FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Lukáš Kriško

Tennenbaum phenomena in models of arithmetic

Computer Science Institute of Charles University

Supervisor of the bachelor thesis: Dr. Neil Dillip Thapen
Study programme: Computer Science
Study branch: General Computer Science

Prague 2024

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In .... date ....

Author's signature

I would like to thank my supervisor Dr. Neil Dillip Thapen, especially, for all the time he has devoted to me and all the patience he has had with me. As every path, except those with no beginning, has to start somewhere, I also want to thank Dr. Thapen for even considering the prospect of being my supervisor.

V neposlednom rade chcem poďakovať mojej rodine, priateľom a obecne komukoľvek kto mi bol nápomocný pri mojej doterajšej ceste životom, mimo iného, vedúcej k napísaniu tejto bakalárskej práce.

Termín odovzdania bakalárskej práce sa stretol s odchodom môjho otca, a tak, venujem túto prácu jeho pamiatke.

Title: Tennenbaum phenomena in models of arithmetic

Author: Lukáš Kriško

Institute: Computer Science Institute of Charles University

Supervisor: Dr. Neil Dillip Thapen, Institute of Mathematics of the Czech Academy of Sciences

Abstract: The main aim of this text is to present and investigate some basic arithmetical functions and relations with regard to being recursive in a countable non-standard model of Peano arithmetic, PA for short, or some weaker fragment, like $I\Delta_0$ or $I\Sigma_1$, of PA.

In PART I, we present a known result called Tennenbaum's theorem. It states that every non-standard model M of PA with domain $\mathbb{N}$ can have neither $+^M$ nor $\times^M$ recursive. Moreover, we present the case for + in a strengthened version for $I\Delta_0$, which is due to K. McAloon. To show that not everything is lost, we also present a well know result stating that $<$ and the successor function can be simultaneously recursive in some non-standard model of PA with domain $\mathbb{N}$.

In PART II, we make our own investigation into the questions related to whether there can be a non-standard model of PA s.t. $x \operatorname{div} y$, the quotient function, and $x \bmod y$, the remainder function, are recursive in it. Furthermore, we often restrict y to some *standard number* n. To give a *non-exhaustive* list of problems we have solved, we showed that there can be no non-standard model of PA with both $x \operatorname{div} n$ and $x \bmod n$ recursive. Furthermore, there can be no non-standard model of $I\Sigma_1$ with $x \operatorname{div} y$ recursive. On the other hand, $x \operatorname{div} n$ and $x \bmod n$ can be separately recursive in a non-standard model of PA.

Keywords: model theory, Peano arithmetic, computability theory, recursive non-standard models, Tennenbaum's theorem, order-type, div, mod

Contents

Introduction

Introducing the problematic

The problematic centers around Tennenbaum's theorem, Tennenbaum [1959] , which is named after its discoverer Stanley Tennenbaum. It states that if M is a non-standard model of PA, short for "Peano Arithmetic", with domain $\mathbb{N}$, then neither $+^M$ nor $\times^M$ is a recursive function.

In a broader scale, the problematic centers around which arithmetical functions/relations can be recursive in a non-standard countable model of PA, or some weaker fragment of it. A closely related specific question is how weak can a fragment of PA be to still satisfy Tennenbaum's theorem.

Now, we explain in some detail some of the vocabulary used in the preceding two paragraphs.

PA

The theory PA represent a particular formalization of the notion "arithmetical theory" and its various properties.

To be more specific about the axiomatization of PA, it consists of axioms that use constants 0 and 1, functional symbols $+$ and $\times$ and a relational symbol $<$ to express basic truth that should hold in any structure interpreting given symbols which is to be called a model of arithmetic. A standard such structure is $\mathbb{N}$.

And to make it clear, the non-logical symbols of the *base* language, denoted as L_A, used for describing PA are constants 0 and 1, binary functions $+$ and $\times$ and a binary relation $<$.

Let us mention, that we often differentiate between PA^- which is axiomatized by axioms defining the basic arithmetical properties of $0, 1, +, \times$ and $<$. And PA which is axiomatized by all the axioms of PA^- + the induction axioms for every L_A formula.

Lastly, let us mention that "Peano Arithmetic" is named after Giuseppe Peano, who introduced this formalization in his work Peano [1889], written in Latin, and one can read an English translation in van Heijenoort [1967, pp. 83-97].

Arithmetical functions/relations

Another arithmetical functions and relations of interest that are not included implicitly in L_A are introduced using defining axioms extending PA or some weaker fragment of it we are considering, by a formula that is built from the language we are extending.

Non-standard models

By non-standard (countable) models of PA are meant those that are not isomorphic to $\mathbb{N}$ (and are countable).

Let us mention that we explain all the mentioned concepts in a greater detail, and with less ambiguity, in the course of the main part of the text as it will be need.

Other work on the subject

As we have already hinted at, there are two, three main kinds of questions about the subject we are discussing.

- How weak a sub-theory of PA can be so that Tennenbaum's theorem holds.
- Inspection of arithmetical functions/relations with respect to being recursive in a non-standard model of PA.
- Combination of the preceding two points. E.g. whether the divisibility relation $|$ can or can not be recursive in a non-standard model of $I\Delta_0$, which is a theory weaker than PA.

Besides these main types of questions, there are other more "exotic" ones, we will comment on them right after the more mainstream results.

In the two subsections to come, we will mention results by *other* authors concerning the introduced questions. And in the third section, we mention some other sources, than this text, of presentations of Tennenbaum's theorem.

Results on the topic

Let us mention that if we state that a model is "recursive", then we mean that the interpretation of $+$ and $\times$ in that model are recursive functions. Furthermore, when we are discussing recursivity, we discuss it with respect to structures which domain is $\mathbb{N}$.

One of the early results is that of Shepherdson [1964], stating that there can be a recursive non-standard model of $IOpen$. Where by $IOpen$ is meant PA^- together with the induction on all quantifier free formula.

This result was later strengthened by Berarducci and Otero [1996] showing that there can be non-standard recursive model of $IOpen$ + normality + with an unbounded set of infinitely many non-standard primes. Where by $IOpen$ + normality is meant the extension of the theory $IOpen$ with the following axiom for all $n \in \mathbb{N}$

$$\forall x \, \forall y \, \forall z_1 \, \ldots \, \forall z_{n-1}$$
$$((y \neq 0 \wedge x^n + z_1 \times x^{n-1} \times y + \ldots + z_{n-1} \times x \times y^{n-1} + y^n = 0) \rightarrow$$
$$\exists z \, (y \times z = x)).$$

In Schmerl [1998] was proved that there exists a non-standard model M of PA with $|^M$, the divisibility relation, recursive and that there exists a non-standard model M of PA with $\wedge^M$ and $\vee^M$ recursive. Where by $\wedge$ is meant a function computing the greatest common divisor and by $\vee$ is meant a function computing the least common multiple.

In McAloon [1982] was proved that there can be no non-standard model M of $I\Delta_0$ where $+^M$ or $\times^M$ is recursive.

Later, in Wilmers [1985] was shown that there can be no non-standard model M of IE_1 with $+^M$ recursive. Where by IE_1 is meant $PA^- +$ induction on quantifier free formulas that may be enclosed by a finitely many bounded existential quantifiers.

In D'Aquino [1997] the author considers a binary function denoted by $\#(x,y)$. It is introduced as an axiomatic extension of the language with the intended interpretation of $\#(x,y) = x^{[log_2 y]}$. Furthermore, if T is some theory, then by $T^\#$ we mean the theory $T +$ defining axioms for $\#$. The respective author shows the following results.

- Let M be a non-standard model of $PA^\#$, then $\#^M$ is not a recursive function.
- If M is a non-standard model of $IE_1^\#$, then neither of $+^M$,$\times^M$ and $\#^M$ is recursive.
- If M is a non-standard model of $IE_1^{-\#}$ and $M \not\models \forall E_1(\mathbb{N})$, then neither of $+^M$,$\times^M$ and $\#^M$ is recursive. Where by $IE_1^{-\#}$ is meant $IE_1^\#$ but only with parameter free induction. And by $\forall E_1(\mathbb{N})$ is meant all the sentences true in $\mathbb{N}$ s.t. they are also provable in $PA^- +$ induction on all the formulas s.t. they are quantifier free enclosed by a finitely, possibly 0, many bounded existential quantifiers which are in turn enclosed by a finitely many, possibly 0, unbounded universal quantifiers.
- Let M be a non-standard model of $\forall E_1^\#(\mathbb{N})$, then then neither of $+^M$,$\times^M$ and $\#^M$ is recursive. Where $\forall E_1(\mathbb{N})$ is explained in the previous item and $\forall E_1^\#(\mathbb{N})$ is basically the same only with the language extended by $\#$.

Furthermore, in D'Aquino [1997] is stated and proved the following statement. If f is a unary function s.t.

- f is computable,
- f is injective,
- $range(f)$ is coinfinite,
- f has no cycles.

Then there is a non-standard model of PA where f, more precisely its representation in that model, is recursive.

Lastly, in Yaegasi [2008] the author concentrates on the recursiveness of unary functions. For example, it is showed there that all the following pairs of functions can not be recursive in a non-standard model of PA.

- $2 \times x$ and $2 \times x + 1$,
- x^2 and $2 \times x^2$,
- 2^x and 3^x.

Furthermore, Yaegasi [2008] shows that for any total computable unary injection $f(x)$ there is a non-standard model of PA where $f(x)$ is recursive. Hence, strengthening the result of D'Aquino [1997].

To the best of our current knowledge, the most interesting unanswered problems are the following ones.

- Can there be a non-standard recursive model of IE_1^-?
- Can there be a non-standard recursive model of $\forall E_1(\mathbb{N})$?

Lastly, in Kaye [1991] is proved (and we have it from D'Aquino [1997]) the following,

(i) $\forall E_1(\mathbb{N}) \vdash IE_1^-$ and

(ii) for every $\phi \in \forall E_1(\mathbb{N})$, if $M \models IE_1^- + \neg\phi$, then M is not recursive.

Hence, the two most interesting unanswered problems boil down to "Can there be a non-standard recursive model of $\forall E_1(\mathbb{N})$?", i.e. the second one.

With respect to the last mentioned question, in Kaye [1990, p. 39] is given a condition, which if holds, then there can be no non-standard recursive model of $\forall E_1(\mathbb{N})$.

More "exotic" results

In Godziszewski and Hamkins [2017] authors prove mainly the following.

- No non-standard model of PA has a computable quotient presentation by a computably enumerable equivalence relation.
- No Σ_1-sound non-standard model of PA has a computable quotient presentation by a complementary computably enumerable equivalence relation.
- No non-standard model of PA in the language $\{+, \times, \leq\}$ has a computably enumerable quotient presentation by a equivalence relation of any complexity.

In Pakhomov [2022] the author proves mainly the following.

- There is a theory definitionally equivalent to PA that has a computable model s.t. the corresponding PA model is non-standard.
- There are no theories definitionally equivalent to $Th(\mathbb{N})$ that have computable models corresponding to non-standard models of PA.

Various presentations of Tennenbaum's theorem

We mention a few, other than this text, expositions of Tennenbaum's theorem.

In Kaye [2011], the author sets the scene with a historical background on the topic. Then presents Tennenbaum's theorem emphasizing its connection to Gödel-Rosser theorem, see Rosser [1936]. And finishes with examining the connections on extensions of Tennenbaum's theorem to diophantine problems in models of PA.

In the book Kaye [1991, pp. 153-158], the same author as of the preceding article, proves Tennenbaum's theorem for $+$ first in PA, i.e. a result of Tennenbaum [1959], and then proves Tennenbaum's theorem for $+$ in $I\Delta_0$, i.e. a result of McAloon [1982].

In Smith [2014] author presents Tennenbaum's theorem for $+$ in PA and the article is in fact inspired by Kaye [1991], i.e. the book we have just mentioned.

Lastly in Boolos et al. [2007, pp. 306-312] there are presentations of the following.

(a) There is no non-standard model of $Th(\mathbb{N})$ with domain $\mathbb{N}$ in which the addition function is arithmetical.

(b) There is no non-standard model of PA with domain $\mathbb{N}$ in which the addition function is recursive.

(c) There is no non-standard model of $Th(\mathbb{N})$ with domain $\mathbb{N}$ in which the multiplication function is arithmetical.

(d) There is no non-standard model of PA with domain $\mathbb{N}$ in which the multiplication function is recursive.

It is worth noting though that the detail of proofs are uneven. To (almost) quote from Boolos et al. [2007, p. 306], where given letters match letters given to respective just stated respective results. "The proof of (a.) will be given in some detail. The modifications needed to prove Theorem (b.) and those needed to prove Theorem (c.) will both be indicated in outline. A combination of both kind of modifications would be needed for Theorem (d.), which will not be further discussed."

This text

Structurally, the thesis is separated into PART I and PART II which are further subdivided into chapters.

Only some introductory-like knowledge of mathematical logic and computability/recursion theory is needed for this text, for an introductory to both one can look at e.g. Boolos et al. [2007]. And occasionally, also some basic knowledge of cardinal arithmetic is useful, one can find further details e.g. in Enderton [1977, Chapter 6].

We will now state in a concise manner what can be found in PART I and PART II. For further details please see chapter 11.3, for example, we state there our results from PART II.

PART I

In PART I, we present Tennenbaum's theorem for $+$ and $\times$. Moreover, we present the case for $+$ in a strengthened version for $I\Delta_0$, which is due to K. McAloon, and to be even more specific we present it for models of PA^- + Overspill for $\mathbb{N}$ on Δ_0 formulas. Then we inspect the order-type of models of PA^- + Overspill for $\mathbb{N}$ on Δ_0 formulas, as a corollary, we get that there is a non-standard model of PA with domain $\mathbb{N}$ s.t. $<$ and the successor are both recursive with respect to it. In order to reach these results, we start PART I with some preliminary work. We introduce PA and its various weaker versions like PA^-, prove a number of properties of the respective theories, recall and prove results from recursion theory and present a way to code sets using models of PA^-, more precisely of $I\Delta_0$.

This part consists of known results and known techniques to solve them.

The reader might ask why not to go rather after one of the sources mentioned in "Various presentations of Tennenbaum's theorem".

We will list some differences to, already mentioned, sources that we have used the most.

- Compared to Kaye [1991, pp. 153-158], we show also the case for $\times$ for non-standard models of PA.
- Compared to Smith [2014], we again show also the case for $\times$, and show it for models of $I\Delta_0$, which is somewhat only hinted at in Smith [2014].
- Compared to Boolos et al. [2007, pp. 306-312] we fill some of the, hinted at, gaps of the proof of Tennenbaum's theorem for $+$ and $\times$, and we actually show it for $I\Delta_0$ as opposite to PA.

Some further differences are loosely mentioned in chapter 11.3.

Regarding the sources for PART I. The PART I is heavily influenced, regarding both the form and content, by Kaye [1991]. Hence, many similarities to Kaye [1991] can be found in this text. More specifically.

- Things were taken from Kaye [1991, Chapters 2 and 4] to produce chapter 1.
- Things were taken from Kaye [1991, Chapters 4, 5 and 6] to produce chapter 2.
- Things were taken from Kaye [1991, Chapter 3] to produce chapter 3.
- Things were taken from Kaye [1991, Chapter 11] to produce chapter 4 and chapter 5.
- Things were taken from Kaye [1991, Chapter 6] to produce chapter 6.

In general, it can be said that we are greatly in debt to Kaye [1991].

Regarding further sources that inspired mainly, but not only i.e. they influenced also other segments, the presentation of Tennenbaum's theorem. We were inspired mainly by Kaye [1991, pp. 153-158], Smith [2014] and Boolos et al. [2007, pp. 306-312]. And there can be again found many similarities to those sources in this text.

PART II

In PART II, we investigate the functions x div y, the quotient function, and x mod y, the remainder function, with respect to being recursive in non-standard models of PA or its weaker fragments. Furthermore, we often restrict the second argument, i.e. y to some *standard number*, and ask the same type of questions. We chose these two functions since they occur very naturally in many questions in computer science and number theory. To reach these goals, we also investigate properties of div and mod in PA, often in $I\Sigma_1$, especially the structure of x div n for n being a standard number. We did not manage to answer all the reasonable questions that have emerged to us when asking about recursiveness of div and mod, nevertheless, we have answered some of them.

Declaration

To conclude this introduction, I want to declare that both the the writing process and the finishing of the writing of the thesis, in order to submit it by the deadline, was a very hectic one and it was caused entirely by me. Therefore, I want to emphasize that all the mistakes, errors,... are solely my responsibility and no one else's.

Part I

Tennenbaum's theorem and the order-type of models of PA

1. Observations and tools in PA^-

In this introductory chapter, we shall get acquainted with the language of arithmetic, L_A, and the theory of PA^- which is formed by a set of $first - order$ axioms with respect to the L_A. Axioms of PA^- more or less formalize obvious mathematical truths that should hold for $\mathbb{N}$ with standard $+, \times$ and $<$.

1.1 What is actually PA^-?

Language of arithmetic - L_A

First, we formally introduce the *first-order language of arithmetic*, denoted as L_A, that will specify which structures we are interested in.

The non-logical symbols of L_A are

- constant symbols 0 and 1,
- two binary functional symbols $+$ and $\times$,
- one binary relational symbol $<$

and inherently the symbol $=$ for equality. The $=$ will represent in every structure equality in its standard interpretation.

Besides the non-logical symbols of L_A just mentioned, we will construct formulas in the framework of the *first-order logic*, also denoted in this text as FOL. I.e. L_A also contains all the well known logical symbols such as

- logical connectives: $\vee, \wedge, \neg$
- quantifiers: $\exists, \forall$
- variables, denumerably many: $x_0, x_1, \ldots$
- parenthesis: (,)

This concludes the formal introduction of the L_A.

We will also use a few meta-logical notations that are not part of the L_A.

- $\equiv$ for *defined as*
- $\Rightarrow, \Leftarrow$ for *implies*, is *implied* by
- $\Leftrightarrow$ or $\iff$ for *is equivalent to*

Let φ,ψ be two formulas in the L_A, we will define “missing“ logical connectives using the already introduced ones:

- $(\varphi \veebar \psi) \equiv ((\varphi \vee \psi) \wedge (\neg(\varphi \wedge \psi)))$, i.e. $\veebar$ is φ or ψ but not both
- $(\varphi \rightarrow \psi) \equiv (\neg(\varphi) \vee \psi)$
- $(\varphi \leftarrow \psi) \equiv (\psi \rightarrow \varphi)$

- $(\varphi \leftrightarrow \psi) \equiv ((\varphi \to \psi) \wedge (\psi \to \varphi))$

Note that $\wedge, \vee$ are associative. Therefore it does not matter how we bracket them, e.g. we can just write $x \wedge y \wedge z$.

We could have introduced those right away with the $\vee$,... , there is no difference for us, i.e. you can freely imagine that they were introduced as primitive connectives. There is no difference for us because if we would have e.g. introduced $\to$ as an undefined connective and we would have defined when $M \models (\varphi \to \psi)$, for any structure M of L_A, then we would surely define it in a way that would satisfy $M \models (\varphi \to \psi) \iff M \models (\neg(\varphi) \vee \psi)$.

Let us introduce one shortcut, if $\overline{y}$ and $\overline{z}$ are two list of variables of length $m+1$, then by $\overline{y} = \overline{z}$ we simply mean $y_0 = z_0 \wedge \ldots \wedge y_m = z_m$.

Now, we shall define a quantifier denoted as $\exists!$ for all of variables x and formulas $\varphi(\overline{y})$ we define

$$\exists! x\ \varphi(\overline{y}, x) \equiv \exists x\ (\varphi(\overline{y}, x) \wedge \forall z\, (\varphi(\overline{x}, z) \to y = z)).$$

Again, the reader might assume that $\exists!$ was introduced as a primitive quantifier with the standard interpretation in mind.

We will often adhere to the typical simplifications as omitting brackets when possible, as always, and necessary, binary relations written in infix notation bind more than $\neg, \exists, \exists!, \forall$ which are more binding than $\wedge, \vee$ which are in turn more binding than $\to$ and $\leftrightarrow$, and to many other standard simplifications and notations.

If not stated otherwise, the considered language will be always L_A or some extension of it. I.e. if no language is stated, then it is implicitly meant that L_A, or some extension of it according to the context, is used.

Axioms of PA^-

Now, we shall approach axioms of the theory PA^- with respect to the language L_A. These axioms embody obvious algebraic arithmetical truths in $\mathbb{N}$. Later, in the section 2.1, we will add infinitely many induction axioms to the theory of PA^- that will result in the creation of the theory PA.
The axioms of $\boldsymbol{PA^-}$, taken almost indentically from Kaye [1991, pp.16-18], are:

- The functions $+$ and $\times$ are commutative and associative, and $\times$ is distributive over $+$.

  Ax.1 $\forall x, y, z\, ((x+y)+z = x+(y+z))$,

  Ax.2 $\forall x, y\, (x+y = y+x)$,

  Ax.3 $\forall x, y, z\, ((x \times y) \times z = x \times (y \times z))$,

  Ax.4 $\forall x, y\, (x \times y = y \times x)$,

  Ax.5 $\forall x, y, z\, (x \times (y+z) = x \times y + x \times z)$.

- Constant 0 is neutral element with respect to $+$ and analogously 1 is neutral element with respect to $\times$. Moreover, when 0 is multiplied by any element, then we get the expected result 0.

  Ax.6 $\forall x\, ((x+0 = x) \wedge (x \times 1 = x))$, Ax.7 $\forall x\, (x \times 0 = 0)$.

- The relation $<$ is a linear order.

Ax.8 $\forall x, y, z\, ((x<y \wedge y<z) \rightarrow x<z)$,

Ax.9 $\forall x\, \neg(x<x)$,

Ax.10 $\forall x, y\, (x<y \vee x=y \vee y<x)$.

- Before stating the next axioms, let us introduce one abbreviation. We define $x \leq y \equiv x < y \vee x = y$. We can look at it as at an abbreviation, i.e. every time we see $x \leq y$ in a L_A formula we simply substitute it for $x < y \vee x = y$. No further result breaks this way since the formula $x < y \vee x = y$ is of very small complexity (namely it is a Δ_0 formula, definition of Δ_0 will be found in section 1.3). Or, on the other hand, we may have extended our language by $\leq$ and added one more axiom to the PA^- namely $x \leq y \leftrightarrow x < y \vee x = y$. We will use the latter approach, but at least for our usage in this text are both ways equivalent. This adding an abbreviation vs. extending a language will happen multiple times throughout this text, therefore we have decided to comment it here a bit more thoroughly. We will comment on it one more time at the start of section 1.4.

  We introduce in an analogous way also $>$ and $\geq$.

  Operations $+$ and $\times$ are well behaved with respect to $<$.

Ax.11 $\forall x, y, z\, (x<y \rightarrow x+z<y+z)$,

Ax.12 $\forall x, y, z\, (0<z \rightarrow (x<y \rightarrow x \times z<y \times z))$,

Ax.13 $\forall x, y\, (x \leq y \rightarrow \exists z\, (x+z=y))$.

- The following last two axioms ensure $<$ to be a discrete order.

Ax.14 $0<1 \wedge \forall x\, (0<x \rightarrow 1 \leq x)$,

Ax.15 $\forall x\, 0 \leq x$.

This concludes the presentation of the axioms forming PA^-.

Remark on the notation

If $\mathcal{M}$ is a L_A structure then we will often use:

- $\mathbb{M}$,M or $dom(\mathcal{M})$ for its domain,
- $0, 1$ for the constants $0^{\mathcal{M}}, 1^{\mathcal{M}}$,
- $+$ for the binary function $+^{\mathcal{M}}$,
- $\times$ for the binary function $\times^{\mathcal{M}}$,
- $<$ for the binary relation $<^{\mathcal{M}}$.

Lastly, we will often simply write M or $\mathbb{M}$ for the whole structure $\mathcal{M}$.

If we use the shorter notation, e.g. $<$ for $<^{\mathcal{M}}$ or $<^M$, then we shall do it only in places where no confusion can arise.

Remark on reducts/expansions

Let $L^0 \subseteq L \subseteq L^1$ be some arbitrary languages, i.e. the logical parts are the same, however the non-logical symbols for constants/functions/relations does not need to have anything in common with L_A. Also let M be some L structure.

Then by a reduct of M to L^0, denoted as $< M, L^0 >$ or (M, L^0) if no confusion arises, we mean a L^0 structure M^0 s.t. $dom(M^0) = dom(M)$ and every symbol of L^0 has the same interpretation in M^0 as in M.

Symmetrically, we say that a L^1 structure M^1 is an expansion/extension of M if M is a reduct of M^1 with respect to L.

Lastly, let us *highlight* that when we write e.g. T is an expansion/extension of PA^- or L is an expansion/extension of L_A, then we do not mean it in strict sense, meaning that $T = PA^-$ or $L = L_A$ can happen.

Standard models of PA^-

The typical structure $\mathbb{N} = (\mathbb{N}, 0, 1, +, \times, <)$ giving the standard interpretation to the L_A obviously satisfies all the axioms of PA^-.

Structures of the L_A satisfying PA^-, or PA, isomorphic to $\mathbb{N}$ are called *standard* models of PA^-, or PA, and those which are not isomorphic to it are called *non-standard* models of PA^-, or PA.

Later on, we will observe that a structure M is *non-standard* iff. M has a "*non-standard* element", *non-standard* elements are introduced later in section 1.4.

Miscellaneous comments

- The later we are in the text, the less we differentiate between words "computable", "algorithmical" and "recursive". Especially in proofs with respect to the "recursion theory" formalism where we give rather intuitive arguments than rigorous ones.

- By Gödel's completeness theorem Gödel [1929], for an English translation see van Heijenoort [1967, pp. 582-591] and for a more up to date proof see Chiswell and Hodges [2007, p. 193, Theorem 7.6.7], we know that some theory T proves some sentence ϕ iff. every model of T models ϕ. Therefore, we often use T proves something with every model of T models something interchangeably.

- By WLOG we mean, as usual, "without loss of generality".

- We use mainly the symbol $\times$ for multiplication. But rarely we omit and write xy instead of $x \times y$, or possibly write $x \cdot y$. I.e. in both cases always imagine that $\times$ is there.

- We define for any $n \in \mathbb{N}$, the expression $[n]$ as the set $\{0, \ldots, n\}$.

1.2 Deductions from the axioms of PA^-

We will note few simple corollaries of the axioms of PA^-.

In the proofs to follow, M is always a model of PA^-.

Since this a just a collection of statements and their respective proofs that should hold in non-negative parts of discretely ordered commutative rings, the reader might want to skip this section, and return to it when/if needed.

Order $<$ behaves as expected

The order relation $<$ behaves as expected.

Observation 1.1. $PA^- \vdash \forall x, y\, (x < y \veebar x = y \veebar x > y)$, i.e. exactly one of those three options will happen.

Proof. By Ax.10 [trichotomy $<$] we know that at least one possibility happens. By Ax.9 [irreflexivity $<$] we get that the first, as well as the last, two options can not happen. First applying Ax.8 [transitivity $<$] and then Ax.9 [irreflexivity $<$] we get that nor the first and the last possibility can happen simultaneously. Therefore exactly one option will happen. ☐

Observation 1.2. $PA^- \vdash \forall x, y\, (x \leq y \wedge z < d \rightarrow x + z < y + d)$.

Proof. If $x = y$, then use Ax.11 [$x < y \rightarrow x + z < y + z$] and afterwards Ax.2 [commutativity $+$]. Otherwise if $x < y$, then use Ax.11 [$x < y \rightarrow x + z < y + z$] to conclude that $x + z < y + z$ and $z + y < d + y$. Afterwards us Ax.2 [commutativity $+$] and Ax.8 [transitivity $<$] to finally conclude that $x + z < y + d$. ☐

Corollary 1.3. $PA^- \vdash \forall x, y\, (x \leq y \rightarrow x < y + 1)$.

Proof. By noting Ax.14 [$0 < 1 \wedge (0 < x \rightarrow 1 \leq x)$], then applying Observation 1.2 and lastly using Ax.6 [$0, 1$ are neutral]. ☐

Max function can be defined well in PA^-

Observation 1.4. Let $M \models PA^-$, $n \in \mathbb{N}$ and $x_0, \ldots, x_n \in M$. Set $X := \{x_0, \ldots, x_n\}$ then

(i) There exist $x \in X$ s.t. $M \models \forall y \in X (y \leq x)$

(ii) In case all x_i's are mutually different, i.e. $|X| = n$, there exists unique $x \in X$ s.t. $M \models \forall y \in X (y \leq x)$.

Proof. (i) Proof is by induction on n. If $n = 0$, then set $x = x_0$. Otherwise assume that we have $X = \{x_0, \ldots, x_{n+1}\}$. Apply the induction hypothesis to $X' := \{x_0, \ldots, x_n\}$ to get x' with the property in the statement of this observation for X'. By Ax.10 [trichotomy $<$] we know that $x' < x_{n+1}$ or $x_{n+1} \leq x'$. In the first this case set $x := x_{n+1}$ and in the second case set $x := x'$. By the way we chose x', Ax.8 [transitivity $<$] and the definition of $\leq$ we get that x satisfies the desired property.

(ii) By the previous point we get that there must exists such a x. If there were two x's, namely x^1, x^2, satisfying the property of this observation, we have that either $x^1 = x^2$, which is what we want. Or that $x^1 < x^2$ and $x^2 < x^1$, by the definition of $\leq$. But using Ax.8 [transitivity $<$] we get that $x^1 < x^1$ which is in contradiction with Ax.9 [irreflexivity $<$]. Therefore $x^1 = x^2$ must hold and the uniqueness of x follows.

☐

Min function can be defined well in PA^-

Observation 1.5. Let $M \models PA^-$, $n \in \mathbb{N}$ and $x_0, \ldots, x_n \in M$. Set $X \coloneqq \{x_0, \ldots, x_n\}$ then

(i) There exist $x \in X$ s.t. $M \models \forall y \in X(x \leq y)$

(ii) In case all x_i's are mutually different, i.e. $|X| = n$, there exists unique $x \in X$ s.t. $M \models \forall y \in X(x \leq y)$.

Proof. Proof is analogous to the one for Observation 1.4. □

Operations $+, \times$ behave as expected

We can cancel terms on both sides of an equation.

Observation 1.6. PA^- proves the following

(i) $x + z = y + z \to x = y$,

(ii) $x \times z = y \times z \wedge 0 < z \to x = y$.

Proof. (i) Assume $x + z = y + z$. If $x < y$, then applying Ax.11 $[x < y \to x + z < y + z]$ we have $x + z < y + z$ but this can not happen by Observation 1.1. Analogously for $y < x$. We may conclude by Ax.10 [trichotomy $<$] that $x = y$ must hold.

(ii) Assume $x \times z = y \times z \wedge 0 < z$. Proof is similar to the one for $+$. Specifically, assume $x < y$, then by Ax.12 $[(x < y \ \wedge 0 < z) \to x \times z < y \times z]$ we have $x \times z < y \times z$ which can not be by Observation 1.1 and our assumption $x \times z = y \times z$. Analogously we get that $y < x$ can not hold. Therefore by Ax.10 [trichotomy $<$] we can conclude that $x = y$.

□

We will note two simple corollaries of Ax.11 $[x < y \to x + z < y + z]$ and Ax.12 $[(x < y \ \wedge 0 < z) \to x \times z < y \times z]$, sort of a weakening of those two.

Corollary 1.7. $PA^- \vdash \forall x, y, z\, (x \leq y \to x + z \leq y + z)$

Proof. If $x = y$ or $z = 0$, then the conclusion is obvious. Otherwise $x < y$ and then the conclusion follows by Ax.11 $[x < y \to x + z < y + z]$. □

Corollary 1.8. $PA^- \vdash \forall x, y, z\, (x \leq y \to x \times z \leq y \times z)$

Proof. If $x = y$ or $z = 0$, then the conclusion is obvious by Ax.7 $[x \times 0 = 0]$. Otherwise by Ax.15 $[0 \leq x]$ we have that $0 < z$ and Ax.12 $[(x < y \ \wedge 0 < z) \to x \times z < y \times z]$ can be applied. □

Also note the following.

Observation 1.9. $PA^- \vdash \forall x, y, z\, x \leq y \to x \leq y + z$

Proof. Since $M \models 0 \leq z$, by Ax.15 $[0 \leq x]$, we get by Corollary 1.7 that $M \models 0 + x \leq z + x$. Using Ax.2 [commutativity $+$] and Ax.6 $[0, 1$ are neutral] we observer $M \models x \leq x + z$.

Continuing, by Ax.11 $[x < y \rightarrow x + z < y + z]$ follows that $M \models x + z \leq y + z$. And finally applying Ax.8 [transitivity $<$] we can conclude that $M \models x \leq y + z$. ☐

Observation 1.10. $PA^- \vdash \forall x, z\,(0 < z \rightarrow x \leq x \times z)$

Proof. Since $M \models 0 \leq z$, by Ax.15 $[0 \leq x]$, we get by Corollary 1.8 that $M \models 0 \times x \leq z \times x$. Using Ax.4 [commutativity $\times$] and Ax.7 $[x \times 0 = 0]$ we observe $M \models x \leq x \times z$. ☐

For Ax.11-.13 also the converses hold.

Observation 1.11. PA^- proves the following

(i) $\forall x, y, z\,(x<y \leftarrow x + z<y + z)$,

(ii) $\forall x, y, z\,(0<z \rightarrow (x<y \leftarrow x \times z<y \times z))$,

(iii) $\forall x, y\,(x\leq y \leftarrow \exists z\,(x + z=y))$.

(iv) $\forall x, y\,(x<y \leftrightarrow \exists z\,(z > 0 \wedge x + z=y))$.

Proof. (i) By Ax.10 [trichotomy $<$], one of the two things can happen $x<y$ or $x\geq y$. If $x\geq y$ then by Ax.11 $[x < y \rightarrow x + z < y + z]$ we get $x + z\geq y + z$. If $x + z = y + z$, then it is a contradiction with Ax.9 [irreflexivity $<$], if $x + z > y + z$, then using Ax.8 [transitivity $<$] we again arrive at a contradiction with Ax.9 [irreflexivity $<$]. Therefore $x<y$ must indeed take place.

(ii) Assume we have, i.e. PA^- proves, $0<z$ and $x \times z<y \times z$. If $x \geq y$, then by Ax.12 $[(x < y \wedge 0 < z) \rightarrow x \times z < y \times z]$ we get $y \times z\leq x \times z$, but we can not have both $y \times z\leq x \times z$ and $x \times z<y \times z$ by Observation 1.1. Therefore we can not have $x \geq y$, and from Ax.10 [trichotomy $<$] we must have $x \geq y$ or $x < y$, therefore we indeed get that $x < y$ must hold, i.e. PA^- proves it from the two starting assumptions.

(iii) Assume that $PA^- \vdash \exists z\,(x + z = y)$. If $PA^- \vdash z = 0$, then by Ax.6 $[0, 1$ are neutral] can be concluded that $PA^- \vdash x \leq y$. Otherwise if we have $0 < z$, then we get by Ax.11 $[x < y \rightarrow x + z < y + z]$ that $0 + x < z + x$, by Ax.2 [commutativity $+$] and Ax.6 $[0, 1$ are neutral], we may conclude that $x < y$. Therefore we got either way the wanted inequality of $x \leq y$.

(iv) $\Rightarrow$: Since $0 < z$ we are getting by Ax.11 $[x < y \rightarrow x + z < y + z]$ that $0 + x < z+x$, therefore by Ax.2 [commutativity $+$] and Ax.6 $[0, 1$ are neutral] we get $x < y$.

$\Leftarrow$: By Ax.13 $[x \leq y \rightarrow \exists z(x + z = y)]$ we get that there exists a z s.t. $x + z = y$. If $z = 0$, then by Ax.6 $[0, 1$ are neutral] we get that $x = y$ which combined with our assumption of $x < y$ produces a contradiction because of Ax.9 [irreflexivity $<$]. Therefore by Ax.15 $[0 \leq x]$ it follows that $0 < z$.

☐

As a one direct corollary of the first item of Observation 1.11 we shall mention the following.

Corollary 1.12. $PA^- \vdash \forall x, y, z\,(x \leq y \leftarrow x + z \leq y + z)$

Proof. Assume that $PA^- \vdash x + z \leq y + z$, if moreover to that $x + z < y + z$, then by Observation 1.11 $x < y$, therefore $x \leq y$. If $x + z = y + z$ then using Observation 1.6 we get that $x = y$ from which $x \leq y$ follows. □

We will also note that the z in Observation 1.11 is unique, therefore we could have used *the* article...

Corollary 1.13. In Observation 1.11 we may also replace $\exists z$ by $\exists! z$. More specifically PA^- proves the following

(i) $\forall x, y\,(x \leq y \rightarrow \exists! z\,(x + z = y))$.

(ii) $\forall x, y\,(x < y \rightarrow (\exists! z\,(x + z = y) \wedge \forall z\,(x + z = y \rightarrow 0 < z)))$.

Proof. The last part in the second item, i.e. $\forall z\,(x + z = y \rightarrow 0 < z)$ assuming $x < y$, can be justified as follows. By Ax.15 $[0 \leq x]\, 0 \leq z$, if $0 = z$, then by Ax.6 $[0, 1$ are neutral$]$ we get $x = y$, and we have both $x < y$ and $x = y$ which can not be by Observation 1.1. Everything else follow by Observation 1.11, Observation 1.6 and Ax.2 [commutativity $+$] . □

Let us highlight two useful , although obvious, corollary.

Corollary 1.14. $PA^- \vdash \forall y\,(1 \leq y \rightarrow \exists! x\,(x + 1 = y))$

Proof. Apply Corollary 1.13 and Ax.2 [commutativity $+$] . □

Corollary 1.15. $PA^- \vdash \forall x\,(x + 1 \neq 0)$

Proof. Assume for contradiction that it can happen. Then by the last item in Observation 1.11 we get that $x < 0$, which is by Ax.15 $[0 \leq x]$ and Observation 1.1 impossible. □

Discreteness of the order $<$.

Observation 1.16. $PA^- \vdash x < y \rightarrow x + 1 \leq y$

Proof. By the last item of Observation 1.11 we get z s.t. $x + z = y \wedge 0 < z$. This z must satisfy by Ax.14 $[0 < 1 \wedge (0 < x \rightarrow 1 \leq x)]$ that $1 \leq z$. Therefore we get by Corollary 1.7 and Ax.2 [commutativity $+$] that $x + 1 \leq x + z$. The wanted conclusion $x + 1 \leq y$ immediately follows. □

Hopefully, it is obvious by now to the reader that we can prove many basic arithmetical truths just from the axioms of PA^-.

1.3 Arithmetical hierarchy

A few classes of formulas turn out to be particularly useful to us, specifically Δ_0 and Σ_1 formulas. But before approaching these classes, and the whole *Arithmetical hierarchy*, we need to introduce the notion of a bounded quantifier.

Bounded quantifiers

Let t be a term without the variable x present, then we say that the quantifier $\exists$ is bounded in the following occurrence $\exists x\, \varphi(\overline{y}, x)$ iff. $\varphi(\overline{y}, x)$ is of the following form $(x < t \wedge \psi(\overline{y}, x))$, or with $\leq$ instead of $<$. And the quantifier $\forall$ is bounded in the following occurrence $\forall x\, \varphi(\overline{y}, x)$ iff. $\varphi(\overline{y}, x)$ is of the following form $(x < t \rightarrow \psi(\overline{y}, x))$, or with $\leq$ instead of $<$.

One more notation is often used, that is the bound is written inside the quantifier, i.e. we write $\exists x < t\, \psi(\overline{y}, x)$ instead of $\exists x\, (x < t \wedge \psi(\overline{y}, x))$. And the same goes for the $\forall$ quantifier.

We will use only the $\exists$ and $\forall$ quantifiers in the definition of the arithmetical hierarchy. But the notion of a bounded quantifier can be obviously extended also to $\exists!$ together with the notation shortcut.

The Arithmetical hierarchy

We will be interested mainly in the classes of Δ_0 and Σ_1 formulas. Since there is not much difference in defining only them compared to the definition of the whole Arithmetical hierarchy we opted for the latter.

Now, we will approach the aforementioned formula classes.

Definition 1.1 (Strict Arithmetical hierarchy)**.** Let $i \in \mathbb{N}$.

Δ_0: A formula $\varphi(\overline{x})$ is a strict Δ_0 formula iff. all the quantifier occurrences which are in $\varphi(\overline{x})$ are bounded. We also extend the notation and say that the a formula is a strict Σ_0, or Π_0, formula iff. it is a strict Δ_0 formula.

Σ_{i+1}: A formula $\varphi(\overline{x})$ is a strict Σ_{i+1} formula iff. it is of the form $\exists \overline{y}\, \psi(\overline{x}, \overline{y})$ where $\psi(\overline{x}, \overline{y})$ is a strict Π_i formula.

Π_{i+1}: A formula $\varphi(\overline{x})$ is a strict Π_{i+1} formula iff. it is of the form $\forall \overline{y}\, \psi(\overline{x}, \overline{y})$ where $\psi(\overline{x}, \overline{y})$ is a strict Σ_i formula.

Where $\exists \overline{y}$ or $\forall \overline{y}$ is a shortcut for a finite, *possibly empty*, list of corresponding quantifiers with single variables. I.e. it symbolizes $Qy_0, \ldots, Qy_{n-1}$, where Q represents $\exists$ or $\forall$ and $n \in \mathbb{N}$ s.t. $\overline{y}$ is a n-tuple.

Definition 1.2 (Arithmetical hierarchy)**.** Let $i \in \mathbb{N}$. We say that $\varphi(\overline{x})$ is a Σ_i or Π_i formula iff. it is equivalent over the theory T we consider, it is going to be always PA^- or some extension of it, to a strict Σ_i or Π_i formula. We also say that $\varphi(\overline{x})$ is a Δ_i formula iff. it is equivalent over the theory T we consider, to both a strict Σ_i and a strict Π_i formula.

Furthermore, we also associate with Δ_i, Σ_i and Π_i the sets of their respective formulas, e.g.

$$\Sigma_i \coloneqq \{\varphi(\overline{x}) | \varphi(\overline{x}) \text{ is equivalent in } T \text{ to a \textit{strict} } \Sigma_i \text{ formula}\}.$$

Since the list of quantifiers may be empty we have e.g. that $\Delta_0 \subseteq \Sigma_1 \subseteq \Pi_2$. And also that $\Delta_0 \subseteq \Sigma_1 \sigma_2$.

Let us note that we will often omit from mentioning over which theory T we mean whether two formulas are equivalent since it should be obvious from the context. And if it does not stem from the context, then always assume that the theory is PA^- or some extension of it we discuss at the moment.

Remark about the Σ_1 class

We mention one, relatively important, observation that any Σ_1 formula "need" only one unbounded existential quantifier.

In the proof to follow the theory T, from Definition 1.2, is always going to be PA^-. Therefore, the result obviously holds also for T being an extension of PA^-.

Observation 1.17. Let $i, k \in \mathbb{N}$ and $\varphi(\overline{x})$ be a L_A formula. If $\varphi(\overline{x})$ is a Σ_1 formula, then it is equivalent in T to a L_A formula $\exists u \psi(\overline{x}, u)$ s.t. $\psi(\overline{x}, u)$ is a Δ_0 formula.

Proof. Since $\varphi(\overline{x})$ is a Σ_1, it is equivalent, in T, to a $\exists \overline{y}\, \vartheta(\overline{x}, \overline{y})$ formula for $\vartheta(\overline{x}, \overline{y})$ a strict Δ_0 formula. But $\exists \overline{y}\, \vartheta(\overline{x}, \overline{y})$ is obviously equivalent over PA^- to the formula $\exists u \exists \overline{y} < u\, \vartheta(\overline{x}, \overline{y})$ where $\exists \overline{y} < u\, \vartheta(\overline{x}, \overline{y})$ is clearly a Δ_0 formula. To be more specific, they are equivalent over PA^- thanks to the fact that max is well defined by Observation 1.4 and Corollary 1.3. Therefore, when showing the $\Rightarrow$, we can just set u to the $max\{y_0, \ldots, y_{n-1}\} + 1$, for n being the length of the $\overline{y}$. And the $\Leftarrow$ is obvious by the FOL. $\square$

We mention, without a proof - for a hint see e.g. Kaye [1991][Chapter 7, p. 80-81], that the just proved result generalizes to Σ_i or Π_i formulas for any $i \in \mathbb{N}$ for a theory S $I\Delta_0$ which is a bit stronger than PA^-, the Δ_0 is introduced in section 2.1. I.e. for any $i \in \mathbb{N}$ and $\varphi(\overline{x})$ in Σ_{i+1} or Π_{i+1}, we have that the formula is always equivalent in S to a $\exists y_0 \forall y_1 \ldots Q y_i \psi(\overline{x}, \overline{y})$ or $\forall y_0 \exists y_1 \ldots Q' y_{i-1} \psi(\overline{x}, \overline{y})$, for $\psi(\overline{x}, \overline{y})$ a Δ_0 formula. Where Q is $\exists$ and Q' is $\forall$ if i is odd, and if i is even it is the other way around.

1.4 Additional notation, functions and relations

In this section, we shall introduce additional functions, relations and notation that will come handy sooner or later.

Introducing new relational and functional symbols

Before introducing new symbols, let us partly repeat one more time the following. Let us also note that T is always going to be PA^- or some extension of it.

To introduce a new n-ary relational symbol R with respect to some theory T we do it by using some L_A, or some extension of it, formula $\varphi(\overline{x})$, where $\overline{x}$ is an n-tuple. S.t. we usually either

- extend our language by R. And we add to our theory T axiom that $R(\overline{x}) \leftrightarrow \varphi(\overline{x})$.

* or we do not extend our language, but we write formulas with R in it keeping in mind that it is just a shortcut for the $\varphi(\overline{x})$.

As you can see these two ways are basically identical.

To introduce a new n-ary functional symbol f with respect to some theory T we do it by using some L_A, or some extension of it, formula $\varphi(\overline{x}, y)$, where $\overline{x}$ is an n-tuple, s.t. we demand that T proves that $\forall \overline{x} \exists! y \varphi(\overline{x}, y)$. Then we usually either

- extend our language by f. And we add the following formula to our set of axioms $\forall\overline{x}\varphi(\overline{x}, f(\overline{x}))$.

* we write formulas with $f(\overline{x}, y)$ but keeping in mind, that it is just a shortcut. Namely if we have occurrences of f in a formula $\psi(\overline{x}, \overline{z})$, then these occurrences must be always "inside" some occurrence of some relational symbol.

  In order to retrieve the actual formula, we simply replace every occurrence of $f(t_0, \dots, t_{n-1})$, for any set of terms $t_0, \dots, t_{n-1}$, in $\psi(\overline{x}, \overline{z})$ step by step in the following fashion.

  Let $t_0, \dots, t_{n-1}$ be some set of terms and $f(t_0, ldots, t_{n-1})$ be some occurrence of f in $\psi(\overline{x}, \overline{z})$ "inside" some occurrence of some relational symbol R, denote this specific occurrence by $R^{'}$.

  We simply replace every occurrence of $f(t_0, ldots, t_{n-1})$ in $R^{'}$ by some variable w not present in $R^{'}$ to get a new occurrence of R, denote it by R^*. And then we replace the occurrence of $R^{'}$ in $\psi(\overline{x}, \overline{z})$ by $\exists w(\varphi(t_0, \dots, t_{n-1}) \wedge R^*)$.

  And we do this for every occurrence of f. Since are all the described steps finite and there is a finite number of occurrences of f in $\psi(\overline{x}, \overline{z})$ we must end sooner or later with a formula that is equivalent, over the extension of PA^- we are considering with an addition of the defining axiom $\forall\overline{x}\varphi(\overline{x}, f(\overline{x}))$, to $\varpi(\overline{x}, \overline{z})$, but now without the symbol f.

We will use the first described approach both for adding new relations and functions, but let us note that there is not some great difference between them.

In the preceding section about the Arithmetical hierarchy, section 1.3, we defined a way to classify formulas, roughly speaking, according to the number of alternating quantifiers. However, when we introduce e.g. a new relational symbol $R(\overline{x})$ defined by the formula $\varrho(\overline{x}) \leftrightarrow R(\overline{x})$, then the formula $\varphi(\overline{x}, \overline{y})$ with R in it might not belong to the same members of the Arithmetical hierarchy as the formula $\psi(\overline{x})$ that we got from $\varphi(\overline{x}, \overline{y})$ by substituting every occurrence of $R(\overline{x})$ by $\varrho(\overline{x})$. Therefore, when classifying a formula in an extension of the L_A we always first transform it into an equivalent, over $T+$ all the defining axioms we are considering, formula formed solely by the L_A. Actually a single step of this transformation process is described by the second items, denoted as "*", which describe one way to introduce a new relational/functional symbol to formulas we consider.

We would also like to note the reader that will classify formulas according to the Arithmetical Hierarchy only a couple of times and every time we will only ask whether a formula belongs to the Δ_0, possibly the Σ_1, class of formulas. Furthermore, the answers to these questions will be, at least intuitively, obvious even without the discussion we just gave.

And probably the most important thing to take from this subsection is that we can always convert formulas in an extension of L_A to formulas in L_A which are equivalent in some theory $T+$ all the defining axioms we are considering.

For additional details see e.g. Kaye [1991, Section 4.2.]. This section does however treat mostly the process of adding new relational/functional symbols with respect to the induction axioms, to be introduced in section 2.1.

Successor, predecessor, minus and divides

Title of the forthcoming subsection reveals what we are going to introduce.

Let us highlight that the process of adding new symbols takes places with respect to PA^- or some extension of it.

Definition 1.3 (Successor - $S(x)$)**.** We introduce a new unary functional symbol $S(x)$, the successor function, by the following formula $\varphi_{S(x)}(x,y) \equiv y = x+1$.

Definition 1.4 (Predecessor - $P(x)$)**.** We introduce a new unary functional symbol $P(x)$, the predecessor function, by the following formula $\varphi_{P(x)}(x,y) \equiv (x = 0 \wedge y = 0) \vee (y+1 = x)$.

Definition 1.5 (minus - $\dot{-}$)**.** We introduce new binary functional symbol $x \dot{-} x$, the subtraction function, by the following formula $\varphi_{\dot{-}}(x,z,y) \equiv (x < z \wedge y = 0) \vee (z+y = x))$.

In the light of section 1.4, we need to show that

$$PA^- \vdash \forall x \exists! y \varphi_{S(x)}(x,y),$$
$$PA^- \vdash \forall x \exists! y \varphi_{P(x)}(x,y),$$
$$PA^- \vdash \forall x \forall z \exists! y \varphi_{\dot{-}}(x,z,y),$$

to justify the definitions we have just given.

Observation 1.18.

(i)
$$PA^- \vdash \forall x \exists! y \varphi_{S(x)}(x,y)$$

(ii)
$$PA^- \vdash \forall x \exists! y \varphi_{P(x)}(x,y),$$

(iii)
$$PA^- \vdash \forall x \forall z \exists! y \varphi_{\dot{-}}(x,z,y),$$

Proof. (i) Existence is obvious as well as uniqueness.

(ii) Existence follow by Ax.15 $[0 \leq x]$, Ax.14 $[0 < 1 \wedge (0 < x \to 1 \leq x)]$ and Observation 1.6. Uniqueness follow by Corollary 1.15 and by a combination of Ax.15 $[0 \leq x]$, Ax.14 $[0 < 1 \wedge (0 < x \to 1 \leq x)]$ and Observation 1.6.

(iii) Existence follow by Ax.10 [trichotomy $<$] and (i) in Corollary 1.13, the first item is used. Uniqueness follow by a combination of the third item in Observation 1.11, Ax.8 [transitivity $<$] and Ax.9 [irreflexivity $<$] and then by a combination of Ax.10 [trichotomy $<$] and the first item in Corollary 1.13. □

Definition 1.6 (Divides - $x_0 \mid x_1$)**.** We introduce new binary relational symbol $x_0 \mid x_1$, the divides relation, by the following formula $\varphi_{|}(x_0,x_1) \equiv \exists z(x_0 \times z = x_1)$.

Let us observe two important facts, namely that $PA^- \vdash a \mid b \wedge b \neq 0 \to a \leq b$ and, as a corollary, that $\varphi_|(x, w)$ is equivalent, over PA^-, to a Δ_0 formula.

Observation 1.19. Let $M \models PA^-$ and $a, b \in M$ s.t. $M \models b \neq 0$ and $M \models a \mid b$, then $M \models a \leq b$.

Proof. Let $c \in M$ be s.t. $M \models a \times c = b$. Since $M \models b \neq 0$ we get by Ax.7 $[x \times 0 = 0]$ that $M \models c \neq 0$.

By Ax.15 $[0 \leq x]$ combined with Ax.14 $[0 < 1 \wedge (0 < x \to 1 \leq x)]$ it follows that $M \models 1 \leq c$. Since $M \models 1 \leq c$, we get by Corollary 1.8 that $M \models a \leq c \times a$.

But we know by Ax.4 [commutativity $\times$] that $M \models c \times a = b$. Therefore $M \models a \leq b$ which is what we wanted to prove. □

Corollary 1.20. Formula $\varphi_|(x, w)$ is equivalent over PA^- to the formula

$$\varrho_|(x, y) \equiv \exists z \leq y (x \times z = y).$$

Proof. We will first show the implication from left to right.

Let $M \models PA^-$ and $a, b \in M$ s.t. $M \models \varphi_|(a, b)$. Surely either $M \models b = 0$ or $M \models b \neq 0$. Let us consider these two cases separately.

$b = 0^M$: Then clearly setting z to 0^M we have that $M \models z \leq b$ and and by Ax.7 $[x \times 0 = 0]$ we have $M \models a \times z = b$.

$b \neq 0^M$: Let $c \in M$ be s.t. $M \models a \times c = b$, by Ax.4 [commutativity $\times$] we know that $M \models c \times a = b$, therefore $M \models \varphi_|(c, b)$.

So we know that $M \models c \mid b \wedge b \neq 0$, therefore by Corollary 1.20 we get that $M \models c \leq b$. Therefore, by setting z in $\varrho_|(a, b)$ to c, we get that $M \models \varrho_|(a, b)$.

As for the other implication. If $M \models \varrho_|(a, b)$ then obviously, by FOL, $M \models \varphi_|(a, b)$. □

Therefore it can be concluded that every function/relation we have introduced can be defined using a Δ_0 formula.

From now on, whenever we write PA^- or some extension of it T, we will actually mean PA^-, or T, with added defining axioms for $S(x), P(x), X \dot{-} z$ and the divisibility relation $|$. Rarely, only to highlight the presence of such a defining axiom/s, we will write e.g. T plus the defining axioms for $S(x)$.

Notation and (non-)standard elements

We shall introduce few notations that act solely as a shortcuts for terms of L_A or, in case of the last one, are one of ours meta-notations.

Definition 1.7 (Definition of $\underline{n}$)**.** We define the following shortcut for every $n \in \mathbb{N}$.

$$\underline{n} := \begin{cases} 0 & n = 0, \\ (\underline{(n-1)} + 1) & 1 \leq n. \end{cases}$$

The 0 and $(\underline{(n-1)}+1)$ on the left, i.e. the value of $\underline{n}$, are terms from the language L_A, of course except the $(n-1)$ which is just evaluated in $\mathbb{N}$. And $n = 0, 1 \leq n$ on the right are conditions evaluated in $\mathbb{N}$.

Note that the in any model of PA^-, or some extension of it, $\underline{0}, \underline{1}$ have the same meaning as the constant symbols $0, 1$ from L_A. However, we will usually use $0, 1$ for $\underline{0}, \underline{1}$. A possibly confusing situation can arise when we talk both about constant symbols $0, 1$ from L_A and $0, 1 \in \mathbb{N}$ in this case we will either use $\underline{0}, \underline{1}$ to make the distinction explicit or we will simply rely on the context that should make the distinction implicit.

In any model M of PA^-, or some extension of it, we introduce the notion of *standard/non-standard* elements.

Definition 1.8 (Standard and non-standard elements)**.** Let $M \models PA^-$ and let $a \in M$. We say that a is a *standard* element of M iff. $\exists n \in \mathbb{N}$ s.t. $a = \underline{n}^M$. And we say that a is a *non-standard* element of M iff a is not a *standard* element of M.

Definition 1.9 (Definition of $x^{\underline{n}}$)**.** We define the following shortcut for every $n \in \mathbb{N}$ and x being any variable from L_A.

$$x^{\underline{n}} := \begin{cases} 1 & n = 0, \\ x \times x^{\underline{(n-1)}} & 1 \leq n. \end{cases}$$

Again, the 1 and $x \times x^{\underline{(n-1)}}$ on the left are terms from the language L_A, of course except the $(n-1)$ which is just evaluated in $\mathbb{N}$. And the conditions on the right are evaluated in $\mathbb{N}$.

1.5 Further observations in PA^-

Behavior of mainly standard elements in PA^- with respect to $+, \times, \dot{-}, |$ and $<$

Similarly as in section 1.2, this *subsection* is just a relatively large collection of algebraic results in models of PA^-. Therefore, if the reader chooses to, this *subsection* can be skipped and returned to when explicitly needed. On the other hand, let us note that compared to section 1.2 is this *subsection* is surely more important.

First, we shall show that the *standard* elements behave in models of PA^- as expected.

Observation 1.21. Let $M \models PA^-$ and $x \in M$ and let n be any member of $\mathbb{N}$. Then the following holds

$$M \models \underline{n} \times x = x + \ldots + x,$$

where x is written on the right side n-times and if $n = 0$ the whole term will stand for the constant symbol 0. Please note that thanks to Ax.1 [associativity +] it does not matter how we bracket the expression on the right.

Proof. Proof is by induction on n, first we show the case for $n = 0$ and then the induction step.

$n = 0$: $M \models \underline{0} \times x = 0 \times x = x \times 0 = 0$ which is what we wanted to show. Note that the first equality follows by Definition 1.7, the second by Ax.4 [commutativity $\times$] and the last one by Ax.7 $[x \times 0 = 0]$.

$n = m + 1$:

$$M \models \underline{n} \times x = x \times \underline{n} = x \times (\underline{m} + 1) = x \times \underline{m} + x \times 1 = x + \ldots + x,\ n - \text{times},$$

which is what we wanted. The first equality follows by Ax.4 [commutativity $\times$], the second by Definition 1.7, the third by Ax.5 [distributivity] and the last one by Ax.6 $[0, 1$ are neutral$]$ and the induction hypothesis on m.

□

Observation 1.22. Let $M \models PA^-$ then for any $k, l \in \mathbb{N}$ we have $M \models \underline{(k +^{\mathbb{N}} l)} = \underline{k} + \underline{l}$.

Proof. Proof is by induction on l.

$l = 0$: In this case $\underline{(k +^{\mathbb{N}} 0)} = \underline{k}$. And by Definition 1.7 and Ax.6 $[0, 1$ are neutral$]$ we have that $M \models \underline{k} + \underline{0} = \underline{k}$. Therefore we can indeed conclude that $M \models \underline{(k +^{\mathbb{N}} l)} = \underline{k} + \underline{l}$

$l = d + 1$: By Definition 1.7 we have that $M \models \underline{k} + \underline{l} = \underline{k} + (\underline{d} + 1)$, by Ax.1 [associativity $+$] and the induction hypothesis we get that $M \models \underline{k} + (\underline{d} + 1) = \underline{(k +^{\mathbb{N}} d)} + 1$. And by Definition 1.7 $M \models \underline{(k +^{\mathbb{N}} d)} + 1 = \underline{((k +^{\mathbb{N}} d) +^{N} 1)} = \underline{(k +^{\mathbb{N}} l)}$, from which immediately follows that $M \models \underline{k} + \underline{l} = \underline{(k +^{\mathbb{N}} l)}$ Therefore we may conclude that the induction step was finished.

□

From now on, when writing $M \models \ldots \underline{n +^{\mathbb{N}} m} \ldots$ we will write only $M \models \ldots \underline{n + m} \ldots$ since it is obvious that we take $+$ in $\mathbb{N}$. We will do the same for $\times$ and relational symbols.

Observation 1.23. Let $M \models PA^-$ and $a, b, c \in M$ s.t. $M \models c \leq b$, then $M \models (a + b) \dot{-} c = a + (b \dot{-} c)$.

Proof. There must exist $z_{a+b}, z_b \in M$ s.t. $M \models (a + b) \dot{-} c = z_{a+b}$ and $M \models b \dot{-} c = z_b$

Since $M \models c \leq b$, and thus also $M \models c \leq (a + b)$ by Observation 1.9, we get by definition of $\dot{-}$ that $M \models c + z_{a+b} = a + b$ and $M \models c + z_b = b$.

Therefore $M \models a + c + z_b = c + z_{a+b}$, and by Observation 1.6 we can conclude that $M \models a + z_b = z_{a+b}$, but that is exactly what we wanted. □

Observation 1.24. Let $M \models PA^-$ and $a, b, c \in M$ s.t. $M \models c \leq b \leq a$, then $M \models (a \dot{-} b) + c = a \dot{-} (b \dot{-} c)$.

Proof. There exists some $z_b \in M$ s.t. $M \models (a \dot{-} b) = z_b$ and therefore $M \models (a \dot{-} b) + c = z_b + c$. And by definition of $\dot{-}$ the following must hold $M \models b + z_b = a$.

Again, there exists some $z_c \in M$ s.t. $M \models (b \dot{-} c) = z_c$. By definition of $\dot{-}$ we know that $M \models c + z_c = b$ and hence by Ax.2 [commutativity +] and more importantly by the third item in Observation 1.11 and lastly our assumption of $M \models b \leq a$ we get that $M \models z_c \leq a$. Therefore by definition of $\dot{-}$ there is some $z \in M$ s.t. $M \models z_c + z = a$ and this z equals $(a \dot{-} z_c)^M$.

We would like to show that $z_b + c = z$.

Since $M \models z_c + z = a$ and $M \models b + z_b = a$ we get that $M \models z_c + z = b + z_b$.

When we add c to both sides of the equality and we employ Ax.1 [associativity +] and Ax.2 [commutativity +] we get $M \models b + z = c + b + z_b$.

Lastly, we can again apply Ax.1 [associativity +], Ax.2 [commutativity +] and most importantly Observation 1.6, i.e. that we cancel certain terms from both sides of an equation, to reach the desired conclusion of $M \models z = c + z_b$.

□

Observation 1.25. Let $M \models PA^-$ and $n, m \in M$ s.t. $m \leq n$, then $M \models \underline{n} \dot{-} \underline{m} = \underline{(n - m)}$.

Proof.

$$M \models \underline{n} \dot{-} \underline{m} = (\underline{(n-m)} + \underline{m}) \dot{-} \underline{m} = \underline{(n-m)} + (\underline{m} \dot{-} \underline{m}) = \underline{(n-m)} + 0 = \underline{(n-m)},$$

which is what we wanted.

As for the equalities, the first follows by Observation 1.22, the second by Observation 1.23, the third as well as the fourth by Ax.6 [0, 1 are neutral]. □

Observation 1.26. Let $M \models PA^-$ and $a, b, c \in M$ s.t. $M \models a + b = c$, then $M \models a = c \dot{-} b$.

Proof. Assume $M \models a + b = c$, then $M \models (a + b) \dot{-} b = c \dot{-} b$.

By Observation 1.23 we have $M \models a + (b \dot{-} b) = c \dot{-} b$ and by Ax.6 [0, 1 are neutral] we may conclude $M \models a = c \dot{-} b$, which is what we wanted. □

Observation 1.27. Let $M \models PA^-$ and $a, b, c \in M$ s.t. $M \models b \leq a$ and $M \models b \leq c$, then $M \models (a \dot{-} b) + c = a + (c \dot{-} b)$.

Proof. First note that since $M \models b \leq c$, we can conclude by Ax.13 [$x \leq y \rightarrow \exists z(x + z = y)$] that $M \models c = b + z$ for some $z \in M$.

Continuing, we have,

$$\begin{gathered} M \models (a \dot{-} b) + c = \\ (a \dot{-} b) + (b + z) = \\ ((a \dot{-} b) + b) + z = \\ (a \dot{-} (b \dot{-} b)) + z = \\ (a \dot{-} 0) + z = \\ a + z = \\ a + (c \dot{-} b). \end{gathered}$$

Where the respective equalities follow by the upcoming arguments.

(i) Follows by $M \models c = b + z$.

(ii) Follows by Ax.1 [associativity +] .

(iii) Follows by $M \models b \leq b \leq a$ and Observation 1.24.

(iv) It is obvious that for any $x \in M$, $M \models x \dot{-} x = 0$.

(v) Follows by Ax.6 $[0, 1$ are neutral$]$.

(vi) Follows by $M \models c = b + z$, Ax.2 [commutativity +] and Observation 1.26.

And the proof is finished. ☐

Observation 1.28. Let $M \models PA^{-}$, $k, l \in \mathbb{N}$. Then the following holds

$$M \models \underline{(k \times l)} = \underline{k} \times \underline{l}.$$

Proof. Proof is again by induction on l.

$l = 0$: By Definition 1.7 and Ax.7 $[x \times 0 = 0]$ we have that $M \models \underline{k} \times \underline{l} = 0$. And since $k * l = k * 0 = 0$, we get by definition 1.7 that $M \models \underline{(k \times l)} = 0$. Therefore we indeed have $M \models \underline{k \times l} = \underline{k} \times \underline{l}$.

$l = d + 1$: We have $M \models \underline{k \times (d + 1)} = \underline{(k \times d) + k}$, by Definition 1.7. By previous Observation 1.22 we get that $M \models \underline{((k \times d) + k)} = \underline{k \times d} + \underline{k}$. Using the induction hypothesis on l we get that $M \models \underline{k \times d} + \underline{k} = (\underline{k} \times \underline{d}) + \underline{k}$. Using Ax.6 $[0, 1$ are neutral$]$, to rewrite $\underline{k}$ as $\underline{k} \times 1$, and Ax.5 [distributivity] we get that $M \models (\underline{k} \times \underline{d}) + \underline{k} = \underline{k} \times (\underline{d} + 1)$. Where by Definition 1.7 we have $M \models \underline{k} \times \underline{d + 1}$, which is precisely what we set out to prove.

☐

Observation 1.29. Let $M \models PA^{-}$ and let $k, l \in \mathbb{N}$. Then $k < l$ iff. $M \models \underline{k} < \underline{l}$.

Proof. We prove the implication from left to right first, and the implication from right to left will follow by the former one.

For the implication from left to right we assume that $k < l$. Since $k < l$, we get $l = k + d + 1$ for $d \in \mathbb{N}$. Furthermore, let us split the proof to the two cases based on the value of k.

$k = 0$: By Definition 1.7 $M \models \underline{k} = 0$. By Ax.15 $[0 \leq x]$ we have $M \models 0 \leq \underline{d}$, therefore $M \models \underline{k} \leq \underline{d}$. And by Corollary 1.3 we get that $M \models \underline{k} < \underline{d} + 1$. Since $\underline{k} = 0$, by Definition 1.7, we get by Ax.2 [commutativity +] and Ax.6 $[0, 1$ are neutral$]$ that $M \models \underline{k} < \underline{k} + (\underline{d} + 1)$. By Definition 1.7 and Observation 1.22 we may finally conclude that $M \models \underline{k} < \underline{l}$.

$0 < k$: Since $0 < d + 1$ we already know, using Definition 1.7,that $M \models 0 < \underline{(d + 1)}$. By Ax.11 $[x < y \rightarrow x + z < y + z]$ we get $M \models 0 + \underline{k} < \underline{(d + 1)} + \underline{k}$. Thanks to Definition 1.7 and Observation 1.22 can be concluded that $M \models \underline{k} < \underline{l}$.

The proof from left to right was finished.

For the implication from right to left. We have that $M \models \underline{k} < \underline{l}$. Assume for contradiction that the conclusion does not hold. Then by Ax.10 [trichotomy <] we have that $k = l$ or $l < k$. If $k = l$, then $M \models \underline{k} = \underline{l}$ which is again in contradiction with Ax.9 [irreflexivity $<$]. Otherwise if $l < k$, then we already know that $M \models \underline{l} < \underline{k}$. And by Ax.8 [transitivity $<$] can be concluded that $M \models \underline{l} < \underline{l}$ which is in contradiction with Ax.9 [irreflexivity $<$]. Either way we got a contradiction and thus the proof by contradiction is finished. □

Corollary 1.30 ($\underline{n}^M$ are distinct elements)**.** Let $M \models PA^-$ and let $m, n \in \mathbb{N}$ then $m = n$ iff. $M \models \underline{n} = \underline{m}$.

Proof. The implication $\Rightarrow$ is trivial. The implication $\Leftarrow$ follows by the previous Observation 1.29 and Ax.9 [irreflexivity $<$]. □

Observation 1.31. Let $M \models PA^-$ and $m \in \mathbb{N}$, then

$$M \models \forall x \, (x \leq \underline{m} \leftrightarrow x = \underline{0} \vee x = \underline{1} \vee \ldots \vee x = \underline{m})$$

Proof. Proof is by induction on m.

If $m = 0$, then the $\Leftarrow$ is immediate. And the $\Rightarrow$ follows immediately by Ax.15 [$0 \leq x$] and the combination of Ax.8 [transitivity $<$] and Ax.9 [irreflexivity $<$].

Let $m > 0$.

$\Leftarrow$: We get the implication from right to left for free using Observation 1.29.

$\Rightarrow$: If $M \models x = \underline{m}$ we are done. Otherwise if $M \models x < \underline{m}$ we have that $M \models x < \underline{(m-1)}+1$, by Definition 1.7 and since $0 < m$ implies $(m-1) \in \mathbb{N}$. Using Observation 1.16 we get that $M \models x + 1 \leq \underline{(m-1)} + 1$. And now applying Corollary 1.12 we finally get that $M \models x \leq \underline{(m-1)}$, but from this, applying the induction hypothesis on $m-1$, it follows that $M \models x = \underline{0} \vee \ldots \vee x = \underline{(m-1)}$ which is what we set out to prove.

□

Observation 1.32. Let $M \models PA^-$ and $l, k \in \mathbb{N}$, then

$$l \mid k \iff M \models \underline{l} \mid \underline{k}.$$

$\Rightarrow$: If $l \mid k$, then there exists $r \in \mathbb{N}$ s.t. $l \times r = k$, therefore $M \models \underline{l \times r} = \underline{k}$. By Observation 1.28 we get that $M \models \underline{l} \times \underline{r} = \underline{k}$, therefore $M \models \underline{l} \mid \underline{k}$.

$\Leftarrow$: If $M \models \underline{l} \mid \underline{k}$ then we get thanks to Corollary 1.20 that there exists $a \in M$ s.t. $M \models a \leq \underline{k} \wedge \underline{l} \times a = \underline{k}$. And by Observation 1.31 we get that there exists $r \in \mathbb{N}$ s.t. $M \models a = \underline{r}$, therefore $M \models \underline{l} \times \underline{r} = \underline{k}$. Therefore, again by Observation 1.28, we observe that $M \models \underline{l \times r} = \underline{k}$ for some $r \in \mathbb{N}$. And by a combination of Observation 1.29 and Observation 1.1 we may finally conclude that $l \times r = k$ from which the desired conclusion follows.

Standard vs. non-standard elements

In this subsection we observe that $\mathbb{N}$ embeds into any model of PA^-, give a characterization of non-standard models using non-standard elements and show that non-standard elements are greater than any standard ones.

Lemma 1.33. Let $M \models PA^-$, then the function $n \to \underline{n}^M$, denote this function as h, is an embedding from $\mathbb{N}$ into M.

Proof. Clearly, the described function h is a well defined function from $\mathbb{N}$ into M.

h maintains constants: $h(0) = \underline{0}^M = 0^M$ and $h(0) = \underline{1}^M = 1^M$, the last equalities are by Definition 1.7

h respects $+$: Let $k, l \in \mathbb{N}$, then

$$h(k + l) = \underline{k + l}^M = \underline{k}^M +^M \underline{l}^M = h(k) +^M h(l)$$

The second equality is by Observation 1.22.

h respects $\times$: Let $k, l \in \mathbb{N}$, then

$$h(k \times l) = \underline{k \times l}^M = \underline{k}^M \times^M \underline{l}^M = h(k) \times^M h(l)$$

The second equality is by Observation 1.28.

h respects $<$: Let $k, l \in \mathbb{N}$, then

$$k < l \iff \underline{k}^M <^M \underline{l}^M \iff h(k) <^M h(k)$$

The first $\iff$ is by Observation 1.29.

Since $<$ and $<^M$ are linear orders on $\mathbb{N}$ and M respectively, we actually only need that they obey Ax.9 [irreflexivity $<$] . and the prescribed function h respects them, it follows that the h must be injective.

We can conclude, from all that was written, that h is indeed an embedding from $\mathbb{N}$ into M. □

Observation 1.34. Let $G, M \models PA^-$ and let f be an embedding from G into M, then it must hold that $\forall n \in \mathbb{N}(f(\underline{n}^G) = \underline{n}^M)$.

Proof. The proof is by induction on n. If $n = 0$ or $n = 1$ the conclusion follows by Definition 1.7 and that f preserves constants by being an embedding. Assume that the observation holds for $0, \ldots, n$, then

$$f(\underline{(n+1)}^G) = f(\underline{n}^G +^G 1^G) = f(\underline{n}^G) +^M f(1^G) = \underline{n}^M +^M 1^M = \underline{(n+1)}^M,$$

where the first $=$ follow by Definition 1.7, the second by f being an embedding, the third by the induction hypothesis and the last one by Definition 1.7.

□

Observation 1.35. Let $M \models PA^-$, then M is a *non-standard* model of PA, i.e. it is not isomorphic to $\mathbb{N}$, iff. M has a *non-standard* element, i.e. it has an element which differs from $\underline{n}^M$ for every $n \in \mathbb{N}$.

Proof. For the implication from left to right. Let h be the embedding from $\mathbb{N}$ to M which is discussed in Lemma 1.33. Since M is a non-standard model we know that h can not be *onto*. Therefore we get an existence of $e \in M$ s.t. $\forall n \in \mathbb{N}\, h(n) \neq e$. It follows, by the definition of h, that e has to be a non-standard element of M.

For the implication from right to left. Assume for contradiction that there exists an isomorphism, call it I, from $\mathbb{N}$ onto M. Since M contains a non-standard element, denote one of those as e, there has to be $n \in \mathbb{N}$ s.t. $I(n) = e$, since I is onto. Applying Observation 1.34, with G being $\mathbb{N}$, we also know that $I(\underline{n}^{\mathbb{N}}) = \underline{n}^M$, where $\underline{n}^{\mathbb{N}}$ is just n. Therefore we get that $\underline{n}^M = e$, which contradicts our assumption that e is a non-standard element of M and finishes our proof. □

Non-standard elements are greater than the standard elements.

Corollary 1.36. Let $M \models PA^-$ and let $e \in M$. Then e is a non-standard element in M iff. $M \models \underline{n} < e$ for any $n \in \mathbb{N}$.

Proof. The implication from left to right follows by Ax.10 [trichotomy $<$] and Observation 1.31. The other implication follows by Ax.9 [irreflexivity $<$]. □

Nonstandardness is preserved with respect to $+$ and $\times$.

Observation 1.37. Let $M \models PA^-$ and let $a, e \in M$ s.t. e is a non-standard element of M. Then $a +^M e = e +^M a$ is a non-standard element of M.

Proof. The first equality follows by Ax.2 [commutativity $+$]. As for the non-standardness. Let $n \in \mathbb{N}$, by Corollary 1.36 $M \models \underline{n} < e$. By Ax.11 [$x < y \rightarrow x + z < y + z$] $M \models \underline{n} + a < e + a$. Using Observation 1.9 it follows that $M \models \underline{n} \leq \underline{n} + a$. And from Ax.8 [transitivity $<$] it follows that $M \models \underline{n} < e + a$. But n was arbitrary, therefore for any $n \in \mathbb{N}$ we have $M \models \underline{n} < e + a$, therefore by Corollary 1.36 we get that $e +^M a$ is a non-standard element of M. □

Observation 1.38. Let $M \models PA^-$ and let $a, e \in M$ s.t. e is a non-standard element of M and $a \neq 0^M$. Then $a \times^M e = e \times^M a$ is a non-standard element of M.

Proof. The first equality follows by Ax.4 [commutativity $\times$]. As for the non-standardness.

Let $n \in \mathbb{N}$, by Corollary 1.36 $M \models \underline{n} < e$. By Ax.15 [$0 \leq x$], i.e. $M \models 0 < a$, and Ax.12 [$(x < y \ \wedge 0 < z) \rightarrow x \times z < y \times z$] $M \models \underline{n} \times a < e \times a$. Using Observation 1.10 it follows that $M \models \underline{n} \leq \underline{n} \times a$. And from Ax.8 [transitivity $<$] it follows that $M \models \underline{n} < e \times a$. But n was arbitrary, therefore for any $n \in \mathbb{N}$ we have $M \models \underline{n} < e \times a$, therefore by Corollary 1.36 we get that $e \times^M a$ is a non-standard element of M. □

This concludes our inspection of the (non-)standard elements in models of PA^-.

One more concluding note, until now, we have always explicitly referenced to Definition 1.7 when using it. From now on, we will omit these types of references since they are hopefully obvious.

1.6 Initial segments

In this section, we observe that any $M \models PA^-$ contains at its beginning an isomorphic copy of $\mathbb{N}$.

First, we make the notion of "at its beginning" precise. Afterwards, we show the hinted result.

Initial segments

Definition 1.10 (Initial segment)**.** Let G, M be two L_A structures. We say that G is an *initial segment* of M, or M is an *end-extension* of G, in symbols $G \subseteq_e M$, iff. the two following conditions are met:

1. G is a substructure of M, denoted also by $G \subseteq M$,
2. for every $a \in G$ and $b \in M$, if $M \models b < a$, then $b \in G$.

As usually, if in addition $G \neq M$, then we say that G is a *proper initial segment* of M.

$\mathbb{N}$ is an "initial segment" of every model of PA^-

We show that for any model of PA^- there is an isomorphic copy of $\mathbb{N}$ which is an initial segment of that model.

Definition 1.11. Let $M \models PA^-$, we define $\mathbb{N}^M := \{\underline{n}^M | n \in \mathbb{N}\}$.

Theorem 1.39. Let $M \models PA^-$, then $\mathbb{N}^M$ is an initial segment of M which is isomorphic to $\mathbb{N}$.

Proof. Take the function h from $\mathbb{N}$ into M defined as follows $h(n) := \underline{n}^M$. By Lemma 1.33 we know that h is an embedding of $\mathbb{N}$ into M. And obviously $h(\mathbb{N}) = \mathbb{N}^M$

Recall that an image I of an embedding function f from L into R is a substructure of R and in fact f is an isomorphism from L onto I. This fact is an elementary model-theoretic observation.

Therefore we infer that

- $\mathbb{N}^M$ is a substructure of M,
- $\mathbb{N}$ is isomorphic to $\mathbb{N}^M$.

Last thing we need to show is that $\mathbb{N}^M$ satisfies the second condition in Definition 1.10.

Let $a \in \mathbb{N}^M$ and $b \in M$ s.t. $M \models b < a$. Since a is a standard element of M, we can conclude by the Corollary 1.36 that b must be a standard element of M. Since b is a standard element of M we immediately get that $b \in \mathbb{N}^M$ which finishes the proof. □

Let $M \models PA^-$, then we will sometimes write, assuming that no confusion arises, n for $\underline{n}^M$, for any $n \in \mathbb{N}$.

1.7 Equivalence of Δ_0 truths

In this section, we will prove a result of high importance, namely that a Δ_0 sentence is modeled by $\mathbb{N}$ iff. it is proved by PA^-.

Elementary substructures

We will start with a definition that will later relate the notion of initial segments to the notion of modeling formulas.

Definition 1.12. Let N, M be two L_A structures and let Γ be a set of L_A formulas. We say that N is a Γ-elementary substructure of M, denoted as $N \prec_\Gamma M$, iff. $N \subseteq M$ and for any $\varphi(\overline{x}) \in \Gamma$ and $\overline{a} \in N$ we have

$$N \models \varphi(\overline{a}) \iff M \models \varphi(\overline{a}).$$

In our usage, we will be setting Γ to Δ_0.

Preservation of Δ_0, Σ_1 truths

Initial segments preserve truth on Δ_0 formulas.

Theorem 1.40. Let $R \subseteq_e M$ be two L_A structures. Then we have $R \prec_{\Delta_0} M$.

Proof. Let R, M be as in the statement of the this theorem, let $\varphi(\overline{x})$ be any Δ_0 formula and $\overline{a} \in R^k$, where k is the length of $\overline{x}$.

We want to show that $R \models \varphi(\overline{a}) \iff M \models \varphi(\overline{a})$ We proceed by induction on the number of $\vee, \neg$ and $\exists$, we omit other logical *symbols* since they can be defined using the already mentioned ones.

Since $N \subseteq M$, then from a basic theorem of model theory stating that substructures "evaluate" quantifier free formulas identically, see for example Kirby [2019][Section 5.3, p. 26], we get that the conclusion of the theorem is true whenever $\varphi(\overline{x})$ is quantifier free. This proves the base step of our induction, and more of course.

Now for the induction steps.

case $\vee$, $\varphi(\overline{x}) \equiv \alpha(\overline{x}) \vee \beta(\overline{x})$:

$$\begin{gathered} R \models \varphi(\overline{a}) \iff R \models \alpha(\overline{a} \vee \beta\overline{a}) \iff \\ R \models \alpha(\overline{a}) \text{ or } R \models \beta(\overline{a}) \text{ by the induction hypothesis } \iff \\ M \models \alpha(\overline{a}) \text{ or } M \models \beta(\overline{a}) \iff \\ M \models \alpha(\overline{a}) \vee \beta(\overline{a}) \iff M \models \varphi(\overline{a}). \end{gathered}$$

case $\neg$, $\varphi(\overline{x}) \equiv \neg\alpha(\overline{x})$:

$$\begin{gathered} R \models \varphi(\overline{a}) \iff R \models \neg\alpha(\overline{a}) \iff \\ R \not\models \alpha(\overline{a}) \text{ by the induction hypothesis } \iff \\ M \not\models \alpha(\overline{a}) \iff \\ M \models \neg\alpha(\overline{a}) \iff M \models \varphi(\overline{a}). \end{gathered}$$

case $\exists$, $\varphi(\overline{x}) \equiv \exists y < t(\overline{x})\alpha(\overline{x}, y)$: Let it be that $R \models \exists y < t(\overline{a})\alpha(\overline{a}, y)$. Then there must be $b \in R$ s.t. $R \models b < t(\overline{a})$ and $R \models \alpha(\overline{a}, b)$, by the base step of our induction and the induction hypothesis we have both $M \models b < t(\overline{a})$ and $M \models \alpha(\overline{a}, b)$. And as such we get $M \models \exists y < t(\overline{a})\, \alpha(\overline{a}, y)$.

For the other direction assume $M \models \exists y < t(\overline{a})\, \alpha(\overline{a}, y)$. Then there must be $b \in M$ s.t. $M \models b < t(\overline{a})$ and $M \models \alpha(\overline{a}, b)$. Since $R \subseteq M$ and $\overline{a} \in R^k$ we know that $t(\overline{a})^M = t(\overline{a})^R$, to prove it formally one can use induction on the complexity of terms. Therefore $M \models b < t(\overline{a})^R$ and since $R \subseteq_e M$ we get that $b \in R$, from which it also follows that $R \models b < t(\overline{a})$, by the base step of our induction. So we have $b \in R$ s.t. $R \models b < t(\overline{a})$ and by the induction hypothesis we have $R \models \alpha(\overline{a}, b)$. Combining everything together we get $R \models \exists y < t(\overline{a})\, \alpha(\overline{a}, y)$, which finishes the proof.

□

Corollary 1.41. Let $M \models PA^-$ and $\varphi(\overline{x})$ be a Δ_0 formula. Then $\forall \overline{n} \in N$ we have $\mathbb{N} \models \varphi(\underline{n}) \iff M \models \varphi(\underline{n})$.

Proof. We have by Theorem 1.39 that $\mathbb{N}^M$ is isomorphic to $\mathbb{N}$ and also that $\mathbb{N}^M \subseteq_e M$.

Therefore by Theorem 1.40, we have that $\mathbb{N}^M \models \varphi(\underline{n}) \iff M \models \varphi(\underline{n})$.

Furthermore, by Kirby [2019][Section 3.4, p.15], we know that "being isomorphic to" preserves validity, which is quite an obvious result. Therefore, $\mathbb{N} \models \varphi(\underline{n}) \iff \mathbb{N}^M \models \varphi(\underline{n})$.

Hence, we can conclude that indeed

$$\mathbb{N} \models \varphi(\underline{n}) \iff M \models \varphi(\underline{n}).$$

□

Corollary 1.42. Let $M \models PA^-$ and ϕ be a Δ_0 sentence. Then $\mathbb{N} \models \phi \iff M \models \phi$.

Proof. This is a direct corollary of Corollary 1.41. □

Corollary 1.43. Let Γ be a set of L_A formulas and R, M two L_A structures s.t. $R \prec_\Gamma M$. Moreover let $\varphi(\overline{x})$ be a formula s.t. $\varphi(\overline{x}) \equiv \exists \overline{y}\, \psi(\overline{x}, \overline{y})$ and $\psi(\overline{x}, \overline{y})$ belongs to Γ. Then if $\overline{a} \in R^k$, where k is the length of $\overline{x}$, we have

$$R \models \varphi(\overline{a}) \Rightarrow M \models \varphi(\overline{a}),$$

Proof. If $R \models \varphi(\overline{a})$, then there has to be $\overline{b} \in R^l$, where l is the length of $\overline{y}$, s.t. $R \models \psi(\overline{a}, \overline{b})$. By $R \prec_\Gamma M$ we have $M \models \psi(\overline{a}, \overline{b})$, from which it follows that $M \models \varphi(\overline{a})$, which finishes the proof.

□

Lemma 1.44 (Σ_1 truth is preserved in PA^-)**.** Let M by any model of PA^- and let σ be a L_A sentence that belongs to the Σ_1 s.t. $\mathbb{N} \models \sigma$. Then $M \models \sigma$.

Proof. Let M and σ be as in the statement of the corollary. Since $\mathbb{N}$ is isomorphic to $\mathbb{N}^M$, by Theorem 1.39, and $\mathbb{N} \models \sigma$ we get that $\mathbb{N}^M \models \sigma$. The fact that isomorphism preserves validity is obvious but can be found e.g. in Kirby [2019][Section 3.4, p.15].

Continuing, again by Theorem 1.39 we have that $\mathbb{N}^M \subseteq_e M$. Therefore by Theorem 1.40 we note that $\mathbb{N}^M \prec_{\Delta_0} M$.

Since $\sigma \in \Sigma_1$ it must be of the form $\exists \overline{y} \psi(\overline{y})$ s.t. $\psi(\overline{y})$ is a Δ_0 formula. But now from Corollary 1.43, where $\overline{x}$ is empty, and keeping in mind that $\mathbb{N}^M \models \sigma$ follows that $M \models \sigma$. □

1.8 Gödel's lemma for $\mathbb{N}$

In this section, we state and prove a variation to Gödel's lemma for $\mathbb{N}$. This lemma is, roughly speaking, about coding sequences of numbers by a single number s.t. retrieving the i-th number from the sequence is (Δ_0) easy.

The proof to come closely follows the discussion given in Kaye [1991, p. 58].

Lemma 1.45 (Gödel's lemma for $\mathbb{N}$)**.** Define a L_A formula $\Theta(x, w, y, z)$ in the following way

$$\Theta(x, w, y, z) \equiv (z < ((y + 1) \times w + 1)) \wedge (\exists q \leq x(x = q \times ((y + 1) \times w + 1) + z)).$$

Then the following holds

(i) $\Theta(x, w, y, z)$ is a Δ_0 formula,

(ii) $\mathbb{N} \models \forall x, w, y \exists! z \Theta(x, w, y, z)$,

(iii) For any $k \in \mathbb{N}$ and $r_0, \ldots, r_k \in \mathbb{N}$ there exists $n, m \in \mathbb{N}$ s.t. $\forall l \leq k$ $\mathbb{N} \models \Theta(n, m, l, r_l)$.

Proof. So that no confusion can arise, everything in this proof is evaluated in the $\mathbb{N}$.

$\Theta(x, w, y, z)$ is obviously a L_A formula. We need to show that it satisfies all the mentioned points.

(i) This item is obvious.

(ii) The second item is obvious from the standard knowledge of $\mathbb{N}$.

(iii) Let $k \in \mathbb{N}$ and $(r_0, \ldots, r_k) \in \mathbb{N}^{k+1}$. First, we determine m and then n.

Determining m: Define $m := (max(r_0, \ldots, r_k, k))!$. Now we will observe that $\forall i, j \leq k$ s.t. $i \neq j$ we have $(i + 1) \times m + 1$ is relatively prime to $(j + 1) \times m + 1$, i.e. they have no common prime divisor.

Assume for contradiction that it is not the case. Therefore $\exists i < j \leq k$ in $\mathbb{N}$ and some prime number $p \in \mathbb{N}$ s.t. $p \mid (i + 1) \times m + 1$ and $p \mid (j + 1) \times m + 1$. Therefore $p \mid (j - i) \times m$. Therefore either $p \mid (j - i)$ or $p \mid m$. Since $(j - i) \in \mathbb{N}$ and $1 \leq (j - i) \leq k$ we again get that $p \mid m$. Either way we know that $p \mid m$. Since $p \mid (i + 1) \times m + 1$ and $p \mid m$ it follows that $p \mid 1$ which is clearly impossible and the proof by contradiction is finished.

Determining n Using the Chinese remainder theorem, see e.g. Pinter [2012][Chapter 23, p.233], we get that there exists $n \in \mathbb{N}$ s.t.

$$n \equiv r_0(\text{mod}(1 \times m + 1))$$
$$\vdots$$
$$n \equiv r_k(\text{mod}((k + 1) \times m + 1))$$

By the way we chose m it is obvious that $r_0, \ldots, r_k < m + 1$, therefore we actually get that

$$n \text{ mod } (1 \times m + 1) = r_0 \tag{1.1}$$
$$\vdots$$
$$n \text{ mod } ((k + 1) \times m + 1) = r_k$$

We immediately get from Equation 1.1 that $\mathbb{N} \models \Theta(n, m, l, r_l)$, for any $l \in [k]$.

□

We may note, that $\Theta(x, w, y, z)$ is intuitively equivalent to $(x \bmod ((y + 1) \times w + 1)) = z$. I.e. $\Theta(x, w, y, z)$ more or less expresses the mod function in $\mathbb{N}$.

To finish this section, we will notice few observation culminating in a very important property of $\Theta(x, w, y, z)$.

Observation 1.46. Let $M \models PA^-$ and let $\Theta(x, w, y, z)$ be as in Lemma 1.45. Also let $a, b, c, d \in M$. If $M \models \Theta(a, b, c, d)$, then $M \models d \le a$.

Proof. Assuming that $M \models \Theta(a, b, c, d)$ we get that there exists $q \in M$ s.t. $M \models a = q \times ((c + 1) \times b + 1) + d$. By Ax.15 $[0 \le x]$ we know that $M \models 0 \le q \times ((c+1) \times b+1)$, and by Corollary 1.7 we have $M \models 0+d \le q \times ((c+1) \times b+1)+d$, using Ax.2 [commutativity +] and Ax.6 [0, 1 are neutral] we finally get that $M \models d \le a$. □

Corollary 1.47. Let $M \models PA^-$ and let $\Theta(x, w, y, z)$ be as in Lemma 1.45. Also let $n \in \mathbb{N}$ and $b, c, d \in M$. If $M \models \Theta(\underline{n}, b, c, d)$, then $d = \underline{u}^M$ for some $n \ge u \in \mathbb{N}$, i.e. d is a standard element of M.

Proof. Proof is obvious by Observation 1.46 and Observation 1.31. □

Corollary 1.48. Let $M \models PA^-$ and let $\Theta(x, w, y, z)$ be as in Lemma 1.45. Also let $n \in \mathbb{N}$, then $M \models \forall w \forall y \exists! z \Theta(\underline{n}, w, y, z)$. Moreover this z is a standard element of M.

Proof. Let $w, y \in M$. We will split the proof into cases according to the different values that can be possessed by w and y.

$w, y \in \mathbb{N}^M$:

First assume that both w, y are standard elements of M, i.e. $w = \underline{m}^M$ and $y = \underline{l}^M$.

existence of z: We know that $\mathbb{N} \models \exists z\, \Theta(\underline{n}, \underline{m}, \underline{l}, z)$ by the second item in Lemma 1.45. Therefore $M \models \exists z \Theta(\underline{n}, \underline{m}, \underline{l}, z)$ by Lemma 1.44.

uniqueness of z: As for the uniqueness assume that $z_0, z_1 \in M$ s.t. $M \models \exists z\, \Theta(\underline{n}, w, y, z_0)$ and $M \models \exists z\, \Theta(\underline{n}, w, y, z_1)$. By Corollary 1.47 we know that $z_0, z_1 \in \mathbb{N}^M$. Therefore there exists $r_0, r_1 \in \mathbb{N}$ s.t. $z_0 = \underline{r_0}^M$ and $z_1 = \underline{r_1}^M$. Therefore we get that $M \models \Theta(\underline{n}, \underline{m}, \underline{l}, \underline{r_0})$ and $M \models \Theta(\underline{n}, \underline{m}, \underline{l}, \underline{r_1})$. By Lemma 1.44 we infer that $N \models \Theta(\underline{n}, \underline{m}, \underline{l}, \underline{r_0})$ and $N \models \Theta(\underline{n}, \underline{m}, \underline{l}, \underline{r_1})$. By the uniqueness of the second item in Lemma 1.45 we observe that $\underline{r_0}^{\mathbb{N}} = \underline{r_1}^{\mathbb{N}}$ which is just a complicated way of writing $r_0 = r_1$. But from the $r_0 = r_1$ follows that $z_0 = z_1$, which is what we wanted to show and the uniqueness is proved.

$w = 0^M$

Note that if $w = 0^M$, then $M \models (y + 1) \times w + 1 = 1$.

existence of z Set $z = 0^M$, setting $q = \underline{n}^M$, $M \models \Theta(\underline{n}, w, y, z)$, by Ax.15 $[0 \le x]$ and Ax.6 [0, 1 are neutral] .

uniqueness of z If z satisfies $\Theta(\underline{n}, w, y, z)$, then $M \models z < 1$ and by Ax.15 $[0 \le x]$, Ax.14 $[0 < 1 \wedge (0 < x \rightarrow 1 \le x)]$, Ax.8 [transitivity $<$] and Ax.9 [irreflexivity $<$] it follows that $M \models z = 0$, uniqueness follows.

otherwise

By Observation 1.37 and Observation 1.38 is $(y +^M 1) \times^M w +^M 1^M$ a non-standard element of M.

existence of z: Setting $z = \underline{n}^M$, then, setting $q = 0^M$, we have that $M \models \Theta(\underline{n}, w, y, z)$, namely by Corollary 1.36, Ax.15 $[0 \leq x]$, Ax.7 $[x \times 0 = 0]$ and Ax.2 [commutativity $+$] in combination withAx.6 $[0, 1$ are neutral$]$.

uniqueness of z Assume that $M \models \Theta(\underline{n}, w, y, z_0)$ and $M \models \Theta(\underline{n}, w, y, z_1)$. Then combining Ax.15 $[0 \leq x]$, Observation 1.38 and Observation 1.37 it follows that q must be set for both z's to 0^M. Therefore by Ax.4 [commutativity $\times$] and Ax.7 $[x \times 0 = 0]$ we get that $M \models \underline{n} = 0 + z_0 = 0 + z_1$. Applying Ax.2 [commutativity $+$] and Ax.6 $[0, 1$ are neutral$]$ we observe that $M \models z_0 = z_1$, which is what we wanted to show.

The moreover part follows directly by corollary 1.47 □

The part in the proof of Corollary 1.48 where w, y are standard elements (of M) is the most important for us. But for the sake of completeness we have decided to prove also the case where w or y is not a standard element (of M).

2. Observations and tools in PA

In this chapter we will extend, as already hinted at many times, axioms of PA^- with infinitely many other induction axioms that will result in a theory PA. We will also look at some "middle ground" theories, i.e. those which are stronger than PA^- and weaker than PA. Besides the already mentioned, we will look at a very useful lemma, called Overspill lemma, state a generalization of Gödels lemma introduced in section 1.8 for any model of PA and lastly we shall formally define the exponentiation function.

2.1 Introducing induction to the PA^-

Induction axioms

Let us start with one meta-definition.

Definition 2.1 (Induction on formula)**.** Let φ be a L_A formula with x being any variable from L_A(recall that we have only denumerably many variables). Then by $I_x\varphi$ we denote the following formula

$$\forall \overline{y}\,(\varphi(0,\overline{y}) \wedge \forall x(\varphi(x,\overline{y}) \rightarrow \varphi(x+1,\overline{y})) \rightarrow \forall x\varphi(x,\overline{y})),$$

where $\overline{y}$ are all the free variables in φ except the variable x.

Two comments are in place.

- Obviously, when x is not a free variable in φ, then $I_x\varphi$ states an obvious truth in any model. However, it does not do anything bad therefore we have decided to leave it like that and not to exclude these harmless cases.
- For the sake of definiteness, we should have chosen the order of variables in $\forall\overline{y}$. I.e. if $\overline{y}$ consists of x_i and x_j, for $i \neq j$, recall the formal definition of L_A from section 1.1, we should have determined whether it is $\forall x_i \forall x_j$ or vice versa. Well, in order to fulfill this need we can either state that the variable that goes first is the one with the smallest index, then the one with the second smallest index and so on. Or, we can just realize, what did probably most readers implicitly realize when reading Definition 2.1, that for the quantifier $\forall$ in its standard interpretation it does not matter how we order $\overline{y}$ in $\forall\overline{y}$.

Definition 2.2. Let Γ be a set of L_A formulas. Then by $I\Gamma$ we mean the theory resulting from the following set of axioms:

- Axioms $Ax.1 - Ax.15$ introduced in the section 1.1.
- The set of all the axioms of the form $I_x\varphi$ for $\varphi \in \Gamma$ and x being any variable in the L_A.

Most important theories for us will be $I\Delta_0$ and $I\Sigma$. And what is $I\Sigma$? It is the long awaited theory PA.

Definition 2.3 (PA)**.** The theory PA is the theory $I\Sigma$.

One remark is in place about the induction axioms. One might ask, why have not we opted, in order to define PA, for the following induction axiom, which might seem a bit more natural.

$$\forall X\,((0 \in X \wedge \forall x\,(x \in X \rightarrow (x+1) \in X)) \rightarrow \forall x\,(x \in X)),$$

where $\forall X$ quantifies over all subsets of the structure's domain. In fact, this axiom was stated by Giuseppe Peano himself, after whom is the PA^- and PA named, in his work Peano [1889], which is written in Latin, and one can read in English about the content of Peano's book in van Heijenoort [1967, p.83-97].

One problem is that trying to use this axiom would take us to the realm of *second-order* Boolos et al. [2007, Chapter 22] logic where standard model-theoretic tools like *Compactness Theorem* Kirby [2019, Chapters 8 and 11] and *Löwenheim–Skolem theorems* Kirby [2019, Chapters 12 and 13] don't hold, for proofs see e.g. Boolos et al. [2007, Chapter 22].

Moreover to that, $\mathbb{N}$ is the only one countable, up to isomorphism, structure satisfying PA^- together with the *second-order* induction axiom, for a beginning steps of a possible proof of the foregoing statement look e.g. at Enderton [1977, Chapter 4, mainly Theorem 4H].

Therefore we defined induction, and PA, this way, in a way trying to replicate the *second-order* induction axiom yet still remaining in the framework of the *first-order* logic.

Least number principle

We will show that using induction we can prove the often used "least number principle".

Lemma 2.1 (Least number principle)**.** Let $M \models PA$ and $\varphi(\overline{y}, x)$ be a L_A formula. Furthermore let $\overline{a} \in M^k$, where k is the length of $\overline{y}$. Then M models

$$(\exists z\,\varphi(\overline{a}, z)) \rightarrow (\exists z\,(\varphi(\overline{a}, z) \wedge \forall w < z\,(\neg\varphi(\overline{a}, w))))$$

Proof. Assume for contradiction that $M \models (\exists z\,\varphi(\overline{a}, z))$ and $M \not\models (\exists z\,(\varphi(\overline{a}, z) \wedge \forall w < z\,(\neg\varphi(\overline{a}, w))))$.

Using the second assumption we will show by induction on x that $M \models \psi(\overline{a}, x) \equiv \forall y \leq x\,\neg\varphi(\overline{a}, y)$ for all $x \in M$. First assume that $M \models x = 0$, we need to show that $M \models \neg\varphi(\overline{a}, 0)$, but this is obvious using our second assumption. Next assume that $M \models \psi(\overline{a}, x)$, then $M \models \forall y \leq x\,\neg\varphi(\overline{a}, y)$ and combining this fact with our second assumption we also get that $M \models \neg\varphi(\overline{a}, x+1)$. Everything combined we get that $M \models \forall y \leq x+1\,\neg\varphi(\overline{a}, y)$, i.e. $M \models \psi(\overline{a}, x+1)$. Then by induction in PA we get that $M \models \forall x\,\psi(\overline{a}, x)$ but this is clearly with a direct contradiction to our first assumption of $M \models (\exists z\,\varphi(\overline{a}, z))$. □

Our usage will be often the case, as usual, when $\varphi(\overline{a}, x)$ is a negation of some some formula $\psi(\overline{a}, x)$ s.t. we want to show $M \models \forall x\,\psi(\overline{a}, x)$ and we assume for contradiction that it does not hold.

2.2 Observations in PA or its weaker versions

Firs of all, we will show that there indeed exists a countable non-standard model of PA, hence also of $I\Delta_0$ and PA^-.

We will show even a stronger result, namely that there is a countable model of $Th(\mathbb{N})$ which is non-standard, where $Th(\mathbb{N})$ is the set of all true sentences in $Th(\mathbb{N})$.

Commentary. Since obviously $Th(\mathbb{N})$ proves everything, and possibly more, than what PA^- proves, we can use the standard terminology of non-standard elements.

Furthermore, again since obviously $Th(\mathbb{N})$ proves everything (because we have standard induction on $\mathbb{N}$), and possibly more, than what PA proves, it follows that a countable non-standard model of $Th(\mathbb{N})$ is a countable non-standard model of PA.

Theorem 2.2 (Non-standard model of $Th(\mathbb{N})$)**.** There exists a countable L_A structure M s.t. $M \models Th(\mathbb{N})$ and $M \ncong \mathbb{N}$, i.e. M is a non-standard countable model of $Th(\mathbb{N})$.

Proof. Let us extended L_A to L_A^c by adding one new constant symbol c.

And define $Th(\mathbb{N})^c := Th(\mathbb{N}) \cup \{\underline{n} \neq c | n \in \mathbb{N}\}$.

Clearly, when we take any finite subset T of $Th(\mathbb{N})^c$, we can define a L_A^c structure $\mathbb{N}^c$ which extends $\mathbb{N}$ by setting $c^{\mathbb{N}^c}$ to sufficiently large natural number. By sufficiently large natural number we mean any number m which is greater than any $n \in \mathbb{N}$ for which $\underline{n} \neq c$ is in T, since T is finite there must exist such a m.

Since $Th(\mathbb{N})$ does not use the constant c we get from $\mathbb{N} \models Th(\mathbb{N})$ that indeed $\mathbb{N}^c \models Th(\mathbb{N})^c$. And be the way we chose $c^{\mathbb{N}^c}$ we must have $\mathbb{N}^c \models (\{\underline{n} \neq c | n \in \mathbb{N}\} \cap T)$. Therefore we may conclude that $\mathbb{N}^c \models T$.

Since T was arbitrary finite subset of $Th(\mathbb{N})^c$ we get by Strong Compactness theorem, see e.g. Kirby [2019, Chapter 11], that there must exist a L_A^c structure M^c s.t. $M^c \models Th(\mathbb{N})^c$ and has cardinality, denoted as $|M^c|$ at most $|\Sigma^c|$, where we mean by Σ^c the set of all L_A^c formulas. For a very brief introduction to what the word "cardinality" mean, or in general to the different sizes of sets, see for a very brief introduction Kirby [2019, Chapter 10] or for a more in-depth look see e.g. Enderton [1977, Chapter 6].

By Kirby [2019, Proposition 10.6] we know that $|\Sigma^c|$ is equal to maximum of $|\mathbb{N}|$ and the size of the set containing exactly non-logical symbols in L_A^c. Since the latter set is finite we get that $|\Sigma^c|$ equals $|\mathbb{N}|$. Therefore we may conclude that $|M^c|$ is at most $|\mathbb{N}|$ which is the same as saying that $|M^c|$ is countable.

Let us forget about the constant c now, i.e. take the reduct of M^c to L_A and call this new structure M.

Now, M is still countable and still has an element e s.t. $M \models \underline{n} \neq e$ for any $n \in \mathbb{N}$. Furthermore, since $M^c \models Th(\mathbb{N})$ and the constant c is not present in any sentence of the $Th(\mathbb{N})$ we have that $M \models Th(\mathbb{N}))$.

Therefore by Observation 1.35 and by $Th(\mathbb{N})$ being a stronger theory than PA^- M must indeed be a countable non-standard model of $Th(\mathbb{N})$. □

Corollary 2.3 (Non-standard model of PA)**.** There exists a countable L_A structure M s.t. $M \models PA$ and $M \ncong \mathbb{N}$, i.e. M is a non-standard countable model of PA.

Proof. Follows directly by Theorem 2.2 and the commentary before it. □

Further follows standard, and important, theorem about unique quotients and remainders when dividing by non-zero divisors.

Theorem 2.4. Let $M \models I\Sigma_1$, and let $a, b \in M$ s.t. $a \neq 0^M$. Then there exists unique $q, r \in M$ s.t.

$$M \models b = q \times a + r \wedge r < a.$$

Proof. existence: Proof is by induction on the formula

$$\varphi(x, y) \equiv (y = 0 \vee \exists q, r((x = q \times y + r) \wedge r < y)),$$

with respect to the variable x. This formula is clearly a Σ_1 formula. And let $y \in M$. If $y = 0^M$, then there is nothing to prove.

Otherwise assume $y \neq 0^M$ which by Ax.15 $[0 \leq x]$ means that $M \models 0 < y$.

If $x = 0^M$, then set $q, r = 0^M$. By axioms Ax.4 [commutativity $\times$], Ax.7 $[x \times 0 = 0]$, Ax.6 [0, 1 are neutral] and Ax.15 $[0 \leq x]$ it follows that the formula is satisfied.

Otherwise assume $M \models \varphi(x, y)$ for some $x \in M$, and we need to show that $M \models \varphi(x + 1, y)$. Since $M \models \varphi(x, y)$ and $M \models y \neq 0$, there exists $q_x, r_x \in M$ s.t. $M \models x = q_x \times y + r_x \wedge r_x < y$.

If $M \models r_x + 1 < y$, then by Ax.1 [associativity $+$] it follows that $M \models \varphi(x + 1, y)$, setting q_{x+1} to q_x and r_{x+1} to $r_x +^M 1^M$.

Otherwise, by Observation 1.16, $M \models r_x + 1 = y$. Then setting q_{x+1} to $q_x +^M 1^M$ and r_{x+1} to 0^M, recall that $M \models 0 < y$, shows by Ax.4 [commutativity $\times$] ,Ax.5 [distributivity] and Ax.1 [associativity $+$] that $M \models \varphi(x + 1, y)$.

uniqueness: Let $x, y \in M$ s.t. $y \neq 0^M$, again recall by Ax.15 $[0 \leq x]$ that $M \models 0 < y$ immediately follows. Moreover, let us have $q, r \in M$ and $k, l \in M$ s.t.

$$M \models x = q \times y + r \wedge r < y$$

and

$$M \models x = k \times y + l \wedge l < y.$$

If $q = k$, then by Observation 1.6 it immediately follows that $r = l$.

It remains to show that $q = k$, assume for contradiction that it does not hold. By Ax.10 [trichotomy $<$] we may WLOG assume that $M \models q < k$.

Since $M \models q < k$ we get by the last item in Observation 1.11 that $M \models k = q + z \wedge 0 < z$, for some $z \in M$ s.t. by Ax.14 $[0 < 1 \wedge (0 < x \rightarrow 1 \leq x)]$ $M \models 1 \leq z$.

Let us observe the following,

$$M \models k \times y + l = (q \times y + z \times y) + l \geq q \times y + z \times y > q \times y + r.$$

The first equality is by Ax.4 [commutativity $\times$] and Ax.5 [distributivity]. The next $\geq$ is by Observation 1.9 and the last $>$ is by applying Ax.11

$[x < y \rightarrow x + z < y + z]$ to $M \models r < z \times y$. And $M \models r < z \times y$ follows by applying Ax.8 [transitivity $<$] to $M \models r < y$ and $M \models y \leq z \times y$. Where in turn $M \models y \leq z \times y$ follows by an application of Corollary 1.8, together with Ax.4 [commutativity $\times$] and Ax.6 [$0, 1$ are neutral], to the fact that $M \models 1 \leq z$.

Now using Ax.8 [transitivity $<$] we can conclude that $M \models k \times y + l > q \times y + r$. But combining $M \models k \times y + l = x = q \times y + r$ and $M \models k \times y + l > q \times y + r$ gives rise to a contradiction with Observation 1.1.

□

We will show that standard primes behave like primes in any model of PA.

Corollary 2.5. Let $M \models I\Sigma_1$, and let $p \in \mathbb{N}$ s.t. p is a prime number in $\mathbb{N}$. Then we have

$$M \models \forall x \forall y((\underline{p} \mid x \times y) \leftrightarrow (\underline{p} \mid x \vee \underline{p} \mid y))$$

Proof. The proof from right to left is obvious.

As for the proof from left to right. Let $x, y \in M$ s.t. $M \models \underline{p} \mid x \times y$, follows that there must be, using Ax.6 [$0, 1$ are neutral] and Observation 1.29, some $z \in M$ s.t. $M \models x \times y = \underline{p} \times z + 0 \wedge 0 < \underline{p}$.

By Theorem 2.4 for $x, \underline{p}^M$ and $y, \underline{p}^M$, and by $M \models 0 < \underline{p}$ which follows by Observation 1.29, we get that there exists unique $q_x, r_x, q_y, r_y \in M$ s.t. $M \models x = q_x \times \underline{p} + r_x \wedge r_x < \underline{p}$ and $M \models y = q_y \times \underline{p} + r_y \wedge r_y < \underline{p}$.

Assume for contradiction that the supposed conclusion does not hold, i.e. $M \models \neg(\underline{p} \mid x \vee \underline{p} \mid y)$. Then it follows that $M \models r_x \neq 0$ and $M \models r_y \neq 0$, using Ax.6 [$0, 1$ are neutral].

Using the Observation 1.31 we get that $M \models r_x = \underline{l}$ and $M \models r_y = \underline{k}$ s.t. $l, k \in \mathbb{N}$ and $0 < l, k < p$.

Evaluating $x \times^M y$ we have

$$M \models x \times y = (q_x \times \underline{p} + \underline{l})(q_y \times \underline{p} + \underline{k}) = \underline{p} \times (q_x q_y \underline{p} + q_x \underline{k} + q_y \underline{l}) + \underline{l \times k}$$

The second equality follows by Ax.1-Ax.5 together with Observation 1.22. Furthermore, since p is a prime number and $0 < l, k < p$ we get that there must by some $q, r \in \mathbb{N}$ s.t. $0 < r < p$ and $l \times k = p \times q + r$. Therefore we get by Observation 1.22, Observation 1.28 and Ax.5 [distributivity] that $M \models x \times y = \underline{p} \times (q_x q_y \underline{p} + q_x \underline{k} + q_y \underline{l} + \underline{q}) + \underline{r} \wedge 0 < \underline{r} < \underline{p}$. Since $M \models 0 < \underline{p}$ and $M \models 0 \neq \underline{r}$ by Observation 1.1, we get that this result is clearly in contradiction with the uniqueness in Theorem 2.4 because we also have $M \models x \times y = \underline{p} \times z + 0 \wedge 0 < \underline{p}$. □

From now on we will often put less detail in justifying every single step of proofs we gave with a hope that the reader is capable of filling all the gaps necessary.

2.3 Overspill lemma for the standard cut $\mathbb{N}$

This section is devoted to a very useful tool called Overspill lemma for $\mathbb{N}$.

Lemma 2.6 (Overspill lemma for $\mathbb{N}$). Let $M \models PA$, M be a non-standard model, and $\varphi(\overline{y}, x)$ be a L_a formula. Moreover let $\overline{a} \in M^k$, where k is the length of $\overline{y}$. Then if $M \models \varphi(\overline{a}, \underline{n})$ for all $n \in \mathbb{N}$ we have that there must exist some non-standard element $e \in M$ s.t. $M \models \varphi(\overline{a}, e)$.

Proof. Suppose for contradiction that the assumptions of the lemma hold but not the conclusion. Then $M \models \varphi(\overline{a}, 0)$ and if $M \models \varphi(\overline{a}, x)$ we necessary have $x \in \mathbb{N}^M$ therefore by our assumption $M \models \varphi(\overline{a}, x+1)$. But applying the induction, which we have on all L_A formulas, we get $M \models \forall x \varphi(\overline{a}, x)$. And since non-standard models have non-standard elements, by Observation 1.35, we get that there must be a non-standard element $e \in M$ s.t. $M \models \varphi(\overline{a}, e)$ which is the contradiction we wanted. □

Let us notice one simpler case of the lemma that holds in $I\Delta_0$, i.e. we have only changed PA for $I\Delta_0$.

Lemma 2.7 (Ovespill lemma on $I\Delta_0$ for $\mathbb{N}$). Let $M \models I\Delta_0$, M be a non-standard model, and $\varphi(\overline{y}, x)$ be a Δ_0 formula. Moreover let $\overline{a} \in M^k$, where k is the length of $\overline{y}$. Then if $M \models \varphi(\overline{a}, \underline{n})$ for all $n \in \mathbb{N}$ we have that there must exist some non-standard element $e \in M$ s.t. $M \models \varphi(\overline{a}, e)$.

Proof. Obviously, when we restrict ourselves to the formulas $\varphi(\overline{y}, x) \in \Delta_0$, then the proof in Lemma 2.6 can be carried out for any $M \models I\Delta_0$. □

This case will be later important for us, since for example using this weakening we can observe that Tennenbaum's theorem for addition holds actually in $I\Delta_0$ and not only in PA.

As you may have already guessed, by the fact that we emphasize "for $\mathbb{N}$" there are more general versions to those two lemmas which are for any *proper cut* I, for a definition see Kaye [1991, p. 70], and not only for $\mathbb{N}$, with the conclusion of $M \models \varphi(\overline{a}, e)$ for some $e \in M$ s.t. $M \models I < e$. There is also one more strengthening with conclusion that $M \models \forall x \leq e \varphi(\overline{a}, e)$ where e is a non-standard element of M. Naturally, a combination of the two extension also holds and the reader can find a proof of it in Kaye [1991, pp.70-71]. However, we will not need any of those for this text.

All of the versions of Overspill lemma, stated or hinted at, are due to Abraham Robinson.

We would like to note two last things. One is that besides this chapter the only time we will use induction will be indirectly through using some form of Overspill lemma. Second is that you can observe in the course of the text to follow, that in PART I only the Overspill lemma for Δ_0 formulas will be used.

2.4 Gödel's lemma in PA

In this section, we state another useful tool in PA. Using this tool we will formally extend our language/theory by the exponentiation function.

Lemma 2.8 (Gödel's lemma in PA). There exists a Δ_0 formula, which we can construct, $T(x, y, z)$ s.t. PA proves all the following points.

- $\forall x, y \, \exists! z \, T(x, y, z)$.

- $\forall z \exists x \, T(x, 0, z)$
- $\forall x, y, z \, \exists w \, ((\forall l \leq y \forall d \, (T(x, l, d) \leftrightarrow T(w, l, d)) \wedge T(w, y + 1, z))$.
- $\forall x, y, z \, (T(x, y, z) \rightarrow z \leq x)$.

We will follow instructive notation used in Kaye [1991, Section 5.2] to denote $T(x, y, z)$ as $(x)_y = z$.

We have decided not to include, quite a technical, proof of this lemma. We will at least mention that it is more or less a formalization of the proof we gave for the "Gödel's lemma for ℕ" in Theorem 1.45. For more details see e.g. Kaye [1991, Section 5.2].

2.5 Introducing the exponentiation function exp

This short section is devoted to the formal introduction of the exp function.

Definition 2.4 (The exp function)**.** We define the $exp(x, y)$ in theory PA, where x is the base and y is the exponent, using the following formula

$$\varphi_{\exp(x,y)}(x, y, z) \equiv \exists w \, ((w)_0 = 1 \wedge (w)_y = z \wedge (\forall l < y \, (w)_{l+1} = (w)_l \times x)).$$

As usual, we need to show the following observation.

Observation 2.9. Let $M \models PA$, then $M \models \forall x, y \exists! z \, \varphi_{\exp(x,y)}(x, y, z)$.

Proof. Let b be any element of M.

existence of z: Proof is by induction on the variable y in the formula

$$\exists z \, \varphi_{\exp(x,y)}(b, y, z).$$

If $M \models y = 0$, then we can just set z to 1^M and use the second item in Gödel's lemma in PA.

Otherwise $M \models \varphi_{\exp(x,y)}(b, y, z^y)$, for some $z^y \in M$, and we want to show that $M \models \varphi_{\exp(x,y)}(b, y + 1, z^{y+1})$ for some $z^{y+1} \in M$. In this case set z^{y+1} to $z^y \times^M b$ and use the third item in Gödel's lemma in PA to construct w to witness $M \models \varphi_{\exp(x,y)}(b, y + 1, z^{y+1})$ from the w witnessing $M \models \varphi_{\exp(x,y)}(b, y, z^y)$ by having $M \models (w)_{y+1} = z^{y+1}$.

uniqueness of z: The proof is again by induction on the variable y in the formula $\psi(b, y) \equiv \forall z_0, z_1 \, ((\varphi_{\exp(x,y)}(b, y, z_0) \wedge \varphi_{\exp(x,y)}(b, y, z_1)) \rightarrow z_0 = z_1)$.

If $M \models y = 0$, then everything works, since $M \models z_0 = 1 = z_1$.

Otherwise, if $M \models \psi(b, y)$ then we want to show that $M \models \psi(b, y + 1)$. Assume that there are $z_0, z_1 \in M$ s.t. $M \models \varphi_{\exp(x,y)}(b, y+1, z_0) \wedge \varphi_{\exp(x,y)}(b, y+1, z_1)$, and take the respective $w^0, w^1 \in M$ witnessing that M actually models the formula for z_0, z_1. Then we have that $M \models z_0 = (w^0)_{y+1} = (w^0)_y \times b$ and $M \models z_1 = (w^1)_{y+1} = (w^1)_y \times b$. But we also clearly have that w^0, w^1 are witnesses to $M \models (\varphi_{\exp(x,y)}(b, y, (w^0)_y) \wedge \varphi_{\exp(x,y)}(b, y, (w^1)_y))$.

Therefore by our induction hypothesis we get that $M \models (w^0)_y = (w^1)_y$ from which the conclusion of $M \models z_0 = z_1$ follows. Therefore we have $M \models \forall y \, \psi(b, y)$ and since b is any member of M we get that $M \models \forall x, y \, \psi(x, y)$, which finishes the proof of uniqueness.

□

Since it is not hard to construct a particular formula of interest over which we want to conduct induction in PA we will, from now on, often omit such a construction.

2.6 Properties of the $\exp$ function

Standard algebraic properties of the $\exp$ function

Observation 2.10 (Algebraic properties of exp)**.** Let $M \models PA$ and $n \in \mathbb{N}$, then

- $M \models \forall x, y, z \ \exp(x, y + z) = \exp(x, y) \times \exp(x, z)$,
- $M \models \forall x, y, z \ \exp(x \times y, z) = \exp(x, z) \times \exp(y, z)$
- $M \models \forall x, y, z \ \exp(\exp(x, y), z) = \exp(x, y \times z)$,
- $M \models \forall x \ \exp(x, \underline{n}) = x^{\underline{n}}$, recall the notation from Definition 1.9.

Proof. Proof of the first three items can be carried out by an induction within PA on z. A possible proof of the third item will also use that the first item is already proved.

Proof of the last item is by induction on n. □

Observation 2.11 (Properties of exp with respect to $<$)**.** Let $M \models PA$, then the following holds

- $M \models \forall x \ \exp(x, 0) = 1$
- $M \models \forall 0 < y \ \exp(0, y) = 0$
- $M \models \forall y \ \exp(1, y) = 1$
- $M \models \forall x \ \exp(x, 1) = x$
- Let $x \in M$ s.t. $M \models 1 < x$, then $M \models \forall y \ \exp(x, y) < \exp(x, y + 1)$, i.e. exp is an increasing function given $M \models 1 < x$.

Proof. First four items are obvious by the definition of exp.

The last item follows by induction on y, case when $M \models 0 = y$ is obvious by the definition of exp and the assumption $M \models 1 < x$. In the inductive step Ax.12 $[(x < y \ \wedge 0 < z) \rightarrow x \times z < y \times z]$ can be used. □

Miscellaneous property of the $\exp$ function

The goal of this subsection is to show that if $M \models \exp(x, y) = \exp(\underline{2}, z) \wedge z \neq 0$, then $M \models x = \exp(\underline{2}, w)$. But to be able to prove this result we will prove one related observation first.

Observation 2.12. Let $M \models PA$ and let $x, y \in M$. Then if $M \models \underline{2} \mid \exp(x, y)$, $M \models \underline{2} \mid x$ follows.

Proof. Proof is by induction on y in PA.

If $M \models y = 0$, then the assumption itself, i.e. $M \models \underline{2} \mid \exp(x, y)$, can not happen. Since $M \models \exp(x, y) = 1$ the first item in Observation 2.11. And that would mean that $M \models \underline{2} \mid \underline{1}$ which can not be by Observation 1.32.

Now, if the statement holds for y, we want to show that it also holds for $y+1$.

We know that $M \models \exp(x, y + 1) = exp(x, y) \times x$, e.g. by definition of exp. Since $M \models \underline{2} \mid \exp(x, y + 1)$, we get that $M \models \underline{2} \mid \exp(x, y) \times x$. By Corollary 2.5 we get that $M \models \underline{2} \mid x \vee \underline{2} \mid \exp(x, y)$. If $M \models \underline{2} \mid x$ we are done and if $M \models \underline{2} \mid \exp(x, y)$ we use the induction hypothesis to again conclude $M \models \underline{2} \mid x$. □

Observation 2.13. Let $M \models PA$ and $x, y, z \in M$ s.t. $M \models 0 < z$ and $M \models \exp(x, y) = \exp(\underline{2}, z)$. Then there exists $w \in M$ s.t. $M \models x = \exp(\underline{2}, w)$.

Proof. First, before the main part of the proof starts, let us mention one obvious fact, used often in the following proof, and namely that $M \models 1 < \underline{2}$.

Proof is going to be by contradiction. Hence, let us assume that there exists some element of M not satisfying the observation.

Let x be then the smallest such member of M not satisfying the observation, we know of its existence by Least number principle.

Since $M \models 0 < z$ we have that there exists $d \in M$ s.t. $M \models z = d + 1$. Therefore $M \models \exp(x, y) = \underline{2} \times \exp(\underline{2}, d)$.

Immediately follows that $M \models \underline{2} \mid \exp(x, y)$ from which we get, using Observation 2.12, that there is $x^{'} \in M$ s.t. $M \models x = \underline{2} \times x^{'}$.

If $M \models x^{'} = 1$, then we are done.

Otherwise $M \models x^{'} \neq 1$. Also note that if $M \models x^{'} = 0$, then $M \models \exp(x, y) \leq 1$ by the first two items of Observation 2.11. But thanks to the assumption that $M \models 0 < z$ and that $M \models \exp(\underline{2}, 0) = 1$, by the first item in Observation 2.11, we get, by the last item in Observation 2.11 - $\exp(\underline{2}, w)$ is an increasing function in M, that $M \models 1 < \exp(\underline{2}, z)$. Therefore the case when $M \models x^{'} = 0$ actually can not happen and we can conclude that $M \models 1 < x^{'}$.

For the same reason, as in the previous paragraph, we want to observe that $M \models 0 < y$. Because otherwise, by the first item of Observation 2.11, we get that $M \models \exp(x, y) = 1 < \exp(\underline{2}, z)$.

We can use the second item in Observation 2.10 to conclude that M models $\exp(x, y) = \exp(\underline{2}, y) \times \exp(x^{'}, y)$. Since $M \models 1 < x^{'}$ and $M \models 0 < y$ we get that $M \models 1 < \exp(x^{'}, y)$, by the last item in Observation 2.11. Similarly we get that $M \models 1 < \exp(\underline{2}, y)$.

From the last paragraph, using the last item in Observation 2.11, we can conclude that $M \models y < z$. Therefore there exist $b \in M$ s.t. $M \models z = y + b \wedge 0 < b$. Using the first item in Observation 2.10 and Observation 1.6, about cancellation from both sides of an equation, we get that $M \models \exp(x^{'}, y) = \exp(\underline{2}, b) \wedge 0 < b$. Since obviously $M \models x^{'} < x$ we have that $M \models x^{'} = \exp(\underline{2}, a)$, for some $a \in M$, recall that x is the smallest member of M not satisfying the observation.

But from the last conclusion in the previous paragraph it follows that $M \models x = \exp(\underline{2}, a + 1)$ which is the desired contradiction and the observation was proved. □

3. Recursion theory preliminaries

This chapter centers around recursive functions and their representability in PA.

Since this text is rather more about PA^-, PA and various theories in between them, we have decided not to include formal definition of (primitive) recursive functions, for one see e.g Boolos et al. [2007, Chapter 6].

As a direct consequence of the lack of the formal definition/s some statements are left unproved or left only with an informal justification.

3.1 Recursive & recursively enumerable sets

Definitions

Informal Definition 3.1 (Recursive (partial) function)**.** Intuitively, f is a *(partial) recursive functions* if f's domain is (a subset) of $\mathbb{N}^k$, for $k \in \mathbb{N}$, and f's range is a subset of $\mathbb{N}$. Moreover, there should be an algorithmic procedure A having $\mathbb{N}^k$ as its input domain satisfying the following.

- If $\overline{n} \in \mathbb{N}^k$ belongs the domain of f we have that A given $\overline{n}$ as its input, written as $A(\overline{n})$, stops after a finitely many finite steps and returns $f(\overline{n})$.
- And otherwise, if $\overline{n}$ does not belong to the domain of f, then $A(\overline{n})$ will never halt (and it will run forever).

With a loose image of (partial) recursive functions in mind, we will define recursive sets.

Intuitively, a set $X \subseteq \mathbb{N}$ is going to be recursive for us, if for every element of $\mathbb{N}$ we can algorithmically decide whether it is a member of $\mathbb{N}$ or not.

Hence the former of the following definitions.

Definition 3.2 (Characteristic function)**.** Let $X \subseteq \mathbb{N}^k$, then the *characteristic function of* X, denoted as χ_X, is a function with a domain $\mathbb{N}^k$ which maps $\mathbb{N}^k$ into $\{0, 1\}$. Moreover to that, $\forall \overline{n} \in \mathbb{N}^k\, (\overline{n} \in X \iff \chi_X(\overline{n}) = 1)$.

Definition 3.3 (Recursive set)**.** Let $X \subseteq \mathbb{N}$, then X is a *recursive* set iff. the characteristic function of X, i.e. χ_X, is a recursive function.

Definition 3.4 (Recursive relation)**.** Let $X \subseteq \mathbb{N}^k$, then X is a *recursive* relation iff. the characteristic function of X, i.e. χ_X, is a recursive function.

Let us recall one standard notation, when we write $g : D \longrightarrow E$ we mean that g is a function with domain D and the range of g is a subset of E.

Next, we will be also interested in recursively enumerable sets. Intuitively, we say that $X \subseteq \mathbb{N}$ is a recursively enumerable set if there exists an algorithmic procedure that will gradually write members of $\mathbb{N}$ to some output s.t. the following two conditions are met.

- Only members of X will be written out to the output.
- Every member of X will be written out (after a finite number of steps) to the output.

Note that we do no require the algorithmic procedure to terminate, i.e. it can go on forever. Also note that it is not problem when a member of X is written to the output more than once.

Hence the following formal definition.

Definition 3.5 (Recursively enumerable sets)**.** Let $X \subseteq \mathbb{N}$, then X is a *recursively enumerable*, r.e. for short, set iff. there exists a (partial) recursive function $f\colon D \longrightarrow \mathbb{N}$, where $D \subseteq \mathbb{N}$, s.t. $X = f[\mathbb{N}]$, i.e. X is the range of f.

Observation 3.1. Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ s.t. f a is partial recursive function. Then $f^{-1}[\{k\}]$ for any $k \in \mathbb{N}$ is a recursively enumerable set. Where $f^{-1}[A]$ is the set of all members x of the domain of f satisfying $f(x) \in A$.

Proof sketch. Since f is a partial recursive function there is some algorithmic procedure A as in Informal Definition 3.1.

We will construct procedures B and C, where the former uses the latter as a sub-procedure to show that indeed $f^{-1}[\{k\}]$ is a recursively enumerable set. Also C will take as its input a single natural number whereas B will take no input at all.

$C(n)$: Run n steps of $A(i)$ for every $i \leq n$. If for some $i \leq n$ $A(i)$ returns k we print i immediately to the output and proceed as planned.

B: We will enumerate whole $\mathbb{N}$ according to $<^{\mathbb{N}}$ and for every $n \in \mathbb{N}$ we run $C(n)$.

Now we claim that B is a witness to recursive enumerability of $f^{-1}[\{k\}]$. Also let us remark that enumeration $\mathbb{N}$ can be surely done recursively.

Clearly, B writes to the output only members of $f^{-1}[\{k\}]$.

On the other hand, when $m \in f^{-1}[\{k\}]$, there must exist some $n \in N$ s.t. $A(m)$ returns k in at most n steps (of A).

Therefore, at latest, when we run the sub-procedure $C(n)$ we will write, during the run of $C(n)$, m to the output. For this argument to work we need to know that $C(i)$ takes a finite number of steps for every $i \in \mathbb{N}$, but this is obvious. And we also need to know that B eventually runs $C(n)$. But that obviously stems from the third item in the following list which in turn follows by the first two items in the following list.

- $C(i)$ takes a finite number of steps for every $i \in \mathbb{N}$.
- We do only finitely many steps between calls of C.
- We enumerate $\mathbb{N}$, hence by the previous two items we call $C(i)$ in B sooner or later for every $i \in \mathbb{N}$.

The proof is finished. □

Relation between recursive and recursively enumerable sets

Observation 3.2. Let $X \subseteq \mathbb{N}$. Then X is a recursive set iff. X and its complement, denoted as $\overline{X}$, are recursively enumerable sets.

Proof sketch. $\Rightarrow$: To recursively enumerate X, we will enumerate whole $\mathbb{N}$ according to $<^{\mathbb{N}}$, which can be surely done recursively, and when considering $i \in \mathbb{N}$ we compute $\chi_X(i)$, recall that χ_X is total. If $\chi_X(i) = 1$, then we write i to the output and proceed to $i+1$. And otherwise, i.e. if $\chi_X(i) = 0$, we do not write i to the output and proceed to $i+1$.

We obviously write to the output only members of X.

And if $n \in X$, we obviously write it the output after finitely many steps. This is because to compute $\chi_X(i)$ for any $i \in \mathbb{N}$ takes us only finitely many steps which in turn follows from the fact that χ_X is a total recursive function.

To show that $\overline{X}$ is recursively enumerable simply write out i iff. $\chi_X(i) = 0$ instead of $\chi_X(i) = 1$.

$\Leftarrow$: Assume that there are algorithmic procedures A_X and $A_{\overline{X}}$ witnessing recursive enumerability of X and $\overline{X}$.

To compute $\chi_X(i)$ for $i \in \mathbb{N}$ we start both processes A_X and $A_{\overline{X}}$, alternating between them, i.e. we run a few steps of A_X, then $A_{\overline{X}}$, then A_X and so on.

If i gets written out to the output during the run of A_X, we immediately halt A_X, return that $\chi_X(i) = 1$ and halt the whole process of computing $\chi_X(i)$. And if i gets written out to the output during the run of $A_{\overline{X}}$, we immediately halt $A_{\overline{X}}$, return that $\chi_X(i) = 0$ and halt the whole process of computing $\chi_X(i)$.

Since $X \cup \overline{X} = \mathbb{N}$, we get that i must be written out to the output sooner or later by one of the two processes. Therefore the whole process of computing $\chi_X(i)$ must eventually halt.

As for the correctness. If we conclude that $\chi_X(i) = 1$, then it must be that i was written during the process A_X. Therefore $i \in X$ and we gave the right answer. On the other hand, if we return that $\chi_X(i) = 0$, then it must be that i was written during the process $A_{\overline{X}}$. Therefore $i \notin X$ and we again gave the right answer.

□

We will now mention two important facts. Proofs of the two statements, in augmented versions, can be found in Boolos et al. [2007].

Lemma 3.3 (Coding of recursive functions)**.** There exits a way to enumerate all the single variable recursive functions into single list $h_0, h_1, \ldots$ I.e. $\forall i \in \mathbb{N}$ h_i is a recursive single variable function and for every single variable recursive function g there exists $j \in \mathbb{N}$ s.t. $g = h_j$.

Proof. Analogous proof, the one in the book is given for Turing machines, can be found in Boolos et al. [2007, Section 4.1]. □

Lemma 3.4 (Universal diagonal recursive function)**.** There exits a recursive function $U : \mathbb{N} \longrightarrow \mathbb{N}$ s.t.

- $U(x)$ is defined iff. $h_x(x)$ is defined.
- Assuming $h_x(x)$ is defined, then $U(x) = h_x(x)$.

Where we use $h_x(y)$ from Lemma 3.3.

Proof. Similar proof can be found in Boolos et al. [2007, Section 8.1]. □

An important notion of recursive inseparability is going to be introduced together with a proof of existence of recursively enumerable recursively inseparable sets.

Definition 3.6 (Recursively inseparable sets)**.** Two sets $A, B \subseteq \mathbb{N}$ are called *recursively inseparable*, r.i. for short, iff.

- A and B are disjoint,
- there exists no recursive set X s.t. $A \subseteq X$ and $B \cap X = \emptyset$.

Since a recursive set X is recursive iff. its complement is recursive, obvious corollary of Observation 3.2 or note that $\chi_{\overline{X}} = 1 \dot{-} \chi_X$ is intuitively a recursive function witnessing the recursiveness of $\overline{X}$, we get that A is recursively inseparable to B iff. B is recursively inseparable to A. Hence the slightly ambiguous wording in the definition does not cause any problems.

Lemma 3.5. There are two recursively inseparable sets s.t. they are both recursively enumerable, r.i.r.e. for short.

Proof. Define two sets $A := \{n \in \mathbb{N} | U(n) \text{ is defined } \wedge U(n) = 0\}$ and $B := \{n \in \mathbb{N} | U(n) \text{ is defined } \wedge U(n) = 1\}$. Since U is a (partial) recursive function it is intuitively sound, by Observation 3.1, that A and B are recursively enumerable. Moreover to that, they are clearly disjoint.

Last step to showing that A, B are r.i.r.e. is showing that there is no recursive set X s.t. $A \subseteq X$ and $B \cap X = \emptyset$.

Assume for contradiction that it is not the case, i.e. there exists a recursive set X with the property stated in the previous paragraph.

Take the *characteristic* function, with respect to X, χ_X. χ_x must be a single variable (total) recursive function. Therefore there exists $x \in \mathbb{N}$ s.t. $\chi_X = h_x$.

Let us inspect whether $x \in X$ or not.

$x \in X$: Then $\chi_X(x) = 1$, therefore $h_x(x) = 1$, therefore $x \in B$ from which follows that $X \cap B \neq \emptyset$.

$x \notin X$: Then $\chi_X(x) = 0$, therefore $h_x(x) = 0$, therefore $x \in A$ from which follows that $A \not\subseteq X$.

Either way we got a contradiction with the assumption that $A \subseteq X$ and $B \cap X = \emptyset$.

Therefore there can not exists such a recursive set X satisfying $A \subseteq X$ and $B \cap X = \emptyset$, and thus the proof is finished. □

3.2 Representing recursive functions in PA^-

Let us mention that the following lemma holds also for the opposite direction, i.e. not only the $\Rightarrow$ holds but also the $\Leftarrow$ holds.

Lemma 3.6 (Representation of recursive functions in $\mathbb{N}$)**.** Let $k \in \mathbb{N}$ and let $f : A \longrightarrow \mathbb{N}$ where $A \subseteq \mathbb{N}^k$. If f is a recursive function, then there exist a Σ_1 formula $\sigma_f(\overline{x}, y)$, where $\overline{x}$ is of length k, s.t. $\forall \overline{n}, m \in \mathbb{N}^{k+1}$ we have

$$(f(\overline{n}) \text{ is defined } \wedge f(\overline{n}) = m) \iff N \models \sigma_f(\overline{n}, m).$$

Proof. Proof can be found in Kaye [1991, Section 3.1]. □

For the following lemma we again have that it holds in the other direction as well, but we will not need that result.

Lemma 3.7 (Representation of recursively enumerable sets in $\mathbb{N}$)**.** Let $X \subseteq \mathbb{N}$ s.t. X is a recursively enumerable set, then there exists a Σ_1 formula $\psi_X(y)$ s.t. for all $n \in \mathbb{N}$ we have $n \in X \iff N \models \psi_X(n)$.

Proof. Let X by a recursively enumerable set (which is by our definition immediately a subset of $\mathbb{N}$).

Since X is r.e. there must exist a partial recursive function f s.t. X is f's range. Moreover let $\sigma_f(\overline{x}, y)$ be a Σ_1 formula from Lemma 3.6.

We claim that $\psi_X(y) \equiv \exists \overline{x}\, \sigma_f(\overline{x}, y)$ satisfies the conclusion of the lemma. Let us verify it.

- If $m \in X$, then $\exists \overline{n} \in \mathbb{N}^k$ s.t. $(f(\overline{n})$ is defined $\wedge f(\overline{n}) = m)$. Therefore, $N \models \sigma_f(\overline{n}, m)$ from which follows that $N \models \exists \overline{x}\, \sigma_f(\overline{x}, m)$ which is the same as $N \models \psi_X(m)$.
- If $m \notin X$, then there is no $\overline{n} \in \mathbb{N}^k$ s.t. $(f(\overline{n})$ is defined $\wedge f(\overline{n}) = m)$ from which follows that $N \not\models \exists \overline{x}\, \sigma_f(\overline{x}, m)$ which is the same as $N \not\models \psi_X(m)$.

□

Next, we introduce a definition, and a corresponding lemma, about representing functions in any extension of PA^-.

Definition 3.7. Let $k \in \mathbb{N}$ and $f : \mathbb{N}^k \longrightarrow \mathbb{N}$. Then we say that f is represented in some theory T extending PA^- if there exists a formula $\vartheta_f(\overline{x}, y)$, where $\overline{x}$ is of length k, s.t. for all $\overline{n}, m \in \mathbb{N}^{k+1}$ the following holds

- $T \vdash \exists! z\, \vartheta_f(\overline{n}, z)$.
- $f(\overline{n}) = m \iff T \vdash \vartheta_f(\underline{n}, \underline{m})$.

Notice that the definition applies only to total functions.

Lemma 3.8 (Representation of recursive functions in PA^-)**.** Let f be a total recursive function, then f is represented in PA^-, and thus in any extension of it.

Proof. Proof can be found in Kaye [1991, Section 3.2]. □

3.3 Representation of the n-th prime function in PA^-

Definition 3.8 (n-th prime function)**.** We will denote by $p(n)$ a function from $\mathbb{N}$ into $\mathbb{N}$ s.t. $p(n)$ is going to be the $(n+1)$-th prime number in $\mathbb{N}$.

E.g. $p(0) = 2, p(1) = 3, \ldots$.

The main point of this section is that $p(n)$ can be represented in PA^- (almost) in the sense of Definition 3.7.

One way of solving this task is to realize the following two points.

- Function $p(n)$ is total - obvious.
- Function $p(n)$ is recursive.

  Intuitively it follows by the following algorithmic procedure $A(n)$ which calls a sub-procedure $B(i)$.

  A: We enumerate $\mathbb{N}$, according to $<^{\mathbb{N}}$. And we call $B(i)$ to test whether i is a prime or not.

  If i is a prime and if so far, not counting i, we have found exactly n primes we return i and end. Otherwise we continue with $i+1$.

  $B(i)$: We check primality of i by checking whether $1 < i$ and whether for every $k, l < i$ we have $k \times l \neq i$.

  Obviously, $B(i)$ takes only finitely many steps as well as A in between different i's. And since A enumerates $\mathbb{N}$ with respect $<^{\mathbb{N}}$, which can be surely done recursively, and $B(i)$ obviously asses whether is i a prime number correctly, we get that A will indeed return $p(n)$.

Hence we got by the previous discussion the following observation.

Observation 3.9. Function $p(n)$ is recursive.

And now we can apply Lemma 3.8 to get actually a good way to represent, using a Σ_1 formula, the n-th prime function in PA^-. Denote such a formula $\Pi(x, y)$. Let us note that we will use this representation often, for its convenience and standardness only, compared to the representation we are going to introduce.

This procedure is perfectly fine for everything that is to come and solely using this way of representing $p(n)$ we would be able to show, using our proof-procedure, that Tennenbaum's theorem for addition holds in $I\Sigma_1$. As we will see later, the actual part that enforces $I\Sigma_1$, and not some weaker theory like $I\Delta_0$, is partly caused by the complexity, from the point of Arithmetical hierarchy, of a formula used to represent the $p(n)$ function.

Since we strive for the stronger result, we prove the lemma named "Representing" $p(n)$ in non-standard models of PA^- by a Δ_0 formula.

Lemma 3.10 ("Representing" $p(n)$ in non-standard models of PA^- by a Δ_0 formula)**.** Let us recall the Δ_0 formula $\Theta(w,t,x,y)$ from Section 1.8, where (w,t) intuitively codes some sequence of which is y the x-th member. Then define $\Pi(z,x,y)$ as $\exists w,t < z\,\psi(z,x,y,w,t)$ where $\psi(z,x,y,w,t)$ is a conjunction of the following Δ_0 formulas

(i) $\Theta(w,t,0,\underline{2})$

(ii) $\forall r_0 < z\,(\Theta(w,t,0,r_0) \to r_0 = \underline{2})$

(iii) $\Theta(w,t,x,y)$

(iv) $\forall l \leq x\,\exists r_l < z\,\Theta(w,t,l,r_l)$

(v) $\forall l \leq x\,\forall r_l < z\,(\Theta(w,t,l,r_l) \to (1 < r_l \wedge \forall a,b < z\,(a \times b = r_l \to a = 1 \vee b = 1)))$

(vi) $\forall l < x\,\forall r_l, r_{l+1} < z\,[(\Theta(w,t,l,r_l) \wedge \Theta(w,t,l+1,r_{l+1})) \to r_l < r_{l+1}]$

(vii) $\forall l < x\,\forall r_l, r_{l+1} < z\,\{[\Theta(w,t,l,r_l) \wedge \Theta(w,t,l+1,r_{l+1})] \to [\forall r_l < q < r_{l+1}\,(q \leq 1 \vee (\exists a,b < z\,(a \times b = q \wedge a \neq 1 \wedge b \neq 1)))]\}$, where $\forall r_l < q < r_{l+1} \ldots \equiv \forall q < r_{l+1}\,(r_l < q \to \ldots)$

For the sake of unambiguity, let us highlight that variables are only pieces of syntax r_l and r_{l+1}, i.e. we do not substitute for l or $l+1$ some actual value.

Now let M be a non-standard model of PA^-, and let e be any non-standard element of e.

Then for every $n \in \mathbb{N}$ we have

- $M \models \forall y_0, y_1\,(\Pi(e,\underline{n},y_0) \wedge \Pi(e,\underline{n},y_1) \to y_0 = y_1)$ and
- $M \models \Pi(e,\underline{n},\underline{p(n)})$.

Proof. Obviously, by the definition of Δ_0 formulas, is $\Pi(z,x,y)$ a Δ_0 formula.

Let us try to interpret intuitively first all the conjuncts of $\psi(z,x,y,w,t)$ where z is set to "infinity".

Recall once more that when $\mathbb{N} \models \Theta(w,t,x,y)$, it means that the pair (w,t) codes y as the x-th element of some sequence. In any model of PA^- we do not have, or we have not shown, that necessarily such a y exists or is unique. Nevertheless, we will still use the terminology of coding.

(i) $\underline{2}^M$ is coded by (w,t) as one of its 0-th members.

(ii) $\underline{2}^M$ is the only 0-th element of (w,t) when we restrict ourselves to elements smaller than z.

(iii) y is the x-th element coded by (w,t).

(iv) For any $M \models l \leq x$ there is some element of M that is coded as l-th element by (w,t).

(v) If $M \models l \leq x$ and we take some l-th element coded by (w,t), we get an element which is greater than 1 and irreducible, both with respect to M.

(vi) If $M \models l < x$ and we take some l-th element, denote it as r_l, and some $(l+1)$-th element, denote it as r_{l+1}, coded by (w, t) we get that $M \models r_l < r_{l+1}$.

(vii) If we again have $M \models l < x$ and we take some l-th element, denote it as r_l, and some $(l+1)$-th element, denote it as r_{l+1}, coded by (w, t) we get that for any element q which is strictly between them, in M, q is not irreducible, in M.

Let us proceed to the actual proof of the two points in the statement of the lemma.

- Assume $M \models \Pi(e, \underline{n}, y_0)$ and $M \models \Pi(e, \underline{n}, y_1)$. Moreover let (w_0, t_0) and (w_1, t_1) be the respective witnesses. Our goal is to show that $M \models y_0 = y_1$.

  We will prove $M \models \forall l \leq \underline{n} \forall z_0, z_1 ((\Theta(w_0, t_0, l, z_0) \wedge \Theta(w_1, t_1, l, z_1)) \rightarrow z_0 = z_1)$. Obviously, the desired result will follow.

  The proof is going to be by standard induction on l in $\mathbb{N}$. More specifically by Observation 1.31 it is enough to show that $\forall l \leq n$, where $l \in \mathbb{N}$, and $\forall z_0, z_1 \in M$ we have $M \models (\Theta(w_0, t_0, \underline{l}, z_0) \wedge \Theta(w_1, t_1, \underline{l}, z_1)) \rightarrow z_0 = z_1$.

  $l = 0$: By the second item we know that $M \models z_0 = \underline{2} = z_1$ assuming that $M \models z_0, z_1 < e$. But by Observation 1.46 we know that only elements $z \in M$ s.t. $M \models z \leq w$ can satisfy $M \models \Theta(w, \_, \_, z)$, for any $w \in M$. And since $M \models w_0, w_1 < e$ it follows that actually $M \models z_0 = z_1$ for any members of M, not only those smaller than e, which is what we wanted.

  $l = k + 1$: Again assume that $M \models \Theta(w_0, t_0, \underline{l}, z_0) \wedge \Theta(w_1, t_1, \underline{l}, z_1)$.
  By the fourth item we know that there is some $a \in M$ s.t. M models $\Theta(w, t, \underline{k}, a)$ and by our induction hypothesis it is a unique one.
  But since

  - $M \models a < z_0, z_1$, by the sixth item,
  - they both must satisfy the same condition α described in the fourth item,
  - there can be no element between any of those two z's and a s.t. it satisfies α, by the seventh item,

  we get that indeed $M \models z_0 = z_1$.
  Therefore the first item in the statement of the lemma holds.

- By the last item in Lemma 1.45 we know that there exits some $w, t \in \mathbb{N}$ s.t. $\forall l \leq n$ we have $\mathbb{N} \models \Theta(w, t, l, p(l))$.

  Since Θ is a Δ_0 formula, we get by Corollary 1.42 that $M \models \Theta(\underline{w}, \underline{t}, \underline{l}, \underline{p(l)})$ for any $l \leq n$.

  Furthermore, since e is a non-standard element, we know that M models $\underline{w}, \underline{t}, \underline{p(l)} < e$, for any $l \in \mathbb{N}$.

  It is not hard to realize that we are done if we manage to show that for any $y \in M$, if $M \models \Theta(\underline{w}, \underline{t}, \underline{l}, y)$ then necessarily $M \models y = \underline{p(l)}$. But this follows immediately by Corollary 1.48.

  Proof of this item, as well as the whole proof, is hereby finished.

□

3.4 When is a model recursive?

Formal definition

Motivation

First of all, only structures that have countable domain will be admitted into the consideration of being recursive/computable.

Intuitively speaking, it is because all the standard models of computation are defined with respect to a countable domain.

Furthermore, it seems only natural that models which do not have countable domain will not be considered recursive/computable. It is since to even represent all the elements of the domain, let alone functions/relations on that domain, using some way which represents

(i) different elements *differently* and

(ii) every element *finitely*

is impossible for an uncountable domain, because otherwise the domain would be countable by "definition".

And when we are unable to sufficiently represent elements of the domain, then it does not make that much of a sense of asking whether we can sufficiently represent functions/relations of a given model algorithmically.

Hence, intuitively speaking, only models of countable domain will be admitted into consideration.

Definition

Furthermore, since we have defined recursive functions/relations to be always functions/relations over $\mathbb{N}$, we will restrict domain of respective models to $\mathbb{N}$.

Definition 3.9 (Recursive model)**.** Let L be some language s.t. $L_A \subseteq L$, $PA^- \subseteq T$ and $M \models T$, i.e. L extends/expands language L_A and T extends the theory PA^-. Furthermore assume that M has domain equal to $\mathbb{N}$.

Then we define the following.

- If f is a functional symbol in L, then we say that M is recursive with respect to f, or f is recursive in M, if f^M is a recursive function.
- If R is a relational symbol in L, then we say that M is recursive with respect to R, or R is recursive in M, if R^M is a recursive relation.

However, this is not much of a restriction. Since if we have some L structure M s.t. $M \models T$, and $dom(M)$ is countable. Then we can define new L structure with domain $\mathbb{N}$ that is isomorphic to M. We will prove it at once in Observation 3.12 but before that let us prove one more observation.

Observation 3.11 (Countable models of PA^- are denumerable)**.** Let $M \models PA^-$, L be some extension of L_A and $dom(M)$ is countable, then it is denumerable, i.e. there is an bijection between $dom(M)$ and $\mathbb{N}$.

Proof. Since $dom(M)$ is countable it means that $dom(M)$ is denumerable or finite. Assume for contradiction that it is finite.

Since L contains constants M can not be empty.

Let $x \in dom(M)$ be the maximum of this set with respect to $<^M$. We know that such an element exists by the second item in Observation 1.4. By Ax.14 $[0 < 1 \wedge (0 < x \to 1 \leq x)]$ we know that $M \models 0 < 1$ therefore by Ax.11 $[x < y \to x + z < y + z]$ we get that $M \models x < 1 + x$, where $(1 + x)^M \in M$.

Hence by Ax.8 [transitivity $<$] there exists $y \in M$ s.t. $\forall z \in M\, (M \models z < y)$, therefore also $M \models y < y$ which is in direct contradiction with Ax.9 [irreflexivity $<$].

Therefore the domain of M can not be finite and is denumerable. □

Observation 3.12 (Every model of PA^- is isomorphic to one with domain $\mathbb{N}$)**.** Let $M \models PA^-$, L be some extension of L_A and $dom(M)$ is countable. Then there exists a L structure G s.t. $dom(G) = \mathbb{N}$, $G \models PA^-$ and $G \cong M$.

Proof. By Observation 3.11 we know that there exists some bijection I from $\mathbb{N}$ onto M, recall that I^{-1} must be a bijection from M onto $\mathbb{N}$.

Let us create the structure G step by step so that I is a witness to $G \cong M$. Let us highlight that we will write $(I(x_0), \dots, I(x_n))$ as $I(\overline{x})$.

- Set $dom(G) = \mathbb{N}$.
- If c is a constant symbol of L then just set c^G to $I^{-1}(c^M)$.
- If f is a function symbol in L, then define $f^G(\overline{n})$ as $I^{-1}(f^M(I(\overline{n})))$.
- If R is a relation symbol in L, then define $\overline{n} \in R^G$ iff $I(\overline{n}) \in R^M$.

Since I is a bijection from $\mathbb{N}$ onto M, I^{-1} is a bijection from M onto $\mathbb{N}$ it follows that G is a well defined L structure which has domain $\mathbb{N}$.

And again since I is bijection from $\mathbb{N}$ onto M combined with the way we have defined interpretation of symbols in L for G, it follows that I is indeed an isomorphism from G to M.

Since $M \models PA^-$ and $G \cong M$, $G \models PA^-$ follows. □

Let us conclude this section on recursivity of models with one useful observation.

Observation 3.13. Let $M \models PA^-$, L be some language expanding L_A, $dom(M)$ equals $\mathbb{N}$ and $l \in \mathbb{N}$. Then there exists a L structure G, s.t.

- $G \cong M$,
- $dom(G) = \mathbb{N}$,
- if $f \in L$ and f is recursive in M, then f is recursive in G,
- if $R \in L$ and R is recursive in M, then R is recursive in G,
- $\forall r \in \mathbb{N}$ s.t. $r \leq l$ we have $\underline{r}^G = r$.

I.e. that there exists a structure isomorphic to the original one s.t. the interpretation of all the terms $0, \dots, \underline{r}$ is known to us and is actually $0, \dots, r$.

Proof. The proof is going to be by induction on l, where we assume that the observation holds for all $r \in \mathbb{N}$ s.t. $r < l$. Other way to look at what will follow is that we present a single step of an algorithm that takes a structure $G^{'}$ satisfying the conclusion for $l - 1$ and creates a structure G satisfying the conclusion for l.

Let $G^{'}$ be the L structure that we get from induction hypothesis. More specifically, if $l = 0$, then set $G^{'}$ to M and otherwise set $G^{'}$ to the structure satisfying the conclusion of the just being proved observation for $l - 1$. I.e. $G^{'}$ either way satisfies the conclusion of the just being proved observation for all $r < l$.

Define s as a function from $\mathbb{N}$ into $\mathbb{N}$ in the following way.

$$s(n) := \begin{cases} \underline{l}^{G^{'}} & n = l, \\ l & n = \underline{l}^{G^{'}}, \\ n & \text{otherwise.} \end{cases}$$

Note that if $l = n = \underline{l}^{G^{'}}$, i.e. both the first and the second condition are satisfied, then nothing bad happens since according to the first condition is $s(n) = \underline{l}^{G^{'}}$ which is the same as $s(n) = l$ by the second condition.

Since $dom(G^{'}) = \mathbb{N}$, s is a well defined function from $\mathbb{N}$ into $\mathbb{N}$.

Since s clearly permutes (at most) two elements on $\mathbb{N}$ and other elements remain intact it follows that s is a bijection on $\mathbb{N}$.

Lastly, since s permutes (at most) two elements, we have $s = s^{-1}$.

Let us construct step by step G, similarly as in Observation 3.12.

- Set $dom(G) = \mathbb{N}$.
- If c is a constant symbol of L then just set c^G to $s^{-1}(c^{G^{'}})$.
- If f is a functional symbol in L, then define $f^G(\overline{n})$ as $s^{-1}(f^{G^{'}}(s(\overline{n})))$.
- If R is a relational symbol in L, then define $\overline{n} \in R^G$ iff $s(\overline{n}) \in R^{G^{'}}$.

We have used s as well as s^{-1} to emphasize the correspondence to Observation 3.12. However, since $s = s^{-1}$ we could have written s instead of all s^{-1}'s.

By the way we have defined G, it is obvious that $dom(G) = \mathbb{N}$, G is a L structure and s is a witnesses to $G \cong M$.

Furthermore, since s permutes only two elements, i.e. makes only a local/finite change, then if some functional/relational symbol f/R was recursive with respect to $G^{'}$, then it must be also recursive with respect to G.

Or to look at it from other perspective, s is obviously a recursive function. Therefore we get f^G as a composition of recursive total functions, hence it is recursive. And, intuitively speaking, recursive functions should be closed under composition since when we have some procedure A that is by it self computable except for calls to other computable procedure B, we still think of A as being computable as a whole.

An analogous, intuitive, argument applies to relations. Since we ask whether some element that we can compute belongs to some relation that is computable, i.e. we can decide whether an element belongs there or not algoritmically.

Last thing to check is whether $\forall r \leq l$ we have $G \models \underline{r}^G = r$. The proof is by induction on r.

$r < l$: Since $r < l$, we have by induction hypothesis that $r = \underline{r}^{G'}$.

Furthermore, since $r \neq l$ we have by Corollary 1.30 that $\underline{r}^{G'} \neq \underline{l}^{G'}$, therefore by the previous observation we have $r \neq \underline{l}^{G'}$, hence $s(r) = r$.

We know, by induction hypothesis, that $G' \models x = \underline{r}$, with x set to r. And since s^{-1} is an isomorphism from G' onto G we get that $G \models x = \underline{r}$ with x set to $s^{-1}(r) = s(r) = r$. And therefore indeed $r = \underline{r}^G$.

$r = l$: First note that $s(\underline{l}^{G'}) = l$.

Clearly $G' \models x = \underline{l}$ for x set to $\underline{l}^{G'}$. And since s^{-1} is an isomorphism from G' onto G we get that $G \models x = \underline{l}$ with x set to $s^{-1}(\underline{l}^{G'}) = s(\underline{l}^{G'}) = l$, which is what we wanted to show.

One commentary is in place. Since $l \in \mathbb{N}$, the induction/algorithm that we have shown a single step of, needs to be applied only $l + 1$, i.e. *finitely*, many times to create G. Therefore we indeed retain recursiveness of respective functions/relations. Since e.g. if $f \in L$ is a recursive function with respect to M, we apply only finitely many times, possibly different, recursive functions s to the the original function f^M, actually $2 \times (l+1)$ times in total when we count all the compositions. Hence f^G is indeed recursive. And an analogous argument holds for relations.

We are mentioning this because if we made some other kind of "induction" where there are needed infinitely many induction steps, to get from the base of an induction to the case we actually wanted to prove in the first place, the described process wouldn't need to work.

The proof is finished. □

Why is not the formal definition actually that important

We would like to highlight to the reader that this subsection is not that precise, nevertheless, we believe that the reader will understand what we are trying to achieve as well as will be, intuitively, conveyed that everything works as is going to be described.

In this subsection, as the title suggest, we will try to relax the definition of recursive models.

It should not be that surprising that the condition on $dom(M) = \mathbb{N}$ is quite a technical one, caused by a specific formalization of algorithmic processes using recursive functions.

First, assume that A, B are two denumerable sets and I is a bijection from A onto B. Intuitively, I codes A onto B and I^{-1} codes B onto A.

Furthermore, if I as well as I^{-1} are computable in some broad sense, then it means that we can computably code A onto B and vice versa.

Assume from now on that I as well as I^{-1} are indeed computable.

Moreover, it should hold that if we come up with some reasonable representation of A and B in $\mathbb{N}$, then there exists a recursive bijection H over $\mathbb{N}$ s.t. when we look at $\mathbb{N}$ as if it was A and B, we get that H coincides with I as well as H^{-1} coincides with I^{-1}.

Furthermore, if $A = \mathbb{N}$ or $B = \mathbb{N}$, then I or I^{-1} are such a reasonable representations mentioned in the last paragraph.

Informal Definition 3.10 (Computable coding)**.** Let A and B be two denumerable set. Furthermore let I be a bijection from A onto B. Then we call I a *computable coding* (of A onto B) iff. I and I^{-1} are computable.

Informal Definition 3.11 (Computably codable set)**.** Let A be a denumerable set, then we say that A is a *computably codable set* iff there exists a *computable coding* from $\mathbb{N}$ onto A.

Commentary. Let us mention, that in practice to show that A is a *computably codable set* it does suffice to show that there exists a *computable coding* from A onto $\mathbb{N}$, since there exists one iff there exists *computable coding* from $\mathbb{N}$ onto A.

What are some simple examples of such a *computably codable sets*? One is $\mathbb{Z}$ and the witness, i.e. respective *computable coding*, is e.g. $I(n) = (-1)^n \times ((n + 1) \text{ div } 2)$, where it is intuitively evident that I and I^{-1} are computable.

For an inventory of *computable codings* used in the course of this text, we will utilize them in section 6.3, section 9.1 and section 11.2, one should look at Appendix A.

Observation 3.14. Let L be some language, M a L-structure, $dom(M)$ be a *computably codable set* and T a theory over L s.t. $M \models T$. Then there exists a L structure G s.t.

- $dom(G) = \mathbb{N}$.
- $G \cong M$.
- $G \models T$.
- If $f \in L$ is a functional symbol and f^M is computable, then f^G is recursive in G.
- If $R \in L$ is a relational symbol and R^M is computable, then R^G is recursive in G.

Proof sketch. Since $dom(M)$ is a *computably codable set*, there exists a bijection I from $\mathbb{N}$ onto $dom(M)$ s.t. I and I^{-1} are computable.

Define now G in the same way as in Observation 3.12. I.e.

- Set $dom(G) = \mathbb{N}$.
- If c is a constant symbol of L then set c^G to $I^{-1}(c^M)$.
- If f is a functional symbol in L, then define $f^G(\overline{n})$ as $I^{-1}(f^M(I(\overline{n})))$.
- If R is a relational symbol in L, then define $\overline{n} \in R^G$ iff $I(\overline{n}) \in R^M$.

Evidently G is a L-structure and $G \cong M$ which implies $G \models T$.

If f^M is computable, and since composition of computable functions is again computable in the same vein as is calling a computable sub-procedure B from a computable procedure A, we get that f^G is a computable function over $\mathbb{N}$, hence f^G is recursive.

Analogously, if R^M is computable, i.e. we can decide algoritmically for any element of $dom(M)$ whether or not it does belong to R^M, and I is also computable, i.e. we can algoritmically find for any $\overline{n}$ the value $I(\overline{n})$, it follows that R^G is computable relation over $\mathbb{N}$, hence R^G is a recursive relation over $\mathbb{N}$.

□

What are some valid examples that satisfy the premises in Observation 3.14?

Continuing with the example $\mathbb{Z}$, which is a computably codable set, L will consist of a binary functional symbol $+$ and a binary relational symbol $<$ as its only, not counting $=$, non-logical symbols. The structure M is going to be $(\mathbb{Z}, +^{\mathbb{Z}}, <^{\mathbb{Z}})$, where $+^{\mathbb{Z}}, <^{\mathbb{Z}}$ will have their standard interpretation in $\mathbb{Z}$ and T is going to be axiomatized by Ax.1, Ax.2, Ax.8, Ax.9 and Ax.10 from Axioms of PA^-. Clearly, L,M and T are a valid example of a premise in Observation 3.14 as well as are $+^{\mathbb{Z}}$ a $<^{\mathbb{Z}}$ intuitively computable functions/relations.

Corollary 3.15. Let L be some language s.t. $L_A \subseteq L$, U be a L-structure, T a L theory extending PA^- and $U \models T$.

Furthermore let $L^0 \subseteq L$, where non-logical symbols as well as $=$ are preserved in L^0. And (U, L^0) be a reduct of U to the language L^0.

Under the listed assumptions, if there exists a L^0 structure U' s.t. $(U, L^0) \cong U'$ and $dom(U')$ is a *computably codable set*,

then there exists a L structure G satisfying the following.

- $dom(G) = \mathbb{N}$
- $G \cong U$
- $G \models T$
- If $f \in L^0$ is a functional symbol and $f^{U'}$ is computable, then f^G is recursive in G.
- If $R \in L^0$ is a relational symbol and $R^{U'}$ is computable, then R^G is recursive in G.

Proof sketch. Let H be an isomorphism from U' onto (U, L^0).

We will define a L structure M s.t. M is an expansion of U' with respect to L^0, i.e. they have the same domain and they interpret symbols from L^0 in the same way.

We define interpretation for symbols in $L \backslash L^0$ in the following way.

- If c is a constant symbol of $L \setminus L^0$ then set c^M to $H^{-1}(c^U)$.
- If f is a functional symbol in $L \setminus L^0$, then define $f^M(\overline{x})$ as $H^{-1}(f^U(H(\overline{x})))$.
- If R is a relational symbol in $L \setminus L^0$, then define $\overline{x} \in R^M$ iff $H(\overline{x}) \in R^U$.

We have that $dom(M)$ is *computably codable set* where M is a L-structure. Furthermore, since $(U, L^0) \cong U'$ and by the way we have interpreted symbols from $L \setminus L^0$ when expanding U' to M we get that $M \cong U$ and therefore also $M \models T$.

Lastly, when we were expanding $U^{'}$ to M the interpretation of symbols from L^0 remained unchanged Therefore functional/relational symbols from L^0 which interpretations were computable, with respect to $U^{'}$, have computable interpretations with respect to M as well.

Combining the last two paragraphs, we can apply Observation 3.14, to get the desired result and the proof is finished. □

Lastly, we would like to emphasize that *codings* in this subsection are not related to the process of coding sets described in chapter 4.

4. Coding sets in PA

A much of this section is inspired by Smith [2014, sections 5 to 8].

4.1 Equivalence of different encodings

Let T be some extension of PA^-.

Definition 4.1 (Canonical coding of sets)**.** Let $M \models T$ and let $X \subseteq \mathbb{N}$. We say that X is *canonically coded* in M iff. there exists $a \in M$ s.t. $\forall n \in \mathbb{N}\,(n \in X \iff M \models \exists z\,(\Pi(\underline{n}, z) \wedge z \mid a))$.

Let us comment that since $\Pi(x, y)$ represents function $p(n)$, from the point of view of Definition 3.7, there is only one element in M satisfying $M \models \Pi(\underline{n}, z)$ for any $n \in \mathbb{N}$ and this element is $\underline{p(n)}^M$.

Definition 4.2 (Coding of sets)**.** Let $M \models T$ and let $X \subseteq \mathbb{N}$. We say that X is *coded* in M iff. there exists a L_A formula $\varphi(\overline{x}, y)$ and $\overline{b} \in M$ s.t. $\forall n \in \mathbb{N}\,(n \in X \iff M \models \varphi(\overline{b}, \underline{n}))$.

Actually, only the implication from right to left, of the following lemma, will be important to us. However, we have decided to show both implications, based on preference, the reader can certainly skip the first one.

Lemma 4.1 (Equivalence of coding sets in $I\Delta_0$)**.** Let M be a non-standard model of $I\Delta_0$ and $X \subseteq \mathbb{N}$. Then X is canonically coded in M iff. it is coded in M by Δ_0 formula.

Proof. $\Rightarrow$: Let $a \in M$ and e be some non-standard element of M, then mainly by Lemma 3.10 and Corollary 1.36, $M \models \exists z\,(\Pi(\underline{n}, z) \wedge z \mid a)$ iff. $M \models \exists z < e\,(\Pi(e, \underline{n}, z) \wedge z \mid a)$. Where $\Pi(z, x, y)$ is a Δ_0, as we know by Lemma 3.10, as well as is the relation $\mid$ expressible by a Δ_0 formula by Corollary 1.20. Therefore the formula $\exists z < w\,(\Pi(w, x, z) \wedge z \mid v)$ is a Δ_0 formula and the $\Rightarrow$ follows.

$\Leftarrow$: Let $\varphi(\overline{x}, y)$ be some Δ_0 formula and let $\overline{b} \in M$ s.t. $\forall n \in \mathbb{N}$ we have the following equivalence $n \in X \iff M \models \varphi(\overline{b}, \underline{n})$.

Let us define $\psi(w, \overline{x}, y)$ as

$$\exists w_0 < w\, \forall y_0 \leq y\, [(\exists z \leq w\, (\Pi(w, y_0, z) \wedge z \mid w_0)) \leftrightarrow \varphi(\overline{x}, y_0)].$$

Since $\Pi(w, y_0, z)$ and $\varphi(\overline{x}, y_0)$ are Δ_0 formulas we get that $\psi(w, \overline{x}, y)$ is a Δ_0 formula.

Let e be a non-standard element of M. We will show that $\forall m \in \mathbb{N}$ we have $M \models \psi(e, \overline{b}, \underline{m})$.

Note that by Observation 1.31 we know that it is sufficient to show the equivalence only for $y_0 = \underline{0}^M, \ldots, \underline{m}^M$.

Define r as $r := \Pi_{l \in (X \cap [m])} p(l)$, this time Π is the standard product function (in case $X \cap [m] = \emptyset$, the product is 1). And set w_0 to $\underline{r}^M$.

Clearly by Corollary 1.36 we have $M \models w_0 < e$. We claim that actually

$$M \models \forall y_0 \leq \underline{m}\, [(\exists z \leq e\, (\Pi(e, y_0, z) \wedge z \mid w_0)) \leftrightarrow \varphi(\bar{b}, y_0)].$$

Let $M \models y_0 \leq \underline{m}$, which, as we have already pointed out, means that $M \models y_0 = \underline{q}$, for some natural number $0 \leq q \leq m$.

$\Rightarrow$: If $M \models (\exists z \leq e\, (\Pi(w, y_0, z) \wedge z \mid w_0))$, then we know by Lemma 3.10, and non-standardness of e, that $M \models \underline{p(q)} \mid \underline{r}$. By Observation 1.32 the $p(q) \mid r$ follows. And by the definition of r we get that $q \in X$, therefore indeed $M \models \varphi(\bar{b}, y_0)$, which is what we wanted to show.

$\Leftarrow$: If $M \models \varphi(\bar{b}, y_0)$ then $q \in X$, since we have $q \leq m$ as well, it follows that $p(q) \mid r$ and by Observation 1.32 $M \models \underline{p(q)} \mid \underline{r}(= w_0)$. And again by properties of $\Pi(\_, \_, \_)$ and since e is a non-standard element $M \models (\exists z \leq e\, (\Pi(e, y_0, z) \wedge z \mid w_0))$, which is what we wanted to show.

Now,Lemma 2.7, i.e. Overspill lemma on Δ_0 formulas, can be applied to acquire a non-standard element $c \in M$ s.t. $M \models \psi(e, \bar{b}, c)$. And since standard elements are below, with respect to $<$, non-standard ones by Corollary 1.36 we get that there exists $a \in M$ s.t. $\forall n \in \mathbb{N}$,

$$M \models (\exists z \leq e\, (\Pi(e, \underline{n}, z) \wedge z \mid a)) \leftrightarrow \varphi(\bar{b}, \underline{n}).$$

And since $\Pi(w, x, y)$ and $\Pi(x, y)$ are equivalent over PA^- when $x \in \mathbb{N}^M$ and w is non-standard we get by Lemma 3.10 that $\forall n \in \mathbb{N}$,

$$M \models (\exists z \leq e\, (\Pi(\underline{n}, z) \wedge z \mid a)) \leftrightarrow \varphi(\bar{b}, \underline{n}).$$

Furthermore, we can replace $\exists z \leq e$ by $\exists z$ since by Definition 3.7 there can be no $z \in M$ that is non-standard, which would follow by $M \models e \leq z$, and $M \models \Pi(\underline{n}, z)$.

Therefore there is $a \in M$ s.t. $\forall n \in \mathbb{N}$ we have

$$(n \in X \iff M \models \exists z\, (\Pi(\underline{n}, z) \wedge z \mid a)),$$

which is precisely what we wanted to show.

□

Commentary. Let us mention that the proof of $\Leftarrow$ in the just proved lemma, namely when we use *Overspill* which is in turn proved by induction on respective Δ_0 formulas, is the point about which we talked in section 3.3.

Specifically, when we were saying that the complexity, with respect to Arithmetical hierarchy, of formula representing $p(n)$ (partly) implies the theory in which we can show that Tennenbaum's theorem for addition holds.

Commentary. Also please bear in mind that the only time we have used $M \models I\Delta_0$ instead of just using $M \models PA^-$ was when we used Overspill lemma for Δ_0 formulas. Therefore, we can replace in Lemma 4.1 the assumption of $M \models I\Delta_0$ by $M \models PA^-$ and M satisfies Overspill lemma for all the Δ_0 formulas.

Lastly, let us mention, as a possible point of interest, that when M is a non-standard model of PA, then M canonically codes a set iff M codes it. (In this case we do not restrict ourselves only to Δ_0 formulas.) One can carry out an analogous proof to the one we gave in Lemma 4.1. Actually, this time it would be easier, since $\Rightarrow$ is trivial and $\Leftarrow$ can be done analogously, and even without using $\Pi(x, y, z)$.

4.2 Encoding of a non-recursive set

Lemma 4.2 (A non-recursive set which can be coded in $I\Delta_0$)**.** Let M be a non-standard model of $I\Delta_0$, then there exists a non-recursive set $X \subseteq \mathbb{N}$ s.t. X can be coded in M by a Δ_0 formula.

Proof. Let us recall that by Lemma 3.5 there exists a recursive inseparable recursively enumerable sets A, B.

By Lemma 3.7 we know that there must exist some Σ_1 formulas representing A, B in $\mathbb{N}$. And by Observation 1.17 these formulas "need" only one unbounded existential quantifier.

To be less ambiguous, we have two Δ_0 formulas $\alpha(x, y)$, $\beta(x, y)$ s.t.

$$n \in A \iff N \models \exists y\, \alpha(\underline{n}, y)$$

and

$$n \in B \iff N \models \exists y\, \beta(\underline{n}, y).$$

Since $A \cap B = \emptyset$, we have for every $m \in \mathbb{N}$ that

$$N \models \forall x \leq \underline{m}\, \forall y_A \leq \underline{m}\, \forall y_B \leq \underline{m}\, (\neg\alpha(x, y_A) \vee \neg\beta(x, y_B)).$$

Moreover, the just written sentence is a Δ_0 sentence. Therefore by Corollary 1.42 we have $\forall m \in \mathbb{N}$ the following

$$M \models \forall x \leq \underline{m} \forall y_A \leq \underline{m} \forall y_B \leq \underline{m}\, (\neg\alpha(x, y_A) \vee \neg\beta(x, y_B)).$$

Using Overspill lemma on Δ_0 formulas, i.e. Lemma 2.7, we get a non-standard element e of M s.t.

$$M \models \forall x \leq e\, \forall y_A \leq e\, \forall y_B \leq e\, (\neg\alpha(x, y_A) \vee \neg\beta(x, y_B)).$$

Let us define now the set X as $\{n \in \mathbb{N} | \varphi(e, \underline{n})\}$ where the $\varphi(y, x)$ is defined as $\exists y_A \leq y\, \alpha(x, y_A)$. Clearly, X is coded in M by a Δ_0 formula.

It remains to show that X is not recursive. For this, it suffices to show that X separates A and B, i.e. $A \subseteq X$ and $B \cap X = \emptyset$, because A and B are recursively inseparable.

$A \subseteq X$: If $n \in A$, then $N \models \exists y\, \alpha(\underline{n}, y)$. Therefore there is $m \in N$ s.t. $N \models \alpha(\underline{n}, \underline{m})$.

By Corollary 1.42 we have $M \models \alpha(\underline{n}, \underline{m})$. And, as we have mentioned many times, since are standard elements below non-standard ones we have $M \models \exists y_A \leq e\, \alpha(\underline{n}, y_A)$, which is the same as $M \models \varphi(e, \underline{n})$. And thus $n \in X$.

$B \cap X = \emptyset$: Assume for contradiction that $\exists n \in B$ s.t. $n \in X$. Then we have $M \models \varphi(\underline{n}, e)$, i.e. $M \models \exists y_A \leq e\, \alpha(\underline{n}, y_A)$.

Moreover, since $n \in B$ we have that $N \models \exists y\, \beta(\underline{n}, y)$. By an analogous argument as in the previous item we get $M \models \exists y_B \leq e\, \beta(\underline{n}, y_B)$.

Everything combined, and again keeping in mind that $M \models \underline{n} \leq e$, we have

$$M \models \exists x \leq e\, \exists y_A \leq e\, \exists y_B \leq e\, (\alpha(x, y_A) \wedge \beta(x, y_B)),$$

which can not be since

$$M \models \forall x \leq e\, \forall y_A \leq e\, \forall y_B \leq e\, (\neg\alpha(x, y_A) \vee \neg\beta(x, y_B)).$$

□

Corollary 4.3 (Canonical coding of a non-recursive set and its complement)**.** Let $M \models I\Delta_0$, then there exists a non-recursive set X s.t. X as well as its complement $\overline{X}$ can be canonically coded in M.

Proof. By Lemma 4.2 there exists a non-recursive set X which can be canonically coded by a Δ_0 formula in M. Obviously, since Δ_0 formulas are closed with respect to negation, we have that also $\overline{X}$ can be code by a Δ_0 formula in M.

Applying Lemma 4.1 we get the desired result. □

Corollary 4.4. Let $M \models PA$, then there exists a non-recursive set X s.t. there exists $a, c \in M$ for which we have

- $n \in X \iff M \models (\exists x\ \exp(x, \underline{p(n)}) = \exp(\underline{2}, a))$
- $n \in \overline{X} \iff M \models (\exists x\ \exp(x, \underline{p(n)}) = \exp(\underline{2}, c))$

Proof. By Corollary 4.3 we know that there exist $a, c \in M$ s.t. $n \in X \iff M \models \underline{p(n)} \mid a$ and $n \in \overline{X} \iff M \models \underline{p(n)} \mid c$.

Let us also note that these a, c must be non-standard elements of M, because otherwise X would be a finite/co-finite, hence recursive, set. We do not spend time to (intuitively) justify the preceding line since actually $M \models 0 < a, c$ is enough for the given proof to work. And if, by contradiction, $a = 0^M \vee b = 0^M$, then X is the empty set or the $\mathbb{N}$, and in this case it is especially obvious that X must be a recursive set.

We will show that a and c we got from Corollary 4.3 actually satisfy the conclusion of this corollary. We will show it only for X, and a, the case for $\overline{X}$, and c, can be proved by the same argument.

$\Rightarrow$: Assume that $n \in X$.

Then, as we know, $M \models \underline{p(n)} \mid a$, therefore there is some $z \in M$ s.t. $M \models \underline{p(n)} \times z = a$. Therefore we must have $M \models \exp(\underline{2}, \underline{p(n)} \times z) = \exp(\underline{2}, a)$.

And by the third item in Observation 2.10 we have

$$M \models \exp(\exp(\underline{2}, z), \underline{p(n)}) = \exp(\underline{2}, a).$$

Therefore the result of $M \models \exists x\, (\exp(x, \underline{p(n)}) = \exp(\underline{2}, a))$ follows.

$\Leftarrow$: Assume that there is $x \in M$ s.t. $M \models \exp(x, \underline{p(n)}) = \exp(\underline{2}, a)$.

By Observation 2.13, there must exist $w \in M$ s.t. $M \models x = \exp(\underline{2}, w)$. And again by the third item in Observation 2.10 we have $M \models \exp(\underline{2}, w \times \underline{p(n)}) = \exp(\underline{2}, a)$.

Since $\exp(\underline{2}, z)$ is an increasing function with respect to z, this follows by the last item in Observation 2.11, we must have $M \models w \times \underline{p(n)} = a$. And thus $M \models \underline{p(n)} \mid a$ and the membership of n in X follows.

□

Corollary 4.5. Let $M \models PA$, then there exists a non-recursive set X s.t. there exists $a, c \in M$ for which we have

- $n \in X \iff M \models \exists x\,(\exp(x, \underline{p(n)}) = a)$
- $n \in \overline{X} \iff M \models \exists x\,(\exp(x, \underline{p(n)}) = c)$

Proof. Obvious corollary of Corollary 4.4. □

Commentary. Let us again highlight that all the occurrences of $M \models I\Delta_0$ can be replaced by $M \models PA^-$ and M satisfies Overspill lemma for all the Δ_0 formulas.

5. Tennenbaum's theorem

At last, we approach the proof of Tennenbaum's theorem.

Let us also recall from Section 3.4 that we do not lose much when we will be considering only non-standard models which have $\mathbb{N}$ as their domain.

Let us recall that the original Tennenbaum's theorem for non-standard models of PA is due to Tennenbaum [1959] and the strengthened version for on-standard models of $I\Delta_0$ is due to McAloon [1982].

5.1 Tennenbaum's theorem for addition in $I\Delta_0$

Lemma 5.1. Let $M \models PA^-$ s.t. $dom(M) = \mathbb{N}$ and $+^M$ is recursive. Then if $X \subseteq \mathbb{N}$ is canonically coded in M we have that X is recursively enumerable.

Proof. Since X is canonically coded it means that there exists $a \in dom(M) = \mathbb{N}$ s.t.

$$n \in X \iff M \models \exists z\,(\underline{p(n)} \times z = a).$$

And that is in turn the same as, by Observation 1.21,

$$n \in X \iff M \models \exists z\,(z + \ldots + z = a),$$

where z is repeated $p(n)$ times.

We will now construct an algorithmic procedure A enumerating X. Furthermore, this procedure A will call a sub-procedure $B(n)$.

A: Enumerate $\mathbb{N}$ according to $<^{\mathbb{N}}$. For every enumerated i invoke the sub-procedure $B(i)$.

$B(i)$:
- First, Compute all the *finitely* many $p(0), \ldots, p(i)$.
- For every $p(l)$, for $l \leq i$, we check for every $m \leq i$ whether the sum with respect to $+^M$ of $p(l)$ m's is equal to a or not.

  If it is equal to a, then print out l to the output, and proceed. Otherwise do not print out anything and proceed.

Since we can surely enumerate $\mathbb{N}$ according to $<^{\mathbb{N}}$ recursively, $p(n)$ is a recursive function by Observation 3.9 and $+^M$ is recursive by our assumption we get that A and $B(i)$ are well defined algorithms.

Now, we check that A enumerates X and the proof will be finished.

- Obviously A, or more precisely B, will write to the output only members of X.
- Let $n \in X$. Then there must be some $m \in \mathbb{N}$ s.t. the sum of $p(n)$-times m, with respect to $+^M$, is equal to a.

  Since $B(i)$ processes only finitely many steps for every $i \in \mathbb{N}$ we get that after a finitely many steps of A, including those of B, $B(max(n, m))$ is called. And during $B(max(n, m))$ we will evidently write n to the output.

□

Theorem 5.2 (Tennenbaum's theorem for addition in $I\Delta_0$)**.** Let M be a non-standard model of $I\Delta_0$ s.t. $dom(M) = \mathbb{N}$. Then $+^M$ can not be a recursive function.

Proof. Assume for contradiction that the assumption holds but not the conclusion, i.e. $+^M$ is recursive.

We know by Corollary 4.3 that there is a non-recursive set $X \subseteq \mathbb{N}$ s.t. X and its complement can be both canonically coded in M.

However, since in addition is $+^M$ recursive, we get by Lemma 5.1 recursive enumerability of both X and $\overline{X}$. But from this result we immediately get the recursiveness of X, namely by Observation 3.2, which is the contradiction we wanted. □

Commentary. Let us also note that the only time we have used induction on Δ_0 formulas to reach this final goal of showing Theorem 5.2 formulas was when we were proving Ovespill lemma on $I\Delta_0$ for $\mathbb{N}$ which we have subsequently used many times.

Therefore we can actually conclude that Tennenbaum's theorem for addition holds for any model of PA^- that also satisfies all the instances of Overspill lemma on Δ_0 formulas (for $\mathbb{N}$), i.e. the conclusion of Lemma 2.7.

5.2 Tennenbaum's theorem for multiplication

As we will see, with all the preparations we have made, the proof of Tennenbaum's theorem for $\times$ is basically identical to the one for $+$.

Lemma 5.3. Let $M \models PA$ s.t. $dom(M) = \mathbb{N}$ and $\times^M$ is recursive. Moreover let X be a subset of $\mathbb{N}$. Then if there exists $a \in M$ s.t.

$$n \in X \iff M \models \exists x \, (\exp(x, \underline{p(n)}) = a),$$

then X is recursively enumerable.

Proof. The proof is analogous to the one in Lemma 5.3.

Only this time use the fourth item in Observation 2.10 to show that

$$n \in X \iff M \models \exists x \, (x^{\underline{p(n)}} = a),$$

where recall that $x^{\underline{p(n)}}$ is just a product of $p(n)$ x's.

And then change suitably chosen $+^M$ to $\times^M$ in Lemma 5.1 and the proof is written. □

Theorem 5.4 (Tennenbaum's theorem for multiplication)**.** Let $M \models PA$ s.t. its domain equals $\mathbb{N}$ and M is non-standard. Then $\times^M$ can not be a recursive function.

Proof. The proof is literally the same as the proof for Tennenbaum's theorem for addition in $I\Delta_0$.

- Change $+^M$ to $\times^M$.

- To acquire non-recursive set X where X and $\overline{X}$ are properly coded, for the proof to work, change Corollary 4.3 to Corollary 4.5.
- And lastly change reference to Lemma 5.1 for a reference to Lemma 5.3.

And the proof is written.

□

Concluding remark

After the two negative results, i.e. there can be no non-standard model of PA where the $+$ or $\times$ can be recursive, the reader might wonder whether there actually is some non-trivial relation or function, which we would possibly get by extending the language and adding a defining axiom to the theory, which can be recursive in some non-standard model of PA.

As we will see, for example, in the next chapter, there actually are some non-trivial relations/functions that are recursive in some non-standard model of PA. And we will not have to even extend the language, since one of them is $<$.

6. Inspection of the order relation

In this chapter, we investigate the structure of the order relation on models of $I\Delta_0$, more specifically on models of PA^- which also satisfy Overspill for $\mathbb{N}$ on all the Δ_0 formulas.

As a consequence of these observations, we will observe that there is a non-standard model of PA with domain $\mathbb{N}$ where the $<$ is recursive.

The results we present here are relatively well known and we have them mainly from Kaye [1991, pp. 73-77].

6.1 Equivalence relation of elements which are apart by a standard distance

Definition 6.1 (Relation $\sim_<$)**.** Let $M \models PA^-$, we define a relation $\sim_<$, with respect to M, as for all $a, b \in M$

$$a \sim_< b \iff \exists k \in \mathbb{N}^M \, (M \models a + k = b \vee a = b + k).$$

Observation 6.1. Let $M \models PA^-$, then $\sim_<$ is an equivalence relation.

Proof. reflexivity: Obvious by setting $k = 0^M$.

symmetricity: Obvious by the symmetricity of the definition of $\sim_<$.

transitivity: Assume $a \sim_< b$ and $b \sim_< c$, furthermore let $k, l \in \mathbb{N}^M$ be the respective witnesses.

Let us consider the four different possibilities that can happen.

- $M \models a = b + k \wedge b = c + l$.
  In this case we obviously have $M \models a = c + (l + k)$, where $(l +^M k) \in \mathbb{N}^M$. Therefore $a \sim_< c$.
- $M \models a = b + k \wedge b + l = c$.
  Let $n, m \in \mathbb{N}$ be such a natural numbers so that $M \models k = \underline{n} \wedge l = \underline{m}$.
  We must have $m \leq n$ or $Mn \leq m$. WLOG $M \models m \leq n$. And by Observation 1.29 we get that $M \models l \leq k$.
  We clearly have $M \models a + l = c + k$.
  Hence we have $M \models (a + l) \dot{-} l = (c + k) \dot{-} l$.
  And we can proceed to conclude by Observation 1.23 that $M \models a + (l \dot{-} l) = c + (k \dot{-} l)$.
  And lastly we get by Observation 1.25 that $M \models a = c + \underline{(n - m)}$. Where $(n - m) \in \mathbb{N}$, hence $a \sim_< c$ holds.
- $M \models a + k = b \wedge b = c + l$.
  We can verify by an analogous argument as in the previous item that indeed $a \sim_< c$.

- $M \models a + k = b \wedge b + l = c$.
  In this case we obviously have $M \models a + (k + l) = c$, where $(k +^M l) \in \mathbb{N}^M$. Therefore $a \sim_< c$.

$\square$

Definition 6.2 (Equivalence classes $e_\mathbb{Z}$)**.** Let $M \models PA^-$ and let $\sim_<$ be the respective equivalence relation. Then for every $e \in M$ we define $e_\mathbb{Z} := [e]_{\sim_<}$.

Observation 6.2. Let $M \models PA^-$ and let $\sim_<$ be the respective equivalence relation. Then for every $e \in M$ we have $e_\mathbb{Z} = \{\ldots, e \dot{-}^M 1^M, e, e +^M 1^M, \ldots\}$, more specifically

$$e_\mathbb{Z} = \{x \in M | \exists k \in \mathbb{N}^M (M \models x = e \dot{-} k)\} \cup \{x \in M | \exists k \in \mathbb{N}^M (M \models x = e + k)\}.$$

Secondly, $\{x \in M | \exists k \in \mathbb{N}^M (M \models x = e \dot{-} k)\}$ equals $\{x \in M | \exists k \in \mathbb{N}^M (M \models x + k = e)\}$.

Lastly, if e is a non-standard element of M and $n \in \mathbb{N} \setminus \{0\}$, then

$$M \models \ldots < e \dot{-} \underline{n} < \ldots < e \dot{-} 1 < e < e + 1 < \ldots < e + \underline{n} < \ldots$$

Proof. Clearly, be definition of $\sim_<$ we have

$$e_\mathbb{Z} = \{x \in M | \exists k \in \mathbb{N}^M (M \models x + k = e)\} \cup \{x \in M | \exists k \in \mathbb{N}^M (M \models x = e + k)\}.$$

As a simple application of Observation 1.26, we can observe that $\{x \in M | \exists k \in \mathbb{N}^M (M \models x + k = e)\}$ equals $\{x \in M | \exists k \in \mathbb{N}^M (M \models x = e \dot{-} k)\}$, and the main result, as well as the (middle) remark, follows.

As for the last "Lastly" part.

Mainly by Observation 1.29 and Ax.11 $[x < y \rightarrow x + z < y + z]$ we can conclude that $M \models e + \underline{n} < e + \underline{n+1}$ for any $n \in \mathbb{N}$.

Next, if $n \in \mathbb{N}$ then since e is non-standard element we get by Ax.13 $[x \leq y \rightarrow \exists z(x + z = y)]$ that there exists $z \in M$ s.t. $M \models e = z + \underline{n+1}$, Which also implies that $M \models e = (z + 1) + \underline{n}$. Therefore, mainly by Observation 1.23 $M \models e \dot{-} \underline{n+1} = z$ and $M \models e \dot{-} \underline{n} = z + 1$. And thus we may conclude that $M \models e \dot{-} \underline{n+1} < e \dot{-} \underline{n}$, which finishes the proof. $\square$

Corollary 6.3. Let $M \models PA^-$, then $0^M_\mathbb{Z} = \mathbb{N}^M$.

Proof. By Observation 6.2 we know that $0^M_\mathbb{Z}$ is equal to

$$\{x \in M | \exists k \in \mathbb{N}^M (M \models x + k = 0)\} \cup \{x \in M | \exists k \in \mathbb{N}^M (M \models x = 0 + k)\}.$$

The second item in the union is obviously $\mathbb{N}^M$, by Ax.2 [commutativity $+$] and Ax.6 $[0, 1$ are neutral$]$.

Let us inspect more carefully the first item in the union, i.e.

$$\{x \in M | \exists k \in \mathbb{N}^M (M \models x + k = 0)\}.$$

Assume that $x \in M$ and $M \models x + k = 0$ for some $k \in \mathbb{N}^M$. Assume furthermore for contradiction that $M \models x \neq 0$. Then by Ax.15 $[0 \leq x]$ $M \models 0 < x$, hence by Ax.11 $[x < y \rightarrow x + z < y + z]$ we have $M \models 0 + k < x + k$.

Applying Ax.15 $[0 \leq x]$ again we have $M \models 0 \leq 0 + k$, therefore by Ax.8 [transitivity $<$] we have both $M \models 0 < x + k$ and $M \models 0 = x + k$ which can not be by Observation 1.1.

Therefore we may conclude that the first set in the union is a subset of a singleton containing only 0^M, actually it is equal to it by Ax.6 [0, 1 are neutral].

Continuing, since the first set in the union is a a subset of $\{0^M\}$ and the second set is $\mathbb{N}^M$ which by it self contains 0^M we may conclude that indeed $0^M_{\mathbb{Z}} = \mathbb{N}^M$. □

Observation 6.4. Let $M \models PA^-$, $a, b \in M$ and let $\sim_<$ be the respective equivalence relation. Then if $a_{\mathbb{Z}} \neq b_{\mathbb{Z}}$ and $M \models a < b$, then $\forall x \in a_{\mathbb{Z}} \forall y \in b_{\mathbb{Z}} (M \models x < y)$.

Proof. First, we will show that $\forall y \in b_{\mathbb{Z}}\, M \models a < y$, and the rest will follow.

Let $y \in b_{\mathbb{Z}}$, then there exits $k \in \mathbb{N}^M$, where $M \models k = \underline{n}$ for some $n \in \mathbb{N}$, s.t. $M \models y = b + k \vee b = y + k$.

Let us argue about these two cases separately.

$y = b +^M k$: By Observation 1.9 we know that $M \models b \leq b + k$. And by Ax.8 [transitivity $<$] we can conclude $M \models a < y$.

$b = y +^M k$: We will show by induction on n that $M \models a < y$.

- $n = 0$: Then $b = y$ and we are finished.
- $n = d + 1$: Assume for contradiction that $M \models a < y$ does not hold.
  By Ax.10 [trichotomy $<$] we get that $M \models a = y \vee y < a$.
  If $M \models a = y$, then $a_{\mathbb{Z}} = b_{\mathbb{Z}}$ which is in contradiction with our assumption of $a_{\mathbb{Z}} \neq b_{\mathbb{Z}}$, hence $M \models a = y$ can not hold.
  If $M \models y < a$, then $M \models y + 1 \leq a$ by Observation 1.16. Also since $M \models b = (y + 1) + \underline{d}$ we get by our induction hypothesis that $M \models a < y + 1$. Combining the last two observations we get a contradiction by Observation 1.1.

Let $x \in a_{\mathbb{Z}}$, then there exists $l \in \mathbb{N}^M$ s.t. $M \models x + l = a$ or $M \models x = a + l$.

In the former case, by the third item in Observation 1.11, $M \models x \leq a$, hence by Ax.8 [transitivity $<$] we have $\forall y \in b_{\mathbb{Z}} (M \models x < y)$.

In the latter case, by Ax.11 $[x < y \rightarrow x + z < y + z]$, $M \models a + k < b + k$ where $(b + k) \in b_{\mathbb{Z}}$. Therefore we can use the same argument as we did at the beginning of this proof for a that $\forall y \in b_{\mathbb{Z}} (M \models (x =)a + k < y)$.

The proof is finished. □

Definition 6.3. Let $M \models PA^-$ and let $\sim_<$ be the respective equivalence relation. Define order, denoted as $<_\sim$, on the equivalence classes in the following way

$$\forall a, b \in M (a_{\mathbb{Z}} <_\sim b_{\mathbb{Z}} \iff ((a_{\mathbb{Z}} \neq b_{\mathbb{Z}}) \wedge (M \models a < b))$$

In the following observation, we justify the word "order" used in the preceding definition.

Observation 6.5 ($<_\sim$ is a well defined order)**.** Let $M \models PA^-$ and let $\sim_<$ be the respective equivalence relation then $<_\sim$ is linear order on $M/\sim_<$.

Proof. Firstly, let us use $\sim$ as a shortcut for the more correct $\sim_<$.

Let $a, b \in M$.

antisymmetri: Assume for contradiction that $a_\mathbb{Z} <_\sim b_\mathbb{Z}$ as well as $b_\mathbb{Z} <_\sim a_\mathbb{Z}$.

Then $a_\mathbb{Z} \neq b_\mathbb{Z}$ and there must be two elements $x, y \in a_\mathbb{Z}$ and two element $w, z \in b_\mathbb{Z}$, s.t. $M \models x < w \wedge z < y$. But this can not happen by Observation 6.4 and the contradiction follows.

transitivity: Obvious by Ax.8 [transitivity $<$] and anti-symmetricity of the relation $<_\sim$.

trichotomy: If $a_\mathbb{Z} = b_\mathbb{Z}$, then we are done. Otherwise $a_\mathbb{Z} \neq b_\mathbb{Z}$ and therefore $a \neq b$ as well.

By Ax.10 [trichotomy $<$] we can conclude that $M \models a < b \vee b < a$, and thus $a_\mathbb{Z} <_\sim b_\mathbb{Z}$ or $b_\mathbb{Z} <_\sim a_\mathbb{Z}$ and the trichotomy follows.

And thus the $<_\sim$ is a well defined linear order. □

6.2 Structure of the order relation

Definition 6.4 (Dense linear order without endpoints)**.** Let $\mathcal{A} = (A, <)$ be some structure over the language with only one, except for $=$, non-logical symbol $<$. We say that $\mathcal{A}$ is a dense linear order without endpoints, DLO for short, if it does model all the following conditions.

(i) $\forall x, y, z\,((x < y \wedge y < z) \to x < z)$, i.e. transitivity.

(ii) $\forall x\,(\neg x < x)$, i.e. irreflexivity.

(iii) $\forall x, y\,(x < y \vee x = y \vee y < x)$, i.e. trichotomy.

(iv) $\forall x \exists y\,(x < y)$, i.e. there is no largest element.

(v) $\forall x \exists y\,(y < x)$, i.e. there is no smallest element.

(vi) $\forall x, y\,(x < y \to (\exists z\, x < z \wedge z < y))$, i.e. density.

Lemma 6.6. Let $M \models I\Delta_0$. Then if we set $A := (M/\sim_<) \setminus \{0^M_\mathbb{Z}\}$, then $(A, <_\sim)$ is a DLO.

Proof. By Observation 6.5 we know that the first three properties hold for $(A, <_\sim)$. (The irreflexivity follows by the anti-symmetricity.)

Let us verify that there are no endpoints in $(A, <_\sim)$ and the density of $(A, <_\sim)$. Furthermore, we would like to emphasize that by Corollary 6.3 all the equivalence classes of which is A made of contain only non-standard elements of M and vice versa, i.e. every non-standard element is a member of some equivalence class in A.

no largest element: Let $a \in M$ s.t. $a_{\mathbb{Z}} \in A$.

Then a must be a nonstandard element as well as $a +^M a$.

Set b to $a +^M a$, we know that $b \in M$ and furthermore that b is a non-standard element of M, hence $b_{\mathbb{Z}} \in A$.

Next, we clearly have $M \models a < b$.

Lastly $a_{\mathbb{Z}} \neq b_{\mathbb{Z}}$ since a is non-standard and therefore by Observation 6.2 $a +^M a$ can not be in $a_{\mathbb{Z}}$.

Therefore we may conclude that $b_{\mathbb{Z}} \in A$ as well as $a_{\mathbb{Z}} <_{\sim} b_{\mathbb{Z}}$ from which immediately follows that $(A, <_{\sim})$ has no largest element.

no smallest element: Let $a \in M$ s.t. $a_{\mathbb{Z}} \in A$.

Since a is a non-standard element, we clearly have the following two inequalities $M \models \underline{m} < (a \dot{-} \underline{m}) \dot{-} 1 < a$ for any $m \in \mathbb{N}$.

Recall that in Definition 1.5 we have defined $M \models y = x \dot{-} z$ as $(x < z \wedge y = 0) \vee (z + y = x))$, which is a Δ_0 formula. Furthermore, it is obvious that if y satisfies the defining formula of $\dot{-}$ it must hold that $M \models y \leq x$. Hence, anytime the term $x \dot{-} z$ emerges within some formula φ we can substitute it by a new, so far unused, variable y and add the following Δ_0 formula

$$\psi(x, z) \equiv \exists y \leq x\, (x < z \wedge y = 0) \vee (z + y = x)),$$

to the outer scope of the φ formula so that the substitued y is encapsulated by it.

It follows that we can use Lemma 2.7, i.e. Overspill lemma on Δ_0 formulas, to get a non-standard element e of M s.t. $M \models e < (a \dot{-} e) \dot{-} 1 < a$.

Again let b be the element of M s.t. $M \models b = (a \dot{-} e) \dot{-} 1$.

Since $M \models e < b$ it follows that b must be a non-standard element of M and thereafter $b_{\mathbb{Z}} \in A$.

Last think to show is that $b_{\mathbb{Z}} <_{\sim} a_{\mathbb{Z}}$, that is $b_{\mathbb{Z}} \cap a_{\mathbb{Z}} = \emptyset$ and $M \models b < a$. The latter is evident and the former follows by b being smaller then every element of $a_{\mathbb{Z}}$ which in turn follows by a and e being non-standard elements.

Therefore we may conclude that $(A, <_{\sim})$ has no smallest element.

density: Let $a_{\mathbb{Z}}, c_{\mathbb{Z}} \in A$ s.t. $a_{\mathbb{Z}} <_{\sim} c_{\mathbb{Z}}$.

Clearly $M \models a < a + \underline{m} + 1$ as well as $M \models a + \underline{m} + 1 < c \dot{-} \underline{m}$, for any $m \in \mathbb{N}$.

The second inequality follows because by Observation 6.2 we know that $(a + \underline{m} + 1)^M \in a_{\mathbb{Z}}$ whereas $c \dot{-} \underline{m} \in c_{\mathbb{Z}}$, and since $a_{\mathbb{Z}} <_{\sim} c_{\mathbb{Z}}$ it follows by Observation 6.4 that $M \models a + \underline{m} + 1 < c \dot{-} \underline{m}$.

Therefore $M \models a < a + \underline{m} + 1 \wedge a + \underline{m} + 1 < c \dot{-} \underline{m}$ for any $m \in \mathbb{N}$.

Hence noting as in the preceding item that the formula is a Δ_0 formula we can apply Lemma 2.7, i.e. Overspill lemma for Δ_0 formulas, to acquire a non-standard element e in M s.t. $M \models a < a + e + 1 < c \dot{-} e$.

Set $b \in M$ so that $M \models b = a + e + 1$.

Clearly, b is a non-standard element of M and hence $b_{\mathbb{Z}} \in A$.

Furthermore, we obviously have, namely by Observation 6.2 and e being a non-standard element, that $a_{\mathbb{Z}} \neq b_{\mathbb{Z}}$ and $c_{\mathbb{Z}} \neq b_{\mathbb{Z}}$.

Lastly, since $M \models a < b$ as well as evidently $M \models b < c$, we can finally conclude that $a_{\mathbb{Z}} <_{\sim} b_{\mathbb{Z}} <_{\sim} c_{\mathbb{Z}}$ where $b_{\mathbb{Z}} \in A$.

From the last paragraph we can come to the conclusion that $(A, <_{\sim})$ is indeed dense.

□

Commentary. Let us highlight that the only time we have used $M \models I\Delta_0$ instead of just $M \models PA^-$ was when we used Ovespill lemma on $I\Delta_0$ for $\mathbb{N}$.

Hence, we can conclude that the foregoing theorem holds for any model of PA^- which also satisfies Overspill lemma on all the instances of Δ_0 formulas (for $\mathbb{N}$).

Theorem 6.7 (Order-type of models of $I\Delta_0$)**.** Let M be a non-standard model of $I\Delta_0$ and recall that $I\Delta_0$ implicitly contains defining axiom for $S(x)$ introduced in Definition 1.3, i.e. for the successor function. Furthermore set $(A, <_{\sim})$ as in Lemma 6.6. Then $(M, <^M, S^M) \cong (\mathbb{N} \cup A \times \mathbb{Z}, <', S')$, where we define $<'$ in the following way.

- Let $n, m \in \mathbb{N}$, then $n <' m \iff n < m$.
- Let $n \in \mathbb{N}$ and $a \in A \times \mathbb{Z}$, then we always set $n <' a$.
- Let $(q, k), (r, l) \in A \times \mathbb{Z}$, then we set $(q, k) <' (r, l)$ iff. $q <_{\sim} r$ or $q = r \wedge k <^{\mathbb{Z}} l$.

And the $S'(x)$ is defined as follows.

- If $x \in \ N$, then $S'(x) = x + 1$.
- If $x = (q, k) \in A \times \mathbb{Z}$, then $S'(x) = (q, k + 1)$.

Proof. Take a function, e.g. by *Axiom of Choice* - for further details see Enderton [1977, p.151], $s \colon A \longrightarrow M$ s.t. $\forall q \in A\, s(q) \in q$.

Now, we will define h, from $(\mathbb{N} \cup A \times \mathbb{Z})$ onto M, that will be a witness to the isomorphism we want to show.

Let $x \in (\mathbb{N} \cup A \times \mathbb{Z})$, then

$$h(x) := \begin{cases} \underline{n}^M & x = n \wedge n \in \mathbb{N}, \\ (s(a_{\mathbb{Z}}) + \underline{k})^M & x = (a_{\mathbb{Z}}, k) \wedge 0 \leq^{\mathbb{Z}} k, \\ (s(a_{\mathbb{Z}}) \dot{-} \underline{l})^M & x = (a_{\mathbb{Z}}, k) \wedge k <^{\mathbb{Z}} 0 \wedge l = -k. \end{cases}$$

h is evidently a well defined function from $(\mathbb{N} \cup A \times \mathbb{Z})$ into M.

It remains to show the following four points.

onto: Let $y \in M$.

Then either $y \in \mathbb{N}^M$ or y is a nonstandard element and $y_{\mathbb{Z}} \in A$.

If $y \in \mathbb{N}^M$, then $y = \underline{n}^M$ for some $n \in \mathbb{N}$. Hence $h(n) = y$.

Otherwise $y_{\mathbb{Z}} \in A$ and

$$y \in y_{\mathbb{Z}} = s(y_{\mathbb{Z}})_{\mathbb{Z}} = \{\dots, (s(y_{\mathbb{Z}}) \dot{-} 1)^M, s(y_{\mathbb{Z}}), (s(y_{\mathbb{Z}}) + 1)^M, \dots\},$$

where the last equality follows by Observation 6.2.

Hence it is obvious that there must exist $k \in \mathbb{Z}$ s.t. $h(y_{\mathbb{Z}}, k) = y$, and we may conclude that h is onto.

injective: By Corollary 1.30 we know that h is injective when restricted to $\mathbb{N}$.

Also, it is is obvious that $h(n) \neq h(a, k)$, for $n \in \mathbb{N}$, $a \in A$ and $k \in \mathbb{Z}$. It is because $h(n) \in 0^M_{\mathbb{Z}}$ and $h(a, k) \in a$, by Observation 6.2, and $a \neq 0^M_{\mathbb{Z}}$ by definition of A.

Continuing, when $a, b \in A$ the by Observation 6.2 we clearly have $h(a, l) \in a$ and $h(b, k) \in b$ for any $l, k \in \mathbb{N}^M$. Therefore if $a \neq b$, then $h(a, l) \neq h(b, k)$.

It only remains to show that for any $a \in A$ is h injective when we restrict the first argument to a. But that follows immediately by the last point in Observation 6.2.

respects order: Let $x, y \in \mathbb{N} \cup A \times \mathbb{Z}$ and $x <' y$.

If $x, y \in \mathbb{N}$, then by Observation 1.29 $M \models h(x) < h(y)$.

If $x \in \mathbb{N}$ and $y \in A \times \mathbb{Z}$, then $h(x) \in \mathbb{N}^M$ whereas by Observation 6.2 is $h(y) \in y_{\mathbb{Z}} \in A$ and hence $h(y) \neq h(x)$.

Case when $y \in A \times \mathbb{Z}$ and $x \in \mathbb{N}$ can not happen.

Last unanalyzed situation is when both $x, y \in A \times \mathbb{Z}$. In this case, there must be $q, r \in A$ and $k, l \in \mathbb{Z}$ s.t. $x = (q, k)$ and $y = (r, l)$. And since $x <' y$ we have that $q <_{\sim} y$ or $q = r \wedge k <^{\mathbb{Z}} l$. Let us argue about these two cases separately.

$q <_{\sim} r$: We know by Observation 6.2 that $h(x) \in q$ and $h(y) \in r$.

Since $q <_{\sim} r$ we have $q \neq r$ and there is an element from q which is smaller, with respect to $<^M$ then some element from r. But applying Observation 6.4 we know that $\forall z \in q \, \forall w \in r \, (M \models z < w)$. Therefore we must have $M \models h(x) < h(y)$, which is what we wanted.

$q = r \wedge k <_{\mathbb{Z}} l$: Then, by the last part in Observation 6.2 we must indeed have $M \models h(x) < h(y)$.

respects S: It suffices to show that for any $x \in (\mathbb{N} \cup A \times \mathbb{Z})$ we have $h(S'(x)) = S^M(h(x))$.

Let us consider separately different possibilities of the value that can be possessed by x.

$x \in \mathbb{N}$: $S'(x) = x + 1$, hence $h(S'(x)) = \underline{x+1}^M$.

As for $h(x)$, we have, $h(x) = \underline{x}^M$ and hence, by Definition 1.3, we get that $S^M(h(x)) = (h(x)+1)^M = (\underline{x}+1)^M$, which is clearly equal to $\underline{x+1}^M$.

$(q,k) = x \in A \times \mathbb{Z}$:

$0 \leq k$: If $0 \leq k$, then also $0 \leq k+1$ and since $S'(x) = (q, k+1)$ we may conclude that $h(S'(x)) = (s(q) + \underline{k+1})^M$.
Continuing, if $0 \leq k$, then we have $h(x) = (s(q) + \underline{k})^M$ and hence $S^M(h(x)) = ((s(q)+\underline{k})+1)^M$ which is obviously equal to $(s(q) + \underline{k+1})^M$, by Ax.1 [associativity +].

$k < 0$: First note that, e.g. by definition of $\dot{-}$, $M \models x \dot{-} 0 = x$.
$S'(x) = (q, k+1)$ and hence $h(S'(x)) = (s(q) \dot{-} \underline{(-(k+1))})^M = (s(q) \dot{-} \underline{(-k-1)})^M$, this first equality follows by definition of $h(y)$ if $k+1 < 0$ and otherwise, i.e. $k+1 = 0$, it follows by the remark we have just made.
When we compute $h(x)$, we have $(s(q) \dot{-} \underline{(-k)})^M$ and when we apply S^M we get $S^M(h(x)) = ((s(q) \dot{-} \underline{(-k)}) + 1)^M$.
However, we may now conclude by

- $1 \leq -k$ and $M \models \underline{(-k)} \leq s(q)$,
- "associativity" of $\dot{-}$ observed in Observation 1.24 for certain specific elements of M,
- the fact that $\dot{-}$ behaves on standard elements quite reasonably, which is observed in Observation 1.25,

that indeed $(s(q) \dot{-} \underline{(-k-1)})^M = ((s(q) \dot{-} \underline{(-k)}) + 1)^M$.

The proof is hereby completed. □

Commentary. One can possibly wonder whether we can have a formula that would be satisfied by exactly one element from every non-standard copy of $\mathbb{Z}$, i.e. $a_{\mathbb{Z}}$ for $a \in A$. However, we will see in the following lines that this is not possible.

Assume for contradiction that $M \models PA$ and there is a L_A formula $\varphi(x)$ for any $a_{\mathbb{Z}} \in M/\sim_<$, where $a_{\mathbb{Z}} \neq 0_{\mathbb{Z}}^M$, exactly one element $e \in a_{\mathbb{Z}}$ satisfies the formula with respect to M, i.e. $M \models \varphi(e)$ and $\forall b \in a_{\mathbb{Z}}\, b \neq a \Rightarrow M \models \neg\varphi(b)$.

However, since we know how $a_{\mathbb{Z}}$ must look like by Observation 6.2 and we know that if $M \models z \leq \underline{m} \to z = \underline{0} \vee \ldots \vee z = \underline{m}$ by Observation 1.31, we get that $M \models \forall z \leq \underline{m}\, \neg\varphi(e+z+1)$ for any $m \in \mathbb{N}$.

Hence by Overspill lemma we get that there must exist $c \in M$ s.t. c is non-standard and $M \models \forall z \leq c\, \neg\varphi(e+z+1)$. Clearly $d = (e+c+1)^M$ is a non-standard element of M s.t. $a_{\mathbb{Z}} <_\sim d_{\mathbb{Z}}$, hence we get by Lemma 6.6 that there is b a non-standard element of M s.t. $M \models a_{\mathbb{Z}} <_\sim b_{\mathbb{Z}} <_\sim d_{\mathbb{Z}}$.

It is not hard to see that $\forall x \in b_{\mathbb{Z}}$ there must exist a $z \in M$ s.t. $M \models z \leq c$ and $x = (a+z+1)^M$. Therefore we can conclude that $\forall x \in b_{\mathbb{Z}}$, where b is a non-standard element of M, $M \models \neg\varphi(x)$ which is in contradiction with our assumption.

Lemma 6.8 ($\mathbb{Q}$ is the only countable DLO)**.** Let $(A, <)$ be a countable DLO, then $(A,<)$ is isomorphic to $(\mathbb{Q}, <^{\mathbb{Q}})$.

Proof. For one, $(\mathbb{Q}, <^{\mathbb{Q}})$ is evidently DLO. By Cantor's theorem, as presented in Kirby [2019, section 15.3], we know that any two countable DLO's are isomorphic to each other.

Hence, combining the last two points, we have that $(A, <) \cong (\mathbb{Q}, <^{\mathbb{Q}})$. □

Corollary 6.9. Let M be a countable non-standard model of $I\Delta_0$, set $(A, <_\sim)$ as in Lemma 6.6, then $(A, <_\sim) \cong (\mathbb{Q}, <^{\mathbb{Q}})$.

Proof. Since $(A, <_\sim)$ is a DLO by Lemma 6.6, the corollary follows by Lemma 6.8. □

Corollary 6.10. Let M be a countable non-standard model of $I\Delta_0$, then $(M, <^M, S^M) \cong (\mathbb{N} \cup \mathbb{Q} \times \mathbb{Z}, <', S')$ where $<'$ is defined in the following way.

- Let $n, m \in \mathbb{N}$, then $n <' m \iff n < m$.
- Let $n \in \mathbb{N}$ and $a \in \mathbb{Q} \times \mathbb{Z}$, then we always set $n <' a$.
- Let $(q, k), (r, l) \in \mathbb{Q} \times \mathbb{Z}$, then we set $(q, k) <' (r, l)$ iff. $q <^{\mathbb{Q}} r$ or $q = r \wedge k <^{\mathbb{Z}} l$.

And the $S'(x)$ is defined as

- If $x \in N$, then $S'(x) = x + 1$.
- If $x = (q, k) \in \mathbb{Q} \times \mathbb{Z}$, then $S'(x) = (q, k + 1)$.

Proof. The result stems from Theorem 6.7, Corollary 6.9 and the relation *isomorphic to* being transitive. □

Corollary 6.11. Let M be a countable non-standard model of PA, then $M, <^M, S^M) \cong (\mathbb{N} \cup \mathbb{Q} \times \mathbb{Z}, <', S')$ where $<'$ and S' are defined as in Corollary 6.10.

Proof. Since PA is a stronger theory than $I\Delta_0$ the result follows by Corollary 6.10. □

6.3 Order and successor can be recursive

Lemma 6.12 ($<$ and S can be recursive)**.** There exists a non-standard model G of PA, recall that PA implicitly includes the defining axiom for $S(x)$ introduced in Definition 1.3, s.t. $dom(G) = \mathbb{N}$ and $<^G$ as well as S^G are recursive.

Proof. First note that there exists a countable non-standard model U of PA by Corollary 2.3.

By Corollary 6.11 we get that $(U, <^U, S^U)$, i.e. the restriction of U to the $<$ and S, is isomorphic to a structure $(\mathbb{N} \cup (\mathbb{Q} \times \mathbb{Z}), <', S')$ where $<'$ and S' are evidently computable. Moreover, $\mathbb{N} \cup (\mathbb{Q} \times \mathbb{Z})$ is a *computable codable set* where the witness to it can be found in Bijection 5.

Now from a discussion in section 3.4, more specifically by Corollary 3.15, follows that there exists a non-standard model G of PA, this follows from $G \cong U$, s.t. $dom(G) = \mathbb{N}$ and S as well as $<$ are recursive with respect to G.

And the lemma was proved. □

Part II

Recursiveness of mod & div in PA

7. Mod & Div functions

In this chapter, we are going to extend our language by binary functional symbols div and mod with their standard interpretation in mind. Furthermore, we will also add unary functional symbols div$\underline{k}$ and mod$\underline{k}$ for every $k \in \mathbb{N}$.

As for the subsequent chapters, we will investigate questions related to the recursiveness of those functions.

7.1 Introducing the div & mod functions

We further extend our language by two binary functional symbols div and mod in the same manner as we have extended our language by e.g. $S(x)$ or $x \dot{-} z$ in section 1.4.

Definition 7.1 (Quotient function - $x \operatorname{div} y$)**.** We introduce a new binary functional symbol div, the quotient function, by the following formula

$$\varphi_{\operatorname{div}}(x, y, z) \equiv ((y = 0 \wedge z = 0) \vee (y \neq 0 \wedge (z \times y \leq x < (z + 1) \times y)).$$

Definition 7.2 (Remainder function - $x \operatorname{mod} y$)**.** We introduce a new binary functional symbol mod, the remainder function, by the following formula

$$\varphi_{\operatorname{mod}}(x, y, z) \equiv ((y = 0 \wedge z = x) \vee (y \neq 0 \wedge (z < y \wedge \exists w \leq x\, (w \times y + z = x))).$$

Let us note that our definition of div rounds down as opposite to rounding up. We have chosen this definition since it seems more standard and natural to us. Furthermore, we get that $M \models x = (x \operatorname{div} y) \times y + x \operatorname{mod} y$, for suitably chosen structure M.

Both definitions are clearly in line with our understanding of the behavior of div and mod in $\mathbb{N}$.

As usual, we will need to show by the following observation that we actually can extend our language with the two binary functional symbols in mention using the just proposed formulas.

Observation 7.1 (div and mod are well defined)**.** Let $M \models I\Sigma_1$, then the following holds.

- $M \models \forall x, y\, \exists! z\, \varphi_{\operatorname{div}}(x, y, z)$,
- $M \models \forall x, y\, \exists! z\, \varphi_{\operatorname{mod}}(x, y, z)$,

Proof. Let $x, y \in M$.

If $y = 0^M$, then the proof for the existence and the uniqueness is simple for both cases.

Otherwise assume for the rest of the proof that $y \neq 0^M$.

We can apply Theorem 2.4, this is why we need $I\Sigma_1$, setting $b := x$ and $a := y$ to get that there *exists* a *unique* pair of $q, r \in M$ s.t. $M \models x = q \times y + r \wedge r < y$.

Since $M \models x = q \times y + r$, we obviously have $M \models q \times y \leq x$ and moreover since $M \models r < y$ we also get that $M \models x < (q + 1) \times y$. Therefore $M \models \varphi_{\operatorname{div}}(x, y, q)$.

We know that $M \models r < y$ and also that there exists $w \in M$, namely setting w to q, s.t. $M \models x = w \times y + r$. Furthermore, as we have already noted, $M \models q \times y \leq x$ and since $y \neq 0^M$, we get that $M \models (w =)q \leq x$. Hence we get that $M \models \varphi_{\text{mod}}(x, y, r)$.

Therefore the existence part of both cases has been proved.

As for the uniqueness part. Assume that $q^{'}, r^{'} \in M$ s.t. $M \models \varphi_{bdiv}(x, y, q^{'})$ and $M \models \varphi_{\text{mod}}(x, y, r^{'})$.

We know that there exists $w \in M$ s.t. $M \models x = w \times y + r^{'} \wedge r^{'} < y$. Now, we get by uniqueness part of theorem 2.4 that $r^{'} = r$ (and also $w = q$). Hence the uniqueness of z in $\varphi_{\text{mod}}(x, y, z)$ has been proved.

We also know that $M \models q^{'} \times y \leq x < (q^{'} + 1) \times y$. Hence there must be some $t \in M$ s.t. $M \models x = q^{'} \times y + t \wedge t < y$. But now we again get by the uniqueness part of Theorem 2.4 that $M \models q^{'} = q$ (and also $t = r$). Thereafter the uniqueness of z in $\varphi_{\text{div}}(x, y, z)$ has been proved. □

From now on, whenever we write $I\Sigma_1$ or some extension of it T, we will actually mean $I\Sigma_1$, or T, with added defining axioms for mod and div. And as in PART I also with the defining axioms of $S(x)$,$P(x)$, $x \dot{-} z$ and $|$, i.e. the divisibility relation, introduced in section 1.4.

Corollary 7.2. Let $M \models I\Sigma_1$ and let $x, y \in M$ s.t. $y \neq 0^M$. Then if $q, r \in M$ are the unique pair for $b := x$ and $a := y$ in Theorem 2.4, i.e. they satisfy $M \models x = q \times y + r \wedge r < y$, then $M \models x \text{ div } y = q$ and $M \models x \text{ mod } y = r$.

Proof. Follows by the proof of the previous observation Observation 7.1. □

Furthermore, let us observe that x div y and x mod y are expressible by Δ_0 formulas.

Observation 7.3. Let $M \models I\Sigma_1$ and $x, y \in M$, then $M \models \exists z \, \varphi_{\text{div}}(x, y, z)$ iff. $M \models \exists z \leq x \, \varphi_{\text{div}}(x, y, z)$, where the latter formula is obviously a Δ_0 formula.

Proof. The implication from right to left is obvious.

As for the implication for left to right assume that $M \models \varphi_{\text{div}}(x, y, z)$ for some $z \in M$. Then we have either $M \models y = 0 \wedge z = 0$ and hence $M \models z \leq x$.

Or we have that $M \models y \neq 0$ and then we have that $M \models z \times y \leq x$. Since $M \models 1 \leq y$ we evidently have $M \models z \leq x$.

Therefore we have either way that $M \models z \leq x$ from which follows that $M \models \exists z \leq x \varphi_{\text{div}}(x, y, z)$. □

Observation 7.4. Let $M \models I\Sigma_1$ and $x, y \in M$, then $M \models \exists z \, \varphi_{\text{mod}}(x, y, z)$ iff. $M \models \exists z \leq (x + y) \, \varphi_{\text{mod}}(x, y, z)$, where the latter formula is obviously a Δ_0 formula.

Proof. The implication from right to left is obvious.

As for the implication from left to right assume that $M \models \varphi_{\text{mod}}(x, y, z)$ for some $z \in M$. Then we have either $M \models y = 0 \wedge z = x$ and hence $M \models z \leq x$ from which follows that $M \models z \leq x + y$.

Or we have that $M \models y \neq 0$ and then we have by definition that $M \models z < y$ which implies $M \models z \leq y$ from which follows that $M \models z \leq x + y$.

Therefore we have either way that $M \models z \leq x + y$ from which follows that $M \models \exists z \leq (x + y) \, \varphi_{\text{mod}}(x, y, z)$. □

To finish this section, let us prove that mod and div behave on standard elements as expected.

Observation 7.5 (mod^M behaves on standard elements as mod$^{\mathbb{N}}$)**.** Let $M \models I\Sigma_1$, then for any $m, n \in \mathbb{N}$ we have

$$M \models \underline{n} \bmod \underline{m} = \underline{n \bmod^{\mathbb{N}} m}.$$

Proof. First assume that $m = 0$, then we clearly get on both sides of the equation $\underline{n}^M$ and hence the observation holds for any $n \in \mathbb{N}$ and $m = 0$.

Now assume that $m \neq 0$, then by Theorem 2.4 we know that there are $q, r \in \mathbb{N}$ s.t. $n = q \times m + r$ and $r < m$.

We clearly have $n \bmod^{\mathbb{N}} m = r$ and therefore $M \models \underline{n \bmod^{\mathbb{N}} m} = \underline{r}$.

As for the left hand side of the equation, we have

$$M \models \underline{n} \bmod \underline{m} = \underline{q \times m + r} \bmod \underline{m} = (\underline{q} \times \underline{m} + \underline{r}) \bmod \underline{m}.$$

The last equality in the just stated equation follows by Observation 1.22 and Observation 1.28, i.e. that $+$ and $\times$ behave on $\mathbb{N}^M$ as expected.

Furthermore since $r < m$ we get by Observation 1.29 that $M \models \underline{r} < \underline{m}$.

We can conclude now by Corollary 7.2, setting x to $\underline{n}^M$ and y to $\underline{m}^M$, that indeed $M \models \underline{n} \bmod \underline{m} = \underline{r}$ and the proof is finished. □

Observation 7.6 (div^M behaves on standard elements as mod$^{\mathbb{N}}$)**.** Let $M \models I\Sigma_1$, then for any $m, n \in \mathbb{N}$ we have

$$M \models \underline{n} \operatorname{div} \underline{m} = \underline{n \operatorname{div}^{\mathbb{N}} m}.$$

Proof. Assume that $m = 0$, then by the definition of div we have that the observation holds.

Assume now that $0 < m$. Then we know, for example from Theorem 2.4 that there exists $q, r \in M$ s.t. $n = q \times m + r$ and $r < m$.

Hence we also have by Observation 1.22 and Observation 1.28 that $M \models \underline{n} = \underline{q} \times \underline{m} + \underline{r}$ and by Observation 1.29 we, moreover, get $M \models \underline{r} < \underline{m}$.

Therefore, we can now conclude by Corollary 7.2, setting x to $\underline{n}^M$ and y to $\underline{m}^M$, that $M \models \underline{n} \operatorname{div} \underline{m} = \underline{q}$.

Ans since evidently $n \operatorname{div} m = q$, we get that indeed $M \models \underline{n} \operatorname{div} \underline{m} = \underline{n \operatorname{div}^{\mathbb{N}} m}$. □

7.2 Introducing the div$\underline{k}$ & mod$\underline{k}$ functions

In the subsequent chapters, we will often talk about the restrictions of $x \operatorname{div} y$ and $x \bmod y$ with respect to their second parameter y. More specifically, we will restrict y to the term $\underline{k}$, for $k \in \mathbb{N}$.

Let us note that from a formal point of view we should introduce two new unary functional symbols, one for $x \operatorname{div} \underline{k}$ and the other for $x \bmod \underline{k}$, for any $k \in \mathbb{N}$ we want to use those two unary function symbols for. And hence the following two definitions follow.

Definition 7.3 (div $\underline{k}$). Let $k \in \mathbb{N}$. We introduce a new unary functional symbol div$\underline{k}$ by the following formula

$$\varphi_{\text{ div } \underline{k}}(x,z) \equiv ((\underline{k}=0 \wedge z=0) \vee (\underline{k} \neq 0 \wedge (z \times \underline{k} \leq x < (z+1) \times \underline{k})).$$

Definition 7.4 (mod$\underline{k}$). Let $k \in \mathbb{N}$. We introduce a new unary functional symbol mod$\underline{k}$ by the following formula

$$\varphi_{\text{ mod } \underline{k}}(x,z) \equiv ((\underline{k}=0 \wedge z=x) \vee (\underline{k} \neq 0 \wedge (z < \underline{k} \wedge \exists w \leq x\, (w \times \underline{k} + z = x))).$$

As always, we need to check the following.

Observation 7.7 (div$\underline{k}$ and mod$\underline{k}$ are well defined). Let $k \in \mathbb{N}$ and $M \models I\Sigma_1$, then the following holds.

- $M \models \forall x\, \exists! z\, \varphi_{\text{ div } \underline{k}}(x,z)$,
- $M \models \forall x\, \exists! z\, \varphi_{\text{ mod } \underline{k}}(x,z)$,

Proof. Since we got $\varphi_{\text{ div } \underline{k}}(x,z)$ and $\varphi_{\text{ mod } \underline{k}}(x,z)$ only by substituting the term $\underline{k}$ in $\varphi_{\text{ div }}(x,y,z)$ and $\varphi_{\text{ mod }}(x,y,z)$ for the variable y we get by an analogous result for x div y and x mod y, i.e. Observation 7.1, that the observation must hold. □

And by the same argument as in Observation 7.7, and the references to the respective results for x div y and x mod y in section 7.1, we have the following two results (analogous to those in section 7.1).

Observation 7.8 (x div $\underline{k}$ can be represented by a Δ_0 formula). Let $M \models I\Sigma_1$, $k \in \mathbb{N}$ and $x \in M$, then $M \models \exists z\, \varphi_{\text{ div } \underline{k}}(x,z)$ iff. $M \models \exists z \leq x\, \varphi_{\text{ div } \underline{k}}(x,z)$, where the latter formula is obviously a Δ_0 formula.

Observation 7.9 (x mod $\underline{k}$ can be represented by a Δ_0 formula). Let $M \models I\Sigma_1$, $k \in \mathbb{N}$ and $x \in M$, then $M \models \exists z\, \varphi_{\text{ mod } \underline{k}}(x,z)$ iff. $M \models \exists z \leq (x+\underline{k})\, \varphi_{\text{ mod } \underline{k}}(x,z)$, where the latter formula is obviously a Δ_0 formula.

Lastly, let us mention the following observation, which justifies the notation for unary functions div$\underline{k}$ and mod$\underline{k}$.

Observation 7.10. Let $M \models I\Sigma_1$, $k \in \mathbb{N}$ and $x \in M$, then if y is set to $\underline{k}^M$, then $M \models x$ div $y = x$ div $\underline{k}$ as well as $M \models x$ mod $y = x$ mod $\underline{k}$. Where the div and mod on the left hand side of the equations are binary functions introduced in section 7.1 and div$\underline{k}$ and mod$\underline{k}$ on the right hand side of the equations are unary functions introduced in the current section.

Proof. Since we got $\varphi_{\text{ div } \underline{k}}(x,z)$ and $\varphi_{\text{ mod } \underline{k}}(x,z)$ only by substituting the term $\underline{k}$ in $\varphi_{\text{ div }}(x,y,z)$ and $\varphi_{\text{ mod }}(x,y,z)$ the result follows. □

By Observation 7.10 we see that we can use the binary functions x div y and x mod y interchangeably with the unary functions x div $\underline{k}$ and x mod $\underline{k}$, when y is set to the interpretation of $\underline{k}$ in the respective model. Therefore, we will often omit from mentioning whether we are using a binary function x div $\underline{k}$ or a unary function x div $\underline{k}$, and hence the same syntactical notation. And the same goes for mod.

Lastly, we can also use more or less any result for x div y and x mod y when we substitute y for $\underline{k}$, and $\underline{k}$ satisfies all the conditions required from y, for x div $\underline{k}$ and x mod $\underline{k}$. For example an analogy to Corollary 7.2 clearly holds for unary functions x div $\underline{k}$ and x mod $\underline{k}$.

From now on, we will mean by $I\Sigma_1$ the "true" $I\Sigma_1$ with defining axioms for both binary functions div and mod. As well as for the infinitely many unary functions div$\underline{k}$ and mod$\underline{k}$ for every $k \in \mathbb{N}$. And as in PART I, also with the defining axioms for $S(x)$,$P(x)$, $x \dot{-} z$ and $|$, i.e. the divisibility relation, introduced in section 1.4.

8. Recursiveness of the div and mod functions

In this chapter, we start our discussion on the recursivity of div and mod. More precisely, we will be interested in questions whether both x div y and x mod y, as binary functions or as unary functions with y set to $\underline{k}$, can be recursive or not.

The subsequent chapter 9 will deal solely with the recursivity of mod and the next two chapters, namely chapter 10 and chapter 11, will deal with the structure and recursivity of div respectively.

8.1 mod and div can not be both recursive in $I\Sigma_1$

A good question to ask at the start is whether there is a non-standard model of PA where are both functions in mention recursive. And the answer to this questions is *no*.

Before that, let us mention few useful observations.

First follows a remark that will be used all the time, although we will not refer to it.

Remark 8.1 (= is a recursive relation). Let $M \models PA^-$ s.t. $dom(M) = \mathbb{N}$. Then $=^M$ is a recursive relation.

Proof. Since we assume only structures that give to = the standard interpretation, i.e. $n =^M m$ iff. $n = m$, then it is obvious that $=^M$ must be a recursive relation. □

Observation 8.2. Let $M \models I\Sigma_1$, furthermore let $x \in M$ s.t. $M \models 1 < x$. Then for any $y \in M$ we have, $M \models y = S(x)$ iff. $M \models y \operatorname{div} x = 1$ and $M \models y \operatorname{mod} x = 1$.

Proof. ⇒: Assume that $M \models y = S(x)$, therefore $M \models y = x+1$ and thereafter $M \models y = 1 \times x + 1 \wedge 1 < x$. And we can by Corollary 7.2, with x, y from Corollary 7.2 set to y, x from this observation, conclude that indeed $M \models y \operatorname{div} x = 1$ and $M \models y \operatorname{mod} x = 1$.

⇐: Assume that $M \models y \operatorname{div} x = 1$ and $M \models y \operatorname{mod} x = 1$. Since furthermore $M \models 0 < x$ then we have by Corollary 7.2 that $M \models y = (y \operatorname{div} x) \times x + (y \operatorname{mod} x) = x + 1$ which is just a restatement of $M \models y = S(x)$.

□

Corollary 8.3 (recursive div and mod implies recursive $S(x)$)**.** Let $M \models I\Sigma_1$, s.t. $dom(M) = \mathbb{N}$, we can interpret $0, 1$ and $\underline{2}$ in M and div is as well as mod recursive with respect to M. Then $S(x)$ is also recursive with respect to M.

Proof. This is a direct corollary of Observation 8.2. □

Observation 8.4 ($x \operatorname{mod} y$ and $S(x)$ can not be both recursive)**.** Let M be a non-standard model of $I\Sigma_1$ s.t. $dom(m) = \mathbb{N}$. Then $x \operatorname{mod} y$ and $S(x)$ can not be both recursive with respect to M.

Proof. Assume for contradiction that both the assumption and the opposite to the conclusion hold. Moreover, we can assume by Observation 3.13 that $0^M = 0$.

First note that we can compute $\underline{n}^M$ for any $n \in \mathbb{N}$ since it is just the result of applying n times S^M to $0^M (= 0)$.

Therefore, since $p(n)$ is computable by Observation 3.9, we can compute $\underline{p(n)}^M$ for any $n \in \mathbb{N}$, recall that $p(n)$ is the $(n+1)$-th prime function.

Continuing, we have by Corollary 4.3 that there exists a non-recursive subset of $\mathbb{N}$, denote it by X, and an element a of M s.t. $\forall n \in \mathbb{N}$,

$$n \in X \iff M \models \underline{p(n)} \mid a.$$

Which is evidently the same as

$$n \in X \iff M \models a \bmod \underline{p(n)} = 0.$$

Now, since we can compute the binary function $b \bmod {}^M c$ for any $b, c \in M$ and we can compute $\underline{p(n)}^M$ for any $n \in \mathbb{N}$, it follows that we can computably decide membership in X which is the desired contradiction. □

Lemma 8.5 (div and mod can not be both recursive)**.** *M be a non-standard model of $I\Sigma_1$ with its domain equal to $\mathbb{N}$. Then div^M and mod^M can not be both recursive.*

Proof. Let M be from the assumption of the lemma. Furthermore, assume for contradiction that div^M and mod^M are both recursive. Also assume, we can do this by Observation 3.13, that $0^M = 0$, $1^M = 1$ and $\underline{2}^M = 2$.

From Corollary 8.3 follows that mod and S are both recursive with respect to M. But that can not be in the light of Observation 8.4, and hence we get a contradiction.

□

Can we get positive result in case we restrict the second parameter in div and mod? E.g. can we have both x div $\underline{4}$ and x mod $\underline{11}$ recursive with respect to some non-standard model M? Or can we have x div $\underline{k}$ and x mod $\underline{k}$, for some fixed $k \in \mathbb{N}$, both recursive with respect to some non-standard model M?

It mostly doesn't seem to be, since actually in the latter mentioned case we again have the negative answer for $2 \leq k$.

Before we end this section, a proof will be presented that for $k < 2$ we have a non-standard model of PA with both $(x \text{ div } \underline{k})^M$ and $(x \bmod \underline{k})^M$ recursive. And the next section, section 8.2 , is devoted to showing that for $2 \leq k$ there can be no such non-standard model.

Observation 8.6. Let $M \models PA$ and $dom(M) = \mathbb{N}$, furthermore assume that we know the interpretation of 0 in M, i.e. we know 0^M. Then $\mathrm{mod}\underline{0}$, $\mathrm{mod}\underline{1}$, $\mathrm{div}\underline{0}$ and $\mathrm{div}\underline{1}$ are all recursive with respect to M.

Proof. Since $(x \bmod \underline{0})^M = x$ as well as $(x \text{ div } \underline{1})^M = x$ for every $x \in M$, i.e. they are the identity functions on $\mathbb{N}$, we get that they are both recursive.

Furthermore, we clearly have $(x \bmod \underline{1})^M = 0^M$ as well as $(x \text{ div } \underline{0})^M = 0^M$, hence they are constant functions returning 0^M which we know how to compute, hence they are also recursive. □

Corollary 8.7. There exists a non-standard model M of PA s.t. $dom(M) = \mathbb{N}$, and all the functions

- $\text{div}\underline{0}$,
- $\text{div}\underline{1}$,
- $\text{mod}\underline{0}$,
- $\text{mod}\underline{1}$,

are recursive with respect to it.

Proof. Recall that there exists a non-standard countable model M' of PA by Corollary 2.3. By Observation 3.12 we get that there must exists one, denote it as M, with domain equal to $\mathbb{N}$, where the non-standardness of M follows by $M' \cong M$. Lastly, by Observation 3.13 we can also assume that $0^M = 0$.

Therefore, there exists a non-standard model M of PA s.t. $dom(M) = \mathbb{N}$ and $0^M = 0$. Hence, the result follows by noting Observation 8.6. □

8.2 For any $2 \leq k$, $\text{mod}\underline{k}$ and $\text{div}\underline{k}$ can not be both recursive in PA

Let us note that the following commentary only hints the ideas to come. And as such, the commentary is very informal.

Commentary. Intuitively speaking, how would one prove that $\text{mod}\underline{k}$ and $\text{div}\underline{k}$ can not be both recursive in some non-standard model of PA?

After all the discussion we went through in chapter 4 and chapter 5, the following idea proposes it self.

We take some non-recursive set $X \subseteq \mathbb{N}$ and code it using some non-standard element e. The coding is going to be s.t. when we look at numbers as in theirs k-ary notation, i.e. with digits $\{0, 1, \ldots, (k-1)\}$ then at the n-th place, for any $n \in \mathbb{N}$, we will have 0 if $n \in X$ and 1 otherwise.

Then to find whether $n \in X$ it does suffice to apply n-times $div\underline{k}$ to e, i.e. $((e \text{ div } \underline{k}) \ldots) \text{ div } \underline{k}$ where $\text{div } \underline{k}$ is n times in that expression, to get some number a. Afterwards to the result of such a computation, i.e. to a, we will apply $\text{mod } \underline{k}$. And if the final result is 0 we return $n \notin X$ and otherwise we return $n \in X$.

We will now formalize the proposed idea to show that there can be no non-standard model of PA where both $\text{mod}\underline{k}$ and $\text{div}\underline{k}$ are recursive.

Commentary. Please also bear in mind that we can not choose just any non-recursive subset of $\mathbb{N}$. It is because there are uncountably many non-recursive subsets of $\mathbb{N}$ and for the proof to work we evidently need to code different sets by different elements of the model in mention. And thus, if we were able to conduct the process for any non-recursive set it would imply that the model in mention has an uncountable domain. But that is not an option, since we have restricted our discussion only to models with domain $\mathbb{N}$, or possibly countable domains which are *computably codable*, see Informal Definition 3.11.

For a proof that there are uncountably many recursive sets see first pages in Boolos et al. [2007, Chapter 4]. The discussion shows that there are only countably many Turing computable functions, hence also there are only countably many recursive functions by a combination of Boolos et al. [2007, Theorem 5.6, p.56] and Boolos et al. [2007, Theorem 5.8, p.61]. And since every recursive subset X of $\mathbb{N}$ determines one distinct recursive function, namely χ_X, we get that there are only countably many recursive subsets of $\mathbb{N}$. And since there are uncountably many subsets of $\mathbb{N}$ in total, see e.g. Boolos et al. [2007, pp.16-17, Theorem 2.1], we get that there are uncountably many non-recursive subsets of $\mathbb{N}$.

Commentary. Lastly, let us mention that we will use the exp function to express by a formula the process of applying n-times the div$\underline{k}$ function to x, i.e. we can obviously write it down as x div exp$(\underline{k}, \underline{n})$. To highlight this use, let us state it as an observation.

Observation 8.8. Let $M \models PA$, $n, k \in \mathbb{N}$, then for any $a \in M$ we have

$$M \models ((a \text{ div } \underline{k}) \ldots \underline{k}) = a \text{ div } \exp(\underline{k}, \underline{n}),$$

where the div$\underline{k}$ is repeated n-times on the left hand side.

Proof. Possible line of proof is by induction on n, we omit the details. □

Since the ideas are very similar to those in chapter 4 and chapter 5 it should not be a surprise that the discussion which follows is going to resemble them. For example, the following lemma is analogous to Lemma 4.1.

Lemma 8.9 (Coding sets using div$\underline{k}$ and mod$\underline{k}$)**.** Let M be a non-standard model of PA and $\varphi(\overline{x}, y)$ be some formula in L_A or some extension of it. Furthermore let $\overline{b} \in M$ and $k \in \mathbb{N}$ s.t. $2 \leq k$. Define $X := \{n \in \mathbb{N} | M \models \varphi(\overline{b}, \underline{n})\}$ and as usual let χ_X be its characteristic function.

Then there exists $a \in M$ s.t. $\forall n \in \mathbb{N}$ we have $n \in X$ iff. $M \models (a \text{ div } \exp(\underline{k}, \underline{n})) \text{ mod } \underline{k} = 0$, or equivalently

$$M \models \varphi(\overline{b}, \underline{n}) \leftrightarrow (a \text{ div } \exp(\underline{k}, \underline{n})) \text{ mod } \underline{k} = 0.$$

Proof. We clearly have for any $m \in \mathbb{N}$ the following

$$M \models \exists a \, \forall n \leq \underline{m} \, (\varphi(\overline{b}, n) \leftrightarrow (a \text{ div } \exp(\underline{k}, n)) \text{ mod } \underline{k} = 0).$$

Specifically, it evidently follows by setting a to $(\chi_X(m) \times \exp(\underline{k}, \underline{m}) + \ldots + \chi_X(0) \times \exp(\underline{k}, \underline{0}))^M$.

Hence, we can apply Overspill lemma, Lemma 2.6, to show that there exists a non-standard element $e \in M$ s.t.

$$M \models \exists a \, \forall n \leq e \, (\varphi(\overline{b}, n) \leftrightarrow (a \text{ div } \exp(\underline{k}, n)) \text{ mod } \underline{k} = 0).$$

And since every standard element is below any non-standard element the conclusion of the just being proved lemma follows. □

Corollary 8.10 (Non-recursive set coded using div$\underline{k}$ and mod$\underline{k}$)**.** Let M be a non-standard model of PA and $k \in \mathbb{N}$ s.t. $2 \leq k$. Then there exists a non-recursive sets $X \subseteq \mathbb{N}$ and $a \in M$ s.t.

$$n \in X \iff M \models (a \text{ div } \exp(\underline{k}, \underline{n})) \text{ mod } \underline{k} = 0.$$

Proof. This is a corollary of the just proved Lemma 8.9 and Lemma 4.2 from section 4.2 which is about being able to code in any non-standard models of PA some non-recursive set with a Δ_0 formula. □

At last, we approach the main lemma of this subsection.

Lemma 8.11 (div$\underline{k}$ and mod$\underline{k}$ can not be both recursive)**.** Let $M \models PA$, with its domain equal to $\mathbb{N}$, and $k \in \mathbb{N}$ s.t. $2 \leq k$. Then the unary functions $x \bmod \underline{k}$ and $x \operatorname{div} \underline{k}$ can not be both recursive.

Proof. Assume that M and k satisfy the assumptions in the statement of the just being proved lemma. And for the contrary assume that $x \bmod \underline{k}$ and $x \operatorname{div} \underline{k}$ are both recursive.

We can again WLOG assume that $0^M = 0$ by Observation 3.13.

But now it is easy to observe, by the just proved Corollary 8.10 and by Observation 8.8, i.e. that $M \models ((a \operatorname{div} \underline{k}) \ldots \underline{k}) = a \operatorname{div} \exp(\underline{k}, \underline{n})$, that we can now computably decide membership in some set $X \subseteq \mathbb{N}$ which is not recursive, which in turn gives rise to a contradiction we want. □

8.3 div$\underline{k}$ with $S(x)$ or $<$ can not be both recursive in PA

Observation 8.12. Let $M \models I\Sigma_1$, $a \in M$ and $k \in \mathbb{N}$ s.t. $0 < k$. Then there exists exactly k elements x of M s.t. $M \models x \operatorname{div} \underline{k} = a$. Furthermore, if we set $b = (\underline{k} \times a)^M$ then they are of the form $b, (b+1)^M, \ldots, (b + \underline{(k-1)})^M$

Proof. Clearly, all the elements $b, (b+1)^M, \ldots, (b + \underline{(k-1)})^M$ satisfy $M \models x \operatorname{div} \underline{k} = a$ by the definition of div.

And for any other $y \in M$ we must have either $M \models y < \underline{k} \times a$ or $M \models ((a+1) \times \underline{k}) \leq y$, which by definition of div implies that y can not satisfy $M \models y \operatorname{div} \underline{k} = a$. □

Let us observe the following two observations.

Observation 8.13 (Recursive div$\underline{k}$ and $S(x)$ implies recursive mod$\underline{k}$)**.** Let M be a model of$I\Sigma_1$, s.t. $dom(M) = \mathbb{N}$ and both div$\underline{k}$ and $S(x)$ are recursive functions with respect to M. Moreover assume that we know the interpretation of 0^M. Then mod$\underline{k}$ is a recursive function with respect to M as well.

Proof. First note that since we know the interpretation of 0^M and $S(x)$ is recursive, then it is evident that we can compute $\underline{n}^M$ for any $n \in M$.

Let $b \in M$ and we want to find $(b \bmod \underline{k})^M$.

First of all compute $(b \operatorname{div} \underline{k})^M$, which we can by our assumption on recursivity of div, and denote the result as a.

Now compute, which we can by recursivity of $S(x)$, $(S(b) \operatorname{div} \underline{k})^M$ and then $(S(S(b)) \operatorname{div} \underline{k})^M$ and so on until we get for the first time result that differs from a.

Since $S(x)$ is clearly an injective function we get by Observation 8.12 that after at most k steps we finish this procedure.

Denote by l the number of steps that we have actually needed. Then since $S(x)$ adds 1^M, with respect to M, we obviously get mainly by Observation 8.12 that

$(b \bmod \underline{k})^M = \underline{(k-l)}^M$, where the expression on the right side of the equation can be computed, as we have already noted at the start of our proof.

We have managed to compute $(b \bmod \underline{k})^M$ for any $b \in M$ and thereafter the proof of the recursivity of mod$\underline{k}$ is finished. ☐

Observation 8.14 (Recursive div$\underline{k}$ and $<$ implies recursive mod$\underline{k}$)**.** Let $M \models I\Sigma_1$, s.t. $dom(M) = \mathbb{N}$ and both div $\underline{k}$ and $<$ are recursive functions with respect to M. Moreover assume that we know the interpretation of 0^M. Then mod$\underline{k}$ is a recursive function with respect to M as well.

Proof. First note that since we know the interpretation of 0^M and $<$ is recursive as well as div$\underline{k}$, then we can compute $\underline{l}^M$ for any $l \in \mathbb{N}$ s.t. $0 \leq l < k$.

Simply recursively enumerate $\mathbb{N}$ with respect to $<^{\mathbb{N}}$ and compute $(x \text{ div } \underline{k})^M$ for the just enumerated x. If the result is 0^M, store such a x. If we have already stored k x's, we stop.

We know that this procedure must stop by Observation 8.12 and we also know by that observation how those x's look like.

Now it is obvious that $\underline{l}^M$ is the $(l+1)$-th smallest x we have stored and we can recursively determine which one is the $(l+1)$-th smallest by using $<^M$ which is recursive.

A part of a proof which is similar to both the part we have already presented and to the proof in Observation 8.13 follows.

Let $b \in M$ and we want to compute $(b \bmod \underline{k})^M$.

First of all compute $(b \text{ div } \underline{k})^M$, which we can by our assumption on recursivity of div, and then denote it as a.

Now recursively enumerate $\mathbb{N}$ with respect to $<^{\mathbb{N}}$ and compute $(x \text{ div } \underline{k})^M$, where x is the enumerated over member of $\mathbb{N}$, whenever the result equals a we store such a x. If we have already stored k x's, we stop.

We know by Observation 8.12 that this procedure must stop.

Now, we can order all the stored x's with respect to recursive $<^M$.

Since we know how these stored x's look like by Observation 8.12 we know that if b, which is stored as one of the x's, is l-th smallest element among the stored x's, with respect to $<^M$, then actually $(b \bmod \underline{k})^M = \underline{(l-1)}^M$, which we can compute by our remark at the start of the proof, since $(l-1) < k$.

We have managed to compute $(b \bmod \underline{k})^M$ for any $b \in M$ and thereafter the proof of the recursivity of mod$\underline{k}$ is finished. ☐

As a corollaries we get the following.

Corollary 8.15 (div$\underline{k}$ and $S(x)$ can not be both recursive)**.** Let M be a non-standard model of PA s.t. $dom(M) = \mathbb{N}$ and let $k \in \mathbb{N}$ s.t. $2 \leq k$. Then we can not have both div$\underline{k}$ and $S(x)$ recursive in M.

Proof. Assume for contradiction that there can be such a non-standard model M. Then by Observation 3.13 we can WLOG assume that $0^M = 0$.

But it now follows by Observation 8.13 that div$\underline{k}$ together with mod$\underline{k}$ are recursive with respect to M which is in direct contradiction with Lemma 8.11. ☐

Corollary 8.16 (div$\underline{k}$ and $<$ can not be both recursive)**.** Let M be a non-standard model of PA s.t. $dom(M) = \mathbb{N}$ and let $k \in \mathbb{N}$ s.t. $2 \leq k$. Then we can not have both div$\underline{k}$ and $<$ recursive in M.

Proof. The proof is exactly the same as in Corollary 8.15, we only substitute the reference to Observation 8.13 for the reference to Observation 8.14. □

Let us state a sharpening of Corollary 8.16, that we will be of use to us later.

Corollary 8.17 (div$\underline{k}$ and restricted $<$ can not be both recursive)**.** Let M be a non-standard model of PA s.t. $dom(M) = \mathbb{N}$ and let $k \in \mathbb{N}$ s.t. $2 \leq k$. Furthermore have some binary function $f_<(x, y)$ s.t. for any $x, y \in M$ where $M \models x < y$ and $x \in y_{\mathbb{Z}}$ it holds $f_<(x, y) = 1$, i.e. $f_<$ computes $<^M$ on elements which are apart by a standard distance. Then we can not have both div$\underline{k}$ recursive with respect to M and $f_<(x, y)$ recursive.

Proof. The proof is the same as for Corollary 8.16.

Only note that in the proof of Observation 8.14 to work we do not need to have $<$ recursive. More specifically, recursive $f_<$ instead of recursive $<$ will do. □

Lastly, let us show that we get as a corollary that $\underline{k} \times x$, $\underline{k} \times x + 1$,...,$\underline{k} \times x + \underline{(k-1)}$ can not be recursive all at once in a non-standard model of PA. (From a strictly formal point of view we should have introduced new unary function symbols for all the mentioned unary functions for any $k \in \mathbb{N}$, however, we believe that everything is understandable anyway.)

Corollary 8.18. Let $M \models PA$ s.t. $dom(M) = \mathbb{N}$ and $k \in \mathbb{N}$ s.t. $2 \leq k$. Then the unary functions $\underline{k} \times x$, $\underline{k} \times x + 1$,...,$\underline{k} \times x + \underline{(k-1)}$ can not be recursive all at once.

Proof. Assume that all the assumptions hold. For contradiction assume the the conclusion does not hold. We can also WLOG assume by Observation 3.13 that $0^M = 0$,...,$\underline{k-1}^M = k - 1$.

Let $x \in M$, we will simultaneously observe how to compute $(x \bmod \underline{k})^M$ and $(x \text{ div } \underline{k})^M$ which can not be by Lemma 8.11.

Enumerate $\mathbb{N}$ recursively according to $<^{\mathbb{N}}$ and denote by y the just enumerated member of $\mathbb{N}$. For every enumerated y we compute $(\underline{k} \times y + \underline{l})^M$ for any $l \in \mathbb{N}$ s.t. $0 \leq l < k$. We do this process until we find such a y and l s.t. $M \models \underline{k} \times y + \underline{l} = x$. And then we return y as a result of $(x \text{ div } \underline{k})^M$ and l as the result of $(x \bmod \underline{k})^M$, for this also recall that $\underline{l}^M = l$.

We know by Theorem 2.4 that there exists q and r in $dom(M) = \mathbb{N}$ s.t. $M \models x = q \times \underline{k} + r \wedge r < \underline{k}$. And recall that by Observation 1.31 we get that $M \models r = \underline{0} \vee \ldots \vee r = \underline{(k-1)}$. Therefore, it can be concluded that the process must eventually stop.

And since $M \models 0 < \underline{k}$, we get by Corollary 7.2 that the correct answer is returned. □

Concluding remarks

Concluding remarks for mod

Since we know by results in section 8.3 that there can be no such non-standard model of PA s.t. div$\underline{k}$ and $S(x)$ or div$\underline{k}$ and $<$ are both recursive in it, we can ask whether the same holds for mod$\underline{k}$ substituted for div$\underline{k}$. As we will see in section 9.1, the analog for mod$\underline{k}$ does not hold. We will even observe in section 9.1 that there is a non-standard model M of PA s.t. all mod$\underline{k}$, $S(x)$ and $<$ are recursive with respect to M.

Last natural question that we will pose for mod, since div and mod can not be both recursive in a non-standard model of $I\Sigma_1$ by Section 8.1, is whether mod on its own can be recursive in some non-standard model of $I\Sigma_1$ or some extension of it e.g. PA. This question got our interest, nevertheless, we did not manage to reach a conclusion. More on this topic in section 9.2.

Concluding remarks for div

Analogues questions as for mod emerge.

After the negative results for the div $\underline{k}$ in section 8.3 a natural question arises, specifically, whether there can be a non-standard model of PA where at least div$\underline{k}$ by its own is recursive? An answer to this question is positive, i.e. there can be such a non-standard model. First, we will develop in chapter 10 a deeper understanding of the behavior of div$\underline{k}$ in models of PA. And then, the result itself will be stated in section 11.2.

However, we also have the negative general result that there can be no non-standard model of $I\Sigma_1$ s.t. both mod and div are recursive with respect to it from Section 8.1. Again, another question arises. Can there be a non-standard recursive model of $I\Sigma_1$ where div is recursive? The answer to this question is negative, i.e. there can be no such a non-standard model, as will be observed in section 11.1.

9. Recursiveness of the mod function

9.1 $x \bmod \underline{k}$ can be recursive in PA

Before we reach the main result of this section we will state a few useful observations.

Observation 9.1 ("distributivity" of mod)**.** Let M be a model of $I\Sigma_1$, then for any $a, k, l, t \in M$ s.t. $M \models l \mid k$ we have

$$M \models (a+t) \bmod l = ((a \bmod k) + t) \bmod l = ((a \bmod k) + (t \bmod k)) \bmod l.$$

Proof. First, let us note that the second equality follows by the first equality and Ax.2 [commutativity +] .

Therefore, we need to show only $M \models (a+t) \bmod l = ((a \bmod k)+t) \bmod l$.

- Assume $k = 0^M$. Then by definition of mod we have $M \models (a \bmod k) = a$, and therefore, we indeed have $M \models (a+t) \bmod l = ((a \bmod k)+t) \bmod l$.
- Assume that $l = 0^M$, then obviously $k = 0^M$ and the same argument as in the previous item applies.
- Lastly, assume $l \neq 0^M$ and $k \neq 0^M$.

  Let us observe the following items which are by the theorem on unique quotients/remainders, i.e. from Theorem 2.4.

  (i) Let $q_1, r_1 \in M$ be s.t. $M \models a = q_1 \times k + r_1 \wedge r_1 < k$.
  (ii) Let $q_2, r_2 \in M$ be s.t. $M \models r_1 + t = q_2 \times l + r_2 \wedge r_2 < l$.
  (iii) Let $q_3, r_3 \in M$ be s.t. $M \models a + t = q_3 \times l + r_3 \wedge r_3 < l$.

  We have by Corollary 7.2 that $M \models r_1 = a \bmod k$, hence, we have again by Corollary 7.2 that $M \models r_2 = ((a \bmod k) + t)) \bmod l$. Furthermore, we can reach that $r_3 = (a+t) \bmod l$ by the same argument. And therefore, it does suffice to show that $r_2 = r_3$.

  By (iii) we have $M \models a+t = q_3 \times l + r_3$ and by (i) we get that $M \models q_1 \times k + r_1 + t = q_3 \times l + r_3$. Lastly, by (ii) we have $M \models q_1 \times k + q_2 \times l + r_2 = q_3 \times l + r_3$.

  Since $M \models l \mid k$, we get that there exists $s \in M$ s.t. $M \models s \times l = k$. Therefore, we get that $M \models (q_1 \times s + q_2) \times l + r_2 = q_3 \times l + r_3$, where both $M \models r_2 < l$ and $M \models r_3 < l$.

  And now since $l \neq 0^M$, we get by the uniqueness part of Theorem 2.4 that indeed $r_2 = r_3$, which finishes the proof.

□

Let us note that we will use the preceding observation with $k, l \in \mathbb{N}^M$, and hence the choice of letters.

Observation 9.2 ($(x \bmod \underline{n})^M$ is a standard element below $\underline{n}^M$)**.** Let $M \models I\Sigma_1$, then for any $a \in M$ and any $n \in \mathbb{N}$ s.t. $n \neq 0$ we have the following.

$$M \models a \bmod \underline{n} = \underline{l},$$

for some $l \in \mathbb{N}$ s.t. $l < n$.

Proof. Let everything be as in the assumption of the observation.

By the definition of mod we see that $M \models a \bmod \underline{n} < \underline{n}$. Therefore, by Observation 1.31, we get that the conclusion must hold. □

Observation 9.3. Let $M \models I\Sigma_1$, $a \in M$ and $k \in \mathbb{N}$. Then there exists $r \in \mathbb{N}$, actually $r \leq k$, s.t.

$$M \models (a + \underline{r}) \bmod \underline{k} = 0.$$

Proof. If $k = 0$, then the observation is trivial, hence assume that $0 < k$.

First, we know by Observation 9.2 that there exists $l \in \mathbb{N}$ s.t. $l < k$ and $M \models \underline{l} = a \bmod \underline{k}$.

There clearly must exist $r \in \mathbb{N}$ s.t. $(l + r) \bmod^{\mathbb{N}} k = 0$ and $r < k$. Take such a r and let us compute $((a + \underline{r}) \bmod \underline{k})^M$.

We have,

$$\begin{gathered} M \models (a + \underline{r}) \bmod \underline{k} = \\ ((a \bmod \underline{k}) + \underline{r}) \bmod \underline{k} = \\ (\underline{l} + \underline{r}) \bmod \underline{k} = \\ \underline{l + r} \bmod \underline{k} = \\ \underline{(l + r) \bmod^{\mathbb{N}} k} = \\ \underline{0} = \\ 0, \end{gathered}$$

which is what we wanted to show.

Where the first = follows by Observation 9.1, second = follows by our assumption, third = follows by Observation 1.22, fourth = follows by Observation 7.5 and the last = follows by the definition of underlined terms. □

The rest of this section is going to have strong resemblance to section 6.2 and section 6.3.

Theorem 9.4 (Structure of the $<$, $S(x)$ and mod$\underline{k}$ in $I\Sigma_1$)**.** Let M be a nonstandard model of $I\Sigma_1$, $k \in \mathbb{N}$ and recall that implicitly M models defining axiom for $S(x)$, introduced in Definition 1.3, and the defining axioms for mod$\underline{k}$, which can be found in Observation 7.9. Furthermore, set $(A, <_\sim)$ as in Lemma 6.6, i.e. $A := (M/\sim_<) \setminus \{0_{\mathbb{Z}}^M\}$ and for $a_{\mathbb{Z}}, b_{\mathbb{Z}} \in A$ we have $a_{\mathbb{Z}} <_\sim b_{\mathbb{Z}}$ iff. $a_{\mathbb{Z}} \neq b_{\mathbb{Z}}$ and $\exists a \in a_{\mathbb{Z}} \, \exists b \in b_{\mathbb{Z}}$ s.t. $M \models a < b$. Then $(M, <^M, S^M, (\text{mod}\underline{k})^M) \cong (\mathbb{N} \cup A \times \mathbb{Z}, <', S', \text{mod}')$, where we define $<', S'$ and mod$'$ in the following manner.
Definition of $<'$.

- Let $n, m \in \mathbb{N}$, then $n <' m \iff n < m$.
- Let $n \in \mathbb{N}$ and $a \in A \times \mathbb{Z}$, then we always set $n <' a$.
- Let $(q, k), (r, l) \in A \times \mathbb{Z}$, then we set $(q, k) <' (r, l)$ iff. $q <_\sim r$ or $q = r \wedge k <^{\mathbb{Z}} l$.

Definition of $S^{'}$.

- If $x \in \mathbb{N}$, then $S^{'}(x) = x + 1$.
- If $x = (q, k) \in A \times \mathbb{Z}$, then $S^{'}(x) = (q, k + 1)$.

Definition of $\text{mod}^{'}$.

- If $x \in\ N$, then $x \text{ mod }^{'} = x \text{ mod }^{\mathbb{N}} k$.
- If $x = (q, l) \in A \times \mathbb{Z}$ and $0 \leq l$, then $x \text{ mod }^{'} = l \text{ mod }^{\mathbb{N}} k$.
- If $x = (q, l) \in A \times \mathbb{Z}$ and $l < 0$, then $x \text{ mod }^{'} = (k - ((-l) \text{ mod }^{\mathbb{N}} k)) \text{ mod }^{\mathbb{N}} k$.

Proof. Take a function, by *Axiom of Choice* - for further details see Enderton [1977, p.151], $s\colon A \longrightarrow M$ s.t. $\forall q \in A\ s(q) \in q$ and $M \models s(q) \text{ mod } \underline{k} = 0$. By Observation 9.3, it easily follows that for any $q \in M$ we must have in $q_{\mathbb{Z}}$ an element x s.t. $M \models x \text{ mod } \underline{k} = 0$, and hence is s a well defined function.

Further define for any $x \in \mathbb{N} \cup A \times \mathbb{Z}$,

$$h(x) := \begin{cases} \underline{n}^M & x = n \wedge n \in \mathbb{N}, \\ (s(a_{\mathbb{Z}}) + \underline{k})^M & x = (a_{\mathbb{Z}}, k) \wedge 0 \leq^{\mathbb{Z}} k, \\ (s(a_{\mathbb{Z}}) \dot{-} \underline{l})^M & x = (a_{\mathbb{Z}}, k) \wedge k <^{\mathbb{Z}} 0 \wedge l = -k. \end{cases}$$

We can now copy-paste the proof in Theorem 6.7 to observe that h is a bijection from $\mathbb{N} \cup A \times \mathbb{Z}$ onto M. S.t. it respects $S(x)$ and $<$.

Therefore, we only need to show that h respects $\text{mod } \underline{k}$, i.e. that $h(x \text{ mod }^{'}) = (h(x) \text{ mod } \underline{k})^M$, for any $x \in M$.

$x \in \mathbb{N}$: Let $n \in N$ s.t. $x = n$.

We evidently have $h(n \text{ mod }^{'}) = \underline{(n \text{ mod }^{\mathbb{N}} k)}^M$.

On the other hand, $(h(x) \text{ mod } \underline{k})^M = (\underline{n} \text{ mod } \underline{k})^M$, which by Observation 7.5 equals $\underline{(n \text{ mod }^{\mathbb{N}} k)}^M$, and the wanted equality follows.

$x = (q, l) \in A \times \mathbb{Z}$:

$0 \leq l$: We have $x \text{ mod }^{'} = l \text{ mod }^{\mathbb{N}} k$. Therefore, we have that $h(x \text{ mod }^{'}) = (\underline{l \text{ mod }^{\mathbb{N}} k})^M$.

On the other hand, we evidently have, since $0 \leq l$, that $h(x) = (s(q) + \underline{l})^M$. Computing $(h(x) \text{ mod } \underline{k})^M$, we get by Observation 9.1 that

$$(h(x) \text{ mod } \underline{k})^M = ((s(q) \text{ mod } \underline{k} + \underline{l}) \text{ mod } \underline{k})^M.$$

Lastly, recalling that $M \models s(q) \text{ mod } \underline{k} = 0$, we get that $(h(x) \text{ mod } \underline{k})^M$ equals to $(\underline{l} \text{ mod } \underline{k})^M$.

Applying Observation 7.5, we have $(\underline{l} \text{ mod } \underline{k})^M = (\underline{l \text{ mod }^{\mathbb{N}} k})^M$, which is what we wanted to show.

$l < 0$: Note that if $k = 0$, then this whole proof is trivial, therefore, from now on assume that $0 < k$.

We have $x \bmod ' = (k - ((-l) \bmod {}^{\mathbb{N}}k)) \bmod {}^{\mathbb{N}}k$. Therefore,

$$h(x \bmod ') = (\underline{(k - ((-l) \bmod {}^{\mathbb{N}}k)) \bmod {}^{\mathbb{N}}k})^M.$$

On the other hand, we have, since $l < 0$, that $h(x) = (s(q) \dot{-} \underline{(-l)})^M$. Therefore,

$$\begin{gathered} M \models h(x) \bmod \underline{k} = \\ (s(q) \dot{-} \underline{(-l)}) \bmod \underline{k} = \\ ((s(q) \dot{-} \underline{(-l)}) + 0) \bmod \underline{k} = \\ ((s(q) \dot{-} \underline{(-l)}) + \underline{(-l) \times k}) \bmod \underline{k} = \\ (s(q) + (\underline{(-l) \times k} \dot{-} \underline{(-l)})) \bmod \underline{k} = \\ (s(q) + \underline{(-l) \times (k-1)}) \bmod \underline{k} = \\ \underline{(-l) \times (k-1)} \bmod \underline{k} = \\ \underline{(-l) \times (k-1) \bmod {}^{\mathbb{N}}k} = \\ \underline{(k - ((-l) \bmod {}^{\mathbb{N}}k)) \bmod {}^{\mathbb{N}}k}, \end{gathered}$$

which is what we wanted to show.

Where the respective equality signs follow by the following points.

(i) By the definition of h.

(ii) By Ax.6 [0, 1 are neutral] .

(iii) By Ax.2 [commutativity +] combined with Observation 9.1, i.e. that mod is "distributive", and by Observation 7.5, i.e. that mod behaves as expected on $\mathbb{N}^M$.

(iv) This equality can be concluded by first noting $M \models \underline{-l} \leq s(q)$ and $M \models \underline{-l} \leq \underline{(-l) \times k}$, and then applying Observation 1.27.

(v) It is because $\dot{-}$ behaves on $\mathbb{N}^M$ as expected when when subtracting $\underline{m}^M$ from $\underline{n}^M$ s.t. $M \models \underline{m} \leq \underline{n}$, for a proof see Observation 1.25.

(vi) Follows mainly by Observation 9.1, i.e. "distributivity" of mod, and using the fact that $M \models s(q) \bmod \underline{k} = 0$, combined with Ax.2 [commutativity +] and Ax.6 [0, 1 are neutral] .

(vii) Follows by Observation 7.5, i.e. that mod behaves on $\mathbb{N}^M$ as expected.

(viii) Standard truth in $\mathbb{N}$.

□

And by the same argument as for Corollary 6.10, we get the following corollary.

Corollary 9.5. Let M be a countable non-standard model of $I\Sigma_1$, $k \in \mathbb{N}$ and recall that implicitly M models defining axiom for $S(x)$, introduced in Definition 1.3, and the defining axioms for mod$\underline{k}$, which can be found in Observation 7.9. Then $(M, <^M, S^M, (\text{mod}\underline{k})^M) \cong (\mathbb{N} \cup Q \times \mathbb{Z}, <', S', \text{mod}')$, where we define $<', S'$ and mod$'$ followingly.

Definition of $<'$.

- Let $n, m \in \mathbb{N}$, then $n <' m \iff n < m$.
- Let $n \in \mathbb{N}$ and $a \in Q \times \mathbb{Z}$, then we always set $n <' a$.
- Let $(q,k), (r,l) \in Q \times \mathbb{Z}$, then we set $(q,k) <' (r,l)$ iff. $q <^{\mathbb{Q}} r$ or $q = r \wedge k <^{\mathbb{Z}} l$.

Definition of S'.

- If $x \in N$, then $S'(x) = x + 1$.
- If $x = (q,k) \in Q \times \mathbb{Z}$, then $S'(x) = (q, k+1)$.

Definition of mod'.

- If $x \in N$, then $x \text{ mod }' = x \text{ mod }^{\mathbb{N}} k$.
- If $x = (q,l) \in Q \times \mathbb{Z}$ and $0 \leq l$, then $x \text{ mod }' = l \text{ mod }^{\mathbb{N}} k$.
- If $x = (q,l) \in Q \times \mathbb{Z}$ and $l < 0$, then $x \text{ mod }' = (k - ((-l) \text{ mod }^{\mathbb{N}} k)) \text{ mod }^{\mathbb{N}} k$.

Proof. The corollary follows immediately by the just proved Theorem 9.4 and Corollary 6.9, which states that $(A, <_{\sim}) \cong (Q, <^{\mathbb{Z}})$. □

We can finally approach one of the main result of this section, note the resemblance to Lemma 6.12.

Lemma 9.6 ($<, S$ and $\text{mod}\underline{k}$ can be all recursive)**.** There exists a non-standard model M of PA, recall that we implicitly include defining axioms for $S(x)$ and $x \text{ mod } \underline{k}$ in PA, s.t. $dom(M) = \mathbb{N}$ and the relation $<$ as well as the functions S and $\text{mod}\underline{k}$ are recursive with respect to it.

Proof. First, let us note that the witness to $(\mathbb{N} \cup \mathbb{Q} \times \mathbb{Z})$ being *computably codable set* can be found in Bijection 5.

Now, since there exists a non-standard countable model of PA by Corollary 2.3 we get by Corollary 9.5, for this recall that if $M \models I\Sigma_1$ then $M \models PA$, and by Corollary 3.15 that the just being proved lemma holds. □

To conclude this section, we will state one, possibly interesting, corollary of Lemma 9.6 as well as a few commentaries related to strengthening Theorem 9.4, which consequently strengthens also Corollary 9.5.

Corollary 9.7 ($<, S$ and $\text{mod}\underline{l}$, for all l in a finite set $F \subseteq \mathbb{N}$, can be all recursive)**.** Let F be a finite subset of $\mathbb{N}$. Then there exits a non-standard model of PA, denote it as M, s.t. M satisfies all the following.

- $dom(M) = \mathbb{N}$.
- $<$ is recursive with respect to M.
- S is recursive with respect to M.
- $\forall l \in F$, we have that $\text{mod}\underline{l}$ is recursive with respect to M.

Proof. Define $p \in \mathbb{N}$ as the following product, $p := \Pi_{l \in F \setminus \{0\}} l$, where least common multiple of $F \setminus \{0\}$ would be sufficient as well. Where, as it is customary, if $F \setminus \{0\} = \emptyset$, then p equals 1.

Let M' be a non-standard model of PA that we can get from Lemma 9.6 with k set to p. More specifically, we have M' s.t. M' is a non-standard model of PA, $dom(M') = \mathbb{N}$, and $<$,S as well as mod$\underline{p}$ are recursive with respect to M'.

Furthermore, by Observation 3.13, we know that there exists a non-standard model of PA, denote it as M, s.t. $dom(M) = \mathbb{N}$, $\forall r \leq p\ \underline{r}^M = r$ and $<$,S as well as mod$\underline{p}$ are recursive with respect to it.

Now, we will show that actually for every $l \in F$ is mod $\underline{l}$ recursive with respect to M, and the proof will be finished.

Since $0 \leq p$, we have that $0^M = 0$. Therefore, we can conclude by Observation 8.6 that mod$\underline{0}$, and also mod$\underline{1}$, are recursive with respect to M.

Let $l \in F \setminus \{0\}$ and x be any element of M.

Since $l \mid p$ implies $M \models \underline{l} \mid \underline{p}$, by Observation 1.32, we get by Observation 9.1 that $M \models x \bmod \underline{l} = (x \bmod \underline{p}) \bmod \underline{l}$.

We can compute, by our assumption, $(x \bmod \underline{p})^M$, denote the result as a.

Evidently $M \models 0 \neq \underline{p}$, hence, $M \models a < \underline{p}$. And by Observation 1.31 we can conclude that a is one of $0^M, \ldots, \underline{(p-1)}^M$. But since $0^M = 0, \ldots, \underline{(p-1)}^M = p - 1$, we can compute the exact $r \in \mathbb{N}$ s.t. $\underline{r}^M = a$.

To remind us of our goal, we need to compute $(a \bmod \underline{l})^M$ which, as we know, is the same as computing $(\underline{r} \bmod \underline{l})^M$.

But computing $(\underline{r} \bmod \underline{l})^M$ is easy. It is because by Observation 7.5 $M \models \underline{r} \bmod \underline{l} = \underline{r \bmod {}^{\mathbb{N}} l}$. And since is mod$^{\mathbb{N}}$ surely computable, we can compute $r \bmod {}^{\mathbb{N}} l$. Continuing, evidently $r \bmod {}^{\mathbb{N}} l \leq l \leq p$, hence, we we can also compute $\underline{r \bmod {}^{\mathbb{N}} l}^M$ because it simply equals $r \bmod {}^{\mathbb{N}} l$.

To summarize, we can compute $\underline{r \bmod {}^{\mathbb{N}} l}^M$ which is the same as $(\underline{r} \bmod \underline{l})^M$, what we set out to compute. □

Commentary. The strengthening we did in Corollary 9.7 can be "pushed" further, namely to Theorem 9.4, and consequently to Corollary 9.5.

More specifically, the statement of Theorem 9.4 can be altered so that we have for any finite subset of $\mathbb{N}$, denote it as $F = \{r_0, \ldots, r_n\}$, that $(M, <^M, S^M, (\text{mod } \underline{r_0})^M, \ldots, (\text{mod}\underline{r_n})^M)$ is isomorphic to $(\mathbb{N} \cup A \times \mathbb{Z}, <', S', \text{mod}'_0, \ldots, \text{mod}'_n)$. We define $<'$ and S' exactly as in Theorem 9.4. As for the mod'_i,for $i \in [0, n]$, we define it in the following manner.

- If $x \in\ N$, then $x \bmod {}'_i = x \bmod {}^{\mathbb{N}} r_i$.
- If $x = (q, l) \in A \times \mathbb{Z}$ and $0 \leq l$, then $x \bmod {}'_i = l \bmod {}^{\mathbb{N}} r_i$.
- If $x = (q, l) \in A \times \mathbb{Z}$ and $l < 0$, then $x \bmod {}'_i = (r_i - ((-l) \bmod {}^{\mathbb{N}} r_i)) \bmod {}^{\mathbb{N}} r_i$.

Note that the definition is analogous to the one for mod$'$ in Theorem 9.4.

The proof of this strengthening is similar to the proof of the original statement. There are two differences, though, worth mentioning.

One is that $s(q)$, for $q \in A$, will now have to satisfy, besides $s(q) \in q$, that for any $i \in [n]$, $M \models s(q) \bmod \underline{r_i} = 0$. Actually, by Observation 9.1, it does suffice if $s(q)$ satisfies that $M \models s(q) \bmod \underline{\Pi_{k \in F \setminus \{0\}} k} = 0$ or $M \models s(q) \bmod \underline{c} = 0$, where c

is least common multiple in $F\backslash\{0\}$. As for the existence of such a $(s(q) =)\, x \in q$, we can again use Observation 9.3.

And the second is that when arguing about h preserving mod_i', for $i \in [n]$, we will now need to use Observation 9.1 in its general form when $l \mid k$, where l, k are from the statement of Observation 9.1, compared to the proof of Theorem 9.4 where we used the observation only with $l = k$.

Commentary. Elaborating on the idea in the preceding commentary and with our knowledge of how to use Theorem 9.4 to proof Lemma 9.6, it is not that hard to see the following for any $F \subseteq \mathbb{N}$.

Assume that there exists M, a non-standard countable model of PA, or $I\Sigma_1$, s.t. $\forall q \in A$, where A is defined as in Theorem 9.4, we can find $s(q)$ s.t. the following holds.

- $s(q) \in q$.
- $M \models s(q) \bmod \underline{r} = 0$, for every $r \in F$.

Then there exists G, a non-standard model of PA, or $I\Sigma_1$, s.t.

- $dom(G) = \mathbb{N}$.
- $<$ and S are recursive with respect to G.
- For every $r \in F$ is $\text{mod}\underline{r}$ recursive with respect to G.

Commentary. And now, a natural question arises. Does every copy of $\mathbb{Z}$ in some non-standard countable model of PA contain an element that is divisible by every standard number?

More formally, does it hold that in some countable non-standard model of PA, or $I\Sigma_1$, we have $\forall q \in A$, where A is defined as usual, that there exists $x \in q$ s.t. $M \models x \bmod \underline{m} = 0$ for every $m \in \mathbb{N}$?

If so, then in the light of the previous commentary, there is a non-standard model of PA, or $I\Sigma_1$, s.t.

- its domain is $\mathbb{N}$,
- $<$, S and $\text{mod}\underline{m}$, for every $m \in \mathbb{N}$, is recursive with respect to it.

Unfortunately, it is not that easy, since as we will see in Section 10.1, for every non-standard model M of PA there exists $q \in A$ s.t. no element x from q satisfies for every $m \in \mathbb{N}$ that $M \models x \bmod \underline{2^m} = 0$.

We would like to conclude this section with one general problem concerning the $x \bmod \underline{k}$ function that we did not manage to solve fully.

Problem 1 (Classification of when can be $\text{mod}\underline{k}$, for all $k \in F \subseteq \mathbb{N}$, recursive)**.** Classify exactly for which sets $F \subseteq \mathbb{N}$ there exists a non-standard model of PA, or $I\Sigma_1$, with domain $\mathbb{N}$ s.t. $\text{mod}\underline{k}$, for every $k \in F$, is recursive with respect to it.

We have seen some valid examples of F, namely that any finite subset of $\mathbb{N}$ is valid with respect to Problem 1. However, there are still many other subsets of $\mathbb{N}$ to which we do not know the answer, with respect to Problem 1.

9.2 Recursiveness of the $x \bmod y$ function

An interesting piece of the puzzle left unanswered is whether there can be a non-standard model of $I\Sigma_1$ or PA, s.t. the binary function $x \bmod y$ is recursive with respect to it.

Unfortunately, we did not manage to come to a conclusion on this matter, and therefore, we state is as an unanswered problem.

Problem 2 (Can $x \bmod y$ be recursive?)**.** Does there exist a non-standard model of PA, or $I\Sigma_1$, s.t. the binary function $x \bmod y$ is recursive with respect to it?

A natural idea is whether when we make the assumption stronger, i.e. when we want also $<$ or $S(x)$ to be recursive, we can give an answer to the aforementioned question.

As we have seen in Observation 8.4, there can be no such non-standard model of $I\Sigma_1$ in the case of $x \bmod y$ and $S(x)$.

And, as for the combination of $x \bmod y$ and $<$, we will see in Observation 9.9 that it is the same as asking whether the $x \bmod y$ can be recursive without the additional assumption of $<$ being recursive.

Observation 9.8 ($x \bmod y$ determines $<$)**.** Let $M \models I\Sigma_1$, then $\forall a, b \in M$ s.t. $b \neq 0^M$ the following holds.

$$M \models a < b \iff M \models a \bmod b = a.$$

Proof. If $M \models a < b$, then $M \models a = 0 \times b + a \wedge a < b$ where $b \neq 0^M$ and $M \models 0 \leq a$, hence by the definition of mod we have $M \models a \bmod b = a$.

On the other hand, if $M \models a \bmod b = a$, then since $0^M \neq b$ we have that $M \models a < b$ again by the definition of mod. □

Observation 9.9 ($x \bmod y$ recursive implies $<$ recursive)**.** Let $M \models I\Sigma_1$, then if $x \bmod y$ is recursive with respect to M, then $<$ is also recursive with respect to M.

Proof. Let $a, b \in M$ and we want to compute $a <^M b$.

First we check whether or not $a =^M b$, which can be done recursively by Remark 8.1. If so, then we return that it is not the case of $a <^M b$.

Otherwise assume that it is not the case of $a =^M b$. Therefore, we have $M \models a < b \vee b < a$.

Let us now realize that we can determine whether $b = 0^M$ or not.

It is because 0^M is clearly the only element $x \in M$ s.t. $M \models x \bmod x = x$. And hence, we can enumerate recursively $\mathbb{N}$ according to $<^{\mathbb{N}}$ and when we, sooner or later, stumble upon x s.t. $M \models x \bmod x = x$ we know that $x = 0^M$. And since we can compute 0^M we can check whether $b = 0^M$ or not.

If $b = 0^M$, then it must indeed be the case of $M \models b < a$ and we return that $a <^M b$ does not hold.

Otherwise we have that $b \neq 0^M$ and therefore we can employ Observation 9.8 to check whether $a <^M b$ by checking whether $a \bmod {}^M b = a$ or not. And since is $\bmod^M$ recursive, we can do also this step recursively, and we can conclude that $<^M$ is computable. □

10. Structure of $(M, x \operatorname{div} \underline{k})$ for $M \models PA$

10.1 A copy of $\mathbb{Z}$ with no 0

The argument in this section was inspired by Jeřábek [2015].

Recall that if $G \models PA^-$ and $x \in G$, then

$$x_{\mathbb{Z}} = \{\dots, (x \dot{-} \underline{n})^G, \dots, (x \dot{-} 1)^G, x, (x+1)^G, \dots, (x+\underline{n})^G, \dots\}.$$

Let $k \in \mathbb{N}$ s.t. $2 \leq k$. The ultimate goal of this section is to show that for any non-standard model of PA, denote it as M, there exists $x \in M$ s.t. $\forall y \in x_{\mathbb{Z}}$ there exists $l \in \mathbb{N}$ s.t. $M \models \neg \underline{k^l} \mid y$, or equivalently $M \models y \bmod \underline{k^l} \neq 0$. We can also note that $x_{\mathbb{Z}}$ surely can not equal to $0^M_{\mathbb{Z}}$.

It can be vaguely rephrased as that for any non-standard model of PA there exists a non-standard copy of Z within it s.t. it does not contain a zero-like element from the point of view of divisibility by standard numbers.

Before we reach this result, we will introduce two useful functions that we will call f_k and g_k. And as expected, we will prove a couple of observations with respect to them. The reader may also note, when we reach the main conclusions of this section, that the choice of f_k and g_k is not that important as long they satisfy certain properties introduced in the course of this section.

Definition 10.1 (f_k)**.** Let $k \in \mathbb{N}$ s.t. $2 \leq k$, then we define a unary function over $\mathbb{N}$ denoted as f_k in the following manner. Let $n \in \mathbb{N}$, then define

$$f_k(n) := \begin{cases} n & n \leq 1, \\ f_k(n-1) & 2 \mid n \wedge 2 \leq n, \\ f_k(n-1) + k^{n-1} & \text{otherwise.} \end{cases}$$

The otherwise. condition can be equivalently replaced by $2 \not| n \wedge 2 \leq n$.

Observation 10.1 (f_k is a recursive function)**.** Let $k \in \mathbb{N}$ s.t. $2 \leq k$. Then f_k is a recursive function.

Proof. Obvious by the definition of f_k. □

Observation 10.2 ($f_k(n) < k^n$)**.** Let $k, n \in \mathbb{N}$ s.t. $2 \leq k$. Then $f_k(n) < k^n$.

Proof. Assume that k, n are as in the statement of the observation. The proof is going to be by induction on n.

$n \leq 1$: This case is trivial.

$2 \mid n \wedge 2 \leq n$: We have

$$f_k(n) = f_k(n-1) < k^{n-1} < k^n,$$

where the first equality is by definition of f_k, the first $<$ is by the induction hypothesis and the second $<$ is by $2 \leq k$.

$2 \not| n \wedge 2 \leq n$: We have

$$f_k(n) = f_k(n-1) + k^{n-1} < k^{n-1} + k^{n-1} \leq k^n,$$

where the first equality is by definition of f_k, the first $<$ is by the induction hypothesis and the $\leq$ is by $2 \leq k$.

□

Observation 10.3 (monotousness of f_k)**.** Let $k \in \mathbb{N}$ s.t. $2 \leq k$. Then f_k is a monotone function on $\mathbb{N}$, furthermore, $\forall n \in \mathbb{N}\ f_k(n) < f_k(n+2)$.

Proof. These properties follow directly from the definition of f_k. □

Corollary 10.4 (f_k is unbounded and monotone)**.** Let $k \in \mathbb{N}$ s.t. $2 \leq k$. Then for every $m \in \mathbb{N}$ there exists $n_0 \in \mathbb{N}$ s.t. $\forall n \in \mathbb{N}\ n_0 \leq n \Rightarrow m < f_k(n)$.

Proof. It is an immediate consequence of the just stated Observation 10.3. □

Definition 10.2 (g_k)**.** Let $k \in \mathbb{N}$ s.t. $2 \leq k$. We define a function g_k over $\mathbb{N}$ for every $n \in \mathbb{N}$ as follows,

$$g_k(n) := k^n - f_k(n).$$

Let us note that by Observation 10.2 is g_k indeed a well defined function from $\mathbb{N}$ into $\mathbb{N}$.

Observation 10.5 (monotonousness of g_k)**.** Let $k \in \mathbb{N}$ s.t. $2 \leq k$. Then we have the following,

(i) g_k is monotone.

(ii) $\forall n \in \mathbb{N}\ g_k(n) < g_k(n+2)$.

Proof. Assume $k \in \mathbb{N}$ s.t. $2 \leq k$ and $n \in \mathbb{N}$.

We will start proving the monotony of g_k, i.e. (i), by showing that $g_k(n) \leq g_k(n+1)$. Alongside the proof of monotonousness, we will also show (ii).

$n \leq 1$: Let us note that $g_k(0) = 1$, $g_k(1) = k - 1$, $g_k(2) = k^2 - 1$ and lastly $g_k(3) = k^3 - (1 + k^2) = k^2 \times (k-1) - 1$.

$n = 0$: Clearly, since $2 \leq k$, $g_k(0) \leq g_k(1)$ as well as $g_k(0) < g_k(2)$, i.e. we have verified both (i) and (ii) for $n = 0$.

$n = 1$: Evidently, since $2 \leq k$, $g_k(1) \leq g_k(2)$ as well as $g_k(1) < g_k(3)$, i.e. we have again verified both (i) and (ii) for $n = 1$.

$n \geq 2$:

$2 \mid n$: We have $f_k(n+1) = k^n + f_k(n)$, hence, $g_k(n+1) = k^{n+1} - k^n - f_k(n) = k^n \times (k-1) - f_k(n)$. Since $k \geq 2$, we have that indeed $g_k(n) \leq g_k(n+1)$. I.e. (i) has been verified.

Furthermore, note that $f_k(n+2) = f_k(n+1) = k^n + f_k(n)$. Hence, $g_k(n+2) = k^{n+2} - k^n - f_k(n)$, therefore by $2 \leq k$, we have $g_k(n+1) < g_k(n+2)$ which in turn implies $g_k(n) < g_k(n+2)$. I.e. the (ii) has been verified as well.

$2 \not| n$: We have, by $2 \leq k$, that

$$g_k(n+1) = k^{n+1} - f_k(n+1) = k^{n+1} - f_k(n) > k^n - f_k(n) = g_k(n),$$

which verifies (i).
Continuing, by $2 \leq k$, we have

$$g_k(n+2) = k^{n+2} - f_k(n+2) = k^{n+2} - f_k(n+1) - k^{n+1} = \\ k^{n+1} \times (k-1) - f_k(n+1) = k^{n+1} \times (k-1) - f_k(n)$$

from which we can infer that (ii) holds as well.

□

Observation 10.6 (Congruence for f_k)**.** Let $k \in \mathbb{N}$ s.t. $2 \leq k$. Furthermore, let $n \in \mathbb{N}$, then $\forall l \in \mathbb{N}\ l \leq n$ we have

$$f_k(l) \equiv f_k(n) (\mathrm{mod} k^l).$$

Proof. We will proceed by induction on n.

$n \leq 1$: This case is obvious.

$n = m + 1$: Assume that the lemma holds for m.

- If $2 \mid n$, then $f_k(n) = f_k(m)$. Therefore, we have by induction hypothesis $\forall l \leq m$ that $f_k(l) \equiv f_k(n) (\mathrm{mod} k^l)$.
  Furthermore, if $l = n$, then evidently $f_k(l) \equiv f_k(n) (\mathrm{mod} k^l)$, hence, we have verified the induction step for n s.t. $2 \mid n$.
- If $2 \not| n$, then $f_k(n) = f_k(m) + k^m$.
  Let $l \leq n$.
  If $l = n$, then we evidently have $f_k(l) \equiv f_k(n) (\mathrm{mod} k^l)$.
  Otherwise $l \leq m$. First note that $k^l \mid k^m$, hence $k^m \bmod k^l = 0$. Therefore, by induction hypothesis on m and the just stated congruence, we have that $f_k(l) \equiv f_k(m) + k^m (\mathrm{mod} k^l)$, which is the same as $f_k(l) \equiv f_k(n) (\mathrm{mod} k^l)$.
  Thus, we have verified the induction step also for n s.t. $2 \not| n$.

□

Observation 10.7. Let $M \models I\Sigma_1$, $a \in M$, $n \in \mathbb{N}$ and $S \subseteq \mathbb{N}$ s.t. S is finite. Then there exists $m \in \mathbb{N}$ s.t.

$$\forall s \in S\ \ M \models a + \underline{m} \bmod \underline{s} = \underline{n} \bmod \underline{s}.$$

Proof. First note that if $0 \in S$, then 0 satisfies the conclusion of the observation for any $m \in \mathbb{N}$. Therefore, let us assume for simplicity that $0 \notin S$, since if we find valid m for such a S then we have actually found m for $S \cup \{0\}$.

Set k as the least common multiple of elements in S, and as always, if $S = \emptyset$, then $k = 1$.

Then by Observation 9.3, having the same a and k as in here, there exists $r \in \mathbb{N}$ s.t. $M \models (a + \underline{r}) \bmod \underline{k} = 0$.

Therefore, by Observation 9.1, we get that $M \models (a + \underline{r}) \bmod \underline{s} = 0$ for every $s \in S$.

Hence, we have for every $s \in S$ that $M \models (((a + \underline{r}) \bmod \underline{s}) + \underline{n}) \bmod \underline{s} = \underline{n} \bmod \underline{s}$.

But again by Observation 9.1, Ax.1 [associativity +] we get that for every $s \in S$ we have, $M \models (a + (\underline{r} + \underline{n})) \bmod \underline{s} = \underline{n} \bmod \underline{s}$.

Therefore, by Observation 1.22, we may finally conclude that for every $s \in S$, $M \models (a + \underline{r + n}) \bmod \underline{s} = \underline{n} \bmod \underline{s}$.

And thus, the proof is finished. □

Lemma 10.8. Let $M \models I\Sigma_1$, $a \in M$ and $k \in \mathbb{N}$ s.t. $2 \leq k$. Then $\forall n \in \mathbb{N}$ there exists $m \in \mathbb{N}$ s.t. $\forall l \leq n$ we have

$$M \models (a + \underline{m}) \bmod \underline{k^l} = \underline{f_k(l)} \bmod \underline{k^l}.$$

Proof. Fix some $a \in M$ and $k, n \in \mathbb{N}$ s.t. $2 \leq k$. We will show that there exists a suitable m satisfying the conclusion of the lemma.

First recall that mod behaves on $\mathbb{N}^M$ as expected by Observation 7.5.

By Observation 10.6 there exists $r \in \mathbb{N}$, namely $f_k(n)$, s.t. $M \models \underline{r} \bmod \underline{k^l} = \underline{f_k(l)} \bmod \underline{k^l}$ for any $l \leq n$.

Now we only need to find $m \in \mathbb{N}$ s.t. $M \models (a + \underline{m}) \bmod \underline{k^l} = \underline{r} \bmod \underline{k^l}$, for any $l \leq n$. But now we can refer to Observation 10.7, with

- a set to the same a as in here,
- n in the observation set to the r in here,
- $S := \{k^0, \ldots, k^n\}$,

to argue that there indeed must exist such a m.

The proof is finished. □

Definition 10.3 (Representing f_k)**.** Let $k \in \mathbb{N}$ s.t. $2 \leq k$. We know by Observation 10.1 that f_k is a recursive, and evidently total, function. Hence, by Lemma 3.8, there exists a Σ_1 formula representing f_k in PA^-, denote from now on such a formula as $F_k(x, y)$. Te recall from Definition 3.7, the properties of F_k are the following.

- For any $n \in \mathbb{N}$, we have $PA^- \vdash \exists! y\, F_k(\underline{n}, y)$.
- For any $n, m \in \mathbb{N}$, we have $f_k(n) = m \iff PA^- \vdash F_k(\underline{n}, \underline{m})$.

Definition 10.4 ($\varphi_k(x, y, z)$)**.** Let $k \in \mathbb{N}$ s.t. $2 \leq k$. We will define one formula, denoted as $\varphi_k(x, y, z)$, that will be of use to us later.

$$\varphi_k(x, y, z) \equiv \exists x \leq u \leq y \, \forall l \leq z \, \exists w$$
$$(F_k(l, w) \wedge u \bmod \exp(\underline{k}, l) = w \bmod \exp(\underline{k}, l)).$$

Definition 10.5 (Closed interval of non-standard length)**.** Let $M \models PA^-$ and $a, b \in M$, then we define a *closed interval* $[a, b]$ as $\{z \in M | M \models a \leq z \leq b\}$. Furthermore, if $\forall n \in \mathbb{N}$ we have $M \models a + \underline{n} \leq b$, then we say that $[a, b]$ is a *closed interval of non-standard length*.

Lemma 10.9. Let $M \models PA$, $a, b \in M$ s.t. $[a, b]$ is a *closed interval of non-standard length.* Furthermore, let $k \in \mathbb{N}$ s.t. $2 \leq k$. Then $M \models \varphi_k(a, b, \underline{n})$ for every $n \in \mathbb{N}$.

Proof. Let $n \in \mathbb{N}$.

By Lemma 10.8 there exists $m \in \mathbb{N}$ s.t. $\forall l \leq n\ M \models a + \underline{m} \equiv \underline{f_k(l)}(\text{mod}\ \exp(\underline{k}, \underline{l}))$. And it does suffice to consider only $l \leq n$, since by Observation 1.31 $M \models z \leq \underline{n} \rightarrow z = \underline{0} \vee \ldots \vee z = \underline{n}$.

Furthermore, $M \models a \leq a + \underline{m} \leq b$ evidently holds.

Therefore, we may conclude that $M \models \varphi_k(a, b, \underline{n})$ by setting u to $(a + \underline{m})^M$, and the proof is finished. □

Corollary 10.10 (Non-standard $d \in M$ s.t. $M \models \varphi_k(a, b, d)$)**.** Let $k \in \mathbb{N}$ s.t. $2 \leq k$ and let M be a non-standard model of PA. Furthermore, let $a, b \in M$ s.t. $[a, b]$ is a *closed interval of non-standard length.* Then there exists a non-standard $d \in M$ s.t. $M \models \varphi_k(a, b, d)$.

Proof. This is a simple corollary to the just proved Lemma 10.9 and to Overspill lemma for $\mathbb{N}$, see Lemma 2.6. □

Definition 10.6 (A meta formula $D_k^M(x)$, $D_k(x)$.)**.** Let $M \models PA^-$ and $k \in \mathbb{N}$, then we will denote by $D_k^M(x)$ a meta formula of a single free variable x s.t. x will be always considered from from $dom(M)$. We define the formula in the following way.

$$D_k^M(x) \equiv \forall l \in \mathbb{N}\ M \models \underline{k^l} \mid x.$$

Furthermore, if it obvious to which M we refer to, then we will denote $D_k^M(x)$ simply as $D_k(x)$.

In order to proceed further, we prove one natural property of mod.

Observation 10.11 ($M \models (a \dot{-} c) \bmod d = (b \dot{-} c) \bmod d$, for $M \models a \bmod d = b \bmod d$)**.** Let $M \models I\Sigma_1$ and $a, b, c, d \in M$ s.t. $M \models c \leq a, b$. Furthermore, assume that $M \models a \bmod d = b \bmod d$. Then, we have that $M \models (a \dot{-} c) \bmod d = (b \dot{-} c) \bmod d$.

Proof. First assume that $M \models d = 0$, then the observation trivially holds.

Otherwise assume $M \models 1 \leq d$, hence, $M \models d = z + 1$ for some $z \in M$.

We have,

$$\begin{gathered} M \models (a \dot{-} c) \bmod d = \\ ((a \dot{-} c) + d \times c) \bmod d = \\ (a + (d \times c \dot{-} c)) \bmod d = \\ (a + ((z+1) \times c \dot{-} c) \bmod d = \\ (a + (((z \times c + c) \dot{-} c) \bmod d = \\ (a + ((z \times c + (c \dot{-} c)) \bmod d = \\ (a + z \times c) \bmod d = \\ (b + z \times c) \bmod d = \\ \vdots \\ (b \dot{-} c) \bmod d \end{gathered}$$

Where the respective equality signs are discussed in the upcoming points.

(i) Follows by Observation 9.1.

(ii) Follows by Observation 1.27, since $M \models c \leq a$ and $M \models c \leq d \times c$.

(iii) By $M \models d = z + 1$.

(iv) By Ax.4 [commutativity $\times$] and Ax.5 [distributivity] .

(v) Follows by Observation 1.23.

(vi) Obviously $M \models c \dot{-} c = 0$, and the equality follows.

(vii) By the assumption of $M \models a \bmod d = b \bmod d$ and Observation 9.1.

(viii) We would do the same steps in a reverse order to reach the last expression.

□

Lemma 10.12 (A copy of $\mathbb{Z}$ with no 0, under the assumption of $M \models \varphi_k(a, b, d)$)**.** Let $M \models PA$, $a, b \in M$, $[a, b]$ is a *closed interval of non-standard length* and $k \in \mathbb{N}$ s.t. $2 \leq k$. Furthermore, assume that there is $d \in M \backslash \mathbb{N}^M$ s.t. $M \models \varphi_k(a, b, d)$.

Moreover, set $e \in M$ to be one of the possible interpretations of u witnessing $M \models \varphi_k(a, b, d)$, i.e. the u from

$$\exists x \leq u \leq y \forall l \leq z, \exists w \ (F_k(l, w) \wedge u \bmod \exp(\underline{k}, l) = w \bmod \exp(\underline{k}, l)).$$

Then, we claim the following.

(i) $\forall x \in e_{\mathbb{Z}} \ \neg D_k(x)$.

(ii) e is a non-standard element of M.

Proof. First, let us note that (i) implies (ii).

Assume for contradiction that $e \in \mathbb{N}^M$, then from Corollary 6.3 follows that $0^M \in e_{\mathbb{Z}}$, hence, $\exists x \in e_{\mathbb{Z}}$ such that $D_k(x)$ holds, which is the desired contradiction.

Point (ii) out of the way, we move to proving (i).

Assume for contradiction that (i) does not hold. Therefore, $\exists x \in e_{\mathbb{Z}}$ s.t.

$$\forall l \in \mathbb{N} \ M \models \underline{k^l} \mid x.$$

$M \models x \leq e$: There must exist $r \in \mathbb{N}$ s.t. $M \models x = e \dot{-} \underline{r}$. Furthermore, let r be the smallest one with such a property, hence, $M \models \underline{r} \leq e$.

By Corollary 10.4, setting m to r from here, there exists $n \in \mathbb{N}$ s.t. $r < f_k(n)$. By Observation 1.29 we also have $M \models \underline{r} < \underline{f_k(n)}$.

By the way we chose e we have that and by properties of exp from Observation 2.10,

$$M \models e \bmod \underline{k^n} = \underline{f_k(n)} \bmod \underline{k^n}.$$

Furthermore, since $M \models \underline{r} \leq e$ and $M \models \underline{r} \leq \underline{f_k(n)}$, by Lemma 10.12 can be conclude that

$$M \models (e \dot{-} \underline{r}) \bmod \underline{k^n} = (\underline{f_k(n)} \dot{-} \underline{r}) \bmod \underline{k^n}.$$

We have by $r \leq f_k(n)$, Observation 1.25 and Observation 7.5 that

$$M \models (\underline{f_k(n)} \dot{-} \underline{r}) \text{ mod } \underline{k^n} = \underline{(f_k(n) - r) \text{ mod } k^n}.$$

We know that $r < f_k(n) < k^n$, the last $<$ is by Observation 10.2. Hence, $0 < (f_k(n)-r) \text{ mod } k^n < k^n$ from which follows that $M \models (e \dot{-} \underline{r}) \text{ mod } \underline{k^n} \neq 0$, where recall that $M \models x = e \dot{-} \underline{r}$.

Hence, we can not evidently have that $M \models \underline{k^n} \mid x$, which is a contradiction to our assumption.

$M \models e \leq x$: In this case, we will mimic the proof given for $M \models x \leq e$.

There again exists $r \in \mathbb{N}$ s.t. $M \models x = e + \underline{r}$.

Furthermore, by Observation 10.5 there must be $1 \leq n \in \mathbb{N}$ s.t. $r < g_k(n)$, which is the same as $r < k^n - f_k(n)$.

Again, by the way we chose e and properties of exp from Observation 2.10, we have that

$$M \models e \text{ mod } \underline{k^n} = \underline{f_k(n)} \text{ mod } \underline{k^n}.$$

Hence, by Observation 9.1, we have that

$$M \models e + \underline{r} \text{ mod } \underline{k^n} = \underline{f_k(n)} + \underline{r} \text{ mod } \underline{k^n}.$$

We know that $0 < r + f_k(n) < k^n$, where the first $<$ is by $1 \leq n$ and Observation 10.3.

Hence, we have by Observation 1.22 and Observation 7.5 the following,

$$M \models \underline{f_k(n)} + \underline{r} \text{ mod } \underline{k^n} = \underline{(f_k(n) + r) \text{ mod } k^n} \neq 0$$

Since $M \models x = e + \underline{r}$ and we evidently have that $M \not\models k^n \mid e + \underline{r}$, we again arrive at a contradiction.

□

Corollary 10.13 (A copy of $\mathbb{Z}$ with no 0)**.** Let $M \models PA$, $a, b \in M$ s.t. $[a, b]$ is a *closed interval of non-standard length*. Also let $2 \leq k \in \mathbb{N}$. Then there exists $e \in [a, b]$ s.t. $e \in M \backslash \mathbb{N}^M$ and $\forall x \in e_{\mathbb{Z}}$ the formula $D_k(x)$ does not hold.

Proof. Is a consequence of Lemma 10.12. □

10.2 Investigation of an equivalence relation $\sim_k$

Observation 10.14 (x div $(y \times z)$ equals $(x$ div $y)$ div z)**.** Let $M \models I\Sigma_1$ and $a, b \in M$. Then if x is any member of M we have,

$$M \models x \text{ div } (a \times b) = (x \text{ div } a) \text{ div } b.$$

Proof. First assume that $a = 0^M$ or $b = 0^M$, then $M \models x \text{ div } (a \times b) = 0$ and $M \models (x \text{ div } a) \text{ div } b = 0$, where both observation follow by the definition of div.

From now on, assume that $M \models 0 < a \wedge 0 < b$. Moreover, note that as a direct consequence of our assumption we get $M \models 0 < a \times b$.

By Theorem 2.4, i.e. the theorem on *unique* quotients and remainders, we have the following.

(i) There exists unique $q_{ab}, r_{ab} \in M$ s.t.

$$M \models x = q_{ab} \times (a \times b) + r_{ab} \wedge r_{ab} < a \times b.$$

(ii) There exists unique $q_a, r_a \in M$ s.t.

$$M \models x = q_a \times a + r_a \wedge r_a < a.$$

(iii) There exists unique $q_b, r_b \in M$ s.t.

$$M \models q_a = q_b \times b + r_b \wedge r_b < b.$$

By Corollary 7.2 we see that

$$M \models x \text{ div } (a \times b) = q_{ab} \wedge (x \text{ div } a) \text{ div } b = q_b.$$

I.e. it only remains to show that $q_{ab} = q_b$.

Combining (ii) and (iii) we observe that,

$$M \models x = q_b \times (a \times b) + r_b \times a + r_a.$$

If we manage to show that $M \models r_b \times a + r_a < a \times b$, and since $M \models 0 < a \times b$, then by the *uniqueness* part in Theorem 2.4 the equality $q_{ab} = q_b$ will follow.

Since $M \models 0 < b$, we have that there must be $z \in M$ s.t. $M \models b = z + 1$.

And because $M \models r_a < 1 \times a$, it is evident that it only remains to show that $M \models r_b \times a \leq z \times a$.

But since $M \models r_b < b$, it follows that $M \models r_b \leq z$, and hence, we indeed have $M \models r_b \times a \leq z \times a$ and the proof is finished.

□

Corollary 10.15. Let $M \models I\Sigma_1$ and $k, l \in N$. Then if x is any member of M we have,

$$M \models x \text{ div } \underline{k}^l = (\ldots(x \text{ div } \underline{k})\ldots) \text{ div } \underline{k}.$$

Where the div $\underline{k}$ is repeated on the right hand side of the equation exactly l times. And if $l = 0$, then the right hand side expression stands for x.

Proof. The proof is by induction on l. If $l \leq 1$, then everything is in order. Otherwise we can use the induction hypothesis together with Observation 10.14.

□

Observation 10.16. Let $M \models I\Sigma_1$, $a \in M$ and $1 \leq \in \mathbb{N}$. Then there exists $s \in \mathbb{N}$ s.t.

$$M \models \underline{k} \times (a \text{ div } \underline{k}) + \underline{s} = a.$$

Proof. Let a and k be as in the statement of the observation.

We know by Theorem 2.4 that there exists unique $q_a, r_a \in M$ s.t. $M \models a = \underline{k} \times q_a + r_a \wedge r_a < \underline{k}$. And by Corollary 7.2 we know that $M \models a \text{ div } \underline{k} = q_a$.

Therefore, $M \models \underline{k} \times (a \text{ div } \underline{k}) + r_a = a$.

By Observation 1.31 and $M \models r_a < \underline{k}$ we know that $r_a \in \mathbb{N}^M$, hence, the proof is finished. ☐

Definition 10.7 (Relation $\sim_k$)**.** Let $2 \leq k$ and $M \models I\Sigma_1$, we will denote by $\sim_k$ a relation on $dom(M)$ which is defined as follows. Let $x, y \in M$, then

$$x \sim_k y \iff \exists l_x, l_y \in \mathbb{N};\ M \models x \text{ div } \underline{k^{l_x}} = y \text{ div } \underline{k^{l_y}}.$$

In proofs to come, we will (often) use $\sim$ instead of longer $\sim_k$.

Note that in the light of Corollary 10.15 we also have $x \sim_k y$ iff. there $\exists l_x, l_y \in \mathbb{N}$ s.t. $(\text{div}\underline{k})^M$ applied l_x-times to x equals $(\text{div}\underline{k})^M$ applied l_y-times to y.

Furthermore, we will not use some kind of notation hinting that $\sim_k$ is with respect to M since that should be always obvious.

Later, we will see why $\sim_k$ is a relation of interest for us. However first, we show that $\sim_k$ is a equivalence relation.

Observation 10.17 ($\sim_k$ is an equivalence relation)**.** Let $2 \leq k$ and $M \models I\Sigma_1$, then $\sim_k$ is an equivalence relation.

Proof. reflexivity: Obvious by setting l_x, l_y to 0.

symmetry: Obvious by the symmetry of Definition 10.7.

transitivity: Let $x, y, z \in M$ s.t. $x \sim y$ and $y \sim z$. There must exist $l_x, l_y, r_y, r_z \in \mathbb{N}$ s.t. $M \models x \text{ div } \underline{k^{l_x}} = y \text{ div } \underline{k^{l_y}}$ and $M \models y \text{ div } \underline{k^{r_y}} = z \text{ div } \underline{k^{r_z}}$.

$l_y = r_y$: In this case, we are obviously done.

$l_y < r_y$: Since $M \models x \text{ div } \underline{k^{l_x}} = y \text{ div } \underline{k^{l_y}}$, we have by Corollary 10.15 that $M \models x \text{ div } \underline{k^{l_x+(r_y-l_y)}} = y \text{ div } \underline{k^{l_y+(r_y-l_y)}}$, note that $l_y + (r_y - l_y) = r_y$. Therefore, $M \models x \text{ div } \underline{k^{l_x+(r_y-l_y)}} = z \text{ div } \underline{k^{r_z}}$ which is what we wanted to show

$l_y > r_y$: We can examine this case analogously to the case of $l_y < r_y$.

☐

Observation 10.18 ($[0^M]_{\sim_k} = \mathbb{N}^M$)**.** Let $M \models I\Sigma_1$ and $2 \leq k \in \mathbb{N}$, then $[0^M]_{\sim_k} = \mathbb{N}^M$.

Proof. We will show the two inclusions separately.

$[0^M]_\sim \subseteq \mathbb{N}^M$ Let $x \in [0^M]_\sim$, then there exists $l_x, l_0 \in \mathbb{N}$ s.t. $M \models x \text{ div } \underline{k^{l_x}} = 0 \text{ div } \underline{k^{l_0}}$. By the definition of div we evidently have that $M \models 0 \text{ div } \underline{k^{l_0}} = 0$. Therefore, $M \models x \text{ div } \underline{k^{l_x}} = 0$.

By Observation 10.16 we know that there exists $s \in \mathbb{N}$ s.t. $M \models \underline{k^{l_x}} \times (x \text{ div } \underline{k^{l_x}}) + \underline{s} = x$, since $M \models x \text{ div } \underline{k^{l_x}} = 0$, we may conclude that $M \models \underline{s} = x$, and therefore, $x \in \mathbb{N}^M$.

$\mathbb{N}^M \subseteq [0^M]_\sim$ Let $x \in \mathbb{N}^M$, then there exists $s \in \mathbb{N}$ s.t. $M \models x = \underline{s}$. There must evidently exists $l_x \in \mathbb{N}$ s.t. $s \operatorname{div} k^{l_x} = 0$, therefore by Observation 7.6, $M \models \underline{s} \operatorname{div} \underline{k^{l_x}} = 0$. Therefore, $M \models x \operatorname{div} \underline{k^{l_x}} = 0 \operatorname{div} \underline{k^1}$, and we can conclude that indeed $x \in [0^M]_\sim$.

□

After examining $[0^M]_{\sim_k}$, we will focus more on the other equivalence classes of $\sim_k$. We will differentiate among them from the point of view of elements satisfying $D_k(x)$, see Definition 10.6.

But before that, one useful observation.

Observation 10.19. Let $M \models PA^-$, $x, y, a, b \in M$ and $M \models y = x + b$. Then if $M \models a \mid y$ and $M \models a \mid x$, then $M \models a \mid b$.

Proof. Assume that indeed $M \models a \mid y$ and $M \models a \mid x$. Then, there must exist $q_y, q_x \in M$ s.t. $M \models y = a \times q_y$ and $M \models x = a \times q_x$.

Therefore, $M \models a \times q_y = a \times q_x + b$. Evidently $M \models q_x \leq q_y$. Hence, there exists $z \in M$ s.t. $M \models q_y = q_x + z$. Therefore, $M \models a \times q_x + a \times z = a \times q_x + b$.

We can conclude that $M \models a \times z = b$ which is equivalent to $M \models a \mid b$, and the proof is finished. □

Observation 10.20. Let $2 \leq k \in \mathbb{N}$, $M \models PA^-$ and $e \in M$. Then there exists at most one $x \in e_\mathbb{Z}$ s.t. $D_k(x)$ holds.

Proof. Assume for contradiction that there exist $x, y \in e_\mathbb{Z}$, where WLOG also assume that $M \models x \leq y$, s.t. $D_k(x)$ and $D_k(y)$ hold.

Since $x, y \in e_\mathbb{Z}$, by Definition 6.1, we know that there must exist $s \in \mathbb{N}$ s.t. $M \models x + \underline{s} = y$.

And by Observation 10.19 we see that $D_k(\underline{s}^M)$ must hold, which obviously can not by Observation 1.32, and the proof by contradiction is finished. □

Definition 10.8 (d_+ and d_-)**.** Let $M \models PA^-$ and $d \in M$, then we define d_+ as $\{(d + k)^M | k \in \mathbb{N}^M\}$ and we define d_- as $\{(d \dot{-} k)^M | k \in \mathbb{N}^M \wedge k \neq 0^M\}$.

Observation 10.21. Let $M \models I\Sigma_1$, $x \in M$ and $k \in \mathbb{N}$. Then $M \models x \operatorname{div} \underline{k} = (x + 1) \operatorname{div} \underline{k}$ or $M \models (x \operatorname{div} \underline{k}) + 1 = (x + 1) \operatorname{div} \underline{k}$

Proof. If $k = 0$, then the result obviously holds. Otherwise assume $1 \leq k$. Also denote $(x + 1)^M$ as y.

By Theorem 2.4 there exist $q_x, q_y, r_x, r_y \in M$ s.t. $M \models x = \underline{k} \times q_x + r_x \wedge r_x < \underline{k}$ and $M \models y = \underline{k} \times q_y + r_y \wedge r_y < \underline{k}$.

Moreover, by Corollary 7.2 we know that $M \models x \operatorname{div} \underline{k} = q_x$ and $M \models y \operatorname{div} \underline{k} = q_y$.

If $q_x = q_y$, then we are done.

Otherwise, we must have $M \models q_x < q_y$. And since $M \models 1 \leq \underline{k}$, then the case of $M \models q_x + 1 < q_y$ can not happen. Therefore, $M \models q_y = q_x + 1$ and the proof is finished. □

Observation 10.22. Let $2 \leq k \in \mathbb{N}$, $M \models I\Sigma_1$ and $x \in M$. Furthermore assume that $D_k(x + 1)$ holds. Then,

(i) $\forall l \in \mathbb{N}$ we have $D_k((x \operatorname{div} \underline{k^l} + 1)^M)$ and

(ii) $\forall l \in \mathbb{N}$ we have $\neg D_k((x \text{ div } \underline{k}^l)^M)$.

Proof. First note that (ii) follows from (i), otherwise would be, by Observation 10.19, 1^M divisible in M by $\underline{k}^{l^M}$ for any $l \in \mathbb{N}$.

So it does suffice to show only (i).

If $l = 0$, then the conclusion evidently holds. Otherwise, thanks to Corollary 10.15, it does suffice to show that if $D_k((y+1)^M)$ holds, then $D_k(((y \text{ div } \underline{k})+1)^M)$ holds.

We know by Observation 10.21 that either $M \models (y \text{ div } \underline{k})+1 = (y+1) \text{ div } \underline{k}$ or $M \models (y \text{ div } \underline{k}) = (y+1) \text{ div } \underline{k}$ In the former case, $D_k(((y+1) \text{ div } \underline{k})^M)$ obviously holds by our assumption of $D_k((y+1)^M)$ being true.

Assume for contradiction that the latter case holds, let $q \in M$ s.t. $M \models q = (y \text{ div } \underline{k}) = (y+1) \text{ div } \underline{k}$. Then by Corollary 7.2 and the fact that $M \models \underline{k} \mid (y+1)$, $M \models (y+1) = q \times \underline{k}$ whereas again by Corollary 7.2 and the fact that $D_k(y)$ evidently can not hold, we get that $M \models y = q \times \underline{k} + r \wedge r \neq 0$ for some $r \in M$. Therefore, $M \models (y+1) < y$ which is a contradiction. □

Observation 10.23. Let $2 \leq k \in \mathbb{N}$, $M \models I\Sigma_1$ and e be a non-standard element of M. Then the following holds.

(i) If $\forall x \in e_{\mathbb{Z}}\ \neg D_k(x)$, then $e_{\mathbb{Z}} \subseteq [e]_{\sim_k}$.

(ii) If $\exists d \in e_{\mathbb{Z}}$ s.t. $D_k(d)$ holds, then we have the following.

  (a) $d_+ \subseteq [d]_{\sim_k}$.

  (b) $d_- \subseteq [(d \dot{-} 1)^M]_{\sim_k}$.

  (c) Furthermore, $[d]_{\sim_k} \cap [(d \dot{-} 1)^M]_{\sim_k} = \emptyset$.

Let us note that options (i) and (ii) for $e_{\mathbb{Z}}$ are evidently non-overlapping and by Observation 10.20 are also exhaustive.

Proof. We will prove the respective cases as are stated in the statement of the observation.

(i) It clearly does suffice to show that if $x \in e_{\mathbb{Z}}$, then $x \sim (x+1)^M$. For further discussion, denote $(x+1)^M$ as y.

By Theorem 2.4 there exist $q_x, q_y, r_x, r_y \in M$ s.t. $M \models x = \underline{k} \times q_x + r_x \wedge r_x < \underline{k}$ and $M \models y = \underline{k} \times q_y + r_y \wedge r_y < \underline{k}$.

Moreover, by Corollary 7.2 we know that $M \models x \text{ div } \underline{k} = q_x$ and $M \models y \text{ div } \underline{k} = q_y$.

If $q_x = q_y$, then we are clearly done.

Otherwise assume that $q_x \neq q_y$, then since $M \models y = x + 1$, we must have $M \models r_y = 0$.

Let $l \in \mathbb{N}$ be the maximum natural number, by our assumption is l well defined, s.t. $M \models \underline{k}^l \mid y$.

By Observation 10.21, we see that $M \models x \text{ div } \underline{k}^l = y \text{ div } \underline{k}^l$, in that case we are done, or $M \models (x \text{ div } \underline{k}^l) + 1 = y \text{ div } \underline{k}^l$.

In the latter case, we must again have that there exists $q, r \in M$, by Theorem 2.4, s.t. $M \models y \text{ div } \underline{k^l} = \underline{k} \times q + r \wedge r < \underline{k}$.

But this time, thanks to the maximality of l, we must have $M \models r \neq 0$. Therefore, we may apply the same argument as the one we just did for x, y but now for $x \text{ div } \underline{k^l}$ and $y \text{ div } \underline{k^l}$ and importantly without the possibility of $M \models r = 0$.

(ii) (a) It again does suffice to show that if $x \in d_+$, then $x \sim (x+1)^M$, where we will denote $(x+1)^M$ as y.

First assume that $x = d$, then since $M \models \underline{k} \mid d$, then evidently $M \models x \text{ div } \underline{k} = (x+1) \text{ div } \underline{k}$.

Otherwise, i.e. $x \neq d$, use the same argument as in (i).

(b) Now, it clearly does suffice to show that if $x \in d_-$ and $M \models x \neq d \dot{-} 1$, then $x \sim (x+1)^M$. And the proof is the same as in (i).

(c) Assume for contradiction that $[d]_{\sim_k} \cap [(d \dot{-} 1)^M]_{\sim_k} \neq \emptyset$. Then, $(d \dot{-} 1)^M \sim d^M$, hence, there exists $l_{d-1}, l_d \in \mathbb{N}$ s.t. $M \models (d \dot{-} 1) \text{ div } \underline{k^{l_{d-1}}} = d \text{ div } \underline{k^{l_d}}$.

But this can not be. First note that since $D_k(d)$ holds, $D_k((d \text{ div } \underline{k^{l_d}})^M)$ must hold as well. On the other hand, by (ii) in Observation 10.22 we get that $D_k(((d \dot{-} 1) \text{ div } \underline{k^{l_{d-1}}})^M)$ does not hold. And thus we arrive at a contradiction.

□

We will state a couple of other observations with respect to div.

Observation 10.24 (x div y is monotone with respect to y)**.** Let $M \models I\Sigma_1$ and $x, a, b \in M$. If $M \models 0 < a \leq b$, then $M \models x \text{ div } b \leq x \text{ div } a$.

Proof. The observation is trivial. □

Observation 10.25. Let $M \models I\Sigma_1$ and $a, b, d \in M$. Then $M \models a \text{ div } d + b \text{ div } d \leq (a+b) \text{ div } d$.

Proof. The statement is obvious. □

Observation 10.26 (preservation of $\sim_<$ when applying div$\underline{k}$)**.** Let $M \models PA$, $x \in M \backslash \mathbb{N}^M$ and $y \in x_{\mathbb{Z}}$. Then we have the following.

(i) $\forall k \in \mathbb{N}$, $(\underline{k} \times y)^M \in (\underline{k} \times x)^M_{\mathbb{Z}}$.

(ii) $\forall k \in \mathbb{N}$, $(y \text{ div } \underline{k})^M \in (x \text{ div } \underline{k})^M_{\mathbb{Z}}$.

(iii) $\forall l, k \in \mathbb{N}\ l \neq k$ we have $(\underline{k} \times y)^M \notin (\underline{l} \times x)^M_{\mathbb{Z}}$.

(iv) $\forall l, k \in \mathbb{N}\ l \neq k$ we have $(y \text{ div } \underline{k})^M \notin (x \text{ div } \underline{l})^M_{\mathbb{Z}}$.

Proof. Although the proof is relatively lengthy, it is quite simple, hence we omit it. Moreover, the validity of the observation is hopefully obvious. □

Definition 10.9 (non-standard gap)**.** Let $M \models PA^-$, then for $a, b \in M$ we say that there is a *non-standard gap* between them if $a_{\mathbb{Z}} \cap b_{\mathbb{Z}} = \emptyset$.

Observation 10.27. Let $M \models I\Sigma_1$ and $a, b, c \in M$ s.t. $M \models a < b < c$ and there is a *non-standard gap* among them, see Definition 10.9. Moreover, let $1 \leq k \in \mathbb{N}$.

Then $M \models a \text{ div } \underline{k} < b \text{ div } \underline{k} < c \text{ div } \underline{k}$. And furthermore, there is again *non-standard gap* among them.

Proof. Let $a, b, c \in M$ and $1 \leq k \in \mathbb{N}$ be as in the premise of the observation.

It clearly does suffice to show that $M \models a \text{ div } \underline{k} < b \text{ div } \underline{k}$ and $(a \text{ div } \underline{k})^M_{\mathbb{Z}} \cap (a \text{ div } \underline{k})^M_{\mathbb{Z}} = \emptyset$.

There must exist $e \in M$ s.t. $M \models a + e = b$. Thanks to our assumption, e is a non-standard element of M.

Since $1 \leq k$, we have by Theorem 2.4 that there exists $q_a, r_a, q_b, r_b, q_e, r_e \in M$ s.t. $M \models a = \underline{k} \times q_a + r_a \wedge r_a < \underline{k}$, $M \models b = \underline{k} \times q_b + r_b \wedge r_b < \underline{k}$ and $M \models e = \underline{k} \times q_e + r_e \wedge r_e < \underline{k}$.

And by Corollary 7.2 we know that $M \models a \text{ div } \underline{k} = q_a$ and $M \models b \text{ div } \underline{k} = q_b$ and $M \models e \text{ div } \underline{k} = q_e$.

By Observation 10.25 we note that $M \models q_a + q_e \leq q_b$. Furthermore, since $e \notin \mathbb{N}^M$ we clearly have that q_e must be a non-standard element as well, the conclusion follows. □

Lemma 10.28. Let $M \models I\Sigma_1$, $e \in M \backslash \mathbb{N}^M$ and $2 \leq k \in \mathbb{N}$.

(i) If there exists, by Observation 10.20 unique, $d \in e_{\mathbb{Z}}$ s.t. $D_k(d)$ holds, we observe the following, setting $B \coloneqq \{(d \text{ div } \underline{k^l})^M | l \in \mathbb{N}\} \cup \{(\underline{k^l} \times d)^M | l \in \mathbb{N}\}$.

(a)
$$[d]_{\sim_k} =$$
$$\ldots \cup (d \text{ div } \underline{k})^M_+ \cup d_+ \cup (\underline{k} \times d)^M_+ \cup \ldots =$$
$$\bigcup_{y \in B} y_+.$$

(b)
$$[(d \dot{-} 1)^M]_{\sim_k} =$$
$$\ldots \cup (d \text{ div } \underline{k})^M_- \cup d_- \cup (\underline{k} \times d)^M_- \cup \ldots =$$
$$\bigcup_{y \in B} y_-.$$

(ii) Otherwise, i.e. if there exists no such $d \in e_{\mathbb{Z}}$ s.t. $D_k(d)$ holds, then we have the following, setting $E \coloneqq \{(e \text{ div } \underline{k^l})^M | l \in \mathbb{N}\} \cup \{(\underline{k^l} \times e)^M | l \in \mathbb{N}\}$

$$[e]_{\sim_k} =$$
$$\ldots \cup (e \text{ div } \underline{k})^M_{\mathbb{Z}} \cup e_{\mathbb{Z}} \cup (\underline{k} \times e)^M_{\mathbb{Z}} \cup \ldots =$$
$$\bigcup_{y \in E} y_{\mathbb{Z}}.$$

Where in all the three series of unions, the individual sets that we union together are disjoint.

Proof. Let us state first that the last remark in the statement of the lemma follows by Observation 10.26.

We will now show respective set equalities, where we split each case to showing $\subseteq$ and $\supseteq$.

$[d]_\sim \supseteq \bigcup_{y \in B} y_+$: Evidently, every $y \in B$ satisfies $D_k(y)$, since d does. Therefore, in the light of Observation 10.23, it does suffice to show that $\forall x, y \in B$ we have $x \sim y$, but that is obvious.

$[(d \dot{-} 1)^M]_\sim \supseteq \bigcup_{y \in B} y_-$: Again note that every $y \in B$ satisfies $D_k(y)$.

Thanks to Observation 10.23, it does suffice to show that for any $x, y \in B$ we have $(x \dot{-} 1)^M \sim (y \dot{-} 1)^M$. For that, thanks to Corollary 10.15, it does suffice to show that for any $y \in B$ we have $M \models (y \dot{-} 1) \operatorname{div} \underline{k} = (y \operatorname{div} \underline{k}) \dot{-} 1$.

By Observation 10.21 we have $M \models (y \dot{-} 1) \operatorname{div} \underline{k} = (y \operatorname{div} \underline{k}) \dot{-} 1$ or $M \models (y \dot{-} 1) \operatorname{div} \underline{k} = (y \operatorname{div} \underline{k})$. But since $D_k(d)$ holds, which implies $M \models \underline{k} \mid y$, the latter case evidently can not hold.

$[e]_\sim \supseteq \bigcup_{y \in E} y_\mathbb{Z}$: For any $x, y \in E$, we evidently have that $x \sim y$.

As a consequence of Observation 10.23, it suffices to show that $\forall x \in E$ we have no $d \in x_\mathbb{Z}$ s.t. $D_k(d)$ holds.

Assume for contradiction that there is $x \in E$ s.t. $d \in x_\mathbb{Z}$ and $D_k(d)$ holds. But this can not be because if there is one such d, then by and (i) or (ii) in Observation 10.26, in case (i) would also apply Observation 10.16, there must exist $c \in e_\mathbb{Z}$ s.t. $D_k(c)$ holds, which can not be.

$[d]_\sim \subseteq \bigcup_{y \in B} y_+$: And let us assume for contradiction that there exists $x \in [d]_\sim$ s.t. $x \notin \bigcup_{y \in B} y_+$.

First note that $x \sim d$.

By $x \notin \bigcup_{y \in B} y_+$, we know that $x \notin \bigcup_{y \in B} y_\mathbb{Z}$, because otherwise $x \in \bigcup_{y \in B} y_- \subseteq [(d \dot{-} 1)^M]_\sim$ which would mean that $x \in [d]_\sim \cap [(d \dot{-} 1)^M]_\sim$. And that is not a possibility by (ii) (c) in Observation 10.23.

Therefore, $x \sim d$ and $x \notin \bigcup_{y \in B} y_\mathbb{Z}$. By Observation 10.27, using also Corollary 10.15, it is evident that elements of B are strictly ordered by $<^M$ in an expected way, i.e. $M \models \ldots < d \operatorname{div} \underline{k} < d < \underline{k} \times d < \ldots$, and there are non-standard gaps among them.

First, we observe that there must exist $y \in B$ s.t. $M \models y \operatorname{div} \underline{k} < x < y$. Otherwise, since $x \notin \bigcup_{y \in B} y_\mathbb{Z}$, it would mean that for any $y \in B$ we have $M \models x < y$ or $M \models y < x$ and hence, by Observation 10.27 and Corollary 10.15, $x \sim d$ can not be.

Therefore, we indeed have $y \in B$ s.t. $M \models y \operatorname{div} \underline{k} < x < y$. Now, since $x \sim d$ and evidently $d \sim y$, we have $x \sim y$.

Hence, there exists $l_x, l_y \in \mathbb{N}$ s.t. $M \models x \operatorname{div} \underline{k^{l_x}} = y \operatorname{div} \underline{k^{l_y}}$. Keep also in mind that $x \notin y_\mathbb{Z}$, i.e. there is a non-standard gap among them.

We will see that none of the possibilities $l_x \neq l_y$, $l_x > l_y$ and $l_x < l_y$ can hold, hence, arriving at a contradiction.

By (iv) in Observation 10.26, we have that $l_x \neq l_y$.

Assume that $l_x > l_y$, by Observation 10.27 we know that $M \models x \operatorname{div} \underline{k^{l_y}} < y \operatorname{div} \underline{k^{l_y}}$. And by Observation 10.24 we know that $M \models x \operatorname{div} \underline{k^{l_x}} \leq x \operatorname{div} \underline{k^{l_y}}$. Hence, $M \models x \operatorname{div} \underline{k^{l_x}} \neq y \operatorname{div} \underline{k^{l_y}}$, contrary to the assumption.

Assume that $l_x < l_y$, we have by Observation 10.27 that $M \models (y \text{ div } \underline{k}) \text{ div } \underline{k^{l_x}} < x \text{ div } \underline{k^{l_x}}$. By Observation 10.24, we infer that $M \models (y \text{ div } \underline{k}) \text{ div } \underline{k^{(l_y-1)}} < x \text{ div } \underline{k^{l_x}}$. And finally by Corollary 10.15 we get that $M \models y \text{ div } \underline{k^{(l_y)}} < x \text{ div } \underline{k^{l_x}}$, implying that $M \models y \text{ div } \underline{k^{(l_y)}} \neq x \text{ div } \underline{k^{l_x}}$.

We got that neither of $l_x \neq l_y$, $l_x > l_y$ and $l_x < l_y$ can hold. Therefore, we get a contradiction we wanted.

$[(d \dot{-} 1)^M]_\sim \subseteq \bigcup_{y \in B} y_-$: The proof can be carried out analogously to the one for $[d]_\sim \subseteq \bigcup_{y \in B} y_+$.

$[e]_\sim \subseteq \bigcup_{y \in E} y_\mathbb{Z}$: This proof can be as well carried out similarly to the one for $[d]_\sim \subseteq \bigcup_{y \in B} y_+$.

□

Observation 10.29. Let $M \models I\Sigma_1$, $2 \leq k \in \mathbb{N}$ and $d, e \in M \backslash \mathbb{N}^M$ s.t. $D_k(d)$ holds and $\forall x \in e_\mathbb{Z}$ we have that $D_k(x)$ does not hold. Then the sets $[d]_{\sim_k}$, $[(d \dot{-} 1)^M]_{\sim_k}$ and $[e]_{\sim_k}$ are disjoint.

Proof. Classes $[d]_{\sim_k}$ and $[(d \dot{-} 1)^M]_{\sim_k}$ are disjoint by Observation 10.23.

By $[d]_{\sim_k} \cap [(d \dot{-} 1)^M]_{\sim_k} = \emptyset$ and the structure of those two classes in mention, observed in Lemma 10.28, we know that neither of $[d]_{\sim_k}$ and $[(d \dot{-} 1)^M]_{\sim_k}$ contains $x_\mathbb{Z}$ for some $x \in M$. On the other hand, by Lemma 10.28, we know that $e_\mathbb{Z} \subseteq [e]_\sim$. Hence, $[e]_\sim$ differs from both $[d]_{\sim_k}$ and $[(d \dot{-} 1)^M]_{\sim_k}$. Therefore, we can conclude that $[e]_{\sim_k} \cap [d]_{\sim_k} = \emptyset$ and $[e]_{\sim_k} \cap [(d \dot{-} 1)^M]_{\sim_k} = \emptyset$. □

Observation 10.30. Let $M \models I\Sigma_1$, $2 \leq k \in \mathbb{N}$ and $x \in M \backslash \mathbb{N}^M$. Then exactly one of the following tree things can happen.

(i) $\exists e \in M \backslash \mathbb{N}^M$ s.t. $\forall y \in e_\mathbb{Z}$ the condition $D_k(y)$ does not hold and $x \in [e]_{\sim_k}$.

(ii) $\exists d \in M \backslash \mathbb{N}^M$ s.t. $D_k(d)$ holds and $x \in [d]_{\sim_k}$.

(iii) $\exists d \in M \backslash \mathbb{N}^M$ s.t. $D_k(d)$ holds and $x \in [(d \dot{-} 1)^M]_{\sim_k}$.

Proof. The fact that at most one of (i)-(iii) can happen follows by Observation 10.29.

The fact that at least one of (i)-(iii) can happen is by noting Observation 10.23. □

Lemma 10.31. Let $M \models I\Sigma_1$ and $2 \leq k \in \mathbb{N}$. Define $C^0 := \{[0^M]_{\sim_k}\}$, $C^{D_k} := \{[d]_{\sim_k} | d \in M \backslash \mathbb{N}^M \wedge D_k(d)\}$, $C^{D_k - 1} := \{[(d \dot{-} 1)^M]_{\sim_k} | d \in M \backslash \mathbb{N}^M \wedge D_k(d)\}$ and $C^{\neg D_k} := \{[e]_{\sim_k} | e \in M \backslash \mathbb{N}^M \wedge \forall x \in e_\mathbb{Z} \neg D_k(x)\}$. Then all the four mentioned sets of equivalence classes of $\sim_k$ are disjoint and are exhaustive, meaning that $\{[x]_{\sim_k} | x \in M\} = C^0 \cup C^{D_k} \cup C^{D_k - 1} \cup C^{\neg D_k}$.

Proof. The disjointedness follows by Observation 10.18 and by Observation 10.29. The exhaustiveness follows by Observation 10.18 and by Observation 10.30. □

Let us note that we will use the notation also $C^0, C^{D_k}, C^{D_k - 1}$ and $C^{\neg D_k}$ later in the text. Furthermore, we do not add to the notation something specifying the respective model M since M will be always evident from the context.

This concludes the first part of investigation in the equivalence relation $\sim_k$. In the section to come, we will find cardinalities of C^{D_k}, $C^{D_k - 1}$ and $C^{\neg D_k}$.

10.3 Counting equivalence classes of $\sim_k$

For the end of this section, a basic knowledge of cardinal arithmetic is necessary. For details see e.g. Enderton [1977, Chapter 6].

First, let us state an obvious corollary.

Corollary 10.32. Let $M \models I\Sigma_1$ and $2 \leq k \in \mathbb{N}$, then $|C^{D_k}| = |C^{D_k - 1}|$.

Proof. This is a consequence of Lemma 10.28. □

First, we will inspect $|C^{D_k}|$.

Definition 10.10 (P_k). Let $2 \leq k \in \mathbb{N}$. Then define $P_k \coloneqq \{p(n) | n \in \mathbb{N} \wedge \neg p(n) \mid k\}$.

Observation 10.33. Let $M \models PA$, M be a non-standard model of PA, $e \in M$ and $2 \leq k \in \mathbb{N}$. If moreover p_1, p_2 are distinct members of P_k, then $M \models \neg(\underline{p_2} \mid (\exp(\underline{k}, e) \times \underline{p_1}))$.

Proof. Let everything be as in the statement of the observation. We will prove the conclusion by an induction on e.

$e = 0^M$: Evidently $M \models \exp(\underline{k}, e) \times \underline{p_1} = \underline{p_1}$, e.g. by the first item in Observation 2.11. And since $\neg p_2 \mid p_1$, we get by Observation 1.32 that $M \models \neg\underline{p_2} \mid \underline{p_1}$. Therefore, the case of $e = 0^M$ has been verified.

$e = (d+1)^M$: We have by the first item in Observation 2.10 and the fourth item in Observation 2.11 that $M \models \exp(\underline{k}, e) = \exp(\underline{k}, d) \times \underline{k}$. By the induction hypothesis, we know that $M \models \neg\underline{p_2} \mid (\exp(\underline{k}, d) \times p_1)$ and by the way we have defined P_k, in combination with Observation 1.32, we know that $M \models \neg\underline{p_2} \mid \underline{p_1}$. Therefore, we can conclude by Corollary 2.5 that indeed $M \models \neg(\underline{p_2} \mid (\exp(\underline{k}, e) \times \underline{p_1}))$

□

Lemma 10.34. Let $M \models I\Sigma_1$, M be a non-standard model of PA, $e \in M \backslash \mathbb{N}^M$ and $2 \leq k \in \mathbb{N}$. Then we have for any distinct $p_1, p_2 \in P_k$ that

$$\neg((\exp(\underline{k}, e) \times \underline{p_1})^M \sim_k (\exp(\underline{k}, e) \times \underline{p_2})^M).$$

Proof. If e is a nonstandard element of M, then we have evidently for any $l \in \mathbb{N}$ that $M \models \exp(\underline{k}, e) \operatorname{div} \underline{k}^l = \exp(\underline{k}, e \dot{-} \underline{l})$.

Therefore, we see that indeed $\neg((\exp(\underline{k}, e) \times \underline{p_1})^M \sim_k (\exp(\underline{k}, e) \times \underline{p_2})^M)$, because otherwise would have $M \models \underline{p_2} \mid \exp(\underline{k}, e \dot{-} \underline{l}) \times \underline{p_1}$ for some $l \in \mathbb{N}$ which can not be by Observation 10.33. □

Corollary 10.35 ($|\mathbb{N}| \leq |C^{D_k}|$). Let $M \models PA$, M is non-standard and $2 \leq k \in \mathbb{N}$. Then $|N| \leq |C^{D_k}| = |C^{D_k - 1}|$.

Proof. The equality follows by Corollary 10.32 and the $\leq$ follows by Lemma 10.34. □

Now, we will investigate in some detail the size of $|C^{\neg D_k}|$. But first, we will prove two useful observations related to div.

Observation 10.36. Let $M \models I\Sigma_1$, $e \in M \backslash \mathbb{N}^M$ and $1 \leq n \in \mathbb{N}$. Then there exists $f \in M \backslash \mathbb{N}^M$ s.t. $M \models e \text{ div } \underline{n+1} + f = e \text{ div } \underline{n}$.

Proof. By Theorem 2.4 we know that there exists $q_{n+1}, r_{n+1}, q_n, r_n \in M$ s.t. $M \models e = \underline{n+1} \times q_{n+1} + r_{n+1} \wedge r_{n+1} < \underline{n+1}$ and $M \models e = \underline{n} \times q_n + r_n \wedge r_n < \underline{n}$.

Furthermore, by Corollary 7.2 $M \models e \text{ div } \underline{n+1} = q_{n+1}$ and $M \models e \text{ div } \underline{n} = q_n$.

Since $e \in M \backslash \mathbb{N}^M$, we evidently have that $q_{n+1}, q_n \in M \backslash \mathbb{N}^M$. Therefore, $M \models q_{n+1} < q_n$, hence, there exists $f \in M$ s.t. $M \models q_{n+1} + f = q_n$.

We get $M \models \underline{n} \times f + r_n = q_{n+1} + r_{n+1}$. Since $q_{n+1} \in M \backslash \mathbb{N}^M$ whereas $\underline{n}^M, r_n \in \mathbb{N}^M$, we can conclude that indeed $f \in M \backslash \mathbb{N}^M$. □

Observation 10.37 (x div $\underline{m}$ is monotone for $1 \leq m$)**.** Let $M \models I\Sigma_1$ and $m \in \mathbb{N}$ s.t. $1 \leq m$. Then if $x, y \in M$ s.t. $M \models x \leq y$, then $M \models x \text{ div } \underline{m} \leq y \text{ div } \underline{m}$.

Proof. If $x = y$, then the conclusion evidently holds. Otherwise, we can assume $M \models x < y$.

Since $1 \leq m$, then by Theorem 2.4 there exists $q_x, r_x, q_y, r_y \in M$ s.t. $M \models x = q_x \times \underline{m} + r_x \wedge r_x < \underline{m}$ and $M \models x = q_y \times \underline{m} + r_y \wedge r_y < \underline{m}$.

Furthermore, by Corollary 7.2 we know that $M \models x \text{ div } \underline{m} = q_x$ and $M \models y \text{ div } \underline{m} = q_y$.

Assume for contradiction that $M \models q_y < q_x$.

First note that $M \models q_y + 1 \leq q_x$. Therefore, $M \models x \geq q_y \times \underline{m} + \underline{m} + r_x \wedge r_x < \underline{m}$. Since $M \models r_y < \underline{m}$, then evidently

$$M \models q_y \times \underline{m} + \underline{m} + r_x > q_y \times \underline{m} + r_y = y.$$

Therefore, $M \models x > y$ and we have arrived at a contradiction, the proof is finished.

□

Lemma 10.38. Let $M \models PA$, M is non-standard and $2 \leq k \in \mathbb{N}$. Then there exists $e^0, e^1, \ldots, e^n, \ldots \in M \backslash \mathbb{N}^M$, i.e. for every $n \in \mathbb{N}$ we have e^n, s.t.

(i) $\forall n \in \mathbb{N} \forall x \in e^n_{\mathbb{Z}}$ the $D_k(x)$ does not hold.

(ii) $\forall n \neq m \in \mathbb{N}$ we have that $\neg(e^n \sim_k e^m)$.

(iii) $M \models e^0 < \ldots < e^n < \ldots < e^1 < \underline{2} \times e^0$ for $n \in \mathbb{N}$. Furthermore, there is a *non-standard gap* between any two of them, see Definition 10.9.

Proof. Let d be any non-standard element of M. Then $[d, (2 \times d)^M]$ is evidently an *closed interval of non-standard length*. Therefore, by Corollary 10.13 there exists $e^0 \in [d, (2 \times d)^M]$ s.t. $e^0 \in M \backslash \mathbb{N}^M$ and $\forall x \in e_{\mathbb{Z}}$ the $D_k(x)$ does not hold.

We will now create *closed intervals of non-standard length* $I_1, \ldots, I_n, \ldots$, i.e. we will have for every $1 \leq n \in \mathbb{N}$ a *closed interval of non-standard length* denoted as I_n, s.t. for every $1 \leq n \in \mathbb{N}$

(a) $\forall x \in I_1$ we have $M \models x < 2 \times e^0$ and there is a *non-standard gap* between them.

(b) $\forall x \in I_{n+1} \forall y \in I_n$ we have $M \models x < y$ and there is a *non-standard gap* between them.

(c) $\forall x \in I_n$ we have $M \models e^0 < x$ and there is a *non-standard gap* between them.

I.e. (a),(b) and (c) can be loosely written as "$M \models e^0 < \ldots < I_n < \ldots < I_1 < 2 \times e^0$" s.t. there is a *non-standard gap* between any two expressions delimited by $<$.

For any $1 \leq n \in \mathbb{N}$ define $a_n := (e^0 + e^0 \text{ div } \underline{2 \times n + 1})^M$ and $b_n := (e^0 + e^0 \text{ div } \underline{2 \times n})^M$. And now define $\forall 1 \leq n \in \mathbb{N}$ the set I_n as $[a_n, b_n]$.

Let $1 \leq n \in \mathbb{N}$, we will verify now all the properties of I_n. By Observation 10.36 applied on $2 \times n$ as n we get that there exists $f_n \in M \backslash \mathbb{N}^M$ s.t. $M \models a_n + f_n = b_n$. Therefore, I_n is indeed a *closed intervals of non-standard length*. Furthermore, again by Observation 10.36 with $2 \times n + 1$ as n, we have that there exists $g_n \in M \backslash \mathbb{N}^M$ s.t. $M \models b_{n+1} + g_n = a_n$. So there is indeed a *non-standard gap* between I_{n+1} and I_n, i.e. there are *non-standard gaps* between any two elements of I_{n+1} and I_n, hence verifying (b). Continuing, applying Observation 10.36 to 1 we get that there exists $g_0 \in M \backslash \mathbb{N}^M$ s.t. $M \models b_1 + g_0 = 2 \times e^0$. Therefore (a) holds. Lastly, $(e^0 \text{ div } \underline{2 \times n + 1})^M$ is evidently a non-standard element of M, where by definition $M \models a_n = e^0 + (e^0 \text{ div } \underline{2 \times n + 1})^M$, and thus (c) holds as well.

For every $n \in \mathbb{N}$ apply Corollary 10.13 to I_n to get $e^n \in I_n$ s.t. $\forall x \in e^n_{\mathbb{Z}}$ the $D_k(x)$ does not hold. By the way we have chosen e^n we have immediately satisfied (i). Since $\forall e^n \in I_n$, we observe that (iii) holds as well.

It remains to verify (ii). And as we will see (iii) follows by (ii), moreover, the proof will have a certain resemblance to the last part in the proof of $[d]_\sim \subseteq \bigcup_{y \in B} y_+$ in Lemma 10.28.

Assume for contradiction that there $\exists n, m \in \mathbb{N}$ s.t. $n \neq m$ and $e^n \sim e^m$. Since $e^n \sim e^m$ we get that there exists $l_n, l_m \in \mathbb{N}$ s.t. $M \models e^n \text{ div } \underline{k^{l_n}} = e^m \text{ div } \underline{k^{l_m}}$. Also WLOG assume that $n < m$, which implies $M \models e^n < e^m$. We also note that $M \models e^0 \leq e^n < e^m < \underline{k} \times e^0$ and there is a *non-standard gap* in place of $<$'s.

Since $e^n \notin e^m_{\mathbb{Z}}$ we observe by (ii) in Observation 10.26 that $l_n \neq l_m$.

If $l_n > l_m$, then by Observation 10.27 we know that $M \models e^n \text{ div } \underline{k^{l_m}} < e^m \text{ div } \underline{k^{l_m}}$. And by Observation 10.24 we get that $M \models e^n \text{ div } \underline{k^{l_n}} < e^m \text{ div } \underline{k^{l_m}}$. Therefore, $M \models e^n \text{ div } \underline{k^{l_n}} \neq e^m \text{ div } \underline{k^{l_m}}$, hence the assumption of $l_n > l_m$ can not hold.

Assume that $l_n < l_m$. We have by Observation 10.27 that $M \models e^m \text{ div } \underline{k^{l_m}} < (\underline{k} \times e^0) \text{ div } \underline{k^{l_m}}$. Evidently $M \models (\underline{k} \times e^0) \text{ div } \underline{k^{l_m}} = e^0 \text{ div } \underline{k^{l_m - 1}}$. And by Observation 10.24 we know that $M \models e^0 \text{ div } \underline{k^{l_m - 1}} \leq e^0 \text{ div } \underline{k^{l_n}}$. And since $M \models e^0 \leq e^n$ we get by Observation 10.37 that $M \models e^0 \text{ div } \underline{k^{l_n}} \leq e^n \text{ div } \underline{k^{l_n}}$. Combining all the $<, =$ and $\leq$, we get that $M \models e^m \text{ div } \underline{k^{l_m}} < e^n \text{ div } \underline{k^{l_n}}$. Therefore, $M \models e^m \text{ div } \underline{k^{l_m}} \neq e^n \text{ div } \underline{k^{l_n}}$, hence, $l_n < l_m$ can not hold.

We got that neither of $l_n = l_m$, $l_n > l_m$ and $l_n < l_m$ can hold, which is the contradiction we wanted.

□

Corollary 10.39. Let $M \models PA$, M is non-standard and $2 \leq k \in \mathbb{N}$. Then $|N| \leq |C^{\neg D_k}|$.

Proof. Follows by Lemma 10.38. □

Now, our goal will be to show that actually for any $2 \leq k \in \mathbb{N}$ and $M \models PA$ we have $|C^{D_k}| = |C^{\neg D_k}| = |M|$.

Lemma 10.40 (injection from $|C^{\neg D_k}|$ into $|C^{D_k}|$)**.** Let M be a non-standard model of PA and let $2 \leq k \in \mathbb{N}$. Moreover, let $a \in M \backslash \mathbb{N}^M$ and let S be some function from $C^{\neg D_k}$ into M s.t. $\forall X \in C^{\neg D_k}$ $S(X) \in X$. Then the later defined h is a function from $C^{\neg D_k}$ into C^{D_k} s.t. h is injective. Definition, $h(X) := [(\exp(\underline{k}, a) \times S(X))^M]_{\sim_k}$.

Proof. First note that h is evidently a well defined function from $C^{\neg D_k}$ into C^{D_k}. Therefore, it does suffice to show that h is injective.

Let $X, Y \in C^{\neg D_k}$ s.t. $X \neq Y$. Since $S(X) \in X$ and $S(Y) \in Y$ we have that $\neg S(X) \sim S(Y)$.

Assume for contradiction that $h(X) = h(Y)$. As a consequence, we get that $(\exp(\underline{k}, a) \times S(X))^M \sim (\exp(\underline{k}, a) \times S(Y))^M$. Hence, there exists $l_X, l_Y \in \mathbb{N}$ s.t. $M \models \exp(\underline{k}, a \dot{-} l_x) \times S(X) = \exp(\underline{k}, a \dot{-} l_y) \times S(Y)$. WLOG $l_x \leq l_y$ and set $r := l_y - l_x$. Then we can conclude that $M \models \underline{k^r} \times S(X) = S(Y)$ which in turn implies a contradiction that $S(X) \sim S(Y)$. □

Commentary. The reader may notice, or has already noticed, that in the light of Corollary 10.39 and Lemma 10.40 the Observation 10.33 and Lemma 10.34 are not actually needed to conclude Corollary 10.35 Nevertheless, we think that it is instructive to show that $|\mathbb{N}| \leq C^{D_k}$ first by a very natural proof idea.

Corollary 10.41. Let $M \models PA$ and $2 \leq k \in \mathbb{N}$. Then $|C^{\neg D_k}| \leq |C^{D_k}|$.

Proof. If M is standard, then $C^{\neg D_k} = C^{D_k} = \emptyset$ and the conclusion holds. Otherwise apply Lemma 10.40. □

Observation 10.42 ($|C^{D_k}| = |M|$)**.** Let M be a non-standard model of PA and $2 \leq k \in \mathbb{N}$. Then $|M| = |C^{D_k}| = |C^{D_k - 1}|$.

Proof. The equality is by Corollary 10.32. By Lemma 10.31 we know that $\{[x]_{\sim_k} | x \in M\} = C^0 \cup C^{D_k} \cup C^{D_k - 1} \cup C^{\neg D_k}$. Furthermore by Lemma 10.28 it is obvious that for any $x \in M$ the $|[x]_{\sim}| = |\mathbb{N}|$.

By Theorem 6.7 it is evident that $|M \backslash 0_{\mathbb{Z}}^M| = |M|$. So we have the following equation, $|M| = |C^{D_k}| \times |\mathbb{N}| + |C^{D_k - 1}| \times |\mathbb{N}| + |C^{\neg D_k}| \times |\mathbb{N}|$. By Corollary 10.32 we get that $|M| = |C^{D_k}| \times |\mathbb{N}| + |C^{\neg D_k}| \times |\mathbb{N}|$. Continuing, by Corollary 10.41, we have $|M| = |C^{D_k}| \times |\mathbb{N}|$. And since $|\mathbb{N}| \leq |C^{D_k}|$, which is by Corollary 10.35, we may finally conclude that $|M| = |C^{D_k}|$. □

Lemma 10.43. Let $M \models PA$, M be non-standard and let $2 \leq k \in \mathbb{N}$. Furthermore let S be some function from C^{D_k} into M s.t. $\forall X \in C^{D_k}$ we have $S(X) \in X$ and $D_k(S(X))$ holds. Furthermore, let F be some function from $C^{\neg D_k}$ into M s.t. $\forall X \in C^{\neg D_k}$ we have $F(X) \in X$. Moreover, define a function L from $\bigcup C^{\neg D_k}$ into $\mathbb{Z}$ in the following manner. Where if $x \in \bigcup C^{\neg D_k}$ denote by X the unique member of $C^{\neg D_k}$ s.t. $x \in X$.

$$L(x) := \begin{cases} l & x \in (\underline{k^l} \times F(X))_{\mathbb{Z}}^M, \\ 0 & x \in F(X)_{\mathbb{Z}}^M, \\ -l & x \in (F(X) \text{ div } \underline{k^l})_{\mathbb{Z}}^M. \end{cases}$$

Note that L is well defined by Lemma 10.28. Lastly let $e \in M \backslash \mathbb{N}^M$ s.t. $\forall x \in e_{\mathbb{Z}}$ $\neg D_k(x)$. Note that picking such a e makes sense thanks to Lemma 10.38. Then the following function h from C^{D_k} into $C^{\neg D_k} \times \mathbb{Z}$ is a well defined injection. $h(X) := ([(S(X) + e)^M]_{\sim_k}, L((S(X) + e)^M))$.

Proof. To show that h is well defined function it clearly does suffice to show that $\forall X \in C^{D_k}$ we have $\forall y \in (S(X)+e)^M_{\mathbb{Z}}$ that $\neg D_k(y)$.

Assume for contradiction that there exists $X \in C^{D_k}$, $y \in (S(X)+e)^M_{\mathbb{Z}}$ and $r \in \mathbb{N}$ s.t. $D_k((S(X)+e+\underline{r})^M)$ or $D_k((S(X)+e \dot{-} \underline{r})^M)$ is true. Since $D_k(S(X))$ holds by our assumption, we get that by Observation 10.19 that $D_k((e+\underline{r})^M)$ or $D_k((e \dot{-} \underline{r})^M)$ hold which can not be by our choice of e.

Now, it remains to show that h is injective. Let $X, Y \in C^{D_k}$ and assume $X \neq Y$. If $\neg((S(X)+e)^M \sim (S(Y)+e)^M)$ then evidently $h(X) \neq h(Y)$.

Otherwise assume $(S(X)+e)^M \sim (S(Y)+e)^M$. Since $X \neq Y$ we have $\neg(S(X) \sim S(Y))$. Therefore $S(X) \neq S(Y)$ and recalling that $D_k(S(X))$ and $D_k(S(Y))$ hold, we get by Observation 10.20 that they can not be in the same copy of $\mathbb{Z}$. More formally there exists $f \in M \backslash \mathbb{N}^M$ s.t. $M \models S(X)+f = S(Y)$ where we WLOG assume that $M \models S(X) < S(Y)$. Hence, we also have $M \models S(X)+f+e = S(Y)+e$. Since $(S(X)+e)^M \sim (S(Y)+e)^M$ we get that the unique $X_1, X_2 \in C^{\neg D_k}$ are actually equal to each other, i.e. $X_1 = X_2$. Therefore, also $F(X_1) = F(X_2)$. But now by $M \models S(X)+f+e = S(Y)+e$, where f is non-standard, it is by Lemma 10.28 evident that $L((S(X)+e)^M) \neq L((S(Y)+e)^M)$. Therefore, we can again conclude that $h(X) \neq h(Y)$ which concludes our verification of h being injective. ☐

Corollary 10.44. Let $M \models PA$ and $2 \leq k \in \mathbb{N}$. Then $|C^{D_k}| \leq |C^{\neg D_k}| \times |\mathbb{N}|$.

Proof. If M is standard model of PA the result is obvious, otherwise apply Lemma 10.43. ☐

Observation 10.45. Let M be a non-standard model of PA, $2 \leq k \in \mathbb{N}$. Then $|C^{\neg D_k}| = |M|$.

Proof. By the same argument as in Observation 10.42 we get that $|M| = |C^{D_k}| \times |\mathbb{N}| + |C^{\neg D_k}| \times |\mathbb{N}|$. By Corollary 10.44 we get that $|M| \leq |C^{\neg D_k}| \times |\mathbb{N}| \times |\mathbb{N}| + |C^{\neg D_k}| \times |\mathbb{N}|$. Furthermore, we know by Corollary 10.39 $|\mathbb{N}| \leq |C^{\neg D_k}|$. Therefore, we can conclude that $|M| = |C^{\neg D_k}|$ indeed holds. ☐

This concludes our inspection of the cardinalities of $|C^{D_k}|$, $|C^{D_k - 1}|$ and $|C^{\neg D_k}|$. We will state one more corollary only to sum up findings of this section.

Corollary 10.46 ($|C^{D_k}| = |C^{D_k-1}| = |C^{\neg D_k}| = |M|$)**.** Let $M \models PA$ and $2 \leq k \in \mathbb{N}$. Then $|C^{D_k}| = |C^{D_k-1}| = |C^{\neg D_k}| = |M|$.

Proof. Follows by Observation 10.42 and Observation 10.45. ☐

10.4 Graph theory intermezzo

In this section, and text, we consider only oriented (infinite) graphs, which are not multigraphs.

Definition 10.11 ($x \to y$, $x \to^n y$, $x \to^{\leq n} y$)**.** Let $G = (V, E)$ be an oriented graph and let $x, y \in V$.

- We use $x \to y$ to denote that there exists a finite path from x to y in G.

- We use $x \to^n y$ to denote that there exists a path of length n from x to y in G.
- And we use $x \to^{\leq n} y$ to denote that there exists a path of length at most n from x to y in G.

Definition 10.12 ($N_+(x), N_-(x)$)**.** Let $G = (V, E)$ be an oriented graph and let $x \in V$ and $B \subseteq V$. Then we define the following.

- $N_+(x) \coloneqq \{y \in V | (y, x) \in E\}$.
- $N_-(x) \coloneqq \{y \in V | (x, y) \in E\}$.
- $N_+(B) \coloneqq \{y \in V | \exists x \in B\ (y, x) \in E\}$.
- $N_-(B) \coloneqq \{y \in V | \exists x \in B\ (x, y) \in E\}$.

When we will be dealing with multiple graphs, with the same domain, it will be evident from the context with respect to what graph we mean $x \to y$, $N_+(y)$,...

Definition 10.13 ($T_G, T_G^n, T_G^{\leq n}$)**.** Let $G = (V, E)$ be an oriented graph. We will define then T_G, T_G^n and $T_G^{\leq n}$ as a functions from V into $\mathcal{P}(V)$. Specifically, if $v \in V$, then we define the following.

- $T_G(v) \coloneqq \{u \in V | u \to v\}$.
- $T_G^n(v) \coloneqq \{u \in V | u \to^n v\}$.
- $T_G^{\leq n}(v) \coloneqq \{u \in V | u \to^{\leq n} v\}$.

Commentary. Note that for any oriented graph $G = (V, E)$ and $v \in V$ we have $T_G(v) = \bigcup_{n \in \mathbb{N}} T_G^{\leq n}(v)$.

In our usage, G induced on $T_G(v), T_G^n(v)$ and $T_G^{\leq n}(v)$ will be a tree, hence the notation.

Lemma 10.47. Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two oriented graphs s.t. $V_1 = V_2 = \mathbb{Z} \times \mathbb{Z}$. Also let $2 \leq k \in \mathbb{N}$. Moreover we assume the following.

(i) $\forall u, v \in \mathbb{Z} \times \mathbb{Z}$ we have that if $\neg u \to v$ in G_1 and $\neg v \to u$ in G_1, then $T_{G_1}(u) \cap T_{G_1}(v) = \emptyset$. $\forall u, v \in \mathbb{Z} \times \mathbb{Z}$ we have that if $\neg u \to v$ and $\neg v \to u$ in G_2, then $T_{G_2}(u) \cap T_{G_2}(v) = \emptyset$.

(ii) $\forall (i, j) \in \mathbb{Z} \times \mathbb{Z} \forall e \in E_1$ we have that if $x \in \mathbb{Z} \times \mathbb{Z}$ and $e = (x, (i, j))$, then $x = (i + 1, l)$ for some $l \in \mathbb{Z}$. Moreover $\forall y \in \mathbb{Z} \times \mathbb{Z}$ we have that $|\{x \in \mathbb{Z} \times \mathbb{Z} | (x, y) \in E_1\}| = k$. Or equivalent said, $\forall (i, j) \in \mathbb{Z} \times \mathbb{Z}$ there are exactly k edges going to (i, j) from k distinct vertices of the form $(i + 1, l)$ for $l \in \mathbb{Z}$. And exactly the same condition applies, and is required from, to G_2.

Then $\forall u \in V_1 \forall v \in V_2$ we have that $G_1[T_{G_1}(u)] \cong G_2[T_{G_2}(v)]$, i.e. we take induced subgraphs of G_1 and G_2 with respect to $T_{G_1}(u)$ and $T_{G_2}(v)$, s.t. one such isomorphism I witnessing $G_1[T_{G_1}(u)] \cong G_2[T_{G_2}(v)]$ satisfies that $I(u) = v$.

Proof sketch. The proof goes as follow. We will by creating isomorphisms $I^0 \subseteq I^1 \subseteq \dots I^n \subseteq \dots$, i.e. for any $n \in \mathbb{N}$ we will have $I^n \subseteq I^{n+1}$, where I^n will be an isomorphism witnessing $G_1[T^{\leq n}_{G_1}(u)] \cong G_2[T^{\leq n}_{G_2}(v)]$. Furthermore, we will have $I^0(u) = v$.

Assuming that everything promised will actually hold, it is then a routine work to check that $I \coloneqq \bigcup_{n\in\mathbb{N}} I^n$ is a witness to $G_1[T_{G_1}(u)] \cong G_2[T_{G_2}(v)]$ s.t. $I(u) = v$.

First, we define $I^0 \coloneqq \{(u, v)\}$. I^0 evidently satisfies everything that it needs to.

Now, we shall describe the process of defining I^{n+1} from I^n for some $n \in \mathbb{N}$. Assume we have I^n satisfying all it needs to satisfy. Take $T^{n+1}_{G_1}(u)$, which is $N_+(T^n_{G_1}(u))$, and $T^{n+1}_{G_2}(v)$, which is $N_+(T^n_{G_2}(v))$. Now, thanks to our conditions, it is not hard to infer that there must exist a bijection f from $T^{n+1}_{G_1}(u)$ onto $T^{n+1}_{G_2}(v)$ s.t. $\forall x \in T^{n+1}_{G_1}(u)$ when we take the the unique $y \in V_1$, actually $y \in T^n_{G_1}(u)$, satisfying $(x, y) \in E_1$ and the unique $y^{'} \in V_2$, actually $y^{'} \in T^n_{G_2}(v)$, satisfying $(f(x), y^{'}) \in E_2$, then $I^n(y) = y^{'}$. And now defining I^{n+1} as $I^n \cup f$ we see that I^{n+1} satisfies what we want it to satisfy.

Let us note that the existence part of the uniqueness of y follows by $x \in T^{n+1}_{G_1}$, i.e. there exists a path from x to u and thus some $y \in T^n_{G_1}(u)$ s.t. $(x, y) \in E_1$, and the "at most one" part follows by (i) and (ii). And the same goes for the uniqueness of $y^{'}$

Also note that we can construct such a f because when we have have $y \in T^n_{G_1}(u)$ and $y^{'} \in T^n_{G_2}(v)$ then by (ii) $|N_+(y)| = k = |N_+(y^{'})|$, note that $|N_+(y)|$ is with respect to G_1 and $|N_+(y^{'})|$ is with respect to G_2, where $N_+(y) \subseteq T^{n+1}_{G_1}(u)$ and $N_+(y^{'}) \subseteq T^{n+1}_{G_2}(v)$. And by (i) we get that for distinct $y, z \in T^n_{G_1}(u)$ we have $N_+(y) \cap N_+(z) = \emptyset$, and the same holds for distinct $y^{'}, z^{'} \in T^n_{G_2}(v)$.

We choose to omit further details. □

Lemma 10.48. Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two oriented graphs s.t. $V_1 = V_2 = \mathbb{Z} \times \mathbb{Z}$. Also let $2 \leq k \in \mathbb{N}$. Moreover let us assume the following.

(i) Same as (i) in Lemma 10.47.

(ii) Same as (ii) in Lemma 10.47.

(iii) $\forall u \in V_1 \, \forall z \in V_1$ there exists $w \in V_1$ s.t. $u \to w$ and $z \in T_{G_1}(w)$

Then $G_1 \cong G_2$.

Proof sketch. Let us call, for any $i \in \mathbb{Z}$, the set $C_i \coloneqq \{(i, l) | l \in \mathbb{Z}\}$ the *i-th layer*.

First, we pick any two elements u^0 and v^0 from $\mathbb{Z} \times \mathbb{Z}$. By Lemma 10.47 there exists I^0, note that it is *not* the I^0 from the proof of Lemma 10.47 but actually the I, s.t. $I^0(u^0) = v^0$ and I^0 is an isomorphism from $G_1[T_{G_1}(u)]$ onto $G_2[T_{G_2}(v)]$.

Let $u^1 \in V_1$ and $v^1 \in V_2$ be the unique vertices s.t. $(u^0, u^1) \in E_1$ and $(v^0, v^1) \in E_2$. The existence of such vertices follows *mainly* by (iii) and the uniqueness by (i) and (ii). Note that u^1, v^1 are "one layer down" from u^0, v^0.

Take $N_+(u^1)$ and $N_+(v^1)$, with respect to G_1 and G_2. Then evidently both sets are of size k and if $u^1 = (i, j)$ and $v^1 = (k, l)$ then $N_+(u^1) \subseteq C_{i+1}$ and $N_+(v^1) \subseteq C_{k+1}$. Furthermore, $T_{G_1}(u^0) \cap N_+(u^1) = \{u^0\}$ and $T_{G_2}(v^0) \cap N_+(v^1) = \{v^0\}$.

Now, let g be any bijection from $N_+(u^1)$ and $N_+(v^1)$ satisfying that $g(u^0) = v^0$. Apply for every $x \in N_+(u^1)$ s.t. $x \neq u^0$ Lemma 10.47 to get an isomorphism witnessing $G_1[T_{G_1}(x)] \cong G_2[T_{G_2}(g(x))]$ that sends x on $g(x)$. Call such an isomorphism H_x. Also define H_{u^0} as I^0.

Then defining $I^1 := \bigcup_{x \in N_+(u^1)} H_x \cup \{(u^1, v^1)\}$ is indeed an isomorphism witnessing $G_1[T_{G_1}(u^1)] \cong G_2[T_{G_2}(g(v^1))]$ s.t. $I(u^1) = v^1$ and $I^0 \subseteq I^1$. I.e. in this case and in general we are not extending I^0, or I^n, row by row or column by column but we are extending the respective trees that represent domain and range of I^0, or I^n.

In an analogous way, we construct I^2 which will among other things satisfy $I^1 \subseteq I^2$.

This way we will construct $I^0 \subseteq I^1 \subseteq \ldots \subseteq I^n \subseteq \ldots$ for any $n \in \mathbb{N}$. It is not hard that to observe that $I := \bigcup_{n \in \mathbb{N}} I^n$ will be an isomorphism from $G_1[V_1^{'}]$ onto $G_2[V_2^{'}]$ for $V_1^{'} \subseteq V_1$ and $V_2^{'} \subseteq V_2$. But now by (iii) it is not hard to observe that $V_1^{'} = V_1$ and $V_2^{'} = V_2$, hence proving the lemma.

We choose to omit further details. $\square$

10.5 Structure of $(M, x \text{ div } \underline{k})$

Observation 10.49. Let $2 \leq k \in \mathbb{N}$. Also define f as a function over $\mathbb{Z} \times \mathbb{Z}$ s.t. for $(l, m) \in \mathbb{Z} \times \mathbb{Z}$ where $i \in [k-1] \wedge k \mid (l + i)$, note that i is unique, we have

$$f(l,m) := \begin{cases} (l-1, (m+i) \text{ div } k) & -i \leq m, \\ (l-1, -(-(m+i+1) \text{ div } k) - 1) & m \leq -i-1. \end{cases}$$

Then $(\mathbb{Z} \times \mathbb{Z}, f)$ is an oriented graph satisfying (i),(ii) and (iii) from Lemma 10.48.

Proof. Verification of (i) is easy. Verification of (ii) and (iii) is technical but possible. We omit the proof. $\square$

Theorem 10.50. Let M be a non-standard model of PA and let $2 \leq k \in \mathbb{N}$. Then $(M, (x \text{ div } \underline{k})^M)$, i.e. M restricted to the unary function $x \text{ div } \underline{k}$, is isomorphic to $(\mathbb{N} \cup (|C^{D_k}| \times \mathbb{Z} \times \mathbb{N} \times \{0\}) \cup (|C^{D_k - 1}| \times \mathbb{Z} \times \mathbb{N} \times \{1\}) \cup (|C^{\neg D_k}| \times \mathbb{Z} \times \mathbb{Z} \times \{2\}), f)$ where $f(x)$ for $x \in \mathbb{N}$ is defined as $x \text{ div } k$. For $x = (s, l, m, j)$ with $j \leq 1$ is defined as $(s, l-1, m \text{ div } k, j)$. Lastly for $j = 2$ and with $i \in [k-1] \wedge k \mid (l+i)$ we define

$$f(s,l,m,j) := \begin{cases} (s, l-1, (m+i) \text{ div } k) & -i \leq m, \\ (s, l-1, -((-(m+i+1)) \text{ div } k) - 1) & m \leq -i-1. \end{cases}$$

Where in the definition of f is div always the standard div on $\mathbb{N}$, i.e. $\text{div}^{\mathbb{N}}$.

Proof sketch. By Lemma 10.31 we know that we can split, in a disjoint and exhaustive manner, elements of M into sets $\{[0^M]_{\sim_k}\}$, C^{D_k}, $C^{D_k - 1}$ and $C^{\neg D_k}$ which contain equivalence classes of $\sim_k$. By Observation 10.18 we know that $0^M]_{\sim_k} = \mathbb{N}^M$. And by Lemma 10.28 we know how elements of C^{D_k}, $C^{D_k - 1}$ and $C^{\neg D_k}$ look like.

Therefore, it can be observed, that to prove the theorem in mention the following does suffice to be shown. Namely, we will present function that will show isomorphism between various restrictions, with respect to domains, of $(M, (\text{ div } \underline{k})^M)$

and $(\mathbb{N}\cup(|C^{D_k}|\times\mathbb{Z}\times\mathbb{N}\times\{0\})\cup(|C^{D_k-1}|\times\mathbb{Z}\times\mathbb{N}\times\{1\})\cup(|C^{\neg D_k}|\times\mathbb{Z}\times\mathbb{Z}\times\{2\}), f)$ from which will follow that there must exist one function witnessing the isomorphism of the two structures in the statetement of the theorem.

(i) We will want to show that $(\mathbb{N}^M, (x \text{ div } \underline{k})^M \restriction \mathbb{N}^M) \cong (\mathbb{N}, f \restriction \mathbb{N})$. A function witnessing the isomorphism,"from right to left", is $g_0(n) = \underline{n}^M$.

(ii) Let $c \in C^{D_k}$ and let $d \in c$, i.e. $[d]_{\sim_k} = c$, s.t. $D_k(d)$ holds. We will want to show that $([d]_{\sim_k}, (x \text{ div } \underline{k})^M \restriction [d]_{\sim_k}) \cong (\{0\} \times \mathbb{Z} \times \mathbb{N} \times \{0\}, f \restriction \{0\} \times \mathbb{Z} \times \mathbb{N} \times \{0\})$. A function witnessing the isomorphism, we omit the $\{0\}$'s, is

$$g_1(l, m) := \begin{cases} (\underline{k^l} \times d + \underline{m})^M & 0 \leq l, \\ (d \text{ div } \underline{k^l} + \underline{m})^M & l < 0. \end{cases}$$

(iii) Let $c \in C^{D_k-1}$ and let $d \in M$ s.t. $[(d \dot{-} 1)^M]_{\sim_k} = c$ and $D_k(d)$ hold. We will want to show that $([(d \dot{-} 1)^M]_{\sim_k}, (x \text{ div } \underline{k})^M f \restriction [(d \dot{-} 1)^M]_{\sim_k}) \cong (\{0\} \times \mathbb{Z} \times \mathbb{N} \times \{1\}, f \restriction \{0\} \times \mathbb{Z} \times \mathbb{N} \times \{1\})$. A function witnessing the isomorphism, we omit the $\{0\}$ and $\{1\}$, is

$$g_2(l, m) := \begin{cases} ((\underline{k^l} \times d \dot{-} 1) \dot{-} \underline{m})^M & 0 \leq l, \\ ((d \text{ div } \underline{k^l} \dot{-} 1) \dot{-} \underline{m})^M & l < 0. \end{cases}$$

(iv) Let $c \in C^{\neg D_k}$ and let $e \in M$ s.t. $[e]_{\sim_k} = c$ and $\forall x \in e_{\mathbb{Z}}$ the $D_k(x)$ does not hold. We will want to show that $([e]_{\sim_k}, (x \text{ div } \underline{k})^M f \restriction [e]_{\sim_k}) \cong (\{0\} \times \mathbb{Z} \times \mathbb{Z} \times \{2\}, f \restriction \{0\} \times \mathbb{Z} \times \mathbb{Z} \times \{2\})$. This time we note, using some abstraction e.g. forgetting $\{0\}$ and $\{2\}$, that these two structures in mention are basically graphs from with vertices $\mathbb{Z} \times \mathbb{Z}$ satisfying condition (i), (ii) and (iii) from Lemma 10.48. Therefore, they are indeed isomorphic.

Points (i)-(iv) can be, although, technically verified. We omit further details.

□

Commentary. Let us note that the point (iv) in the construction of isomorphism in Theorem 10.50 is the only point where we do not necessarily retain the successor function, the order or at least the order on (non-)standard copies of $\mathbb{Z}$ is inevitable. Because it is not hard to observe, be an argument that we are about to encounter in Lemma 11.7, that otherwise there would be a non-standard model of PA with domain $\mathbb{N}$ s.t. $(x \text{ div } \underline{k})^M$ would be a recursive function and also

- S^M or
- $<^M$ or
- $<^M$ restricted on copies of $\mathbb{Z}$

would be recursive. But that is not possible by Corollary 8.15, Corollary 8.16 and Corollary 8.17.

This argument also shows that in *principle*, i.e. in general case, we can not find an isomorphism between two graphs satisfying (i),(ii) and (iii) from Lemma 10.48 that would retain some reasonably defined the order or the successor function on the graphs in mention satisfying the condition (i)-(iii) from Lemma 10.48.

Corollary 10.51. Let M be a non-standard model of PA and let $2 \leq k \in \mathbb{N}$. Then $(M, (\mathrm{div}\underline{k})^M)$, i.e. M restricted to the unary function $x \operatorname{div} \underline{k}$, is isomorphic to $(\mathbb{N} \cup (|M| \times \mathbb{Z} \times \mathbb{N} \times \{0\}) \cup (|M| \times \mathbb{Z} \times \mathbb{N} \times \{1\}) \cup (|M| \times \mathbb{Z} \times \mathbb{Z} \times \{2\}), f)$ where $f(x)$ for $x \in \mathbb{N}$ is defined as x div k. For $x = (s, l, m, j)$ with $j \leq 1$ is defined as $(s, l-1, m \text{ div } k, j)$. Lastly for $j = 2$ and with $i \in [k-1] \wedge k \mid (l+i)$ we define

$$f(s, l, m, j) := \begin{cases} (s, l-1, (m+i) \text{ div } k) & -i \leq m, \\ (s, l-1, -(-(m+i+1) \text{ div } k) - 1) & m \leq -i-1. \end{cases}$$

Where in the definition of f is div always the standard div on $\mathbb{N}$, i.e. $\mathrm{div}^{\mathbb{N}}$.

Proof. Follows by Theorem 10.50 and Corollary 10.46. □

11. Recursiveness of the div function

11.1 x div y can not be recursive in $I\Sigma_1$

Observation 11.1 (div determines $<$)**.** Let $M \models I\Sigma_1$, then we can determine $<^M$ using div. I.e. the following holds for any $a, b \in M$ and $b \neq 0^M$.

$$M \models a < b \iff M \models a \text{ div } b = 0.$$

Proof. Assume that $M \models a < b$. Then we have $M \models b \neq 0$ and $M \models 0 \times b \leq a < 1 \times b$, and thus by the definition of div we get $M \models a \text{ div } b = 0$.

As for the other direction assume that $M \models a \text{ div } b = 0$. Then since $b \neq 0^M$ we have $M \models 0 \times b \leq a < 1 \times b$ which implies the desired conclusion of $M \models a < b$. □

Corollary 11.2 (recursive div implies recursive $<$)**.** Let $M \models I\Sigma_1$, s.t. $dom(M)$ equals $\mathbb{N}$, we know the interpretation of 0 in M and div is recursive with respect to M. Then $<$ is also recursive with respect to M.

Proof. This is but a direct corollary of Remark 8.1, i.e. that $=^M$ is recursive, and the just proved Observation 11.1. □

Observation 11.3 (recursive div implies recursive S on $\mathbb{N}^M$)**.** Let $M \models I\Sigma_1$, s.t. $dom(M) = \mathbb{N}$, we know the interpretation of $0, 1$ and $\underline{2}$ in M and div is recursive with respect to M. Then we can compute $\underline{n}^M$ for any given $n \in \mathbb{N}$, i.e. we can compute the successor function S^M on standard elements of M.

Proof. Assume that we already know the interpretation of $0, 1, \underline{2}, \ldots, \underline{k}$ in M for some $k \in \mathbb{N}$ s.t. $2 \leq k$. Then we show how to compute $\underline{(k+1)}^M$.

If we manage to show and justify the just proposed procedure, i.e. computing $\underline{(k+1)}^M$, then it evidently follows that we can compute $\underline{n}^M$ for any $n \in \mathbb{N}$.

Computing $\underline{k+1}^M$.

(i) Enumerate $\mathbb{N}$ recursively according to $<^{\mathbb{N}}$ and denote by x the just enumerated element of $\mathbb{N}$. Where for every such enumerated x compute $x \text{ div }^M \underline{k}^M$. If the result of such computation returns 1^M, then store such x. And if you have already stored k such x's, then stop and move to the next step (ii).

(ii) We know that we can compute $<^M$ by Corollary 11.2. Therefore we can order all the k stored x's from the previous step and pick the second smallest one, denote it by y.

(iii) We return y as we claim that $y = \underline{(k+1)}^M$.

By Observation 8.12 we know that there are indeed exactly k such x's considered in step (i), hence it is obvious that the described procedure always ends and is computable.

And again by Observation 8.12 we know that the x's are of the form $\underline{k}^M$, $\underline{k+1}^M, \ldots, \underline{(k+k-1)}^M$, and hence it is evident that $y = \underline{(k+1)}^M$ and we have returned the right answer. □

Observation 11.4 (Determining $\underline{k} \mid x$ by using div)**.** Let $M \models I\Sigma_1$, $b \in M$ and $k \in \mathbb{N}$. Then $M \models \underline{k} \mid b$ iff. b is the smallest element of all such $x \in M$ s.t. $M \models x \operatorname{div} \underline{k} = b \operatorname{div} \underline{k}$.

Proof. First assume that $M \models \underline{k} = 0$. Then clearly both sides hold iff. $b = 0^M$.

Then assume that $M \models \underline{k} = 1$, then the observation again evidently holds since $M \models a \mid b$ holds always and b is the smallest one, since it is the only one, such x.

From now on we can, and will, assume $M \models 2 \leq \underline{k}$.

$\Rightarrow$: Assume that $M \models \underline{k} \mid b$, hence, there exists $a \in M$ s.t. $M \models \underline{k} \times a = b$.

Since necessarily $M \models 0 < \underline{k}$, which also implies $M \models 0 \neq \underline{k}$, we evidently have that $M \models a \times \underline{k} \leq b < (a+1) \times \underline{k}$ and hence $M \models b \operatorname{div} \underline{k} = a$ by definition.

But using Observation 8.12 we see that b is indeed the smallest $x \in M$ s.t. $M \models x \operatorname{div} \underline{k} = a \,(= b \operatorname{div} \underline{k})$.

$\Leftarrow$: Let $a \in M$ s.t. $M \models b \operatorname{div} \underline{k} = a$. Since evidently $0 < k$, we get by Observation 8.12 that if b is the smallest $x \in M$ s.t. $M \models x \operatorname{div} \underline{k} = a$, then $M \models b = \underline{k} \times a$.

Hence, $M \models \underline{k} \mid b$ and the proof is finished.

□

Observation 11.5 (Deciding $\underline{k} \mid b$ by using computable div)**.** Let $M \models I\Sigma_1$, $b \in M$ and $k \in \mathbb{N}$. Furthermore, assume that div is recursive with respect to M and we know the interpretation of $\underline{k}$ and 0 in M. Then, we can recursively decide whether or not $M \models \underline{k} \mid b$.

Proof. If $\underline{k}^M = 0^M$, then if $b = 0^M$ we can evidently return *yes*, and otherwise, if $b \neq 0^M$, we can evidently return *no* .

From now on assume that $\underline{k}^M \neq 0^M$.

(i) Enumerate $\mathbb{N}$ recursively according to $<^{\mathbb{N}}$ s.t. we will store x's which satisfy $M \models x \operatorname{div} \underline{k} = b \operatorname{div} \underline{k}$. And if we have exactly k of them, we stop this part of the computation and proceed to the next one, i.e. (ii). Let us note that by Observation 8.12 this sub-procedure must come to an end after a finite number of steps.

(ii) Now order all the stored x's, we can do it by Corollary 11.2 - i.e. the recursivity of $<$, and check whether b equals to the smallest x.

(iii) If it does, then return *yes* and otherwise *no*.

The validity of the just described algorithmic procedure follows by the just proved Observation 11.4.

And since are all the described steps finite in nature and computable, we can conclude that the observation being proved holds. □

We shall now state and prove the main result of this section.

Lemma 11.6 (div can not be recursive in non-standard model of $I\Sigma_1$)**.** Let M be a non-standard model of $I\Sigma_1$ with its domain equal to $\mathbb{N}$. Then the binary function x div y can not be recursive with respect to M.

Proof. Assume for contradiction that the premises hold whereas the conclusion does not, i.e. div^M is a recursive function. Furthermore we can WLOG assume by Observation 3.13 that $0^M = 0, 1^M = 1$ and $\underline{2}^M = 2$.

Applying Corollary 4.3 we get that there exists $X \subseteq \mathbb{N}$ s.t. X is not recursive and there exists $b \in M$ s.t. $\forall n \in \mathbb{N}$

$$n \in X \iff M \models \underline{p(n)} \mid b.$$

But now since $p(n)$ is computable by Observation 3.9, we get by Observation 11.3, which is about computing $\underline{k}^M$ for any $k \in \mathbb{N}$, that we can compute $\underline{p(n)}^M$ for any $n \in \mathbb{N}$.

And thus we get by Observation 11.5, which is about deciding divisibility, that we can algorithmically decide for any $n \in \mathbb{N}$ whether $M \models \underline{p(n)} \mid b$ or not.

Therefore, we can algorithmically decide membership in X which is the contradiction we wanted. □

Commentary. The just proved result directly implies the one in Lemma 8.5, however, it seemed only natural to us to prove the weaker version first.

11.2 x div $\underline{k}$ can be recursive in PA

This section is basically one, described in detail, corollary of the work done in chapter 10.

Lemma 11.7 (x div $\underline{k}$ can be recursive)**.** Let $k \in \mathbb{N}$. Then, there exists a non-standard model M of PA, s.t. $dom(M) = \mathbb{N}$ and $\text{div}\underline{k}$ is recursive with respect to M.

Proof. **First assume that $k < 2$.**

The result follows immediately by Corollary 8.7, since it states all in the just being proved lemma (and more).

Assume that $2 \leq k$.

Let U be any countable non-standard model of PA. By Corollary 2.3 we know that there is one.

We know by Corollary 10.51 that $(U, (\text{div}\underline{k})^U)$, i.e. U restricted to $\text{div}\underline{k}$, is isomorphic to a structure (A, f) with f being a computable function and where

$$A = \mathbb{N} \cup (\mathbb{N} \times \mathbb{Z} \times \mathbb{N} \times [1]) \cup (\mathbb{N} \times \mathbb{Z} \times \mathbb{Z} \times \{2\}).$$

Furthermore, by Bijection 8 we know that A is a *computably codable set.*

Therefore, we can conclude by Corollary 3.15 that there must be G a model of PA s.t. $dom(G) = \mathbb{N}$, $G \cong M$, hence it is non-standard model of PA, s.t. $\text{div}\underline{k}$ is recursive with respect to G.

And the proof is finished. □

Lemma 11.8. Let $k \in \mathbb{N}$. Then there exists a non-standard model M of PA, s.t. $dom(M) = \mathbb{N}$ and for every $l \in \mathbb{N}$ is $\text{div}\underline{k^l}$ recursive with respect to M.

Proof. The lemma follows by Lemma 11.7 and by noting Corollary 10.15. □

11.3 One middle ground observation

We have seen in section 11.1 that x div y can not be recursive in a non-standard model of $I\Sigma_1$. Whereas, we have seen in section 11.2 that for any $k \in \mathbb{N}$ there is a non-standard model of PA with div$\underline{k^l}$ recursive for every $l \in \mathbb{N}$.

How about for some middle ground results? I.e. where we demand more than just div$\underline{k^l}$ to be recursive but still with some restriction on x or y in the binary function x div y.

A question of interest might be the following.

Problem 3 (Classification of when can be div$\underline{k}$, for all $k \in F \subseteq \mathbb{N}$, recursive)**.** Classify exactly for which sets $F \subseteq \mathbb{N}$ there exists a non-standard model of PA, or $I\Sigma_1$, with domain $\mathbb{N}$ s.t. div$\underline{k}$, for every $k \in F$, is recursive with respect to it.

Although, we have seen some examples of valid F's in section 11.2, we did not manage to answer Problem 3 in its fullnes

Nevertheless, there is one thing that we would like to mention that is possibly remotely related to Problem 3.

First, let us recall the following. Imagine for a moment that $M \models I\Sigma_1$ and we want to show by contradiction that some function or relation can not be recursive with respect to M. As we have already seen, in this and the preceding chapters, it is very useful if we are able to compute $\underline{n}^M$ for all $n \in \mathbb{N}$. It is because we can compute then $\underline{p(n)}^M$ for any $n \in \mathbb{N}$, which was often a powerful tool in deciding membership in some non-recursive subset of $\mathbb{N}$, and hence arriving at a contradiction.

Therefore, a natural question to ask is which sets $F \subseteq \mathbb{N}$ enable us to compute $\underline{n}^M$, for every $n \in \mathbb{N}$, in some respective model M for which we can compute $(x \text{ div } \underline{l})^M$ for every $l \in F$.

We did not manage to answer this question fully, however, we have observed, as will be seen in Lemma 11.16, that there are some pairs of natural numbers s.t. if F contains them, then we can compute $\underline{n}^M$ for every $n \in \mathbb{N}$.

Let us first state a few useful observations and one useful condition on pairs of natural numbers.

Note that the following observation is taking place in $\mathbb{N}$.

Observation 11.9. Let $2 \leq n, m \in \mathbb{N}$ and $l \in \mathbb{N}$ s.t. $n^l < m$. Also assume that $r_0, \ldots, r_l \in \mathbb{N}$ s.t. $r_1, \ldots, r_l < n$. Then there exists $b_0 \in \mathbb{N}$ s.t. $\forall b \in \mathbb{N}\ b_0 \leq b$ we get that

$$(n \times (\ldots (n \times (b + r_0) + r_1) \ldots) + r_l) \text{ div } m < b,$$

where the $n\times$ is repeated l-times.

Proof. We can WLOG assume $r_1 = \ldots = r_l = n - 1$. We can do it since x div m is obviously monotone in $\mathbb{N}$, for a proof see Observation 10.37.

Set $b_0 \coloneqq (r_0 + 1) \times m$ and assume $b = b_0$.

Observe that,

$$n \times (\ldots (n \times (b + r_0) + r_1) \ldots) + r_l =$$
$$n^l \times b + n^l \times r_0 + n^{l-1} \times (n - 1) + \ldots + n^0 \times (n - 1) =$$
$$n^l \times b + n^l \times r_0 + n^l - 1.$$

The last expression is, by $n^l < m$, clearly smaller than or equal to

$$n^l \times b + m \times r_0 + n^l - 1.$$

Furthermore, $(n^l \times b + m \times r_0 + (n^l - 1))$ div $m = n^l \times (r_0 + 1) + r_0$, by the choice of $b = b_0 = (r_0 + 1) \times m$ and $n^l < m$.

Hence, by the result of Observation 10.37 , i.e. x div m being monotone, we have $(n \times (\ldots(n \times (b + r_0) + r_1)\ldots) + r_l)$ div $m \leq n^l \times (r_0 + 1) + r_0$.

By $n^l < m$ we get that $n^l \times (r_0+1)+r_0 < (n^l+1)\times(r_0+1) \leq m\times(r_0+1) = b$.

Therefore $(n \times (\ldots(n \times (b + r_0) + r_1)\ldots) + r_l)$ div $m < b$.

Now it remains to show the same if $b = b_0+c$ for some $c \in \mathbb{N}$. By a well known truth in $\mathbb{N}$, or by using Theorem 2.4, there must exist $d, t \in \mathbb{N}$ s.t. $c = d \times m + t$ and $t < m$. Therefore, from now on, we can assume that $b = b_0+d\times m+t \wedge t < m$ for some $d, t \in \mathbb{N}$.

We still have that $n\times(\ldots(n\times(b+r_0)+r_1)\ldots)+r_l = n^l\times b+n^l\times r_0+n^l-1$.

Furthermore, we have,

$$n^l \times b + n^l \times r_0 + n^l - 1 =$$
$$n^l \times b_0 + n^l \times m \times d + n^l \times t + n^l \times r_0 + n^l - 1.$$

Continuing, we have by $n^l < m$ and the value of b_0 the following,

$$n^l \times b_0 + n^l \times m \times d + n^l \times t + n^l \times r_0 + n^l - 1 \leq$$
$$n^l \times (r_0 + 1) \times m + n^l \times m \times d + m \times t + m \times r_0 + (n^l - 1).$$

Computing $(n^l \times (r_0+1) \times m + n^l \times m \times d + m \times t + m \times r_0 + (n^l - 1))$ div m, we get by $n^l < m$ that the result equals to $n^l \times (r_0 + 1) + n^l \times d + t + r_0$.

Recall that $n^l\times(r_0+1)+r_0 < b_0$, and since $n^l < m$, we have $n^l\times d+t \leq m\times d+t$, hence, $n^l \times (r_0 + 1) + n^l \times d + t + r_0 < b$. Therefore,

$$(n^l \times (r_0 + 1) \times m + n^l \times m \times d + m \times t + m \times r_0 + (n^l - 1)) \text{ div } m < b.$$

To summarize.

- $$n \times (\ldots(n \times (b + r_0) + r_1)\ldots) + r_l \leq$$
  $$n^l \times (r_0 + 1) \times m + n^l \times m \times d + m \times t + m \times r_0 + (n^l - 1).$$
- x div m is monotone by Observation 10.37.
- $(n^l \times (r_0 + 1) \times m + n^l \times m \times d + m \times t + m \times r_0 + (n^l - 1))$ div $m < b$.

Therefore, $(n \times (\ldots(n \times (b + r_0) + r_1)\ldots) + r_l)$ div $m < b$, which finishes the proof. □

What follows, is a version of the preceding observation for any model of $I\Sigma_1$.

Observation 11.10. Let $M \models I\Sigma_1$. Let $2 \leq n, m \in \mathbb{N}$ and $l \in \mathbb{N}$ s.t. $n^l < m$. Also assume that $r_0, \ldots, r_l \in \mathbb{N}$ s.t. $r_1, \ldots, r_l < n$. Then there exists $b_0 \in \mathbb{N}$ s.t. $\forall b \in \mathbb{N}\ b_0 \leq b$ we get that

$$(\underline{n} \times (\ldots(\underline{n} \times (b + \underline{r_0}) + \underline{r_1})\ldots) + \underline{r_l}) \text{ div } \underline{m} < b,$$

where the $\underline{n}\times$ is repeated l-times.

Proof. We can evidently make the same proof as for Observation 11.9, only in a slightly formalized fashion.

It is mainly because of the following.

- By all the properties we have learned in section 1.2, in section 1.5 and by axioms of PA^- mentioned in section 1.1. I.e. how $+, \times$ and $<$ behave on elements of M and especially on elements in $\mathbb{N}^M$.
- div behaves on N^M as expected from Observation 7.6.
- x div $\underline{m}$ is monotone in M with respect to x, for a proof see Observation 10.37.
- We can always find for any $c \in \mathbb{N}$ (s.t. $M \models b = b_0 + \underline{c}$) elements d, t in N s.t. $M \models \underline{c} = \underline{d} \times \underline{m} + \underline{t} \wedge \underline{t} < \underline{m}$, it follows mainly by Theorem 2.4.

□

Observation 11.11. Let $M \models I\Sigma_1$ s.t. $dom(M) = \mathbb{N}$ and let $n \in \mathbb{N}$ s.t. $2 \leq n$. Furthermore, assume that div$\underline{n}$ is recursive with respect to M. Then if $a \in M$, then you can compute $(\underline{n} \times a)^M$,$(\underline{n} \times a + 1)^M$,..., $(\underline{n} \times a + \underline{(n-1)})^M$.

Proof. Let a be some given member of M.

The description of an algorithm follows.

Enumerate $\mathbb{N}$ recursively according to $<^{\mathbb{N}}$. Whenever you find x s.t. $(x \text{ div } \underline{n})^M = a$, which we can verify, store such a x. If you have stored so far n x's, then stop and return them.

By Observation 8.12, it follows that the algorithm must stop sooner or later. And we get from the same Observation 8.12 that we return the right answer. □

Condition 1. Let $n, m \in \mathbb{N}$, then we say that they *compute standard numbers*, if they satisfy the following conditions where we WLOG assume that $n \leq m$, otherwise swap them.

- $2 \leq n, m$.
- $\forall k \in \mathbb{N}\ n^k \neq m$.
- If $l \in \mathbb{N}$ is the unique natural number s.t. $n^l < m < n^{l+1}$, then $m < 2 \times n^l$.

We will introduce a new notation that will be useful for us in the proof of Lemma 11.16.

Definition 11.1 ($L(n, x, l)$)**.** Assume that $M \models PA^-$, $x \in M$, $n, l \in \mathbb{N}$ and $1 \leq n$. Define,

$$L(n, x, l) := \begin{cases} \{x\} & l = 0, \\ \bigcup_{y \in L(q,x,r)} \{(\underline{n} \times y)^M, \ldots, ((\underline{n} \times y) + \underline{(n-1)})^M\} & l = r + 1. \end{cases}$$

Observation 11.12 (Properties of $L(n, x, l)$)**.** Let $M \models PA^-$, $x, y \in M$ s.t. $x \neq y$ and $n, l \in \mathbb{N}$ s.t. $1 \leq n$. Then the following holds.

(i) $L(n, x, l) = \{(\underline{n^l} \times x)^M, \ldots, ((\underline{n^l} \times x) + \underline{(n^l - 1)})^M\}$.

(ii) $|L(n,x,l)| = |L(n,y,l)| = n^l$.

(iii) $L(n,x,l) \cap L(n,y,l) = \emptyset$.

(iv) $\forall z, w \in L(n,x,l)\, \forall a \in M\ (M \models z \leq a \leq w \Rightarrow a \in L(n,x,l))$, i.e. that $L(n,x,l)$ is one continuous chunk of elements or equivalently said, it does not contain holes.

(v) If $\exists w \in L(n,x,l)\, \exists z \in L(n,y,l)$ s.t. $M \models w < z$, then $\forall a \in L(n,x,l)\, \forall b \in L(n,y,l)$ we have $M \models a < b$.

Proof. (i) Follows by induction on l, and that $\times, +$ behave reasonably in models of PA^-, especially with respect to standard elements, i.e. $\mathbb{N}^M$.

(ii) Follows by (i).

(iii) WLOG assume $M \models x < y$, then in the light of (i), it does suffice to show that $M \models \underline{n^l} \times x + \underline{(n^l - 1)} < \underline{n^l} \times y$. Since, $M \models x < y$ implies $M \models x + 1 \leq y$, the strict inequality we want to prove is obvious.

(iv) Follows by (i).

(v) Follows by (i) and (iii).

□

Observation 11.13 (Properties of $L(n,x,l)$ with respect to computability)**.** Let $M \models I\Sigma_1$, $dom(M) = \mathbb{N}$, x is some given element from M and $n, l \in \mathbb{N}$ s.t. $1 \leq n$. Furthermore, assume that $\text{div}\underline{n}$ is recursive with respect to M. Then we can compute $L(n,x,l)$.

Proof. We can obviously compute $L(n,x,0)$.

Furthermore, we can by Observation 11.11 inductively compute $L(n,x,r+1)$ from $L(n,x,r)$ for any $r \in \mathbb{N}$.

Hence, we can evidently compute $L(n,x,l)$. □

Definition 11.2 ($L_d(n,x,l,m)$)**.** Assume that $M \models I\Sigma_1$, $x \in M$ and $n, l, m \in \mathbb{N}$ s.t. $1 \leq n$. We define then the following.

$$L_d(n,x,l,m) := \{(z \text{ div } \underline{m})^M | z \in L(n,x,l)\}.$$

Observation 11.14 (Size of $L(n,x,l,m)$)**.** Let $M \models I\Sigma_1$, $x \in M$, $n, l, m \in \mathbb{N}$ s.t. $1 \leq n$ and $n^l < m$. Then $1 \leq |L_d(n,x,l,m)| \leq 2$.

Proof. The observation follows by (i) in Observation 11.12 and Observation 8.12. □

Definition 11.3 (Min and max in $L(n,x,l,m)$)**.** Let $M \models I\Sigma_1$, $n, l, m \in \mathbb{N}$ s.t. $1 \leq n$ and $n^l < m$. In the light of Observation 11.14 it makes sense talking about maximum and minimum element in $L_d(n,x,l,m)$ with respect to $<^M$. Therefore, we will denote them as $Max(L_d(n,x,l,m))$ and $Min(L_d(n,x,l,m))$ respectively.

Observation 11.15. Let $M \models I\Sigma_1$, $x, y \in M$, $n, l, m \in \mathbb{N}$ s.t. $1 \leq n, n^l < m$ and $m < 2 \times n^l$. Furthermore assume $x \neq y$. Then the following holds,

$$M \models x < y \iff M \models Min(L_d(n,x,l,m)) < Max(L_d(n,y,l,m)).$$

Proof. Let us denote $Min(L_d(n,x,l,m))$ as a and $Max(L_d(n,y,l,m))$ as b.

$\Rightarrow$: Assume that $M \models x < y$.

Then it means by div being monotone, for a proof see Observation 10.37, and by (i) in Observation 11.12 that $M \models \underline{n^l} \times x \text{ div } \underline{m} = a$ and $M \models (\underline{n^l} \times y + \underline{(n^l - 1)}) \text{ div } \underline{m} = b$.

Since, $M \models x < y$ we have $M \models \underline{n^l} \times x < \underline{n^l} \times y + \underline{(n^l - 1)}$, hence by Observation 10.37, $M \models a \leq b$.

Assume for contradiction that $M \models a = b$.

Therefore, by Observation 10.37 we get that for any $z \in M$ s.t. $M \models \underline{n^l} \times x \leq z \leq \underline{n^l} \times y + \underline{(n^l - 1)}$ we have $M \models z \text{ div } \underline{m} = a$.

But evidently by (i) in Observation 11.12 all the elements z from $L(n,x,l)$ and $L(n,y,l)$ satisfy that $M \models \underline{n^l} \times x \leq z \leq \underline{n^l} \times y + \underline{(n^l - 1)}$. Hence, for all the elements $z \in (L(n,x,l) \cup L(n,y,l))$ we have $M \models z \text{ div } \underline{m} = a$.

Recall that by (ii) and (iii) from Observation 11.12 $|L(n,y_i,l) \cup L(n,y_j,l)|$ equals $2 \times n^l$.

However, by Observation 8.12 we know that there are exactly m elements $z \in M$ s.t. $M \models z \text{ div } \underline{m} = a$. Therefore, $2 \times n^l \leq m$ which can not be by our assumption of $m < 2 \times n^l$, and thus we have arrived at a contradiction.

Therefore $a = b$ can not hold, hence, $M \models a < b$.

$\Leftarrow$: Assume that $M \models a < b$.

Then there exists $w \in L(n,x,l)$ and $z \in L(n,y,l)$ s.t. $M \models w \text{ div } \underline{m} = a$ and $M \models z \text{ div } \underline{m} = b$.

Since, $M \models a < b$ and $x \text{ div } \underline{m}$ is a monotone function with respect to x, we get that $M \models w < z$.

Therefore, by the last point in Observation 11.12, we get

$$\forall c \in L(n,x,l)\, \forall d \in L(n,y,l)\ M \models c < d.$$

But from this we can conclude that $M \models \underline{n^l} \times x < \underline{n^l} \times y$ which in turn implies $M \models x < y$.

□

And now, we can approach the main lemma of this section.

Lemma 11.16 (Pairs n, m which enable us to compute $\underline{k}$)**.** Let $M \models PA$, $dom(M) = \mathbb{N}$ and $n, m \in \mathbb{N}$ s.t. they *compute standard numbers*, i.e. they satisfy Condition 1.

Also let $l \in \mathbb{N}$ be the natural number from Condition 1 satisfying $n^l < m < n^{l+1}$.

Furthermore, assume that $\forall t \leq b_0\ \underline{t}^M = t$, where b_0 is the b_0 from Observation 11.10 when having n, m, l with the same interpretation as in here and $r_0, \ldots, r_l$ set to $n - 1$.

Lastly, assume that $\text{div}\underline{n}$ and $\text{div}\underline{m}$ are recursive with respect to M.

Then for any $k \in \mathbb{N}$ we can compute $\underline{k}^M$.

Proof. We will now present an evidently algorithmic procedure on how to compute $\underline{d}^M$, and possibly more, from knowing $0^M, \ldots, \underline{(d-1)}^M$ for $b_0 \leq (d-1)$.

If we manage to present such an algorithmic procedure, then, since we know by our assumption the interpretation of $\underline{t}^M$ for all $t \leq b_0$, it is obvious how to construct an algorithm for computing $\underline{k}^M$ for any $k \in \mathbb{N}$.

So, once again assume that we already know $0^M, \ldots, \underline{(d-1)}^M$ for $b_0 \leq (d-1)$ and we want to compute $\underline{d}^M$.

Algorithmic procedure.

Finding $\underline{d}^M, \ldots, \underline{(d+s)}^M$.

By Theorem 2.4, i.e. the theorem on unique quotients/remainders, there must exist $q_d, r_d \in M$ s.t. $M \models \underline{d} = q_d \times \underline{n} + r_d \wedge r_d < \underline{n}$.

Evidently, by Corollary 7.2, $M \models \underline{d} \text{ div } \underline{n} = q_d$. And by Observation 7.6 we also know that $M \models \underline{d} \text{ div } \underline{n} = \underline{d \text{ div } n}$. Hence $q_d = \underline{d \text{ div } n}^M$.

Since $\text{div}^{\mathbb{N}}$ is evidently a computable function, we can compute $d \text{ div }^{\mathbb{N}} n$, and if $d \text{ div }^{\mathbb{N}} n \leq d-1$, then we know how to interpret $\underline{d \text{ div } n}$ in M, hence, we know q_d. But since $2 \leq n$ and $b_0 \leq (d-1) < d$, we get that indeed $d \text{ div } n \leq d-1$, hence, we truly know how to find q_d.

Recall Observation 1.31 from which we know that $M \models r_d < \underline{n}$ implies $M \models r_d = 0^M \vee r_d = 1^M \vee \ldots \vee r_d = \underline{n-1}^M$.

Let us consider now $\underline{d}^M = (q_d \times \underline{n} + r_d)^M$, $\underline{d+1}^M = (q_d \times \underline{n} + (r_d + 1))^M$ up to $\underline{d+s}^M = (q_d \times \underline{n} + \underline{(n-1)})^M$, for some $s \in \mathbb{N}$, where if $r_d = \underline{i}^M$, then $s = n - 1 - i$.

Since we know q_d, as we have already noted, and how to compute $x \text{ div } \underline{n}$ with respect to M, we can by Observation 11.11 compute

$$(q_d \times \underline{n})^M, \ldots, \underline{d}^M, \ldots, (q_d \times \underline{n} + \underline{n-1})^M.$$

From being able to compute those elements, and from already knowing $0^M, \ldots, \underline{(d-1)}^M$, we can separate from them $\underline{d}^M, \ldots, \underline{d+s}^M$, hence, we can compute them.

Denote these computed elements as $y_0, \ldots, y_s$. Remember, that we do not know, at least for now, how to differentiate among them, e.g. we do not know whether $y_0 = \underline{d}^M \vee \ldots \vee y_0 = \underline{d+s}^M$. We have only computed some $y_0, \ldots, y_s \in M$ s.t. $\{y_0, \ldots, y_s\} = \{\underline{d}^M, \ldots, \underline{d+s}^M\}$.

Now, we will show how to differentiate among $y_0, \ldots, y_s$, i.e. to identify which one is which from $\underline{d}^M, \ldots, \underline{(d+s)}^M$. From that, it will immediately follow that we can compute any element from $\{\underline{d}^M, \ldots, \underline{d+s}^M\}$, hence, we can compute $\underline{d}^M$.

Differentiating among $y_0, \ldots, y_s$.

If $s = 0$, then we are clearly done, since $y_0 = \underline{d}^M = \ldots = \underline{d+s}^M$.

Otherwise assume $0 < s$.

By Observation 11.13 we can compute $L(n, y_0, l), \ldots, L(n, y_s, l)$, and so assume we did.

Now, we would like to show that for any $i \in [s]$, $\forall x \in L(n, y_i, l)$ we have $M \models x \text{ div } \underline{m} \leq \underline{(d-1)}$.

By (i) in Observation 11.12 and by Observation 10.37, i.e. div being monotone, it clearly does suffice to show that $M \models ((\underline{n^l} \times \underline{(d+s)}) + \underline{(n^l-1)}) \text{ div } \underline{m} < \underline{d}$.

Note that since $s \leq n-1$, then evidently

$$M \models ((\underline{n^l} \times \underline{(d+s)}) + \underline{(n^l-1)}) \leq$$
$$\underline{n} \times (\ldots(\underline{n} \times (\underline{d+n-1}) + \underline{n-1})\ldots) + \underline{(n-1)},$$

where the $n\times$ is repeated l times.

Therefore, by x div $\underline{m}$ being monotone, we have

$$M \models ((\underline{n^l} \times \underline{(d+s)}) + \underline{(n^l-1)}) \text{ div } \underline{m} \leq$$
$$(\underline{n} \times (\ldots(\underline{n} \times (\underline{d+n-1}) + \underline{n-1})\ldots) + \underline{(n-1)}) \text{ div } \underline{m}.$$

Hence, by the choice of b_0 and $b_0 \leq d$, we indeed must have

$$M \models ((\underline{n^l} \times \underline{(d+s)}) + \underline{(n^l-1)}) \text{ div } \underline{m} < \underline{d}.$$

Lastly, by Observation 1.29, we know that $((\underline{n^l} \times \underline{(d+s)}) + \underline{(n^l-1)}) \text{ div } \underline{m}$, is one of $0^M, \ldots, \underline{(d-1)}^M$, i.e. one of the expressions we know.

By the remarks we have just made, we get that for any $i \in [s]$, $L_d(n, y_i, l, m)$ is a subset $\{0^M, \ldots, \underline{(d-1)}^M\}$.

Since div $\underline{m}$ is computable, we can compute $L_d(n, y_i, l, m)$. Furthermore, by $L_d(n, y_i, l, m) \subseteq \{0^M, \ldots, \underline{(d-1)}^M\}$, it follows that we can algorithmically find such a $k, r \in \mathbb{N}$ s.t. $L_d(n, y_i, l, m) = \{\underline{k}^M, \underline{r}^M\}$.

To summarize.

- We can compute $y_0, \ldots, y_s$, s.t. $\{y_0, \ldots, y_s\} = \{\underline{d}^M, \ldots, \underline{(d+s)}^M\}$.
- Hence, we can compute for any $i \in [s]$ the set $L(n, y_i, l)$.
- Hence, we can compute for any $i \in [s]$ the set $L_d(n, y_i, l, m)$.
- Hence, we can compute $k, r \in \mathbb{N}$ s.t. $L_d(n, y_i, l, m) = \{\underline{k}^M, \underline{r}^M\}$,
- Furthermore, since $k <^{\mathbb{N}} r \iff M \models \underline{k} < \underline{r}$. we can compute such a $k, r \in \mathbb{N}$ s.t. $\underline{k}^M = Min(L_d(n, y_i, l, m))$ and $\underline{r}^M = Max(L_d(n, y_i, l, m))$.

Let $y_i \neq y_j$, where $i, j \in [s]$, and assume $\underline{k}^M = Min(L_d(n, y_i, l, m))$ and $\underline{r}^M = Max(L_d(n, y_j, l, m))$, where $k, r \in \mathbb{N}$.

Suppose, we manage to show that $M \models y_i < y_j \iff k <^{\mathbb{N}} r$.

Then, we will be able to computably compare elements from $\{y_0, \ldots, y_s\}$ with respect to $<^M$, also recall that $=^M$ is computable.

Furthermore, by Observation 1.29, we know that $M \models \underline{d} < \underline{d+1} < \ldots < \underline{d+s}$.

Lastly, since $<^M$ is a linear order on M, we can conclude that we will be able to tell which element from $\{y_0, \ldots, y_s\}$ is which from $\{\underline{d}^M, \ldots, (\underline{d+s})^M\}$. Hence, the proof as well as the loose description of an algorithmic procedure for finding $\underline{d}^M$ will be complete.

Since by Observation 1.29,

$$\begin{gathered} k <^{\mathbb{N}} r \iff M \models \underline{k} < \underline{r} \iff \\ M \models Min(L_d(n, y_i, l, m)) < Max(L_d(n, y_j, l, m)), \end{gathered} \tag{11.1}$$

we may conclude by Observation 11.15 that what we have supposed to hold indeed holds. And thus, the proof is finished.

□

After the proof was finished, we would like to make a few concluding commentaries with respect to Lemma 11.16.

Commentary. First note that if we are given $n, m \in \mathbb{N}$ satisfying Condition 1, then we can compute in $\mathbb{N}$ the value of l from Condition 1 and b_0 from the statement of Lemma 11.16. I.e. these values do not have to be given to us.

It is obvious for l. Since we have constructed b_0 in the proof of Observation 11.9 constructively, it follows that we can also compute in $\mathbb{N}$ the value of b_0.

Commentary. Notice that the assumption on having $\forall t \leq b_0\ \underline{t}^M = t$ is not that limiting.

It is because we know by Observation 3.13 that if there exists such a structure M satisfying every other assumption in Lemma 11.16 besides the just mentioned one, then there must exist one which satisfy all of the assumptions (in Lemma 11.16).

Commentary. Lastly, we would like to point out that the conditions in Condition 1 are not only *sufficient* but also *necessary* for *our* procedure of computing $\underline{n}^M$ to work. It is not that hard to observe it and thus we choose to omit a proof of it.

However, we would like to emphasize the word *our* in the preceding paragraph one more time. We do not claim that there can not be some other procedure that would enable us to compute $\underline{n}$ from some other pairs that do not satisfy the conditions in Condition 1.

Conclusion

Goals of the thesis

To quote a part of the bachelor thesis assignment, “Give a presentation of it and investigate related questions, such as how weak a theory of arithmetic can be used, or which aspects of the model can be made computable.” Where by “it” was meant the Tennenbaum’s theorem.

To summarize the mentioned goals.

(i) Give a presentation of the well known Tennenbaum’s theorem.

(ii) Investigate related questions, such as how weak a theory of arithmetic can be used, or

(iii) which aspects of the model can be made computable.

Naturally, two more sub-goals, besides a presentation of the Tennenbaum’s theorem, of (i) have emerged.

1. To give a sensible introduction to PA^-, PA, recursion theory and their respective parts like properties of standard/non-standard numbers, the Arithmetical hierarchy, Gödels lemma, Overspill lemma and many others. Optimally, in a way that would be understandable by someone who has went trough an introductory classes on mathematical logic and computability theory, e.g. like courses “Propositional and Predicate logic” and “Introduction to Complexity and Computability”, plus some introduction into the formalism of recursive functions, which are being taught at MFF CUNI.

2. To show, on the contrary to the Tennenbaum’s theorem, that not every non-trivial relation/function has to be non-recursive in a non-standard model of PA (with domain $\mathbb{N}$).

Fulfillment of the respective goals

(i) As for the first goal, with all of its sub-goals, we believe that we have managed to fulfill it.

Firstly, the presentation of the respective preliminaries is a rather thorough one so that someone who has not seen PA yet will not get lost. And almost the same goes for preliminaries from the recursion/computability theory.

Secondly, we have presented Tennenbaum’s theorem for $+$ not only for PA but also for a weaker theory $I\Delta_0$, which is due to K. McAloon. Whereas the presentation for $\times$ was done for models of PA. Moreover, the proof was done in a quite detailed fashion. We want to highlight that we have showed Tennenbaum’s theorem for $\times$ because it is not rare that in expository proofs that can be found only the version for $+$ is proved, and is often proved using a standard theorem on unique quotients remainders which does not have much of analogy for the case of $\times$.

Furthermore, a thing that appears under the hood of many proofs related to proving Tennenbaum-like results, is representing the n-th prime function in PA^-. In this text, namely in section 3.3, we have showed that the function in mention can be in a certain way, sufficient to our needs, represented by a Δ_0 formula. Showing such a representation by a Δ_0 formula does not seem to us to be found in other expository proofs of Tennnebaum's theorem that we have delved into.

Lastly, we have presented a relatively detailed proof of the order-type of models of $I\Delta_0$ together with a corollary that there exists a non-standard model of PA with domain $\mathbb{N}$ with recursive $<$ and $S(x)$. This result was presented not only to show that non-trivial functions/relations can be recursive in non-standard models, but they were also of use to us in PART II.

Therefore, and furthermore, we hope that PART I of this work is accessible to anyone with a basic knowledge of mathematical logic and computability theory. Hence, for a *complete beginner* to the topic, it might be even a place to learn a little about PA and its weaker fragments, Tennenbaum's theorem and order-type of models of arithmetic.

(ii) A one think that we did in PART I, related to how a weak theory can be to still have the Tennenbaum phenomena, was that we tried to put some emphasis on presenting Tennenbaum's theorem for $+$, as well as the inspection of the order-type, in a relatively weak fragment of PA, namely $I\Delta_0$, or to be even more precise in PA^- with Overspill for $\mathbb{N}$ on Δ_0 formulas.

Furthermore, we have added throughout the text, both in PART I and PART II, various comments.

But in general, we chose not to pursue this goal in a greater depth.

(iii) We chose to investigate recursiveness of x div y and x mod y.

Before we list most of the results that we came across (and solved), we want to state the following. As far as our current knowledge on the research in the topic goes, the upcoming results have not been published in some other work, survey or paper. And the same goes for some, more elaborate, discussion of the recursiveness of the functions div and mod in non-standard models of PA. An exception to what has been just written are some weaker versions of results mentioned in the upcoming list. Namely, in Yaegasi [2008] the author of that article proves points (b) and (d) for $k = 2$, and we show it for any $2 \leq k$.

(a) In Corollary 8.7, we show that there is a non-standard model of PA with all x div $\underline{0}$, x div $\underline{1}$, x mod $\underline{0}$ and x mod $\underline{1}$ recursive with respect to it.

(b) In Lemma 8.11, we show that there can be no non-standard model of PA s.t. x mod $\underline{k}$ and x div $\underline{k}$ are both recursive with respect to it.

(c) In Corollary 8.15, we show that there can be no non-standard model of PA with both the x div $\underline{k}$, for $2 \leq k$, and the successor function recursive with respect to it. And an analogous result has been shown for x div $\underline{k}$, for $2 \leq k$, and the order relation, $<$, in Corollary 8.17.

(d) In Corollary 8.18, we show that the the unary functions $\underline{k} \times x$, $\underline{k} \times x + 1$,...,$\underline{k} \times x + \underline{(k-1)}$ can not be recursive all at once in a non-standard model of PA.

(e) In Corollary 9.7, we show that for any finite subset F of $\mathbb{N}$ there exists a non-standard model of PA s.t. all the functions x mod $\underline{k}$, for $k \in F$, together with $<$ and the successor function are recursive with respect to it.

(f) In Lemma 11.6, we show that there can be no non-standard model of $I\Sigma_1$ with x div y recursive.

(g) In Lemma 11.8, we show that that for any $k \in \mathbb{N}$ there exists a non-standard model of PA with x div $\underline{k}^l$, for every $l \in \mathbb{N}$, recursive with respect to it.

(h) One miscellaneous lemma in section 11.3, namely Lemma 11.16, witnesses pairs of natural numbers n, m which enable us to compute $\underline{k}$ in some respective model assuming that x div $\underline{n}$ and x div $\underline{m}$ are recursive in that model in mention.

(i) Lastly, we have inspected in chapter 10 the structure of $(M, \text{div } \underline{k})$, see namely Theorem 10.50 or Corollary 10.51, for $2 \leq k$, where $M \models PA$. The inspection was conducted in the same spirit as the inspection of the order-type in chapter 6.

One thing is that the investigation in mention helped us to show that x div $\underline{k}$ can be recursive in a non-standard model of PA.

And secondly, the result on its own is of its own beauty and importance, as far as our subjective view goes.

We hope that PART II gave some insight on how the functions div and mod behave with respect to their recursiveness in models of PA or $I\Sigma_1$.

As argued, we believe that we have fulfilled the mentioned goals to a sufficient extent.

Problems that remained unsolved (and are of interest to us)

A great amount of problems related to the recursiveness of x div y and x mod y in non-standard models of PA, or some weaker theories like $I\Sigma_1$, that we have not solved can be listed.

There are three problems that arose to us in a quite natural way, and are also of interest to us. We have already mentioned them throughout the text as Problem 1, Problem 2 and Problem 3 in section 9.1, section 9.2 and section 11.3 respectively. Nevertheless, we mention them here one more time concluding this text.

Problem 1 (Classification of when can be mod$\underline{k}$, for all $k \in F \subseteq \mathbb{N}$, recursive)**.** Classify exactly for which sets $F \subseteq \mathbb{N}$ there exists a non-standard model of PA, or $I\Sigma_1$, with domain $\mathbb{N}$ s.t. mod$\underline{k}$, for every $k \in F$, is recursive with respect to it.

Problem 2 (Can x mod y be recursive?)**.** Does there exist a non-standard model of PA, or $I\Sigma_1$, s.t. the binary function x mod y is recursive with respect to it?

In regard to Problem 2, at the beginning of our investigations we were quite convinced that there can be no such non-standard model. To some extent, we still believe it a tiny bit more than the opposite. On the other hand, since we have failed in our thought experiments many times to show that there can be no such non-standard model, we definitely do not rule out the possibility that there can be indeed such a non-standard model.

Problem 3 (Classification of when can be div$\underline{k}$, for all $k \in F \subseteq \mathbb{N}$, recursive)**.** Classify exactly for which sets $F \subseteq \mathbb{N}$ there exists a non-standard model of PA, or $I\Sigma_1$, with domain $\mathbb{N}$ s.t. div$\underline{k}$, for every $k \in F$, is recursive with respect to it.

A. Computable bijections

Commentary. Please notice that every considered bijection, alongside with its inverse, is at least intuitively computable. And when we reasonably represent domain and range of the respective bijections in $\mathbb{N}$ they would be even recursive.

Therefore also theirs finite addition, composition, etc., when respecting their domains/ranges, produce bijections that are again computable, as well as their inverses.

Commentary. All of the considered computable bijections are standard ones e.g. the standard Cantor's Zig-Zag bijection between $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$, see e.g. Boolos et al. [2007, p. 7, Example 1.2], and/or it is hopefully evident from the definition of the just being considered function that it is indeed a bijection between the given two sets in consideration. Therefore we have chosen to omit (full) proofs of why the functions are indeed bijective.

Bijection 1 (Bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$)**.** By $I_{\mathbb{N}\times\mathbb{N}\leftrightarrow\mathbb{N}}$ we will denote a standard bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$. The definition follows.

$$I_{\mathbb{N}\times\mathbb{N}\leftrightarrow\mathbb{N}}(m,n) \coloneqq 1+2+\ldots+(m+n)+(m+1) = \frac{(m+n)\times(m+n+1)}{2}+m+1,$$

which is obviously computable.

The 1 is for the number of pairs (k,l) s.t. $k+l=0$. The 2 is for the number of pairs (k,l) s.t. $k+l=1$. The $(m+n)$ is for the number of pairs (k,l) s.t. $k+l=m+n-1$ and lastly $m+1$ is for the first part of the ordered pair (m,n) with added 1.

Clearly $\forall m,n \in \mathbb{N}$ we have $m,n \leq I_{\mathbb{N}\times\mathbb{N}\leftrightarrow\mathbb{N}}(m,n)$ and hence is $I_{\mathbb{N}\leftrightarrow\mathbb{N}\times\mathbb{N}} \coloneqq I^{-1}_{\mathbb{N}\times\mathbb{N}\leftrightarrow\mathbb{N}}$ computable as well.

Bijection 2 (Bijection between $\mathbb{N}$ and $\mathbb{Z}$)**.** By $I_{\mathbb{N}\leftrightarrow\mathbb{Z}}$ we will denote a bijection between $\mathbb{N}$ and $\mathbb{Z}$. The definition follows.

$$I_{\mathbb{N}\leftrightarrow\mathbb{Z}}(n) \coloneqq (-1)^n \times ((n+1) \text{ div } 2),$$

which is obviously computable.

And when we define $I_{\mathbb{Z}\leftrightarrow\mathbb{N}} \coloneqq I^{-1}_{\mathbb{N}\leftrightarrow\mathbb{Z}}$ we can observe that actually the following holds.

$$I_{\mathbb{Z}\leftrightarrow\mathbb{N}}(k) = \begin{cases} 2\times k & k \geq 0, \\ (2\times(-k))-1 & k < 0. \end{cases}$$

And hence is $I_{\mathbb{Z}\leftrightarrow\mathbb{N}}$ also computable.

Commentary. For the next bijection, let us recall that by $p(n)$ we mean $(n+1)$-th prime number. Where, as we have observed in Observation 3.9, is $p(n)$ computable. And it is not hard to observe that also the prime decomposition of any number m is computable.

Since obviously if $p(m) \mid m$ then $p(m) \leq m$ and also $p(n) < p(n+1)$ we can easily compute all the finitely many primes that can possibly be in a prime decomposition of m.

And from that, since computing div and mod is obviously computable, and also from $x \text{ div } p(m) < x$ for any positive natural number we can evidently find m's prime decomposition in finite time.

Bijection 3 (Bijection between $\mathbb{Z}$ and $\mathbb{Q}$)**.** By $I_{\mathbb{Z}\leftrightarrow\mathbb{Q}}$ we will denote a bijection between $\mathbb{Z}$ and $\mathbb{Q}$. The definition follows.

$$I_{\mathbb{Z}\leftrightarrow\mathbb{Q}}(k) = \begin{cases} p(0)^{I_{\mathbb{N}\leftrightarrow\mathbb{Z}}(l_0)} \times \cdots \times p(s)^{I_{\mathbb{N}\leftrightarrow\mathbb{Z}}(l_s)} & k > 0 \wedge k = p(0)^{l_0} \dots p(s)^{l_s}, \\ 0 & k = 0, \\ -p(0)^{I_{\mathbb{N}\leftrightarrow\mathbb{Z}}(l_0)} \times \cdots \times p(s)^{I_{\mathbb{N}\leftrightarrow\mathbb{Z}}(l_s)} & k < 0 \wedge -k = p(0)^{l_0} \dots p(s)^{l_s}. \end{cases}$$

Let us note that in case $k = 1$ or $k = -1$ is $p(0)^{l_0} \dots p(s)^{l_s}$, and $p(0)^{I_{\mathbb{N}\leftrightarrow\mathbb{Z}}(l_0)} \times \cdots \times p(s)^{I_{\mathbb{N}\leftrightarrow\mathbb{Z}}(l_s)}$ as well as the minus versions of them an empty product, hence equal to 1 and -1 respectively.

By the commentary which preceded definition of this function and the fact that $I_{\mathbb{N}\leftrightarrow\mathbb{Z}}$ is computable, it is obvious that $I_{\mathbb{Z}\leftrightarrow\mathbb{Q}}$ is indeed computable.

And since $I_{\mathbb{N}\leftrightarrow\mathbb{Z}}$ is a bijection from $\mathbb{N}$ onto $\mathbb{Z}$ it is not that hard to see that $I_{\mathbb{Z}\leftrightarrow\mathbb{Q}}$ is indeed a bijection from $\mathbb{Z}$ onto $\mathbb{Q}$.

Let us define $I_{\mathbb{Q}\leftrightarrow\mathbb{Z}} \coloneqq I^{-1}_{\mathbb{Z}\leftrightarrow\mathbb{Q}}$, therefore $I_{\mathbb{Q}\leftrightarrow\mathbb{Z}}$ is a bijection from $\mathbb{Q}$ onto $\mathbb{Z}$, and observe the following where m and n do not have a common divisor except for 1.

$$I_{\mathbb{Q}\leftrightarrow\mathbb{Z}}(q) = \begin{cases} p(0)^{I_{\mathbb{Z}\leftrightarrow\mathbb{N}}(l_0)} \times \cdots \times p(s)^{I_{\mathbb{Z}\leftrightarrow\mathbb{N}}(l_s)} \times p(0)^{I_{\mathbb{Z}\leftrightarrow\mathbb{N}}(l_0)} \times \cdots \times p(t)^{I_{\mathbb{Z}\leftrightarrow\mathbb{N}}(l_t)} \\ \qquad \text{where } q > 0 \wedge q = m/n \wedge \\ \qquad |m| = p(0)^{l_0} \dots p(s)^{l_s} \wedge |n| = p(0)^{l_0} \dots p(t)^{l_t}, \\ 0 \qquad q = 0, \\ -p(0)^{I_{\mathbb{Z}\leftrightarrow\mathbb{N}}(l_0)} \times \cdots \times p(s)^{I_{\mathbb{Z}\leftrightarrow\mathbb{N}}(l_s)} \times p(0)^{I_{\mathbb{Z}\leftrightarrow\mathbb{N}}(l_0)} \times \cdots \times p(t)^{I_{\mathbb{Z}\leftrightarrow\mathbb{N}}(l_t)} \\ \qquad \text{where } q < 0 \wedge q = m/n \wedge \\ \qquad |m| = p(0)^{l_0} \dots p(s)^{l_s} \wedge |n| = p(0)^{l_0} \dots p(t)^{l_t}. \end{cases}$$

Please note, that if m and n have no common divisors, besides 1, and $q = m/n$, then (m, n) are uniquely determined, up to the minus sign. Also note that $I_{\mathbb{Z}\leftrightarrow\mathbb{N}}$ is a well defined bijection from $\mathbb{Z}$ onto $\mathbb{N}$, hence it is easy to understand that the equality actually holds.

If $q \in \mathbb{Q}$, and we represent q as some pair (r, l) s.t. $q = (r, l)$, then it is obviously easy to algorithmically find a pair (m, n) s.t. they m and n are co-prime. Simply enumerate $i \in \{1, \dots, m\}$, starting with $i = m$ and going downwards, and if $m \bmod i = n \bmod i = 0$, then we set $m \coloneqq m \text{ div } i$ as well as $n \coloneqq n \text{ div } i$ and we can end the procedure. Hence $I_{\mathbb{Q}\leftrightarrow\mathbb{Z}}$ is also computable.

Bijection 4 (Bijection between $\mathbb{N}$ and $\mathbb{Q}$)**.** By $I_{\mathbb{N}\leftrightarrow\mathbb{Q}}$ we will denote a bijection from $\mathbb{N}$ onto $\mathbb{Q}$. The definition is,

$$I_{\mathbb{N}\leftrightarrow\mathbb{Q}}(n) \coloneqq I_{\mathbb{Z}\leftrightarrow\mathbb{Q}}(I_{\mathbb{N}\leftrightarrow\mathbb{Z}}(n)).$$

$I_{\mathbb{N}\leftrightarrow\mathbb{Q}}$ is obviously a valid bijection from $\mathbb{N}$ onto $\mathbb{Q}$.

Define $I_{\mathbb{Q}\leftrightarrow\mathbb{N}} \coloneqq I^{-1}_{\mathbb{N}\leftrightarrow\mathbb{Q}}$.

Moreover, since $I_{\mathbb{Z}\leftrightarrow\mathbb{Q}}$ and $I_{\mathbb{N}\leftrightarrow\mathbb{Z}}$ are computable, as are also their inverses, then $I_{\mathbb{N}\leftrightarrow\mathbb{Q}}$ as well as $I^{-1}_{\mathbb{N}\leftrightarrow\mathbb{Q}} = I_{\mathbb{Q}\leftrightarrow\mathbb{N}}$ are also computable.

Bijection 5 (Bijection between $\mathbb{N}$ and $\mathbb{N} \cup (\mathbb{Q} \times \mathbb{Z})$)**.** By $I_{\mathbb{N}\leftrightarrow N\cup(\mathbb{Q}\times\mathbb{Z})}$ we will denote a bijection from $\mathbb{N}$ onto $\mathbb{N} \cup (\mathbb{Q} \times \mathbb{Z})$. The definition follows.

$$I_{\mathbb{N}\leftrightarrow\mathbb{N}\cup(\mathbb{Q}\times\mathbb{Z})}(n) := \begin{cases} n & I_{\mathbb{N}\leftrightarrow\mathbb{N}\times\mathbb{Z}}(n) = (0, k), \\ (I_{N\leftrightarrow\mathbb{Q}}(l-1), I_{\mathbb{N}\leftrightarrow\mathbb{Z}}(k)) & I_{\mathbb{N}\leftrightarrow\mathbb{N}\times\mathbb{N}}(n) = (l, k) \wedge l > 0. \end{cases}$$

$I_{\mathbb{N}\leftrightarrow\mathbb{N}\cup(\mathbb{Q}\times\mathbb{Z})}(n)$ is clearly a bijection with domain $\mathbb{N}$ and range $\mathbb{N} \cup (\mathbb{Q} \times \mathbb{Z})$.
Define $I_{\mathbb{N}\cup(\mathbb{Q}\times\mathbb{Z})\leftrightarrow\mathbb{N}} := I^{-1}_{\mathbb{N}\leftrightarrow\mathbb{N}\cup(\mathbb{Q}\times\mathbb{Z})}$.

Since $I_{\mathbb{N}\leftrightarrow\mathbb{N}\times\mathbb{Z}}$ is computable as well as its inverse, we get that $I_{\mathbb{N}\leftrightarrow\mathbb{N}\cup(\mathbb{Q}\times\mathbb{Z})}$ is computable as well as its inverse.

Bijection 6 (Bijection between $\mathbb{N}$ and $\mathbb{N}^k$)**.** For a positive integer k, we will denote by $I_{\mathbb{N}\leftrightarrow\mathbb{N}^k}$ a bijection from $\mathbb{N}$ onto $\mathbb{N}^k$. The definition will be recursive with respect k.

Also let us note that if two sets are identical, e.g. $\mathbb{N}^2$ and $\mathbb{N} \times \mathbb{N}$, then by $I_{\mathbb{N}\leftrightarrow\mathbb{N}^2}$ we will mean exactly the same function as by $I_{\mathbb{N}\leftrightarrow\mathbb{N}\times\mathbb{N}}$

$k = 1$ $I_{\mathbb{N}\leftrightarrow\mathbb{N}}(n) := n$, this function is clearly the wanted bijection and is, as well as its, inverse computable.

$k = 2$ $I_{\mathbb{N}\leftrightarrow\mathbb{N}^2}$ was already defined as $I_{\mathbb{N}\leftrightarrow\mathbb{N}\times\mathbb{N}}$ in Bijection 1.

By the discussion in Bijection 1, we know that $I_{\mathbb{N}\leftrightarrow\mathbb{N}^2}$ is the desired computable bijection which has also its inverse computable.

$k \geq 3$

$$I_{\mathbb{N}\leftrightarrow\mathbb{N}^k} := (I_{\mathbb{N}\leftrightarrow\mathbb{N}^{(k-1)}}(m), l), \text{ where } I_{\mathbb{N}\leftrightarrow\mathbb{N}^2}(n) = (m, l).$$

Evidently, $I_{\mathbb{N}\leftrightarrow\mathbb{N}^k}$ is a bijection from $\mathbb{N}$ onto $\mathbb{N}^k$.

Since we can assume that $I_{\mathbb{N}\leftrightarrow\mathbb{N}^{(k-1)}}$ and $I_{\mathbb{N}\leftrightarrow\mathbb{N}^2}$ are computable bijections which have also computable inverses, we have that $I_{\mathbb{N}\leftrightarrow\mathbb{N}^k}$ and its inverse are computable.

Define, as usual, also the following $I_{\mathbb{N}^k\leftrightarrow\mathbb{N}} := I^{-1}_{\mathbb{N}\leftrightarrow\mathbb{N}^k}$.

Bijection 7 (Bijection between $\mathbb{N}$ and $\mathbb{N} \times [k]$)**.** For $k \in \mathbb{N}$, we will denote by $I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[k]}$ a bijection from $\mathbb{N}$ onto $\mathbb{N} \times [k]$.

The definition will be recursive with respect k.

$k = 0$ $I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[0]}(n) := (n, 0)$, this function is clearly the wanted bijection and is as well as its inverse computable.

$k = 1$ $I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[1]} := (n \text{ div } 2, n \bmod 2)$.

$I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[1]}$ is obviously a bijection from $\mathbb{N}$ onto $\mathbb{N} \times [1]$.

Since div and mod are evidently computable so is $I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[1]}$.

Continuing, since $2 \times m$ and $m + 1$ are again evidently computable we get that $I^{-1}_{\mathbb{N}\leftrightarrow\mathbb{N}\times[1]}$ is computable as well.

$k \geq 2$

$$I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[k]}(n) \coloneqq \begin{cases} (m,0) & I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[1]}(n) = (m,0), \\ (l, r+1) & I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[1]}(n) = (m,1) \wedge I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[(k-1)]}(m) = (l,r). \end{cases}$$

Clearly, $I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[k]}$ is a bijection from $\mathbb{N}$ onto $\mathbb{N}\times[k]$.

And since we can assume that $I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[l]}$ is computable for any $l \in \mathbb{N}$ s.t. $l < k$, and has computable inverse, we can conclude that $I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[k]}$ and its inverse are computable.

As usual define $I_{\mathbb{N}\times[k]\leftrightarrow\mathbb{N}} \coloneqq I^{-1}_{\mathbb{N}\leftrightarrow\mathbb{N}\times[k]}$.

Bijection 8 (Bijection between $\mathbb{N}$ and $\mathbb{N}\cup(\mathbb{N}\times\mathbb{Z}\times\mathbb{N}\times[1])\cup(\mathbb{N}\times\mathbb{Z}\times\mathbb{Z}\times\{2\})$)**.** Let us denote by A the syntactical expression $\mathbb{N}\cup(\mathbb{N}\times\mathbb{Z}\times\mathbb{N}\times[1])\cup(\mathbb{N}\times\mathbb{Z}\times\mathbb{Z}\times\{2\})$.

We will define,

$$I_{\mathbb{N}\leftrightarrow A}(n) \coloneqq \begin{cases} m & I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[3]}(n) = (m,0), \\ (a, I_{\mathbb{N}\leftrightarrow\mathbb{Z}}(b), c, l-1) & I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[3]}(n) = (m,l) \wedge 1 \leq l \leq 2 \wedge \\ & I_{\mathbb{N}\leftrightarrow\mathbb{N}^3}(m) = (a,b,c), \\ (a, I_{\mathbb{N}\leftrightarrow\mathbb{Z}}(b), I_{\mathbb{N}\leftrightarrow\mathbb{Z}}(c), 2) & I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[3]}(n) = (m,3) \wedge \\ & I_{\mathbb{N}\leftrightarrow\mathbb{N}^3}(m) = (a,b,c). \end{cases}$$

Clearly, $I_{\mathbb{N}\leftrightarrow A}$ is a bijection from $\mathbb{N}$ onto A.

Define $I_{A\leftrightarrow\mathbb{N}} \coloneqq I^{-1}_{\mathbb{N}\leftrightarrow A}$.

Since $I_{\mathbb{N}\leftrightarrow\mathbb{N}\times[3]}$, $I_{\mathbb{N}\leftrightarrow\mathbb{Z}}$ and $I_{\mathbb{N}\leftrightarrow\mathbb{N}^3}$ and their inverses are computable, it is evident that $I_{\mathbb{N}\leftrightarrow A}$ and $I_{A\leftrightarrow\mathbb{N}}$ are also computable bijections.

Bibliography

Alessandro Berarducci and Margarita Otero. A recursive nonstandard model of normal open induction. *The Journal of Symbolic Logic*, 61(4):1228–1241, 1996. ISSN 00224812. URL `http://www.jstor.org/stable/2275813`.

G.S. Boolos, J.P. Burgess, and R.C. Jeffrey. *Computability and Logic*. Cambridge University Press, 2007.

I. Chiswell and W. Hodges. *Mathematical Logic*. Oxford Texts in Logic. OUP Oxford, 2007.

Paola D'Aquino. Toward the limits of the tennenbaum phenomenon. *Notre Dame Journal of Formal Logic*, 38(1):81–92, 1997. doi: 10.1305/ndjfl/1039700698.

H.B. Enderton. *Elements of Set Theory*. Elsevier Science, 1977.

Michał Tomasz Godziszewski and Joel David Hamkins. Computable quotient presentations of models of arithmetic and set theory. In Juliette Kennedy and Ruy J.G.B. de Queiroz, editors, *Logic, Language, Information, and Computation*, pages 140–152, Berlin, Heidelberg, 2017. Springer Berlin Heidelberg. ISBN 978-3-662-55386-2.

Kurt Gödel. *Über die Vollständigkeit des Logikkalküls*. PhD thesis, University of Vienna, 1929.

Emil Jeřábek, April 2015. URL `https://mathoverflow.net/questions/201764/divisible-by-all-standard-prime-numbers`. Accessed:11.1.2024; an answer at mathoverflow.

R. Kaye. *Models of Peano Arithmetic*. Oxford logic guides. Clarendon Press, 1991.

Richard Kaye. Diophantine induction. *Annals of Pure and Applied Logic*, 46 (1):1–40, 1990. ISSN 0168-0072. doi: https://doi.org/10.1016/0168-0072(90)90076-E. URL `https://www.sciencedirect.com/science/article/pii/016800729090076E`.

Richard Kaye. *Tennenbaum's theorem for models of arithmetic*, page 66–79. Lecture Notes in Logic. Cambridge University Press, 2011.

J. Kirby. *An Invitation to Model Theory*. Cambridge University Press, 2019.

Kenneth McAloon. On the complexity of models of arithmetic. *Journal of Symbolic Logic*, 47(2):403–415, 1982. doi: 10.2307/2273150.

Fedor Pakhomov. How to escape tennenbaum's theorem. 2022. arXiv:2209.00967 [math.Lo].

Giuseppe Peano. *Arithmetices Principia Novo Methodo Exposita*. Bocca, 1889.

C.C. Pinter. *A Book of Abstract Algebra: Second Edition*. Dover Publications, 2012.

Barkley Rosser. Extensions of some theorems of gödel and church. *The Journal of Symbolic Logic*, 1(3):87–91, 1936. ISSN 00224812. URL `http://www.jstor.org/stable/2269028`.

James H. Schmerl. Recursive models and the divisibility poset. *Notre Dame Journal of Formal Logic*, 39(1):140–148, 1998. doi: 10.1305/ndjfl/1039293026.

J. C. Shepherdson. A non-standard model for a free variable fragment of number theory. *Bulletin de l'Académie Polonaise des Sciences, Série des sciences mathématiques, astronomiques et physiques*, 12:79–86, 1964.

Peter Smith. Tennenbaum's theorem, 2014. URL `https://www.logicmatters.net/resources/pdfs/tennenbaum_new.pdf`. Accessed: 14.12.2023, lecture notes.

Stanley Tennenbaum. Non-archimedean models for arithmetic. *Notices of the American Mathematical Society*, 6(270):44, 1959.

J. van Heijenoort. *From Frege to Gödel: A Source Book in Mathematical Logic, 1879–1931.* Source Books in the History of the Sciences. Harvard University Press, 1967.

George Wilmers. Bounded existential induction. *The Journal of Symbolic Logic*, 50(1):72–90, 1985. ISSN 00224812. URL `http://www.jstor.org/stable/2273790`.

Sakae Yaegasi. Tennenbaum's Theorem and Unary Functions. *Notre Dame Journal of Formal Logic*, 49(2):177 – 183, 2008. doi: 10.1215/00294527-2008-006. URL `https://doi.org/10.1215/00294527-2008-006`.