



UNIVERSITAT DE
BARCELONA

Facultat de Matemàtiques
i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Presburger Arithmetic & Other Fragments of Number Theory

Gioia Ponsdomènech Filipponi

Director: Dr. Enrique Casanovas Ruiz-Fornells

Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 10 de juny de 2025

Acknowledgements

Before beginning this study on first-order logic, I would like to express my gratitude to those who supported me throughout this process. To my family and friends: thank you for your constant encouragement and understanding during the ups and downs of this journey.

To my advisor, Enrique: I am deeply thankful for your guidance and patience. From you, I have learned the value of striving to prove every step, even those often overlooked by others. Your dedication and patience in assisting me have been essential to the completion of this work.

Abstract

This work studies the decidability of different simplified versions of the first-order theory of natural numbers, focusing on languages that include the successor function, the order relation, and addition. It begins by introducing the key concepts of first-order logic needed to understand the problem. Then, it looks at the natural numbers with just the successor function, and next with the addition of the order relation, showing that both of these theories are decidable using a technique called quantifier elimination. The work concludes with a proof of Presburger's theorem, which proves that the first-order theory of natural numbers with addition, order, and successor is also decidable.

Contents

Introduction	1
1 Preliminaries: First-Order Logic	3
1.1 The Language of First-Order Logic	3
1.2 Structures and Truth	4
1.3 Key Logical Notions	5
1.4 Soundness and Compactness theorems	6
1.5 Models of Theories	8
1.5.1 Size of Models	8
1.5.2 Theories	9
2 Natural Numbers with Successor	11
2.1 Theory of $\mathfrak{N}_S$ and axiomatization	11
2.2 Elimination of Quantifiers	16
2.3 Definability	20
3 Natural Numbers with Order	25
3.1 Theory of $\mathfrak{N}_L$ and axiomatization	25
3.2 Quantifier elimination and decidability	28
4 Natural Numbers with Addition	35
4.1 Theory of $\mathfrak{N}_A$ and axiomatization	35
4.2 Presburger Theorem	40
Bibliography	47

Introduction

Some Context

Since the early days of mathematical logic, one of the big questions has been: can we always decide whether a given mathematical statement is true or false? This challenge was a central question in mathematics during the early 20th century. A key figure was the mathematician David Hilbert, his *Hilbert Program* was a major project to give all of mathematics a secure and logical foundation. A central goal of this program was to solve the *Entscheidungsproblem* (the “decision problem”), which asked for an algorithm that could determine the truth or falsity of any logical statement. The central goal was to find a decision procedure for the theory of natural numbers $\mathbb{N}$ with its usual arithmetic operations—addition and multiplication.

It was in this context that Mojżesz Presburger, a Polish-Jewish student of the great logician Alfred Tarski in Warsaw, began his work in 1929. Rather than tackling the full theory of arithmetic his approach—guided by Tarski—was to investigate whether significant, non-trivial *fragments* of the theory could be proven decidable. This was a crucial strategy: if a part of arithmetic could be shown to have a positive solution to the decision problem, it would be a major step for Hilbert’s program.

Presburger’s search led him to isolate the first-order theory of natural numbers equipped only with the successor function and addition. In his 1929 master’s thesis, he proved that this theory, now known as *Presburger arithmetic*, is indeed *decidable*. This was one of the major positive results for a decidable theory related to numbers. The key to his success was the development of an advanced *quantifier elimination* procedure, a technique that simplifies complicated logical statements into easier, equivalent ones without losing their meaning.

His work stood in contrast to what would be discovered shortly after. In 1931, the work of Kurt Gödel delivered a profound blow to the original ambitions of the Hilbert Program. Gödel showed that the full first-order theory of arithmetic—with both addition and multiplication—is *undecidable*. In simple terms, there is no

algorithm that can determine the truth of every statement in that richer language. This result showed the importance of Presburger's work. It was no longer seen as just a step towards a larger goal, but as a key study that helped define the boundary between decidable and undecidable theories. Tragically, Presburger would not have the chance to build upon this brilliant early work, as he perished during the Holocaust.

Objective and Structure of the Work

The primary objective of this work is to explore the fundamental concept of decidability. While the complete first-order theory of natural numbers, including both addition and multiplication, is famously undecidable, this work investigates the fragments that emerge when we simplify its language. By methodically restricting the available operations, we can identify portions of arithmetic that are decidable.

This investigation is structured progressively through three fragments, building in complexity:

1. First, we will examine the most basic structure: the natural numbers equipped only with the *successor function*. We will establish its decidability through a direct application of the quantifier elimination technique.
2. Next, the language will be expanded to include the *order relation*. We will show that this richer theory remains decidable, once again by proving that it admits quantifier elimination.
3. Finally, the work culminates with a detailed exploration of *Presburger arithmetic*, the theory of natural numbers with *addition*, order, and successor. We will present a complete proof of Presburger's theorem, demonstrating that even this significantly more powerful fragment is decidable.

Throughout the work, the exposition closely follows Enderton's *Introduction to Mathematical Logic*, with adaptations to clarify and present the proofs in an accessible manner. Most results from the degree course *Mathematical Logic* are used without proof.

Chapter 1

Preliminaries: First-Order Logic

This chapter briefly introduces the key notation, concepts and results of first-order logic that have already been studied in the course of Mathematical Logic. The goal here is merely to recall the essentials for proving and understanding the results presented in the subsequent chapters. These include notions such as the definition of model, theory, and fundamental metatheorems like soundness, completeness, compactness, and enumerability.

1.1 The Language of First-Order Logic

To discuss mathematical properties formally, we must first specify the exact symbols we are allowed to use. This collection of symbols is called a *first-order language*.

A *first-order language* consists of a set of specified non-logical symbols, called *parameters*. These symbols are categorized as follows:

1. *Constant symbols*: Symbols that name specific, fixed elements in our domain of study (e.g., 0).
2. *Function symbols*: Symbols that represent functions, each with a fixed number of arguments (arity). For example, a successor function 'S' (unary) or addition '+' (binary).
3. *Relation symbols* (or *predicate symbols*): Symbols that represent relations or properties. Each relation symbol P also has a fixed arity (e.g., equality '=' or order '<').

In addition to these parameters, any first-order language includes a fixed set of *logical symbols*: connectives ($\neg, \wedge, \vee, \rightarrow$), quantifiers ($\forall, \exists$), parentheses, and an infinite set of variables.

Definition 1.1. The set of *variables*, denoted V , is a countably infinite set of symbols, typically written as $v_0, v_1, v_2, \dots$ or $x, y, z, \dots$. Variables function as placeholders for arbitrary elements of the domain.

Using these symbols, we can build expressions. *Terms* are expressions that name objects.

Definition 1.2. A *term* is defined recursively:

1. Every variable is a term.
2. Every constant symbol is a term.
3. If f is an n -ary function symbol and $t_1, \dots, t_n$ are terms, then $f(t_1, \dots, t_n)$ is a term.

From terms, we build *atomic formulas*, which are the most basic statements that can be asserted to be true or false.

Definition 1.3. An *atomic formula* is an expression of one of two forms:

1. $t_1 = t_2$, where t_1 and t_2 are terms.
2. $P(t_1, \dots, t_n)$, where P is an n -ary relation symbol and $t_1, \dots, t_n$ are terms.

Finally, we combine atomic formulas using logical connectives and quantifiers to build complex statements, which are called *well-formed formulas* (wffs).

Definition 1.4. The set of *well-formed formulas* (wffs) is defined recursively:

1. Every atomic formula is a wff.
2. If φ is a wff, then $(\neg\varphi)$ is a wff.
3. If φ and ψ are wffs, then $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, and $(\varphi \rightarrow \psi)$ are wffs.
4. If φ is a wff and x is a variable, then $(\forall x \varphi)$ and $(\exists x \varphi)$ are wffs.

1.2 Structures and Truth

The syntax defined above only tells us how to write formulas. To discuss whether a formula is true or false, we must provide a *meaning* or *interpretation* for the symbols. This is done using a mathematical *structure*.

Definition 1.5. A *structure* $\mathfrak{A}$ for a language $\mathcal{L}$ consists of:

1. A non-empty set $|\mathfrak{A}|$, called the *domain* or *universe* of the structure.

2. An interpretation for each parameter in $\mathcal{L}$:

- For each constant symbol c , an element $c^{\mathfrak{A}} \in |\mathfrak{A}|$.
- For each n -ary function symbol f , a function $f^{\mathfrak{A}} : |\mathfrak{A}|^n \rightarrow |\mathfrak{A}|$.
- For each n -ary relation symbol P , an n -ary relation $P^{\mathfrak{A}} \subseteq |\mathfrak{A}|^n$.

A formula can contain variables like $x + y = z$. To determine its truth, we must first assign a value from the domain to each variable.

Definition 1.6. An *assignment* into a structure $\mathfrak{A}$ is a function $s : V \rightarrow |\mathfrak{A}|$ that maps each variable in the set V to an element in the domain of $\mathfrak{A}$.

With a structure and an assignment, we can formally define what it means for a formula to be true. This is known as the *satisfaction relation*, written $\mathfrak{A} \models \varphi[s]$, and read as " $\mathfrak{A}$ satisfies φ with assignment s ". The definition is recursive, following the structure of the formula. For example, $\mathfrak{A} \models (\varphi \wedge \psi)[s]$ holds if and only if both $\mathfrak{A} \models \varphi[s]$ and $\mathfrak{A} \models \psi[s]$ hold. For a quantifier, $\mathfrak{A} \models (\forall x \varphi)[s]$ holds if and only if for every element $a \in |\mathfrak{A}|$, the structure $\mathfrak{A}$ satisfies φ with an assignment s' which is identical to s except that $s'(x) = a$.

1.3 Key Logical Notions

Some variables in a formula are tied to a quantifier, while others are not. This distinction is crucial for understanding sentences.

Definition 1.7. An occurrence of a variable x in a formula is *bound* if it is within the scope of a quantifier $\forall x$ or $\exists x$. An occurrence of a variable is *free* if it is not bound.

Example 1.8. In the formula $\exists y (x = y + y)$, the variable y is bound by the quantifier $\exists y$. The variable x is free.

The most important formulas are those whose truth value does not depend on an assignment of values to free variables.

Definition 1.9. A *sentence* is a well-formed formula that has no free variables.

For a sentence σ , its truth value in a structure $\mathfrak{A}$ is independent of any particular assignment. If $\mathfrak{A} \models \sigma[s]$ for some (and thus every) assignment s , we say that σ is *true* in $\mathfrak{A}$, or that $\mathfrak{A}$ is a *model* of σ . We write this as $\models_{\mathfrak{A}} \sigma$. If σ is not true in $\mathfrak{A}$, we write $\not\models_{\mathfrak{A}} \sigma$. We say that $\mathfrak{A}$ is a model of a set of sentences Γ if and only if it is a model of every sentence in Γ .

Definition 1.10. Let Γ be a set of wffs and φ a wff. Then Γ *logically implies* φ , written $\Gamma \models \varphi$, iff for every structure $\mathfrak{A}$ and every assignment $s : V \rightarrow |\mathfrak{A}|$, if $\mathfrak{A}$ satisfies every member of Γ with s , then $\mathfrak{A}$ also satisfies φ with s .

- We say that φ and ψ are *logically equivalent* (written $\varphi \equiv \psi$) iff $\varphi \models \psi$ and $\psi \models \varphi$.
- A wff φ is *valid* iff $\emptyset \models \varphi$ (written simply, $\models \varphi$). A sentence is valid if it is true in every structure.

Definition 1.11. A k -ary relation on $|\mathfrak{A}|$ is said to be *definable* in $\mathfrak{A}$ iff there is a formula φ (whose free variables are among $v_1, \dots, v_k$) that defines it there. That is, the relation is exactly the set

$$\{\langle a_1, \dots, a_k \rangle \mid \models_{\mathfrak{A}} \varphi[a_1, \dots, a_k].\}$$

While semantics deals with truth and models, the *deductive calculus* provides a purely syntactical way to derive formulas from a given set of assumptions. The deductive system consists of a predefined set of *logical axioms* and rules of inference.

Definition 1.12. Let Λ be the set of logical axioms. A *deduction* of a formula φ from a set of formulas Γ is a finite sequence $\langle \alpha_0, \dots, \alpha_n \rangle$ such that α_n is φ and for each $k \leq n$, one of the following holds:

- $\alpha_k \in \Gamma \cup \Lambda$.
- α_k is obtained by *modus ponens* from two earlier formulas in the sequence; that is, for some $i, j < k$, the formula α_j is $(\alpha_i \rightarrow \alpha_k)$.

If such a deduction exists, we say that φ is *deducible* from Γ , and we write $\Gamma \vdash \varphi$.

1.4 Soundness and Compactness theorems

In this section we introduce two major theorems: the soundness of our deductive calculus and its completeness. We will then introduce some of their immediate consequences.

The soundness theorem states that if a conclusion can be derived from a deduction, then it must be true in every interpretation where the axioms are true.

Theorem 1.13 (Soundness Theorem). Let Γ be a set of formulas, and φ a formula. Then

$$\Gamma \vdash \varphi \Rightarrow \Gamma \models \varphi.$$

Recall that a set of formulas Γ is *consistent* iff there is no formula φ such that both $\Gamma \vdash \varphi$ and $\Gamma \vdash \neg\varphi$. Define Γ to be *satisfiable* iff there is some structure $\mathfrak{A}$ and assignment s such that $\mathfrak{A}$ satisfies every member of Γ with s .

With this in mind, the Soundness Theorem admits the following reformulation:

Theorem 1.14 (Soundness Theorem). Let Γ be a set of formulas. If Γ is satisfiable, then Γ is consistent.

The Completeness Theorem is the converse to the Soundness Theorem and asserts if a formula is valid, then there is a finite deduction (a formal proof) of the formula within the given deductive system.

Theorem 1.15 (Completeness Theorem). The Completeness Theorem admits the following equivalent formulations:

- (a) Let Γ be a set of formulas. If $\Gamma \models \varphi$, then $\Gamma \vdash \varphi$.
- (b) Every consistent set of formulas is satisfiable.

A consequence of the two theorems is the following:

Theorem 1.16 (Compactness Theorem). Let Γ be a set of formulas. The Compactness Theorem admits the following equivalent formulations:

- (a) If $\Gamma \models \varphi$, then for some finite $\Gamma_0 \subseteq \Gamma$, we have $\Gamma_0 \models \varphi$.
- (b) If every finite subset Γ_0 of Γ is satisfiable, then Γ is satisfiable.

We begin by recalling some definitions before stating the next result

Definition 1.17. A set Σ is *decidable* iff there exists an effective procedure that given an expression α , will decide whether or not $\alpha \in \Sigma$.

Definition 1.18. A set A of expressions is *effectively enumerable* iff there exists an effective procedure that lists, in some order, the members of A .

And finally:

Definition 1.19. A *reasonable language* is one whose set of symbols can be effectively enumerated and such that the two relations

$$\{\langle P, n \rangle \mid P \text{ is an } n\text{-place predicate symbol}\}$$

and

$$\{\langle f, n \rangle \mid f \text{ is an } n\text{-place function symbol}\}$$

are decidable.

Now we can state our result of interest.

Theorem 1.20 (Enumerability Theorem). For a reasonable language, the set of valid wffs can be effectively enumerated.

A direct consequence of this theorem is:

Corollary 1.21. Let Γ be a decidable set of formulas in a reasonable language.

- (a) The set of theorems of Γ is effectively enumerable.
- (b) The set $\{\varphi \mid \Gamma \models \varphi\}$ of formulas logically implied by Γ is effectively enumerable.

Another consequence is:

Corollary 1.22. Assume that Γ is a decidable set of formulas in a reasonable language, and that for every sentence σ , either $\Gamma \models \sigma$ or $\Gamma \models \neg\sigma$. Then the set of sentences logically implied by Γ , that is, $\text{Cn } \Gamma$, is decidable.

1.5 Models of Theories

1.5.1 Size of Models

Definition 1.23. For any structure $\mathfrak{A}$, the *theory of $\mathfrak{A}$* , written $\text{Th } \mathfrak{A}$, is the set of all sentences that are true in $\mathfrak{A}$.

If we restrict ourselves to finite structures and finite languages, we have:

Theorem 1.24. For a finite language, the set $\{\sigma \mid \sigma \text{ has a finite model}\}$ is effectively enumerable.

Later, we will use the following version of the Löwenheim-Skolem Theorem.

Theorem 1.25 (Löwenheim-Skolem Theorem). (a) Let Γ be a satisfiable set of formulas in a language of cardinality λ . Then Γ is satisfiable in some structure of size $\leq \lambda$.

- (b) Let Σ be a set of sentences in a language of cardinality λ . If Σ has any model, then it has a model of cardinality $\leq \lambda$.

Another essential result is the upward Löwenheim-Skolem Theorem, known as Löwenheim-Skolem-Tarski (LST) Theorem.

Theorem 1.26 (LST Theorem). Let Γ be a set of formulas in a language of cardinality λ , and assume that Γ is satisfiable in some infinite structure. Then for every cardinal $\kappa \geq \lambda$, there exists a structure of cardinality κ in which Δ is satisfiable.

1.5.2 Theories

We can define theories in a more general way.

Definition 1.27. A *theory* is a set of sentences closed under logical implication. That is, T is a theory iff T is a set of sentences such that for any sentence σ of the language,

$$T \models \sigma \Rightarrow \sigma \in T.$$

Definition 1.28. For a class $\mathcal{K}$ of structures (for the language), define the *theory* of $\mathcal{K}$, written $\text{Th } \mathcal{K}$, by the equation

$$\text{Th } \mathcal{K} = \{\sigma \mid \sigma \text{ is true in every member of } \mathcal{K}\}.$$

The above concept arose previously in the case $\mathcal{K} = \{\mathfrak{A}\}$.

Definition 1.29. Let Σ be a set of sentences. Define $\text{Mod } \Sigma$ to be the class of all models of Σ . Then $\text{Th Mod } \Sigma$ is the set of all sentences that are true in all models of Σ .

This set coincides with the set of all sentences logically implied by Σ , which we call the *set of consequences* of Σ , and denote by $\text{Cn } \Sigma$. Thus,

$$\text{Cn } \Sigma = \{\sigma \mid \Sigma \models \sigma\} = \text{Th Mod } \Sigma.$$

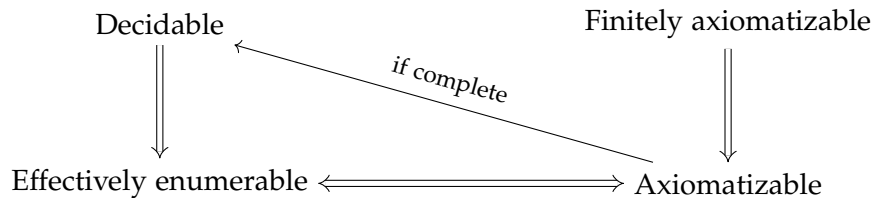
Definition 1.30. A theory T is said to be *complete* iff for every sentence σ , either $\sigma \in T$ or $(\neg\sigma) \in T$.

Definition 1.31. A theory T is *axiomatizable* iff there exists a decidable set Σ of sentences such that $T = \text{Cn } \Sigma$. A theory is *finitely axiomatizable* iff there exists a finite set Σ of sentences such that $T = \text{Cn } \Sigma$.

The following theorem will prove useful:

Theorem 1.32. If $\text{Cn } \Sigma$ is finitely axiomatizable, then there exists a finite subset $\Sigma_0 \subseteq \Sigma$ such that $\text{Cn } \Sigma_0 = \text{Cn } \Sigma$.

As a consequence of the previous theorem and Corollary 1.21 and Corollary 1.22, we have the following diagram:



Definition 1.33. Two structures $\mathfrak{A}$ and $\mathfrak{B}$ for a given language are *elementarily equivalent* if for every sentence σ , we have $\mathfrak{A} \models \sigma$ if and only if $\mathfrak{B} \models \sigma$. We write $\mathfrak{A} \equiv \mathfrak{B}$ to indicate that $\mathfrak{A}$ and $\mathfrak{B}$ are elementarily equivalent.

Proposition 1.34. A theory T is complete if and only if all of its models are elementarily equivalent. That is, for any two models $\mathfrak{A}$ and $\mathfrak{B}$ of T , it holds that $\mathfrak{A} \equiv \mathfrak{B}$.

We end this chapter with another theorem that we will use later, but first we need a definition:

Definition 1.35. A theory T is said to be $\aleph_0$ -categorical iff all the infinite countable models of T are isomorphic (i.e., there is a bijection between their domains that preserves constants, functions, and relations). More generally, for a cardinal κ , T is κ -categorical iff all models of T having cardinality κ are isomorphic.

Theorem 1.36 (Łoś-Vaught Test). Let T be a theory in a countable language. Assume that T has no finite models.

- (a) If T is $\aleph_0$ -categorical, then T is complete.
- (b) If T is κ -categorical for some infinite cardinal κ , then T is complete.

Chapter 2

Natural Numbers with Successor

Having established the basic concepts of first-order logic, we now turn our attention to a specific theory: the natural numbers equipped with the successor function S . Our primary goal here is to determine whether the first-order theory of the natural numbers with successor is decidable.

2.1 Theory of $\mathfrak{N}_S$ and axiomatization

We will begin with a relatively simple reduct of $\mathfrak{N}$, that of natural numbers with successor. By only considering the symbols $\forall$, 0 , and S we have

$$\mathfrak{N}_S = (\mathbb{N}; 0, S).$$

We want to find out if the set $\text{Th } \mathfrak{N}_S$ is decidable, that is, if there is an effective procedure that can, for any sentence φ , determine whether it belongs to $\text{Th } \mathfrak{N}_S$ or not; in other words, we want to find out if we can always tell whether a sentence φ is true in $\mathfrak{N}_S$ or not.

We will start by listing some sentences true in $\mathfrak{N}_S$ that we will later prove to be an axiomatization for the theory:

$$\begin{array}{lll} \forall x & Sx \neq 0 & (\text{S1}) \\ \forall x \forall y & (Sx = Sy \rightarrow x = y) & (\text{S2}) \\ \forall y & (y \neq 0 \rightarrow \exists x y = Sx) & (\text{S3}) \\ \forall x & Sx \neq x & (\text{S4.1}) \\ \forall x & SSx \neq x & (\text{S4.2}) \\ \dots & & \\ \forall x & S^n x \neq x & (\text{S4.n}) \end{array}$$

Let A_S be the infinite set consisting of the above sentences S1, S2, S3, S4. n ($n = 1, 2, \dots$). Clearly, these sentences are true in $\mathfrak{N}_S$; i.e., $\mathfrak{N}_S$ is a model of A_S . Hence

$$\text{Cn } A_S \subseteq \text{Th } \mathfrak{N}_S$$

(Anything true in every model of A_S is true in this model.) What is not so obvious is that equality holds. To prove this we will consider arbitrary models of A_S .

Consider an arbitrary model $\mathfrak{A} = (|\mathfrak{A}|; 0^{\mathfrak{A}}, S^{\mathfrak{A}})$ of the axioms A_S . S1, $\forall x(Sx \neq 0)$, ensures that $0^{\mathfrak{A}}$ is not in the range of $S^{\mathfrak{A}}$. S2, $\forall x \forall y(Sx = Sy \rightarrow x = y)$, states that $S^{\mathfrak{A}}$ is a one-to-one (injective) function. S3, $\forall y(y \neq 0 \rightarrow \exists x(y = Sx))$, means that every element in $|\mathfrak{A}| \setminus \{0^{\mathfrak{A}}\}$ is in the range of $S^{\mathfrak{A}}$. Together, these imply that $S^{\mathfrak{A}}$ must be a one-to-one map of $|\mathfrak{A}|$ onto $|\mathfrak{A}| \setminus \{0^{\mathfrak{A}}\}$. Furthermore, by axioms S4. n , $\forall x(S^n x \neq x \text{ for } n \geq 1)$, there can be no $S^{\mathfrak{A}}$ -loops of any finite size n .

Thus, $|\mathfrak{A}|$ must contain the "standard" points:

$$0^{\mathfrak{A}} \xrightarrow{S^{\mathfrak{A}}} (S^{\mathfrak{A}})^1(0^{\mathfrak{A}}) \xrightarrow{S^{\mathfrak{A}}} (S^{\mathfrak{A}})^2(0^{\mathfrak{A}}) \xrightarrow{S^{\mathfrak{A}}} \dots$$

which are all distinct. The arrow $\xrightarrow{S^{\mathfrak{A}}}$ indicates the action of $S^{\mathfrak{A}}$.

Definition 2.1. The *standard part* of a model $\mathfrak{A}$ of A_S , denoted $\tilde{0}^{\mathfrak{A}}$, is the set

$$\{a \mid \exists n \in \mathbb{N} \text{ such that } (S^{\mathfrak{A}})^n(0^{\mathfrak{A}}) = a\}.$$

(Here, $(S^{\mathfrak{A}})^0(0^{\mathfrak{A}}) = 0^{\mathfrak{A}}$).

This collection of standard points, $\tilde{0}^{\mathfrak{A}}$, forms a structure isomorphic to the standard model of natural numbers $(\mathbb{N}; 0, S)$.

Proposition 2.2. Let $\mathfrak{A}$ be a model of A_S . Its standard part $(\tilde{0}^{\mathfrak{A}}; 0^{\mathfrak{A}}, S^{\mathfrak{A}}|_{\tilde{0}^{\mathfrak{A}}})$ is isomorphic to $(\mathbb{N}; 0, S)$.

Proof. Define the map $f : \mathbb{N} \rightarrow \tilde{0}^{\mathfrak{A}}$ by $f(n) = (S^{\mathfrak{A}})^n(0^{\mathfrak{A}})$.

1. $f(0) = (S^{\mathfrak{A}})^0(0^{\mathfrak{A}}) = 0^{\mathfrak{A}}$.
2. $f(S(n)) = f(n+1) = (S^{\mathfrak{A}})^{n+1}(0^{\mathfrak{A}}) = S^{\mathfrak{A}}((S^{\mathfrak{A}})^n(0^{\mathfrak{A}})) = S^{\mathfrak{A}}(f(n))$. Thus, f is a homomorphism.
3. To show f is injective, suppose $f(n) = f(m)$ for $n, m \in \mathbb{N}$. Then $(S^{\mathfrak{A}})^n(0^{\mathfrak{A}}) = (S^{\mathfrak{A}})^m(0^{\mathfrak{A}})$. Assume, without loss of generality, that $n < m$. Let $m = n + k$ for some $k \in \mathbb{N}$ with $k > 0$. Then $(S^{\mathfrak{A}})^n(0^{\mathfrak{A}}) = (S^{\mathfrak{A}})^{n+k}(0^{\mathfrak{A}}) = (S^{\mathfrak{A}})^n((S^{\mathfrak{A}})^k(0^{\mathfrak{A}}))$. Since $S^{\mathfrak{A}}$ is injective (by S2), repeated application implies $0^{\mathfrak{A}} = (S^{\mathfrak{A}})^k(0^{\mathfrak{A}})$. However, S4. k states $\forall x(S^k x \neq x)$, so for $x = 0^{\mathfrak{A}}$, $(S^{\mathfrak{A}})^k(0^{\mathfrak{A}}) \neq 0^{\mathfrak{A}}$ for $k > 0$. This is a contradiction. Thus, n cannot be less than m . Similarly, m cannot be less than n . Hence $n = m$, and f is injective.

4. The map f is surjective onto $\tilde{0}^{\mathfrak{A}}$ by the definition of $\tilde{0}^{\mathfrak{A}}$.

Therefore, f is an isomorphism. □

There may or may not be other points in $|\mathfrak{A}|$. If there is another point $a \in |\mathfrak{A}| \setminus \tilde{0}^{\mathfrak{A}}$ (a non-standard element), then there will be the successor of a , its successor, etc. By S3 and S2, a also has a unique predecessor, say a_{-1} , such that $S^{\mathfrak{A}}(a_{-1}) = a$. Since $a \notin \tilde{0}^{\mathfrak{A}}$, a_{-1} cannot be $0^{\mathfrak{A}}$, so a_{-1} also has a unique predecessor a_{-2} , and so on. This generates an infinite chain of distinct predecessors and successors for a . This entire chain cannot contain $0^{\mathfrak{A}}$ and cannot loop upon itself (by S4.n). Such a structure is called a Z-chain.

Definition 2.3. A Z-chain $\tilde{a}$ in a model $\mathfrak{A}$ of A_S , containing an element $a \in |\mathfrak{A}| \setminus \tilde{0}^{\mathfrak{A}}$, is the set $\{(S^{\mathfrak{A}})^z(a) \mid z \in \mathbb{Z}\}$. For $z < 0$, $(S^{\mathfrak{A}})^z(a)$ denotes applying the unique predecessor operation $|z|$ times to a .

Each such Z-chain $\tilde{a}$ is isomorphic to $(\mathbb{Z}; S)$, where S here denotes the standard successor on integers.

Proposition 2.4. Let $\mathfrak{A}$ be a model of A_S . Any Z-chain $(\tilde{a}; S^{\mathfrak{A}}|_{\tilde{a}})$ in $\mathfrak{A}$ is isomorphic to $(\mathbb{Z}; S)$.

Proof. Let a be an arbitrary element in a Z-chain $\tilde{a}$. Define the map $g : \mathbb{Z} \rightarrow \tilde{a}$ by $g(z) = (S^{\mathfrak{A}})^z(a)$.

1. $g(S_{\mathbb{Z}}(z)) = g(z + 1) = (S^{\mathfrak{A}})^{z+1}(a) = S^{\mathfrak{A}}((S^{\mathfrak{A}})^z(a)) = S^{\mathfrak{A}}(g(z))$. Thus, g is a homomorphism.
2. To show g is injective, suppose $g(n) = g(m)$ for $n, m \in \mathbb{Z}$. Then $(S^{\mathfrak{A}})^n(a) = (S^{\mathfrak{A}})^m(a)$. We consider three cases:
 - *Case 1:* $n, m \geq 0$. Assume $n < m$. Let $m = n + k$ for some $k \in \mathbb{N}, k > 0$. Then $(S^{\mathfrak{A}})^n(a) = (S^{\mathfrak{A}})^n((S^{\mathfrak{A}})^k(a))$. By injectivity of $S^{\mathfrak{A}}$ (from S2), $a = (S^{\mathfrak{A}})^k(a)$. This contradicts S4.k, as $k > 0$.
 - *Case 2:* $n, m < 0$. Let $n = -n'$ and $m = -m'$ for $n', m' \in \mathbb{N}$ with $n', m' > 0$. Then $(S^{\mathfrak{A}})^{-n'}(a) = (S^{\mathfrak{A}})^{-m'}(a)$. Let this common element be c . So, $a = (S^{\mathfrak{A}})^{n'}(c)$ and $a = (S^{\mathfrak{A}})^{m'}(c)$. Assume $n' < m'$ (if $m' < n'$, let $m' = n' + k$ for some $k \in \mathbb{N}, k > 0$. Then $(S^{\mathfrak{A}})^{n'}(c) = (S^{\mathfrak{A}})^{n'+k}(c) = (S^{\mathfrak{A}})^{n'}((S^{\mathfrak{A}})^k(c))$. This implies $c = (S^{\mathfrak{A}})^k(c)$, which contradicts S4.k as $k > 0$).

- Case 3: $n \geq 0$ and $m < 0$ (the case $n < 0$ and $m \geq 0$ is symmetric). Let $m = -m'$ for $m' \in \mathbb{N}$ with $m' > 0$. Then $(S^{\mathfrak{A}})^n(a) = (S^{\mathfrak{A}})^{-m'}(a)$. Let $c = (S^{\mathfrak{A}})^{-m'}(a)$, so $a = (S^{\mathfrak{A}})^{m'}(c)$. The equation becomes $(S^{\mathfrak{A}})^n((S^{\mathfrak{A}})^{m'}(c)) = c$, which simplifies to $(S^{\mathfrak{A}})^{n+m'}(c) = c$. Since $n \geq 0$ and $m' > 0$, their sum $k = n + m' > 0$. This gives $(S^{\mathfrak{A}})^k(c) = c$, contradicting S4.k.

Therefore, $g(n) = g(m)$ implies $n = m$, so g is injective.

3. The map g is surjective onto $\tilde{a}$ by its definition as $\{(S^{\mathfrak{A}})^z(a) \mid z \in \mathbb{Z}\}$.

Hence, g is an isomorphism. □

The domain $|\mathfrak{A}|$ can be partitioned into equivalence classes under the relation $x \sim y$ if $y = (S^{\mathfrak{A}})^z(x)$ for some $z \in \mathbb{Z}$. The equivalence class of $0^{\mathfrak{A}}$ is the standard part $\tilde{0}^{\mathfrak{A}}$. Any other equivalence class, generated by an element $a \notin \tilde{0}^{\mathfrak{A}}$, is a $\mathbb{Z}$ -chain $\tilde{a}$. These components (the standard part and the $\mathbb{Z}$ -chains) are disjoint.

Theorem 2.5 (Characterization of Models of A_S). Any model $\mathfrak{A}$ of A_S is a disjoint union of its standard part $\tilde{0}^{\mathfrak{A}}$ and a collection (possibly empty) of $\mathbb{Z}$ -chains $\{\tilde{a}_i\}_{i \in I}$. The standard part $\tilde{0}^{\mathfrak{A}}$ is isomorphic to $(\mathbb{N}; 0, S)$, and each $\mathbb{Z}$ -chain $\tilde{a}_i$ is isomorphic to $(\mathbb{Z}; S)$. Conversely, any structure formed as such a disjoint union is a model of A_S .

Proof. The decomposition into equivalence classes under $\sim$ yields the standard part $\tilde{0}^{\mathfrak{A}}$ and various $\mathbb{Z}$ -chains $\tilde{a}_i$. Propositions 2.2 and 2.4 establish their isomorphic structures. Disjointness of $\tilde{0}^{\mathfrak{A}}$ from any $\mathbb{Z}$ -chain $\tilde{a}$ follows because elements of $\tilde{a}$ are not in $\tilde{0}^{\mathfrak{A}}$ by definition of non-standard elements. Disjointness of two distinct $\mathbb{Z}$ -chains $\tilde{a}$ and $\tilde{b}$ follows because if they shared an element x , then both chains would be identical to the chain $\tilde{x}$, contradicting their distinctness. The converse statement (that any such structure is a model of A_S) can be verified by checking that each axiom in A_S holds in such a structure. □

Remark 2.6. (Cardinality of Models). The standard part $\tilde{0}^{\mathfrak{A}}$ and each $\mathbb{Z}$ -chain $\tilde{a}$ are countably infinite (cardinality $\aleph_0$). If a model $\mathfrak{A}$ of A_S has λ $\mathbb{Z}$ -chains, the cardinality of $|\mathfrak{A}|$ is $\aleph_0 + \lambda \cdot \aleph_0$. This is $\aleph_0$ if λ is countable (finite or $\aleph_0$), and λ if λ is an uncountable cardinal. Thus, if a model $\mathfrak{A}$ is countable, it must consist of its standard part and at most a countably infinite number of $\mathbb{Z}$ -chains.

Lemma 2.7. If $\mathfrak{A}$ and $\mathfrak{A}'$ are models of A_S having the same number (cardinality) of $\mathbb{Z}$ -chains, then they are isomorphic.

Proof. An isomorphism can be constructed by mapping the standard part of $\mathfrak{A}$ to the standard part of $\mathfrak{A}'$ (using Proposition 2.2). Since there is a one-to-one correspondence between the set of Z-chains of $\mathfrak{A}$ and that of $\mathfrak{A}'$, map each Z-chain in $\mathfrak{A}$ isomorphically to its corresponding Z-chain in $\mathfrak{A}'$ (using Proposition 2.4). Combining these individual isomorphisms (which uses the Axiom of Choice if there are infinitely many Z-chains) yields an isomorphism from $\mathfrak{A}$ onto $\mathfrak{A}'$. Thus, a model of A_S is determined up to isomorphism by the number of its Z-chains. $\square$

The property of being standard (i.e., isomorphic to $\mathfrak{N}_S$ and thus having no Z-chains) is not first-order definable within the language of A_S . Specifically, no set of sentences Σ can isolate $\mathfrak{N}_S$. For if it could, $\text{Th } \mathfrak{N}_S$ itself would be such a set. However, by the Löwenheim-Skolem Theorem, $\text{Th } \mathfrak{N}_S$ must have uncountable models. Any such uncountable model $\mathfrak{A}$, being elementarily equivalent to $\mathfrak{N}_S$ and thus a model of A_S , possesses Z-chains because its uncountability arises from them (as an uncountable model's cardinality equals its number of Z-chains). This contradicts $\mathfrak{N}_S$, which has no Z-chains. Therefore, no first-order theory in this language uniquely characterizes the standard model.

Theorem 2.8. If $\mathfrak{A}$ and $\mathfrak{B}$ are two uncountable models of A_S that share the same cardinality, then $\mathfrak{A}$ and $\mathfrak{B}$ are isomorphic.

Proof. From the analysis of models of A_S , it was established that for any uncountable model $\mathfrak{M}$, its cardinality is precisely the number of its Z-chains. Furthermore, it was shown that models of A_S are isomorphic if and only if they possess the same number of Z-chains. Given that $\mathfrak{A}$ and $\mathfrak{B}$ are uncountable and $\text{card}(\mathfrak{A}) = \text{card}(\mathfrak{B})$ by hypothesis, they must therefore have the same (uncountable) number of Z-chains. This implies their isomorphism. $\square$

Theorem 2.9 (Completeness of A_S). The theory $\text{Cn } A_S$ is complete.

Proof. The proof relies on the Łoś-Vaught Test. The theory $\text{Cn } A_S$ satisfies the conditions of this test: its language is countable, and it is satisfiable (as $\mathfrak{N}_S$ is a model). As demonstrated by Theorem 2.8, $\text{Cn } A_S$ is κ -categorical for all uncountable cardinals κ . Additionally, A_S possesses no finite models because the standard part $\tilde{0}^{\mathfrak{A}}$ present in any model $\mathfrak{A}$ is itself infinite. Given these conditions, the Łoś-Vaught Test concludes that $\text{Cn } A_S$ is a complete theory. $\square$

Corollary 2.10. $\text{Cn } A_S = \text{Th } \mathfrak{N}_S$.

Proof. We already have $\text{Cn } A_S \subseteq \text{Th } \mathfrak{N}_S$.

Now, since $\text{Th } \mathfrak{N}_S$ is the set of all sentences true in $\mathfrak{N}_S$, it is satisfiable, and hence consistent by the Soundness Theorem.

From the previous Corollary we know that $\text{Cn } A_S$ is complete, so for any sentence σ , either $\sigma \in \text{Cn } A_S$ or $\neg\sigma \in \text{Cn } A_S$.

Now let $\sigma \in \text{Th } \mathfrak{N}_S$, that is, $\mathfrak{N}_S \models \sigma$. Suppose, for contradiction, that $\sigma \notin \text{Cn } A_S$. Then, by completeness, $\neg\sigma \in \text{Cn } A_S$, this implies $\neg\sigma \in \text{Th } \mathfrak{N}_S$, so $\mathfrak{N}_S \models \neg\sigma$, a contradiction. Therefore, $\sigma \in \text{Cn } A_S$, and thus $\text{Th } \mathfrak{N}_S \subseteq \text{Cn } A_S$. □

With this corollary, we can now prove our property of interest.

Corollary 2.11. $\text{Th } \mathfrak{N}_S$ is decidable.

Proof. From Theorem 2.9 and Corollary 2.10, we know that $\text{Th } \mathfrak{N}_S$ is complete. Since $\text{Th } \mathfrak{N}_S$ is axiomatizable, we have that it is also decidable. □

2.2 Elimination of Quantifiers

Definition 2.12. A theory T admits *elimination of quantifiers* if and only if for every formula φ there exists a quantifier-free formula ψ such that

$$T \models (\varphi \leftrightarrow \psi).$$

Quantifier-free formulas are generally easier to work with, as their truth in a structure can be determined without having to consider bound variables or complex logical nesting. When a theory admits elimination of quantifiers, every formula is equivalent to a quantifier-free one. This not only allows us to construct a decision procedure to determine whether a sentence belongs to the theory, but also leads to alternative proofs of completeness and decidability, since the logical behavior of quantifier-free sentences is easier to characterize.

In fact, it is enough to consider a specific type of formula φ to prove that a theory admits elimination of quantifiers.

Before continuing with the next theorems we will use a result from the course of Mathematical Logic.

Lemma 2.13. For every formula φ in sentential logic, there exist formulas φ_d and φ_c such that:

$$\varphi \equiv \varphi_d \equiv \varphi_c,$$

where φ_d is in disjunctive normal form (DNF) (a disjunction of conjunctions of literals¹) and φ_c is in conjunctive normal form (CNF) (a conjunction of disjunc-

¹An atomic formula or a negation of an atomic formula.

tions of literals). Moreover, the propositional variables occurring in φ_d and φ_c are exactly those occurring in φ .

Now we can prove the following crucial theorem.

Theorem 2.14. Assume that for every formula φ of the form

$$\exists x (\alpha_0 \wedge \cdots \wedge \alpha_k),$$

where each α_i is either an atomic formula or the negation of an atomic formula, there exists a quantifier-free formula ψ such that $T \models (\varphi \leftrightarrow \psi)$. Then T admits elimination of quantifiers.

Proof. We proceed by induction on the construction of α .

Suppose α is an atomic formula. Then α is quantifier-free by definition.

Let α (resp. β) be quantifier-free such that α' (resp. β') is equivalent in T to α (resp. β). We have that $T \models (\alpha \leftrightarrow \alpha')$, therefore

$$T \models (\neg\alpha \leftrightarrow \neg\alpha')$$

also holds.

If

$$T \models (\alpha \leftrightarrow \alpha') \quad \text{and} \quad T \models (\beta \leftrightarrow \beta'),$$

then

$$T \models ((\alpha \wedge \beta) \leftrightarrow (\alpha' \wedge \beta')).$$

Now, consider $\exists x\alpha$. We suppose as the Inductive Hypothesis that there exists α' quantifier-free such that

$$T \models (\alpha \leftrightarrow \alpha').$$

Then,

$$T \models (\exists x\alpha \leftrightarrow \exists x\alpha').$$

We have $\exists x\alpha'$ with α' quantifier free. By the disjunctive normal form, α' is equivalent to

$$(\alpha_0 \vee \cdots \vee \alpha_k),$$

where each α_i is a conjunction of atomic or negated atomic formulas. Therefore, $\exists x\alpha'$ is equivalent to

$$(\exists x\alpha_0 \vee \cdots \vee \exists x\alpha_k),$$

By the initial hypothesis, for each i , we have a quantifier-free formula β_i equivalent in T to $\exists x\alpha_i$. Hence,

$$T \models (\exists x\alpha \leftrightarrow (\beta_0 \vee \cdots \vee \beta_k)).$$

□

Theorem 2.15. Th $\mathfrak{N}_S$ admits elimination of quantifiers.

Proof. By Theorem 2.14, it suffices to consider formulas of the form

$$\exists x(\alpha_0 \wedge \cdots \wedge \alpha_k),$$

where each α_i is atomic or the negation of an atomic formula. We describe how to replace such a formula with a quantifier-free formula.

In the language of $\mathfrak{N}_S$, the only terms are of the form $S^k u$, where u is either 0 or a variable. The only atomic formulas are equations. Without loss of generality, assume the variable x occurs in every α_i . If not, since

$$\exists x(\alpha \wedge \beta) \equiv \alpha \wedge \exists x\beta,$$

we may separate out those α_i not containing x .

Hence each α_i is of the form

$$S^m x = S^n u$$

or its negation, where u is 0 or a variable. Furthermore, assume $u \neq x$ because an equation

$$S^m x = S^n x$$

can be replaced by $0 = 0$ if $m = n$ (reflexivity), and by $0 \neq 0$ if $m \neq n$ (If $m > n$, let $m = n + k$ with $k \geq 1$. Then $S^{n+k} x = S^n x \implies S^k x = x$ by repeated application of S2. This contradicts S4.k).

Case 1: Suppose every α_i is the negation of an equation. Since the natural numbers are infinite (derived from S1 ensuring $Sx \neq 0$ and S2 ensuring S is injective, which together imply $0, S0, SS0, \dots$ are all distinct), we can always find an x that is different from all those specific values forbidden by the negated equations (Each equation $S^p y = t$ has at most one solution for y by repeated application of S2; thus, only a finite number of values for x are excluded by the conjunction). Then the formula is equivalent to

$$0 = 0.$$

Case 2: Suppose there is at least one α_i not negated; without loss of generality, let α_0 be

$$S^m x = t,$$

where the term t does not contain x . Since the solution for x must be a natural number (non-negative), replace α_0 by the conjunction

$$t \neq 0 \wedge \cdots \wedge t \neq S^{m-1} 0,$$

or by $0 = 0$ if $m = 0$. (This conjunction is necessary for $S^m x = t$ to yield a solution $x \geq 0$; it ensures $t \notin \{0, S0, \dots, S^{m-1}0\}$, which follows from axioms S1 and S2. If these conditions on t are met, S3 then ensures such an x exists.)

For each other α_j of the form

$$S^k x = u,$$

replace it first by

$$S^{k+m} x = S^m u,$$

(justified by the injectivity derived from S2) which becomes

$$S^k t = S^m u.$$

At this point, the variable x no longer appears. Hence, the quantifier can be dropped, and this completes the quantifier elimination. □

Remark 2.16. The preceding proof for quantifier elimination was presented for formulas that contain free variables. We note that this is not a limitation, as the algorithm can also be applied to sentences (i.e., formulas without free variables), provided that the language contains at least one constant symbol.

In the case where a sentence σ contains constants $(c_1, \dots, c_n)$, we proceed by replacing these constants with new variables $x_1, \dots, x_n$ to create a formula $\varphi(x_1, \dots, x_n)$. We then apply the standard quantifier elimination algorithm to $\varphi(x_1, \dots, x_n)$, which yields an equivalent quantifier-free formula $\psi(x_1, \dots, x_n)$.

The final equivalence for the original sentence is obtained by substituting the constants back:

$$T \vdash \sigma \leftrightarrow \psi(c_1, \dots, c_n)$$

This procedure allows any such sentence to be reduced to an equivalent quantifier-free sentence, assuming the language contains at least one constant symbol.

Remark 2.17. The proof of Theorem 2.15 showed how given a formula φ , to find a quantifier-free ψ . Since the steps followed only required the axioms A_S , we have that:

$$A_S \models (\varphi \leftrightarrow \psi).$$

The quantifier elimination procedure leads to an alternative proof of the completeness of $\text{Cn } A_S$.

Corollary 2.18. $\text{Cn } A_S$ is a complete theory.

Proof. Given a sentence σ , quantifier elimination yields an equivalent quantifier-free sentence τ , so $A_S \models (\sigma \leftrightarrow \tau)$. We claim that $A_S \models \tau$ or $A_S \models \neg\tau$.

The sentence τ is constructed from atomic sentences, and these atomic sentences are of the form $S^k 0 = S^l 0$. Such an atomic sentence is deducible from A_S if $k = l$, and its negation is deducible if $k \neq l$ (by S1 and S2).

Since every atomic sentence can thus be deduced or refuted from A_S , so can any quantifier-free sentence τ . This establishes the claim that τ is decided by A_S . Consequently, as $A_S \models (\sigma \leftrightarrow \tau)$, it follows that $A_S \models \sigma$ or $A_S \models \neg\sigma$, which proves the completeness of A_S . □

2.3 Definability

Another result of the quantifier elimination process concerns the problem of definability in $\mathfrak{N}_S$. Specifically, for any formula φ whose only free variables are v_1 and v_2 , the process of quantifier elimination allows us to find a quantifier-free formula ψ that has precisely the same free variables (v_1 and v_2) such that:

$$\models_{\mathfrak{N}_S} \forall v_1 \forall v_2 (\varphi \leftrightarrow \psi).$$

Thus, any relation on $\mathfrak{N}_S$ that is definable by the formula $\varphi(v_1, v_2)$ (even if φ contains quantifiers) is also definable by the corresponding quantifier-free formula $\psi(v_1, v_2)$. This principle naturally extends to formulas with any number of free variables.

With this idea in mind we can prove the following result:

Proposition 2.19. A subset of $\mathbb{N}$ is definable in $\mathfrak{N}_S$ iff either it is finite or its complement in $\mathbb{N}$ is finite².

Proof. ($\Rightarrow$) Suppose $A \subseteq \mathbb{N}$ is definable in $\mathfrak{N}_S$. This means there exists a formula $\varphi(v_1)$ such that

$$A = \{n \in \mathbb{N} \mid \mathfrak{N}_S \models \varphi(S^n 0)\}.$$

Since $\text{Th } \mathfrak{N}_S$ admits quantifier elimination, $\varphi(v_1)$ is equivalent in $\text{Th}(\mathfrak{N}_S)$ to a quantifier-free formula $\psi(v_1)$. Thus, A is defined by this quantifier-free formula $\psi(v_1)$.

We now show that the set defined by any such quantifier-free formula $\psi(v_1)$ is either finite or cofinite. Any such $\psi(v_1)$ is equivalent to one in Disjunctive Normal Form (DNF):

$$\bigvee_i \left(\bigwedge_j \lambda_{ij}(v_1) \right),$$

²Or simply cofinite.

where each $\lambda_{ij}(v_1)$ is a literal.

Each literal is built from an atomic formula. Atomic formulas in $\mathfrak{N}_S$ with v_1 as the only free variable are equations of the form $S^k v_1 = S^l v_1$ or $S^k v_1 = S^m 0$.

An equation $S^k v_1 = S^l v_1$ defines $\mathbb{N}$ if $k = l$, or $\emptyset$ if $k \neq l$ (by repeated use of S2 and then S4.j). An equation $S^k v_1 = S^m 0$ defines $\emptyset$ if $k > m$ (by S2 and S1), or a singleton set $\{S^{m-k} 0\}$ if $k \leq m$ (by S2). In all instances, an atomic formula and therefore also its negation (a literal) defines either a finite or a cofinite set.

A conjunction $\bigwedge_j \lambda_{ij}(v_1)$ represents an intersection of finitely many sets, each defined by a literal. Since each literal defines a finite or cofinite set, if any of these sets in the intersection is finite, the entire intersection is finite. If all sets in the intersection are cofinite, their intersection is also cofinite. Thus, each conjunction $\bigwedge_j \lambda_{ij}(v_1)$ defines a set that is either finite or cofinite.

Going back to the DNF structure $\bigvee_i (\bigwedge_j \lambda_{ij}(v_1))$, this represents a union of sets, each defined by a conjunction. If all sets forming this union are finite, then the set A (defined by $\psi(v_1)$) is finite. If at least one set in the union is cofinite, then the set A is cofinite. Therefore, any set A definable in $\mathfrak{N}_S$ is either finite or cofinite.

($\Leftarrow$) Suppose $A \subseteq \mathbb{N}$ is finite or its complement A^c is finite. We consider two cases:

Case 1: A is finite.

If $A = \emptyset$, it can be defined by the quantifier-free formula $Sv_1 = v_1$, which is false in $\mathfrak{N}_S$ by S4.1.

If $A = \{k_1, k_2, \dots, k_m\}$ for some $m \geq 1$, where each $k_i \in \mathbb{N}$, then A is defined by the quantifier-free formula:

$$(v_1 = S^{k_1} 0) \vee (v_1 = S^{k_2} 0) \vee \dots \vee (v_1 = S^{k_m} 0).$$

This formula uses only allowed symbols from the language of $\mathfrak{N}_S$ and is quantifier-free. Thus, any finite set A is definable in $\mathfrak{N}_S$.

Case 2: A^c is finite (i.e., A is cofinite).

If $A^c = \emptyset$, then $A = \mathbb{N}$. This can be defined by the quantifier-free formula $v_1 = v_1$.

If $A^c = \{k_1, k_2, \dots, k_m\}$ for some $m \geq 1$, then $A = \mathbb{N} \setminus \{k_1, \dots, k_m\}$. This set A is defined by the quantifier-free formula:

$$(v_1 \neq S^{k_1} 0) \wedge (v_1 \neq S^{k_2} 0) \wedge \dots \wedge (v_1 \neq S^{k_m} 0).$$

Each $v_1 \neq t$ is the negation of an atomic formula, $\neg(v_1 = t)$, and is thus a quantifier-free literal. The entire formula is therefore quantifier-free in the language of $\mathfrak{N}_S$. Thus, any cofinite set A is definable in $\mathfrak{N}_S$.

In both scenarios, A is definable in $\mathfrak{N}_S$.

□

The following result motivates the next chapter: we will demonstrate that the ordering relation $<$ is not definable in $\mathfrak{N}_S$. To proceed, we begin with two definitions and a lemma.

Definition 2.20. A relation $L \subseteq \mathbb{N} \times \mathbb{N}$ is called a *line* if it is the set of points $\langle v_1, v_2 \rangle$ satisfying an atomic formula of one of the following forms, where $k, m, c \in \mathbb{N}$:

1. $v_1 = S^c 0$ (a *vertical line*).
2. $v_2 = S^c 0$ (a *horizontal line*).
3. $S^k v_1 = S^m v_2$ (a *diagonal line*).

Definition 2.21. A relation $R \subseteq \mathbb{N} \times \mathbb{N}$ is *linear* if it can be covered by a finite number of lines. We call a relation R *colinear* if its complement, $(\mathbb{N} \times \mathbb{N}) \setminus R$, is a linear relation.

Lemma 2.22. Any relation $R \subseteq \mathbb{N} \times \mathbb{N}$ definable in $\mathfrak{N}_S$ is either linear or colinear.

Proof. By quantifier elimination, any definable relation in $\mathfrak{N}_S$ is defined by a quantifier-free formula $\varphi(v_1, v_2)$, which we may assume is written in disjunctive normal form: $\varphi \equiv \bigvee_i \bigwedge_j \lambda_{ij}$, where each λ_{ij} is a literal.

Atomic formulas in $\mathfrak{N}_S$ are of the form $S^m t = S^n u$ for $t, u \in \{v_1, v_2, 0\}$. The sets defined by such formulas are either lines, the empty set, or the full set $\mathbb{N} \times \mathbb{N}$. The complement of a line is colinear, the complement of the full set is the empty set (linear), and the complement of the empty set is the full set (colinear). It follows that each literal λ_{ij} defines either a linear or colinear set.

Consider now a conjunction $C_i = \bigwedge_j \lambda_{ij}$. If any literal in the conjunction defines a line, then the whole conjunction defines a subset of that line and is therefore linear. If all literals define colinear sets, then each is either the full set or the complement of a line, and so their intersection is the complement of a finite union of lines, which is colinear. Thus, every conjunction C_i defines a linear or colinear set.

Finally, since φ is a disjunction of such conjunctions, the set it defines is a finite union of linear or colinear sets. If all disjuncts define linear sets, then their union is linear. Otherwise, if any disjunct is colinear, then the complement of the relation is contained in the complement of that disjunct, which is linear, and so the relation itself is colinear. □

Now we can prove our result of interest:

Proposition 2.23. The ordering relation $R_{<} = \{\langle v_1, v_2 \rangle \mid v_1 < v_2 \text{ in } \mathbb{N}\}$ is not definable in the structure $\mathfrak{N}_S$.

Proof. By the preceding lemma, any relation definable in $\mathfrak{N}_5$ is either linear or colinear. The relation $R_<$ is neither.

Assume $R_<$ is linear, and let n be the least number such that the line $v_1 = n$ is not part of the covering. Then there are infinitely many elements $\langle v_1, v_2 \rangle \in R_<$ with $v_1 = n$, but only finitely many of them can be covered by the finitely many remaining lines. So $R_<$ is not linear.

Assume $R_<$ is colinear. Then its complement $R_<^c = \{\langle v_1, v_2 \rangle \mid v_1 \geq v_2\}$ is linear. By the same argument, there is some n such that the line $v_2 = n$ is not covered, and then infinitely many elements of $R_<^c$ lie on that line, contradicting linearity.

Therefore, $R_<$ is neither linear nor colinear, and thus not definable in $\mathfrak{N}_5$.

□

Chapter 3

Natural Numbers with Order

3.1 Theory of $\mathfrak{N}_L$ and axiomatization

We are now going to expand the language from the previous chapter by introducing the ordering symbol $<$. As a result, our structure will be defined as

$$\mathfrak{N}_L = (\mathbb{N}; 0, S, <)$$

We want to prove that the theory of the structure $\text{Th } \mathfrak{N}_L$ is also decidable. To do this, we will provide an axiomatization of the theory and show that the set of its consequences allows for the elimination of quantifiers, which will, in turn, enable the proof of decidability and other corollaries.

To simplify notation, we will write $x \leq y$ as an abbreviation for $(x < y \vee x = y)$. $x \not< y$ abbreviates the negation of $x < y$, and $x \not\leq y$ that of $x \leq y$.

Since $<$ denotes the usual strict ordering relation on $\mathbb{N}$, we can metatheoretically extract some of its fundamental properties: the relation is total, transitive, and has a least element (0). Based on these observations, we now introduce a set of axioms to formally characterize the structure. Other properties of $<$, such as irreflexivity, will be derived as consequences of this axiomatization. The set of axioms for $\text{Th } \mathfrak{N}_L$, denoted A_L , consists of the following sentences:

$$\forall y \quad (y \neq 0 \rightarrow \exists x (y = Sx)) \quad (\text{S3})$$

$$\forall x \forall y \quad (x < Sy \leftrightarrow x \leq y) \quad (\text{L1})$$

$$\forall x \quad (x \not< 0) \quad (\text{L2})$$

$$\forall x \forall y \quad (x < y \vee x = y \vee y < x) \quad (\text{L3})$$

$$\forall x \forall y \quad (x < y \rightarrow y \not< x) \quad (\text{L4})$$

$$\forall x \forall y \forall z \quad (x < y \wedge y < z \rightarrow x < z) \quad (\text{L5})$$

It is obvious that they are all true in $\mathfrak{N}_L$, thus we have $\text{Cn } A_L \subseteq \text{Th } \mathfrak{N}_L$. Before proceeding to prove that A_L admits elimination of quantifiers, we will first

examine some useful consequences.

Lemma 3.1 (Irreflexivity). $\forall x \, x \not< x$

Proof. We will prove this by contradiction. Suppose $x < x$. Then, by L4, which states $\forall x \, \forall y \, (x < y \rightarrow y \not< x)$, we have $x \not< x$. But this implies both $x < x$ and $x \not< x$, a contradiction. Therefore, our assumption must be false, and $x \not< x$. $\square$

Lemma 3.2. $\forall x \, x < Sx$

Proof. If we take $y := x$ in L1, we get $x < Sx \leftrightarrow x \leq x$. Since in fact $x = x$, this implies that $x < Sx$. $\square$

Lemma 3.3. $\forall x \, \forall y \, (x \not< y \leftrightarrow y \leq x)$

Proof. ($\rightarrow$) Suppose $x \not< y$. Then, by L3, we have $x = y \vee y < x$, which is the equivalent of $y \leq x$.

($\leftarrow$) Suppose $y \leq x$. We proceed by contradiction: assume also that $x < y$.

By L4, it follows that $y \not< x$. But since $y \leq x$, by definition we have $y < x$ or $y = x$, so we must have $y = x$.

Substituting this into our assumption $x < y$, we obtain $x < x$, which contradicts Lemma 3.1. Therefore, our assumption must be false, and it follows that $x \not< y$. $\square$

Lemma 3.4. $\forall x \, \forall y \, (x < y \leftrightarrow Sx < Sy)$

Proof.

$$\begin{aligned} x < y &\leftrightarrow y \not\leq x \quad (\text{by Lemma 3.3}) \\ &\leftrightarrow y \not< Sx \quad (\text{by L1}) \\ &\leftrightarrow Sx \leq y \quad (\text{by Lemma 3.3}) \\ &\leftrightarrow Sx < Sy \quad (\text{by L1}) \end{aligned}$$

$\square$

Lemma 3.5. (a) $\forall x \, (Sx \neq 0)$ (S1)

(b) $\forall x \, \forall y \, (Sx = Sy \rightarrow x = y)$ (S2)

(c) $\forall x \, (S^n x \neq x)$ (S4.n for $n = 1, 2, \dots$)

Proof. (a) We prove this by contradiction. For any arbitrary x , suppose $Sx = 0$.

From Lemma 3.2, we have $\forall x (x < Sx)$, so substituting $Sx = 0$, we obtain $x < 0$.

But this contradicts L2: $\forall x (x \not< 0)$. Hence, our assumption is false, and we conclude $Sx \neq 0$.

(b) Assume $Sx = Sy$, we want to prove $x = y$. Suppose for contradiction that $x \neq y$. By Lemma 3.3, we then have either $x < y$ or $y < x$.

If $x < y$, then by Lemma 3.4, $Sx < Sy$. But since $Sx = Sy$, this implies $Sx < Sx$, which contradicts Lemma 3.1.

If $y < x$, then $Sy < Sx$, and again $Sx = Sy$ leads to $Sx < Sx$, contradicting Lemma 3.1.

In both cases we reach a contradiction; therefore, we can conclude that $x = y$.

(c) For an arbitrary x , we proceed by induction on n .

Base case: $n = 1$. We must prove $Sx \neq x$. From Lemma 3.2, we have $x < Sx$, and by Lemma 3.1, $x \not< x$. Therefore, $Sx \neq x$, as desired.

Inductive Step: Assume the inductive hypothesis: $S^n x \neq x$.

By using $x < Sx$ and transitivity (by L5) it is always correct to state $x < S^n x$.

We must prove:

$$S^{n+1}x \neq x$$

From the inductive hypothesis and Lemma 3.2, we have:

$$x < S^n x \quad \text{and} \quad S^n x < S^{n+1}x$$

Then by transitivity of $<$ (by L5), it follows that:

$$x < S^{n+1}x$$

And since $x < x$ is false by Lemma 3.1, we conclude:

$$S^{n+1}x \neq x$$

□

Remark 3.6. Lemma 3.5 shows that the set of axioms for Th $\mathfrak{N}_L$ can be derived from the axioms of A_S . Consequently, every model $\mathfrak{A}$ of A_L satisfies the axioms of A_S when the order relation $<^{\mathfrak{A}}$ is disregarded. Thus, its domain includes a

standard initial segment isomorphic to $\mathbb{N}$, possibly accompanied by additional components, each forming a copy of $\mathbb{Z}$, that is, $\mathbb{Z}$ -chains.

As we already saw in the previous chapter, in the setting of models of A_S , these $\mathbb{Z}$ -chains are unordered among themselves, since they are disjoint and the theory does not specify a relation between elements of different chains. However, when the full language of A_L is considered, including the order symbol, this changes: the order $<^{\mathfrak{M}}$ being total implies that, for any two distinct elements in the model, their relative order is determined. As a result, the $\mathbb{Z}$ -chains within the model become linearly arranged, even though their internal structure remains that of the integers.

3.2 Quantifier elimination and decidability

We will follow an analogous process to the previous chapter in order to prove the decidability of $\mathfrak{N}_L$.

Theorem 3.7. The theory $\text{Cn } A_L$ admits elimination of quantifiers.

Proof. We will do a similar proof to the one seen in Theorem 2.14. Consider a formula

$$\exists x(\beta_0 \wedge \cdots \wedge \beta_k),$$

where each β_i is atomic or the negation of an atomic formula.

The terms are, as in the previous chapter, of the form $S^k u$, where u is either 0 or a variable. There are two possible atomic formulas:

$$S^k u = S^\ell t \quad \text{and} \quad S^k u < S^\ell t.$$

Replace $t_1 \not< t_2$ by $t_2 < t_1 \vee t_1 = t_2$ (by L3), and replace $t_1 \neq t_2$ by $t_1 < t_2 \vee t_2 < t_1$ (by L4).

By regrouping the atomic formulas and using the equivalence

$$\exists x(\varphi \wedge \psi) \equiv \exists x\varphi \wedge \exists x\psi,$$

we may rewrite the formula as

$$\exists x(\alpha_0 \wedge \cdots \wedge \alpha_q),$$

where each α_i is atomic.

We may assume the variable x occurs in each α_i . Otherwise, use

$$\exists x(\alpha \wedge \beta) \equiv \alpha \wedge \exists x\beta.$$

Also assume x appears on only one side of each α_i . For $S^k x = S^\ell x$, the formula is equivalent to:

$$0 = 0 \quad \text{if } k = \ell, \quad \text{and} \quad 0 \neq 0 \quad \text{otherwise,}$$

since if $k \neq \ell$, we would have $S^m x = x$ for some $m \geq 1$, contradicting S4.m. For $S^k x < S^\ell x$, we replace the formula by

$$0 = 0 \quad \text{if } k < \ell, \quad \text{and} \quad 0 \neq 0 \quad \text{otherwise,}$$

justified by L1 and L4.

Case 1: Suppose some α_i is an equality. Then we proceed as in Case 2 of the quantifier-elimination proof of Theorem 2.14.

Case 2: Otherwise, each α_i is an inequality. Then the formula becomes

$$\exists x \left(\bigwedge_i t_i < S^{m_i} x \wedge \bigwedge_j S^{n_j} x < u_j \right).$$

If there are no upper bounds (i.e., the second conjunction is empty), then we replace the formula by

$$0 = 0,$$

because any sufficiently large x satisfies the inequalities (using S3: the domain is infinite).

If there are no lower bounds (i.e., the first conjunction is empty), then we replace the formula by

$$\bigwedge_j S^{n_j} 0 < u_j,$$

asserting that zero satisfies all upper bounds (as ensured by L2 and L4).

Otherwise, we proceed with the following transformations:

$$\exists x \bigwedge_{i,j} (t_i < S^{m_i} x \wedge S^{n_j} x < u_j); \tag{1}$$

$$\exists x \bigwedge_{i,j} (S^{n_j} t_i < S^{m_i+n_j} x < S^{m_i} u_j); \tag{2}$$

$$\left(\bigwedge_{i,j} S^{n_j+1} t_i < S^{m_i} u_j \right) \wedge \bigwedge_j S^{n_j} 0 < u_j. \tag{3}$$

The transition from (1) to (2) uses that the successor function S is strictly increasing (by L1). Applying S^{n_j} to $t_i < S^{m_i} x$ gives $S^{n_j} t_i < S^{m_i+n_j} x$, and applying S^{m_i} to $S^{n_j} x < u_j$ gives $S^{m_i+n_j} x < S^{m_i} u_j$.

The transition from (2) to (3) asserts that for a value of x to exist between all the lower and upper bounds, there must be a gap:

$$S^{n_i+1} t_i < S^{m_i} u_j,$$

which again relies on the fact that S is discrete and strictly increasing (axioms L1 and L5).

Additionally, we require that

$$S^{n_j} 0 < u_j,$$

so that x is not forced below zero (using L2 and L4).

Thus, in each case, we reduce the formula to a quantifier-free equivalent. $\square$

The above theorem has some key results.

Corollary 3.8. $\text{Cn } A_L$ is a complete theory.

Proof. Let σ be a sentence in the language of A_L . Since $\text{Cn } A_L$ admits elimination of quantifiers, there exists a quantifier-free sentence τ such that

$$A_L \models (\sigma \leftrightarrow \tau),$$

(as in Remark 2.17). We claim that either $A_L \models \tau$ or $A_L \models \neg\tau$.

The sentence τ is a combination of atomic sentences of the form $S^k 0 = S^\ell 0$ or $S^k 0 < S^\ell 0$.

Consider first the case of $S^k 0 = S^\ell 0$. As in Corollary 2.18, such a sentence is deducible from A_L if $k = \ell$, and its negation is deducible if $k \neq \ell$, because the axioms S1 and S2 used in that proof are derivable from A_L (see Lemma 3.5).

Now consider atomic sentences of the form $S^k 0 < S^\ell 0$. If $k < \ell$, then $\ell = k + j$ for some $j \geq 1$. Repeated application of Lemma 3.2 ($\forall x(x < Sx)$) and L5 transitivity of $<$) yields

$$A_L \models S^k 0 < S^{k+1} 0 < \dots < S^{k+j} 0 = S^\ell 0,$$

so $A_L \models S^k 0 < S^\ell 0$.

If $k = \ell$, then the sentence becomes $S^k 0 < S^k 0$, which is false by irreflexivity (Lemma 3.1), derivable from A_L . Hence,

$$A_L \models \neg(S^k 0 < S^k 0).$$

If $k > \ell$, then $A_L \models S^\ell 0 < S^k 0$, by the previous case with k and ℓ swapped. By L4 ($\forall x \forall y (x < y \rightarrow \neg(y < x))$), it follows that

$$A_L \models \neg(S^k 0 < S^\ell 0).$$

Therefore, every atomic sentence of either form is decided by A_L , and since τ is a Boolean combination of such atomic sentences, τ is decided by A_L as well:

$$A_L \models \tau \quad \text{or} \quad A_L \models \neg\tau.$$

From $A_L \models (\sigma \leftrightarrow \tau)$, we conclude that

$$A_L \models \sigma \quad \text{or} \quad A_L \models \neg\sigma,$$

which proves the completeness of A_L . □

Following the exact same process as in the proof of Corollary 2.10

Corollary 3.9. $\text{Cn } A_L = \text{Th } \mathfrak{N}_L$

Since any complete, axiomatizable theory is decidable, this leads us directly to the result of interest.

Corollary 3.10. $\text{Th } \mathfrak{N}_L$ is decidable .

Similarly to the previous chapter, we have:

Corollary 3.11. A subset $A \subseteq \mathbb{N}$ is definable in $\mathfrak{N}_L$ iff it is finite or cofinite.

Proof. Let $A \subseteq \mathbb{N}$. We use the fact that $\text{Th } \mathfrak{N}_L$ admits quantifier elimination. Thus, any formula $\varphi(v_1)$ defining A is equivalent to a quantifier-free formula $\psi(v_1)$, which can be taken to be in Disjunctive Normal Form (DNF):

$$\bigvee_i \left(\bigwedge_j \lambda_{ij}(v_1) \right),$$

where each $\lambda_{ij}(v_1)$ is a literal.

($\Rightarrow$) Suppose A is definable in $\mathfrak{N}_L$. Then A is defined by such a quantifier-free DNF $\psi(v_1)$. The atomic formulas in the language of $\mathfrak{N}_L$ involving v_1 are of the form $S^k v_1 = S^m 0$, $S^k v_1 = S^l v_1$, $S^k v_1 < S^m 0$, $S^m 0 < S^k v_1$, or $S^k v_1 < S^l v_1$.

Each such atomic formula, and thus each literal, defines a subset of $\mathbb{N}$ that is either finite or cofinite. For instance, $S^k v_1 = S^m 0$ defines at most a singleton (finite); $S^k v_1 < S^m 0$ defines a finite initial segment of $\mathbb{N}$ (i.e., a set of the form $\{0, 1, \dots, c\}$, possibly empty); and $S^m 0 < S^k v_1$ defines a cofinite final segment of $\mathbb{N}$ (i.e., a set of the form $\{c, c+1, \dots\}$, possibly $\mathbb{N}$ itself). Formulas like $S^k v_1 = S^l v_1$ or $S^k v_1 < S^l v_1$ resolve to define either $\mathbb{N}$ (cofinite) or $\emptyset$ (finite), respectively.

A conjunction of literals corresponds to an intersection of the finite or cofinite sets defined by these literals. Such an intersection is finite if any component set

is finite; if all component sets are cofinite, their intersection is also cofinite. Thus, each conjunction defines a finite or cofinite set.

The DNF formula $\psi(v_1)$ is a disjunction of these conjunctions. This corresponds to a union of the finite or cofinite sets defined by each conjunction. Such a union is finite if all component sets are finite; if at least one component set is cofinite, the union is also cofinite. Consequently, the set defined by $\psi(v_1)$ is finite or cofinite. Therefore, if A is definable in $\mathfrak{N}_L$, it is either finite or cofinite.

($\Leftarrow$) Conversely, suppose $A \subseteq \mathbb{N}$ is either finite or cofinite. We consider two cases:

Case 1: A is finite.

If $A = \emptyset$, it can be defined by the quantifier-free formula $v_1 \neq v_1$ (or $Sv_1 < v_1$).

If $A = \{k_1, k_2, \dots, k_p\}$ for some $p \geq 1$, where each $k_i \in \mathbb{N}$, then A is defined by the quantifier-free formula:

$$(v_1 = S^{k_1}0) \vee (v_1 = S^{k_2}0) \vee \dots \vee (v_1 = S^{k_p}0).$$

This formula is in the language of $\mathfrak{N}_L$. Thus, any finite set A is definable.

Case 2: A^c is finite.

If $A^c = \emptyset$, then $A = \mathbb{N}$. This can be defined by the quantifier-free formula $v_1 = v_1$.

If $A^c = \{k_1, k_2, \dots, k_p\}$ for some $p \geq 1$, then $A = \mathbb{N} \setminus \{k_1, \dots, k_p\}$. This set A is defined by the quantifier-free formula:

$$(v_1 \neq S^{k_1}0) \wedge (v_1 \neq S^{k_2}0) \wedge \dots \wedge (v_1 \neq S^{k_p}0).$$

Each $v_1 \neq t$ is a literal. The entire formula is therefore quantifier-free in the language of $\mathfrak{N}_L$. Thus, any cofinite set A is definable.

In all these cases, A is definable by a quantifier-free formula in the language of $\mathfrak{N}_L$. Thus, any finite or cofinite subset of $\mathbb{N}$ is definable in $\mathfrak{N}_L$. □

To conclude this chapter, we present the following result, which serves as motivation for what comes next.

Corollary 3.12. The addition relation, $\{\langle m, n, p \rangle \mid m + n = p\}$, is not definable in $\mathfrak{N}_L$.

Proof. If addition were definable, then the property of x being even, defined by the formula

$$\varphi(x) = \exists y(x = y + y),$$

would also be definable in the language of $\mathfrak{N}_L$.

This would imply that the set of even numbers is definable in $\mathfrak{N}_L$. However, this set is neither finite nor cofinite, which contradicts the previous corollary.

□

Chapter 4

Natural Numbers with Addition

4.1 Theory of $\mathfrak{N}_A$ and axiomatization

Now we will augment the language of the previous chapter by the addition symbol $+$, therefore our structure will be

$$\mathfrak{N}_A = (\mathbb{N}; 0, S, <, +)$$

We will prove that the first-order is decidable, but first we will give a convenient axiomatization of the theory and some useful consequences for later on.

The axioms of $\text{Th } \mathfrak{N}_A$ will be a set A_A including the axioms of A_L and some new axioms for the addition.

$$\begin{array}{lll} \forall y & (y \neq 0 \rightarrow \exists x (y = Sx)) & (\text{S3}) \\ \forall x \forall y & (x < Sy \leftrightarrow x \leq y) & (\text{L1}) \\ \forall x & (x \not< 0) & (\text{L2}) \\ \forall x \forall y & (x < y \vee x = y \vee y < x) & (\text{L3}) \\ \forall x \forall y & (x < y \rightarrow y \not< x) & (\text{L4}) \\ \forall x \forall y \forall z & (x < y \wedge y < z \rightarrow x < z) & (\text{L5}) \\ \forall x & (x + 0 = x) & (\text{A1}) \\ \forall x \forall y & (x + Sy = S(x + y)) & (\text{A2}) \end{array}$$

And for every formula $\varphi(x, x_1, \dots, x_k)$:

$$\begin{aligned} \forall x_1, \dots, x_k \Big(\Big(\varphi(0, x_1, \dots, x_k) \wedge \forall x (\varphi(x, x_1, \dots, x_k) \rightarrow \varphi(Sx, x_1, \dots, x_k)) \Big) \rightarrow \\ \rightarrow \forall x \varphi(x, x_1, \dots, x_k) \Big) \end{aligned} \quad (\text{A3})$$

Observe that A3 corresponds to the *Induction Axiom* and actually refers to an infinite amount of axioms. Now we will move on to proving some useful results.

Lemma 4.1 (Associativity). $\forall x \forall y \forall z ((x + y) + z = x + (y + z))$

Proof. We will prove the statement by induction on z .

Base Case: $z = 0$

$$x + (y + 0) = x + y = (x + y) + 0 \quad (\text{by A1})$$

Inductive Hypothesis: Assume $(x + y) + z' = x + (y + z')$ for some z' . We will prove that $(x + y) + Sz' = x + (y + Sz')$:

$$\begin{aligned} (x + y) + Sz' &= S((x + y) + z') && (\text{by A2}) \\ S((x + y) + z') &= S(x + (y + z')) && (\text{by IH}) \\ S(x + (y + z')) &= x + S(y + z') = x + (y + Sz') && (\text{by A2}) \end{aligned}$$

□

Lemma 4.2. *The following statements hold:*

1. $\forall x (0 + x = x)$
2. $\forall x \forall y (S(x) + y = S(x + y))$

Proof. (1) We prove $0 + x = x$ by induction on x . *Base Case* ($x = 0$): $0 + 0 = 0$, which is true by A1.

Inductive Step: Assume $0 + x = x$. We must show $0 + S(x) = S(x)$.

$$\begin{aligned} 0 + S(x) &= S(0 + x) \quad (\text{by A2}) \\ &= S(x) \quad (\text{by IH}) \end{aligned}$$

(2) We prove $S(x) + y = S(x + y)$ by induction on y .

Base Case ($y = 0$): We must show $S(x) + 0 = S(x + 0)$. By axiom A1, the left side is $S(x)$ and the right side is $S(x)$. The identity holds.

Inductive Step: Assume $S(x) + y = S(x + y)$. We must show $S(x) + S(y) = S(x + S(y))$.

$$\begin{aligned} S(x) + S(y) &= S(S(x) + y) \quad (\text{by A2}) \\ &= S(S(x + y)) \quad (\text{by IH}) \\ &= S(x + S(y)) \quad (\text{by A2}) \end{aligned}$$

□

Lemma 4.3 (Commutativity). $\forall x \forall y (x + y = y + x)$

Proof. We use the results from Lemma 4.2. The proof is by induction on y .

Base Case ($y = 0$): We must show $x + 0 = 0 + x$. By axiom (A1), we have $x + 0 = x$. By Lemma 4.2(a), we have $0 + x = x$. Thus, $x + 0 = 0 + x$.

Inductive Step: Assume $x + y = y + x$ for some y . We must prove that $x + S(y) = S(y) + x$.

$$\begin{aligned} x + S(y) &= S(x + y) \quad (\text{by A2}) \\ &= S(y + x) \quad (\text{by IH}) \\ &= S(y) + x \quad (\text{by Lemma 4.2(b)}) \end{aligned}$$

This completes the proof. □

Remark 4.4. From now on we will freely use both commutativity and associativity since in future demonstrations there will be parenthesis eliminations and more general commutativity that can be easily proved by these.

Lemma 4.5. $\forall x \forall y \forall z (x < y \leftrightarrow x + z < y + z)$

Proof. We will prove the statement by induction on z .

Base Case: $z = 0$

$$x < y \leftrightarrow x + 0 < y + 0$$

By A1, we have:

$$x + 0 = x \quad \text{and} \quad y + 0 = y$$

Thus, the statement becomes $x < y \leftrightarrow x < y$, which is trivially true.

Inductive Hypothesis: Assume that for some z' , $\forall x \forall y (x < y \leftrightarrow x + z' < y + z')$.

We will prove that $\forall x \forall y, (x < y \leftrightarrow x + Sz' < y + Sz')$

($\rightarrow$) Assume $x < y$. By the Inductive Hypothesis, $x + z' < y + z'$.

$$\begin{aligned} x + Sz' &= S(x + z') \quad \text{and} \quad y + Sz' = S(y + z') && (\text{by A2}) \\ x + z' < y + z' &\rightarrow S(x + z') < S(y + z') && (a < b \leftrightarrow S(a) < S(b)) \end{aligned}$$

Thus:

$$x + Sz' = S(x + z') < S(y + z') = y + Sz' \rightarrow x + Sz' < y + Sz'$$

($\leftarrow$) Assume $x + Sz' < y + Sz'$.

$$\begin{aligned} S(x + z') &= x + Sz' < y + Sz' = S(y + z') && (\text{by A2}) \\ S(x + z') < S(y + z') &\rightarrow x + z' < y + z' && (a < b \leftrightarrow S(a) < S(b)) \end{aligned}$$

By the Inductive Hypothesis $x + z' < y + z' \rightarrow x < y$ □

Lemma 4.6. $\forall x \forall y \forall z (x = y \leftrightarrow x + z = y + z)$.

Proof. We prove both directions of the biconditional.

($\rightarrow$) Assume $x = y$. We can replace x with y in the term $x + z$ to obtain $y + z$. Thus, $x + z = y + z$.

($\leftarrow$) Assume $x + z = y + z$. We will prove $x = y$ by contradiction. Assume for the sake of contradiction that $x \neq y$. By the L3, if $x \neq y$, then either $x < y$ or $y < x$.

1. If $x < y$, then by Lemma 4.5, we must have $x + z < y + z$. This contradicts our initial assumption that $x + z = y + z$.
2. If $y < x$, then by Lemma 4.5, we must have $y + z < x + z$. This also contradicts our initial assumption that $x + z = y + z$.

Therefore, we conclude that $x = y$. □

Definition 4.7. Let t be a term in our language and $n \in \mathbb{N}$, $nt = t + \dots + t$.

Lemma 4.8. $\forall x \forall y (x = y \leftrightarrow x + x = y + y)$

Proof. ($\rightarrow$) Assume $x = y$. Then, by the logical principle of substitutivity of equality, we may replace one side with the other in any expression. Applying this to $x + x$, we get:

$$x + x = y + y$$

($\leftarrow$) Assume $x + x = y + y$.

We want to show that $x = y$. Suppose $x \neq y$.

Without loss of generality, assume $x < y$ (the case $y < x$ is symmetric).

$$\begin{aligned} x + x &< y + x \text{ and } y + x < y + y && \text{(by Lemma 4.5)} \\ x + x &< y + y && \text{(by L5)} \end{aligned}$$

This contradicts the assumption that $x + x = y + y$. Therefore, $x \neq y$ leads to a contradiction, and we conclude $x = y$. □

Corollary 4.9. Let $n \in \mathbb{N}$, then $\forall x \forall y (x = y \leftrightarrow nx = ny)$.

Lemma 4.10. $\forall x \forall y (x < y \leftrightarrow x + x < y + y)$

Proof. ($\rightarrow$) Assume $x < y$.

$$\begin{aligned} x + x &< y + x \text{ and } y + x < y + y && \text{(by Lemma 4.5)} \\ x + x &< y + y && \text{(by L5)} \end{aligned}$$

($\leftarrow$) Assume $x + x < y + y$.

We want to show $x < y$. Suppose for contradiction that $x \not< y$. By L3, either $x = y$ or $y < x$.

If $x = y$, then $x + x = y + y$ by Lemma 4.8. This contradicts $x + x < y + y$.

If $y < x$:

$$\begin{aligned} y + y &< x + y \text{ and } x + y < x + x && \text{(by Lemma 4.5)} \\ y + y &< x + x && \text{(by L5)} \end{aligned}$$

Contradicting $x + x < y + y$.

Thus, both cases lead to contradictions, so $x \not< y$ is false, and we conclude $x < y$. □

Corollary 4.11. Let $n \in \mathbb{N}$, then $\forall x \forall y (x < y \leftrightarrow nx < ny)$.

Lemma 4.12. For any natural numbers a and b

$$S^a 0 + S^b 0 = S^{a+b} 0.$$

Proof. The proof is by induction on b .

Base Case: For $b = 0$, the left-hand side is $S^a 0 + S^0 0 = S^a 0 + 0$, which equals $S^a 0$ by axiom (A1). The right-hand side is $S^{a+0} 0 = S^a 0$, so the equality holds.

Inductive Step: Assume the property holds for b . We then prove it for $S(b)$:

$$\begin{aligned} S^a 0 + S^{b+1} 0 &= S^a 0 + S(S^b 0) \\ &= S(S^a 0 + S^b 0) && \text{(by A2)} \\ &= S(S^{a+b} 0) && \text{(by IH)} \\ &= S^{a+(b+1)} 0. \end{aligned}$$

The result follows by the principle of induction. □

Lemma 4.13 (Division with remainder). Given $n \neq 0$, $\forall x \exists y (x = ny \vee x = ny + S^0 0 \vee \dots \vee x = ny + S^{n-1} 0)$.

Proof. The proof is by induction on x .

Base Case: For $x = 0$, we choose $y = 0$. We have $n0 = 0$ by A1. Thus the disjunct $x = ny$ becomes $0 = 0$, which is true.

Inductive Step: Assume the lemma holds for x , so $x = ny + S^r 0$ for some y and some integer r with $0 \leq r < n$. We show the property holds for $S(x)$.

- If $r < n - 1$, then $S(x) = S(ny + S^r 0) = ny + S^{r+1} 0$ by A2. The property holds with the same quotient y and a new remainder $r + 1$.

- If $r = n - 1$, then $S(x) = S(ny + S^{n-1}0) = ny + S^n 0 = ny + nS^1 0$. Using the previous lemma repeatedly. Now, $ny + nS^1 0 = n(y + S^1 0) = nS(y)$, by notation and use of A2. The property holds with quotient $S(y)$ and a new remainder of 0.

In both cases, the property holds for $S(x)$, which completes the induction. $\square$

Lemma 4.14. Given a term $t = t(x_1, \dots, x_k)$, there exist $n_0, n_1, \dots, n_k \in \mathbb{N}$ such that

$$A_A \vdash t = S^{n_0}0 + n_1x_1 + \dots + n_kx_k.$$

Proof. We will prove the statement by induction on t .

Base Case: $t = 0$ and $t = x_i$

Trivially, for $t = 0$ we take $n_i = 0$ for every n_i . And for $t = x_i$ we take $n_0 = 0$, $n_i = 1$, $n_j = 0$ where $1 \leq j < i$ and $i + 1 \leq j \leq k$.

Case St:

Inductive Hypothesis: Assume $t = S^{n_0}0 + n_1x_1 + \dots + n_kx_k$. We will prove that St can be expressed in the same form.

$$St = S(S^{n_0}0 + n_1x_1 + \dots + n_kx_k) \stackrel{\text{by A2}}{=} S^{n_0+1}0 + n_1x_1 + \dots + n_kx_k$$

Case $t + t'$:

Inductive Hypothesis: Assume $t = S^{n_0}0 + n_1x_1 + \dots + n_kx_k$ and $t' = S^{n'_0}0 + n'_1x_1 + \dots + n'_kx_k$. We will prove that $t + t'$ can be expressed in the same form.

$$t + t' = (S^{n_0}0 + n_1x_1 + \dots + n_kx_k) + (S^{n'_0}0 + n'_1x_1 + \dots + n'_kx_k) = S^{n_0+n'_0}0 + (n_1 + n'_1)x_1 + \dots + (n_k + n'_k)x_k, \text{ by Lemmas 4.1 \& 4.3.}$$

$\square$

4.2 Presburger Theorem

For any $n \in \mathbb{N}$ and any variable z , we define the term nz as an abbreviation for repeated addition:

$$nz = \underbrace{z + z + \dots + z}_{n \text{ times}}$$

By convention, if $n = 0$, we define $0z = 0$.

Definition 4.15. We define the following equivalence relation

$$x \equiv_n y \leftrightarrow \exists z (x + nz = y) \vee \exists z (x = y + nz)$$

Remark 4.16. From now on L_A^+ will refer to the expanded language of L_A : $L_A \cup \{\equiv_n \mid n > 1\}$. The notation $A_A + \{\equiv_n\}$ will refer to the set formed by the union of the axioms A_A and the definition of $\equiv_n$.

Lemma 4.17. $\forall x \forall y (\neg x \equiv_n y \leftrightarrow x \equiv_n y + S0 \vee x \equiv_n y + S^2 0 \vee \dots \vee x \equiv_n y + S^{n-1} 0)$

Proof. This statement is logically equivalent to

$$\forall x \forall y (x \equiv_n y \vee x \equiv_n y + S0 \vee x \equiv_n y + S^2 0 \vee \dots \vee x \equiv_n y + S^{n-1} 0)$$

and thus we will demonstrate the second one.

Lemma 4.13 stated that given $n \neq 0$, $\forall z \exists w (z = nw \vee z = nw + S0 \vee \dots \vee z = nw + S^{n-1} 0)$. By using the definition of $\equiv_n$, this can be converted into the following statement for $n \neq 0$:

$$\forall z (z \equiv_n 0 \vee z \equiv_n S0 \vee z \equiv_n S^2 0 \vee \dots \vee z \equiv_n S^{n-1} 0)$$

Now, for any x, y , consider $z = x - y$. Then:

$$x \equiv_n y \leftrightarrow x - y \equiv_n 0 \leftrightarrow z \equiv_n 0$$

So, applying the above result to $z = x - y$, we get:

$$x - y \equiv_n 0 \vee x - y \equiv_n S0 \vee \dots \vee x - y \equiv_n S^{n-1} 0$$

which translates to:

$$x \equiv_n y \vee x \equiv_n y + S0 \vee x \equiv_n y + S^2 0 \vee \dots \vee x \equiv_n y + S^{n-1} 0$$

This proves the equivalent form of the lemma. Hence the original statement also holds. □

Before proving the main result of this section, we must prove some results.

Lemma 4.18. If $\mathcal{M} \models A_A$, then there exists an expansion $\mathcal{M}^+$ of $\mathcal{M}$ to the language L_A^+ such that $\mathcal{M}^+ \models A_A + \{\equiv_n\}$.

Proof. Let $\mathcal{M}$ be a model of A_A . We construct the expansion $\mathcal{M}^+$ by retaining the same universe, $|\mathcal{M}|$, and the same interpretations for all symbols from the original language L_A .

For each new relation symbol $\equiv_n$ in the expanded language L_A^+ , we introduce its interpretation. We define the relation $(\equiv_n)^{\mathcal{M}^+}$ to be:

$$(\equiv_n)^{\mathcal{M}^+} := \{\langle a, b \rangle \in |\mathcal{M}|^2 \mid \mathcal{M} \models \exists z(a = b + nz) \vee \mathcal{M} \models \exists z(b = a + nz)\}$$

By this construction, the expanded structure $\mathcal{M}^+$ satisfies the definitions of all the $\equiv_n$ relations. Since $\mathcal{M}^+$ is an expansion of $\mathcal{M}$, it also remains a model of A_A . Thus, $\mathcal{M}^+ \models A_A + \{\equiv_n\}$. □

Lemma 4.19. Let $\mathcal{M}$ be a structure for the language L_A and let $\mathcal{M}^+$ be an expansion of $\mathcal{M}$ to the language L_A^+ . If φ is a sentence in the original language L_A and $\mathcal{M}^+ \models \varphi$, then $\mathcal{M} \models \varphi$.

Proof. By definition, an expansion $\mathcal{M}^+$ and its reduct $\mathcal{M}$ provide identical interpretations for all symbols in the original language L_A . Since the sentence φ is composed solely of symbols from L_A , its truth value is necessarily the same in both structures. Therefore, if φ is true in $\mathcal{M}^+$, it must also be true in $\mathcal{M}$. □

Proposition 4.20. For every sentence φ of our language L_A ,

$$A_A \models \varphi \Leftrightarrow A_A + \{\equiv_n\} \models \varphi$$

Proof. ($\Rightarrow$) Trivial. If $A_A \models \varphi$, then since A_A is a subset of $A_A + \{\equiv_n\}$, it follows immediately that $A_A + \{\equiv_n\} \models \varphi$.

($\Leftarrow$) Suppose $A_A + \{\equiv_n\} \models \varphi$. We must show that $A_A \models \varphi$. To do this, we will show that any arbitrary model of A_A must also be a model of φ .

Let $\mathcal{M}$ be any model of A_A (in the language L_A). By Lemma 4.18, because $\mathcal{M} \models A_A$, there exists an expansion $\mathcal{M}^+$ of $\mathcal{M}$ to the language L_A^+ such that $\mathcal{M}^+ \models A_A + \{\equiv_n\}$.

By our initial supposition that $A_A + \{\equiv_n\} \models \varphi$, any model of this expanded theory must satisfy φ . Therefore, we must have $\mathcal{M}^+ \models \varphi$.

Now, since φ is a sentence written purely in the original language L_A , we can apply Lemma 4.19. This lemma states that if φ is true in the expansion $\mathcal{M}^+$, then it must also be true in the reduct $\mathcal{M}$.

From $\mathcal{M}^+ \models \varphi$, we can therefore conclude that $\mathcal{M} \models \varphi$. Since we have shown that an arbitrary model $\mathcal{M}$ of A_A must also be a model of φ , we have proven that $A_A \models \varphi$. □

Lemma 4.21. The theory of $\mathfrak{N}_A$ does not admit elimination of quantifiers.

Proof. To prove this, we provide a formula in the language of $\mathfrak{N}_A$ that cannot be equivalent to any quantifier-free formula. Consider the formula $\varphi(x)$ given by:

$$\varphi(x) := \exists y(x = y + y)$$

This formula defines the set of even natural numbers. If the theory of $\mathfrak{N}_A$ admitted quantifier elimination, there would have to exist a quantifier-free formula, let's call it $\psi(x)$, that is logically equivalent to $\varphi(x)$.

A quantifier-free formula is a Boolean combination of atomic formulas. An atomic formula with one free variable, x , must be a linear equality or inequality, such as $kx + c_1 \doteq d_1$ or $kx + c_1 < d_1$.

1. A linear equality defines either a finite set (the empty set or a singleton) or the entire set $\mathbb{N}$ (which is cofinite).
2. A linear inequality defines either a finite initial segment of $\mathbb{N}$, a cofinite final segment of $\mathbb{N}$, the empty set $\emptyset$ (which is finite), or the entire set $\mathbb{N}$ (which is cofinite).

In all cases, an atomic formula with one free variable defines a set that is either finite or cofinite. Finite or cofinite sets are closed under the Boolean operations of union, intersection, and complement. Therefore, any set definable by a quantifier-free formula in this language must be either finite or cofinite. This is a contradiction, as the set of even natural numbers is neither finite nor cofinite. $\square$

Theorem 4.22 (Presburger). The theory of the structure $\mathfrak{N}_A = (\mathbb{N}; 0, S, <, +)$ is decidable.

Proof. We will prove the decidability of $\mathfrak{N}_A = (\mathbb{N}; 0, S, <, +)$ using a quantifier elimination procedure. The theory of $\mathfrak{N}_A$ itself does not admit elimination of quantifiers; however, as a consequence of Proposition 4.20, it is equivalent to finding a quantifier elimination procedure for the theory T of the expanded structure $\mathfrak{N}_A^{\equiv} = (\mathbb{N}; 0, S, <, +, \equiv_2, \equiv_3, \dots)$.

From now on we will refer to $A_A + \{\equiv_n\}$ as T . To show that T admits quantifier elimination, it is sufficient to demonstrate that any formula of the form $\exists x(\alpha_1 \wedge \dots \wedge \alpha_n)$, where each α_i is a literal, has a quantifier-free equivalent in T .

The atomic formulas in our current language L_A^+ are of the form $t = t'$, $t < t'$ or $t \equiv_m t'$. We can eliminate negations by carrying out the following substitutions:

$$\neg(t = t') \text{ is replaced by } (t < t' \vee t' < t) \text{ by L3}$$

and

$$\neg(t \equiv_m t') \text{ is replaced by } (t \equiv_m t' + S0 \vee t \equiv_m t' + S^2 0 \vee \dots \vee t \equiv_m t' + S^{m-1} 0),$$

by Lemma 4.17. After applying these rules and converting the formula to Disjunctive Normal Form, the problem reduces to eliminating the quantifier from a formula of the form

$$\exists x(\beta_1 \wedge \dots \wedge \beta_m)$$

where every β_i is an atomic formula.

We can suppose that x appears in every β_i (since $\exists x(\alpha \wedge \beta) \equiv \alpha \wedge \exists x\beta$ if x is not free in α). Now we show that any atomic formula can be rewritten such that x appears in only one term. This is possible due to Lemma 4.1, Lemma 4.3, and the cancellation property from Lemma 4.6.

1. Form $nx + t = u$: An equality of the form $n'x + t' = n''x + t''$ can be rewritten as $(n' - n'')x + t' = t''$ (assuming $n' \geq n''$ and using subtraction as shorthand). By renaming, this takes the form $nx + t = u$.
2. Form $nx + t < u$ or $u < nx + t$: An inequality $n'x + t' < n''x + t''$ is rewritten as $(n' - n'')x + t' < t''$ (form $nx + t < u$) if $n' > n''$, or as $t' < (n'' - n')x + t''$ (form $u < nx + t$) if $n' < n''$.
3. Form $nx + t \equiv_m u$: A congruence $n'x + t' \equiv_m n''x + t''$ is equivalent to $(n' - n'')x + t' \equiv_m t''$. This takes the desired form $nx + t \equiv_m u$.

Now, we proceed with the core elimination algorithm for $\exists x \phi(x)$, where $\phi(x)$ is a conjunction of atomic formulas of the forms above.

Step 1: Uniformize Coefficients. Let p be the least common multiple¹ of the coefficients n of x appearing in all the atomic formulas in the conjunction. We transform each atomic formula to one where the coefficient of x is p . For a factor k , such that $k = p/n$:

1. An equality $nx + t = u$ becomes $px + kt = ku$ by Corollary 4.9.
2. An inequality $nx + t < u$ becomes $px + kt < ku$ by Corollary 4.11.
3. A congruence $nx + t \equiv_m u$ is multiplied by k . This requires adjusting the modulus, as $nx + t \equiv_m u$ iff $k(nx + t) \equiv_{km} ku$. This gives $px + kt \equiv_{km} ku$ by the definition of congruence.

After this process, all terms involving x are of the form px .

Step 2: Eliminate the Coefficient. Our formula now has the form $\exists x(\psi(px))$, where ψ is a conjunction of atomic formulas where x only appears inside px . We

¹The concept of the least common multiple (LCM) can be defined without using the multiplication symbol. The statement " x is the LCM of $n_1, \dots, n_k$ " is equivalent to the formula:

$$(x > 0) \wedge \bigwedge_{i=1}^k (x \equiv_{n_i} 0) \wedge \forall y \left(\left((y > 0) \wedge \bigwedge_{i=1}^k (y \equiv_{n_i} 0) \right) \rightarrow x \leq y \right).$$

introduce a new variable y to stand for px . This substitution is valid if we add that y must be a multiple of p by adding the conjunct $y \equiv_p 0$:

$$\exists y(\psi(y) \wedge y \equiv_p 0)$$

The atomic formulas inside $\psi(y)$ now have a coefficient of 1 for the variable y , simplifying them to the forms $y + t' = u'$, $y + t' < u'$, $u' < y + t'$, and $y + t' \equiv_{m'} u'$.

Step 3: The Special Case of Equality. If the conjunction $\psi(y) \wedge y \equiv_p 0$ contains an equality involving y , say $y + t' = u'$, we can eliminate the quantifier directly. A formula of the form $\exists y(y + t' = u' \wedge \chi(y))$ is equivalent to:

$$\chi(u' - t') \wedge t' \leq u'$$

Here, $\chi(u' - t')$ is shorthand for substituting y in $\chi(y)$ and transposing terms to eliminate subtraction². For instance, if $\chi(y)$ contains the conjunct $y < v$, the substitution yields $u' - t' < v$, which is rewritten as $u' < v + t'$. The condition $t' \leq u'$ ensures that the value substituted for y is in $\mathbb{N}$. The existence of a unique non-negative solution for y is guaranteed by axioms S3 and L1. If such an equality exists, the quantifier is eliminated.

Step 4: General Case. If the conjunction does not contain an equality, then the formula is equivalent to:

$$\exists y \left(\bigwedge_{j < n} A_j < y \wedge \bigwedge_{i < m} y < B_i \wedge \bigwedge_{k < l} y \equiv_{m'_k} C_k \right)$$

where the terms A_j, B_i, C_k do not contain y .

Let M be the least common multiple of all the m'_k for $k < l$. Since $a + M \equiv_{m'_k} a$ for any a , a property which follows from the definition of congruence and the axioms of addition, the pattern of residues of y modulo each m'_k repeats with a period of M . Thus, in searching for a solution to the congruences, we only need to search M consecutive integers.

The formula asserts the existence of a natural number y that is greater than a set of lower bounds $\{A_0, \dots, A_{n-1}\}$, less than a set of upper bounds $\{B_0, \dots, B_{m-1}\}$, and satisfies the given congruences. If any such solution exists, then one constructed "close" to a lower bound must exist. To ensure we find a non-negative solution, we add 0 to the set of lower bounds. Let $\mathcal{L} = \{A_0, \dots, A_{n-1}\} \cup \{0\}$ be the set of all lower bounds.

²This notation is a conceptual shorthand. As the theory does not include a subtraction operator, the substitution is performed by algebraic transposition of terms from the equality.

If a solution exists, then one of the following numbers must be a solution:

$$\begin{aligned} &A_0 + 1, \dots, A_0 + M, \\ &A_1 + 1, \dots, A_1 + M, \\ &\dots \\ &A_{n-1} + 1, \dots, A_{n-1} + M, \\ &0, 1, \dots, M - 1 \end{aligned}$$

Our formula asserting the existence of a solution y can now be replaced by a quantifier-free disjunction. This disjunction asserts that one of the test candidates—constructed by adding an integer from 1 to M to one of the lower bounds in $\mathcal{L}$ —is a valid solution satisfying all original conditions.

The final quantifier-free equivalent formula is:

$$\bigvee_{A \in \mathcal{L}} \bigvee_{q=1}^M \left[\bigwedge_{A' \in \mathcal{L}} A' < (A + S^q 0) \wedge \bigwedge_{i < m} (A + S^q 0) < B_i \wedge \bigwedge_{k < l} (A + S^q 0) \equiv_{m'_k} C_k \right]$$

This formula, while large, is free of quantifiers. This completes the quantifier elimination procedure.

Conclusion. The above procedure tells us how to find a quantifier-free sentence τ that is true if and only if a given sentence σ is true. To find the truth value of the quantifier-free sentence τ , it is enough to look at its atomic sentences. Any variable-free term in the language can be put in the form $S^k 0$ for some natural number k . Therefore, any atomic sentence is equivalent to one of the following forms:

- $S^k 0 = S^p 0$, which is true iff $k = p$.
- $S^k 0 < S^p 0$, which is true iff $k < p$. The truth of these first two types of sentences is decidable as a consequence of axioms L1-L5.
- $S^k 0 \equiv_n S^p 0$, which is true iff $k \equiv_n p$. The truth of this is decidable by the effective algorithm from Lemma 4.13, which is provable from axiom A3.

The quantifier elimination procedure is effective: for any sentence σ , we can mechanically produce an equivalent quantifier-free sentence τ . Since we can determine the truth value of every atomic sentence within τ , we can compute the truth value of τ itself. Because σ is true if and only if τ is true, this gives us an algorithm to decide the truth of any sentence σ .

A theory for which such a decision algorithm exists is, by definition, decidable.

□

Bibliography

- [1] Boolos, G. S., Burgess, J. P., & Jeffrey, R. C. (2007). *Computability and logic* (5th ed.). Cambridge University Press.
- [2] Enderton, H. B. (2001). *A mathematical introduction to logic* (2nd ed.). Harcourt/Academic Press.
- [3] Haase, C. (2018). A survival guide to Presburger arithmetic. *ACM SIGLOG News*, 5(3), 67–82.
- [4] Mendelson, E. (2015). *Introduction to mathematical logic* (6th ed.). CRC Press.
- [5] Rautenberg, W. (2010). *A concise introduction to mathematical logic* (3rd ed.). Springer.