$ which follows immediately from the definition of lcm. For the induction step, we define $T = \{k \geq \underline{1}, \mathrm{prime}(p) \wedge p \mid \mathrm{lcm}[f(i), i < k] \to \exists i < k(p \mid f(i)), \mathrm{prime}(p) \wedge p \mid \mathrm{lcm}[f(i), i < \mathbf{S}k]\}$ and we need to show

$$T \vdash_{\mathrm{PA}} \exists i < \mathbf{S}k(p \mid f(i)). \tag{19}$$

We have

$$\begin{aligned} T, j < k &\vdash_{\mathrm{PA}} f(j) \mid \mathrm{lcm}[f(i), i < k] && (1.)\\ &\vdash_{\mathrm{PA}} f(j) \mid \mathrm{lcm}[f(i), i < k] \cdot f(k) && (2.24.2) \end{aligned}$$

and, due to Lemma 2.24.2, also $T \vdash_{\mathrm{PA}} f(k) \mid \mathrm{lcm}[f(i), i < k] \cdot f(k)$ which leads to

$$\begin{aligned} T &\vdash_{\mathrm{PA}} \forall j < \mathbf{S}k(f(j) \mid \mathrm{lcm}[f(i), i < k] \cdot f(k))\\ &\vdash_{\mathrm{PA}} \mathrm{lcm}[f(i), i < \mathbf{S}k] \mid \mathrm{lcm}[f(i), i < k] \cdot f(k) && (2.)\\ &\vdash_{\mathrm{PA}} p \mid \mathrm{lcm}[f(i), i < k] \cdot f(k) && (2.23.3)\\ &\vdash_{\mathrm{PA}} p \mid \mathrm{lcm}[f(i), i < k] \vee p \mid f(k). && (2.26) \end{aligned}$$

Using $(\vee 1)$, we can now consider the two cases obtained above separately. The case $p \mid f(k)$ implies (19) clearly. The other case follows by making use of the induction hypothesis.

⊣

The following proposition indicates that any $x > \underline{1}$ has a prime divisor.

**Proposition 2.34.** $\vdash_{\mathrm{PA}} \forall x(x > \underline{1} \to \exists p(\mathrm{prime}(p) \wedge p \mid x))$.

*Proof.* We will use strong induction to prove $\vdash_{\mathrm{PA}} \forall x \varphi(x)$ where $\varphi(x)$ denotes the formula $(x > \underline{1} \to \exists p(\mathrm{prime}(p) \wedge p \mid x)$. Since the cases $x = \mathbf{0}$ and $x = \underline{1}$ are obvious, we have to verify

$$\forall z < x \varphi(z), x > \underline{1} \vdash_{\mathrm{PA}} \varphi(x) \tag{20}$$

which implies the claim by (DT) and strong induction. By $(\vee 2)$ it suffices to show

$$\forall z < x \varphi(z), x > \underline{1}, \mathrm{prime}(x) \vdash_{\mathrm{PA}} \varphi(x), \tag{21}$$

$$\forall z < x \varphi(z), x > \underline{1}, \neg\mathrm{prime}(x) \vdash_{\mathrm{PA}} \varphi(x). \tag{22}$$

The first claim follows from 2.23.1 and $(\wedge)$. In order to show (22) we note

$$\begin{aligned} \neg\mathrm{prime}(x) &\equiv_{\mathrm{PA}} \neg(x > \underline{1} \wedge \forall y(y \mid x \to (y = \underline{1} \vee y = x))) && (2.30)\\ &\equiv_{\mathrm{PA}} \neg(x > \underline{1}) \vee \neg(\forall y(y \mid x \to (y = \underline{1} \vee y = x))) && (\mathrm{F}.1)\\ &\equiv_{\mathrm{PA}} \neg(x > \underline{1}) \vee \exists y(\neg(\neg y \mid x \vee (y = \underline{1} \vee y = x))) && (\mathrm{K}.1, \mathrm{E})\\ &\equiv_{\mathrm{PA}} \neg(x > \underline{1}) \vee \exists y(y \mid x \wedge \neg(y = \underline{1} \vee y = x)) && (\mathrm{F}.2, \mathrm{A})\\ &\equiv_{\mathrm{PA}} \neg(x > \underline{1}) \vee \exists y(y \mid x \wedge y \neq \underline{1} \wedge y \neq x). && (\mathrm{F}.2, \mathrm{C}.2) \end{aligned}$$

By (A) and ($\vee$3) we thus obtain $\forall z < x\varphi(z), x > \underline{1}, \neg\text{prime}(x) \vdash_{\text{PA}} \exists y(y \mid x \wedge y \neq \underline{1} \wedge y \neq x)$. This implies

$$\begin{aligned}\forall z < x\varphi(z), x > \underline{1}, y \mid x \wedge y \neq \underline{1} \wedge y \neq x &\vdash_{\text{PA}} y < x \wedge y > \underline{1} \\ &\vdash_{\text{PA}} \exists p(\text{prime}(p) \wedge p \mid y)\end{aligned}$$

and thus

$$\begin{aligned}\forall z < x\varphi(z), x > \underline{1}, y \mid x \wedge y \neq \underline{1} \wedge y \neq x, \text{prime}(p) \wedge p \mid y &\vdash_{\text{PA}} p \mid x \\ &\vdash_{\text{PA}} \varphi(x).\end{aligned} \tag{2.23.3}$$

By applying twice ($\exists$), we obtain (20). $\dashv$

The previous proposition enables us to weaken substantially the definition of relative primiality.

**Proposition 2.35.** $\vdash_{\text{PA}} \forall x\forall y\big[\text{coprime}(x, y) \leftrightarrow \forall p(\text{prime}(p) \rightarrow \neg(p \mid x \wedge p \mid y))\big]$.

*Proof.* Due to ($\leftrightarrow$), we can split the proof into two parts, where we omit the trivial cases $x = \mathbf{0}$ respectively $y = \mathbf{0}$.

(23) $\quad \text{coprime}(x, y) \vdash_{\text{PA}} x \geq \underline{1} \wedge y \geq \underline{1} \wedge \forall p(\text{prime}(p) \rightarrow \neg(p \mid x \wedge p \mid y))$,

(24) $\quad x \geq \underline{1} \wedge y \geq \underline{1} \wedge \forall p(\text{prime}(p) \rightarrow \neg(p \mid x \wedge p \mid y)) \vdash_{\text{PA}} \text{coprime}(x, y)$.

Claim (23) can easily be shown using contraposition

$$\begin{aligned}\text{coprime}(x, y), p \mid x \wedge p \mid y &\vdash_{\text{PA}} p = \underline{1} \\ &\vdash_{\text{PA}} \neg\text{prime}(p).\end{aligned}$$

This implies (23), since $\text{coprime}(x, y) \vdash_{\text{PA}} x \geq \underline{1} \wedge y \geq \underline{1}$ is given by definition. In order to prove (24), we use contradiction. Again, the condition $x \geq \underline{1} \wedge y \geq \underline{1}$ is trivial and can thus be ignored.

$$\forall p(\text{prime}(p) \rightarrow \neg(p \mid x \wedge p \mid y)), z \mid x \wedge z \mid y, z > \underline{1} \vdash_{\text{PA}} \exists p(\text{prime}(p) \wedge p \mid z). \tag{2.34}$$

Then the transitivity of divisibility implies

$$\forall p(\text{prime}(p) \rightarrow \neg(p \mid x \wedge p \mid y)), z \mid x \wedge z \mid y, z > \underline{1}, \text{prime}(p) \wedge p \mid z \vdash_{\text{PA}} p \mid x \wedge p \mid y$$

which is obviously a contradiction, thus the claim follows from ($\exists$). $\dashv$

The above preparations finally allow the formulation and proof of the Chinese Remainder Theorem within Peano Arithmetic.

**Theorem 2.36** (Chinese Remainder Theorem)**.** *Let $f$ and $g$ be two unary functions which can be defined in PA. Then we have*

$$\begin{aligned}\vdash_{\text{PA}} \forall k\Big[\big[\forall i < k(\underline{1} < g(i) \wedge f(i) < g(i)) \wedge \forall i\forall j(i < j \wedge j < k \rightarrow \text{coprime}(g(i), g(j))\big] \\ \rightarrow \exists x\forall i < k(\text{rest}(x, g(i)) = f(i))\Big].\end{aligned}$$

*Proof.* We set

$$\varphi(k) = \big[\forall i < k(\underline{1} < g(i) \wedge f(i) < g(i)) \wedge \forall i \forall j(i < j \wedge j < k \to \mathrm{coprime}(g(i), g(j))\big].$$

and

$$\psi(x,k) = \forall i < k(\mathrm{rest}(x.g(i)) = f(i)).$$

It suffices to verify

$$\vdash_{\mathrm{PA}} \forall k(\varphi(k) \to \exists x \psi(x,k)). \tag{25}$$

Since the case $k = \mathbf{0}$ is obvious due to $\vdash_{\mathrm{PA}} \forall i \neg(i < \mathbf{0})$ by taking $x = \underline{1}$, we can use induction on $k$ with lower bound $\underline{1}$. The base case for $k = \underline{1}$ is also clear by taking $x = f(\mathbf{0})$ because of $\varphi(\underline{1}) \vdash_{\mathrm{PA}} f(\mathbf{0}) < g(\mathbf{0})$.
The premises to conclude the induction step are the formulas in $\{\varphi(k) \to \exists x \psi(x,k), \varphi(\mathbf{S}k)\}$. As a consequence of $\vdash_{\mathrm{PA}} \varphi(\mathbf{S}k) \to \varphi(k)$ and $(\exists)$ it is sufficient to presuppose only $T = \{\psi(x,k), \varphi(\mathbf{S}k)\}$. Firstly, we show that $\mathrm{lcm}[g(i), i < k]$ and $g(k)$ are coprime.

$$T, \mathrm{prime}(p) \wedge p \mid \mathrm{lcm}[g(i), i < k] \vdash_{\mathrm{PA}} \exists i < k(p \mid g(i)). \tag{2.33.3}$$

This leads to

$$\begin{aligned} T, \mathrm{prime}(p), p \mid \mathrm{lcm}[g(i), i < k], i < k, p \mid g(i) &\vdash_{\mathrm{PA}} \mathrm{coprime}(g(i), g(k)) \\ &\vdash_{\mathrm{PA}} \neg(p \mid g(i) \wedge p \mid g(k)) && (2.35) \\ &\vdash_{\mathrm{PA}} \neg(p \mid g(i)) \vee \neg(p \mid g(k)) && (\mathrm{F}.1) \\ &\vdash_{\mathrm{PA}} \neg(p \mid g(k)) && (\vee 4) \\ &\vdash_{\mathrm{PA}} \neg(p \mid \mathrm{lcm}[g(i), i < k] \wedge p \mid g(k)). && (\mathrm{B}.1) \end{aligned}$$

Again making use of Proposition 2.35 and Bézout's Lemma, we obtain as desired

$$\begin{aligned} T &\vdash_{\mathrm{PA}} \mathrm{coprime}(g(k), \mathrm{lcm}[g(i), i < k]) && (2.35) \\ &\vdash_{\mathrm{PA}} \exists u \exists v(\mathrm{lcm}[g(i), i < k]u + \underline{1} = g(k)v. && (2.27) \end{aligned}$$

We set $S = \{a = \mathrm{lcm}[g(i), i < k], u' = u(x + (a - \underline{1})f(k)), v' = (x + (a - \underline{1})f(k))v, x' = a(u' + f(k)) + x\}$. In the following, we will omit the details, as they only involve standard arithmetical calculations.

$$\begin{aligned} T \cup S, au + \underline{1} = g(k)v \vdash_{\mathrm{PA}} & au' + af(k) - f(k) + x \\ &= au' + x + (a - \underline{1})f(k) \\ &= au(x + (a - \underline{1})f(k)) + x + (a - \underline{1})f(k) \\ &= x(au + \underline{1}) + (a - \underline{1})(au + \underline{1})f(k) \\ &= xg(k)v + (a - \underline{1})g(k)vf(k) = v'g(k). \end{aligned}$$

Thus we obtain $T \cup S, au + \underline{1} = g(k)v \vdash_{\mathrm{PA}} x' = a(u' + f(k)) = v'g(k) + f(k)$. In order to prove that $x'$ satisfies the desired condition indeed, we need

$$T \cup S, i < k \vdash_{\mathrm{PA}} \mathrm{rest}(x', g(i)) = f(i), \tag{26}$$

$$T \cup S \vdash_{\mathrm{PA}} \mathrm{rest}(x', g(k)) = f(k). \tag{27}$$

The induction step then follows using $(\vee 1)$ applied to $\vdash_{\mathrm{PA}} i < \mathbf{S}k \leftrightarrow i < k \vee i = k$, hence it is enough to prove the above claims. The first one holds due to

$$\begin{aligned} T \cup S, i < k &\vdash_{\mathrm{PA}} g(i) \mid a && (2.33.1)\\ &\vdash_{\mathrm{PA}} g(i) \mid a(u' + f(k)) && (2.24.2)\\ &\vdash_{\mathrm{PA}} \mathrm{rest}(x', g(i)) = \mathrm{rest}(x, g(i)) = f(i) && (2.25.2) \end{aligned}$$

and (27) is a result of

$$T \cup S, i < k \vdash_{\mathrm{PA}} \mathrm{rest}(x', g(k)) = \mathrm{rest}(f(k), g(k)) = f(k). \tag{2.25}$$

⊣

## 2.4 Gödel's $\beta$-function

In the following, we will introduce the so-called $\beta$-function which allows the encoding of finite sequences by a single number.

**Lemma 2.37.** *Let $f$ be a unary function. Then one has*

$$\vdash_{\mathrm{PA}} \forall k > \mathbf{0} \exists! x (\exists i < k (f(i) = x) \wedge \forall i < k (f(i) \leq x)).$$

*Proof.* The existence can be shown using the induction schema $(\mathrm{I}_{\varphi_{\geq \underline{1}}})$ for $\varphi(k) = \exists x (\exists i < k(f(i) = x) \wedge \forall i < k(f(i) \leq x))$. The base case (i.e. the case $k = \underline{1}$) is clear by taking $x = f(\mathbf{0})$. Due to

$$k \geq \underline{1}, \exists i < k (f(i) = x) \wedge \forall i < k (f(i) \leq x) \vdash_{\mathrm{PA}} f(k) \leq x \vee f(k) > x$$

we can use $(\vee 1)$ to consider each case separately. Firstly, we note

$$\begin{aligned} k \geq \underline{1}, \exists i < k (f(i) = x) \wedge \forall i < k (f(i) \leq x), f(k) \leq x &\vdash_{\mathrm{PA}} \forall i < \mathbf{S}k (f(i) \leq x)\\ &\vdash_{\mathrm{PA}} \varphi(\mathbf{S}k). \end{aligned}$$

In the second case, we can choose $f(k)$ as the maximum.

$$\begin{aligned} k \geq \underline{1}, \exists i < k (f(i) = x) \wedge \forall i < k (f(i) \leq x), f(k) > x &\vdash_{\mathrm{PA}} \forall i < k (f(i) \leq x) \wedge x \leq f(k)\\ &\vdash_{\mathrm{PA}} \forall i < k (f(i) \leq f(k)) \qquad (2.9.4)\\ &\vdash_{\mathrm{PA}} \varphi(\mathbf{S}k). \end{aligned}$$

Hence the induction is a consequence of $(\exists)$. In order to prove uniqueness, we set $\psi(x, k) = \exists i < k (f(i) = x) \wedge \forall i < k (f(i) \leq x)$.

$$\begin{aligned} \psi(x, k), \psi(y, k), i < k \wedge f(i) = x, j < k \wedge f(j) = y &\vdash_{\mathrm{PA}} x = f(i) \leq y\\ &\vdash_{\mathrm{PA}} y = f(j) \leq x\\ &\vdash_{\mathrm{PA}} x = y. \qquad (2.9.3) \end{aligned}$$

Again, $(\exists)$ proves the assertion. ⊣

**Definition 2.38.** Let $f$ be a unary function, which may also depend on some parameters. We can define

$$\max[f(i), i < k] = x :\leftrightarrow \exists i < k(f(i) = x) \wedge \forall i < k(f(i) \leq x),$$
$$\max(x, y) = z :\leftrightarrow (x \geq y \wedge z = x) \vee (x < z \wedge z = y).$$

Furthermore, we can introduce the so-called $\alpha$-function with the aid of which the $\beta$-function is constructed. We can then formulate and prove Gödel's $\beta$-Function-Lemma which will be a direct consequence of the next two propositions.

**Definition 2.39.** We extend the language $\mathcal{L}_{\mathrm{PA}}$ to include the ternary function symbol

$$\alpha(x, y, i) := \mathrm{rest}(x, \underline{1} + (i + \underline{1}) \cdot y).$$

**Proposition 2.40.** *Let $f$ be a unary function which may depend on some parameters. Then the following holds:*

$$\vdash_{\mathrm{PA}} \forall k \exists x \exists y \forall i < k(\alpha(x, y, i) = f(i)).$$

*Proof.* We set $T = \{m = \max(k, \max[f(i), i < k]) + \underline{1}, y = \mathrm{lcm}[i + \underline{1}, i < m]\}$ and we have

$$T \vdash_{\mathrm{PA}} m > \max(k, \max[f(i), i < k])$$
$$\vdash_{\mathrm{PA}} m > k \wedge \forall i < k(m > f(i)). \tag{28}$$

We would like to prove

$$T \vdash_{\mathrm{PA}} \forall i \forall j(i < j \wedge j < k \to \mathrm{coprime}(\underline{1} + (i + \underline{1})y, \underline{1} + (j + \underline{1})y)). \tag{29}$$

For the verification of (29) we apply Proposition 2.35 and the Chinese Remainder Theorem. We set $T' = T \cup \{i < j, j < k, \mathrm{prime}(p), p \mid (\underline{1} + (i + \underline{1})y), p \mid (\underline{1} + (j + \underline{1})y)\}$.

$$T' \vdash_{\mathrm{PA}} \underline{1} + (i + \underline{1})y < \underline{1} + (j + \underline{1})y \tag{2.11}$$
$$\vdash_{\mathrm{PA}} p \mid (\underline{1} + (j + \underline{1})y - (\underline{1} + (i + \underline{1})y = (j - i)y \tag{2.24.1}$$
$$\vdash_{\mathrm{PA}} p \mid (j - i) \vee p \mid y.$$

Thus we can consider each case separately using $(\vee 1)$.

$$T', p \mid (j - i) \vdash_{\mathrm{PA}} \underline{1} \leq j - i < k < m \tag{28}$$
$$\vdash_{\mathrm{PA}} (j - i) - \underline{1} < m$$
$$\vdash_{\mathrm{PA}} j - i = ((j - i) - \underline{1}) + \underline{1} \mid y$$
$$\vdash_{\mathrm{PA}} p \mid y. \tag{2.23.3}$$

This obviously leads to

$$T' \vdash_{\mathrm{PA}} p \mid y$$
$$\vdash_{\mathrm{PA}} p \mid (i + \underline{1})y \tag{2.24.2}$$
$$\vdash_{\mathrm{PA}} p \mid (\underline{1} + (i + \underline{1})y) - (i + \underline{1})y = \underline{1}, \tag{2.24.1}$$

which contradicts $\mathrm{prime}(p)$. Hence $(\lightning)$ implies (29). Now we can apply the chinese remainder theorem for $g(i) = g_y(i) = 1 + (i + 1)y$ and $f$ and the claim follows. ⊣

This proposition constitutes the basis for the encoding of finite sequences, and the following proposition states that such sequences can always be extended.

**Proposition 2.41.** $\vdash_{\mathrm{PA}} \forall x\forall y\forall k\forall z\exists x'\exists y'[\alpha(x',y',k) = z \wedge \forall i < k(\alpha(x',y',i) = \alpha(x,y,i))]$.

*Proof.* We define $f(i) = r \leftrightarrow (i < k \wedge \alpha(x,y,i) = r) \vee (i \geq k \wedge r = z)$. Then the proposition follows directly from the previous proposition. ⊣

The $\alpha$-function allows the encoding of any finite sequence by a pair $(x,y)$ by regarding the sequence as a function $f$ and considering $f(i), i < k$. Thus the sequence is characterizied uniquely by $\alpha(x,y,i), i < k$. However, this approach can still be improved by encoding pairs as single numbers.

**Lemma 2.42.** $\vdash_{\mathrm{PA}} \forall x(\underline{2} \mid x \vee \underline{2} \mid \mathbf{S}x)$.

*Proof.* Let $\varphi(x) = \underline{2} \mid x \vee \underline{2} \mid \mathbf{S}x$. We show $\vdash_{\mathrm{PA}} \forall x\varphi(x)$ using induction on $x$.

The base case is a direct consequence of ($\mathrm{PA}_5$). For the induction step we have to consider the cases $\underline{2} \mid x$ respectively $\underline{2} \mid \mathbf{S}x$ separately (using ($\vee 1$)). We state only the first case.

$$\begin{aligned} \underline{2} \cdot y = x &\vdash_{\mathrm{PA}} \underline{2} \cdot \mathbf{S}y \overset{\mathrm{PA}_6}{=} (\underline{2} \cdot y) + \underline{2} \overset{\mathrm{L}_{18}}{=} x + \underline{2} \overset{\mathrm{PA}_4}{=} \mathbf{S}(\mathbf{S}x) \\ &\vdash_{\mathrm{PA}} \underline{2} \mid \mathbf{S}(\mathbf{S}x) \\ &\vdash_{\mathrm{PA}} \varphi(\mathbf{S}x). \end{aligned} \tag{$\mathrm{L}_7$}$$

Hence ($\exists$) implies $\underline{2} \mid x \vdash_{\mathrm{PA}} \varphi(\mathbf{S}x)$. ⊣

**Definition 2.43.** The above lemma shows $\vdash_{\mathrm{PA}} \forall x\forall y(\underline{2} \mid (x + y + \underline{1})(x + y))$. This legitimizes the definition

$$\langle x,y\rangle := \frac{(x + y + \underline{1})(x + y)}{\underline{2}} + y.$$

**Lemma 2.44.** $\vdash_{\mathrm{PA}} \forall z\exists!x\exists!y(\langle x,y\rangle = z)$.

*Proof.* The statement follows from

(30) $\vdash_{\mathrm{PA}} \forall z\exists x\exists y(\langle x,y\rangle = z)$

(31) $\vdash_{\mathrm{PA}} \forall x\forall y\forall u\forall v(\langle x,y\rangle = \langle u,v\rangle \to x = u \wedge y = v)$,

since (30) proves the existence and (31) proves uniqueness. Firstly, we show (30). We set $\varphi(z) = \exists x\exists y(\langle x,y\rangle = z)$ and we show $\vdash_{\mathrm{PA}} \forall z\varphi(z)$ using induction. The base case follows from $\vdash_{\mathrm{PA}} \langle \mathbf{0},\mathbf{0}\rangle = \mathbf{0}$. The induction step can be proved by cases; inductively, one can easily show

$$y \neq \mathbf{0} \vdash_{\mathrm{PA}} \frac{x}{y} + z = \frac{x + zy}{y}. \tag{32}$$

This leads to the case $x = \mathbf{0}$:

$$\langle x, y\rangle = z, x = \mathbf{0} \vdash_{\mathrm{PA}} \mathbf{S}z = z + \underline{1} = \frac{(y+\underline{1})y}{\underline{2}} + y + \underline{1} \overset{32}{=} \frac{(y+\underline{1})y + (y+1)\underline{2}}{\underline{2}}$$

$$= \frac{(y+\underline{1})(y+\underline{2})}{\underline{2}} = \langle y + \underline{1}, \mathbf{0}\rangle. \tag{33}$$

We consider the case $x > \mathbf{0}$:

$$\begin{aligned}\langle x, y\rangle = z, x > \mathbf{0} &\vdash_{\mathrm{PA}} (x - \underline{1}) + \underline{1} = x \\ &\vdash_{\mathrm{PA}} x + y + \underline{1} = (x - \underline{1}) + \underline{1} + y + \underline{1} = (x - \underline{1}) + (y + \underline{1}) + \underline{1} \\ &\vdash_{\mathrm{PA}} x + y = (x - \underline{1}) + (y + \underline{1}). \end{aligned} \tag{2.5}$$

Thus we obtain

$$\langle x, y\rangle = z, x > \mathbf{0} \vdash_{\mathrm{PA}} \mathbf{S}z = z + \underline{1} = (\frac{(x+y+\underline{1})(x+y)}{\underline{2}} + y) + \underline{1}$$

$$= \frac{((x-\underline{1}) + (y+\underline{1}) + \underline{1})((x-\underline{1}) + (y+\underline{1}))}{\underline{2}} + (y + \underline{1})$$

$$= \langle x - \underline{1}, y + \underline{1}\rangle. \tag{34}$$

All in all, (33) and (34) imply $\langle x, y\rangle = z \vdash_{\mathrm{PA}} \varphi(\mathbf{S}z)$. The induction step is then a consequence of $(\exists)$.

In order to prove (31) one has to show first inductively

$$z \mid x, z \mid y, x \leq y \vdash_{\mathrm{PA}} \frac{x}{z} \leq \frac{y}{z} \tag{35}$$

the proof of which shall be omitted. Now we use contradiction to get

$$\langle x, y\rangle = \langle u, v\rangle \vdash_{\mathrm{PA}} x + y = u + v. \tag{36}$$

$$\begin{aligned}\langle x, y\rangle = \langle u, v\rangle, x + y < u + v &\vdash_{\mathrm{PA}} x + y + \underline{1} = \mathbf{S}(x + y) \leq u + v \\ &\vdash_{\mathrm{PA}} \langle x, y\rangle = \frac{(x+y+\underline{1})(x+y)}{\underline{2}} + y \\ &< \frac{(x+y+\underline{1})(x+y)}{\underline{2}} + x + y + \underline{1} \\ &\overset{(32)}{=} \frac{(x+y+\underline{1})(x+y) + (x+y+\underline{1})\underline{2}}{\underline{2}} \\ &= \frac{(x+y+\underline{1})(x+y+\underline{2})}{\underline{2}} \leq \frac{(u+v)(u+v+\underline{1})}{\underline{2}} \\ &= \langle u, v\rangle = \langle x, y\rangle\end{aligned}$$

which is a contradiction. Similarly, one can also rule out the case $x + y > u + v$ which means that (36) holds. Furthermore, one has

$$\langle x, y\rangle = \langle u, v\rangle \vdash_{\mathrm{PA}} y = \langle x, y\rangle - \frac{(x+y)(x+y+\underline{1})}{\underline{2}} \overset{(35)}{=} \langle u, v\rangle - \frac{(u+v)(u+v+\underline{1})}{\underline{2}} = v$$

$$\vdash_{\mathrm{PA}} x = (x + y) - y = (u + v) - v = u \tag{36}$$

$$\vdash_{\mathrm{PA}} x = u \wedge y = v. \tag{$\wedge$}$$

Thus we have shown that (31) is satisfied. ⊣

**Definition 2.45.** The previous lemma legitimizes the following definitions, in particular that of the $\beta$-function.

$$\begin{aligned} \text{first}(z) = x &:\leftrightarrow \exists y(\langle x, y\rangle = z), \\ \text{second}(z) = y &:\leftrightarrow \exists x(\langle x, y\rangle = z). \end{aligned}$$

Thus we have $\vdash_{\text{PA}} \forall z(\langle \text{first}(z), \text{second}(z)\rangle = z)$. Furthermore, we define

$$\beta(x, i) = z :\leftrightarrow \alpha(\text{first}(x), \text{second}(x), i) = z.$$

The $\beta$-function allows us to enconde any finite sequence as $\beta(x, i), i < k$ for some $x, k$. For the gödelization of Peano Arithmetic, it makes sense to use the alternative definitions

$$\begin{aligned} \text{length}(x) &:= \text{second}(x), \\ (x)_i &:= \beta(\text{first}(x), i), \\ (x)_{\text{last}} &:= (x)_{\text{length}(x)-\underline{1}}. \end{aligned}$$

With these notations, one can restate Propositions 2.40 and 2.41 equivalently as

**Theorem 2.46** ($\beta$-Function-Lemma)**.** *Let $f$ be a unary function in PA. Then we have*

1. $\vdash_{\text{PA}} \forall k \exists x \forall i < k(\beta(x, i) = f(i))$,
2. $\vdash_{\text{PA}} \forall x \forall k \forall y \exists x'[\beta(x', k) = y \wedge \forall i < k(\beta(x', i) = \beta(x, i))]$.

# Chapter 3

# Encoding finite sequences and gödelization

In this chapter, we will use a method called gödelization in order to express within PA that some number encodes a variable, term or formula. Furthermore, this permits the introduction of a new relation provable($x$) which, in the case that $x$ is the code of a formula, states that the formula encoded by $x$ is provable in PA.

Unlike for the previous chapter, we require the existence of the standard model $\mathbb{N}$ of PA. Therefore the first step will be the introduction of natural numbers in PA as terms of the form $\mathbf{S}\ldots\mathbf{S0}$.

## 3.1 Natural numbers in Peano Arithmetic

*Notation.* We can define the natural numbers of the standard model in Peano Arithmetic using the successor function and the zero element by considering $\underline{n}$ to be the $n$-th successor of $\mathbf{0}$ for any $n \in \mathbb{N}$ (i.e. $\underline{n} = \underbrace{\mathbf{S}\ldots\mathbf{S}}_{n}\mathbf{0}$); more formally, this signifies

$$\underline{0} := \mathbf{0},$$
$$\underline{n+1} = \mathbf{S}\underline{n}$$

for any $n \in \mathbb{N}$.

This means that any model of Peano Arithmetic has to contain a set isomorphic to the set of natural numbers. In particular, it is possible to state and prove number theoretical results concerning natural numbers of the form $\underline{n}$ in PA; however, in order to prove a statement in PA for all $\underline{n}$, $n \in \mathbb{N}$, we have to use metainduction which means that we show that for each $n$ the statement is derivable from PA using induction over $n \in \mathbb{N}$ in the "background". The proof of the following proposition is an example of metainduction.

**Proposition 3.1.** *Any two natural numbers $n, m \in \mathbb{N}$ satisfy the properties*

(N1) $\vdash_{\mathrm{PA}} \underline{m} + \underline{n} = \underline{m+n}$,

(N2) $\vdash_{\mathrm{PA}} \underline{m} \cdot \underline{n} = \underline{mn}$,

(N3) $m = n \Rightarrow \vdash_{\mathrm{PA}} \underline{m} = \underline{n}$ and $m \neq n \Rightarrow \vdash_{\mathrm{PA}} \underline{m} \neq \underline{n}$,

(N4) $m \leq n \Rightarrow \vdash_{\mathrm{PA}} \underline{m} \leq \underline{n}$ and $m \not\leq n \Rightarrow \vdash_{\mathrm{PA}} \underline{m} \not\leq \underline{n}$,

(N5) $\vdash_{\mathrm{PA}} \forall x(x \leq \underline{n} \leftrightarrow \bigvee_{k=0}^{n} (x = \underline{k}))$.

*Proof.*

(N1) We use induction over $m \in \mathbb{N}$. For $m = 0$ the statement to be shown is $\vdash_{\mathrm{PA}} \underline{0} + \underline{n} = \underline{0+n}$ which is obviously true since $\underline{0}$ is $\mathbf{0}$. For the induction step we assume that $\vdash_{\mathrm{PA}} \underline{m} + \underline{n} = \underline{m+n}$ holds and conclude

$$\begin{aligned} \vdash_{\mathrm{PA}} \underline{m+1} + \underline{n} &= \mathbf{S}\underline{m} + \underline{n} = \underline{1} + \underline{m} + \underline{n} = \underline{1} + \underline{m+n} = \mathbf{S}(\underline{m+n}) \\ &= \underline{(m+n)+1} = \underline{(m+1)+n}. \end{aligned}$$

(N2) Again, we use induction over $m$. The case $m = 0$ is clear. We assume that $\vdash_{\mathrm{PA}} \underline{m} \cdot \underline{n} = \underline{mn}$ is satisfied. Then we obtain the claim using the induction hypothesis and (N1):

$$\begin{aligned} \vdash_{\mathrm{PA}} \underline{m+1} \cdot \underline{n} &= (\underline{m} + \underline{1})\underline{n} = \underline{m} \cdot \underline{n} + \underline{1} \cdot \underline{n} \\ &= \underline{mn} + \underline{n} = \underline{mn+n} = \underline{(m+1)n}. \end{aligned}$$

(N3) The first statement is trivial. Secondly, suppose that $m < n$. Then there exists $k \in \mathbb{N}$ such that $k \neq 0$ and $m + k = n$. Condition (N1) implies $\vdash_{\mathrm{PA}} \underline{m} + \underline{k} = \underline{m+k} = \underline{n}$. Since $k \neq 0$, there exists $l \in \mathbb{N}$ such that $k = l + 1$. Therefore $\vdash_{\mathrm{PA}} \underline{k} = \underline{l+1} = \mathbf{S}\underline{l}$ and hence by ($\mathrm{PA}_1$) we obtain $\vdash_{\mathrm{PA}} \underline{k} \neq \mathbf{0}$. The case $n < m$ can be handled in a similar way.

(N4) In (N3) we have shown that $m = n$ implies $\vdash_{\mathrm{PA}} \underline{m} = \underline{n}$ as well as $m < n$ implies $\vdash_{\mathrm{PA}} \underline{m} < \underline{n}$. Thus the first condition is satisfied. Note that $m \not\leq n$ is equivalent to $m > n$ from which we can conclude (again as in the proof of (N3)) that $\vdash_{\mathrm{PA}} \underline{m} > \underline{n}$. Hence the second statement holds.

(N5) The direction ($\leftarrow$) is a consequence of the previous statement. We show ($\rightarrow$) by induction over $n$. The base case is trivial. Suppose that

$$\vdash_{\mathrm{PA}} x \leq \underline{n} \rightarrow \bigvee_{k=0}^{n} (x = \underline{k})$$

is satisfied. Now we can distinguish between two cases due to $x \leq \underline{n+1} = \mathbf{S}\underline{n} \vdash_{\mathrm{PA}} x \leq \underline{n} \vee x = \underline{n+1}$. The first case follows from the induction hypothesis and the second one is trivial.

⊣

**Definition 3.2.** Suppose that $\delta(\vec{x}, y)$ is a formula satisying $\vdash_{\mathrm{PA}} \forall\vec{x}\exists!y\delta(\vec{x}, y)$. Then we can introduce an $n$-ary function symbol $f$ in PA as $f(\vec{x}) = y :\leftrightarrow \delta(\vec{x}, y)$. We say that $f$ is $\mathbb{N}$**-conform**, if $\vdash_{\mathrm{PA}} \delta(\underline{\vec{a}}, \underline{f^{\mathbb{N}}(\vec{a})})$ for all $\vec{a} \in \mathbb{N}^n$. Equivalently, this means that $\vdash_{\mathrm{PA}} f(\underline{\vec{a}}) = \underline{f^{\mathbb{N}}(\vec{a})}$.

**Definition 3.3.** An $n$-ary relation symbol $R$ defined by $R(\vec{x}) :\leftrightarrow \delta(\vec{x})$ is called $\mathbb{N}$**-conform**, if for all $\vec{a} \in \mathbb{N}^n$ the properties

(a) if $\mathbb{N} \models \delta(\vec{a})$, then $\vdash_{\mathrm{PA}} \delta(\underline{\vec{a}})$, and

(b) if $\mathbb{N} \models \neg\delta(\vec{a})$, then $\vdash_{\mathrm{PA}} \neg\delta(\underline{\vec{a}})$

are satisfied.

*Example* 3.4. Note that (N1) and (N2) state that the binary functions $+$ and $\cdot$ (which are defined by the formulas $x_1 + x_2 = y, x_1 \cdot x_2 = y$) are $\mathbb{N}$-conform. Moreover, due to (N3) and (N4) we obtain the $\mathbb{N}$-conformity of the relations $=$ and $\leq$.

**Proposition 3.5.** *Let $\delta(\vec{x})$ (respectively $\delta(\vec{x}, y)$), $\delta_1(\vec{x})$ and $\delta_2(\vec{x})$ define $\mathbb{N}$-conform relations. Then so do $\neg\delta, \delta_1 \wedge \delta_2, \delta_1 \vee \delta_2, \delta_1 \to \delta_2, \exists y \leq f(\vec{x})\delta(\vec{x}, y)$, and $\forall y \leq f(\vec{x})\delta(\vec{x}, y)$, where $f$ is a function which is $\mathbb{N}$-conform.*

*Proof.* Since $\delta_1 \vee \delta_2 \equiv \neg(\neg\delta_1 \wedge \neg\delta_2), \delta_1 \to \delta_2 \equiv \neg(\delta_1 \wedge \neg\delta_2)$ and $\forall x \leq f(\vec{x})\delta(\vec{x}) \equiv \neg\exists y \leq f(\vec{x})\neg\delta(\vec{x}, y)$ it is enough to show that $\neg\delta, \delta_1 \wedge \delta_2$ and $\exists y \leq f(\vec{x})\delta(\vec{x}, y)$ are $\mathbb{N}$-conform.

- We assume that $\delta$ is $\mathbb{N}$-conform and show that so is $\neg\delta$. Let $\vec{a} \in \mathbb{N}^n$. For the first property, we assume $\mathbb{N} \models \neg\delta(\vec{a})$. Then since $\delta$ satisfies (b), we have $\vdash_{\mathrm{PA}} \neg\delta(\underline{\vec{a}})$. The second property can be shown similarly using $\neg\neg\delta \equiv \delta$.

- Suppose that $\delta_1$ and $\delta_2$ are $\mathbb{N}$-conform, and let $\vec{a} \in \mathbb{N}^n$. Firstly, we assume that $\mathbb{N} \models (\delta_1 \wedge \delta_2)(\vec{a})$. This means that $\mathbb{N} \models \delta_1(\vec{a})$ and $\mathbb{N} \models \delta_2(\vec{a})$. Therefore, by (a) we have $\vdash_{\mathrm{PA}} \delta_1(\underline{\vec{a}})$ and $\vdash_{\mathrm{PA}} \delta_2(\underline{\vec{a}})$. Hence, the first property is a consequence of $(\wedge)$. Secondly, suppose that $\mathbb{N} \models \neg(\delta_1 \wedge \delta_2)(\vec{a})$. We have by (F.1) that $\neg(\delta_1 \wedge \delta_2) \equiv \neg\delta_1 \vee \neg\delta_2$. This implies that either $\mathbb{N} \models \neg\delta_1(\vec{a})$ or $\mathbb{N} \models \neg\delta_2(\vec{a})$. Without loss of generality, we assume the former. Then by assumption we have

  $\vdash_{\mathrm{PA}} \neg\delta_1(\underline{\vec{a}})$ (b)
  $\vdash_{\mathrm{PA}} (\delta_1(\underline{\vec{a}}) \wedge \delta_2(\underline{\vec{a}})) \to \delta_1(\underline{\vec{a}})$ ($\mathrm{L}_3$)
  $\vdash_{\mathrm{PA}} \neg\delta_1(\underline{\vec{a}}) \to \neg(\delta_1(\underline{\vec{a}}) \wedge \delta_2(\underline{\vec{a}}))$ (B.1)
  $\vdash_{\mathrm{PA}} \neg(\delta_1(\underline{\vec{a}}) \wedge \delta_2(\underline{\vec{a}}))$. (MP)

  This proves (b).

- We assume that $\delta$ and $f$ are $\mathbb{N}$-conform. Let $\vec{a} \in \mathbb{N}^n$ be arbitrary. Firstly, suppose that $\mathbb{N} \models \exists y \leq f^{\mathbb{N}}(\vec{a})\delta(y, \vec{a})$. Hence there exists $b \in \mathbb{N}$ such that $b \leq f^{\mathbb{N}}(\vec{a})$

with $\mathbb{N} \models \delta(\vec{a}, b)$. By $\mathbb{N}$-conformity of $\delta$ we obtain $\vdash_{\mathrm{PA}} \delta(\underline{\vec{a}}, \underline{b})$ and (N4) states that $\vdash_{\mathrm{PA}} \underline{b} \leq \underline{f^{\mathbb{N}}(\vec{a})}$. Furthermore, using that $f$ is $\mathbb{N}$-conform, we can deduce $\vdash_{\mathrm{PA}} \underline{b} \leq f(\underline{\vec{a}})$ and therefore (a) is satisfied. Secondly, suppose that $\mathbb{N} \models \neg\exists y \leq f(\vec{a})\delta(\vec{a}, y)$. This signifies that there exists no $b \in \mathbb{N}$ such that $b \leq f^{\mathbb{N}}(\vec{a})$ and $\mathbb{N} \models \delta(\vec{a}, b)$. Therefore for all $b \leq n$ we have $\mathbb{N} \models \neg\delta(\vec{a}, b)$, where $n = f^{\mathbb{N}}(\vec{a})$. By $\mathbb{N}$-conformity of $\delta$, we obtain

$$\vdash_{\mathrm{PA}} \neg\delta(\underline{\vec{a}}, \underline{b}) \tag{1}$$

for all such $b \leq n$. We prove (b) by contradiction.

$$\begin{aligned} y \leq f(\underline{\vec{a}}) \wedge \delta(\underline{\vec{a}}, y) &\vdash_{\mathrm{PA}} y \leq \underline{n} && (f \text{ } \mathbb{N}\text{-conform}) \\ &\vdash_{\mathrm{PA}} \bigvee_{k=0}^{n} y = \underline{k} && (\mathrm{N5}) \\ &\vdash_{\mathrm{PA}} \bigvee_{k=0}^{n} \delta(\underline{\vec{a}}, \underline{k}). \end{aligned}$$

This contradicts (1) and due to $(\exists)$ so does $\exists y \leq f(\underline{\vec{a}})\delta(\underline{\vec{a}}, y)$. This concludes the proof of (b).

⊣

**Proposition 3.6.** *Let $f$ be a function in PA defined by the formula $\delta(\vec{x}, y)$. If $f$ satisfies one of the conditions*

1. *the relation given by $\delta$ is $\mathbb{N}$-conform, or*
2. *the function $f(\vec{x})$ is $g(f_1(\vec{x}), \ldots, f_k(\vec{x}))$ for $\mathbb{N}$-conform functions $g, f_1, \ldots, f_k$,*

*then $f$ is $\mathbb{N}$-conform.*

*Proof.* 1. Let $\vec{a} \in \mathbb{N}^n$ and $b = f^{\mathbb{N}}(\vec{a})$. Then obviously $\mathbb{N} \models \delta(\vec{a}, b)$. Since $\delta$ is $\mathbb{N}$-conform, this leads to $\vdash_{\mathrm{PA}} \delta(\underline{\vec{a}}, \underline{b})$. On the other hand, since $\delta$ defines a function, we know $\vdash_{\mathrm{PA}} \exists! y \delta(\underline{\vec{a}}, y)$ and hence $\vdash_{\mathrm{PA}} f(\underline{\vec{a}}) = \underline{b}$.

2. Let $\vec{a} \in \mathbb{N}^n$, $b_i^{\mathbb{N}} = f_i^{\mathbb{N}}(\vec{a})$ for all $i \in \{1, \ldots, k\}$ and $b = g^{\mathbb{N}}(\vec{b}) = g^{\mathbb{N}}(b_1, \ldots, b_k)$. Therefore, this means $f^{\mathbb{N}}(\vec{a}) = b$. Moreover, by $\mathbb{N}$-conformity of $f_i$ we have $\vdash_{\mathrm{PA}} f_i(\underline{\vec{a}}) = \underline{b_i}$ for all $i$. The same argument leads to

$$\vdash_{\mathrm{PA}} f(\underline{\vec{a}}) = g(f_1(\underline{\vec{a}}), \ldots, f_k(\underline{\vec{a}})) = g(\underline{\vec{b}}) = \underline{g^{\mathbb{N}}(\vec{b})} = \underline{f^{\mathbb{N}}(\vec{a})}.$$

⊣

*Remark* 3.7. The following two methods allow the construction of new $\mathbb{N}$-conform functions from $\mathbb{N}$-conform functions.

(i) If $f(x, y)$ is $\mathbb{N}$-conform, then so is $g(u, v) := f(x/v, y/v)$.

(ii) If $f(x)$ is $\mathbb{N}$-conform, then so is $g(x, y) := f(x)$.

More formally, the newly constructed formulas are defined by $\gamma(u, v, z) :\leftrightarrow \delta(x/v, y/u, z)$ respectively $\gamma(x, y, z) :\leftrightarrow \delta(x, z)$, where $\delta(x, y, z)$ respectively $\delta(x, z)$ defines $f$.

Furthermore, without much effort one can generalize each statement to $n$-ary functions $f$, where in the first case $g$ is obtained by permuting the variables of $f$ for any permutation $\pi \in \mathrm{S}_n$ and in the second case $g$ is the result of adding multiple fictional input variables.

*Remark* 3.8. Using Propositions 3.5 and 3.6 as well as Remark 3.7 one can easily show that all in the previous chapters newly introduced relations and functions are indeed $\mathbb{N}$-conform. For this, it suffices to show that all defining formulas are equivalent to formulas using only bounded quantification. One can show without much effort that the following relations satisfy

$$\begin{aligned} x \leq y &\equiv_{\mathrm{PA}} \exists r \leq y(x + r = y), \\ x \mid y &\equiv_{\mathrm{PA}} x > \mathbf{0} \wedge \exists z \leq y(y = xz), \\ \mathrm{prime}(x) &\equiv_{\mathrm{PA}} x \geq \underline{1} \wedge \forall y \leq x(y \mid x \to (y = \underline{1} \vee y = x), \\ \mathrm{coprime}(x, y) &\equiv_{\mathrm{PA}} x \geq \underline{1} \wedge y \geq \underline{1} \wedge \forall z \leq x(z \mid x \wedge z \mid y \to z = \underline{1}). \end{aligned}$$

and similarly for the functions

$$\begin{aligned} \mathrm{int\_div}(x, y) = z &\equiv_{\mathrm{PA}} (y = \mathbf{0} \wedge z = \mathbf{0}) \vee (y > \mathbf{0} \wedge \exists r < y(x = yz + r)), \\ \mathrm{rest}(x, y) = z &\equiv_{\mathrm{PA}} (y = \mathbf{0} \wedge z = \mathbf{0}) \vee (y > \mathbf{0} \wedge z < y \wedge \exists s \leq x(x = ys + z)), \\ \mathrm{first}(z) = x &\equiv_{\mathrm{PA}} \exists y \leq z(\langle x, y \rangle = z), \\ \mathrm{second}(z) = x &\equiv_{\mathrm{PA}} \exists x \leq z(\langle x, y \rangle = z). \end{aligned}$$

The $\mathbb{N}$-conformity of all other relations and functions are immediate consequences of 3.5, 3.6 and 3.7.

## 3.2 Encoding finite sequences

The goal of this section is to define a relation in Peano Arithmetic that states that a given number is the code of a finite sequence and indicate its fundamental properties as well as operations to concatenate and truncate finite sequences. The following definitions concerning finite sequences in PA are based on the ones presented in [Boo95].

**Definition 3.9.** Since the $\beta$-function does not produce a unique code, we take shortest possible code in order to encode finite sequences uniquely as follows:

$$\begin{aligned} \mathrm{seq}(s) &:\leftrightarrow \forall x < \mathrm{first}(s) \exists i < \mathrm{length}(s)(\beta(x, i) \neq (s)_i), \\ \mathrm{empty\_seq}(s) &:\leftrightarrow \mathrm{length}(s) = \mathbf{0}, \\ \mathrm{nseq}(s) &:\leftrightarrow \mathrm{seq}(s) \wedge \neg \mathrm{empty\_seq}(s). \end{aligned}$$

**Lemma 3.10.** $\vdash_{\mathrm{PA}} \forall s \forall s'((\mathrm{seq}(s) \wedge \mathrm{seq}(s') \wedge \mathrm{length}(s) = \mathrm{length}(s') \wedge \forall i < \mathrm{length}(s)((s)_i = (s')_i) \to s = s')$.

*Proof.* We set $T = \{\mathrm{seq}(s) \wedge \mathrm{seq}(s') \wedge \mathrm{length}(s) = \mathrm{length}(s') \wedge \forall i < \mathrm{length}(s) ((s)_i = (s')_i\}$ and we need to show $T \vdash_{\mathrm{PA}} s = s'$. By Lemma 2.44 it is sufficient to prove $T \vdash_{\mathrm{PA}} \mathrm{first}(s) = \mathrm{first}(s')$ which follows by contradiction from the definition of seq. ⊣

We can also cut parts of sequences off and concatenate two sequences.

**Lemma 3.11.** $\vdash_{\mathrm{PA}} \forall s \forall k \forall n(\mathrm{seq}(s) \wedge \mathrm{length}(s) = k \to \exists! s'(\mathrm{seq}(s') \wedge \mathrm{length}(s') = \mathbf{S}k \wedge \forall i < k((s')_i = (s)_i) \wedge (s')_k = n)$.

*Proof.* Uniqueness is a consequence of Lemma 3.10. For the existence we use

$$\mathrm{seq}(s), \mathrm{length}(s) = k \vdash_{\mathrm{PA}} \exists x[\beta(x,k) = n \wedge \forall i < k(\beta(x,i) = (s)_i)] \tag{2.46.1}$$

which, for $T = \{\mathrm{seq}(s), \mathrm{length}(s) = k, \beta(x,k) = n \wedge \forall i < k(\beta(x,i) = (s)_i), s' = \langle x, \mathbf{S}k\rangle\}$ leads to

$$\begin{aligned} T &\vdash_{\mathrm{PA}} \mathrm{length}(s') = \mathrm{second}(s') = \mathbf{S}k \\ &\vdash_{\mathrm{PA}} \forall i < k((s')_i = \beta(x,i) = (s)_i) \wedge (s')_k = \beta(x,k) = n. \end{aligned}$$

Thus by $(\exists)$ we obtain

$$\mathrm{seq}(s), \mathrm{length}(s) = k \vdash_{\mathrm{PA}} \exists s'(\mathrm{length}(s') = \mathbf{S}k \wedge \forall i < k((s')_i = (s)_i) \wedge (s)_k = n$$

and hence the Least Number Principle implies the result using the definition of seq. ⊣

**Proposition 3.12.** *The following statements hold:*

1. $\vdash_{\mathrm{PA}} \mathrm{seq}(s) \wedge \mathrm{length}(s) = k \wedge l \leq k \to \exists! s'(\mathrm{seq}(s') \wedge \mathrm{length}(s') = j \wedge \forall i < j((s')_i = (s)_i))$,
2. $\vdash_{\mathrm{PA}} \mathrm{seq}(s) \wedge \mathrm{seq}(s') \wedge \mathrm{length}(s) = k \wedge \mathrm{length}(s') = k' \to \exists! s''(\mathrm{seq}(s'') \wedge \mathrm{length}(s'') = k + k' \wedge \forall i < k + k'(i < k \to (s'')_i = (s)_i \wedge i \geq k \to (s'')_i = (s')_{i-k}))$.

The previous proposition allows the introduction of the following two operations on finite sequences in PA.

**Definition 3.13.** We define the binary functions $(s)_{<j}$ and $s * s'$ as

$$\begin{aligned} s_{<j} = s' :\leftrightarrow &(\mathrm{seq}(s) \wedge \mathrm{seq}(s') \wedge j \leq \mathrm{length}(s) \wedge \mathrm{length}(s') = j \wedge \forall i < j((s')_i = (s)_i)) \\ &\vee (\neg\mathrm{seq}(s) \wedge s' = \mathbf{0}), \end{aligned}$$

$$\begin{aligned} s * s' = s'' :\leftrightarrow &(\mathrm{seq}(s) \wedge \mathrm{seq}(s') \wedge \mathrm{seq}(s'') \wedge \mathrm{length}(s'') = \mathrm{length}(s) + \mathrm{length}(s') \wedge \\ &\forall i < \mathrm{length}(s'')(i < \mathrm{length}(s) \to (s'')_i = (s)_i) \wedge i \geq \mathrm{length}(s) \to (s'')_i \\ &= (s')_{i-\mathrm{length}(s)})) \vee (\neg\mathrm{seq}(s) \vee \neg\mathrm{seq}(s') \wedge s'' = \mathbf{0}). \end{aligned}$$

We note that the first operation allows cutting off at the end of some sequence and the second one permits two sequences to be concatenated.

*Remark* 3.14. One can easily show that $*$ is an associative operation, i.e.

$$\vdash_{\mathrm{PA}} \forall s \forall s' \forall s''(\mathrm{seq}(s) \wedge \mathrm{seq}(s') \wedge \mathrm{seq}(s'') \to (s * s') * s'' = s * (s' * s'')).$$

Therefore, the brackets can be omitted.

*Proof of Proposition 3.12.* We will leave out all the formal details, since they would make the proof tedious and less transparent.

1. Obviously, $s' = \langle \mathrm{first}(s), j \rangle$ satisfies $\mathrm{length}(s') = j \wedge \forall i < j((s')_i = (s)_i)$ and thus by the Least Number Principle we can also assume $\mathrm{seq}(s')$. Uniqueness follows from Lemma 3.10.

2. Again, it is sufficient to show existence. We prove the statement by induction on $k'$. In the case that $k' = \mathbf{0}$, we obviously have that $s'$ is the empty sequence and we can thus choose $s''$ to be $s$. The induction step is a consequence of the induction hypothesis applied to $(s')_{<k'}$ which has length $k'$ and then by appending the last value $(s')_{k'}$ using Lemma 3.11.

⊣

**Lemma 3.15.** $\vdash_{\mathrm{PA}} \forall n \exists! s(\mathrm{seq}(s) \wedge \mathrm{length}(s) = \underline{1} \wedge (s)_{\mathbf{0}} = n)$.

*Proof.* Uniqueness follows directly from Lemma 3.10. For the existence one takes simply $s = \langle n, \underline{1} \rangle$ and applies then the Least Number Principle. ⊣

This allows the definition of sequences consisting of just one element as follows:

**Definition 3.16.** $[n] = s :\leftrightarrow \mathrm{seq}(s) \wedge \mathrm{length}(s) = \underline{1} \wedge (s)_{\mathbf{0}} = n$.

By interpreting powers $x^k$ as sequences of the form $(1, x, \ldots, x^k)$, the $\beta$-function enables the definition of powers in Peano Arithmetic.

**Definition 3.17.** We introduce the function

$$x^k = y :\leftrightarrow \exists s(\mathrm{nseq}(s) \wedge \mathrm{length}(s) = \mathbf{S}k \wedge (s)_0 = \underline{1} \wedge \forall i < \mathbf{S}k((s)_{\mathbf{S}i} = x \cdot (s)_i) \wedge (s)_k = y).$$

*Remark* 3.18. The definition of $x^k$ is well-defined due to Lemma 3.10. In particular, one has

$$\vdash_{\mathrm{PA}} x^{\mathbf{0}} = \underline{1}, \text{ and} \tag{2}$$

$$\vdash_{\mathrm{PA}} \forall x \forall k(x^{\mathbf{S}k} = x \cdot x^k). \tag{3}$$

This can be verified without much effort using induction on $k$.

It is possible to show in PA that every number has a unique prime decomposition; however, for our purpose it is enough to consider only primes up to $\underline{5}$, since gödelization is only concerned with the primes $\underline{2}, \underline{3}$ and $\underline{5}$. Note that the fact that these numbers are primes follows directly from the fact that $2, 3$ and $5$ are primes in $\mathbb{N}$ and that the relation prime is $\mathbb{N}$-conform.

**Lemma 3.19.** $\vdash_{\mathrm{PA}} \underline{2}^x \cdot \underline{3}^y \cdot \underline{5}^z = \underline{2}^{x'} \cdot \underline{3}^{y'} \cdot \underline{5}^{z'} \to x = x' \wedge y = y' \wedge z = z'$.

*Proof.* We show by induction on $x$ that

$$\vdash_{\mathrm{PA}} \underline{2}^x \cdot \underline{3}^y \cdot \underline{5}^z = \underline{2}^{x'} \cdot \underline{3}^{y'} \cdot \underline{5}^{z'} \to x = x' \tag{4}$$

holds. By showing the analogue of (4) for $y$ and $z$ and by applying (H.1) one can conclude the claim. Firstly, we verify

$$\vdash_{\mathrm{PA}} \forall y \forall z (\underline{2} \nmid \underline{3}^y \cdot \underline{5}^z). \tag{5}$$

Since $\underline{2}$ is prime and because of the tautologies (B.1) and (F.2) it is enough to show

$$\vdash_{\mathrm{PA}} \underline{2} \nmid \underline{3}^y \wedge \underline{2} \nmid \underline{5}^z. \tag{6}$$

In order to show $\vdash_{\mathrm{PA}} \underline{2} \nmid \underline{3}^y$ we use induction on $y$. The case $y = \mathbf{0}$ is clear and the case $y = \underline{1}$ as well because $\underline{2}$ is prime. The inductive step is a consequence of

$$\begin{aligned} \underline{2} \mid \underline{3}^{\mathbf{S}y} &\vdash_{\mathrm{PA}} \underline{2} \mid \underline{3} \cdot \underline{3}^y && (3)\\ &\vdash_{\mathrm{PA}} \underline{2} \mid \underline{3} \vee \underline{2} \mid \underline{3}^y && (2.26) \end{aligned}$$

since both cases contradict the induction hypothesis. Analogously, one verifies $\vdash_{\mathrm{PA}} \underline{2} \nmid \underline{5}^z$. Therefore we can conclude (6) using $(\wedge)$. Now we consider the induction basis:

$$\begin{aligned} \underline{2}^{\mathbf{0}} \cdot \underline{3}^y \cdot \underline{5}^z = \underline{2}^{x'} \cdot \underline{3}^{y'} \cdot \underline{5}^{z'}, x' = \mathbf{S}u &\vdash_{\mathrm{PA}} \underline{3}^y \cdot \underline{5}^z = \underline{2} \cdot \underline{2}^u \cdot \underline{3}^{y'} \cdot \underline{5}^{z'} && (3)\\ &\vdash_{\mathrm{PA}} \underline{2} \mid \underline{3}^y \cdot \underline{5}^z && (2.22) \end{aligned}$$

which contradicts (5). Therefore using $(\vee 4)$ applied to Lemma 2.6 we obtain the base case. For the inductive step we set $\varphi = \forall x' (\underline{2}^x \cdot \underline{3}^y \cdot \underline{5}^z = \underline{2}^{x'} \cdot \underline{3}^{y'} \cdot \underline{5}^{z'} \to x = x')$ and note

$$\begin{aligned} \varphi, \underline{2}^{\mathbf{S}x} \cdot \underline{3}^y \cdot \underline{5}^z = \underline{2}^{x'} \cdot \underline{3}^{y'} \cdot \underline{5}^{z'}, x' = \mathbf{S}u &\vdash_{\mathrm{PA}} \underline{2} \cdot \underline{2}^x \cdot \underline{3}^y \cdot \underline{5}^z = \underline{2} \cdot \underline{2}^u \cdot \underline{3}^{y'} \cdot \underline{5}^{z'} && (3)\\ &\vdash_{\mathrm{PA}} \underline{2}^x \cdot \underline{3}^y \cdot \underline{5}^z = \underline{2}^u \cdot \underline{3}^{y'} \cdot \underline{5}^{z'} && (2.10)\\ &\vdash_{\mathrm{PA}} x = u && (\mathrm{IH})\\ &\vdash_{\mathrm{PA}} \mathbf{S}x = \mathbf{S}u = x'. \end{aligned}$$

The case $x' = \mathbf{0}$ is already handled in the base case. ⊣

*Remark* 3.20. Using metainduction, one can easily conclude from Remark 3.18 that

$$\vdash_{\mathrm{PA}} x^{\underline{n}} = \underbrace{x \cdot \ldots \cdot x}_{n} \tag{7}$$

for all natural numbers $n$. Using (7) one can show that the power function is $\mathbb{N}$-conform. For this, suppose $a, n \in \mathbb{N}$. Then we obtain

$$\vdash_{\mathrm{PA}} \underline{a}^{\underline{n}} \overset{(7)}{=} \underbrace{\underline{a} \cdot \ldots \underline{a}}_{n} \overset{(\mathrm{N2})}{=} \underline{a^n}.$$

All other functions and relations defined in this section are obviously $\mathbb{N}$-conform due to 3.5, 3.6 and 3.7.

## 3.3 Gödelization of Peano Arithmetic

In a first step, every logical and non-logical symbol $\zeta$ of Peano Arithmetic is assigned a natural number $\#\zeta$, called **Gödel number** of $\zeta$. A similar version of gödelization can be found in [GJ98].

| Symbol $\zeta$ | Gödel number $\#\zeta$ |
|---|---|
| $0$ | $2$ |
| $\mathbf{s}$ | $4$ |
| $+$ | $6$ |
| $\cdot$ | $8$ |
| $=$ | $10$ |
| $\neg$ | $12$ |
| $\wedge$ | $14$ |
| $\vee$ | $16$ |
| $\rightarrow$ | $18$ |
| $\exists$ | $20$ |
| $\forall$ | $22$ |
| $x_n$ | $2n+1$ |

Secondly, we can encode $\mathcal{L}_{\mathrm{PA}}$-terms and formulas as follows.

| Term $\tau$ | Gödel number $\#\tau$ |
|---|---|
| $0$ | $2$ |
| $x_n$ | $2n+1$ |
| $\mathbf{S}t$ | $2^{\#\mathbf{s}} \cdot 3^{\#t}$ |
| $t_1 + t_2$ | $2^{\#+} \cdot 3^{\#t_1} \cdot 5^{\#t_2}$ |
| $t_1 \cdot t_2$ | $2^{\#\cdot} \cdot 3^{\#t_1} \cdot 5^{\#t_2}$ |

| Formula $\varphi$ | Gödel number $\#\varphi$ |
|---|---|
| $\tau_1 = \tau_2$ | $2^{\#=} \cdot 3^{\#\tau_1} \cdot 5^{\#\tau_2}$ |
| $\neg\psi$ | $2^{\#\neg} \cdot 3^{\#\psi}$ |
| $\psi_1 \wedge \psi_2$ | $2^{\#\wedge} \cdot 3^{\#\psi_1} \cdot 5^{\#\psi_2}$ |
| $\psi_1 \vee \psi_2$ | $2^{\#\vee} \cdot 3^{\#\psi_1} \cdot 5^{\#\psi_2}$ |
| $\psi_1 \rightarrow \psi_2$ | $2^{\#\rightarrow} \cdot 3^{\#\psi_1} \cdot 5^{\#\psi_2}$ |
| $\exists x\psi$ | $2^{\#\exists} \cdot 3^{\#x} \cdot 5^{\#\psi}$ |
| $\forall x\psi$ | $2^{\#\forall} \cdot 3^{\#x} \cdot 5^{\#\psi}$ |

In order to encode symbols, terms and formulas within PA, we define

$$\ulcorner \zeta \urcorner := \underline{\#\zeta}$$

for an arbitrary symbol, term or formula $\zeta$. In particular, this definition implies

*Remark* 3.21. Let $t, t_1, t_2$ be terms and $\varphi, \varphi_1$ and $\varphi_2$ be formulas. Then we have

- $\vdash_{\mathrm{PA}} \ulcorner x_n \urcorner = \underline{2} \cdot \underline{n} + \underline{1}$,
- $\vdash_{\mathrm{PA}} \ulcorner \mathbf{S}t \urcorner = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{\ulcorner t \urcorner}$ and $\vdash_{\mathrm{PA}} \ulcorner t_1 * t_2 \urcorner = \underline{2}^{\ulcorner * \urcorner} \cdot \underline{3}^{\ulcorner t_1 \urcorner} \cdot \underline{5}^{\ulcorner t_2 \urcorner}$ for $* \in \{+, \cdot\}$,
- $\vdash_{\mathrm{PA}} \ulcorner t_1 = t_2 \urcorner = \underline{2}^{\ulcorner = \urcorner} \cdot \underline{3}^{\ulcorner t_1 \urcorner} \cdot \underline{5}^{\ulcorner t_2 \urcorner}$,
- $\vdash_{\mathrm{PA}} \ulcorner \neg\varphi \urcorner = \underline{2}^{\ulcorner \neg \urcorner} \cdot \underline{3}^{\ulcorner \varphi \urcorner}$, $\vdash_{\mathrm{PA}} \ulcorner \varphi_1 \square \varphi_2 \urcorner = \underline{2}^{\ulcorner \square \urcorner} \cdot \underline{3}^{\ulcorner \varphi_1 \urcorner} \cdot \underline{5}^{\ulcorner \varphi_2 \urcorner}$ for $\square \in \{\wedge, \vee, \to\}$ and $\vdash_{\mathrm{PA}} \ulcorner \Diamond x \varphi \urcorner = \underline{2}^{\ulcorner \Diamond \urcorner} \cdot \underline{3}^{\ulcorner x \urcorner} \cdot \underline{5}^{\ulcorner \varphi \urcorner}$ for $\Diamond \in \{\exists, \forall\}$.

All statements are immediate consequences of the $\mathbb{N}$-conformity of $+, \cdot$ and the power function using induction on the construction of terms respectively formulas.

The next step consists in the introduction of new relations that indicate whether some number is the code of a term, variable or formula.

**Definition 3.22.** We define

$$\begin{aligned}
\mathrm{var}(v) &:\leftrightarrow \exists n (v = \underline{2} \cdot n + \underline{1}),\\
\mathrm{c_term}(c, t) &:\leftrightarrow \mathrm{nseq}(c) \wedge (c)_{\mathrm{last}} = t \wedge \forall k < \mathrm{length}(c) \big[ \mathrm{var}((c)_k) \vee (c)_k = \ulcorner \mathbf{0} \urcorner \\
&\qquad \vee \exists i < k \exists j < k ((c)_k = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{(c)_i} \vee (c)_k = \underline{2}^{\ulcorner + \urcorner} \cdot \underline{3}^{(c)_i} \cdot \underline{5}^{(c)_j} \\
&\qquad \vee (c)_k = \underline{2}^{\ulcorner \cdot \urcorner} \cdot \underline{3}^{(c)_i} \cdot \underline{5}^{(c)_j}) \big],\\
\mathrm{term}(t) &:\leftrightarrow \exists c (\mathrm{c_term}(c, t)),\\
\mathrm{equation}(e) &:\leftrightarrow \exists t_1 \exists t_2 (\mathrm{term}(t_1) \wedge \mathrm{term}(t_2) \wedge e = \underline{2}^{\ulcorner = \urcorner} \cdot \underline{3}^{t_1} \cdot \underline{5}^{t_2}),\\
\mathrm{c_formula}(c, f) &:\leftrightarrow \mathrm{nseq}(c) \wedge (c)_{\mathrm{last}} = f \wedge \forall k < \mathrm{length}(c) (\mathrm{equation}((c)_k) \vee \exists i < k \exists j < k \\
&\qquad ((c)_k = \underline{2}^{\ulcorner \neg \urcorner} \cdot \underline{3}^{(c)_i} \vee (c)_k = \underline{2}^{\ulcorner \wedge \urcorner} \cdot \underline{3}^{(c)_i} \cdot \underline{5}^{(c)_j} \vee (c)_k = \underline{2}^{\ulcorner \vee \urcorner} \cdot \underline{3}^{(c)_i} \cdot \underline{5}^{(c)_j} \vee \\
&\qquad (c)_k = \underline{2}^{\ulcorner \to \urcorner} \cdot \underline{3}^{(c)_i} \cdot \underline{5}^{(c)_j} \vee \exists v (\mathrm{var}(v) \wedge ((c)_k = \underline{2}^{\ulcorner \exists \urcorner} \cdot \underline{3}^{v} \cdot \underline{5}^{(c)_i} \vee (c)_k \\
&\qquad = \underline{2}^{\ulcorner \forall \urcorner} \cdot \underline{3}^{v} \cdot \underline{5}^{(c)_i})) \big],\\
\mathrm{formula}(f) &:\leftrightarrow \exists c (\mathrm{c_formula}(c, f)).
\end{aligned}$$

The motivation for the above definition is given by

**Lemma 3.23.** *Let $x$ be a variable, $t$ a term and $\varphi$ a formula in the language $\mathcal{L}_{\mathrm{PA}}$. Then the following statements hold:*

1. $\vdash_{\mathrm{PA}} \mathrm{var}(\ulcorner x \urcorner)$,
2. $\vdash_{\mathrm{PA}} \mathrm{term}(\ulcorner t \urcorner)$,
3. $\vdash_{\mathrm{PA}} \mathrm{formula}(\ulcorner \varphi \urcorner)$.

*Proof.* For the first statement suppose that $x$ is $x_n$. Then $\vdash_{\mathrm{PA}} \ulcorner x \urcorner = \underline{2n+1} = \underline{2} \cdot \underline{n} + \underline{1}$ and hence by $(\exists)$ we obtain $\vdash_{\mathrm{PA}} \mathrm{var}(\ulcorner x \urcorner)$. The second claim can be proved using induction on the construction of the term $t$. The cases that $t$ is a variable or $\mathbf{0}$ are clear. Let therefore $t = \mathbf{S}t'$ for some term $t'$ which satisfies $\vdash_{\mathrm{PA}} \mathrm{term}(t')$. This implies

$$\mathrm{c\_term}(c', \ulcorner t' \urcorner) \vdash_{\mathrm{PA}} \mathrm{c\_term}(c' * [\underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{\ulcorner t' \urcorner}], \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{\ulcorner t' \urcorner})$$

which leads to $\vdash_{\mathrm{PA}} \mathrm{term}(\ulcorner t \urcorner)$ because $\vdash_{\mathrm{PA}} \ulcorner t \urcorner = \ulcorner \mathbf{S}t' \urcorner = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{\ulcorner t' \urcorner}$ by Remark 3.21. The cases $t = t_1 + t_2$ and $t = t_1 \cdot t_2$ have analogous proofs. The third statement can be shown in a similar way by induction on the construction of $\varphi$. ⊣

Conversely, we have

**Lemma 3.24.** *Let $n \in \mathbb{N}$ be a natural number. Then we have*

1. *There exists a variable $x$ such that $\vdash_{\mathrm{PA}} \mathrm{var}(\underline{n}) \to \underline{n} = \ulcorner x \urcorner$,*
2. *There is a term $t$ with $\vdash_{\mathrm{PA}} \mathrm{term}(\underline{n}) \to \underline{n} = \ulcorner t \urcorner$,*
3. *There exists a formula $\varphi$ satisfying $\vdash_{\mathrm{PA}} \mathrm{formula}(\underline{n}) \to \underline{n} = \ulcorner \varphi \urcorner$.*

*Proof.* Since 2. and 3. can be shown using similar arguments, we omit the proof of the third statement.

1. Let $n \in \mathbb{N}$. We have

$$\underline{n} = \underline{2}x + \underline{1} \vdash_{\mathrm{PA}} x \leq \underline{n}$$
$$\vdash_{\mathrm{PA}} \bigvee_{k=0}^{n} x = \underline{k} \tag{N5}$$

   and thus the claim follows from $\underline{n} = \underline{2}x + \underline{1}, x = \underline{k} \vdash_{\mathrm{PA}} \underline{n} = \underline{2k+1} = \ulcorner x_k \urcorner$ using (N2) and $(\vee 1)$.

2. We show the second statement by induction on $n \in \mathbb{N}$. For $n = 0$ we obviously have $\vdash_{\mathrm{PA}} \neg\mathrm{term}(\mathbf{0})$ and thus by $(\mathrm{L}_{10})$ $\vdash_{\mathrm{PA}} \mathrm{term}(\mathbf{0}) \to \mathbf{0} = \ulcorner t \urcorner$ for any $\mathcal{L}_{\mathrm{PA}}$-term $t$. For the induction step, suppose that $n > 0$ and that the claim holds for all $m < n$. We have to consider each case which appears in the definition of c_term separately. The

case var($\underline{n}$) is dealt with in 1. and the case $\underline{n} = \ulcorner \mathbf{0} \urcorner$ is trival. The case that the term encoded by $\underline{n}$ is a the successor of another term follows from

$$\begin{aligned} \text{c\_term}(c, \underline{n}), i < \text{length}(c), \underline{n} = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{(c)_i} &\vdash_{\text{PA}} (c)_i < \underline{n} \\ &\vdash_{\text{PA}} \bigvee_{k=0}^{n-1} (c)_i = \underline{k} \end{aligned} \tag{N5}$$

and from

$$\begin{aligned} \text{c\_term}(c, \underline{n}), i < \text{length}(c), \underline{n} = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{(c)_i}, (c)_i = \underline{k} &\vdash_{\text{PA}} \text{term}(\underline{k}) \\ &\vdash_{\text{PA}} \text{term}(\underline{k}) \to \underline{k} = \ulcorner t \urcorner && \text{(IH)} \\ &\vdash_{\text{PA}} \underline{k} = \ulcorner t \urcorner && \text{(MP)} \\ &\vdash_{\text{PA}} \underline{n} = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{\ulcorner t \urcorner} = \ulcorner \mathbf{S} t \urcorner && (3.21) \end{aligned}$$

using ($\exists$) and ($\vee 1$). The other two cases follow in the same manner.

$\dashv$

**Definition 3.25.** In order to encode also the logical axioms and the axioms of PA, it is necessary to gödelize first the substitution of terms.

$$\text{var\_in\_term}(v, t) :\leftrightarrow \text{var}(v) \wedge \exists c[\text{c\_term}(c, t) \wedge \exists i < \text{length}(c)((c)_i = v)],$$

$$\begin{aligned} \text{var\_in\_formula}(v, f) :\leftrightarrow \exists c(\text{c\_formula}(c, f) \wedge \exists i < \text{length}(c) \exists t_1 \exists t_2 [(c)_i = \underline{2}^{\ulcorner = \urcorner} \cdot \underline{3}^{t_1} \cdot \underline{5}^{t_2} \\ \wedge (\text{var\_in\_term}(v, t_1) \vee \text{var\_in\_term}(v, t_2))], \end{aligned}$$

$$\begin{aligned} \text{bound\_in\_formula}(v, f) :\leftrightarrow \exists c[\text{c\_formula}(c, f) \wedge \exists f' \exists i < \text{length}(c)(\text{var\_in\_formula}(v, f') \\ \wedge ((c)_i = \underline{2}^{\ulcorner \exists \urcorner} \cdot \underline{3}^{v} \cdot \underline{5}^{f'} \vee (c)_i = \underline{2}^{\ulcorner \forall \urcorner} \cdot \underline{3}^{v} \cdot \underline{5}^{f'}))]. \end{aligned}$$

To simplify substitution, we allow the substitution $\varphi(x/t)$ only for formulas $\varphi$ where $x$ and all the variables of $t$ appear only free in $\varphi$. We can thus define

$$\begin{aligned} \text{sub\_allowed}(v, t, f) :\leftrightarrow \text{var\_in\_formula}(v, f) \wedge \neg \text{bound\_in\_formula}(v, f) \\ \wedge \forall v' (\text{var\_in\_term}(v', t) \to \neg \text{bound\_in\_formula}(v', f)), \end{aligned}$$

$$\begin{aligned} \text{c\_sub\_in\_term}(c, c', c'', v, t_0, t, t') :\leftrightarrow \text{var}(v) \wedge \text{c\_term}(c, t) \wedge \text{c\_term}(c'', t_0) \wedge \text{c\_term}(c', t') \wedge \\ \text{length}(c') = \text{length}(c) + \text{length}(c'') \wedge \forall k < \text{length}(c'') \\ ((c')_k = (c'')_k) \wedge \forall k < \text{length}(c)((c)_k = v \to \\ (c')_{\text{length}(c'')+k} = t_0 \wedge (\text{var}((c)_k) \wedge (c)_k \neq v \to (c')_k = \\ (c)_k) \wedge \forall i < k((c)_i = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{(c)_i} \to (c')_{\text{length}(c'')+k} = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \\ \cdot \underline{3}^{(c')_{\text{length}(c'')+i}}) \wedge \forall n \forall i < k \forall j < k((c)_i = \underline{2}^{n} \cdot \underline{3}^{(c)_i} \cdot \underline{5}^{(c)_j} \\ \to (c')_{\text{length}(c'')+k} = \underline{2}^{n} \cdot \underline{3}^{(c')_{\text{length}(c'')+i}} \cdot \underline{5}^{(c')_{\text{length}(c'')+j}})), \end{aligned}$$

$$\text{sub\_in\_term}(v, t_0, t, t') :\leftrightarrow \exists c \exists c' \exists c''(\text{c\_sub\_in\_term}(c, c', c'', v, t_0, t, t')),$$

$$\begin{aligned}\text{c\_sub\_in\_formula}(c,c',v,t_0,f,f') :\leftrightarrow &\text{sub\_allowed}(v,t_0,f)\wedge \text{c\_formula}(c,f)\wedge \text{c\_formula}(c',f')\\ &\wedge \text{length}(c')=\text{length}(c)\wedge\forall k<\text{length}(c)(\forall t\forall t'\forall s\forall s'\\ &((c)_k=\underline{2}^{\ulcorner=\urcorner}\cdot\underline{3}^t\cdot\underline{5}^{t'}\wedge\text{sub\_in\_term}(v,t_0,t,s)\wedge\\ &\text{sub\_in\_term}(v,t_0,t',s')\rightarrow(c')_k=\underline{2}^{\ulcorner=\urcorner}\cdot\underline{3}^s\cdot\underline{5}^{s'})\wedge\\ &\forall i<k((c)_k=\underline{2}^{\ulcorner\neg\urcorner}\cdot\underline{3}^{(c)_i}\rightarrow(c')_k=\underline{2}^{\ulcorner\neg\urcorner}\cdot\underline{3}^{(c')_i})\wedge\forall n\\ &\forall v'\forall i<k((c)_k=\underline{2}^n\cdot\underline{3}^{v'}\cdot\underline{5}^{(c)_i}\rightarrow(c')_k=\underline{2}^n\cdot\underline{3}^{v'}\cdot\underline{5}^{(c')_i})\\ &\wedge\forall n\forall i<k\forall j<k((c)_k=\underline{2}^n\cdot\underline{3}^{(c)_i}\cdot\underline{5}^{(c)_j}\rightarrow(c')_k=\\ &\underline{2}^n\cdot\underline{3}^{(c')_i}\cdot\underline{5}^{(c')_j})),\end{aligned}$$

$$\text{sub\_in\_formula}(v,t_0,f,f') :\leftrightarrow \exists c\exists c'(\text{c\_sub\_in\_formula}(c,c',v,t_0,f,f').$$

*Remark* 3.26. One can easily show that the substitution is unique, i.e it does not depend on the choice of the codes of $v, t_0$ and $t$ (respectively $f$):

1. $\vdash_{\text{PA}} \text{sub\_in\_term}(v,t_0,t,t')\wedge\text{sub\_in\_term}(v,t_0,t,t'')\rightarrow t'=t''$
2. $\vdash_{\text{PA}} \text{sub\_in\_formula}(v,t_0,f,f')\wedge\text{sub\_in\_formula}(v,t_0,f,f'')\rightarrow f'=f''$.

**Definition 3.27.** Now, we can also encode logical axioms and the axioms of Peano Arithmetic. For example, we define

$$\text{axiom\_L}_1(f) :\leftrightarrow \exists f'\exists f''(\text{formula}(f')\wedge\text{formula}(f'')\wedge f=\underline{2}^{\ulcorner\rightarrow\urcorner}\cdot\underline{3}^{f'}\cdot\underline{5}^{\underline{2}^{\ulcorner\rightarrow\urcorner}\cdot\underline{3}^{f''}\cdot\underline{5}^{f'}}),$$

$$\text{axiom\_L}_{12}(f) :\leftrightarrow \exists f'\exists f''\exists v\exists t(\text{sub\_in\_formula}(v,t,f',f'')\wedge f=\underline{2}^{\ulcorner\rightarrow\urcorner}\cdot\underline{3}^{\underline{2}^{\ulcorner\forall\urcorner}\cdot\underline{3}^{v}\cdot\underline{5}^{f'}}\cdot\underline{5}^{f''}),$$

$$\text{axiom\_L}_{16}(f) :\leftrightarrow \exists t(\text{term}(t)\wedge f=\underline{2}^{\ulcorner=\urcorner}\cdot\underline{3}^t\cdot\underline{5}^t),$$

$$\text{axiom\_PA}_1(f) :\leftrightarrow f=\ulcorner\forall x\neg(\mathbf{S}x=\mathbf{0})\urcorner,$$

$$\begin{aligned}\text{ind\_axiom}(f) :\leftrightarrow &\exists f'\exists f''\exists f'''\exists v\exists r(\text{sub\_in\_formula}(v,\ulcorner\mathbf{0}\urcorner,f',f'')\wedge\text{sub\_in\_formula}(v,\\ &\underline{2}^{\ulcorner\mathbf{S}\urcorner}\cdot\underline{3}^v,f',f''')\wedge\neg\text{bound\_in\_formula}(v,f')\wedge f=\ulcorner\underline{2}^{\ulcorner\rightarrow\urcorner}\cdot\underline{3}^{\underline{2}^{\ulcorner\wedge\urcorner}\cdot\underline{3}^{f''}\cdot\underline{5}^{r}}\\ &\cdot\underline{5}^{\underline{2}^{\ulcorner\forall\urcorner}\cdot\underline{3}^{v}\cdot\underline{5}^{f'}}\wedge r=\underline{2}^{\ulcorner\forall\urcorner}\cdot\underline{3}^v\cdot\underline{5}^{\underline{2}^{\ulcorner\rightarrow\urcorner}\cdot\underline{3}^{f'}\underline{5}^{f'''}}).\end{aligned}$$

Similarly, one can gödelize all logical axioms as $\text{axiom\_L}_1(f),\ldots,\text{axiom\_L}_{18}(f)$ and the Peano axioms as $\text{axiomPA}_1(f),\ldots,\text{axiomPA}_6(f)$. Furthermore, we define

$$\begin{aligned}\text{logical\_axiom}(f) &:\leftrightarrow \text{axiom\_L}_1(f)\vee\cdots\vee\text{axiom\_L}_{18}(f),\\ \text{peano\_axiom}(f) &:\leftrightarrow \text{axiom\_PA}_1(f)\vee\cdots\vee\text{axiom\_PA}_6(f)\vee\text{ind\_axiom}(f),\\ \text{axiom}(f) &:\leftrightarrow \text{logical\_axiom}(f)\vee\text{peano\_axiom}(f).\end{aligned}$$

The next step consists of the encoding of derivation rules and formal proofs.

**Definition 3.28.** We introduce the relations

$$\mathrm{MP}(f', f'', f) :\leftrightarrow \mathrm{formula}(f') \wedge \mathrm{formula}(f) \wedge f'' = \underline{2}^{\ulcorner\to\urcorner} \cdot \underline{3}^{f'} \cdot \underline{5}^{f},$$

$$\mathrm{GR}(v, f', f) :\leftrightarrow \mathrm{var}(v) \wedge \mathrm{formula}(f') \wedge f = \underline{2}^{\ulcorner\forall\urcorner} \cdot \underline{3}^{v} \cdot \underline{5}^{f'},$$

$$\begin{aligned}\mathrm{proof}(c, f) :\leftrightarrow \mathrm{nseq}(c) \wedge (c)_{\mathrm{last}} = f \wedge \forall k < \mathrm{length}(c)\big[&\mathrm{axiom}((c)_k) \vee \exists i < k \exists j < k \\ &(\mathrm{MP}((c)_i, (c)_j, (c)_k)) \vee \exists i < k \exists v(\mathrm{var}(v) \wedge \mathrm{GR}((c)_i, v, (c)_k))\big],\end{aligned}$$

$$\mathrm{provable}(f) :\leftrightarrow \exists c(\mathrm{proof}(c, f)).$$

**Lemma 3.29.** *Let $t$ and $t_0$ be two terms, $\varphi$ a formula and $x$ a variable such that the substitution $\varphi(x/t_0)$ is admissible. Then one has*

1. $\vdash_{\mathrm{PA}} \mathrm{sub\_in\_term}(\ulcorner x\urcorner, \ulcorner t_0\urcorner, \ulcorner t\urcorner, s) \leftrightarrow s = \ulcorner t(x/t_0)\urcorner$,
2. $\vdash_{\mathrm{PA}} \mathrm{sub\_in\_formula}(\ulcorner x\urcorner, \ulcorner t_0\urcorner, \ulcorner \varphi\urcorner, f) \leftrightarrow f = \ulcorner \varphi(x/t_0)\urcorner$.

*Proof.* We only show the first statement. By Remark 3.26 it is enough to show $\vdash_{\mathrm{PA}}$ $\mathrm{sub\_in\_term}(\ulcorner x\urcorner, \ulcorner t_0\urcorner, \ulcorner t\urcorner, \ulcorner t(x/t_0)\urcorner)$. For this, we use induction on the construction of the term $t$. Firstly, we assume that $t$ is a variable. We have two cases; either $t$ is $x$ or $t$ is some other variable $y \neq x$. We consider the first case. We obviously have that $[\ulcorner x\urcorner]$ is already the code of the therm $\ulcorner t\urcorner = \ulcorner x\urcorner$. Thus we have

$$\begin{aligned}\mathrm{c\_term}(c, t_0) &\vdash_{\mathrm{PA}} \mathrm{c\_term}([\ulcorner x\urcorner], \ulcorner x\urcorner) \\ &\vdash_{\mathrm{PA}} \mathrm{c\_term}(c * [\ulcorner t_0\urcorner], \ulcorner t_0\urcorner) \\ &\vdash_{\mathrm{PA}} \mathrm{sub\_in\_term}(\ulcorner x\urcorner, \ulcorner t_0\urcorner, \ulcorner x\urcorner, \ulcorner t_0\urcorner)\end{aligned}$$

by definiton of the predicate sub_in_term. Since $x(x/t_0)$ is obviously the term $t_0$, the claim holds. The case that $t$ is a variable $y \neq x$ can be handled in a similar way using $y(x/t_0) = y$.

Now we assume that $t$ is the term $\mathbf{S}t'$ for some term $t'$ which already satisfies the claim. Then the assumption gives

$$\vdash_{\mathrm{PA}} \mathrm{sub\_in\_term}(\ulcorner x\urcorner, \ulcorner t_0\urcorner, \ulcorner t'\urcorner, \ulcorner t'(x/t_0)\urcorner). \tag{8}$$

Hence for $\alpha = \mathrm{c\_sub\_in\_term}(c', c'', c, \ulcorner x\urcorner, \ulcorner t_0\urcorner, \ulcorner t'\urcorner, \ulcorner t'(x/t_0)\urcorner)$ we have

$$\begin{aligned}\alpha &\vdash_{\mathrm{PA}} \mathrm{c\_term}(c' * [\underline{2}^{\ulcorner\mathbf{S}\urcorner} \cdot \underline{3}^{\ulcorner t'\urcorner}], \ulcorner \mathbf{S}t'\urcorner) \\ &\vdash_{\mathrm{PA}} (c'')_{\mathrm{last}} = \ulcorner t'(x/t_0)\urcorner \\ &\vdash_{\mathrm{PA}} \mathrm{c\_sub\_in\_term}(c' * [\underline{2}^{\ulcorner\mathbf{S}\urcorner} \cdot \underline{3}^{\ulcorner t'\urcorner}], c'' * [\underline{2}^{\ulcorner\mathbf{S}\urcorner} \cdot \underline{3}^{(c'')_{\mathrm{last}}}], c, \ulcorner x\urcorner, \ulcorner t_0\urcorner, \ulcorner \mathbf{S}t'\urcorner, \ulcorner t(x/t_0)\urcorner)\end{aligned}$$

since $t(x/t_0) = \mathbf{S}(t'(x/t_0))$ and thus $\vdash_{\mathrm{PA}} \ulcorner t(x/t_0)\urcorner = \ulcorner \mathbf{S}(t'(x/t_0))\urcorner = \underline{2}^{\ulcorner\mathbf{S}\urcorner} \cdot \underline{3}^{\ulcorner t'(x/t_0)\urcorner}$. The claim is a consequence of (8) using $(\exists)$. The cases that $t$ is obtained from two other terms by addition respectively multiplication can be dealt with in a similar way.

For the second statement, note that one has to prove first that if the substitution $\varphi(x/t_0)$ is admissible, then $\vdash_{\mathrm{PA}}$ $\mathrm{sub\_allowed}(\ulcorner x\urcorner, \ulcorner t_0\urcorner, \ulcorner \varphi\urcorner)$. Consequently, the proof of 2. can be handled according to the proof of the first assertion.

$\dashv$

# Chapter 4

# The Incompleteness Theorems

Finally, we will be able to prove both the First and the Second Incompleteness Theorems. The proofs shown here differ from proofs shown in most books such as [Boo95] or [Rau08] which use recursion theoretic results, in particular for the verification of the Derivability Conditions which will be discussed in the third section as a prerquisite for the Second Incompleteness Theorem.

## 4.1 The Diagonalization Lemma

**Definition 4.1.** We can define a binary predicate which states that $m$ encodes the $n$-th successor of $\mathbf{0}$ as follows:

$$\begin{aligned}\mathrm{c\_succ}(c,n,m) :\leftrightarrow &\mathrm{nseq}(c) \wedge \mathrm{length}(c) = \mathbf{S}n \wedge (c)_{\mathbf{0}} = \ulcorner \mathbf{0} \urcorner \wedge \forall i < n((c)_{\mathbf{S}i} = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{(c)_i}) \wedge \\ &(c)_{\mathrm{last}} = m,\end{aligned}$$

$$\mathrm{succ}(n,m) :\leftrightarrow \exists c(\mathrm{c\_succ}(c,n,m)).$$

**Lemma 4.2.** *For any natural number $n \in \mathbb{N}$ we have $\vdash_{\mathrm{PA}} \mathrm{succ}(\underline{n}, \ulcorner \underline{n} \urcorner)$. In particular, for any $\mathcal{L}_{\mathrm{PA}}$-formula $\varphi$, this means $\vdash_{\mathrm{PA}} \mathrm{succ}(\ulcorner \varphi \urcorner, \ulcorner \ulcorner \varphi \urcorner \urcorner)$.*

*Proof.* We show the assertion using metainduction on $n$. For $n = 0$ the term $\underline{0}$ is the same as $\mathbf{0}$ and we have $\vdash_{\mathrm{PA}} \mathrm{nseq}([\ulcorner \mathbf{0} \urcorner]) \wedge \mathrm{length}([\ulcorner \mathbf{0} \urcorner]) = \mathbf{S0} \wedge ([\ulcorner \mathbf{0} \urcorner])_{\mathbf{0}} = \ulcorner \mathbf{0} \urcorner$. This proves $\vdash_{\mathrm{PA}} \mathrm{succ}(\underline{0}, \ulcorner \underline{0} \urcorner)$.

We assume that for some $n \in \mathbb{N}$ the claim holds. Then we can conclude

$$\begin{aligned}\mathrm{c\_succ}(c, \underline{n}, \ulcorner \underline{n} \urcorner), c' = c * [\ulcorner \underline{n+1} \urcorner] &\vdash_{\mathrm{PA}} \mathrm{length}(c') = \mathrm{length}(c) + \underline{1} = \mathbf{S}\underline{n} + \underline{1} = \mathbf{S}(\underline{n+1}) \\ &\vdash_{\mathrm{PA}} (c')_{\mathrm{last}} = \ulcorner \underline{n+1} \urcorner = \ulcorner \mathbf{S}\underline{n} \urcorner = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{\ulcorner \underline{n} \urcorner} \\ &\vdash_{\mathrm{PA}} \mathrm{c\_succ}(c', \underline{n+1}, \ulcorner \underline{n+1} \urcorner).\end{aligned}$$

⊣

**Definition 4.3.** We define the unary function

$$\mathrm{goen}(n) = m :\leftrightarrow \exists c(\mathrm{succ}(n,c) \wedge c = m) \vee \neg \exists c(\mathrm{succ}(n,c) \wedge c = \mathbf{0}).$$

The definition is legitimate, since one can easily prove using Lemma 3.10 that $\vdash_{\mathrm{PA}} \mathrm{succ}(n,m) \wedge \mathrm{succ}(n,m') \to m = m'$. In particular, the previous lemma states that for any $\mathcal{L}_{\mathrm{PA}}$-formula $\varphi$ we have

$$\vdash_{\mathrm{PA}} \mathrm{goen}(\ulcorner\varphi\urcorner) = \ulcorner\ulcorner\varphi\urcorner\urcorner. \tag{1}$$

Now we can show the so-called Diagonalization Lemma which will be an important tool for the proof of the incompleteness theorems.

**Theorem 4.4** (Diagonalization Lemma)**.** *Let $\varphi(x_0)$ be an $\mathcal{L}_{\mathrm{PA}}$-formula with one free variable. Then there exists a closed $\mathcal{L}_{\mathrm{PA}}$-formula $\sigma$ such that $\sigma \equiv_{\mathrm{PA}} \varphi(x_0/\ulcorner\sigma\urcorner)$.*

*Proof.* We define $\psi(x) = \forall y(\mathrm{sub\_in\_formula}(\ulcorner x\urcorner, \mathrm{goen}(x), x, y) \to \varphi(x_0/y))$ and $\sigma = \psi(x/\ulcorner\psi\urcorner)$. This implies

$$\begin{aligned}
\sigma &\equiv_{\mathrm{PA}} \forall y(\mathrm{sub_in_formula}(\ulcorner x\urcorner, \mathrm{goen}(\ulcorner\psi\urcorner), \ulcorner\psi\urcorner, y) \to \varphi(x_0/y)) \\
&\equiv_{\mathrm{PA}} \forall y(\mathrm{sub_in_formula}(\ulcorner x\urcorner, \ulcorner\ulcorner\psi\urcorner\urcorner, \ulcorner\psi\urcorner, y) \to \varphi(x_0/y)) && (1) \\
&\equiv_{\mathrm{PA}} \forall y(y = \ulcorner\psi(x/\ulcorner\psi\urcorner)\urcorner \to \varphi(x_0/y)) && (3.29) \\
&\equiv_{\mathrm{PA}} \varphi(x_0/\ulcorner\psi(x/\ulcorner\psi\urcorner)\urcorner) \\
&\equiv_{\mathrm{PA}} \varphi(x_0/\ulcorner\sigma\urcorner).
\end{aligned}$$

⊣

## 4.2 The First Incompleteness Theorem

In order to show Peano Arithmetic to be incomplete, we introduce a relation which for inputs of the form $\ulcorner\varphi\urcorner$, where $\varphi$ is an $\mathcal{L}_{\mathrm{PA}}$-formula, states that if $\varphi$ is provable, then there exists a shorter proof of its negation. This idea is called "Rosser's Trick" and was first used by B. Rosser in [Ros36].

**Definition 4.5.** We define

$$\begin{aligned}
\mathrm{proof}^R(x,y) &:\leftrightarrow \mathrm{proof}(x,y) \wedge \neg\exists z \leq x(\mathrm{proof}(z, \underline{2}^{\ulcorner\neg\urcorner} \cdot \underline{3}^y)) \text{ and} \\
\Box^R\varphi &:\leftrightarrow \exists x(\mathrm{proof}^R(x, y/\ulcorner\varphi\urcorner))
\end{aligned}$$

for an arbitrary $\mathcal{L}_{\mathrm{PA}}$-formula $\varphi$.

**Proposition 4.6.** *Let $\varphi$ be any closed $\mathcal{L}_{\mathrm{PA}}$-formula. Then one has*

1. *If $\vdash_{\mathrm{PA}} \varphi$, then there exists $n \in \mathbb{N}$ such that $\vdash_{\mathrm{PA}} \mathrm{proof}(\underline{n}, \ulcorner\varphi\urcorner)$.*
2. *If $\nvdash_{\mathrm{PA}} \varphi$, then $\vdash_{\mathrm{PA}} \neg\mathrm{proof}(\underline{n}, \ulcorner\varphi\urcorner)$ for all $n \in \mathbb{N}$.*

*Proof.*

1. Suppose that $\vdash_{\mathrm{PA}} \varphi$ holds. Then there exists $n \in \mathbb{N}$ such that there is a sequence of formulas $\varphi_0, \ldots, \varphi_n$ which is a formal proof of $\varphi$ and there is no shorter proof of $\varphi$. We will prove by induction on $n$ that there exists some $k$ such that $\mathrm{proof}(\underline{k}, \ulcorner\varphi\urcorner)$. If $n = 0$, then $\varphi$ is an axiom. As in Lemma 3.23 one can easily show that if $\varphi$ is an axiom, then $\vdash_{\mathrm{PA}} \mathrm{axiom}(\ulcorner\varphi\urcorner)$. Thus we have $\vdash_{\mathrm{PA}} \mathrm{proof}([\ulcorner\varphi\urcorner], \ulcorner\varphi\urcorner)$ and since the function $[.]$ is $\mathbb{N}$-conform, the induction basis holds.

   We assume that the assertion holds for all formulas having a proof of length $< n$, where $n > 0$. Since $n$ is the minimal length of a proof of $\varphi$, $\varphi$ is not an axiom.

   - Suppose that there are $i, j < n$ such that $\varphi_j$ is $\varphi_i \to \varphi$. We obviously have that $\vdash_{\mathrm{PA}} \varphi_i$ and $\vdash_{\mathrm{PA}} \varphi_i \to \varphi_j$. Hence there exist $k, l \in \mathbb{N}$ satisfying $\vdash_{\mathrm{PA}} \mathrm{proof}(\underline{k}, \ulcorner\varphi_i\urcorner)$ and $\vdash_{\mathrm{PA}} \mathrm{proof}(\underline{l}, \ulcorner\varphi_i \to \varphi\urcorner)$. Moreover, it holds that $\vdash_{\mathrm{PA}} \mathrm{MP}(\ulcorner\varphi_i\urcorner, \ulcorner\varphi_i \to \varphi\urcorner, \ulcorner\varphi\urcorner)$. Consequently, we get

     $$\vdash_{\mathrm{PA}} \mathrm{proof}(\underline{k} * \underline{l} * [\ulcorner\varphi\urcorner], \ulcorner\varphi\urcorner)$$

     which implies the assertion due to $\mathbb{N}$-conformity of all occurring functions (i.e. of $*, [.], \cdot$ and powers).
   - Let $i < n$ such that $\varphi$ is $\forall x \varphi_i$ for some variable $x$. Thus $\vdash_{\mathrm{PA}} \varphi_i$ and by induction hypothesis there exists $k \in \mathbb{N}$ such that $\vdash_{\mathrm{PA}} \mathrm{proof}(\underline{k}, \ulcorner\varphi_i\urcorner)$. By Lemma 3.23 we get $\vdash_{\mathrm{PA}} \mathrm{var}(\ulcorner x\urcorner)$ and thus

     $$\vdash_{\mathrm{PA}} \mathrm{proof}(\underline{k} * [\ulcorner\varphi\urcorner], \ulcorner x\urcorner, \ulcorner\varphi\urcorner)$$

     from which we can conclude the claim as in the previous case.

2. We show by metainduction on $n \in \mathbb{N}$ that if $\nvdash_{\mathrm{PA}} \varphi$ for an $\mathcal{L}_{\mathrm{PA}}$-formula $\varphi$, then $\vdash_{\mathrm{PA}} \neg\mathrm{proof}(\underline{n}, \ulcorner\varphi\urcorner)$. The case $n = 0$ is obvious, since $\mathbf{0}$ is the empty sequence. Suppose now that $n > 0$ and that the assumption holds for any natural number $< n$. Let $\varphi$ be an arbitrary $\mathcal{L}_{\mathrm{PA}}$-formula with $\nvdash_{\mathrm{PA}} \varphi$. We will show the statement by contradiction.

   Firstly, note that as in Lemma 3.24 one can show that for all $m \in \mathbb{N}$ there exists an axiom $\psi$ such that

   $$\vdash_{\mathrm{PA}} \mathrm{axiom}(\underline{m}) \to \underline{m} = \ulcorner\psi\urcorner.$$

   In particular, for $m = \#\varphi$ this means

   $$\vdash_{\mathrm{PA}} \mathrm{axiom}(\ulcorner\varphi\urcorner) \to \ulcorner\varphi\urcorner = \ulcorner\psi\urcorner \tag{2}$$

   for some axiom $\psi$. However, due to $\nvdash_{\mathrm{PA}} \varphi$, $\varphi$ cannot be an axiom and thus $\varphi$ and $\psi$ are distinct formulas. Hence $\#\varphi \neq \#\psi$ and (N3) yields thus $\vdash_{\mathrm{PA}} \ulcorner\varphi\urcorner \neq \ulcorner\psi\urcorner$. To sum up, by contradiction (2) implies $\vdash_{\mathrm{PA}} \neg\mathrm{axiom}(\ulcorner\varphi\urcorner)$.

Secondly, we assume that the code of $\varphi$ is obtained form the code of two other formulas using (MP).

$$\begin{aligned}
\text{proof}(\underline{n}, \ulcorner\varphi\urcorner), \text{MP}((\underline{n})_i, (\underline{n})_j, \ulcorner\varphi\urcorner) &\vdash_{\text{PA}} (\underline{n})_j = \underline{2}^{\ulcorner\to\urcorner} \cdot \underline{3}^{(\underline{n})_i} \cdot \underline{5}^{\ulcorner\varphi\urcorner} \\
&\vdash_{\text{PA}} (\underline{n})_i < \underline{n} \wedge (\underline{n})_j < \underline{n} \\
&\vdash_{\text{PA}} \Big(\bigvee_{k=0}^{n-1} (\underline{n})_i = \underline{k}\Big) \wedge \Big(\bigvee_{l=0}^{n-1} (\underline{n})_j = \underline{l}\Big). \qquad \text{(N5)}
\end{aligned} \tag{3}$$

Now suppose $k \in \{0, \ldots, n-1\}$. Due to Lemma 3.24 there is a formula $\psi$ satsifying

$$\vdash_{\text{PA}} \text{formula}(\underline{k}) \to \underline{k} = \ulcorner\psi\urcorner. \tag{4}$$

This leads to

$$\begin{aligned}
\text{proof}(\underline{n}, \ulcorner\varphi\urcorner), \text{MP}((\underline{n})_i, (\underline{n})_j, \ulcorner\varphi\urcorner), (\underline{n})_i = \underline{k} &\vdash_{\text{PA}} \text{formula}(\underline{k}) \\
&\vdash_{\text{PA}} \text{formula}(\underline{k}) \to \underline{k} = \ulcorner\psi\urcorner && (4) \\
&\vdash_{\text{PA}} (\underline{n})_i = \underline{k} = \ulcorner\psi\urcorner && (\text{MP}) \\
&\vdash_{\text{PA}} (\underline{n})_j = \ulcorner\psi \to \varphi\urcorner && (3.21) \\
&\vdash_{\text{PA}} \text{proof}((\underline{n})_{<i}, \ulcorner\psi\urcorner) && (5) \\
&\vdash_{\text{PA}} \text{proof}((\underline{n})_{<j}, \ulcorner\psi \to \varphi\urcorner). && (6)
\end{aligned}$$

As a result of $\nvdash_{\text{PA}} \varphi$ we obviously have either $\nvdash_{\text{PA}} \psi$ or $\nvdash_{\text{PA}} \psi \to \varphi$, since otherwise using (MP) also $\varphi$ would be provable. On the other hand, $\nvdash_{\text{PA}} \psi$ contradicts (5) and the second option contradicts (6) as a consequence of the $\mathbb{N}$-conformity of the truncation function $(s)_{<i}$ and the induction hypothesis. Due to the fact that $k$ was arbitrarily chosen and using (3) and ($\vee$1), the possibility $\text{proof}(\underline{n}, \ulcorner\varphi\urcorner), \text{MP}((\underline{n})_i, (\underline{n})_j, \ulcorner\varphi\urcorner)$ can be dismissed. Using similar arguments, one can show that the assumption $\text{proof}(\underline{n}, \ulcorner\varphi\urcorner), \text{GR}(v, (\underline{n})_i, \ulcorner\varphi\urcorner)$ leads to a contradiction as well. Therefore, due to ($\vee$1) and ($\lightning$) we can conclude $\vdash_{\text{PA}} \neg\text{proof}(\underline{n}, \ulcorner\varphi\urcorner)$.

⊣

*Remark* 4.7. Alternatively, one could show that all relations defined in Definitions 3.22, 3.25, 3.27 and 3.28 (except the relation provable) are $\mathbb{N}$-conform. Then the proof of Proposition 4.6 is trivial. Nonetheless, e.g. showing that the relations term and formula are equivalent to formulas using only bounded quantification is nontrivial. An upper bound of term can be found in [Boo95].

**Theorem 4.8.** *If* PA *is consistent, then it is incomplete.*

*Proof.* We apply the Diagonalization Lemma to the formula $\neg\exists x(\text{proof}^R(x, y))$ in order to obtain a closed $\mathcal{L}_{\text{PA}}$-formula $\sigma$ with

$$\sigma \equiv_{\text{PA}} \neg\Box^R\sigma \tag{7}$$

which leads to

$$\sigma \equiv_{\mathrm{PA}} \forall x[\mathrm{proof}(x, \ulcorner\sigma\urcorner) \to \exists z \leq x(\mathrm{proof}(z, \ulcorner\neg\sigma\urcorner))] \tag{8}$$

due to (A) and (K.1). We would like to show that $\nvdash_{\mathrm{PA}} \sigma$ and $\nvdash_{\mathrm{PA}} \neg\sigma$.

By contradiction, we assume that $\vdash_{\mathrm{PA}} \sigma$. Then by Proposition 4.6 there exists a natural number $n \in \mathbb{N}$ encoding a proof of $\sigma$, i.e. $\vdash_{\mathrm{PA}} \mathrm{proof}(\underline{n}, \ulcorner\sigma\urcorner)$. Moreover, (8) and (MP) yield $\vdash_{\mathrm{PA}} \exists z \leq \underline{n}(\mathrm{proof}(z, \ulcorner\neg\sigma\urcorner))$. Furthermore, as a consequence of (N5) we obtain

$$\vdash_{\mathrm{PA}} \bigvee_{k=0}^{n} \mathrm{proof}(\underline{k}, \ulcorner\neg\sigma\urcorner). \tag{9}$$

On the other hand, since PA is consistent, we have $\nvdash_{\mathrm{PA}} \neg\sigma$ and hence by 4.6 also $\vdash_{\mathrm{PA}} \neg\mathrm{proof}(\underline{k}, \ulcorner\neg\sigma\urcorner)$ for all $k \in \mathbb{N}$. Due to the fact that this contradicts (9), we get $\nvdash_{\mathrm{PA}} \sigma$.

Secondly, suppose that $\vdash_{\mathrm{PA}} \neg\sigma$ holds. Again, we can apply Proposition 4.6 to find some $n \in \mathbb{N}$ with

$$\vdash_{\mathrm{PA}} \mathrm{proof}(\underline{n}, \ulcorner\neg\sigma\urcorner). \tag{10}$$

Moreover, (7) and (A) imply

$$\vdash_{\mathrm{PA}} \exists x(\mathrm{proof}(x, \ulcorner\sigma\urcorner) \wedge \neg\exists z \leq x(\mathrm{proof}(z, \ulcorner\neg\sigma\urcorner))).$$

Hence we get

$$\mathrm{proof}(x, \ulcorner\sigma\urcorner) \wedge \neg\exists z \leq x(\mathrm{proof}(z, \ulcorner\neg\sigma\urcorner)) \vdash_{\mathrm{PA}} \underline{n} > x \tag{10}$$

$$\vdash_{\mathrm{PA}} \bigvee_{k=0}^{n-1} x = \underline{k} \tag{N5}$$

$$\vdash_{\mathrm{PA}} \bigvee_{k=0}^{n-1} \mathrm{proof}(\underline{k}, \ulcorner\sigma\urcorner). \tag{11}$$

However, $\nvdash_{\mathrm{PA}} \sigma$ implies that $\vdash_{\mathrm{PA}} \neg\mathrm{proof}(\underline{k}, \ulcorner\sigma\urcorner)$ for all $k \in \mathbb{N}$ which contradicts (11). To sum up, we can conclude $\nvdash_{\mathrm{PA}} \sigma$ as well as $\nvdash_{\mathrm{PA}} \neg\sigma$ which means that PA is incomplete. ⊣

**Corollary 4.9** (First Incompleteness Theorem)**.** *Any consistent theory given by finitely many axioms resp. axiom schemas containig* PA *is incomplete.*

*Proof.* Let $T$ be an extension of PA which is given by finitely many axioms resp. axiom schemas. Since for the language of $T$ we have $\mathcal{L}_T \supseteq \mathcal{L}_{\mathrm{PA}}$ we have that all previously introduced functions and relations can be defined in $T$ as well. Furthermore, all sentences which are provable in PA are also provable in $T$. We modify only the relation proof and include the gödelization of all finitely many axiom schemas of $T$ which do not form part of Peano Arithmetic. Then the incompleteness of $T$ is shown as in the proof of Theorem 4.8. ⊣

## 4.3 The Derivability Conditions

*Notation.* We abbreviate the definition given for the predicate that states that a $\mathcal{L}_{\mathrm{PA}}$-formula $\varphi$ is provable by

$$\Box\varphi :\leftrightarrow \mathrm{provable}(\ulcorner\varphi\urcorner).$$

In order to prove the second incompleteness theorem, we need to prove the following three so-called Derivability Conditions (stated by Hilbert, Bernays and Löb):

(D1) $\vdash_{\mathrm{PA}} \varphi \Rightarrow \vdash_{\mathrm{PA}} \Box\varphi$,

(D2) $\vdash_{\mathrm{PA}} \Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$,

(D3) $\vdash_{\mathrm{PA}} \Box\varphi \to \Box\Box\varphi$.

In most proofs of (D1)-(D3), recursion theory is used; here, however, we will show a proof that does not make use of any recursion theoretic results. Note that (D1) is an immediate result of Proposition 4.6. However, it is also possible to show (D1) as a consequence of (D2). We will thus include an alternative proof of the first Derivability Condition.

*Proof of* (D2). We show the equivalent statement $\Box\varphi, \Box(\varphi \to \psi) \vdash_{\mathrm{PA}} \Box\psi$. We have

$$\mathrm{proof}(c, \ulcorner\varphi\urcorner), \mathrm{proof}(c', \ulcorner\varphi \to \psi\urcorner), c'' = c * c' * [\ulcorner\varphi\urcorner] \vdash_{\mathrm{PA}} \mathrm{nseq}(c'') \wedge (c'')_{\mathrm{last}} = \ulcorner\psi\urcorner.$$

and we have to verify that $c''$ is indeed the code of a proof of $\psi$. We define thus $T = \{\mathrm{proof}(c, \ulcorner\varphi\urcorner), \mathrm{proof}(c', \ulcorner\varphi \to \psi\urcorner), c'' = c * c' * [\ulcorner\psi\urcorner], \mathrm{length}(c) = l, \mathrm{length}(c') = l', k < \mathrm{length}(c'')\}$ and we have to show

$$T, k < l + l' + \underline{1} \vdash_{\mathrm{PA}} \mathrm{axiom}((c'')_k) \vee \exists i < k \exists j < k (\mathrm{MP}((c'')_i, (c'')_j, (c'')_k)) \vee \exists i < k \exists v \\ (\mathrm{var}(v) \wedge \mathrm{GR}((c)_i, v, (c)_k)).$$

The cases $k < l$ and the cases $l \leq k < l'$ are obvious by construction of $c''$. For the last case, we note

$$\begin{aligned} T, k = l + l' &\vdash_{\mathrm{PA}} (c'')_k = (c'')_{\mathrm{last}} = \ulcorner\psi\urcorner \\ &\vdash_{\mathrm{PA}} (c'')_{l-\underline{1}} = (c)_{\mathrm{last}} = \ulcorner\varphi\urcorner \\ &\vdash_{\mathrm{PA}} (c'')_{l+l'-\underline{1}} = (c')_{\mathrm{last}} = \ulcorner\varphi \to \psi\urcorner = \underline{2}^{\ulcorner\to\urcorner} \cdot \underline{3}^{\ulcorner\varphi\urcorner} \cdot \underline{5}^{\ulcorner\psi\urcorner} \\ &\vdash_{\mathrm{PA}} \mathrm{MP}((c'')_{l-\underline{1}}, (c'')_{l+l'-\underline{1}}, (c'')_k). \end{aligned} \tag{3.21}$$

To sum up, we obtain

$$\mathrm{proof}(c, \ulcorner\varphi\urcorner), \mathrm{proof}(c', \ulcorner\varphi \to \psi\urcorner) \vdash_{\mathrm{PA}} \mathrm{proof}(c * c' * \ulcorner\psi\urcorner, \ulcorner\varphi\urcorner)$$

which implies using ($\mathrm{L}_{13}$) and ($\exists$) finally $\Box\varphi, \Box(\varphi \to \psi) \vdash_{\mathrm{PA}} \Box\psi$. ⊣

**Lemma 4.10.** *If $\varphi$ is an $\mathcal{L}_{\mathrm{PA}}$-formula and $x$ is a variable, then*

$$\vdash_{\mathrm{PA}} \Box\varphi \to \Box(\forall x\varphi).$$

*Proof.* By (DT), we can show the equivalent statement $\Box\varphi \vdash_{\mathrm{PA}} \Box(\forall x\varphi)$. We have

$$\mathrm{proof}(c, \ulcorner\varphi\urcorner), c' = c * [\ulcorner\forall x\varphi\urcorner] \vdash_{\mathrm{PA}} \mathrm{nseq}(c') \wedge (c')_{\mathrm{last}} = \ulcorner\forall x\varphi\urcorner.$$

As in the proof of (D2), one can verify that $c'$ encodes a proof of $\forall x\varphi$ indeed. ⊣

*Alternative Proof of* (D1). Let $\varphi$ be an $\mathcal{L}_{\mathrm{PA}}$-formula satisfying $\vdash_{\mathrm{PA}} \varphi$. Then there exists a finite sequence of $\mathcal{L}_{\mathrm{PA}}$-formulas $\varphi_0, \ldots, \varphi_n$ such that $\varphi_n$ is $\varphi$. We prove the statement by induction over the length $n$ of the proof of $\varphi$. For $n = 0$ the proof consists of only one formula, thus $\varphi$ is an axiom. This means that $\vdash_{\mathrm{PA}} \mathrm{axiom}(\ulcorner\varphi\urcorner)$ and hence $[\ulcorner\varphi\urcorner]$ is already the code of a proof of $\varphi$. Therefore, we can conclude $\vdash_{\mathrm{PA}} \Box\varphi$.
In order to prove the induction step, we assume that $n > 0$ and $\vdash_{\mathrm{PA}} \Box\varphi_i$ for all $i < n$. There are three possibilities:

1. $\varphi$ is a logical axiom or an axiom of Peano Arithmetic;
2. There exist $i < n$ and $j < n$ such that $\varphi$ is obtained from $\varphi_i$ and $\varphi_j$ using Modus Ponens, i.e. $\varphi_j$ is $\varphi_i \to \varphi$;
3. There exists $i < n$ such that $\varphi$ is obtained from $\varphi_i$ using the generalization rule, i.e. $\varphi$ is $\forall x\varphi_i$ for some variable $x$.

The first possibility corresponds to the base case. In the second case, we can apply (D2).

$\vdash_{\mathrm{PA}} \Box\varphi_i$ (IH)
$\vdash_{\mathrm{PA}} \Box(\varphi_i \to \varphi)$ (IH)
$\vdash_{\mathrm{PA}} \Box(\varphi_i \to \varphi) \to (\Box\varphi_i \to \Box\varphi)$ (D2)
$\vdash_{\mathrm{PA}} \Box\varphi_i \to \Box\varphi$ (MP)
$\vdash_{\mathrm{PA}} \Box\varphi$. (MP)

For the third case, we make use of Lemma 4.10.

$\vdash_{\mathrm{PA}} \Box\varphi_i$ (IH)
$\vdash_{\mathrm{PA}} \Box\varphi_i \to \Box\varphi$ (4.10)
$\vdash_{\mathrm{PA}} \Box\varphi$. (MP)

⊣

**Corollary 4.11.** *Let $\varphi$ and $\psi$ be arbitrary sentences in $\mathcal{L}_{\mathrm{PA}}$. If $\varphi \equiv_{\mathrm{PA}} \psi$, then $\Box\varphi \equiv_{\mathrm{PA}} \Box\psi$.*

*Proof.* Suppose that $\varphi \equiv_{\mathrm{PA}} \psi$. This implies

$\vdash_{\mathrm{PA}} \varphi \to \psi$ ($\leftrightarrow$)
$\vdash_{\mathrm{PA}} \Box(\varphi \to \psi)$ (D1)
$\vdash_{\mathrm{PA}} \Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$ (D2)
$\vdash_{\mathrm{PA}} \Box\varphi \to \Box\psi$. (MP)

In a similar manner, one shows $\vdash_{\mathrm{PA}} \Box\psi \to \Box\varphi$ concluding the claim. ⊣

**Corollary 4.12.** *Let $\varphi$ and $\psi$ be any two $\mathcal{L}_{\mathrm{PA}}$-formulas. Then*

$$\vdash_{\mathrm{PA}} \Box\varphi \wedge \Box\psi \leftrightarrow \Box(\varphi \wedge \psi).$$

*Proof.* The first direction follows from

$$\begin{aligned}
\Box\varphi \wedge \Box\psi &\vdash_{\mathrm{PA}} \Box\varphi && (\wedge)\\
&\vdash_{\mathrm{PA}} \Box\psi && (\wedge)\\
&\vdash_{\mathrm{PA}} \psi \to (\varphi \to (\varphi \to \psi)) && (\mathrm{L}_5)\\
&\vdash_{\mathrm{PA}} \Box(\psi \to (\varphi \to (\varphi \to \psi)) && (\mathrm{D1})\\
&\vdash_{\mathrm{PA}} \Box(\psi \to (\varphi \to (\varphi \to \psi)) \to (\Box\psi \to \Box(\varphi \to \varphi \wedge \psi)) && (\mathrm{D2})\\
&\vdash_{\mathrm{PA}} \Box\psi \to \Box(\varphi \to \varphi \wedge \psi) && (\mathrm{MP})\\
&\vdash_{\mathrm{PA}} \Box(\varphi \to \varphi \wedge \psi) && (\mathrm{MP})\\
&\vdash_{\mathrm{PA}} \Box(\varphi \to \varphi \wedge \psi) \to (\Box\varphi \to \Box(\varphi \wedge \psi)) && (\mathrm{D2})\\
&\vdash_{\mathrm{PA}} \Box\varphi \to \Box(\varphi \wedge \psi) && (\mathrm{MP})\\
&\vdash_{\mathrm{PA}} \Box(\varphi \wedge \psi) && (\mathrm{MP})
\end{aligned}$$

by applying the deduction theorem.

For the second direction, by symmetry and using $(\wedge)$, it is enough to show $\vdash_{\mathrm{PA}} \Box(\varphi \wedge \psi) \to \Box\varphi$. We note that $\ulcorner \varphi \wedge \psi \urcorner$ is $\underline{2}^{\ulcorner \wedge \urcorner} \cdot \underline{3}^{\ulcorner \varphi \urcorner} \cdot \underline{5}^{\ulcorner \psi \urcorner}$.

$$\begin{aligned}
\mathrm{proof}(c, \ulcorner \varphi \wedge \psi \urcorner) &\vdash_{\mathrm{PA}} \mathrm{L_3_axiom}(\underline{2}^{\ulcorner \to \urcorner} \cdot \underline{3}^{\ulcorner \varphi \wedge \psi \urcorner} \cdot \underline{5}^{\ulcorner \varphi \urcorner})\\
&\vdash_{\mathrm{PA}} \mathrm{MP}(\ulcorner \varphi \wedge \psi \urcorner, \underline{2}^{\ulcorner \to \urcorner} \cdot \underline{3}^{\ulcorner \varphi \wedge \psi \urcorner} \cdot \underline{5}^{\ulcorner \varphi \urcorner}, \ulcorner \varphi \urcorner)\\
&\vdash_{\mathrm{PA}} \mathrm{proof}(c * [\underline{2}^{\ulcorner \to \urcorner} \cdot \underline{3}^{\ulcorner \varphi \wedge \psi \urcorner} \cdot \underline{5}^{\ulcorner \varphi \urcorner}] * [\ulcorner \varphi \urcorner], \ulcorner \varphi \urcorner)\\
&\vdash_{\mathrm{PA}} \Box\varphi.
\end{aligned}$$

Hence $(\exists)$ and (DT) imply $\vdash_{\mathrm{PA}} \Box(\varphi \wedge \psi) \to \Box\varphi$. ⊣

**Lemma 4.13.** *The following statements hold:*

1. $\vdash_{\mathrm{PA}} \forall v(\mathrm{var}(v) \to \Box(\mathrm{var}(v))$,
2. $\vdash_{\mathrm{PA}} \forall t(\mathrm{term}(t) \to \Box\mathrm{term}(t))$,
3. $\vdash_{\mathrm{PA}} \forall f(\mathrm{formula}(f) \to \Box\mathrm{formula}(f))$.

*Proof.*

1. For the first statement we note

$$\begin{aligned}
&\vdash_{\mathrm{PA}} \mathrm{var}(2n+1)\\
&\vdash_{\mathrm{PA}} \Box(\mathrm{var}(2n+1)) && (\mathrm{D1})
\end{aligned}$$

which implies $v = 2n+1 \vdash_{\mathrm{PA}} \Box(\mathrm{var}(v))$. The claim is then a consequence of $(\exists)$.

2. The idea is to use induction on the length of the sequence that defines $t$ as a term. We set $\varphi(l) = \forall c \forall t(\text{c\_term}(c,t) \wedge \text{length}(c) = l \to \Box\text{term}(t))$ and by (DT) and ($\exists$) it is sufficient to prove $\vdash_{\text{PA}} \forall l \varphi(l)$ using strong induction.

   For $l = \mathbf{0}$ we obtain that $c$ is the empty sequence and hence the statement is trivial. The case $l = \underline{1}$ means that the sequence encoded by $c$ consists only of the single element $t$. Thus there are only the possibilities $t = \ulcorner \mathbf{0} \urcorner$ and $\text{var}(t)$. Therefore, it suffices to show $t = \ulcorner \mathbf{0} \urcorner \vdash_{\text{PA}} \Box\text{term}(t)$ and $\text{var}(t) \vdash_{\text{PA}} \Box\text{term}(t)$. Both cases are obvious, since $\vdash_{\text{PA}} \text{term}(\ulcorner \mathbf{0} \urcorner)$ and $\vdash_{\text{PA}} \text{term}(2n+1)$ and thus by (D1) also $\vdash_{\text{PA}} \Box\text{term}(\ulcorner \mathbf{0} \urcorner)$ repectively $\vdash_{\text{PA}} \Box\text{term}(2n+1)$.

   We show the induction step. By definition of the predicate c_term we have

$$\begin{aligned}\forall l' < l \varphi(l'), \text{c\_term}(c,t) \wedge \text{length}(c) = l \vdash_{\text{PA}} (c)_{\text{last}} = t \wedge \forall k < l \big[ \text{var}((c)_k) \vee (c)_k = \\ \ulcorner \mathbf{0} \urcorner \vee \exists i < k \exists j < k ((c)_k = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{(c)_i} \vee \\ (c)_k = \underline{2}^{\ulcorner + \urcorner} \cdot \underline{3}^{(c)_i} \cdot \underline{5}^{(c)_j} \vee (c)_k = \underline{2}^{\ulcorner \cdot \urcorner} \\ \cdot \underline{3}^{(c)_i} \cdot \underline{5}^{(c)_j}) \big].\end{aligned}$$

   Thus we can distinguish between five cases for $t = (c)_{l-\underline{1}}$; the cases $\text{var}(t)$ and $t = \ulcorner \mathbf{0} \urcorner$ are clear by the base case. For the sake of simplicity, we will only consider the case $\exists i < l - \underline{1}(t = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{(c)_i})$. Firstly, we note

$$\begin{aligned}\text{c\_term}(d,t'), t = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{t'} &\vdash_{\text{PA}} \text{c\_term}(d * [t], t) \\ &\vdash_{\text{PA}} \text{term}(t).\end{aligned}$$

   Using ($\exists$) and (DT) this leads to

$$\begin{aligned}&\vdash_{\text{PA}} \text{term}(t') \to \text{term}(\underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{t'}) \\ &\vdash_{\text{PA}} \Box(\text{term}(t') \to \text{term}(\underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{t'})) && \text{(D1)} \\ &\vdash_{\text{PA}} \Box(\text{term}(t') \to \text{term}(\underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{t'})) \to (\Box\text{term}(t') \to \Box\text{term}(\underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{t'})) && \text{(D2)}\end{aligned}$$

   and therefore by Modus Ponens we obtain

$$\vdash_{\text{PA}} \Box\text{term}(t') \to \Box\text{term}(\underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{t'}). \tag{12}$$

   We set $T = \{\forall l' < l \varphi(l), \text{c\_term}(c,t) \wedge \text{length}(c) = l, i < l - \underline{1} \wedge t = \underline{2}^{\ulcorner \mathbf{S} \urcorner} \cdot \underline{3}^{(c)_i}\}$.

$$\begin{aligned}&T \vdash_{\text{PA}} \text{c\_term}(c_{<\mathbf{S}i}, (c)_i) \\ &\quad \vdash_{\text{PA}} \text{length}(c_{<\mathbf{S}i}) = \mathbf{S}i \leq l - \underline{1} < l \\ &\quad \vdash_{\text{PA}} \Box\text{term}((c)_i) && \text{(IH)} \\ &\quad \vdash_{\text{PA}} \Box\text{term}((c)_i) \to \Box\text{term}(t) && \text{(12)} \\ &\quad \vdash_{\text{PA}} \Box\text{term}(t). && \text{(MP)}\end{aligned}$$

   Using ($\exists$) and strong induction, the first statement follows.

3. The proof of 3. is omitted since it uses similar arguments as the proof of the second statement.

⊣

*Proof of* (D3). The proof of (D3) uses the same ideas as the proof of Lemma 4.13. We define $\psi(l) = \forall c \forall f(\text{proof}(c,f) \wedge \text{length}(c) = l \rightarrow \Box(\text{provable}(f))$. If we show that $\vdash_{\text{PA}} \forall l \psi(l)$ holds, we can conclude (D3) by substituting $\ulcorner\varphi\urcorner$ for $f$. To achieve this, we apply strong induction.

The case $l = \mathbf{0}$ is trivial. For $l = \underline{1}$ the sequence $c$ encoding a proof of $f$ consists only of $(c)_{\mathbf{0}} = (c)_{\text{last}} = f$ and thus we have either logical_axiom$(f)$ or peano_axiom$(f)$. Each case consists of multiple cases with similar proofs, and thus we will only consider the case axiom_L$_1(f)$ and prove $\vdash_{\text{PA}}$ axiom_L$_1(f) \rightarrow \Box$provable$(f)$. We define $T = \{\text{formula}(f') \wedge \text{formula}(f'') \wedge f = \underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f'} \cdot \underline{5}^{\underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f''} \cdot \underline{5}^{f'}}\}$. Then

$$
\begin{aligned}
&T \vdash_{\text{PA}} \Box(\text{formula}(f')) && (4.13)\\
&\vdash_{\text{PA}} \Box(\text{formula}(f'')) && (4.13)\\
&\vdash_{\text{PA}} \underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f'} \cdot \underline{5}^{\underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f''} \cdot \underline{5}^{f'}} = \underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f'} \cdot \underline{5}^{\underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f''} \cdot \underline{5}^{f'}} && (\text{L}_{16})\\
&\vdash_{\text{PA}} \Box(\underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f'} \cdot \underline{5}^{\underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f''} \cdot \underline{5}^{f'}} = \underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f'} \cdot \underline{5}^{\underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f''} \cdot \underline{5}^{f'}}) && (\text{D1})\\
&\vdash_{\text{PA}} \Box(\text{formula}(f') \wedge \text{formula}(f'') \wedge \underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f'} \cdot \underline{5}^{\underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f''} \cdot \underline{5}^{f'}}\\
&\qquad = \underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f'} \cdot \underline{5}^{\underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f''} \cdot \underline{5}^{f'}}) && (4.12)\\
&\vdash_{\text{PA}} \Box(\text{logical\_axiom}(f)).
\end{aligned}
$$

Due to $\vdash_{\text{PA}}$ logical_axiom$(f) \rightarrow$ provable$(f)$ we obtain with (D1) $\vdash_{\text{PA}} \Box$(logical_axiom$(f)$ $\rightarrow$ provable$(f)$) and thus using (D2) $\vdash_{\text{PA}} \Box(\text{logical\_axiom}(f)) \rightarrow \Box(\text{provable}(f))$. All in all, this implies using (MP), ($\exists$) and (DT) that $\vdash_{\text{PA}}$ logical_axiom$(f) \rightarrow \Box$(provable$(f)$) is satisfied.

For the induction step we use

$$
\begin{aligned}
\forall l' < l \psi(l'), \text{proof}(c,f) \wedge \text{length}(c) = l \vdash_{\text{PA}} (c)_{\text{last}} = f \wedge \forall k < l \big[&\text{axiom}((c)_k) \vee \exists i < k\\
&\exists j < k(\text{MP}((c)_i,(c)_j,(c)_k)) \vee \exists i < k \exists v(\text{var}(v)\\
&\wedge \text{GR}((c)_i, v, (c)_k))\big].
\end{aligned}
$$

The case that $f$ is the code of a logical axiom or of an axiom of Peano Arithmetic is already handled in the base case. For the case that the formula encoded by $f$ is obtained from two other formulas using Modus Ponens, we note

$$
\begin{aligned}
\text{proof}(c', f'), \text{proof}(c'', f''), f'' = \underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f'} \cdot \underline{5}^{f} &\vdash_{\text{PA}} \text{proof}(c' * c'' * [f], f)\\
&\vdash_{\text{PA}} \text{provable}(f).
\end{aligned}
$$

Therefore, we obtain using ($\exists$) and (DT)

$$
\begin{aligned}
&\vdash_{\text{PA}} \text{provable}(f') \wedge \text{provable}(\underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f'} \cdot \underline{5}^{f}) \rightarrow \text{provable}(f)\\
&\vdash_{\text{PA}} \Box(\text{provable}(f') \wedge \text{provable}(\underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f'} \cdot \underline{5}^{f}) \rightarrow \text{provable}(f)) && (\text{D1})\\
&\vdash_{\text{PA}} \Box(\text{provable}(f') \wedge \text{provable}(\underline{2}^{\ulcorner\rightarrow\urcorner} \cdot \underline{3}^{f'} \cdot \underline{5}^{f})) \rightarrow \Box(\text{provable}(f)). && (\text{D2, MP})
\end{aligned}
$$

Therefore, using Corollary 4.12 and the substitution theorem we can derive

$$\vdash_{\mathrm{PA}} \Box(\mathrm{provable}(f')) \wedge \Box(\mathrm{provable}(\underline{2}^{\ulcorner\to\urcorner} \cdot \underline{3}^{f'} \cdot \underline{5}^{f})) \to \Box(\mathrm{provable}(f)). \tag{13}$$

We define $T' = \{\forall l' < l\psi(l'), \mathrm{proof}(c, f), \mathrm{length}(c) = l, i < l - \underline{1}, j < l - \underline{1}, \mathrm{MP}((c)_i, (c)_j, f)\}$ and get

$$\begin{aligned}
T' &\vdash_{\mathrm{PA}} (c)_j = \underline{2}^{\ulcorner\to\urcorner} \cdot \underline{3}^{(c)_i} \cdot \underline{5}^{f} \\
&\vdash_{\mathrm{PA}} \mathrm{proof}(c_{<\mathbf{S}i}, (c)_i) \wedge \mathrm{length}(c_{<\mathbf{S}i}) = \mathbf{S}i \leq l - \underline{1} < l \\
&\vdash_{\mathrm{PA}} \Box(\mathrm{provable}((c)_i) && \text{(IH)} \\
&\vdash_{\mathrm{PA}} \Box(\mathrm{provable}((c)_j) && \text{(analogous)} \\
&\vdash_{\mathrm{PA}} \Box(\mathrm{provable}((c)_i)) \wedge \Box(\mathrm{provable}(\underline{2}^{\ulcorner\to\urcorner} \cdot \underline{3}^{(c)_i} \cdot \underline{5}^{f})) && (\wedge) \\
&\vdash_{\mathrm{PA}} (\Box(\mathrm{provable}((c)_i)) \wedge \Box(\mathrm{provable}(\underline{2}^{\ulcorner\to\urcorner} \cdot \underline{3}^{(c)_i} \cdot \underline{5}^{f}))) \to \Box(\mathrm{provable}(f)) && (13) \\
&\vdash_{\mathrm{PA}} \Box(\mathrm{provable}(f)). && \text{(MP)}
\end{aligned}$$

The last possibility is that the formula encoded by $f$ is obtained from another formula using the generalization rule. We have

$$\begin{aligned}
\mathrm{proof}(c', f'), \mathrm{var}(v), f = \underline{2}^{\ulcorner\forall\urcorner} \cdot \underline{3}^{v} \cdot \underline{5}^{f'} &\vdash_{\mathrm{PA}} \mathrm{proof}(c' * [f], f) \\
&\vdash_{\mathrm{PA}} \mathrm{provable}(f)
\end{aligned}$$

which implies

$$\vdash_{\mathrm{PA}} \mathrm{provable}(f') \wedge \mathrm{var}(v) \to \mathrm{provable}(\underline{2}^{\ulcorner\forall\urcorner} \cdot \underline{3}^{v} \cdot \underline{5}^{f'})$$

and hence in a similar way as above (using (D1) and (D2))

$$\vdash_{\mathrm{PA}} \Box(\mathrm{provable}(f')) \wedge \Box(\mathrm{var}(v)) \to \Box(\mathrm{provable}(f)). \tag{14}$$

We set $T'' = \{\forall l' < l\psi(l'), \mathrm{proof}(c, f), \mathrm{length}(c) = l, i < l - \underline{1}, \mathrm{var}(v), \mathrm{GR}((c)_i, v, f)\}$. Then the following holds:

$$\begin{aligned}
T'' &\vdash_{\mathrm{PA}} \mathrm{proof}(c_{<\mathbf{S}i}, (c)_i) \wedge \mathrm{length}(c_{<\mathbf{S}i}) = \mathbf{S}i < l \\
&\vdash_{\mathrm{PA}} \Box(\mathrm{provable}((c)_i)) && \text{(IH)} \\
&\vdash_{\mathrm{PA}} \Box(\mathrm{var}(v)) && (4.13) \\
&\vdash_{\mathrm{PA}} \Box(\mathrm{provable}((c)_i)) \wedge \Box(\mathrm{var}(v)) && (\wedge) \\
&\vdash_{\mathrm{PA}} \Box(\mathrm{provable}(f)). && (14)
\end{aligned}$$

Therefore, using $(\exists)$ and proof by cases, we obtain the induction step. $\dashv$

## 4.4 The Second Incompleteness Theorem

At last, we are able to prove the Second Incompleteness Theorem. A slightly different proof can be encountered in [Rau08]. As a last prerequisite for the Second Incompleteness, we need to formalize the notion of consistency.

**Definition 4.14.** We define the formula

$$\mathrm{Con}_{\mathrm{PA}} := \neg\Box\bot,$$

where $\bot$ is a contradiction of the form $\bot = \alpha \wedge \neg\alpha$ for some sentence $\alpha$.

*Remark* 4.15. The formula $\mathrm{Con}_{\mathrm{PA}}$ is well-defined: Assume that $\alpha$ and $\beta$ are two sentences in $\mathcal{L}_{\mathrm{PA}}$. Then we have by $(\bot)$ that $\alpha \wedge \neg\alpha \equiv \beta \wedge \neg\beta$ and thus the claim is a consequence of Corollary 4.11.

**Theorem 4.16.** *If* PA *is consistent, then* $\nvdash_{\mathrm{PA}} \mathrm{Con}_{\mathrm{PA}}$.

*Proof.* Using the Diagonalization Lemma 4.4 we can find a closed $\mathcal{L}_{\mathrm{PA}}$-formula $\sigma$ satisfying

$$\sigma \equiv_{\mathrm{PA}} \neg\Box\sigma. \tag{15}$$

We assume that $\vdash_{\mathrm{PA}} \mathrm{Con}_{\mathrm{PA}}$ holds. Since $\sigma \wedge \neg\sigma \equiv_{\mathrm{PA}} \sigma \wedge \Box\sigma$ due to (15) and (A), the assumption is equivalent to

$$\begin{aligned} &\vdash_{\mathrm{PA}} \neg\Box(\sigma \wedge \Box\sigma) \\ (16)\quad &\vdash_{\mathrm{PA}} \neg(\Box\sigma \wedge \Box\Box\sigma). \end{aligned} \tag{4.12}$$

As a consequence of (D3), $(\wedge)$ and the Deduction Theorem, we have $\vdash_{\mathrm{PA}} \Box\sigma \to \Box\sigma \wedge \Box\Box\sigma$ and thus using $(\mathrm{L}_3)$ we obtain

$$\Box\sigma \equiv_{\mathrm{PA}} \Box\sigma \wedge \Box\Box\sigma. \tag{17}$$

To sum up, (16) and (17) imply

$$\begin{aligned} &\vdash_{\mathrm{PA}} \neg\Box\sigma \\ (18)\quad &\vdash_{\mathrm{PA}} \Box(\neg\Box\sigma). \end{aligned} \tag{D1}$$

On the other hand, we have $\neg\Box\sigma \equiv_{\mathrm{PA}} \neg\Box(\neg\Box\sigma)$ due to (15) which obviously contradicts the consistency of PA because of (18). Hence $\nvdash_{\mathrm{PA}} \mathrm{Con}_{\mathrm{PA}}$. ⊣

**Corollary 4.17** (Second Incompleteness Theorem)**.** *Let* $T \supseteq$ PA *be an extension of PA which is given by finitely many axioms resp. axiom schemas. As in the case of* PA *one can gödelize* $T$ *and in particular, one can introduce a relation* $\mathrm{Con}_T$ *in the same way as in* PA. *If* $T$ *is consistent, then we have* $\nvdash_{\mathrm{PA}} \mathrm{Con}_T$.

# Chapter 5

# Presburger Arithmetic

## 5.1 Basic number theory in Presburger Arithmetic

The Presburger Arithmetic was introduced by Mojżesz Presburger in [Pre29] after whom it is named. It consists of the axioms of Peano Arithmetic which are not concerned with multiplication.

**Definition 5.1.** The Presburger Arithmtic (Pres) consists of the following axioms in the language $\mathcal{L}_{\text{Pres}} = \{\mathbf{0}, \mathbf{S}, +\}$:

($\text{PA}_1$) $\forall x(\mathbf{S}x \neq \mathbf{0})$,

($\text{PA}_2$) $\forall x \forall y(\mathbf{S}x = \mathbf{S}y \to x = y)$,

($\text{PA}_3$) $\forall x(x + \mathbf{0} = x)$,

($\text{PA}_4$) $\forall x \forall y(x + \mathbf{S}y = \mathbf{S}(x + y))$.

If $\varphi = \varphi(x, \vec{y})$ is an $\mathcal{L}_{\text{Pres}}$-formula with $\text{free}(\varphi) = \{x, y_0, \ldots, y_n\}$, we denote by ($\text{I}_\varphi$) the following axiom schema, called the induction schema:

$$\forall \vec{y}\Big[\varphi(\mathbf{0}, \vec{y}) \wedge \forall x\big(\varphi(x, \vec{y}) \to \varphi(\mathbf{S}x, \vec{y})\big) \to \forall x \varphi(x, \vec{y})\Big].$$

*Convention.* From now on, we will use the convention that $\equiv$ means $\equiv_{\text{Pres}}$.

We can prove all standard results of arithmetic concerning addition and $<$ resprectively $\leq$, but not multiplication, in the same way as in PA.

Presburger originally axiomatized the theory in a distinct manner; in particular, he renounced the induction axiom and allowed also the existence of negative numbers and hence subtraction by the axiom $\vdash_{\text{Pres}} \forall x \forall y \exists z(x + z = y)$.

As in Peano Arithmetic, we are able to define the natural numbers

$$\underline{n} = \underbrace{\mathbf{S} \ldots \mathbf{S}}_{n} \mathbf{0}$$

for any $n \in \mathbb{N}$.

Due to the completeness of Presburger Arithmetic (which will be shown in the subsequent sections), it is clear that it is impossible to define multiplication using addition and the successor function. However, it is possible to define the multiplication with a natural number of the form $\underline{n}, n \in \mathbb{N}$:

**Definition 5.2.** We define $\underline{0} \cdot x = \mathbf{0}$ and $\underline{n+1} \cdot x = \underline{n} \cdot x + x$ for any $n \in \mathbb{N}$ and for any variable $x$. Concretely, this means $\underline{n} \cdot x = \underbrace{x + \cdots + x}_{n}$.
For the sake of simplicity, we usually write $\underline{n}x$ instead of $\underline{n} \cdot x$.

*Remark* 5.3. As in the case of Peano Arithmetic, one can show that the properties stated in Proposition 3.1 hold. Note that the proof of (N2) shown in 3.1 can be realized in the same way for the definition of multiplication with natural numbers presented in 5.2.

Furthermore, for $m, n \in \mathbb{N}$ one has the associative as well as the distributive laws:

(1) $\vdash_{\text{Pres}} \forall x \forall y(\underline{n}(x+y) = \underline{n}x + \underline{n}y)$ and $\vdash_{\text{Pres}} \forall x \forall y(\underline{n}(x-y) = \underline{n}x - \underline{n}y)$,

(2) $\vdash_{\text{Pres}} \forall x(\underline{m+n}x = \underline{m}x + \underline{n}x)$ and $\vdash_{\text{Pres}} \forall x(\underline{m-n}x = \underline{m}x - \underline{n}x)$, if $m \geq n$,

(3) $\vdash_{\text{Pres}} \forall x(\underline{mn}x = \underline{m} \cdot (\underline{n}x))$.

*Proof.* In order to prove (1), we use metainduction on $n \in \mathbb{N}$. The case $n = 0$ is trivial. The induction step is a result of

$$\begin{aligned} \underline{n}(x+y) = \underline{n}x + \underline{n}y \vdash_{\text{Pres}} \underline{n+1}(x+y) &= \underline{n}(x+y) + (x+y) = (\underline{n}x + \underline{n}y) + (x+y) \\ &= (\underline{n}x + x) + (\underline{n}y + y) = \underline{n+1}x + \underline{n+1}y. \end{aligned}$$

The second property follows from the first one using $\vdash_{\text{Pres}} \underline{n}(x-y) + \underline{n}y = \underline{n}((x-y)+y) = \underline{n}x$. The equations (2) and (3) can be verified similarly by induction on $m$. ⊣

*Remark* 5.4. An easy consequence of (N1) is that for $m, n \in \mathbb{N}$ with $m > n$ we have $\vdash_{\text{Pres}} \underline{m-n} + \underline{n} = \underline{(m-n)+n} = \underline{m}$, hence we get the $\mathbb{N}$-conformity of $-$, i.e.

(4) $$\vdash_{\text{Pres}} \underline{m-n} = \underline{m} - \underline{n}.$$

**Lemma 5.5.** *For all natural numbers $n \geq 1$ we have*

1. $\vdash_{\text{Pres}} \forall x \forall y(\underline{n}x = \underline{n}y \leftrightarrow x = y)$,
2. $\vdash_{\text{Pres}} \forall x \forall y(\underline{n}x < \underline{n}y \leftrightarrow x < y)$.

*Proof.* Since both statements can be shown similarly, we omit the proof of 2. For 1. we prove the the direction $(\rightarrow)$ by cases using $\vdash_{\text{Pres}} \forall x \forall y(x < y \vee x = y \vee y > x)$ and hence by $(\vee 4)$ and symmetry it is sufficient to show

(5) $$\underline{n}x = \underline{n}y, x < y \vdash_{\text{Pres}} \bot.$$

For this, we have to show first using metainduction that

$$x < y \vdash_{\text{Pres}} \underline{n}x < \underline{n}y. \tag{6}$$

The case $n = 1$ is obvious. For the induction step we assume that $x < y \vdash_{\text{Pres}} \underline{n}x < \underline{n}y$ is satisfied.

$$\begin{aligned} x < y &\vdash_{\text{Pres}} \underline{n}x < \underline{n}y \\ &\vdash_{\text{Pres}} \underline{n+1}x = \underline{n}x + x < \underline{n}y + y = \underline{n+1}y. \end{aligned}$$

Therefore (6) holds and hence so does (5). The second direction can be shown easily using metainduction. ⊣

**Definition 5.6.** For $n \in \mathbb{N}$, $n \geq 2$, we define

$$x \equiv_n y :\leftrightarrow \exists z(\underline{n}z + x = y \vee \underline{n}z + y = x).$$

We call formulas of the form $x \equiv_n y$ **congruences**.

**Lemma 5.7.** *Let $n \geq 2$ be a natural number. Then one has*

1. $\vdash_{\text{Pres}} \forall x(x \equiv_n x)$,
2. $\vdash_{\text{Pres}} \forall x \forall y(x \equiv_n y \leftrightarrow y \equiv_n x)$,
3. $\forall x \forall y \forall z(x \equiv_n y \wedge y \equiv_n z \rightarrow x \equiv_n z)$.

*Proof.* All proofs are straightforward and follow immediately from the definition. ⊣

**Lemma 5.8.** *Let $n \geq 2$ be a natural number. Then*

$$\vdash_{\text{Pres}} \forall x \forall y \forall z(x \equiv_n y \leftrightarrow x + z \equiv_n y + z).$$

*Proof.* For both directions, we can use $(\exists)$ and $(\vee 1)$ and prove each case in the definition of congruences separately. Thus we need to show

$$\begin{aligned} \underline{n}w + x = y &\vdash_{\text{Pres}} x + z \equiv_n y + z \\ \underline{n}w + x + z = y + z &\vdash_{\text{Pres}} x \equiv_n y. \end{aligned}$$

Both statements are shown easily using basic results from Peano Arithmetic (which do not involve multiplication). ⊣

**Lemma 5.9.** *For any $n \in \mathbb{N}$ such that $n \geq 2$, we have $\vdash_{\text{Pres}} \forall x \exists y(\bigvee_{k=0}^{n-1}(\underline{n}y + \underline{k} = x))$.*

*Proof.* Let $n \geq 2$ be a natural number. We show the assertion using induction on $x$. The base case is clearly satisfied for $y = \mathbf{0}$ and $k = 0$ by applying ($L_6$) respectively ($L_7$) $n-1$ times. For the induction step, we show using ($\vee 1$)

$$\underline{n}y + \underline{k} = x \vdash_{\text{Pres}} \exists z(\bigvee_{l=0}^{n-1}(\underline{n}z + \underline{l} = \mathbf{S}x)). \tag{7}$$

We distinguish between two cases, each of which implies (7) using ($L_6$) respectively ($L_7$) multiple times. Firstly, we have

$$\begin{aligned}\underline{n}y + \underline{k} = x, \underline{k} < \underline{n-1} &\vdash_{\text{Pres}} \underline{k+1} = \underline{k} + \underline{1} \leq \underline{n-1} \\ &\vdash_{\text{Pres}} \underline{n}y + \underline{k+1} = \underline{n}y + \underline{k} + \underline{1} = x + \underline{1} = \mathbf{S}x.\end{aligned}$$

By (N3) and (N4) we know that $k < n-1$, hence the first case follows. Now, since $k \leq n-1$, the case $\underline{k} \geq \underline{n-1}$ is equivalent to $\underline{k} = \underline{n-1}$ (and thus $k = n-1$), again by (N4). Moreover,

$$\begin{aligned}\underline{n}y + \underline{k} = x, \underline{k} = \underline{n-1} &\vdash_{\text{Pres}} \underline{n} \cdot \mathbf{S}y + \underline{0} = \underline{n}(y + \underline{1}) \overset{(1)}{=} \underline{n}y + \underline{n} = \underline{n}y + \underline{k+1} \\ &= \underline{n}y + \underline{k} + \underline{1} = x + \underline{1} = \mathbf{S}x.\end{aligned}$$

Hence we can conclude the induction step. ⊣

*Remark* 5.10. In particular, the previous lemma shows

$$\vdash_{\text{Pres}} \forall x \bigvee_{k=0}^{n-1}(x \equiv_n \underline{k})$$

for an arbitrary natural number $n \geq 2$.

**Lemma 5.11.** *Let $n \in \mathbb{N}$ such that $n \geq 2$. Then*

$$\vdash_{\text{Pres}} \forall x \forall y(\neg(x \equiv_n y) \leftrightarrow \bigvee_{k=1}^{n-1}(x + \underline{k} \equiv_n y)).$$

*Proof.* We show the assertion by induction on $x$.

- We consider the case $x = \mathbf{0}$. For ($\rightarrow$), we note that Lemma 5.9 implies

$$\vdash_{\text{Pres}} \exists w(\bigvee_{k=0}^{n-1}(\underline{n}w + \underline{k} = y)).$$

Using ($\vee 1$), it is enough to show for all $1 \leq l \leq n-1$ that one has

$$\neg(\mathbf{0} \equiv_n y), \underline{n}w = y \vdash_{\text{Pres}} \bigvee_{k=1}^{n-1}(\underline{k} \equiv_n y), \tag{8}$$

$$\neg(\mathbf{0} \equiv_n y), \underline{n}w + \underline{l} = y \vdash_{\text{Pres}} \bigvee_{k=1}^{n-1}(\underline{k} \equiv_n y). \tag{9}$$

Condition (8) follows from ($\perp$) due to $\underline{n}w = y \vdash_{\text{Pres}} \mathbf{0} \equiv_n y$ and (9) holds because of $\underline{n}w + \underline{l} = y \vdash_{\text{Pres}} \underline{l} \equiv_n y$.
The second direction is also shown by contradiction with the help of ($\vee$1). Let $1 \leq k \leq n-1$. Then we have

$$\underline{k} \equiv_n y, \mathbf{0} \equiv_n y \vdash_{\text{Pres}} \underline{k} \equiv_n \mathbf{0} \tag{5.7}$$
$$\vdash_{\text{Pres}} \exists z(\underline{n}z + \underline{k} = \mathbf{0} \vee \underline{k} = \underline{n}z).$$

This leads to a contradiction, since $\underline{n}z + \underline{k} = \mathbf{0} \vdash_{\text{Pres}} \underline{k} = \mathbf{0}$ and $\underline{k} = \underline{n}z \vdash_{\text{Pres}} \underline{k} = \mathbf{0} \vee \underline{k} \geq \underline{n}$ which contradicts $1 \leq k \leq n-1$ by (N4). Thus we obtain $\underline{k} \equiv_n y \vdash_{\text{Pres}} \neg(\mathbf{0} \equiv_n y)$.

- For the induction step we consider the case $y = \mathbf{0}$ and $y \geq \underline{1}$ separately; the first case is similar to the base case and can thus be omitted. Let

$$T = \{\forall y(\neg(x \equiv_n y) \leftrightarrow \bigvee_{k=1}^{n-1}(x + \underline{k} \equiv_n y)), y \geq \underline{1}\}.$$

Then we have

$$T \vdash_{\text{Pres}} \mathbf{S}x \equiv_n y \leftrightarrow x \equiv_n y - \underline{1} \tag{5.7}$$
$$\vdash_{\text{Pres}} \neg(\mathbf{S}x \equiv_n y) \leftrightarrow \neg(x \equiv_n y - \underline{1}) \tag{B.2}$$
$$\vdash_{\text{Pres}} \neg(x \equiv_n y - \underline{1}) \leftrightarrow \bigvee_{k=1}^{n-1}(x + \underline{k} \equiv_n y - \underline{1})$$
$$\vdash_{\text{Pres}} x + \underline{k} \equiv_n y - \underline{1} \leftrightarrow \mathbf{S}x + \underline{k} \equiv_n y \tag{5.7}$$
$$\vdash_{\text{Pres}} \bigvee_{k=1}^{n-1}(x + \underline{k} \equiv_n y - \underline{1}) \leftrightarrow \bigvee_{k=1}^{n-1}(\mathbf{S}x + \underline{k} \equiv_n y) \tag{H.2}$$
$$\vdash_{\text{Pres}} \neg(\mathbf{S}x \equiv_n y) \leftrightarrow \bigvee_{k=1}^{n-1}(\mathbf{S}x + \underline{k} \equiv_n y) \tag{D.4}$$

which concludes the proof.

$\dashv$

## 5.2 Equations and congruences in Presburger Arithmetic

In order to prove the completeness of Presburger Arithmetic, we need some general statements about equations and congruences and their negations. We will then apply these results in the next section in order to eliminate all quantifiers and thus conclude that all closed formulas in $\mathcal{L}_{\text{Pres}}$ are decidable.

*Notation.* We denote equations and congruences as **ground statements**.

**Lemma 5.12.** *The following statements hold:*

1. *Let* $\approx \in \{=, \neq\} \cup \{\equiv_n | \ n \in \mathbb{N}, n \geq 2\}$. *Then we have* $\vdash_{\text{Pres}} \forall w \forall x \forall y \forall z (w = x \wedge y \approx z \leftrightarrow w = x \wedge y + w \approx z + x)$.
2. *Let* $n \geq 2$ *be a natural number. Then we have* $\vdash_{\text{Pres}} \forall w \forall x \forall y \forall y (w \equiv_n x \wedge y \equiv_n z \leftrightarrow w \equiv_n z \wedge y + w \equiv_n z + x)$.

*Proof.*

1. Since all three cases are proved in the same manner, we will only consider the first one. Using $(\leftrightarrow)$ we show each direction separately. Firstly, we have

$$\begin{aligned} w = x \wedge y = z &\vdash_{\text{Pres}} y + w = z + x && (\text{L}_{18}) \\ &\vdash_{\text{Pres}} w = x \wedge y + w = z + x. && (\wedge) \end{aligned}$$

   The second direction is a result of

$$\begin{aligned} w = x \wedge y + w = z + x &\vdash_{\text{Pres}} y + (w + x) = (y + w) + x = (y + w) + w \\ &\qquad = (z + w) + x = z + (w + x) \\ &\vdash_{\text{Pres}} y = z \\ &\vdash_{\text{Pres}} w = x \wedge y = z. \end{aligned}$$

2. The proof essentially follows from Lemma 5.8 using the same arguments as above.

⊣

**Lemma 5.13.** *Any equation in* $\mathcal{L}_{\text{Pres}}$ *containing the variable* $x$ *is equivalent to an equation of the form* $\underline{n}x + t = s$ *for* $\mathcal{L}_{\text{Pres}}$*-terms* $t$ *and* $s$ *with* $x \notin \text{var}(t) \cup \text{var}(s)$ *and* $n \in \mathbb{N}$.

*Proof.* Let $t$ be any $\mathcal{L}_{\text{Pres}}$-term. We will prove by induction on the construction of terms that $t \sim \underline{n}x + s$ for some $n \in \mathbb{N}$ and a term $s$ with $x \notin \text{var}(x)$.

- If $t$ is $x$, then $t \sim \underline{1}x + \mathbf{0}$. If $t$ is $y$ for some other variable $y$, then $t \sim \underline{0}x + y$. In both cases, the desired condition is fulfilled.
- Let $t$ be $\mathbf{S}(\underline{n}x + s)$ with $n \in \mathbb{N}$ and $x \notin \text{var}(s)$. Then $t \sim \underline{n}x + \mathbf{S}s$.
- Let $t$ be $(\underline{n}x + s) + (\underline{n'}x + s')$ with $n, n' \in \mathbb{N}$ and $x \notin \text{var}(s) \cup \text{var}(s')$. Then we have that $t \sim (\underline{n} + \underline{n'})x + (s + s') \sim \underline{n + n'}x + (s + s')$ and $x \notin \text{var}(s + s')$.

Let now $t = t'$ be an equation in $\mathcal{L}_{\text{Pres}}$. Then, by what we have shown above, we can write the equation equivalently as $\underline{n}x + s = \underline{n'}x + s'$. Without loss of generality, we may assume that $n > n'$. Then (N3) and (N4) imply $\vdash_{\text{Pres}} \underline{n} > \underline{n'}$. Thus using (2) we obtain that $(t = t') \equiv ((\underline{n}x - \underline{n'}x) + t = s) \equiv (\underline{n - n'}x + t = s)$. ⊣

*Remark* 5.14. Similarly, one can prove that every congruence in $\mathcal{L}_{\text{Pres}}$ is equivalent to a congruence of the form $\underline{m}x + t \equiv_n s$ for $n, m \in \mathbb{N}$ with $n, m \geq 2$ and for $\mathcal{L}_{\text{Pres}}$-terms $t$ and $s$ with $x \notin \text{var}(t) \cup \text{var}(s)$. We call such equations and congruences to be in $x$**-normal form**.

**Lemma 5.15.** *Let $\alpha$ be an equation in $x$-normal form $\underline{n}x + t = s$. Then for any $m \in \mathbb{N}\backslash\{0\}$ such that $n|m$ we have $\alpha \equiv (\underline{m}x + t' = s')$ for some $\mathcal{L}_{\text{Pres}}$-terms $t', s'$ that do not contain the variable $x$.*

*Proof.* Let $k \in \mathbb{N}$ such that $kn = m$ and let $\beta$ be the equation $\underline{m}x + \underline{k}t = \underline{k}s'$. Then $\beta$ is also in $x$-normal form and Lemma 5.5 implies that $\alpha \equiv \beta$. ⊣

**Lemma 5.16.** *Let $\alpha$ denote the congruence $\underline{n}x + t \equiv_m s$ in $x$-normal form. Then for any $k \in \mathbb{N}$ s.t. $m|k$, $\alpha$ is equivalent to congruences in $x$-normal form of the type $\underline{n'}x + t' \equiv_k s'$ and $\underline{k}x + t'' \equiv_{m'} s''$.*

*Proof.* By multiplication with $\frac{k}{\underline{m}}$ (respectively with $\frac{k}{\underline{n}}$) and (3) it is enough to prove the more general statement

$$t \equiv_n s \text{ is equivalent to } \underline{m}t \equiv_{mn} \underline{m}s. \tag{10}$$

To prove this, we use $(\vee 1)$ and prove for both directions (by symmetry) only one of the two cases in the definition of congruences.
The first direction follows then from

$$\begin{aligned} \underline{n}x + t = s &\vdash_{\text{Pres}} \underline{mn}x + \underline{m}t \overset{(3)}{=} \underline{m} \cdot \underline{n}x + \underline{m}t \overset{(1)}{=} \underline{m}(\underline{n}x + t) = \underline{m}s \\ &\vdash_{\text{Pres}} \underline{m}t \equiv_{mn} \underline{m}s \end{aligned}$$

and $(\exists)$. The second direction is again a consequence of $(\exists)$, this time in combination with

$$\begin{aligned} \underline{mn}x + \underline{m}t = \underline{m}s &\vdash_{\text{Pres}} \underline{m}(\underline{n}x + t) \overset{(1)}{=} \underline{m} \cdot \underline{n}x + \underline{m}t \overset{(3)}{=} \underline{mn}x + \underline{m}t = \underline{m}s \\ &\vdash_{\text{Pres}} \underline{n}x + t = s \\ &\vdash_{\text{Pres}} t \equiv_n s. \end{aligned} \tag{5.5}$$

Therefore we have verified (10) and the claim holds. ⊣

**Lemma 5.17.** *Let $\underline{n}x + t \equiv_m s$ be a congruence in $x$-normal form. Then $\exists x(\underline{n}x + t \equiv_m s)$ is equivalent to $t \equiv_k s$, where $k = gcd(m, n)$.*

*Proof.* Let $m', n' \in \mathbb{N}$ such that $km' = m$ and $kn' = n$. We will show each direction separately.

1. The first direction is simple. We have to consider two cases (by the definition of

congruence) but since both can be shown similarly, we only consider the first one.

$$\begin{aligned}\underline{m}y + \underline{n}x + t = s &\vdash_{\text{Pres}} \underline{k}(\underline{m'}y + \underline{n'}x) + t \overset{(1)}{=} \underline{k} \cdot \underline{m'}y + \underline{k} \cdot \underline{n'}x + t \overset{(3)}{=} \underline{km'}y + \underline{kn'}x + t \\ &= \underline{m}y + \underline{n}x = s \\ &\vdash_{\text{Pres}} t \equiv_k s.\end{aligned}$$

2. The second direction requires more work. We know that $m'$ and $n'$ are coprime, hence there exist $a, b \in \mathbb{N}$ such that $n'a = m'b + 1$ (or $n'a + 1 = m'b$, but we will only consider the first possibility). Again, we have either $\exists x(\underline{k}x + t = s)$ or $\exists x(t = \underline{k}x + s)$ and without loss of generality we assume the first statement. Then

$$\begin{aligned}\underline{k}y + t = s &\vdash_{\text{Pres}} s = \underline{1} \cdot \underline{k}y + t = \underline{n'a - m'b} \cdot \underline{k}y + t = \underline{na - mb} \cdot y + t && (3) \\ &= \underline{nay} - \underline{mby} + t = \underline{n} \cdot \underline{ay} - \underline{m} \cdot \underline{by} + t && (2, 3) \\ &\vdash_{\text{Pres}} \underline{n} \cdot \underline{ay} + t = \underline{m} \cdot \underline{by} + s \\ &\vdash_{\text{Pres}} \exists x(\underline{n}x + t \equiv_m s).\end{aligned}$$

⊣

**Lemma 5.18.** *Let $\alpha$ be a ground statement or a negated equation. Then there exists a ground statement $\alpha'$ with $x \notin \text{var}(\alpha')$ such that $\exists x\alpha \equiv \alpha'$.*

*Proof.* We can assume $\alpha$ to be in $x$-normal form. We have to consider the following three cases.

- If $\alpha$ is the equation $\underline{n}x + t = s$, then $\exists x\alpha = (t \equiv_n s)$ which is again a ground statement.
- Suppose that $\alpha$ is the negated equation $\neg(\underline{n}x + t = s)$. Then we obviously have $\vdash_{\text{Pres}} \exists x\alpha$ and hence $\exists x\alpha \equiv (\mathbf{0} = \mathbf{0})$.
- Lastly, we assume that $\alpha$ is the congruence $\underline{n}x + t \equiv_m s$. Then by 5.17, $\exists x\alpha$ is equivalent to a congruence.

⊣

**Lemma 5.19.** *Let $\alpha$ and $\beta$ be either two ground statements or an equation and a negated equation, and let $x$ be a variable. Then there exist ground statements (or an equation and a negated equation) $\alpha'$ and $\beta'$ such that $x \notin \text{var}(\beta')$ and $\alpha \wedge \beta \equiv \alpha' \wedge \beta'$.*

*Proof.* Let $\alpha = (\underline{n}x + t \approx_1 s)$ and $\beta = (\underline{n'}x + t' \approx_2 s')$ where $\approx_1, \approx_2 \in \{=, \neq\} \cup \{\equiv_m | \ m \in \mathbb{N}, m \geq 2\}$ satisfy the conditions specified above. In the cases that not both $\alpha$ and $\beta$ are congruences, due to 5.15 and 5.16 (by taking the least common multiple of $n$ and $n'$), we can assume that $n = n'$.
In the case that $\approx_1$ is $\equiv_m$ and $\approx_2$ is $\equiv'_m$, we can assume (by taking the least common multiple of $m$ and $m'$ and using 5.16) that $m = m'$. Thus let $\alpha$ be $\underline{n}x + t \equiv_m t$ and $\beta$ be

$\underline{n'}x + t' \equiv_m s'$. The next goal is to show that we can assume $n$ and $n'$ to be equal. If this is not the case, we can proceed as follows:

Without loss of generality, we can assume $n' < n$. We set $n'' := n - n'$. Then we have

$$\begin{aligned}
\alpha \wedge \beta &\equiv (\underline{n}x + t \equiv_m s \wedge \underline{n'}x + t' \equiv_m s') \\
&\equiv (\underline{n}x + t + s' \equiv_m s + \underline{n'}x + t' \wedge \underline{n'}x + t' \equiv_m s') && (5.12) \\
&\equiv (\underline{n}x - \underline{n'}x + t + s' \equiv_m s + t' \wedge \underline{n'}x + t' \equiv_m s') && (5.12) \\
&\equiv (\underline{n''}x + t + s' \equiv_m s + t' \wedge \underline{n'}x + t' \equiv_m s'). && (2)
\end{aligned}$$

We can repeat this procedure finitely many times until we obtain two congruences in $x$-normal form with the same coefficient before $x$. In particular, we can assume, without loss of generality, that $n = n'$.

By (C.1) it is sufficient to assume that either $\approx_1$ is $=$ or $\approx_1$ and $\approx_2$ are both the same congruence $\equiv_n$. Thus we can apply Lemma 5.12 to obtain the assertion.

$$\begin{aligned}
\alpha \wedge \beta &= (\underline{n}x + t \approx_1 s) \wedge (\underline{n}x + t' \approx_2 s') \\
&\equiv (\underline{n}x + t \approx_1 s) \wedge (\underline{n}x + t' + s \approx_2 s' + \underline{n}x + t) && (5.12) \\
&\equiv (\underline{n}x + t \approx_1 s) \wedge (t' + s \approx_2 s' + t) && (5.8) \\
&= \alpha' \wedge \beta',
\end{aligned}$$

where $\alpha' = (\underline{n}x + t \approx_1 s)$ and $\beta' = (t' + s \approx_2 s' + t)$. ⊣

**Lemma 5.20.** *Conjunctions of negated equations can be handled in the following way.*

1. *Let $\alpha_1, \ldots, \alpha_n$ be negated equations. Then $\exists x(\alpha_1 \wedge \ldots, \wedge\alpha_n)$ is equivalent to $\mathbf{0} = \mathbf{0}$.*
2. *Let $\alpha$ be a congruence and $\alpha_1, \ldots, \alpha_n$ negated equations. Then $\exists x(\alpha \wedge \alpha_1 \wedge \cdots \wedge \alpha_n)$ is equivalent to a congruence $\alpha'$.*

*Proof.*

1. Since $\vdash_{\text{Pres}} \mathbf{0} = \mathbf{0}$ holds, it suffices to show $\vdash_{\text{Pres}} \exists x(\alpha_1 \wedge \cdots \wedge \alpha_n)$. Without loss of generality let $\alpha_1, \ldots, \alpha_n$ all be in $x$-normal form with the same coefficient before $x$, i.e. $\neg(\underline{m}x + t_i = s_i)$ for all $1 \leq i \leq n$.

$$\begin{aligned}
&\vdash_{\text{Pres}} \underline{m}(s_1 + \cdots + s_n + \underline{1}) + t_i \geq s_i + \underline{1} > s_i \text{ for all } 1 \leq i \leq n \\
&\vdash_{\text{Pres}} \bigwedge_{i=1}^{n} \neg(\underline{m}(s_1 + \cdots + s_n) + t_i = s_i) \\
&\vdash_{\text{Pres}} \exists x(\alpha_1 \wedge \cdots \wedge \alpha_n).
\end{aligned}$$

2. By Lemma 5.17 it is enough to prove $\exists x\alpha \vdash_{\text{Pres}} \exists x(\alpha \wedge \alpha_1 \wedge \cdots \wedge \alpha_n)$. We can again assume $\alpha$ and $\alpha_i$ to be in $x$-normal form for all $1 \leq i \leq n$ with the same coefficient before $x$ (by taking the least common multiple). Thus we can write $\alpha = (\underline{k}x + t \equiv_m s)$

and $\alpha_i = \neg(\underline{k}x + t_i = s_i)$ for all $1 \leq i \leq n$. Without loss of generality, let $k \geq 1$. Then we have for all $1 \leq i \leq n$:

$$\begin{aligned}
\underline{m}y + \underline{k}x + t = s, \underline{k}x + t_i = s_i &\vdash_{\text{Pres}} \underline{m}y + \underline{k}(x + \underline{m}y) + t = s + \underline{m} \cdot \underline{k}y && (1, 3)\\
&\vdash_{\text{Pres}} \underline{k}(x + \underline{m}y) + t = \underline{m} \cdot \underline{k-1}y + s && (1, 2)\\
&\vdash_{\text{Pres}} \underline{k}(x + \underline{m}y) + t \equiv_m s\\
&\vdash_{\text{Pres}} \underline{k}(x + \underline{m}y) + t_i > \underline{k}x + t_i = s_i && (5.5.2)\\
&\vdash_{\text{Pres}} \neg(\underline{k}(x + \underline{m}y) + t_i = s_i).
\end{aligned}$$

Thus we obtain

$$\begin{aligned}
\underline{m}y + \underline{k}x + t = s, \bigvee_{i=1}^{n}(\underline{k}x + t_i = s_i) &\vdash_{\text{Pres}} \bigwedge_{i_1}^{n} \neg(\underline{k}(x + \underline{m}y) + t_i = s_i)\\
&\vdash_{\text{Pres}} \underline{m}y + \underline{k}x + t = s \wedge \bigwedge_{i_1}^{n} \neg(\underline{k}(x + \underline{m}y) + t_i = s_i)\\
&\vdash_{\text{Pres}} \exists x(\alpha \wedge \alpha_1 \wedge \cdots \wedge \alpha_n).
\end{aligned}$$

Due to

$$\bigvee_{i=1}^{n}(\underline{k}x + t_i = s_i) \equiv \neg \bigwedge_{i=1}^{n} \neg(\underline{k}x + t_i = s_i)$$

and the triviality of the second case

$$\underline{m}y + \underline{n}x + t = s, \bigwedge_{i=1}^{n} \neg(ukx + t_i = s_i) \vdash_{\text{Pres}} \exists x(\alpha \wedge \alpha_1 \wedge \cdots \wedge \alpha_n),$$

we can deduce by $(\vee 2)$ that $\underline{m}y + \underline{n}x + t = s \vdash_{\text{Pres}} \exists x(\alpha \wedge \alpha_1 \wedge \cdots \wedge \alpha_n)$ holds. The claim is then a consequence of $(\exists)$ and $(\vee 1)$ (by also considering the case $\underline{n}x + t = \underline{m}y + s$ which follows in a similar way).

⊣

## 5.3 Completeness of Presburger Arithmetic

The idea of Presburger's completeness proof is the elimination of all quantifiers with the exception that existential quantifiers in congruences are permitted. From now on, we are only interested in equivalence classes of formulas, since we have $\vdash_{\text{Pres}} \varphi \leftrightarrow \psi \Longrightarrow (\vdash_{\text{Pres}} \varphi \Leftrightarrow \vdash_{\text{Pres}} \psi)$ for any two $\mathcal{L}_{\text{Pres}}-$ formulas $\varphi, \psi$.

We eliminate all quantifiers of an $\mathcal{L}_{Pres}$-sentence according to the following algorithm.

**First step: elimination of $\rightarrow$ and $\leftrightarrow$**

By definition, we have that $\varphi \leftrightarrow \psi$ is $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$ and by (K.0) we know that $\varphi \rightarrow \psi \equiv \neg\varphi \vee \psi$ for any formulas $\varphi$ and $\psi$.

**Second step: shifting quantifiers to the beginning**

This step has the goal to write any formula in the form $\diamond_1 x_1 \dots \diamond_n x_n \varphi$, where $\varphi$ is free of quantifiers and $\diamond_i \in \{\forall, \exists\}$ for all $1 \leq i \leq n$.

Let $\alpha$ be an arbitrary $\mathcal{L}_{\text{Pres}}-$formula. We show by induction on the construction of formulas that there is an equivalent formula whose existential quantifiers are all at the beginning.

- If $\alpha$ is a ground statement, then $\alpha$ already satisfies the desired condition.
- If $\alpha = \varphi \wedge \psi$ or $\alpha = \varphi \vee \psi$ for two formulas $\varphi, \psi$ whose quantifiers are at the beginning, then by multiple applications of (L.1), (L.2) and (L.3), we can assume all variables of $\varphi$ and $\psi$ to be distinct. By making use of (N.1)-(N.5) (or, in the case of $\alpha = \varphi \vee \psi$, (O.1)-(O.5)) various times, we obtain a formula equivalent to $\alpha$ where all quantifiers are at the beginning.
- If $\alpha$ is $\neg\varphi$, where all the quantifiers of $\varphi$ are at the beginning, then we can successively shift the negation symbol to the end of the string of quantifers by multiple applications of $\neg\exists x \psi \equiv \forall x \neg\psi$ and $\neg\forall x \psi \equiv \exists x \neg\psi$.
- If $\alpha = \exists x \varphi$ or $\forall x \varphi$, where all quantifiers of $\varphi$ are at the initial position of the formula, then the same holds also for $\alpha$.

In particular, we obtain that any $\mathcal{L}_{\text{Pres}}$-sentence is equivalent to an $\mathcal{L}_{\text{Pres}}$-formula whose quantifiers are all at the beginning.

**Third step: elimination of the $\forall$-quantifier**

Since we have $\forall x \varphi \equiv \neg\exists x \neg\varphi$ for any formula $\varphi$ by the tautology (K.2), every formula is equivalent to a formula of the form $(\neg)\exists x_1, \dots, (\neg)\exists x_n \varphi$ for some formula $\varphi$ which does not contain any quantifiers.

**Fourth step: the disjunctive normal form**

We consider now only formulas of the form $\alpha = (\neg)\exists x_1, \dots, (\neg)\exists x_n \varphi$ with $\text{var}(\varphi) = \text{free}(\varphi)$. We will now show how $\varphi$ can be written equivalently as a formula in the disjunctive normal form meaning that it is a disjunction of conjunctive clauses of the form $((\neg)\alpha_{1,1}\wedge, \dots, \wedge(\neg)\alpha_{1,k_1})\vee, \dots, \vee((\neg)\alpha_{n,1}\wedge, \dots, \wedge(\neg)\alpha_{n,k_n})$ where $\alpha_{i,j}$ are ground statements for all $i$ and $j$. We obtain this according to the following algorithm which can also be found in [HA28].

1. We shift all negation symbols to the inside of the formula until every negation refers to a ground statement rather than to a conunction or disjunction. For this, we apply (F.1) and (F.2) which imply that $\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$ and $\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$ for all ground statements $\alpha$ and $\beta$ until the desired condition is attained.
2. We eliminate all negations until there is either one or no negation symbol before every ground statement. This can be achieved by applying $\neg\neg\alpha \equiv \alpha$ for all ground statements $\alpha$ (which follows from (A)) various times.

3. In order to obtain a disjunction of conjunctive clauses, we need to use (I.2) and (C.1) which imply that $(\alpha \vee \beta) \wedge \gamma \equiv (\alpha \wedge \gamma) \vee (\beta \wedge \gamma)$ and $\alpha \wedge (\beta \vee \gamma) \equiv (\alpha \wedge \gamma) \vee (\alpha \wedge \beta)$ for any three (possibly negated) ground statements $\alpha, \beta$ and $\gamma$.

**Fifth step: elimination of the existential quantifiers**

The idea is to eliminate step by step the existential quantifers, starting with the innermost one. Since $\exists x(\alpha \vee \beta) \equiv \exists x\alpha \vee \exists x\beta$ for any two (possibly negated) ground statements $\alpha$ and $\beta$, we can write the formula in disjunctive normal form (DNF) equivalently as

$$(\neg)\exists x_1, \ldots, (\neg)\exists x_{n-1}(\neg)(\exists x_n(\alpha_{1,1}\wedge, \ldots, \wedge\alpha_{1,k_1})\vee, \ldots, \vee\exists x_n(\alpha_{n,1}\wedge, \ldots, \wedge\alpha_{n,k_n})).$$

Therefore, it is enough to show that any formula of the form $\exists x(\alpha_1\wedge, \ldots, \wedge\alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are ground statements or negated ground statements, can be written equivalently without the existential quantifier. Then this process can be repeated for all the existential quantifiers. In the case that a quantifier is negated, it is necessary to restore the disjunctive normal form as described in the previous step.

We will thus show using induction over $n$ that the existential quantifier in $\exists x(\alpha_1\wedge, \ldots, \wedge\alpha_n)$ is equivalent to a quantifier-free conjunction of (possibly negated) ground statements. Since by Lemma 5.11 any negated congruence is equivalent to a disjunction of congruences, we can assume without loss of generality (by restoring the DNF) that no $\alpha_i$ is the negation of a congruence.

- Let $n = 1$. Then Lemma 5.16 implies that $\exists x\alpha_1$ is equivalent to a quantifier-free ground statement.
- We assume that the claim holds for some $n \geq 1$, let $\alpha_1, \ldots, \alpha_{n+1}$ be ground statements or negations of equations. We distinguish between the following three cases:
  - Suppose that $\alpha_1 \ldots, \alpha_{n+1}$ are all negated equations. Then $\exists x(\alpha_1 \wedge \cdots \wedge \alpha_n) \equiv (\mathbf{0} = \mathbf{0})$ by Lemma 5.20.1.
  - If there exists $i \in \{1, \ldots, n+1\}$ such that $\alpha_i$ is a congruence and $\alpha_j$ is a negated equation for all $j \neq i$, then by (C.1) we can assume that $i = 1$. Thus Lemma 5.20.2 implies that $\exists x(\alpha_1 \wedge \cdots \wedge \alpha_{n+1}) \equiv \alpha_1$.
  - We consider now the general case, i.e. there exists $i, j \in \{1, \ldots, n\}$ such that $\alpha_i$ is an equation or both $\alpha_i$ and $\alpha_j$ are congruences. By (C.1) we can assume that $i = n$ and $j = n + 1$. Then by Lemma 5.19 there exist ground statements (or negated equations) $\alpha'_n$ and $\alpha'_{n+1}$ such that $x \notin \mathrm{var}(\alpha'_{n+1})$. Therefore, we obtain

    $$\begin{aligned}\exists x(\alpha_1\wedge, \ldots, \wedge\alpha_n \wedge \alpha_{n+1}) &\equiv \exists x(\alpha_1\wedge, \ldots, \wedge\alpha_{n-1} \wedge \alpha'_n \wedge \alpha'_{n+1}) \\ &\equiv \exists x(\alpha_1\wedge, \ldots, \wedge\alpha_{n-1} \wedge \alpha'_n) \wedge \alpha'_{n+1}. \qquad \text{(N.4)}\end{aligned}$$

    By the induction hypothesis we know that $\exists x(\alpha_1\wedge, \ldots, \wedge\alpha_{n-1} \wedge \alpha'_n)$ is equivalent to a quantifier-free conjunction of ground statements, and hence so is $\exists x(\alpha_1\wedge, \ldots, \wedge\alpha_{n+1})$. This proves the induction step.

We can iterate this procedure until we obtain a quantifier-free disjunction of conjunctions of ground statements.

**Sixth Step: Decidability of closed $\mathcal{L}_{\text{Pres}}$-formulas**

Let now $\varphi$ be an arbitrary closed $\mathcal{L}_{\text{Pres}}$-formula. By the previous steps, we know that $\varphi \equiv \psi$ where $\psi$ is a quantifier-free closed formula in DNF where all formulas in the conjunctive clauses are equations, congruences or negations of equations. In particular, $\psi$ doesn't contain any variables.

Now we will show that for any $\mathcal{L}_{\text{Pres}}$-term $t$ with $\text{var}(t) = \emptyset$ there exists some $n \in \mathbb{N}$ such that $t \sim \underline{n}$. We prove this using induction on the construction of terms.

- If $t$ is $\mathbf{0}$, then $t = \mathbf{0} = \underline{0}$ by definition.
- If $t = \mathbf{S}t'$ where $t' \sim \underline{n}$ for some $n \in \mathbb{N}$, then $t' \sim \underline{n+1}$.
- If $t = t_1 + t_2$ where $t_1 \sim \underline{n_1}$ and $t_2 \sim \underline{n_2}$ for some $n_1, n_2 \in \mathbb{N}$, then $t \sim \underline{n_1 + n_2}$ by (N2).

Therefore, each ground statement or negated equation without variables is equivalent to one of the forms $\underline{m} = \underline{n}$, $\underline{m} \equiv_k \underline{n}$ ($k \geq 2$) or $\neg(\underline{m} = \underline{n})$. Such formulas are obviously decidable, and hence so are their conjunctions and disjunctions. In the case of the congruence, the decidability follows from the fact that we have $\vdash_{\text{Pres}} \underline{m} \equiv_k \underline{n} \Leftrightarrow m \equiv n \bmod k$ which is not hard to verify.

# Chapter 6

# Conclusions and Outlook

To sum up, this thesis contains a rigorous but still comprehensive proof of both Incompleteness Theorems. It has been shown that recursion theory is not necessary in order to achieve this. Nevertheless, the proofs presuppose the existence of the standard model $\mathbb{N}$ of Peano Arithmetic, or at least the existence of an infinite set of finite numbers in which addition and multiplication is possible and where one can use induction (we do not need to regard it as a model of Peano Arithmetic).

Furthermore, the contrast between the incomplete theory PA and the complete Presburger Arithmetic has been illustrated. In particular, this shows that it is impossible to define multiplication using addition and the successor function. The question that then arises is why one usually considers PA as the axiomatization of the natural numbers instead of Presburger Arithmetic, since Presburger Arithmetic actually allows the multiplication of standard natural numbers. As Mojżesz Presburger already points out in [Pre29], the main problem lies in the fact that in Presburger Arithmetic it is impossible to state a sentence concerning multiplication for all numbers, but only for one particular number; e.g. we can state the theorem

$$\vdash_{\text{Pres}} \forall x \forall y(\underline{n}(x+y) = \underline{n}x + \underline{n}y)$$

for every natural number $n \in \mathbb{N}$, but we cannot express this within Presburger Arithmetic, since there is no predicate that indicates that some number is a standard natural number.

As an idea for future projects, it would thus be interesting to analyze and compare nonstandard models of both theories.

# Bibliography


[Boo95] G.S. Boolos, *The logic of provability*, Cambridge University Press, 1995.

[GJ98] M. Goldstern and H. Judah, *The incompleteness phenomenon*, Peters, 1998.

[HA28] D. Hilbert and W. Ackermann, *Grundzüge der theoretischen Logik*, Berlin, Heidelberg (1928).

[Hal11] L.J. Halbeisen, *Combinatorial Set Theory: With a Gentle Introduction to Forcing*, Springer, 2011.

[Kay91] R. Kaye, *Models of Peano arithmetic*, Clarendon Press, 1991.

[Pre29] M. Presburger, *Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt*, Comptes Rendus du I congrès de Mathématiciens des Pays Slaves (1929), 92–101.

[Rau08] W. Rautenberg, *Einführung in die mathematische Logik: Ein Lehrbuch*, Vieweg+ Teubner Verlag, 2008.

[Ros36] Barkley Rosser, *Extensions of some theorems of Gödel and Church*, The Journal of Symbolic Logic **1** (1936), no. 3, 87–91.

[SB06] A.B. Slomson and J.L. Bell, *Models and ultraproducts: An introduction*, Dover Publications, 2006.

# Appendices

# Appendix A

# Logical Axioms

Numerous equivalent ways to axiomatize all universally valid formulas have been discovered. In the following we will show one particular set of logical axioms which are in fact axiom schemas. The choices of the set of logical axioms and the inference rules are interdependent. For the purpose of this work, we will use only two inference rules and eighteen schemas of logical axioms which can be encountered in [Hal11].

The inference rules that we will apply are:

**Modus Ponens (MP):** $\dfrac{\varphi \to \psi, \psi}{\varphi}$

**Generalization ($\forall$):** $\dfrac{\varphi}{\forall x \varphi}$.

For first-order formulas $\varphi, \varphi_1, \varphi_2$ and $\psi$ the following are schemas of logical axioms:

($L_1$) $\varphi \to (\psi \to \varphi)$

($L_2$) $(\psi \to (\varphi_1 \to \varphi_2)) \to ((\psi \to \varphi_1) \to (\psi \to \varphi_2))$

($L_3$) $(\varphi \wedge \psi) \to \varphi$

($L_4$) $(\varphi \wedge \psi) \to \psi$

($L_5$) $\psi \to (\varphi \to (\varphi \wedge \psi))$

($L_6$) $\varphi \to (\varphi \vee \psi)$

($L_7$) $\psi \to (\varphi \vee \psi)$

($L_8$) $(\varphi_1 \to \varphi_3) \to ((\varphi_2 \to \varphi_3) \to ((\varphi_1 \vee \varphi_2) \to \varphi_3))$

($L_9$) $(\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi)$

($L_{10}$) $\neg\varphi \to (\varphi \to \psi)$

($L_{11}$) $\varphi \vee \neg\varphi$.

For a formula $\varphi$ and a term $t$ such that the substitution $\varphi(x/t)$ is admissible, we have

($L_{12}$) $\forall x\varphi(x) \to \varphi(t)$

($L_{13}$) $\varphi(t) \to \exists x\varphi(x)$.

If $\psi$ is a formula and $t$ is a term with $t \notin \text{free}(\psi)$, then

($L_{14}$) $\forall x(\psi \to \varphi(x)) \to (\psi \to \forall x\varphi(x))$

($L_{15}$) $\forall x(\varphi(x) \to \psi) \to (\exists x\varphi(x) \to \psi)$.

Furthermore, for terms $t, t_1, \ldots, t_n, t'_1, \ldots, t'_n$, an $n$-ary relation symbol $R$ and an $n$-ary function symbol $F$, the following are logical axioms:

($L_{16}$) $t = t$

($L_{17}$) $(t_1 = t'_1 \wedge \cdots \wedge t_n = t'_n) \to (R(t_1, \ldots, t_n) \to R(t'_1, \ldots, t'_n))$

($L_{18}$) $(t_1 = t'_1 \wedge \cdots \wedge t_n = t'_n) \to (F(t_1, \ldots, t_n) = F(t'_1, \ldots, t'_n))$.

# Appendix B

# Tautologies and Methods of Proof

In the following, we will derive some methods of proof and tautologies from the system of logical axioms defined in the last section. All of them constitute useful tools for handling formal proofs based on these logical axioms as well as non-logical axioms such as Peano Arithmetic.

## B.1 Methods of Proof

**Lemma B.1.** *Let $\varphi$ be a formula. Then $\vdash \varphi \to \varphi$ holds.*

*Proof.*

$\vdash \varphi \vee \neg\varphi$ ($L_{11}$)
$\vdash (\varphi \to (\varphi \to \varphi)) \to ((\neg\varphi \to (\varphi \to \varphi)) \to ((\varphi \vee \neg\varphi) \to (\varphi \to \varphi)))$ ($L_8$)
$\vdash \varphi \to (\varphi \to \varphi)$ ($L_1$)
$\vdash (\neg\varphi \to (\varphi \to \varphi)) \to ((\varphi \vee \neg\varphi) \to (\varphi \to \varphi))$ (MP)
$\vdash \neg\varphi \to (\varphi \to \varphi)$ ($L_{10}$)
$\vdash (\varphi \vee \neg\varphi) \to (\varphi \to \varphi)$ (MP)
$\vdash \varphi \to \varphi.$ (MP)

$\dashv$

**Proposition B.2.** *Let $T$ be a set of formulas, and $\varphi, \psi$ any two formulas. Then*

$$(\wedge) \quad T \vdash \varphi \text{ and } T \vdash \psi \quad \Leftrightarrow \quad T \vdash \varphi \wedge \psi$$

*holds. In particular, we have*

$$(\leftrightarrow) \quad T \vdash \varphi \to \psi \text{ and } T \vdash \psi \to \varphi \quad \Leftrightarrow \quad T \vdash \varphi \leftrightarrow \psi.$$

*Proof.* "⇒": We assume $T \vdash \varphi$ and $T \vdash \psi$.

$$\begin{aligned} T &\vdash_{\mathrm{PA}} \psi \to (\varphi \to (\varphi \wedge \psi)) && (\mathrm{L}_5)\\ &\vdash_{\mathrm{PA}} \psi \\ &\vdash_{\mathrm{PA}} \varphi \to (\varphi \wedge \psi) && (\mathrm{MP})\\ &\vdash_{\mathrm{PA}} \varphi \\ &\vdash_{\mathrm{PA}} \varphi \wedge \psi. && (\mathrm{MP}) \end{aligned}$$

"⇐": We assume $T \vdash \varphi \wedge \psi$. Then we have

$$\begin{aligned} T &\vdash \varphi \wedge \psi \\ &\vdash (\varphi \wedge \psi) \to \varphi && (\mathrm{L}_3)\\ &\vdash \varphi && (\mathrm{MP}) \end{aligned}$$

and similarly one shows $T \vdash \psi$ using $(\mathrm{L}_4)$ instead of $(\mathrm{L}_3)$.

⊣

**Proposition B.3** (Deduction Theorem)**.** *Let $T$ be a set of formulas, $\varphi$ and $\psi$ any formulas. Then the equivalence*

$$(\mathrm{DT}) \quad T \cup \{\psi\} \vdash \varphi \quad \Leftrightarrow \quad T \vdash \psi \to \varphi$$

*holds, if in the proof of $\varphi$ from $T \cup \{\psi\}$ the generalization rule $(\forall)$ is not applied to any of the free variables of $\psi$.*

*Proof.* It is clear that $T \vdash \psi \to \varphi$ implies $T \cup \{\psi\} \vdash \varphi$. For the other direction, suppose that $T \cup \{\psi\} \vdash \varphi$ holds and let the sequence $\varphi_0, \ldots, \varphi_n$ with $\varphi_n = \varphi$ be a formal proof for $\varphi$ in $T \cup \{\psi\}$. For each $i \leq n$ we will exchange the formula $\varphi_i$ for a sequence of formulas which ends with $\psi \to \varphi_i$. We will prove this inductively by the construction of the formula $\psi$. Let $i \leq n$.

- If $\varphi_i$ is a logical axiom or $\varphi_i \in T$, we have

$$\begin{aligned} T &\vdash \varphi_i \\ &\vdash \varphi_i \to (\psi \to \varphi_i) && (\mathrm{L}_1)\\ &\vdash \psi \to \varphi_i. && (\mathrm{MP}) \end{aligned}$$

- The case $\varphi_i = \psi$ follows directly from Lemma B.1.

- If $\varphi_i$ is obtained by (MP) from $\varphi_j$ and $\varphi_k = (\varphi_j \to \varphi_i)$ with $j < k < i$, we have

$$\begin{aligned} T &\vdash \psi \to \varphi_j && (\text{since } j < i)\\ &\vdash \psi \to (\varphi_j \to \varphi_i) && (\text{since } k < i)\\ &\vdash (\psi \to (\varphi_j \to \varphi_i)) \to ((\psi \to \varphi_j) \to (\psi \to \varphi_i)) && (\mathrm{L}_2)\\ &\vdash (\psi \to \varphi_j) \to (\psi \to \varphi_i) && (\mathrm{MP})\\ &\vdash \psi \to \varphi_i. && (\mathrm{MP}) \end{aligned}$$

- If $\varphi_i$ is $\forall x \varphi_j$ with $j < i$ and $x \notin \text{free}(\psi)$, the claim follows from

$$\begin{aligned} T &\vdash \psi \to \varphi_j && \text{(since } j < i\text{)} \\ &\vdash \forall x(\psi \to \varphi_j) && (\forall) \\ &\vdash \forall x(\psi \to \varphi_j) \to (\psi \to \varphi_i) && (\mathrm{L}_{14}) \\ &\vdash \psi \to \varphi_i. && (\mathrm{MP}) \end{aligned}$$

⊣

**Corollary B.4** (Generalized Deduction Theorem)**.** *Let $T$ be a set of formulas and $\varphi$ and $\psi_1, \ldots, \psi_n$ formulas. Then we have*

$$T \cup \{\psi_1, \ldots, \psi_n\} \vdash \varphi \quad \Leftrightarrow \quad T \vdash \psi_1 \wedge \cdots \wedge \psi_n \to \varphi,$$

*if in the proof of $\varphi$ from $T \cup \{\psi_1, \ldots, \psi_n\}$ the generalization rule $(\forall)$ is not applied to any of the free variables of $\psi_1, \ldots, \psi_n$.*

Note that the formula $\psi_1 \wedge \cdots \wedge \psi_n$ is well-defined because of the tautology (C.2) which will be shown in Theorem B.16.

*Proof.* As in the last theorem, it is clear that $T \cup \{\psi_1 \wedge \cdots \wedge \psi_n\} \vdash \varphi$ implies $T \vdash \psi_1 \wedge \cdots \wedge \psi_n$ (using $(\wedge)$ $n$ times). We use induction over $n$ in order to prove the other direction. For $n = 1$ the statement is (DT) and therefore satisfied. In order to prove the induction step, we assume that it holds for some $n \geq 1$ and that $T \cup \{\psi_1, \ldots, \psi_n, \psi_{n+1}\} \vdash \varphi$. Thus by (DT) we obtain $T \cup \{\psi_1, \ldots, \psi_n\} \vdash \psi_{n+1} \to \varphi$ and by the induction hypothesis we obtain

$$\begin{aligned} & T \vdash (\psi_1 \wedge \cdots \wedge \psi_n) \to (\psi_{n+1} \to \varphi) \\ T \cup \{\psi_1 \wedge \ldots \psi_n \wedge \psi_{n+1}\} &\vdash \psi_1 \wedge \cdots \wedge \psi_n && (\wedge) \\ &\vdash \psi_{n+1} \to \varphi && (\mathrm{MP}) \\ &\vdash \psi_{n+1} && (\wedge) \\ &\vdash \varphi. && (\mathrm{MP}) \end{aligned}$$

The claim follows then from (DT). ⊣

**Proposition B.5.** *Let $T$ be a set of formulas and $\varphi$ be any formula. Let $\bot := \alpha \wedge \neg\alpha$ for an arbitrary formula $\alpha$. Then we have*

$$(\bot) \quad T \vdash \bot \quad \Rightarrow \quad T \vdash \varphi.$$

*In particular, the definition of $\bot$ does not depend on the choice of $\alpha$.*

*Proof.* We assume that $T \vdash \alpha \wedge \neg\alpha$ holds. Then

$$
\begin{aligned}
&T \vdash \alpha \wedge \neg\alpha \\
&\quad \vdash \alpha && (\wedge)\\
&\quad \vdash \neg\alpha && (\wedge)\\
&\quad \vdash \neg\alpha \to (\alpha \to \varphi) && (\mathrm{L}_{10})\\
&\quad \vdash \alpha \to \varphi && (\mathrm{MP})\\
&\quad \vdash \varphi. && (\mathrm{MP})
\end{aligned}
$$

$\dashv$

**Proposition B.6** (Proof by Cases)**.** *Let $T$ be a set of formulas and $\varphi$,$\psi$ and $\alpha$ formulas. Then the following statements hold:*

($\vee$1) *$T \vdash \varphi \vee \psi$ and $T \cup \{\varphi\} \vdash \alpha$ and $T \cup \{\psi\} \vdash \alpha \Rightarrow T \vdash \alpha$, where ($\forall$) is not applied to any of the free variables of $\varphi$ or $\psi$ in the proof of $\alpha$ from $T \cup \{\varphi\}$ respectively $T \cup \{\psi\}$,*

($\vee$2) *$T \cup \{\varphi\} \vdash \psi$ and $T \cup \{\neg\varphi\} \vdash \psi \Rightarrow T \vdash \psi$, where ($\forall$) is not applied to any of the free variables of $\varphi$ in the proof of $\psi$ from $T \cup \{\varphi\}$ respectively $T \cup \{\neg\varphi\}$,*

($\vee$3) *$T \vdash \varphi \vee \psi \Rightarrow T \cup \{\neg\varphi\} \vdash \psi$,*

($\vee$4) *$T \vdash \varphi \vee \psi$ and $T \cup \{\varphi\} \vdash \bot \Rightarrow T \vdash \psi$.*

*Proof.*

($\vee$1) We assume $T \vdash \varphi \vee \psi$.

$$
\begin{aligned}
&T \vdash \varphi \to \alpha && (\mathrm{DT})\\
&\quad \vdash \psi \to \alpha && (\mathrm{DT})\\
&\quad \vdash (\varphi \to \alpha) \to ((\psi \to \alpha) \to ((\varphi \vee \psi) \to \alpha)) && (\mathrm{L}_8)\\
&\quad \vdash (\psi \to \alpha) \to ((\varphi \vee \psi) \to \alpha) && (\mathrm{MP})\\
&\quad \vdash (\varphi \vee \psi) \to \alpha && (\mathrm{MP})\\
&\quad \vdash \varphi \vee \psi && (\text{Assumption})\\
&\quad \vdash \alpha. && (\mathrm{MP})
\end{aligned}
$$

($\vee$2) Is a special case of ($\vee$1), since $T \vdash \varphi \vee \neg\varphi$ holds by ($\mathrm{L}_4$).

($\vee$3) We assume $T \vdash \varphi \vee \psi$.

$$\begin{aligned}
T \cup \{\neg\varphi\} &\vdash \varphi \vee \psi \\
&\vdash \neg\varphi \\
&\vdash (\varphi \to \psi) \to ((\psi \to \psi) \to ((\varphi \vee \psi) \to \psi)) && (L_8) \\
&\vdash \neg\varphi \to (\varphi \to \psi) && (L_{10}) \\
&\vdash \varphi \to \psi && (MP) \\
&\vdash (\psi \to \psi) \to ((\varphi \vee \psi) \to \psi) && (MP) \\
&\vdash (\varphi \vee \psi) \to \psi && (MP) \\
&\vdash \psi. && (MP)
\end{aligned}$$

($\vee$4) By ($\vee$2) it is enough to verify $T \cup \{\varphi\} \vdash \psi$ and $T \cup \{\neg\varphi\} \vdash \psi$. The first statement follows directly from ($\bot$)and the second one from ($\vee$3).

$\dashv$

**Corollary B.7** (Generalized Proof by Cases)**.** *Let $T$ be a set of formulas, and $\psi_1, \ldots, \psi_n$, $\varphi$ formulas. Then*

$$T \vdash \psi_1 \vee \cdots \vee \psi_n \text{ and } T \cup \{\psi_i\} \vdash \varphi \text{ for all } i \in \{1 \ldots n\} \Rightarrow T \vdash \varphi,$$

*where ($\forall$) is not applied to any of the free variables of $\psi_i$ in the proof of $\varphi$ from $T \cup \{\psi_i\}$.*

Since Corollary B.7 is a generalization of ($\vee$1), we will also denote all instance of this form by ($\vee$1). Note that the formula $\psi_1 \vee \cdots \vee \psi_n$ is well-defined due to (D.2) which will be shown in Theorem B.16.

*Proof.* We show the statement using induction over $n$. For $n = 2$ it is exactly ($\vee$1) and is therefore satisfied. We assume that $n \geq 2$ and $T \vdash \psi_1 \vee \cdots \vee \psi_n \vee \psi_{n+1}$ as well as $T \cup \{\psi_i\} \vdash \varphi$ for all $i \in \{1, \ldots, n, n+1\}$. By the induction hypothesis we can deduce $T \cup \{\psi_1 \vee \cdots \vee \psi_n\} \vdash \varphi$ and thus due to ($\vee$1) by considering $\psi_1 \vee \cdots \vee \psi_n$ and $\psi_{n+1}$ the result $T \vdash \varphi$ follows. $\dashv$

**Proposition B.8** (Contrapositon)**.** *Let $T$ be a set of formulas, and $\varphi$ and $\psi$ two arbitrary formulas. Then we have*

$$\text{(CP)} \quad T \cup \{\neg\psi\} \vdash \neg\varphi \quad \Rightarrow \quad T \cup \{\varphi\} \vdash \psi.$$

*Proof.* By ($\vee$2) it suffices to show $T \cup \{\varphi, \psi\} \vdash \psi$ and $T \cup \{\varphi, \neg\psi\} \vdash \psi$. The first statement is obvious and the second one is a consequence of

$$\begin{aligned}
T \cup \{\varphi, \neg\psi\} &\vdash \neg\varphi \\
&\vdash \varphi \\
&\vdash \bot && (\wedge) \\
&\vdash \psi. && (\bot)
\end{aligned}$$

$\dashv$

**Proposition B.9** (Proof by Contradiction)**.** *Let $T$ be a set of formulas, and $\varphi$ be an arbitrary formula. Then the statements*

$$(\lightning) \quad T \cup \{\neg\varphi\} \vdash \bot \quad \Rightarrow \quad T \vdash \varphi, \text{ respectively}$$

$$T \cup \{\varphi\} \vdash \bot \quad \Rightarrow \quad T \vdash \neg\varphi$$

*hold, where $\bot := \alpha \wedge \neg\alpha$ for any formula $\alpha$.*

*Proof.* We consider only the first statement, since both proofs are similar. By ($\vee$2) it is enough to verify $T \cup \{\varphi\} \vdash \varphi$ and $T \cup \{\neg\varphi\} \vdash \varphi$. The first condition is clearly satisfied and the second one follows directly from ($\wedge$) and ($\bot$). ⊣

**Proposition B.10** ($\exists$−Introduction)**.** *Let $T$ be a set of formulas, $\varphi(x)$ a formula with $x \in \text{free}(\varphi)$ and $\psi$ an arbitary formula. Then:*

$$(\exists) \quad T \cup \{\varphi(x)\} \vdash \psi \quad \Rightarrow \quad T \cup \{\exists x\varphi(x)\} \vdash \psi.$$

*Proof.* We will use (DT) twice:

$$\begin{aligned}
&T \vdash \varphi(x) \to \psi && \text{(DT)}\\
&\vdash \forall x(\varphi(x) \to \psi) && (\forall)\\
&\vdash \forall x(\varphi(x) \to \psi) \to (\exists x\varphi(x) \to \psi) && (\text{L}_{15})\\
&\vdash \exists x\varphi(x) \to \psi. && \text{(MP)}
\end{aligned}$$

⊣

## B.2 Tautologies

**Lemma B.11.** *Let $\varphi_1, \varphi_2$ and $\varphi_3$ be formulas. Then we have $\{\varphi_1 \to \varphi_2, \varphi_2 \to \varphi_3\} \vdash \varphi_1 \to \varphi_3$.*

*Proof.* The claim follows from

$$\begin{aligned}
\{\varphi_1 \to \varphi_2, \varphi_2 \to \varphi_3, \varphi_1\} &\vdash \varphi_1 \to \varphi_2\\
&\vdash \varphi_1\\
&\vdash \varphi_2 && \text{(MP)}\\
&\vdash \varphi_2 \to \varphi_3\\
&\vdash \varphi_3 && \text{(MP)}
\end{aligned}$$

using (DT). ⊣

**Lemma B.12.** *Let $T$ be a set of formulas and $\varphi, \psi$ and $\chi$ be formulas. Then the following statements hold:*

1. $T \vdash \varphi \leftrightarrow \varphi$,

2. $T \vdash \varphi \leftrightarrow \psi \Rightarrow T \vdash \psi \leftrightarrow \varphi$,

3. $T \vdash \varphi \leftrightarrow \psi$ *and* $T \vdash \psi \leftrightarrow \chi \Rightarrow T \vdash \varphi \leftrightarrow \chi$.

*Proof.*

1. Follows directly from Lemma B.1 and $(\leftrightarrow)$.

2. The second assertion is a consequence of using $(\leftrightarrow)$ three times.

3. Due to $(\leftrightarrow)$ it is sufficient to prove $T \vdash \varphi \to \chi$ and $T \vdash \chi \to \varphi$.

$$\begin{aligned} & T \vdash \varphi \leftrightarrow \psi \\ & \quad \vdash \varphi \to \psi && (\leftrightarrow) \\ & \quad \vdash \psi \leftrightarrow \chi \\ & \quad \vdash \psi \to \chi && (\leftrightarrow) \\ & \quad \vdash \varphi \to \chi. && \text{(B.11)} \end{aligned}$$

Similarly, one shows $T \vdash \chi \to \varphi$.

⊣

**Definition B.13.** For any set $T$ of formulas and for any two formulas $\varphi$ and $\psi$ we write $\varphi \equiv_T \psi$ instead of $T \vdash \varphi \leftrightarrow \psi$. For $T = \emptyset$ we write $\equiv$ for $\equiv_\emptyset$. Lemma B.12 states that $\equiv_T$ is an equivalence relation.

**Lemma B.14.** *Let $\varphi, \varphi_1, \varphi_2, \psi, \psi_1$ and $\psi_2$ be formulas. Then we have the equivalences*

1. $\vdash (\varphi \leftrightarrow \psi) \leftrightarrow (\neg\varphi \leftrightarrow \neg\psi)$,

2. $\{\varphi_1 \leftrightarrow \varphi_2, \psi_1 \leftrightarrow \psi_2\} \vdash (\varphi_1 \to \psi_1) \leftrightarrow (\varphi_2 \to \psi_2)$,

3. $\{\varphi_1 \leftrightarrow \varphi_2, \psi_1 \leftrightarrow \psi_2\} \vdash (\varphi_1 \wedge \psi_1) \leftrightarrow (\varphi_1 \wedge \psi_2)$,

4. $\{\varphi_1 \leftrightarrow \varphi_2, \psi_1 \leftrightarrow \psi_2\} \vdash (\varphi_1 \vee \psi_1) \leftrightarrow (\varphi_1 \vee \psi_2)$,

5. $\{\varphi \leftrightarrow \psi\} \vdash \forall x\varphi \leftrightarrow \forall x\psi$,

6. $\{\varphi \leftrightarrow \psi\} \vdash \exists x\varphi \leftrightarrow \exists x\psi$.

*Proof.*

1. Will be shown in Theorem B.16 denoted by (B.2).

2. By $(\leftrightarrow)$ it is enough to prove $\{\varphi_1 \leftrightarrow \varphi_2, \psi_1 \leftrightarrow \psi_2\} \vdash (\varphi_1 \to \psi_1) \to (\varphi_2 \to \psi_2)$ and $\{\varphi_1 \leftrightarrow \varphi_2, \psi_1 \leftrightarrow \psi_2\} \vdash (\varphi_2 \to \psi_2) \to (\varphi_1 \to \psi_1)$. Since both statements have

similar proofs, we neglect the second one.

$$\begin{aligned}
\{\varphi_1 \leftrightarrow \varphi_2, \psi_1 \leftrightarrow \psi_2, \varphi_1 \to \psi_1, \varphi_2\} &\vdash \varphi_1 \leftrightarrow \varphi_2 \\
&\vdash \varphi_2 \to \varphi_1 && (\leftrightarrow) \\
&\vdash \varphi_2 \\
&\vdash \varphi_1 && (\mathrm{MP}) \\
&\vdash \varphi_1 \to \psi_1 \\
&\vdash \psi_1 && (\mathrm{MP}) \\
&\vdash \psi_1 \leftrightarrow \psi_2 \\
&\vdash \psi_1 \to \psi_2 && (\leftrightarrow) \\
&\vdash \psi_2.
\end{aligned}$$

3. The second assertion can be shown in a similar way using $(\wedge)$ various times.

4. Again, due to $(\leftrightarrow)$ and symmetry, it suffices to prove one direction.

$$\begin{aligned}
\{\varphi_1 \leftrightarrow \varphi_2, \psi_1 \leftrightarrow \psi_2, \varphi_1 \to \psi_1, \varphi_1 \vee \psi_1, \varphi_1\} &\vdash \varphi_1 \leftrightarrow \varphi_2 \\
&\vdash \varphi_1 \to \varphi_2 && (\leftrightarrow) \\
&\vdash \varphi_1 \\
&\vdash \varphi_2 && (\mathrm{MP}) \\
&\vdash \varphi_2 \to (\varphi_2 \vee \psi_2) && (\mathrm{L}_6) \\
&\vdash \varphi_2 \vee \psi_2. && (\mathrm{MP})
\end{aligned}$$

Similarly, one shows $\{\varphi_1 \leftrightarrow \varphi_2, \psi_1 \leftrightarrow \psi_2, \varphi_1 \to \psi_1, \varphi_1 \vee \psi_1, \psi_1\} \vdash \varphi_1 \vee \psi_2$. The claim is thus a consequence of $(\vee 1)$ and (DT).

5. Using $(\leftrightarrow)$ and (DT) it is sufficient to verify $\{\varphi \leftrightarrow \psi, \forall x\varphi\} \vdash \forall x\psi$ as well as $\{\varphi \leftrightarrow \psi, \forall x\psi\} \vdash \forall x\varphi$. By symmetry, we only show the first condition.

$$\begin{aligned}
\{\varphi \leftrightarrow \psi, \forall x\varphi\} &\vdash \forall x\varphi \\
&\vdash \forall x\varphi \to \varphi && (\mathrm{L}_{12}) \\
&\vdash \varphi && (\mathrm{MP}) \\
&\vdash \varphi \leftrightarrow \psi \\
&\vdash \varphi \to \psi && (\leftrightarrow) \\
&\vdash \psi && (\mathrm{MP}) \\
&\vdash \forall x\psi. && (\forall)
\end{aligned}$$

6. Once more, we only show the first direction.

$$\begin{aligned}
\{\varphi \leftrightarrow \psi, \varphi\} &\vdash \varphi \leftrightarrow \psi \\
&\vdash \varphi \rightarrow \psi && (\leftrightarrow) \\
&\vdash \varphi \\
&\vdash \psi && (\mathrm{MP}) \\
&\vdash \psi \rightarrow \exists x \psi && (\mathrm{L}_{13}) \\
&\vdash \exists x \psi. && (\mathrm{MP})
\end{aligned}$$

Then (∃) implies $\{\varphi \leftrightarrow \psi, \exists x \varphi\} \vdash \exists x \psi$ and the claim follows from (DT).

⊣

**Theorem B.15** (Substitution Theorem (ST))**.** *Let $T$ be a set of formulas, and let $\varphi, \psi, \alpha$ three arbitrary formulas. Let $\beta$ be the formula obtained from $\alpha$ by replacing one or multiple occurences of $\varphi$ by $\psi$. Then we have*

$$\varphi \equiv_T \psi \quad \Longrightarrow \quad \alpha \equiv_T \beta.$$

*Proof.* We prove the theorem by induction on the recursive construction of the formula $\alpha$.

- The cases that $\alpha = \varphi$ or $\varphi$ does not appear in $\alpha$ are trivial.
- If $\alpha = \neg\alpha'$ and $T \vdash \alpha' \leftrightarrow \beta'$, where $\beta = \neg\beta'$, we have

$$\begin{aligned}
T &\vdash \alpha' \leftrightarrow \beta' \\
&\vdash (\alpha \leftrightarrow \beta) \leftrightarrow (\neg\alpha' \leftrightarrow \neg\beta') && (\text{B.14.1}) \\
&\vdash \neg\alpha' \leftrightarrow \neg\beta' && (\leftrightarrow) \\
&\vdash \alpha \leftrightarrow \beta.
\end{aligned}$$

- If $\alpha = \alpha' \rightarrow \alpha''$ and $T \vdash \alpha' \leftrightarrow \beta'$ and $T \vdash \alpha'' \leftrightarrow \beta''$, where $\beta = \beta' \rightarrow \beta''$, then (B.14.2) implies that $T \vdash \alpha \leftrightarrow \beta$. The cases $\alpha = \alpha' \wedge \alpha''$ respectively $\alpha = \alpha' \vee \alpha''$ follow similarly using (B.14.3) and (B.14.4).
- Last but not least, suppose that $\alpha = \forall x \alpha'$, where $T \vdash \alpha' \leftrightarrow \beta'$ and $\beta = \forall x \beta'$. Again, the result can be derived directly using a tautology, in this case (B.14.5). The case $\alpha = \exists x \alpha'$ follows from (B.14.6).

⊣

**Theorem B.16** (Tautologies)**.** *Let $\varphi, \varphi_1, \varphi_2, \varphi_3$ and $\psi$ be formulas. Then the following equivalences hold:*

(A) $\varphi \equiv \neg\neg\varphi$

(B.1) $\varphi \to \psi \equiv \neg\psi \to \neg\varphi$

(B.2) $\varphi \leftrightarrow \psi \equiv \neg\varphi \leftrightarrow \neg\psi$

(C.1) $\varphi_1 \wedge \varphi_2 \equiv \varphi_2 \wedge \varphi_1$

(C.2) $(\varphi_1 \wedge \varphi_2) \wedge \varphi_3 \equiv \varphi_1 \wedge (\varphi_2 \wedge \varphi_3)$

(D.1) $\varphi_1 \vee \varphi_2 \equiv \varphi_2 \vee \varphi_1$

(D.2) $(\varphi_1 \vee \varphi_2) \vee \varphi_3 \equiv \varphi_1 \vee (\varphi_2 \vee \varphi_3)$

(E) $\varphi \to \psi \equiv \neg\varphi \vee \psi$

(F.1) $\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$

(F.2) $\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$

(G) $\varphi_1 \to (\varphi_1 \to \varphi_3) \equiv (\varphi_1 \wedge \varphi_2) \to \varphi_3$

(H.1) $(\varphi_1 \to \varphi_2) \wedge (\varphi_1 \to \varphi_3) \equiv \varphi_1 \to (\varphi_2 \wedge \varphi_3)$

(H.2) $(\varphi_1 \to \varphi_3) \wedge (\varphi_2 \to \varphi_3) \equiv (\varphi_1 \vee \varphi_2) \to \varphi_3$

(I.1) $(\varphi_1 \wedge \varphi_2) \vee \varphi_3 \equiv (\varphi_1 \vee \varphi_3) \wedge (\varphi_2 \vee \varphi_3)$

(I.2) $(\varphi_1 \vee \varphi_2) \wedge \varphi_3 \equiv (\varphi_1 \wedge \varphi_3) \vee (\varphi_2 \wedge \varphi_3)$

(K.1) $\exists x\varphi \equiv \neg\forall x\neg\varphi$

(K.2) $\forall x\varphi \equiv \neg\exists x\neg\varphi$

(L.1) $\varphi(x) \equiv \varphi(y)$, *if $y$ does not appear in $\varphi(x)$*

(L.2) $\exists x\varphi(x) \equiv \exists y\varphi(y)$, *if $y$ does not appear in $\varphi(x)$*

(L.3) $\forall x\varphi(x) \equiv \forall y\varphi(y)$, *if $y$ does not appear in $\varphi(x)$*

(M.1) $\exists x\exists y\varphi \equiv \exists y\exists x\varphi$

(M.2) $\exists x\exists x\varphi \equiv \exists x\varphi$

(N.1) $\exists x\varphi \wedge \exists y\psi \equiv \exists x\exists y(\varphi \wedge \psi)$, $x \notin \text{free}(\psi), y \notin \text{free}(\varphi)$

(N.2) $\forall x\varphi \wedge \forall y\psi \equiv \forall x\forall y(\varphi \wedge \psi)$, $x \notin \text{free}(\psi), y \notin \text{free}(\varphi)$

(N.3) $\exists x\varphi \wedge \forall y\psi \equiv \exists x\forall y(\varphi \wedge \psi),\ x \notin \text{free}(\psi), y \notin \text{free}(\varphi)$

(N.4) $\exists x\varphi \wedge \psi \equiv \exists x(\varphi \wedge \psi),\ x \notin \text{free}(\psi)$

(N.5) $\forall x\varphi \wedge \psi \equiv \forall x(\varphi \wedge \psi),\ x \notin \text{free}(\psi)$

(O.1) $\exists x\varphi \vee \exists y\psi \equiv \exists x\exists y(\varphi \vee \psi),\ x \notin \text{free}(\psi), y \notin \text{free}(\varphi)$

(O.2) $\forall x\varphi \vee \forall y\psi \equiv \forall x\forall y(\varphi \vee \psi),\ x \notin \text{free}(\psi), y \notin \text{free}(\varphi)$

(O.3) $\exists x\varphi \vee \forall y\psi \equiv \exists x\forall y(\varphi \vee \psi),\ x \notin \text{free}(\psi), y \notin \text{free}(\varphi)$

(O.4) $\exists x\varphi \vee \psi \equiv \exists x(\varphi \vee \psi),\ x \notin \text{free}(\psi)$

(O.5) $\forall x\varphi \vee \psi \equiv \forall x(\varphi \vee \psi),\ x \notin \text{free}(\psi)$.

*Proof.*

(A) The first direction ($\vdash \varphi \to \neg\neg\varphi$) follows using (DT) from $\{\varphi\} \vdash \neg\neg\varphi$ which is a consequence of ($\vee 4$) due to $\{\varphi\} \vdash \neg\varphi \vee \neg\neg\varphi$ (by ($L_{11}$)) and $\{\varphi, \neg\varphi\} \vdash \bot$. For the second direction we clearly have $\{\neg\neg\varphi, \varphi\} \vdash \varphi$ and by ($\bot$) also $\{\neg\neg\varphi, \neg\varphi\} \vdash \varphi$ and thus we can apply ($\vee 2$) to conclude $\{\neg\neg\varphi\} \vdash \varphi$. (DT) implies the claim.

(B.1) By ($\leftrightarrow$) and (DT) we need to show $\{\varphi \to \psi\} \vdash \neg\psi \to \neg\varphi$ and $\{\neg\psi \to \neg\varphi\} \vdash \varphi \to \psi$. These two conditions follow from

$$\begin{aligned}
\{\varphi \to \psi, \neg\psi\} &\vdash \varphi \to \psi \\
&\vdash (\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi) && (L_9)\\
&\vdash (\varphi \to \neg\psi) \to \neg\varphi && (MP)\\
&\vdash \neg\psi \\
&\vdash \neg\psi \to (\varphi \to \neg\psi) && (L_1)\\
&\vdash \varphi \to \neg\psi && (MP)\\
&\vdash \neg\varphi && (MP)
\end{aligned}$$

and

$$\begin{aligned}
\{\neg\psi \to \neg\varphi, \neg\psi\} &\vdash \neg\psi \\
&\vdash \neg\psi \to \neg\varphi \\
&\vdash \neg\varphi && (MP)\\
\{\neg\psi \to \neg\varphi, \varphi\} &\vdash \psi && (CP)
\end{aligned}$$

using (DT).

(B.2) Follows from (B.1) with multiple applications of ($\leftrightarrow$).

(C.1) (and (C.2)) Both proofs are straightforward consequences of ($\wedge$).

(D.1) By ($\wedge$) and (DT) it is enough to prove $\{\varphi_1 \vee \varphi_2\} \vdash \varphi_2 \vee \varphi_1$ and $\{\varphi_2 \vee \varphi_1\} \vdash \varphi_1 \vee \varphi_2$. By symmetry it is sufficient to verify the first assertion. We obviously have

$\{\varphi_1 \vee \varphi_2, \varphi_1\} \vdash \varphi_2 \vee \varphi_1$ by ($L_7$) and similarly (using ($L_6$)) $\{\varphi_1 \vee \varphi_2, \varphi_2\} \vdash \varphi_2 \vee \varphi_1$. Hence the claim follows from ($\vee$1).

(D.2) Again, we only consider the first direction.

$$\begin{aligned}
\{(\varphi_1 \vee \varphi_2) \vee \varphi_3, \varphi_1 \vee \varphi_2, \varphi_1\} &\vdash \varphi_1 \\
&\vdash \varphi_1 \to \varphi_1 \vee (\varphi_2 \vee \varphi_3) && (L_6)\\
&\vdash \varphi_1 \vee (\varphi_2 \vee \varphi_3) && (MP)\\
\{(\varphi_1 \vee \varphi_2) \vee \varphi_3, \varphi_1 \vee \varphi_2, \varphi_2\} &\vdash \varphi_2 \\
&\vdash \varphi_2 \to \varphi_2 \vee \varphi_3 && (L_6)\\
&\vdash \varphi_2 \vee \varphi_3 && (MP)\\
&\vdash \varphi_2 \vee \varphi_3 \to \varphi_1 \vee (\varphi_2 \vee \varphi_3) && (L_7)\\
&\vdash \varphi_1 \vee (\varphi_2 \vee \varphi_3) && (MP)\\
\{(\varphi_1 \vee \varphi_2) \vee \varphi_3, \varphi_1 \vee \varphi_2\} &\vdash \varphi_1 \vee (\varphi_2 \vee \varphi_3) && (\vee 1)\\
\{(\varphi_1 \vee \varphi_2) \vee \varphi_3, \varphi_3\} &\vdash \varphi_1 \vee (\varphi_2 \vee \varphi_3). && (\text{similarly})
\end{aligned}$$

Thus, again using ($\vee$1) we obtain as desired $\{(\varphi_1 \vee \varphi_2) \vee \varphi_3\} \vdash \varphi_1 \vee (\varphi_2 \vee \varphi_3)$.

(E) For the first direction we note

$$\begin{aligned}
\{\neg\psi \to \neg\varphi, \neg\psi\} &\vdash \neg\psi \to \neg\varphi \\
&\vdash \neg\varphi \to (\neg\varphi \vee \neg\psi) && (L_6)\\
&\vdash \neg\psi \to (\neg\varphi \vee \neg\psi) && (B.11)\\
&\vdash \neg\psi \\
&\vdash \neg\varphi \vee \psi && (MP)
\end{aligned}$$

and by ($L_7$) we have $\{\neg\psi \to \neg\varphi, \psi\} \vdash \neg\varphi \vee \psi$ and thus ($\vee$2) implies $\{\neg\psi \to \neg\varphi\} \vdash \neg\varphi \vee \psi$. The first direction is a consequence of (B.1). For the second direction we clearly have $\{\neg\varphi \vee \psi, \varphi, \neg\varphi\} \vdash \psi$ by ($\perp$) and $\{\neg\varphi \vee \psi, \varphi, \psi\} \vdash \psi$ which leads to $\{\neg\varphi \vee \psi, \varphi\} \vdash \psi$ by ($\vee$1). We get the equivalence by applying (DT).

(F.1) Firstly, we note that by (E) $\neg\varphi \vee \neg\psi \equiv \varphi \to \neg\psi$. The first direction follows from

$$\begin{aligned}
\{\neg(\varphi \wedge \psi), \varphi, \psi\} &\vdash \varphi \wedge \psi && (\wedge)\\
&\vdash \neg(\varphi \wedge \psi) \\
&\vdash \perp && (\wedge)\\
\{\neg(\varphi \wedge \psi), \varphi\} &\vdash \neg\psi && (\vee 4)
\end{aligned}$$

and (DT). The second direction is a consequence of

$$\begin{aligned}
\{\varphi \to \neg\psi, \varphi \wedge \psi\} &\varphi \wedge \psi \\
&\vdash \varphi && (\wedge)\\
&\vdash \psi && (\wedge)\\
&\vdash \varphi \to \neg\psi \\
&\vdash \neg\psi && (MP)\\
&\vdash \perp && (\wedge)
\end{aligned}$$

and ($\lightning$).

(F.2) We use the substitution theorem and previous tautologies to obtain $\neg(\varphi_1 \vee \varphi_2) \overset{(A)}{\equiv} \neg(\neg\neg\varphi \vee \neg\neg\psi) \overset{(F.1)}{\equiv} \neg(\neg(\neg\varphi \wedge \neg\psi)) \overset{(A)}{\equiv} \neg\varphi \wedge \neg\psi$.

(G) $\varphi_1 \to (\varphi_2 \to \varphi_3) \overset{(E)}{\equiv} \varphi_1 \to (\neg\varphi_2 \vee \varphi_3) \overset{(E)}{\equiv} \neg\varphi_1 \vee (\neg\varphi_2 \vee \varphi_3) \overset{(D.2)}{\equiv} (\neg\varphi_1 \vee \neg\varphi_2) \vee \varphi_3 \overset{(F.1)}{\equiv} \neg(\varphi_1 \wedge \varphi_2) \vee \varphi_3 \overset{(E)}{\equiv} (\varphi_1 \wedge \varphi_2) \to \varphi_3$.

(H.1) The first direction holds because of

$$
\begin{aligned}
\{(\varphi_1 \to \varphi_2) \wedge (\varphi_1 \to \varphi_3), \varphi_1\} &\vdash \varphi_1 \\
&\quad (\varphi_1 \to \varphi_2) \wedge (\varphi_1 \to \varphi_3) \\
&\vdash \varphi_1 \to \varphi_2 && (\wedge) \\
&\vdash \varphi_2 && (\text{MP}) \\
&\vdash \varphi_1 \to \varphi_3 && (\wedge) \\
&\vdash \varphi_3 && (\text{MP}) \\
&\vdash \varphi_2 \wedge \varphi_3 && (\wedge)
\end{aligned}
$$

and (DT). Secondly, we have

$$
\begin{aligned}
\{\varphi_1 \to (\varphi_2 \wedge \varphi_3)\} &\vdash \varphi_1 \to (\varphi_2 \wedge \varphi_3) \\
&\vdash (\varphi_2 \wedge \varphi_3) \to \varphi_2 && (\text{L}_3) \\
&\vdash \varphi_1 \to \varphi_2 && (\text{B.11}) \\
&\vdash (\varphi_2 \wedge \varphi_3) \to \varphi_3 && (\text{L}_4) \\
&\vdash \varphi_1 \to \varphi_3 && (\text{B.11}) \\
&\vdash (\varphi_1 \to \varphi_2) \wedge (\varphi_1 \to \varphi_3). && (\wedge)
\end{aligned}
$$

(H.2) For the first direction, we observe

$$
\begin{aligned}
\{(\varphi_1 \vee \varphi_2) \to \varphi_3, \varphi_1\} &\vdash \varphi_1 \\
&\vdash \varphi_1 \to (\varphi_1 \vee \varphi_2) && (\text{L}_6) \\
&\vdash (\varphi_1 \vee \varphi_2) && (\text{MP}) \\
&\vdash (\varphi_1 \vee \varphi_2) \to \varphi_3 \\
&\vdash \varphi_3 && (\text{MP}) \\
\{(\varphi_1 \vee \varphi_2) \to \varphi_3, \varphi_2\} &\vdash \varphi_3 && (\text{similarly})
\end{aligned}
$$

and hence the claim follwos from (DT) and ($\wedge$). The second direction is a consequence of

$$
\begin{aligned}
\{(\varphi_1 \to \varphi_3) \wedge (\varphi_2 \to \varphi_3)\} &\vdash \varphi_1 \to \varphi_3 && (\wedge) \\
&\vdash (\varphi_1 \to \varphi_3) \to ((\varphi_2 \to \varphi_3) \to ((\varphi_1 \vee \varphi_2) \to \varphi_3)) && (\text{L}_8) \\
&\vdash (\varphi_2 \to \varphi_3) \to ((\varphi_1 \vee \varphi_2) \to \varphi_3) && (\text{MP}) \\
&\vdash \varphi_2 \to \varphi_3 && (\wedge) \\
&\vdash (\varphi_1 \vee \varphi_2) \to \varphi_3. && (\text{MP})
\end{aligned}
$$

(I.1) $(\varphi_1 \wedge \varphi_2) \vee \varphi_3 \overset{(A)}{\equiv} \neg\neg(\varphi_1 \wedge \varphi_2) \vee \varphi_3 \overset{(E)}{\equiv} \neg(\varphi_1 \wedge \varphi_2) \to \varphi_3 \overset{(F.1)}{\equiv} (\neg\varphi_1 \vee \neg\varphi_2) \to \varphi_3 \overset{(H.2)}{\equiv} (\neg\varphi_1 \to \varphi_3) \wedge (\neg\varphi_2 \to \varphi_3) \overset{(E)}{\equiv} (\neg\neg\varphi_1 \vee \varphi_3) \wedge (\neg\neg\varphi_2 \vee \varphi_3) \overset{(A)}{\equiv} (\varphi_1 \vee \varphi_3) \wedge (\varphi_2 \vee \varphi_3)$.

(I.2) $(\varphi_1 \vee \varphi_2) \wedge \varphi_3 \overset{(A)}{\equiv} (\neg\neg\varphi_1 \vee \neg\neg\varphi_2) \wedge \neg\neg\varphi_3 \overset{(F.1)}{\equiv} \neg(\neg\varphi_1 \wedge \neg\varphi_2) \wedge \neg\neg\varphi_3 \overset{(F.2)}{\equiv} \neg((\neg\varphi_1 \wedge \neg\varphi_2) \vee \neg\varphi_3) \overset{(I.1)}{\equiv} \neg((\neg\varphi_1 \vee \neg\varphi_3) \wedge (\neg\varphi_2 \vee \neg\varphi_3)) \overset{(F.1)}{\equiv} \neg(\neg\varphi_1 \vee \neg\varphi_3) \vee \neg(\neg\varphi_2 \vee \neg\varphi_3) \overset{(F.2)}{\equiv} (\neg\neg\varphi_1 \wedge \neg\neg\varphi_3) \vee (\neg\neg\varphi_2 \wedge \neg\neg\varphi_3) \overset{(A)}{\equiv} (\varphi_1 \wedge \varphi_3) \vee (\varphi_2 \wedge \varphi_3)$.

(K.1) Firstly, we observe

$$\begin{aligned}
\{\varphi, \forall x\neg\varphi\} &\vdash \varphi \\
&\vdash \forall x\neg\varphi \\
&\vdash \forall x\neg\varphi \to \neg\varphi && (\mathrm{L}_{12}) \\
&\vdash \neg\varphi && (\mathrm{MP}) \\
&\vdash \bot && (\wedge) \\
\{\exists x\varphi, \forall x\neg\varphi\} &\vdash \bot && (\exists) \\
\{\exists x\varphi\} &\vdash \neg\exists x\neg\varphi && (\lightning)
\end{aligned}$$

and secondly, we have

$$\begin{aligned}
\{\neg\exists x\varphi, \varphi\} &\vdash \varphi \\
&\vdash \varphi \to \exists x\varphi && (\mathrm{L}_{13}) \\
&\vdash \exists x\varphi && (\mathrm{MP}) \\
&\vdash \neg\exists x\varphi \\
&\vdash \bot && (\wedge) \\
\{\neg\exists x\varphi\} &\vdash \neg\varphi && (\lightning) \\
&\vdash \forall x\neg\varphi && (\forall) \\
&\vdash \neg\neg\forall x\neg\varphi && (\mathrm{A}) \\
\{\neg\forall x\neg\varphi\} &\vdash \exists x\varphi. && (\mathrm{CP})
\end{aligned}$$

(K.2) $\forall x\varphi \overset{(A)}{\equiv} \neg\neg\forall x\neg\neg\varphi \overset{(K.1)}{\equiv} \neg\exists x\neg\varphi$.

(L.1) By $(\leftrightarrow)$ and symmetry, we only show $\vdash \varphi(x) \to \varphi(y)$ which follows from

$$\begin{aligned}
\{\varphi(x)\} &\vdash \varphi(x) \\
&\vdash \forall x\varphi(x) && (\forall) \\
&\vdash \forall x\varphi(x) \to \varphi(y) && (\mathrm{L}_{12}) \\
&\vdash \varphi(y) && (\mathrm{MP})
\end{aligned}$$

by (DT).

(L.2) Again by symmetry, we will only show one direction.

$$\begin{aligned}
\{\forall x\varphi(x)\} &\vdash \forall x\varphi(x) \\
&\vdash \forall x\varphi(x) \to \varphi(x) && (\mathrm{L}_{12}) \\
&\vdash \varphi(x) && (\mathrm{MP}) \\
&\vdash \varphi(y). && (\mathrm{L}.1)
\end{aligned}$$

The claim is thus a consequence of (DT).

(L.3) Due to symmetry, we consider just the first direction.

$$\begin{aligned}
\{\forall x\varphi(x)\} &\vdash \forall x\varphi(x) \\
&\vdash \forall x\varphi(x) \to \varphi(x) && (\mathrm{L}_{12}) \\
&\vdash \varphi(x) && (\mathrm{MP}) \\
&\vdash \varphi(x) \leftrightarrow \varphi(y) && (\mathrm{T}.1) \\
&\vdash \varphi(x) \to \varphi(y) && (\leftrightarrow) \\
&\vdash \varphi(y). && (\mathrm{MP})
\end{aligned}$$

The claim is thus a consequence of (DT).

(M.1) By symmetry, it is sufficient to prove $\vdash \exists x\exists y\varphi \to \exists y\exists x\varphi$.

$$\begin{aligned}
\{\varphi\} &\vdash \varphi \\
&\vdash \varphi \to \exists x\varphi && (\mathrm{L}_{13}) \\
&\vdash \exists x\varphi && (\mathrm{MP}) \\
&\vdash \exists x\varphi \to \exists y\exists x\varphi && (\mathrm{L}_{13}) \\
&\vdash \exists y\exists x\varphi. && (\mathrm{MP})
\end{aligned}$$

Applying $(\exists)$ twice implies $\{\exists x\exists y\varphi\} \vdash \exists y\exists x\varphi$ and thus the claim follows from (DT).

(M.2) The first direction follows directly from $\{\exists x\varphi\} \vdash \exists x\varphi$, $(\exists)$ and (DT). $(\mathrm{L}_{13})$ yields the other direction.

(N.1) For the first direction, we note:

$$\begin{aligned}
\{\varphi, \psi\} &\vdash \varphi \wedge \psi && (\wedge) \\
&\vdash (\varphi \wedge \psi) \to \exists y(\varphi \wedge \psi) && (\mathrm{L}_{13}) \\
&\vdash \exists y(\varphi \wedge \psi) && (\mathrm{MP}) \\
&\vdash \exists y(\varphi \wedge \psi) \to \exists x\exists y(\varphi \wedge \psi) && (\mathrm{L}_{13}) \\
&\vdash \exists x\exists y(\varphi \wedge \psi). && (\mathrm{MP})
\end{aligned}$$

Hence $(\exists)$ implies $\{\varphi, \exists y\psi\} \vdash \exists x\exists y(\varphi \wedge \psi)$ and with the same argument we obtain $\{\exists x\varphi, \exists y\psi\} \vdash \exists x\exists y(\varphi \wedge \psi)$. Thus, by $(\wedge)$ we get $\{\exists x\varphi \wedge \exists y\psi\} \vdash \exists x\exists y(\varphi \wedge \psi)$ from

which we can deduce the first direction by (DT). Secondly, we have

$$\begin{aligned}
\{\varphi \wedge \psi\} &\vdash \varphi && (\wedge)\\
&\vdash \psi && (\wedge)\\
&\vdash \varphi \to \exists x\varphi && (\mathrm{L}_{13})\\
&\vdash \exists x\varphi && (\mathrm{MP})\\
&\vdash \psi \to \exists y\psi && (\mathrm{L}_{13})\\
&\vdash \exists y\psi && (\mathrm{MP})\\
&\vdash \exists x\varphi \wedge \exists y\psi. && (\wedge)
\end{aligned}$$

Hence by applying ($\exists$) twice and (DT), we obtain the second direction.

The tautologies (N.2)-(N.5) can be shown using similar arguments. (O.1)-(O.5) are consequences of (N.1)-(N.5) using (A),(F.1),(F.2), (K.1) and (K.2). ⊣

Last but not least, we will prove that the binary relation $=$ is an equivalence relation. This enables us to handle equations in the usual way.

**Lemma B.17.** *Let $x, y$ and $z$ be arbitrary variables. Then the following statements hold:*

1. $\vdash x = x$,
2. $\vdash x = y \to y = x$,
3. $\vdash (x = y \wedge y = z) \to x = z$.

*Proof.*

1. Follows directly from axiom ($\mathrm{L}_{16}$).
2. The second statement is a consequence of the following arguments and (DT):

$$\begin{aligned}
\{x = y\} &\vdash x = y\\
&\vdash x = x && (\mathrm{L}_{16})\\
&\vdash x = y \wedge x = x && (\wedge)\\
&\vdash (x = y \wedge x = x) \leftrightarrow (x = x \leftrightarrow y = x) && (\mathrm{L}_{17})\\
&\vdash x = x \leftrightarrow y = x && (\mathrm{MP})\\
&\vdash y = x. && (\mathrm{MP})
\end{aligned}$$

3. For the transitivity, we use again (DT) and

$$
\begin{aligned}
\{x = y \wedge y = z\} &\vdash x = y \wedge y = z \\
&\vdash x = y && (\wedge) \\
&\vdash y = z && (\wedge) \\
&\vdash x = x && (\mathrm{L}_{16}) \\
&\vdash x = x \wedge y = z && (\wedge) \\
&\vdash (x = x \wedge y = z) \to (x = y \to x = z) && (\mathrm{L}_{17}) \\
&\vdash x = y \to x = z && (\mathrm{MP}) \\
&\vdash x = z. && (\mathrm{MP})
\end{aligned}
$$

$\dashv$