FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

MASTER THESIS

Mykyta Narusevych

Models of bounded arithmetic

Department of Algebra

Supervisor of the master thesis: prof. RNDr. Jan Krajíček, DrSc.
Study programme: Mathematics
Study branch: Mathematical Structures

Prague 2022

I declare that I carried out this master 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 dedicate this thesis to my parents and my wife for their support and help. I also want to thank my supervisor Jan Krajíček for the time he spent providing valuable comments and helping me with answering many questions.

Finally, I want to thank the whole Charles University where I have met wonderful people and gained all my knowledge of mathematics. I hope to continue the path I have chosen and to push the boundary of human knowledge a little bit further.

Title: Models of bounded arithmetic

Author: Mykyta Narusevych

Department: Department of Algebra

Supervisor: prof. RNDr. Jan Krajíček, DrSc., Department of Algebra

Abstract: We study mutual relations of various versions of the pigeonhole principle over bounded arithmetic theory $T^1_2(R)$. The main two variants are the ordinary $PHP^{n+1}_n(R)$, formalizing that R is not the graph of an injective function from $[n+1]$ into $[n]$, and its weak version, $WPHP^{2m}_m(S)$, formalizing that S is not the graph of an injective function from $[2m]$ into $[m]$. It is known that $T^1_2(R)$ does not prove $PHP^{n+1}_n(R)$. We generalize this proof to show directly that the theory $T^1_2(R)$ plus $\forall m\, WPHP^{2m}_m(\Box^p_1(R))$ does not prove $PHP^{n+1}_n(R)$ (where $\Box^p_1(R)$ denotes relations polynomial-time definable from R). This already follows from the known facts of the area, however, our direct proof is simpler and allows us to prove a partial result towards an open problem mentioned by M. Ajtai (1990).

Keywords: bounded arithmetic, pigeonhole principle, forcing

Název: Modely omezené aritmetiky

Řešitel: Mykyta Narusevych

Katedra: Katedra Algebry

Vedoucí: prof. RNDr. Jan Krajíček, DrSc., Katedra Agebry

Abstrakt: Práce zkoumá vzájemné vztahy různých verzí zásuvkového principu (též princip holubníku) nad teorií omezené aritmetiky $T^1_2(R)$. Základní dvě varianty jsou obyčejný $PHP^{n+1}_n(R)$, formalizující že R není grafem injektivní funkce z $[n+1]$ do $[n]$, a jeho slabší verze, $WPHP^{2m}_m(S)$, formalizující že S není grafem injektivní funkce z $[2m]$ do $[m]$. Je známo, že teorie $T^1_2(R)$ nedokazuje $PHP^{n+1}_n(R)$. Práce zobecňuje známe metody a ukazuje, že teorie $T^1_2(R)$ plus $\forall m\, WPHP^{2m}_m(\Box^p_1(R))$ nedokazuje $PHP^{n+1}_n(R)$ (kde $\Box^p_1(R)$ označuje relace polynomiálně definovatelné z R). Plyne to z již známých faktů, náš důkaz je ale elementárnější a umožňuje nám dokázat částečný výsledek směrem k otevřenému problému, který zmínil M. Ajtai (1990).

Klíčová slova: omezená aritmetika, zásuvkový princip, princip holubníku, forsing

Contents

Introduction

One of the biggest theoretical advancements of the previous century is the notion of *computability.* Trying to understand what does it mean for a problem to be algorithmically solvable, mathematicians developed concepts like *Turing machine* (Turing [1936]) and *λ-calculus* (Church [1932]). According to the now famous *Church-Turing thesis* (Kleene [1952]), these mathematical definitions fully grasp our intuitive understanding of an algorithm. The formal capture of this intuition provided mathematicians a way to prove many deep and surprising results concerning computability, e.g. Turing's theorem on *undecidability of the halting problem* (Turing [1936]), Church's theorem on *unsolvability of the Entscheidungsproblem* (Church [1936]). Early results from the theory of computations also provided an alternative way to prove the famous Gödel's *incompleteness theorems* (Kleene [1943]). Then, following theoretical advances, computers were invented.

Further into the twentieth century it started to become apparent that computable does not mean *feasible.* If the problem can be algorithmically solved, but the algorithm must run for a time longer than the age of our universe, then it is clear that we can not say such a problem is solvable feasibly. Restrictions on time and space started to play a major role both theoretically and practically. These reflections resulted in the development of the *polynomial-time computability*, which is now being a universally accepted synonym (with variants allowing randomization) of the feasible computation (Cobham [1965]).

Throughout the dramatic advances of computer science, mathematical logic has always served as a main theoretical framework and a tool to achieve these results. Of particular interest are relations between *computability classes* and *arithmetic formulas.* For example, Post's theorem established a correspondence between *arithmetic hierarchy* and *Turing degrees* (Rogers [1967]).

The main object of study of this thesis is the *bounded arithmetic* firstly defined by Buss [1985]. It was developed as a possible candidate for being the formalization of a *feasible reasoning* (see Krajíček [1995] for the history of these developments). As we will explain below, there are various connections between *weak fragments* of bounded arithmetic and computational classes with some restrictions on time and space. Our work focuses on mutual unprovability of various *pigeonhole principles* over bounded arithmetic. The reasons to study provability of combinatorial statements inside the weak fragments are plenty. For example, such proofs can be translated into short propositional proofs in some *proofs systems* (Krajíček [2019][10.5.1]), or may provide efficient *witnesses* to certain algorithmical problems (Krajíček [1995][7.2.3]). Although interesting, the formal treatment of this connections is beyond the scope of the thesis.

We assume the reader has background in mathematical logic. We also assume some basic understanding of complexity theory, although we will not utilize any deep results, besides some basic definitions.

Section 1.1 formulates various arithmetic theories and mentions their connection to complexity theory. This area contains many deep and profound results, although none of them are proved in this thesis. We also spend a little time describing *coding of sequences* in the arithmetic theories.

Section 1.2 introduces the reader to the pigeonhole principle. The main theorem of the thesis is also stated in this section.

Section 2.1 is devoted to the proof of the theorem of Paris and Wilkie [1985], which serves as a first step towards the main goal of the thesis.

Section 2.2 studies *forcing*. We prove some basic properties and, using this new language, give a new proof of the theorem from the previous section. All the statements of this chapter are already known, although we still provide all the proofs, since it is important to understand the technicalities for the main theorem.

Section 2.3 contains the proof of an easier variant of the main theorem. We utilize forcing together with certain combinatorial arguments to show unprovability of the bijective pigeonhole principle in the weak arithmetic theory $I\exists_1$ augmented by instances of the *weak pigeonhol principle* for *open formulas*.

Section 3.1 provides a proof of a modification of the theorem of Paris and Wilkie [1985] for the new arithmetic language and corresponding theory (Krajíček [1995][12.7]).

Section 3.2 provides a proof for the main theorem. We also show one interesting corollary, which provides an answer to a simplified version of an open problem posed by Ajtai [1990][page 3].

1. Preliminaries

1.1 Languages and theories

The current chapter closely follows the first parts of the book of Krajíček [1995]. We first formulate the main languages and theories which describe arithmetic.

Definition 1.1.1. The language of Peano arithmetic (denoted by L_{PA}) consists of constant 0, unary symbol S (successor function), binary symbols $+$ and $\cdot$ and binary relation $\leq$.

One of the most important theories associated with this language is Robinson arithmetic (denoted by Q) which consists of the following axioms (free variables are assumed to be universally quantified):

- $S(x) \neq 0$,
- $(S(x) = S(y)) \rightarrow (x = y)$,
- $(x \neq 0) \rightarrow \exists y(x = S(y))$,
- $x + 0 = x$,
- $x + S(y) = S(x + y)$,
- $x \cdot 0 = 0$,
- $x \cdot S(y) = (x \cdot y) + x$,
- $(x \leq y) \leftrightarrow \exists z(x + z = y)$.

Notice that $\mathbb{N}$ with the standard interpretation of the symbols of L_{PA} is a model of Q. Also notice that the symbol $\leq$ can be omitted, since the last axiom defines the meaning of this predicate.

It can be shown that Q is Σ_1-complete, i.e. Q can prove all true arithmetic sentences of the form $\exists \overline{x}\, \phi(\overline{x})$, where $\phi(\overline{x})$ is bounded, meaning all the quantifiers appearing in $\phi(\overline{x})$ are of the form $\exists y \leq t(\overline{x})$ or $\forall y \leq s(\overline{x})$. This is then complemented by showing that all *recursively enumerable relations* are Σ_1-representable in Q. This can further be used to show that Q is strong enough to be able to code sequences and so to talk about syntactic concepts. This makes Q the base theory for modern formulations of *Gödel's incompletness theorems* (Kleene [1943]).

On the other hand, Q is pretty weak. For example, it is not able to prove that the operation $+$ is commutative. It is often more convenient to extend Q to a stronger theory PA^- and consider it as the base theory for the other arithmetic theories (we also extend our language by adding binary predicate $<$ and constant 1 and call this new language L_{PA} as well).

Definition 1.1.2. The theory PA^- is an extension of Q by the following axioms (we omit discussion whether some of these new axioms are actually redundant):

- $(x < y) \leftrightarrow ((x \leq y) \land (x \neq y))$,

- $S(x) = x + 1$,
- $(x + y) + z = x + (y + z)$,
- $x + y = y + x$,
- $(0 < x) \to (1 \leq x)$,
- $(x \leq y) \to ((x + z) \leq (y + z))$,
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
- $x \cdot y = y \cdot x$,
- $((x \leq y) \wedge (z \neq 0)) \to ((x \cdot z) \leq (y \cdot z))$,
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

The theory PA^- corresponds to the theory of the *positive part of dicreetly-ordered rings* (Kaye [1991][2.1]).

Peano arithmetic (denoted PA) is the theory in language L_{PA} which extends PA^- by the induction axioms of the form:

$$\forall \overline{x}\, ((\phi(0, \overline{x}) \wedge \forall y\, (\phi(y, \overline{x}) \to \phi(S(y), \overline{x}))) \to \forall y\, (\phi(y, \overline{x})))$$

for all L_{PA}-formulas $\phi(y, \overline{x})$.

It is easy to see that $\mathbb{N}$ is a model of PA. However, there are other (some also countable) models of PA which are not isomorphic to $\mathbb{N}$. They are called non-standard models of arithmetic (Kaye [1991][1]).

Such models have been extensively studied and we will be using facts about them throughout the whole thesis. In particular, every non-standard model $\mathbb{N}^*$ of PA contains a *cut* I such that it is isomoprhic to $\mathbb{N}$. By cut we mean that I is closed under S and for any element $m \in I$ and $n \in \mathbb{N}^*$, such that $n \leq m$, it holds that n is also contained in I. So we can always assume that $\mathbb{N} \subseteq \mathbb{N}^*$.

In the thesis we will be mostly interested in weak subtheories of PA. To define such theories we first need to show important classes and hierarchies of arithmetic formulas.

Definition 1.1.3. A formula $\phi(\overline{x})$ is said to be contained in Σ_0 if it is bounded. Class Σ_0 is also denoted Π_0 and Δ_0.

A formula $\phi(\overline{x})$ is said to be contained in Σ_{n+1} if it is equivalent (in predicate calculus) to a formula $\exists \overline{y}\, \psi(\overline{y}, \overline{x})$, where $\psi(\overline{y}, \overline{x})$ is in Π_n.

A formula $\phi(\overline{x})$ is said to be contained in Π_{n+1} if it is equivalent (in predicate calculus) to the a formula $\forall \overline{y}\, \psi(\overline{y}, \overline{x})$, where $\psi(\overline{y}, \overline{x})$ is in Σ_n.

A formula $\phi(\overline{x})$ is said to be contained in Δ_n if it is contained in Σ_n and Π_n.

The class $\exists_1$ is defined as the subclass of Σ_1 containing formulas which are equivalent to formulas with no bounded quantifiers, i.e. formulas of the form $\exists \overline{y}\, \psi(\overline{y}, \overline{x})$, where $\psi(\overline{y}, \overline{x})$ is a quantifier-free formula.

It is easy to see that $\Delta_n, \Sigma_n, \Pi_n \subseteq \Delta_{n+1}, \Sigma_{n+1}, \Pi_{n+1}$ and so these classes form an increasing hierarchy of formulas which is called the arithmetic hierarchy. It can also be proven that this hierarchy *does not collapse*, i.e. $\Sigma_n \subsetneq \Sigma_{n+1}$ and $\Pi_n \subsetneq \Pi_{n+1}$ for all $n \geq 0$ and also $\Delta_n \subsetneq \Sigma_n, \Pi_n$ and $\Sigma_n \cup \Pi_n \subsetneq \Delta_{n+1}$ for all $n \geq 1$. This can be established via connections between arithmetic hierarchy and *Turing degrees* (Rogers [1967]), which is beyond the scope of the thesis.

It is also known that each Σ_1-formula is equivalent over PA to a $\exists_1$-formula. This follows from the solution of *Hilbert's 10th problem* (Matiyasevich [1993]).

The classes of formulas defined above give rise to *weak fragments* of Peano arithmetic among which of the most prominence is *Bounded arithmetic.*

Definition 1.1.4. Theory $I\Delta_0$ called Bounded arithmetic is the subtheory of PA with induction axioms restricted to Δ_0-formulas. We can similarly define weak theories $I\Delta_n$, $I\Sigma_n$ and $I\Pi_n$, although we will not use these theories throughout the thesis.

Let us now show an expressive power of Δ_0-formulas, i.e. how complex the subsets of $\mathbb{N}$ defined by Δ_0-formulas can be.

We define $\Delta_0(\mathbb{N})$ as a set of all Δ_0-definable subsets of $\mathbb{N}$. It is not hard to show that all members of $\Delta_0(\mathbb{N})$ are computable. In fact, it can be shown that:

$$\mathrm{Lin}H = \Delta_0(\mathbb{N}),$$

where $\mathrm{Lin}H$ denotes *linear-time hierarchy* (Wrathall [1978]).

It can also be proven that:

$$\mathrm{TimeSpace}(n^c, n^\epsilon) \subseteq \Delta_0(\mathbb{N})$$

for any $c > 0$ and $1 > \epsilon > 0$ (Nepomnjascij [1970]). By $\mathrm{TimeSpace}(f(n), g(n))$ we mean the class of languages recognized by a deterministic Turing machine working simultaneously in time $f(n)$ and space $g(n)$.

As a corollary of the above fact we can show that:

$$\mathrm{LogSpace} \subseteq \Delta_0(\mathbb{N}).$$

There are also more concrete examples of sets inside $\Delta_0(\mathbb{N})$. The theorem of Adleman and Manders [1977] shows that $\Delta_0(\mathbb{N})$ contains an NP-complete set:

$$\{(x, y, z) \mid \exists u < z \; \exists v < z : xu^2 + yv = z\}.$$

The theorem of Bennett [1962] shows that $\Delta_0(\mathbb{N})$ contains the graph of exponentiation:

$$\{(x, y, z) \mid x^y = z\}.$$

We can now return to $I\Delta_0$ and show main theorems regarding this theory. The first one provides an easy way to construct models of $I\Delta_0$ from another models of the same theory (Krajíček [1995][5.1.3]).

Theorem 1.1.5. Let $\mathbb{M}$ be a model of $I\Delta_0$ and $I \subseteq \mathbb{M}$ be a cut of $\mathbb{M}$ closed under $+$ and $\cdot$. Then I is a model of $I\Delta_0$.

In principle, however, constructing non-standard models of bounded arithmetic is hard, since, by the theorem of Tennenbaum [1959], there is no countable *recursive* non-standard model of $I\Delta_0$ and, in fact, not even of the weak subtheory IE_1 of $I\Delta_0$ (Paris [1984]). The class E_1 consists of formulas equivalent to the ones of the form $\exists \overline{y} \leq t(\overline{x})\ \phi(\overline{x}, \overline{y})$ for quantifier-free $\phi(\overline{x}, \overline{y})$.

There is also one more serious limitation of $I\Delta_0$.

Theorem 1.1.6 (Parikh [1971])**.** Assume $\phi(y, \overline{x})$ is a Δ_0-formula and

$$I\Delta_0 \vdash \forall \overline{x} \exists y \phi(\overline{x}, y).$$

Then, there is a term $t(\overline{x})$ such that

$$I\Delta_0 \vdash \forall \overline{x} \exists y \leq t(\overline{x})\ \phi(\overline{x}, y).$$

Combining the above Theorem with the Theorem of [Bennett, 1962], we see that even though we can Δ_0-define the relation $2^x = y$, we can not prove that the exponential function is *total*, i.e.:

$$I\Delta_0 \nvdash \forall x \exists y : 2^x = y.$$

There are various reasons why totality of the exponentiation and its weaker versions are crucial. Most importantly for us, coding polynomial-length proofs and computations requires totality of functions $2^{|x|^k}$, where k is standard and $|x|$ means the binary length of x, i.e $|x|$ is of order $\log(x)$. This leads to the following theory.

Definition 1.1.7 (Paris and Wilkie [1981])**.** The theory $I\Delta_0 + \Omega_1$ is defined as the extension of $I\Delta_0$ by the axiom Ω_1 of the form:

$$\forall x \exists y : x^{|x|} = y.$$

The above theory is still too weak to prove totality of the exponentiation, although it is strong enough to talk about polynomial-time computations.

As a side remark, let us mention that there are further extensions of $I\Delta_0 + \Omega_1$ by imposing totality of functions $\omega_k(x)$, where $\omega_1(x)$ is defined as $x^{|x|}$ and $\omega_{k+1}(x)$ is defined as $2^{(|\omega_k(x)|)}$. Such theories are *interpretable* in $I\Delta_0$, meaning one can define a cut in $I\Delta_0$ closed under $\omega_k(x)$ (Hájek and Pudlák [1993]). However, there is an interesting negative result saying, that there is no definable cut that would be provably in $I\Delta_0$ closed under all $\omega_k(x)$ (Wilkie [1986], Paris and Wilkie [1987]). In particular, no definable cut is provably closed under 2^x, since exponentiation majorizes all $\omega_k(x)$.

We can now formulate the next important language which was defined by [Buss, 1985]. The idea is that we want to extend L_{PA} by adding symbols which help us with coding of syntactical objects.

Definition 1.1.8. The language L extends L_{PA} by three new function symbols $\lfloor \frac{x}{2} \rfloor$, $|x|$ and $x \# y$.

The intended meaning of $|x|$ is $\lfloor \log(x) \rfloor + 1$ and of $x \# y$ is $2^{|x| \cdot |y|}$.

Definition 1.1.9. The theory *BASIC* consists of the following axioms:

- $1 = S(0)$,
- $x + 1 = S(x)$,
- $(x < y) \leftrightarrow ((x \leq y) \wedge (x \neq y))$,
- $(x \leq y) \rightarrow (x \leq (y + 1))$,
- $x \neq x + 1$,
- $0 \leq x$,
- $(x < y) \rightarrow ((x + 1) \leq y)$,
- $(x \neq 0) \rightarrow (2x \neq 0)$,
- $(x \leq y) \vee (y \leq x)$,
- $((x \leq y) \wedge (y \leq x)) \rightarrow x = y$,
- $((x \leq y) \wedge (y \leq z)) \rightarrow x \leq z$,
- $|0| = 0$,
- $(x \neq 0) \rightarrow ((|2x| = |x| + 1) \wedge (|2x + 1| = |x| + 1))$,
- $|1| = 1$,
- $(x \leq y) \rightarrow (|x| \leq |y|)$,
- $|x\#y| = |x| \cdot |y| + 1$,
- $|0\#x| = 1$,
- $(x \neq 0) \rightarrow ((1\#(2x) = 2(1\#x)) \wedge (1\#(2x + 1) = 2(1\#x)))$,
- $x\#y = y\#x$,
- $|x| = |y| \rightarrow (x\#z = y\#z)$,
- $(|x| = |y| + |z|) \rightarrow (x\#u = (y\#u) \cdot (z\#u))$,
- $x \leq x + y$,
- $((x \leq y) \wedge (x \neq y)) \rightarrow ((2x + 1 \leq 2y) \wedge (2x + 1 \neq 2y))$,
- $x + y = y + x$,
- $x + 0 = x$,
- $x + (y + z) = (x + y) + z$,
- $((x + y) \leq (x + z)) \rightarrow y \leq z$,
- $x \cdot 0 = 0$,
- $x \cdot (y + 1) = x \cdot y + x$,

- $x \cdot y = y \cdot x$,
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$,
- $(1 \leq x) \rightarrow (((x \cdot y) \leq (x \cdot z)) \leftrightarrow (y \leq z))$,
- $(x \neq 0) \rightarrow (|x| = |\lfloor \frac{x}{2} \rfloor| + 1)$,
- $(x = \lfloor \frac{y}{2} \rfloor) \leftrightarrow (2x = y \vee 2x + 1 = y)$.

It is not hard to show that $\mathbb{N}$ with the standard interpretation of the symbols of L is a model of $BASIC$.

The classes Σ_n, Π_n and Δ_n still make sense in the new language, although the additional symbols allows one to define more subtle types of formulas.

Definition 1.1.10. A quantifier is said to be sharply bounded if it is of the form $\exists x \leq |t|$ or $\forall x \leq |t|$, where term t does not contain x.

The class $\Sigma_0^b = \Pi_0^b$ is defined as the class of sharply bounded formulas, i.e. formulas with all quantifiers sharply bounded.

For $i \geq 0$ the classes Σ_{i+1}^b and Π_{i+1}^b are defined as the smallest classes of formulas satisfying the following properties:

- $\Sigma_i^b \cup \Pi_i^b \subseteq \Sigma_{i+1}^b \cap \Pi_{i+1}^b$,
- Σ_{i+1}^b and Π_{i+1}^b are closed under sharply bounded quantification, conjunction and disjunction,
- Σ_{i+1}^b is closed under bounded existential quantification,
- Π_{i+1}^b is closed under bounded universal quantification,
- the negation of a Σ_{i+1}^b-formula is a Π_{i+1}^b-formula and vice versa.

The class Σ_∞^b of bounded L-formulas is defined as $\bigcup_i \Sigma_i^b = \bigcup_i \Pi_i^b$.

A Σ_i^b-formula is said to be in Δ_i^b if it is equivalent (in predicate calculus) to a Π_i^b-formula.

We also define formula to be in Δ_i^b in a theory T if the equivalence above is established in T.

It is also possible to define classes Σ_i^b and Π_i^b explicitly as in the Definition 1.1.3. To do so, we first need to push the negation signs inside the quantifier-free part and then count the number of alterations of bounded (but not sharply bounded) quantifiers.

There is an important characterization of Σ_∞^b-definable subsets of $\mathbb{N}$ similar to the characterization of Δ_0-definable sets. Namely, there is a theorem of Stockmeyer:

$$\mathrm{PH} = \Sigma_\infty^b(\mathbb{N}),$$

where PH denotes the *polynomial-time hierarchy* (Stockmeyer [1977]).

We can now formulate analogues of theories $I\Sigma_n$ for our new language.

Definition 1.1.11. Theory T_2^i in the language L is the theory extending $BASIC$ by axioms of induction for Σ_i^b-formulas. Theory T_2 is defined as the union $\bigcup_i T_2^i$.

There are two other types of induction specific for the extended arithmetic language L. Namely, for an L-formula $\phi(x)$ possibly with some other free variables there is a *polynomial induction*:

$$\phi(0) \wedge \forall x(\phi(\lfloor \frac{x}{2} \rfloor) \to \phi(x)) \to \forall x \phi(x),$$

and a *length induction*:

$$\phi(0) \wedge \forall x(\phi(x) \to \phi(x+1)) \to \forall x \phi(|x|).$$

It is possible to show that the theory $BASIC$ augmented with the length induction for Σ_i^b-formulas is the same as the theory $BASIC$ augmented with the polynomial induction for Π_i^b-formulas (Krajíček [1995][5.2.5]). Such theory is called S_2^i and the union $\bigcup_i S_2^i$ is denoted as S_2. It holds that $S_2^i \subseteq T_2^i \subseteq S_2^{i+1}$ and thus $S_2 = T_2$.

Along with the induction, there is one more crucial combinatorial principle, which gives rise to different theories of arithmetic.

Definition 1.1.12. The least number principle (denoted LNP) for a formula $\phi(y, \overline{x})$ is the sentence:

$$\forall \overline{x}\, (\exists y \phi(y, \overline{x}) \to \exists y(\phi(y, \overline{x}) \wedge \forall z < y\, \neg\phi(z, \overline{x}))).$$

The theories $LNP(\Sigma_i)$, $LNP(\Sigma_i^b)$, and so on, are defined as extensions of PA^- (resp. of $BASIC$) by the least number principle restrictied to the corresponding class of formulas.

Theorem 1.1.13.

$$LNP(\Sigma_i) = I\Sigma_i,$$

$$LNP(\Sigma_i^b) = I\Sigma_i^b,$$

$$LNP(\exists_1) = I\exists_1.$$

There are also variants of the least number principle corresponding to the length and polynomial inductions (Krajíček [1995][5.2.6]), although we will not work with such inductions throughout the thesis.

Turns out, the theories $I\Delta_0 + \Omega_1$ and T_2 $(= S_2)$ are, in a sense, the same, since it holds that S_2 is a *conservative* extension of $I\Delta_0 + \Omega_1$, i.e. any L_{PA}-formula provable in S_2 is already provable in $I\Delta_0 + \Omega_1$ (Krajíček [1995][5.2.15]).

Before we proceed to the next Section, let us talk a bit about *coding of sequences* in arithmetical theories. We will provide only a brief overview and for a more thorough and detailed discussion the reader is advised to consult Krajíček [1995][5.4].

Theorem 1.1.14. There is a Δ_0-formula $\theta(w, i, x)$, which we will write as $(w)_i = x$, such that $I\Delta_0 + \Omega_1$ proves:

- $(w)_i = x \wedge (w)_i = y \to x = y$,

- $(w)_i = x \wedge j < i \rightarrow (\exists y \leq w : (w)_j = y)$,
- $\exists w \, \forall i \, \forall x : (w)_i \neq x$,
- $\forall w \, \exists! l \, \forall i : (\exists x (w)_i = x) \leftrightarrow i < l$,
- $\forall w, y, n \leq len(w) \, \exists w' \, \forall x \, \forall i : (w')_i = x \leftrightarrow (((w)_i = x \wedge i \neq n) \vee (x = y \wedge i = n))$,

where $len(w)$ is defined as l from the third statement.

Theorem 1.1.15. There is a Δ_1^b-formula $\theta(w, i, x)$, which we will write as $(w)_i = x$, such that S_2^1 proves:

- $(w)_i = x \wedge (w)_i = y \rightarrow x = y$,
- $(w)_i = x \wedge j < i \rightarrow (\exists y \leq w : (w)_j = y)$,
- $\exists w \forall i \forall x : (w)_i \neq x$,
- $\forall w \, \exists! l \, \forall i : (\exists x (w)_i = x) \leftrightarrow i < l$,
- $\forall w, y, n \leq len(w) \, \exists w' \, \forall x \, \forall i : (w')_i = x \leftrightarrow (((w)_i = x \wedge i \neq n) \vee (x = y \wedge i = n))$,

where $len(w)$ is defined as l from the third statement.

The formula $(w)_i = x$ can be interpreted as saying that x is the i-th element in the sequence coded by w. Then, the first two statements ensure that the coding is well-defined, i.e. only one element can inhabit the i-th position of the sequence and, if there is a j-th element inside our sequence, then there exists an i-th element for any $i \leq j$. The third statement tells us that there is the code for the empty sequence. The fourth statement ensures that each sequence has length. The final statement allows us to extend any given sequence by any element, or to change any element in any given sequence.

We can represent sets as sequences with elements arranged in strictly increasing order. This can be formulated by the predicate $Set(w)$:

$$Set(w) \iff \forall i < j < len(w) \, \forall x, y((w)_i = x \wedge (w)_j = y \rightarrow x < y).$$

Under this convention $len(w)$ denotes the size of the set coded by w.

Strong theories, like PA, are able to provide coding for any bounded definable sets, which we can formulate in a *model theoretic* language.

Theorem 1.1.16. For any model $\mathbb{M}$ of PA and any L_{PA}-formula (possibly with parameters from $\mathbb{M}$) $\phi(x)$ and $m \in \mathbb{M}$ it holds that there exists some $w \in \mathbb{M}$ so that:

$$\forall x((\exists i (w)_i = x) \leftrightarrow ((\phi(x)) \wedge (x \leq m))),$$

and:

$$\forall i < j < len(w) \, \forall x, y((w)_i = x \wedge (w)_j = y \rightarrow x < y).$$

If we restrict ourselves to the classes Δ_0, Δ_1^b, then the theorem above is true for the theories $I\Delta_0 + \Omega_1$, S_2^1, respectively (assuming m is the length of some element of the model). This is known as *bounded collection principles* ([Krajíček, 1995][5.2.11]).

Using the *pairing function* (denoted $\langle x, y\rangle$), it is then possible to code sets of tuples and iterating $\langle x, y\rangle$ allows us to code triples, quadruples and so on.

We can also code bounded sets of bounded sets and so on, which allows us to talk about relations and functions. For example, the statement: ”for every bounded function σ it holds that σ is injective”, can be coded as:

$$\forall \sigma (Set(\sigma) \wedge Func(\sigma)) : Inj(\sigma),$$

where $Func(\sigma)$ is defined as:

$$\forall z, z' \, \forall x, y, x', y' (\langle x, y\rangle = z \wedge \langle x', y'\rangle = z') : (\exists i, j((\sigma)_i = z \wedge (\sigma)_j = z')) \rightarrow ...$$

$$... \rightarrow (x \neq x' \vee y = y'),$$

and $Inj(\sigma)$ is defined as:

$$\forall z, z' \, \forall x, y, x', y' (\langle x, y\rangle = z \wedge \langle x', y'\rangle = z') : (\exists i, j((\sigma)_i = z \wedge (\sigma)_j = z')) \rightarrow ...$$

$$... \rightarrow (x \neq x' \vee y \neq y').$$

We can go even further and code Turing machines in the similar manner.

Theorem 1.1.17 (Buss [1985])**.** Any set $A \subseteq \mathbb{N}$ computable by a polynomial-time Turing machine is definable by an L-formula $\phi(x)$, i.e. $a \in A$ if and only if $\mathbb{N} \vDash \phi(a)$. Moreover, $\phi(x)$ is Δ_1^b in S_2^1.

The theorem above is easily generalized to computable relations, i.e. $A^k \subseteq \mathbb{N}$.

We will consider the following situation. For a model $\mathbb{M}$ of S_2^1 and a relation R on $\mathbb{M}$, such that $(\mathbb{M}, R)$ satisfies theory $S_2^1(R)$, we shall consider class - to be denoted $\Box_1^p(R)$ - of all relations on $\mathbb{M}$ that are definable by *polynomial-time oracle* Turing machine with oracle access to R. By the discussion above, this notion is well-defined, since the corresponding class of formulas is $\Delta_1^b(R)$ in $S_2^1(R)$.

It then holds that for any Turing machine corresponding to a formula from $\Box_1^p(R)$ and an input $u \in \mathbb{M}$, it is possible to produce the computation tree, which branches according to answers of the oracle R and whose depth is bounded by $|u|^c$ for some standard number c.

1.2 Pigeonhole principles

Among different combinatorial principles expressible in the language of arithmetic one of the most prominent is the *pigeonhole principle*. In its basic form it states that there is no injective function between the sets $\{m|m < n+1\}$ and $\{m|m < n\}$ (such sets are denoted $[n + 1]$ and $[n]$, respectively). However, since we are not allowed to quantify over functions, we need to modify this formulation in order to ask for a proof of such statement inside arithmetic theories. One possible way is to extend L_{PA} by a new function symbol f (denote this new language as $L_{PA}(f)$) and add to PA induction axioms for all $L_{PA}(f)$-formulas (resulting theory is denoted $PA(f)$). Then, to prove the pigeonhole principle inside $PA(f)$, is to prove the statement:

$$\forall n((\forall m < n+1 : f(m) < n) \to (\exists m_1 \neq m_2 < n+1 : f(m_1) = f(m_2))).$$

Due to various reasons it is actually more common to state pigeonhole principle not for a function symbol f, but for a binary relation R, which meant to represent the graph of a possible witness to failure of the pigeonhole principle.

Definition 1.2.1. The pigeonhole principle for a relation R (denoted $PHP(R)$) is the disjunction of the following formulas (n is universally quantified before the disjunction):

- $\exists m < n+1\, \forall k < n : \neg R(m,k)$,
- $\exists k_1 \neq k_2 < n\, \exists m < n+1 : R(m,k_1) \wedge R(m,k_2)$,
- $\exists m_1 \neq m_2 < n+1\, \exists k < n : R(m_1,k) \wedge R(m_2,k)$.

Here, the first disjunct states that R is not definable on the whole $[n+1]$, the second states that R is not a function and the third states that R is not injective.

Proposition 1.2.2.

$$PA(R) \vdash PHP(R).$$

Proof. We will prove the statement by induction on n. Actually, we will prove the stronger statement which says that R does not define the graph of a function between pair of sets of sizes $n+1$ and n, respectively (original formulation talked only about sets $[n+1]$ and $[n]$, which are a particular case of our generalization). Note that we can safely state such proposition inside PA since this theory can code finite sequences.

The statement clearly holds for $n = 0$. Assume now that it holds for some $n \geq 0$. Let R define graph of a function between sets A and B of sizes $n+2$ and $n+1$. It is enough to show that such function is not injective.

Let $a \in A$ and $b \in B$ such that $R(a,b)$. If there is $a' \neq a \in A$ so that $R(a',b)$, then R is not injective. Otherwise, R defines graph of a function between $A \setminus \{a\}$ and $B \setminus \{b\}$. But since sizes of $A \setminus \{a\}$ and $B \setminus \{b\}$ are $n+1$ and n, respectively, such function can not be injective. □

There are different variations of the pigeonhole principle. We will be interested in the following two.

Definition 1.2.3. Surjective pigeonhole principle for a relation R (denoted as $ontoPHP(R)$) is defined as a disjunction of the following formulas (n is universally quantified before the disjunction):

- $\exists m < n+1\, \forall k < n : \neg R(m,k)$,
- $\exists k_1 \neq k_2 < n\, \exists m < n+1 : R(m,k_1) \wedge R(m,k_2)$,

- $\exists m_1 \neq m_2 < n+1\, \exists k < n : R(m_1,k) \wedge R(m_2,k)$,
- $\exists k < n\, \forall m < n+1 : \neg R(m,k)$.

Weak pigeonhole principle for a relation R (denoted $WPHP(R)$) is defined as a disjunction of the following formulas (n is universally quantified before the disjunction):

- $\exists m < 2n\, \forall k < n : \neg R(m,k)$,
- $\exists k_1 \neq k_2 < n\, \exists m < 2n : R(m,k_1) \wedge R(m,k_2)$,
- $\exists m_1 \neq m_2 < 2n\, \exists k < n : R(m_1,k) \wedge R(m_2,k)$.

It is clear that $ontoPHP(R)$ says that R is not the graph of a bijection between $[n{+}1]$ and $[n]$ and $WPHP(R)$ says that R is not the graph of an injective function from $[2n]$ to $[n]$.

Since PA proves PHP, it can easily prove the other variants. By a more detailed analysis of the Theorem 1.2.2, we can actually see that $I\Sigma_1$ already proves PHP and all its variants, since it is enough to be able to talk about bounded sets of numbers in order to complete the proof.

So, from the point of view of PA (or even $I\Sigma_1$), all such principles are equally true. It turns out, however, this does not hold for weaker theories.

Theorem 1.2.4 ([Paris and Wilkie, 1985])**.**

$$I\exists_1(R) \nvdash ontoPHP(R),$$

$$I\exists_1(R) \nvdash WPHP(R),$$

$$I\exists_1(R) \nvdash PHP(R).$$

Theorem 1.2.5 ([Krajíček, 1995](12.7))**.**

$$T^1_2(R) \nvdash ontoPHP(R),$$

$$T^1_2(R) \nvdash WPHP(R),$$

$$T^1_2(R) \nvdash PHP(R).$$

We will describe proofs of the above statements in greater details, since the main result of the thesis heavily relies upon those theorems.

It can be shown that (Paris, Wilkie, and Woods [1988]):

$$T^2_2(R) \vdash WPHP(R),$$

while (Ajtai [1988], Krajíček, Pudlák, and Woods [1995] and Pitassi, Beame, and Impagliazzo [1995]):

$$T_2(R) \nvdash ontoPHP(R).$$

In particular:

$$T_2^2(R) \nvdash \mathit{ontoPHP}(R).$$

The proof of the above resluts utilizes probabilistic combinatorics and, in particular, a suitable variant of the well-known *switching lemma* (Håstad [1987]), which is far beyond the scope of the thesis.

We can finally formulate the main goal of the thesis. To do so, let us denote, for a class C of $L + \{R\}$-formulas, the $WPHP(C)$ as a set of instances of the weak pigeonhole principle for all binary relations definable using formulas from C. Then, combining the previous statements, it is possible to show:

$$T_2^1(R) + WPHP(\Box_1^p(R)) \nvdash \mathit{ontoPHP}(R),$$

that is, that $T_2^1(R)$ extended by the weak pigeonhole principle for $\Box_1^p(R)$-formulas cannot prove that bijective pigeonhole principle holds for R.

The above proof depends, in particular, on a difficult argument in probabilistic combinatorics. Our aim is to prove this statement directly by a simpler *forcing argument* similar to the one used in the proof of 1.2.5 as will be explained below.

The reasons to consider such direct proofs are plenty. It is known that proofs in T_2^1 provide bounds for the propositional proofs is certain *proof systems* (Krajíček [2019][10.5.1]). These proofs also provide witnesses for certain algorithmic problems (Krajíček [1995][7.2.3]). These connections are, however, beyond the scope of the thesis.

As an interesting by-product of our direct proof we get the following statement:

$$T_2^1(R) + PHP_{\frac{n}{2}}^{\frac{n}{2}+1}(\Box_1^p(R)) \nvdash PHP_n^{n+1}(R).$$

There is an interesting conjecture proposed by Ajtai [1990][page 3], which can be formulated as:

$$T_2(R) + PHP_{\frac{n}{2}}^{\frac{n}{2}+1}(\Sigma_\infty^b(R)) \nvdash PHP_n^{n+1}(R),$$

that is, the fact that the pigeonhole principle holds up to $\frac{n}{2}$ for all functions whose graphs are definable from R by bounded formulas does not imply that it necessary holds for R up to n. This is in contrast to the induction, since it is possible to show that if induction holds up to n, then it holds up to any finite power of n (Ajtai [1990][page 3]).

However, the methods described in this thesis are not strong enough to provide a full proof of the above conjecture.

2. Forcing

2.1 Theorem of Paris and Wilkie

We will now present the original proof of the theorem 1.2.4 (Paris and Wilkie [1985]), as it inspires our construction later on. Recall that we want to show:

$$I\exists_1(R) \nvdash ontoPHP(R).$$

Proof. The proof is done by constructing a model of $I\exists_1(R) + \neg ontoPHP(R)$. We first pick a countable non-standard model of PA and denote it $\mathbb{M}$.

We then want to interpret R inside this model so that such R would violate $ontoPHP(R)$ but would not violate the least number principle for $\exists_1(R)$-formulas (recall that $I\exists_1(R)$ is equivalent to the $LNP(\exists_1(R))$ by 1.1.13).

Fix a non-standard $n \in \mathbb{M}$. We want to create an increasing chain of *conditions* $\sigma_0 \subseteq \sigma_1 \subseteq ...$, where a condition will be the graph of a standard finite partial injective function between $[n+1]$ and $[n]$, so that $\bigcup_i \sigma_i$ would define us a bijective function between $[n+1]$ and $[n]$. Then, interpreting R as such union, gets us $(\mathbb{M}, R) \vDash \neg ontoPHP(R)$.

At first, note that for any chain of conditions it holds that their union is an injective function defined on a subset of $[n+1]$ with image inside $[n]$. Now fix some enumerations of elements of sets $[n+1]$ and $[n]$. So, elements of $[n+1]$ are enumerated as $n_0, n_1, ...$ and elements of $[n]$ as $m_0, m_1, ...$ To ensure that the resultant function is a bijection between $[n+1]$ and $[n]$, we specify that in each $(2i+1)$-st step of the construction of σ's we pick the first n_j from the enumeration of $[n+1]$ such that it is not in the domain of σ_{2i} and similarly for m_j from the enumeration of $[n]$. We then extend σ_{2i} by adding the pair (n_j, m_j) to it and denote the newly acquired condition as σ_{2i+1}. Note that the union of chain created this way is always a bijection between $[n+1]$ and $[n]$ no matter how we proceed in each $(2i)$-th step.

It remains to specify each even step of the construction of our chain. Recall that we need to ensure $I\exists_1(R)$ would hold for R interpreted as $\bigcup_i \sigma_i$. Let us now enumerate all $\exists_1(R)$-formulas with one free variable and possibly some parameters from $\mathbb{M}$. There are only countably many such formulas and so we can provide such an enumeration.

We will now define *-$forcing$. This notion is intended to characterize which open sentences can be deduced from a finite information about R, using the hypothesis that R is a bijection between $[n+1]$ and $[n]$.

For an open $L_{PA}(R)$-sentence θ (possibly with parameters from $\mathbb{M}$) and a condition σ, we will say that σ *-forces θ (denoted $\sigma \Vdash^* \theta$) in the following situations:

- if θ does not contain R, then $\sigma \Vdash^* \theta$ iff $\mathbb{M} \vDash \theta$,
- if θ is $R(t,s)$, then $\sigma \Vdash^* \theta$ iff $(a,b) \in \sigma$, where t and s are closed terms with values a, b, respectively,
- if θ is $\neg R(t,s)$, then $\sigma \Vdash^* \theta$ iff $(a',b) \in \sigma$ or $(a,b') \in \sigma$ for $a \neq a'$ and $b \neq b'$, where t and s are closed terms with values a, b, respectively,

- if θ is $\theta_0 \wedge \theta_1$, then $\sigma \Vdash^* \theta$ iff $\sigma \Vdash^* \theta_1$ and $\sigma \Vdash^* \theta_0$,
- if θ is $\theta_0 \vee \theta_1$, then $\sigma \Vdash^* \theta$ iff either $\sigma \Vdash^* \theta_1$ or $\sigma \Vdash^* \theta_0$,
- if θ is $\neg\theta_0$ for non-atomic θ_0, then $\sigma \Vdash^* \theta$ iff $\sigma \Vdash^* \theta_0'$, where we get θ_0' by pushing negation inside θ_0 using De Morgan's laws.

For an $L_{PA}(R)$-sentence (possibly with parameters) $\exists\overline{x}\theta(\overline{x})$ in the prenex normal form we write $\sigma \Vdash^* \exists\overline{x}\theta(\overline{x})$ iff there is a tuple of elements $\overline{a}$ from $\mathbb{M}$ so that $\sigma \Vdash^* \theta(\overline{a})$.

For an $L_{PA}(R)$-sentence (possibly with parameters) $\forall\overline{x}\theta(\overline{x})$ in the prenex normal form we write $\sigma \Vdash^* \forall\overline{x}\theta(\overline{x})$ iff for all tuples of elements $\overline{a}$ from $\mathbb{M}$ it holds that $\sigma \Vdash^* \theta(\overline{a})$.

To define *-forcing for a general sentence, we first need to get it's prenex normal form and then apply the above definition.

It is not hard to show that, if $\sigma \Vdash^* \theta$, then, for any possible extension of σ to a full bijection between $[n+1]$ and $[n]$ whose graph gives rise to an interpretation of R, it holds that $(\mathbb{M}, R) \vDash \theta$. The opposite implication is, however, not true. We will see the reasons for this later.

Let us now go back to the construction of R. Assume we are in the $(2i)$-th step and we have already constructed σ_{2i-1}. We also let σ_{-1} be $\emptyset$.

Let $\exists\overline{x}\theta(\overline{x}, y)$ be the i-th formula of the enumeration of all $\exists_1(R)$-formulas, where $\theta(\overline{x}, y)$ is open. If, for any possible bijection between $[n+1]$ and $[n]$ whose graph extends σ_{2i-1}, it holds that for R, interpreted as such a graph, $(\mathbb{M}, R) \vDash \neg\exists\overline{x}\theta(\overline{x}, a)$ for any $a \in \mathbb{M}$, then we can put σ_{2i} to be just σ_{2i-1}, since no matter how we proceed further, the resulting interpretation of R would satisfy $\forall y(\neg\exists\overline{x}\theta(\overline{x}, y))$ and so the least number principle would automatically hold for $\exists\overline{x}\theta(\overline{x}, y)$.

So assume there is some bijection extending σ_{2i-1} such that for some $a \in \mathbb{M}$ it holds that $(\mathbb{M}, R) \vDash \exists\overline{x}\theta(\overline{x}, a)$ for R interpreted as a graph of such bijection. Pick a tuple $\overline{b}$ from $\mathbb{M}$ so that $(\mathbb{M}, R) \vDash \theta(\overline{b}, a)$. Since $\theta(\overline{b}, a)$ is an open sentence, it is clear that we can find some condition $\tau \supseteq \sigma_{2i}$ so that $\tau \Vdash^* \theta(\overline{b}, a)$ and so $\tau \Vdash^* \exists\overline{x}\theta(\overline{x}, a)$. It further holds that we can assume the size of such τ is bounded from above by the size of σ_{2i-1} plus some finite number k which depends only on the formula $\theta(\overline{x}, y)$ (this k equals the number of appearances of atomic formulas of type $R(t(\overline{x}, y), s(\overline{x}, y))$ inside $\theta(\overline{x}, y)$).

Consider a set:

$$\{b \mid b \leq a \wedge \exists\tau(\tau \supseteq \sigma_{2i-1} \wedge |\tau| \leq (|\sigma_{2i-1}| + k) \wedge \tau \Vdash^* \exists\overline{x}\theta(\overline{x}, b))\},$$

where $|\sigma|$ denotes the size of σ. Due to the bound on the size of τ, such set is actually definable by an L_{PA}-formula inside $\mathbb{M}$. Since $\mathbb{M} \vDash PA$, it follows that this set contains the least element c. For such an element pick τ so that $\tau \supseteq \sigma_{2i-1}$ and $\tau \Vdash^* \exists\overline{x}\theta(\overline{x}, c)$. Then, for all $b < c$, it holds that any possible extension of σ_{2i-1} (and subsequently of τ) interpreted as R would satisfy $(\mathbb{M}, R) \vDash \neg\exists\overline{x}\theta(\overline{x}, b)$ and so we may put σ_{2i} to be just τ. This implies that for any extension of σ_{2i} to a full bijection intepreted as R, the least number principle for $\exists\overline{x}\theta(\overline{x}, y)$ would hold true in $(\mathbb{M}, R)$. □

Note that by changing conditions to be finite partial injective functions between $[2n]$ and $[n]$ we can show that:

$$I\exists_1(R) \nvdash WPHP(R).$$

We can go even further and show that, for any two non-standard natural numbers n and m, it is consistent with $I\exists_1(R)$ that R is the graph of a bijective function between $[n]$ and $[m]$ or even that R is the graph of a bijective function which maps the whole $\mathbb{M}$ onto $[m]$.

2.2 Forcing set-up

The Theorem of Krajíček (1.2.5) can be proven in a similar manner as the one of Paris and Wilkie which we have just showed ([Krajíček, 1995][12.7]). We will, however, describe a more general method which will then serve as a framework in which one can present the proof of 1.2.5 as well as the proof of our result.

The method in question is *forcing*.

Definition 2.2.1. Let P be partially ordered set with an ordering $\leq$. We call σ from P a condition.

For two conditions σ and τ we say that they are compatible (denoted $\sigma \| \tau$) if there is some δ so that $\delta \geq \sigma$ and $\delta \geq \tau$. Otherwise, we call σ and τ incompatible (denoted $\sigma \perp \tau$).

We call $D \subseteq P$ dense, if for any $\sigma \in P$ there is $\tau \in D$ so that $\tau \geq \sigma$.

We call $D \subseteq P$ pre-dense, if for any $\sigma \in P$ there is $\tau \in D$ so that $\tau \| \sigma$.

It is clear that every dense set is pre-dense. There is also a canonical way of creating a dense set out of a pre-dense one.

Proposition 2.2.2. For a pre-dense set $D \subseteq P$ it holds that the set:

$$D' = \{\sigma \mid \exists \tau (\tau \in D \wedge \sigma \geq \tau)\}$$

is dense in P. Such set is called generated by D.

Proof. Let δ be from P. Then, there is $\sigma \in D$ so that $\sigma \| \delta$. Since these two conditions are compatible, it follows that there is some $\tau \in P$ so that $\tau \geq \delta$ and $\tau \geq \sigma$. From the definition of D' it follows that $\tau \in D'$, proving D' is dense. □

Definition 2.2.3. We call $G \subseteq P$ a filter, if it satisfies the following two conditions:

- G is *closed downwards*, i.e. for any $\sigma \in G$ and $\tau \in P$ so that $\tau \leq \sigma$ it holds that $\tau \in G$,
- for any two $\sigma, \tau \in G$ there is some $\delta \in G$ so that $\sigma \leq \delta$ and $\tau \leq \delta$.

In particular, any two conditions from G must be compatible.

From now on we will focus on a particular partially ordered set P containing finite partial injective functions between $[n+1]$ and $[n]$ as in the previous section. The ordering is just the usual inclusion. It is then clear that $\sigma \| \tau$ iff $\sigma \cup \tau \in P$.

In the next chapter we will consider P^* - a set of partial injective functions between $[n+1]$ and $[n]$ which are definable in $\mathbb{M}$ and have sizes bounded by $|n|^k$ for a standard k. Recall that $|n|$ is about $\log n$, so conditions in P^* are of size $(\log n)^k$, i.e. much smaller than the n itself. All the arguments of the current chapter would still hold true for P^* and the reason we are not proceeding in a more general way already, is that we want to show the core ideas in their simplest form.

Proposition 2.2.4. For a filter $G \subseteq P$ it holds that $\bigcup G$ is a partial injective function between $[n+1]$ and $[n]$.

We then say that G defines the graph of a partial injective function which is denoted by G, as well.

Proof. This easily follows from the fact that all conditions of G are compatible. □

Definition 2.2.5. We say that a dense set $D \subseteq P$ is dense-definable, if there is an L_{PA}-formula $\phi(x)$ (possibly with parameters from $\mathbb{M}$) so that:

$$D = \{\sigma \in P \mid \phi(\sigma)\},$$

where we identify the set σ with the number coding it inside the $\mathbb{M}$.

In a similar way we define pre-dense-definable sets.

We say that a filter G is generic, if, for any dense-definable set D, it holds that $G \cap D \neq \emptyset$.

Note that the definability of a dense set D according to the above definition does not mean that such set itself is definable in the logical sense, since, for example, the set P is dense-definable but is not definable inside $\mathbb{M}$, since otherwise one could define standard numbers as the sizes of conditions in P, thus violating induction in $\mathbb{M}$ ([Kaye, 1991][6.1]).

Proposition 2.2.6. The function G, which is defined by a generic filter G, is a bijection between $[n+1]$ and $[n]$.

Proof. Note that for any $a \in [n+1]$ the set:

$$D_a = \{\sigma \mid \sigma \text{ is defined on } a\}$$

is dense-definable. In a similar way, for any $b \in [n]$ the set:

$$D^b = \{\sigma \mid b \text{ is in the image of } \sigma\}$$

is dense-definable, as well. Since G is generic, it should be definable on all elements of $[n+1]$ and contain every element of $[n]$ in the image. From the proposition 2.2.4 it follows that G is an injective function which finishes the proof. □

The sets D_a and D^b (or, more generally, the sets $D_{\overline{a}}^{\overline{b}}$ containing all the functions defined on $\overline{a}$ and having $\overline{b}$ in their images) are a canonical example of dense-definable subsets of P. The sets ${}_cD_a$ containing all the functions defined on a and of sizes $\leq c$ for a standard c are a canonical example of pre-dense-definable subsets (similarly for ${}_cD^b$ and ${}_cD_{\overline{a}}^{\overline{b}})$. Note that ${}_cD_a$ is note dense, and D_a is the set generated by ${}_cD_a$ as in the Proposition 2.2.2.

Proposition 2.2.7. A generic filter G exists.

Proof. It is crucial to note that there are only countably many dense-definable sets, since $\mathbb{M}$ is countable and there are countably many formulas of L_{PA} (even with parameters from $\mathbb{M}$). So we may enumerate all the dense-definable sets as $D_1, D_2, ...$ We then create G by a recursive process.

Put G_0 to be $\emptyset$. To create G_{i+1} take D_{i+1}. Assume G_i equals $\{\sigma \mid \sigma \leq \tau\}$ for some fixed condition τ. Since D_{i+1} is dense, we can find some $\delta \in D_{i+1}$ so that $\delta \geq \tau$. Put G_{i+1} to be $\{\sigma \mid \sigma \leq \delta\}$. It is then clear that $\bigcup_i G_i$ is a generic filter. □

Using the similar argument as in the Proposition above, we can prove that, for any fixed condition $\sigma \in P$, there exists a generic filter G which extends σ, i.e. $\sigma \subseteq \bigcup G$.

Generic filters also intersect all the pre-dense-definable sets, as in the proposition below.

Proposition 2.2.8. If G is generic, then, for any pre-dense-definable set D, it holds that there is some $\sigma \in D$ so that $\sigma \subseteq \bigcup G$ (actually, $\sigma \in G$).

Proof. Let D' be the dense set generated by D as in the Proposition 2.2.2. Note that if D is definable, then so is D'. Since G is generic, it holds that there is some $\tau \in D'$ so that $\tau \in G$. But then, there is some $\sigma \in D$ so that $\sigma \leq \tau$. Since G is closed downwards, it follows that $\sigma \in G$, finishing the proof. □

We can finally define *forcing*.

Definition 2.2.9. Let ϕ be an $L_{PA}(R)$-sentence possibly with parameters from $\mathbb{M}$. We say that a condition $\sigma \in P$ forces ϕ (denoted as $\sigma \Vdash \phi$), if, for any generic filter G which extends σ, it follows that $(\mathbb{M}, G) \vDash \phi$, where $(\mathbb{M}, G)$ denotes an $L_{PA} + R$-structure, where R is interpreted as the graph of a function definable by G.

Let us go back to the relation $\Vdash^*$, which was defined during the proof of the Theorem 1.2.4. Recall the Definition 2.1.

We have shown that $\sigma \Vdash^* \theta$ implies $\sigma \Vdash \theta$. The opposite, however, does not hold. As a counterexample consider $\sigma = \emptyset$ and $\theta = R(a, b) \vee \neg R(a, b)$. It is then clear that $\sigma \Vdash \phi$, although σ does not *-force $R(a, b)$ nor $\neg R(a, b)$.

However, the fact is that $\sigma \Vdash \theta$ does provide certain information about $\Vdash^*$, assuming θ is not very complex.

Proposition 2.2.10. Assume θ is an open $L_{PA}(R)$-sentence with parameters and σ is a condition. Then:

- if θ does not contain R, then $\sigma \Vdash \theta$ iff $\sigma \Vdash^* \theta$,

- if θ is $R(a,b)$, then $\sigma \Vdash \theta$ iff $\sigma \Vdash^* \theta$,
- if θ is $\neg R(a,b)$, then $\sigma \Vdash \theta$ iff $\sigma \Vdash^* \theta$.

Proof. The first equivalence is clear. To prove the second, note that it is enough to show $\sigma \Vdash \theta$ implies $\sigma \Vdash^* \theta$, since the other direction has been already discussed.

Let θ be $R(a,b)$ and assume $\sigma \Vdash \theta$. Assume that $\sigma \nVdash^* \theta$, meaning $(a,b) \notin \sigma$. Then, we may find some $b' \neq b$ so that $\{(a,b')\} \| \sigma$. This implies $\sigma' = \sigma \cup \{(a,b')\}$ is in P and $\sigma' \Vdash \neg R(a,b)$, contradicting our initial assumptions.

The third case is done analogously. □

It is also clear that forcing a sentence θ is equivalent to forcing a sentence ϕ which is equivalent to θ in predicate calculus. This will be helpful as it allows us to work with prenex normal forms and CNFs/DNFs.

We are almost ready to give a proof of the Theorem 1.2.4 in this new forcing language. But first, we need the following lemma.

Lemma 2.2.11. Let θ be an open $L_{PA}(R)$-sentence and σ be a condition. Then, $\sigma \nVdash \theta$ implies that there is some condition τ so that $\sigma \subseteq \tau$ and $\tau \Vdash \neg\theta$.

Proof. Since $\sigma \nVdash \theta$, we may find some generic G extending σ so that $(\mathbb{M}, G) \vDash \neg\theta$. Since θ is open, we may rewrite $\neg\theta$ is as a formula D in DNF (that is D is equivalent to $\neg\theta$ for in all $(\mathbb{M}, G)$):

$$\bigvee_i R^{i_1}(a_1^i, b_1^i) \wedge ... \wedge R^{i_k}(a_k^i, b_k^i),$$

where $i_k \in \{-1, 1\}$ and $R^1(a,b)$ denotes $R(a,b)$, while $R^{-1}(a,b)$ denotes $\neg R(a,b)$. The rewriting procedure first puts θ into DNF according to rules of predicate calculus. Then, we evaluate atomic subformulas inside $\mathbb{M}$ to get their truth values. Finally, we evaluate all the terms inside $\mathbb{M}$ so that $R(t(a,b), s(a,b))$ may be rewritten to $R(a', b')$, where $\mathbb{M} \vDash (t(a,b) = a') \wedge (s(a,b) = b')$. It is then clear, that to force $\neg\theta$ is the same as to force D. Since D is true in $(\mathbb{M}, G)$, we may find some particular i so that:

$$(\mathbb{M}, G) \vDash R^{i_1}(a_1^i, b_1^i) \wedge ... \wedge R^{i_k}(a_k^i, b_k^i).$$

This means, G contains map ρ consisting of pairs (a_j^i, b_j^i) which are inside the *positive occurrences* of R (i.e. $i_j = 1$) and some $({a'}_j^i, {b'}_j^i)$ which contradict pairs (a_j^i, b_j^i) appearing in negative occurrences of R. Note that all such pairs are compatible with σ, since G extends σ, and there are only finitely many of them. So we can define τ to be the union of σ and ρ we have just considered. Then $\tau \in P$ and $\tau \Vdash D$, implying $\tau \Vdash \neg\theta$. □

Note that in the proof above the size of τ is bounded by the size of σ plus some finite number, which depends only on θ.

Corollary 2.2.12. For $\sigma \in P$ and an open $L_{PA}(R)$-formula with parameters θ, it holds that:

- if θ is $\bigwedge_i \theta_i$, then $\sigma \Vdash \theta$ iff $\sigma \Vdash \theta_i$ for all i,
- if θ is $\bigvee_i \theta_i$, then $\sigma \Vdash \theta$ iff $\forall \tau \supseteq \sigma\ \exists \tau' \supseteq \tau\ \exists i : \tau' \Vdash \theta_i$.

Proof. Let us start with the first statement. If $\sigma \Vdash \theta_i$ for all i, then, clearly, $\sigma \Vdash \theta$. So, assume $\sigma \nVdash \theta_i$ for some i. Using the lemma above, we can find some $\tau \supseteq \sigma$ so that $\tau \Vdash \neg\theta_i$. Then, clearly, $\tau \Vdash \neg\theta$ and so $\sigma \nVdash \theta$.

Let us now focus on the second part of the corollary. Assume $\sigma \nVdash \theta$. Then, we can find some $\tau \supseteq \sigma$ so that $\tau \Vdash \neg\theta$. From the first part of the corollary, it follows that $\tau \Vdash \neg\theta_i$ for all i and so there is no $\tau' \supseteq \tau$ so that $\exists i : \tau' \Vdash \theta_i$.

Finally, assume $\exists \tau \supseteq \sigma \, \forall \tau' \supseteq \tau \, \forall i : \tau' \nVdash \theta_i$. In particular, $\forall i : \tau \nVdash \theta_i$. Then, we can extend τ to τ_1 so that $\tau_1 \Vdash \neg\theta_1$. Since $\tau_1 \nVdash \theta_i$ for all i, we can extend it to τ_2 so that $\tau_2 \Vdash \neg\theta_2$. Note that $\tau_2 \Vdash \neg\theta_1$, since it extends τ_1. We proceed inductively to create τ_k so that $\tau_k \Vdash \neg\theta_i$ for all i. Using the first part of the corollary, it follows that $\tau_k \Vdash \neg\theta$ and, since $\tau_k \supseteq \sigma$, it follows that $\sigma \nVdash \theta$. □

Again, as in the previous lemma, the size of τ' from the second part of the previous corollary can be bounded by the size of τ plus some finite number, which depends only on θ.

Corollary 2.2.13. For $\sigma \in P$ and an open $L_{PA}(R)$-formula with parameters $\theta(\overline{x})$ it holds that:

- $\sigma \Vdash \forall \overline{x} \theta(\overline{x})$ iff $\sigma \Vdash \theta(\overline{a})$ for all $\overline{a} \in \mathbb{M}$,
- $\sigma \Vdash \exists \overline{x} \theta(\overline{x})$ iff $\forall \tau \supseteq \sigma \exists \tau' \supseteq \tau \exists \overline{a} \in \mathbb{M} : \tau' \Vdash \theta(\overline{a})$.

Proof. The first claim is clear. To prove the second statement, at first assume $\sigma \Vdash \exists \overline{x} \theta(\overline{x})$ and $\tau \supseteq \sigma$. Pick any generic G extending τ. Note $(\mathbb{M}, G) \models \exists \overline{x} \theta(\overline{x})$ and so we may find $\overline{a} \in \mathbb{M}$ such that $(\mathbb{M}, G) \models \theta(\overline{a})$. Since $\theta(\overline{x})$ is open, it follows that there is a finite τ' so that $\tau' \Vdash \theta(\overline{a})$. Also note that we can assume such τ' is compatible with τ and so $\tau' \cup \tau \in P$.

Finally, assume $\forall \tau \supseteq \sigma \exists \tau' \supseteq \tau \exists \overline{a} \in \mathbb{M} : \tau' \Vdash \theta(\overline{a})$. Note that the set:

$$\{\tau' \in P \mid (\tau' \perp \sigma) \vee (\exists \overline{a} \in \mathbb{M} : \tau' \Vdash \theta(\overline{a}))\}$$

is definable and the assumption above implies it is dense. This finishes the whole proof. □

We can now formulate a proof of:

$$I\exists_1(R) \nvdash \mathit{ontoPHP}(R),$$

using forcing.

Recall, that any generic G defines bijection between $[n+1]$ and $[n]$ as was shown in 2.2.6. This can be stated as:

$$\emptyset \Vdash (\forall a < n+1 \, \exists! b < n : R(a,b)) \wedge (\forall b < n \, \exists! a < n+1 : R(a,b)).$$

It is now enough to show that, for any $\exists_1(R)$-formula with parameters and one free variable $\theta(x)$, the set $D_{\theta(x)}$ defined as:

$$\{\sigma \in P \mid \sigma \Vdash LNP(\theta(x))\}$$

is dense-definable.

Assuming the above is true, it follows that for any generic G and any $\exists_1(R)$-formula with one free variable $\theta(x)$, G intersects $D_{\theta(x)}$ and so $(\mathbb{M}, G) \vDash LNP(\theta(x))$ implying $(\mathbb{M}, G) \vDash I\exists_1(R)$, while also $(\mathbb{M}, G) \vDash \neg ontoPHP(R)$.

The density of $D_{\theta(x)}$ has been already shown in the proof of 1.2.4, which was done in the beginning of the current Chapter. Recall, that for a given condition σ we have constructed $\tau \supseteq \sigma$ so that $\tau \Vdash^* \theta(a)$, while for any $b < a$ and any possible extension of τ to a full bijection between $[n+1]$ and $[n]$ it was true that for R interpreted as graph of such bijection $(\mathbb{M}, R) \vDash \neg\theta(b)$, which in our new language can be formulated as:

$$\tau \Vdash \theta(a) \wedge (\forall b < a \neg\theta(b)),$$

implying $\tau \Vdash LNP(\theta(x))$. Thus, $\tau \supseteq \sigma$ is a member of $D_{\theta(x)}$.

Definability of $D_{\theta(x)}$ can be shown by a detailed analysis of the sentence $LNP(\theta(x))$ and by using Propositions 2.2.13, 2.2.12 and 2.2.10, as in the original proof in the Section 2.1. This finishes the proof of 1.2.4.

2.3 WPHP for open formulas

Recall that the main goal of this thesis it to prove the following statement:

$$T_2^1(R) + WPHP(\Box_1^p(R)) \nvdash ontoPHP(R).$$

We first prove an easier variant which, in turn, explains the main idea without technical complications caused by working in $T_2^1(R)$.

Theorem 2.3.1.

$$I\exists_1(R) + WPHP(open(R)) \nvdash ontoPHP(R),$$

where *open*(R) denotes the class of quantifier-free $L_{PA}(R)$-formulas with parameters.

The proof of this theorem occupies the rest of the subsection and is summarized at the end. We proceed in the same way as during the earlier proof of 1.2.4. The only difference is that we start with a countable non-standard model of $Th(\mathbb{N})$, instead of PA, so that some arguments become easier. The theory $Th(\mathbb{N})$ consists of all L_{PA}-sentences which are true in $\mathbb{N}$. The existence of a countable non-standard model of $Th(\mathbb{N})$ is established in the similar way as for a countable non-standard models of PA (Kaye [1991][1]).

Fix some non-standard $n \in \mathbb{M}$ and let P be the set of all finite partial injective functions between $[n+1]$ and $[n]$ ordered by inclusion.

We have already proven that (2.2.6):

$$\emptyset \Vdash \neg ontoPHP(R),$$

and also (1.2.4):

$$\emptyset \Vdash I\exists_1(R).$$

The majority of the following subsection occupies the proof of the Lemma below.

Lemma 2.3.2. For any open formula with parameters $\theta(x, y)$ and $m \in \mathbb{M}$ the set of all conditions forcing $WPHP^{2m}_m(\theta(x, y))$ is dense (definability of such set can be shown using Propositions 2.2.13, 2.2.12 and 2.2.11).

The Lemma above implies:

$$\emptyset \Vdash WPHP^{2m}_m(\theta(x, y)),$$

for any open $\theta(x, y)$ and $m \in \mathbb{M}$, which, in turn, finishes the proof of 2.3.1. Recall that $WPHP^{2m}_m(\theta(x, y))$ is a disjunction of the following sentences:

- $\exists k < 2m\, \forall l < n : \neg\theta(k, l)$
- $\exists l_1 \neq l_2 < m\, \exists k < 2m : \theta(k, l_1) \wedge \theta(k, l_2)$
- $\exists k_1 \neq k_2 < 2m\, \exists l < m : \theta(k_1, l) \wedge \theta(k_2, l)$.

To prove the Lemma 2.3.2, note that we may assume m is non-standard, since, for any finite number m, the $WPHP^{2m}_m(\theta(x, y))$ holds in $(\mathbb{M}, R)$ for any interpretation of R.

Assume the Lemma 2.3.2 is false. This implies existence of a $\sigma \in P$ which cannot be extended to any other condition τ such that $\tau \Vdash WPHP^{2m}_m(\theta(x, y))$. We will show that the above is a contradiction for any $\sigma \in P$. First, consider the case $\sigma = \emptyset$.

Proposition 2.3.3. For any open $L_{PA}(R)$-formula with parameters $\theta(x, y)$ it holds that there exists standard k so that for any $(a, b) \in [n + 1] \times [n]$ the sentence $\theta(a, b)$ is equivalent to:

$$\bigvee_i R^{i_1}(a^i_1, b^i_1) \wedge ... \wedge R^{i_k}(a^i_k, b^i_k),$$

where the equivalence is meant in a forcing sense, i.e. forcing $\theta(a, b)$ is the same as forcing the sentence written above. The DNF above can also be made so no two different DNF-terms are compatible.

Proof. Since $\theta(x, y)$ is an open $L_{PA}(R)$-formula, it can be rewritten to:

$$\bigvee_i R^{i_1}(t_{i_1}(x, y), s_{i_1}(x, y)) \wedge ... \wedge R^{i_n}(t_{i_n}(x, y), s_{i_n}(x, y)) \wedge \theta_i(x, y),$$

where $\theta_i(x, y)$ does not contain R. The rewriting procedure is made in the similar way as in the proof of the Lemma 2.2.11. However, we can not get rid of the part without R and evaluate all the terms inside $\mathbb{M}$ as before, since the part free of R and arithmetic terms, respectively, may contain free variables x and y. Only after we substitute some particular values for the x and y, the form identical to the one in Lemma 2.2.11 is achieved, meaning, for any $a \in [2m]$ and $b \in [m]$, the sentence $\theta(a, b)$ is equivalent to:

$$\bigvee_i R^{i_1}(a^i_1, b^i_1) \wedge ... \wedge R^{i_k}(a^i_k, b^i_k),$$

where the equivalence is meant in a forcing sense, i.e. forcing $\theta(a, b)$ is the same as forcing the sentence written above. It is also clear that we can force all DNF-terms to be of the same standard length k as above. The final part of the Proposition can be achieved by possibly prolonging all the DNF-terms. □

Using the above Proposition we shall now proceed to define a set $[\theta(a,b)]$, which is associated to $\theta(a,b)$.

Definition 2.3.4. Let $\theta(x,y)$ and a,b be as above. Put $\theta(a,b)$ into DNF as in the Proposition 2.3.3. Then, $[\theta(a,b)]$ is defined as a union of $[D_i]$, where D_i is a DNF-term:

$$R^{i_1}(a^i_1, b^i_1) \wedge ... \wedge R^{i_k}(a^i_k, b^i_k).$$

The $[D_i]$ is then defined as a set of all $\subseteq$-minimal conditions $\sigma \in P$ satisfying the following properties:

- for all $i_j = 1$ it holds that $(a^i_j, b^i_j) \in \sigma$,
- for all $i_j = -1$ it holds that $({a'}^i_j, b^i_j) \in \sigma$ and $(a^i_j, {b'}^i_j) \in \sigma$, where ${a'}^i_j \neq a^i_j$ and ${b'}^i_j \neq b^i_j$.

Notice that the size of conditions inside $\theta(a,b)$ is bounded by $2k$, where k is the length of every DNF-term D_i. It is clear that, for any $\sigma \in [D_i]$, it holds that $\sigma \Vdash^* D_i$, implying $\sigma \Vdash^* \theta(a,b)$. So, for any $\sigma \in [\theta(a,b)]$, it follows that $\sigma \Vdash \theta(a,b)$. It further holds that any two different σ and σ' from $[\theta(a,b)]$ are incompatible.

Proposition 2.3.5. Asuming $\sigma = \emptyset$ cannot be extended to any condition τ so that $\tau \Vdash WPHP^{2m}_m(\theta(x,y))$, it follows that:

$$\forall a, a' \in [2m]\, \forall b \in [m]\, \forall \sigma \in [\theta(a,b)]\, \forall \sigma' \in [\theta(a',b)]\, (\sigma \neq \sigma') : \sigma \perp \sigma', \qquad (2.1)$$

$$\forall a \in [2m]\, \forall b, b' \in [m]\, \forall \sigma \in [\theta(a,b)]\, \forall \sigma' \in [\theta(a,b')]\, (\sigma \neq \sigma') : \sigma \perp \sigma', \qquad (2.2)$$

$$\forall a \in [2m]\, \forall \tau \in P\, \exists b \in [m]\, \exists \sigma \in [\theta(a,b)] : \tau \| \sigma. \qquad (2.3)$$

Proof. The (2.1) is true, since, otherwise, for $\tau = \sigma \cup \sigma'$, it would hold that $\tau \in P$ and $\tau \Vdash \theta(a,b) \wedge \theta(a',b)$, implying $\tau \Vdash WPHP^{2m}_m(\theta(x,y))$. The (2.2) is true by the similar argument.

To prove (2.3) it is enough to show that its negation implies (by the Lemma 2.2.12) existence of $\tau \in P$ so that:

$$\exists a \in [2m]\, \forall b \in [m] : \tau \Vdash \neg\theta(a,b),$$

since such τ forces $WPHP^{2m}_m(\theta(x,y))$.

The negation of (2.3) is the following statement:

$$\exists a \in [2m]\, \exists \tau \in P\, \forall b \in [m]\, \forall \sigma \in [\theta(a,b)] : \tau \perp \sigma.$$

We pick τ and a as above and try to show $\tau \Vdash \forall b \in [m] : \neg\theta(a,b)$. Due to the Corollary 2.2.13, it is the same as showing $\tau \Vdash \neg\theta(a,b)$ for all $b \in [m]$.

Recall that $\neg\theta(a,b)$ is equivalent (in a forcing sense) to:

$$\neg(\bigvee_i R^{i_1}(a^i_1, b^i_1) \wedge ... \wedge R^{i_k}(a^i_k, b^i_k)),$$

which, in turn, is equivalent to:

$$\bigwedge_i R^{-i_1}(a^i_1, b^i_1) \vee ... \vee R^{-i_k}(a^i_k, b^i_k).$$

We have assumed $\forall \sigma \in [\theta(a, b)] : \tau \perp \sigma$, which implies:

$$\forall i \exists j : \tau \Vdash^* R^{-i_j}(a^i_j, b^i_j).$$

This, in turn, implies:

$$\forall i : \tau \Vdash^* R^{-i_1}(a^i_1, b^i_1) \vee ... \vee R^{-i_k}(a^i_k, b^i_k),$$

and so:

$$\tau \Vdash^* \bigwedge_i R^{-i_1}(a^i_1, b^i_1) \vee ... \vee R^{-i_k}(a^i_k, b^i_k).$$

Since $\Vdash^*$ implies $\Vdash$, it follows that $\tau \Vdash \neg\theta(a, b)$ and so the (2.3) holds.

□

The Proposition above has been shown true under the assumption that $\sigma = \emptyset$ can not be extended to any condition τ, so that τ forces $WPHP^{2m}_m(\theta(x, y))$. The final step is to show that this Proposition is contradictory.

We can think of (2.1), (2.2) and (2.3) as properties of a certain combinatorial structure. This leads to the following definition.

Definition 2.3.6. Let c be a standard number. Denote $A^c_{n,m}$ a two-dimensional array indexed by $(a, b) \in [2m] \times [m]$ and consisting of sets of partial injective functions σ from $[n + 1]$ to $[n]$ of size $\leq c$ satisfying the following properties:

- $\forall a, a' \in [2m]\, \forall b \in [m]\, \forall \sigma \in A^c_{n,m}(a, b)\, \forall \sigma' \in A^c_{n,m}(a', b)\, (\sigma \neq \sigma') : \sigma \perp \sigma'$,
- $\forall a \in [2m]\, \forall b, b' \in [m]\, \forall \sigma \in A^c_{n,m}(a, b)\, \forall \sigma' \in A^c_{n,m}(a, b')\, (\sigma \neq \sigma') : \sigma \perp \sigma'$,
- $\forall a \in [2m]\, \forall \tau \in P\, \exists b \in [m]\, \exists \sigma \in A^c_{n,m}(a, b) : \tau \| \sigma$.

Proposition 2.3.7. Assuming $\sigma = \emptyset$ can not be extended to any τ so that $\tau \Vdash WPHP^{2m}_m(\theta(x, y))$, it follows that $A^c_{n,m}$ exists for some standard c.

Proof. Just note that $c = 2k$ and $A^c_{n,m}(a, b) = [\theta(a, b)]$ satisfy all the properties above, assuming $\sigma = \emptyset$ can not be extended to any τ forcing $WPHP^{2m}_m(\theta(x, y))$.

□

If we prove that for any standard c the $A^c_{n,m}$ does not exist, then $\sigma = \emptyset$ can be extended to some $\tau \in P$ so that $\tau \Vdash WPHP^{2m}_m(\theta(x, y))$. We first show non-existence of $A^c(n, m)$ for $c = 1$, so as to explain the idea.

Theorem 2.3.8. An array $A^1_{n,m}$ does not exist for any non-standard n and m.

Proof. Assume such an array exists and denote it A. Denote N as a number of all functions inside A. More precisely, $N = \sum_{a,b} |A(a, b)|$. We want to compute N in two different ways. Notice that, due to the first and second properties of

$A^c_{n,m}$, it follows that the same $\sigma \in P$ can appear only once in each row and each column. This implies:

$$N = \sum_a |\bigcup_b A(a,b)| = \sum_b |\bigcup_a A(a,b)|.$$

Firstly, we analyze the maximum number of functions inside any column of A. Note that the first property of $A^c_{n,m}$ says that any two functions of the same column are incompatible. Since $c = 1$, any function of our array is just a pair $(a,b) \in [n+1] \times [n]$. For such pairs (a,b) and (a',b') to be incompatible means that either $a = a'$ and $b \neq b'$, or $a \neq a'$ and $b = b'$. The size of the set of pairs satisfying the property above is $\leq n+1$. To see this, assume the size is $\geq n+2$ and denote such set as S. Pick two different pairs (a,b) and (a',b') from S. Since they are incompatible, we may assume $b = b'$ and $a \neq a'$. Since the number of elements of S is at least $n+2$, it follows that S contains a pair (a'',b'') so that $a'' \neq a$. Then, either (a,b) or (a,b') is compatible to (a'',b''), resulting in a contradiction.

Since there are m columns, it follows that:

$$N \leq m \cdot (n+1).$$

We now want to find a minimum number of functions inside any row of A. Note that the third property of $A^c_{n,m}$ implies that for any finite function $\tau \in P$ we can find some pair (a,b) in our row so that such pair would be compatible with τ. We claim that the size of the set of pairs satisfying the property above is $\geq n$. Assume there exists such set with fewer elements and denote it as S. Pick any pair (a,b) from S. Denote $PHP_{(a,b)}$ as the set of all functions $\sigma \in P$ so that $|\sigma| = 2$ and σ is defined on a, while also σ contains b in it's image. Since all the elements of S are pairwise-incompatible (second property of $A^c_{n,m}$) and $(a,b) \in S$, it follows that, for any $(a',b') \in S$ and $\sigma \in PHP_{(a,b)}$, either $\sigma \perp (a',b')$, or σ extends (a',b'). Since $|S| < n$, it follows that we can find some $b' \in [n]$ so that $(a,b') \notin S$. Then, $PHP_{(a,b)}$ contains precisely n functions σ extending (a,b'). All such functions are of the form $\{(a,b'),(a',b)\}$ and, since $|S| < n$, we can pick some $(a'',b) \notin S$, which defines us $\sigma = \{(a,b'),(a'',b)\}$. Such σ does not extend any of the functions from S. But σ is incompatible with all the elements of S, contradicting the initial assumption.

Since there are $2m$ rows it follows that:

$$N \geq 2m \cdot n.$$

Combining the two inequalities above, gets us:

$$\frac{n+1}{n} \geq 2,$$

which is a contradiction, since $n > 1$ and $\mathbb{M}$ is a model of true arithmetic. □

It remains to generalize the proof for the case $c \geq 1$. Note that the assumption $c = 1$ allowed us to derive an explicit form of all the elements from each row and column from $A^c_{n,m}$. This is not so easy for the general c. However, we can still utilize the ideas of the Theorem 2.3.8.

So assume some $A^c_{n,m}$ exists and let us call it A. We want to proceed as before and estimate $N = \sum_a |\bigcup_b A(a,b)| = \sum_b |\bigcup_a A(a,b)|$ in two different, contradictory, ways.

We start by analyzing the rows of A. Note that each row contains $(\leq c)$-large pairwise incompatible partial injective functions betwenn $[n+1]$ and $[n]$ so that for any $\tau \in P$ there is some function σ inside the row satisfying $\sigma \| \tau$.

The lower bound on the size of rows can be achieved using *PHP-trees* which we have already seen in the proof of 2.3.8.

Definition 2.3.9. A PHP-tree over $D \subseteq [n+1]$ and $R \subseteq [n]$ is defined by induction as follows:

- a single node (a root) is a PHP-tree over any D and R,
- for every $a \in D$ the following is a PHP-tree over D, R:
  - at the root the tree branches according to all $b \in R$, labeling the corresponding edge (a, b),
  - at the end-point of the edge (a, b) the tree continues as a PHP-tree over $D \setminus \{a\}, R \setminus \{b\}$;
- for every $b \in R$ the following is a PHP-tree over D, R:
  - at the root the tree branches according to all $a \in D$, labeling the corresponding edge (a, b),
  - at the end-point of the edge (a, b) the tree continues as a PHP-tree over $D \setminus \{a\}, R \setminus \{b\}$.

A PHP-tree is defined as a PHP-tree over $[n+1], [n]$. We will further assume that all PHP-trees are *uniform in depth*, i.e. all the paths which start at the root are of the same depth. We identify each PHP-tree with a set of partial functions corresponding to maximal paths which start in a root.

For $\sigma \in P$ we define PHP_σ-tree as a PHP-tree T of depth $2|\sigma|$ so that for each $\tau \in T$ it holds that either $\tau \perp \sigma$, or τ extends σ. For any $\tau \in P$ with the domain D and image R we define PHP^τ_σ-tree (assuming $\sigma \| \tau$) as a PHP_σ-tree over $[n+1] \setminus D$ and $[n] \setminus R$.

The PHP-trees play major role in the proof of the famous Ajtai's theorem ([Krajíček, 2019][15.1]). In the original definition they need not be uniform in depth, although this assumption will be helpful for us.

Lemma 2.3.10. Let S be a set of $(\leq c)$-large pairwise incompatible partial injective functions betwenn $[n+1]$ and $[n]$ so that for any $\tau \in P$ there exists some function $\sigma \in S$ satisfying $\sigma \| \tau$. Then, there exists a set S' containing d-large pairwise incompatible partial injective functions between $[n+1]$ and $[n]$ for some standard d dependent on c only, so that $|S'| \geq d!\binom{n}{d}$ and, for any $\tau \in S'$, there exists a unique $\sigma \in S$ such that τ extends σ.

Proof. Note that the size of any PHP-tree of depth d is $\geq d!\binom{n}{d}$, where by size we mean the size of the corresponding set of partial injective functions.

We will define S' in c steps. At first, pick some $\sigma \in S$. Define S_1 to be a PHP_σ-tree of size $\leq 2c$. Note that for any $\tau \in S_1$ and $\sigma \in S$ such that $\sigma \| \tau$ it holds that $|\sigma \cap \tau| \geq 1$.

Assume we have just finished the i-th step ($i \geq 1$) and assume S_i is a PHP-tree of depth $2ic$. Assume further that for any $\tau \in S_i$ and $\sigma \in S$ such that $\sigma \| \tau$ it holds that $|\sigma \cap \tau| \geq i$.

For any $\tau \in S_i$ we can pick some $\sigma_\tau \in S$ so that $\sigma_\tau \| \tau$. Define S_i^τ to be a $PHP_{\sigma_\tau}^\tau$-tree of size $\leq 2c$. We then define S_{i+1} as a PHP-tree which is constructed by attaching each S_i^τ to the corresponding leaf of S_i. Note that the resulting PHP-tree may not be uniform in depth, but we can prolong it so that the uniformity condition will hold. We can also prolong our tree so that its depth would be $2(i+1)c$.

It is enough to show that for any $\delta \in S_{i+1}$ and $\sigma \in S$ so that $\sigma \| \delta$ it holds that $|\sigma \cap \delta| \geq (i+1)$. So pick any $\delta \in S_{i+1}$ and $\sigma \in S$ as above. Note that, since S_{i+1} extends S_i, it follows that $|\sigma \cap \delta| \geq i$. Pick $\tau \in S_i$ such that δ extends τ and note that $|\sigma \cap \tau| \geq i$. It holds that $\delta \setminus \tau$ is (a subset of) a member of a $PHP_{\sigma_\tau}^\tau$-tree S_i^τ and so, in case $\sigma \nsubseteq \tau$, it is true that $|(\delta \setminus \tau) \cap \sigma| \geq 1$, proving $|\sigma \cap \delta| \geq (i+1)$. In case $\sigma \subseteq \tau$, it follows that $\sigma \subseteq \delta$ and so $|\sigma \cap \delta| = c$.

So let S' be S_c. For any $\sigma \in P$ and $\tau \in S'$ it holds that either $\sigma \perp \tau$, or $|\sigma \cap \tau| \geq c$, implying $\tau \supseteq \sigma$, since the size of σ is c. It further holds that S' extends S and, since it is a PHP-tree of depth $2c^2$, it follows that $|S'| \geq (2c^2)!\binom{n}{2c^2}$. □

Let us shift our focus to columns of A. Note that such columns contain ($\leq c$)-large pairwise incompatible partial injective functions between $[n+1]$ and $[n]$. As we will see below, using the Theorem 2.3.10, we will create the new array A' containing partial injective functions of the same standard size d. This new array would still satisfy properties (2.1) and (2.2) (and even (2.3), which will not be so important for us).

We can also interpret members of such A' as d-large matchings of a complete bipartite graph with components of sizes $n+1$ and n. Using the graph-theoretic language we can proceed as in the proof of the famous *Erdős–Ko–Rado theorem* [Katona, 1972].

Lemma 2.3.11. Assume $\mathfrak{F}$ is a family of d-large pairwise incompatible matchings of a complete bipartite graph with components of sizes u and v, where $u \geq v$. Then:

$$|\mathfrak{F}| \leq d!\binom{u}{d}.$$

Proof. For $v = d$ the claim holds, since the set of all matchings of $K_{u,d}$ satisfies the property above.

For any v-large matching of $K_{u,v}$ denoted as M, it holds that any two submatchings of M are compatible, and so $\mathfrak{F}$ can contain at most one d-large submatching of M.

There are $d!\binom{u}{d}\binom{v}{d}$-many different d-large matchings of $K_{u,v}$ and, since each d-large matching of $K_{u,v}$ can be extended to $(v-d)!\binom{u-d}{v-d}$-many v-large matchings, it follows that:

$$|\mathfrak{F}| \leq v!\binom{u}{v} \cdot \frac{1}{(v-d)!\binom{u-d}{v-d}} = \frac{u!}{(u-d)!}\frac{(u-v)!}{(u-d)!} = d!\binom{u}{d}.$$

□

The the upper bound given above is tight, since we can produce a set of pairwise incompatible d-large matchings of size $d!\binom{u}{d}$ by picking d elements from the smaller component of $K_{u,v}$ and defining S to be the set of all d-large matchings which cover the elements we have picked.

We can, finally, combine the Lemmas 2.3.11 and 2.3.10 to prove the following theorem.

Theorem 2.3.12. An array $A^c_{n,m}$ does not exist for any finite c.

Proof. Assume such an array exists and denote it A. Each row A_a satisfies the conditions of the lemma 2.3.10 and so we can create sets A'_a as in the lemma.

We now create a new array A'. For each $a \in [2m]$ and $b \in [m]$ we put τ from A'_a inside $A'(a,b)$ if and only if τ extends some $\sigma \in A(a,b)$. Due to the Lemma 2.3.10, it follows that each τ extends some σ from A_a and such σ is unique, so A' is well-defined.

Notice that for any $a \in [2m]$ and $b, b' \in [m]$ it is true that for any two different $\tau \in A'(a,b)$ and $\tau' \in A'(a,b')$ it holds that $\tau \perp \tau'$. This holds, since τ extends some $\sigma \in A(a,b)$ and τ' extends some $\tau' \in A(a,b')$ and, since $\tau \neq \tau'$, it follows that $\sigma \neq \sigma'$, implying $\sigma \perp \sigma'$. Then, clearly, $\tau \perp \tau'$.

The same is true for different τ, τ' from the same column, i.e. $\tau \perp \tau'$.

Let us now calculate:

$$N = \sum_a |\bigcup_b A(a,b)| = \sum_b |\bigcup_a A(a,b)|.$$

The Lemma 2.3.11 implies:

$$N \leq m \cdot (2c^2)!\binom{n+1}{2c^2},$$

while 2.3.10 and the way A' is constructed implies:

$$2m \cdot (2c^2)!\binom{n}{2c^2} \leq N.$$

Combining these two inequalities, gets us:

$$2 \leq \frac{n+1}{n-2c^2},$$

which is a contradiction, since n is non-standard and c is finite and $\mathbb{M}$ is a model of true arithmetic. □

So $A^c_{n,m}$ does not exist for any non-standard n, m and finite c. This implies $\sigma = \emptyset$ can be extended to some $\tau \in P$ so that $\tau \Vdash WPHP^{2m}_m(\theta(x,y))$ for fixed non-standard m and an $L_{PA}(R)$-formula with parameters $\theta(x,y)$.

Recall that we are trying to show that the set of all conditions which force $WPHP^{2m}_m(\theta(x,y))$ is dense. This will imply:

$$\emptyset \Vdash WPHP(open(R)),$$

finishing the proof of 2.3.2 and, in turn, the Theorem 2.3.1.

So pick $\sigma \in P$ and assume it can not be extended to any $\tau \in P$ so that $\tau \Vdash WPHP^{2m}_m(\theta(x,y))$. By the same arguments as for $\sigma = \emptyset$ (2.3.7), this implies the existence of an array $A^c_{n,m,\sigma}$ denoted as A, which satisfies all the properties of $A^c_{n,m}$ plus all it's members are partial functions between $[n+1] \setminus Dom(\sigma)$ and $[n] \setminus Im(\sigma)$, where $Dom(\sigma)$ denotes the domain of σ and $Im(\sigma)$ denotes the image of σ. This condition is important, since we are now focusing only on those $\tau \in P$ which extend σ, which is the same as to work with those partial injective functions, whose domains are inside $[n+1] \setminus Dom(\sigma)$ and whose ranges are inside $[n] \setminus Im(\sigma)$.

Then, we proceed in the exact same way as in the Theorem 2.3.12 and create a new array A' whose rows are of size $\geq (2c^2)!\binom{n-|\sigma|}{2c^2}$ and which satisfies first two conditions of $A^{2c^2}_{n,m}$-arrays. This can be done in the same way as in the Lemma 2.3.10 by considering PHP-trees over $[n+1] \setminus Dom(\sigma)$ and $[n] \setminus Im(\sigma)$, instead of the ones over $[n+1]$ and $[n]$.

Finally, we count:

$$N = \sum_a |\bigcup_b A'(a,b)| = \sum_b |\bigcup_a A'(a,b)|.$$

The Lemma 2.3.11 implies $N \leq m \cdot (2c^2)!\binom{n+1-|\sigma|}{2c^2}$ and the way A' is constructed implies $N \geq 2m \cdot (2c^c)!\binom{n-|\sigma|}{2c^2}$. Combining these two inequalities, gets us:

$$2 \leq \frac{n+1-|\sigma|}{n-|\sigma|-2c^2},$$

which is a contradiction, since n is non-standard and c, $|\sigma|$ are finite. This finishes the proof of 2.3.2 and, in turn, of 2.3.1.

Let us briefly summarize the proof. We have started with a model of $Th(\mathbb{N})$, denoted as $\mathbb{M}$. We have then considered P to be a set of all partial injective functions from $[n+1]$ to $[n]$ of standard sizes. Using 2.2.6 we have established:

$$\emptyset \Vdash \neg ontoPHP(R),$$

and, using 1.2.4:

$$\emptyset \Vdash I\exists_1(R).$$

The next step was to show:

$$\emptyset \Vdash WPHP^{2m}_m(\theta(x,y))$$

for any open $L_{PA}(R)$-formula with parameters $\theta(x,y)$ and $m \in \mathbb{M}$. We have achieved this by showing a stronger statement, i.e. that the set of all conditions forcing $WPHP^{2m}_m(\theta(x,y))$ is dense-definable, where definability easily followed from the Propositions 2.2.13, 2.2.12 and 2.2.11.

Density of the above set was proved by contradiction. Assuming the above set was not dense and σ being the witness, we have defined an array $[\theta(a,b)]$ and showed that such array satisfied properties (2.1), (2.2) and (2.3). Finally, by combinatorial arguments (2.3.11) and (2.3.10), we have proved that an array satisfying mentioned properties cannot exist (2.3.12).

3. WPHP for polynomial-time machines

3.1 Case for $T^1_2(R)$

We will now prove the Theorem 1.2.5:

$$T^1_2(R) \nvdash ontoPHP(R),$$

using the forcing machinery from previous section (the original proof used proof theory and witnessing functions).

Proof. Recall that $T^1_2(R)$ is axiomatized by the least number principle for all $\Sigma^b_1(R)$-formulas. To proceed as in the proof of 1.2.4, we need to pick a countable non-standard model of $Th(\mathbb{N})$ denoted $\mathbb{M}$. Pick some non-standard n from $\mathbb{M}$. We consider a cut $\mathbb{M}_n \subseteq \mathbb{M}$ defined as:

$$\{a \mid a \leq 2^{|n|^c}, c \text{ is standard}\}.$$

Similarly to the Theorem 1.1.5 it is possible to show that $\mathbb{M}_n$ is a model of T_2. This $\mathbb{M}_n$ would serve as a base model which we want to expand by interpreting R.

Define P^* as the set containing all the partial injective functions between $[n+1]$ and $[n]$ of sizes $\leq |n|^c$, for some standard number c. This means each such condition σ is coded by some $w \in \mathbb{M}_n$ so that $len(w) \leq |n|^c$ for some standard c dependent on w.

Propositions 2.2.6 and 2.2.7 are true for P^*, implying:

$$\emptyset \Vdash \neg ontoPHP(R).$$

We will now show that the set of all conditions forcing the least number principle for $\Sigma^b_1(R)$-formulas with parameters from $\mathbb{M}_n$ is dense-definable. So let $\theta(x)$ be such formula and let σ be from P^*. It is possible to represent each instance $\theta(a)$ as a DNF inside $\mathbb{M}_n$. To achieve this, first push negations inside the atomic subformulas of $\theta(a)$. Then, replace universal and existential quantifiers by conjunctions, respectively disjunctions, over all possible witnesses. Finally, put the formula into DNF denoted D. Since all the quantifiers are bounded, this formula is well-defined in $\mathbb{M}_n$. Note that all the universal quantifiers in the original instance $\theta(a)$ (after we push the negation to the atomic subformulas) are bounded by $|n|^c$ for some standard c. So, all the DNF-terms of D are of the size $\leq |n|^d$, for some standard d dependent on $\theta(a)$ only, since $|2^{|n|^{c_1}}|^{c_2} = |n|^{c_1 \cdot c_2}$.

Assume $\sigma \nVdash LNP(\theta(x))$ and let G be a generic filter extending σ for which $(\mathbb{M}_n, G) \models \theta(a)$ for some $a \in \mathbb{M}_n$. As in the proof of 1.2.4, it is possible to find some $\tau \supseteq \sigma$ so that:

$$\tau \Vdash \theta(a).$$

We can also show that the size of such τ can be made $\leq |\sigma| + |n|^d$, for some standard d dependent on $\theta(a)$ only. Again, as in the proof of 1.2.4, we can then define a set:

$$\{b \mid b \leq a \wedge \exists \tau(\tau \supseteq \sigma \wedge |\tau| \leq (|\sigma| + |n|^d) \wedge \tau \Vdash \theta(a))\}.$$

Since $\mathbb{M}_n$ is a model of T_2, this set has the least element e. It follows that there exists $\tau \supseteq \sigma$ so that $|\tau| \leq |\sigma| + |n|^d$ and $\tau \Vdash \theta(e)$, while for any $b < e$ there is no $\tau' \supseteq \sigma$ and subsequently $\tau' \supseteq \tau$ forcing $\theta(b)$, thus showing $\tau \Vdash LNP(\theta(x))$.

□

3.2 Polynomial-time machines

We are now ready to prove the main theorem of the thesis.

Theorem 3.2.1.

$$T_2^1(R) + WPHP(\Box_1^p(R)) \nvdash ontoPHP(R).$$

Proof. We have already shown:

$$\emptyset \Vdash \neg ontoPHP(R),$$

and:

$$\emptyset \Vdash T_2^1(R).$$

We are left to prove:

$$\emptyset \Vdash WPHP(\Box_1^p(R)),$$

which we will show by arguing that the set of all conditions from P^* forcing $WPHP_m^{2m}$ for any fixed polynomial-time machine with an oracle access to R is dense-definable (as usual, definability of such set is clear and so we will focus on density).

Let M be such a machine and assume $\sigma \in P^*$ cannot be extended to any τ so that $\tau \Vdash WPHP_m^{2m}(M)$. We can then create a two-dimensional array A^* indexed by $[2m] \times [m]$, such that $A^*(a, b)$ contains maximal paths in the computation tree of M on input (a, b) corresponding to the computation asserting (a, b) is accepted. Since $T_2^1(R)$ extends $S_2^1(R)$, it follows that such tree is bounded in depth by $|n|^c$. Each path of this tree is a conjunction of atomic and negated atomic statements $R(s, t)$ and we can represent it by all $\subseteq$-minimal maps from P^* compatible with the answers. Note that each such map has the size bounded by $|n|^c$, for some standard c dependent on the given map.

Proceeding as in the proof of 2.3.5, we derive that such an array, denoted A^*, satisfies the following properties:

$$\forall a, a' \in [2m]\, \forall b \in [m]\, \forall \sigma \in A^*(a, b)\, \forall \sigma' \in A^*(a', b)\, (\sigma \neq \sigma') : \sigma \perp \sigma', \qquad (3.1)$$

$$\forall a \in [2m]\, \forall b, b' \in [m]\, \forall \sigma \in A^*(a, b)\, \forall \sigma' \in A^*(a, b')\, (\sigma \neq \sigma') : \sigma \perp \sigma', \qquad (3.2)$$

$$\forall a \in [2m]\, \forall \tau \in P^* \, \exists b \in [m]\, \exists \sigma \in A^*(a,b) : \tau \| \sigma. \tag{3.3}$$

We then proceed as in the Theorem 2.3.12 and prove that such an array cannot exist, since, otherwise, we could extend it to an array $(A^*)'$ so that that each row of $(A^*)'$ contained $\geq (2|n|^{2c})!\binom{n+1-|\sigma|}{2|n|^{2c}}$ different functions and each column of $(A^*)'$ contained $\leq (2|n|^{2c})!\binom{n-|\sigma|}{2|n|^{2c}}$ different functions. Then, since $|\sigma| \leq |n|^l$ for some standard l, it would follow:

$$2 \leq \frac{n+1-|n|^l}{n-|n|^l-2|n|^{2c}},$$

which is a contradiction, since n is non-standard and both c and l are standard.

□

Using the same ideas as in the above proof, we can show the following statement, which has been already discussed in the first chapter.

Theorem 3.2.2.

$$T^1_2(R) + PHP^{\frac{n}{2}+1}_{\frac{n}{2}}(\Box^p_1(R)) \nvdash ontoPHP(R).$$

Proof. As before, assuming that the statement is not true, we create an array indexed by $[\frac{n}{2}+1] \times [\frac{n}{2}]$ which satisfies the properties (3.1), (3.2), (3.3). Then:

$$(\frac{n}{2}+1)(2|n|^{2c})!\binom{n-|n|^k}{2|n|^{2c}} \leq \frac{n}{2}(2|n|^{2c})!\binom{n+1-|n|^k}{2|n|^{2c}},$$

implying:

$$(\frac{n}{2}+1)(n-|n|^k-2|n|^{2c}) \leq \frac{n}{2}(n+1-|n|^k).$$

The above inequality leads to:

$$n-|n|^k-2|n|^{2c}(\frac{n}{2}+1) \leq \frac{n}{2},$$

which is a clear contradiction. □

Conclusion

In Section 1.1 we have described several basic arithmetic theories. In Section 1.2 we have defined pigeonhole principles and formulated the main theorem of the thesis. We have also stated an open problem posed by Ajtai [1990][page 3] regarding mutual unprovability of the pigeonhole principle for different parameters over the bounded arithmetic theory T_2.

In Section 2.1 we have showed a proof of the theorem of Paris and Wilkie [1985]. We have then developed some theory behind the forcing and reinterpreted the proof of the previous section's theorem in the new language. In Section 2.3 we have showed a proof of an easier variant of the main theorem. To achieve this, we have defined certain combinatorial structures and, using different counting arguments, proved that such structures cannot exist.

In Section 3.1 we have provided a proof of the theorem of Krajíček [1995][12.7], which can be thought of as a modification of the Theorem of Paris and Wilkie [1985] for the extended arithmetical language and corresponding theory. In Section 3.2 we have provided a proof for the main theorem and stated some corollaries.

As we have already discussed, direct proofs in T_2^1 provide bounds for propositional proofs (Krajíček [2019][10.5.1]) and witnesses to certain algorithmical problems (Krajíček [1995][7.2.3]). The next possible step after the proof of the main theorem would be to treat those connections and, possibly, derive some interesting results in the corresponding areas of mathematical logic.

We have also answered an easier version of the open problem posed by Ajtai [1990][page 3] and so it is tempting to ask, whether it is possible to achieve stronger results using the methods we have developed.

Bibliography

L. Adleman and K. Manders. Reducibility, randomness, and intractability. In *Proceedings of the 9th Annual ACMS Symposium on Theory of Computing*, pages 151 – 163, 1977.

M. Ajtai. The complexity of the pigeonhole principle. In *Proceedings of the IEEE 29th Annual Symposium on Foundations of Computer Science*, pages 346 – 355, 1988.

M. Ajtai. Parity and the Pigeonhole Principle. In S. Buss and P. Scott, editors, *Feasible mathematics*, Progress in Computer Science and Applied Logic, pages 1 – 24. Birkhäuser, 1990. ISBN 978-0-8176-3483-4.

J. H. Bennett. *On Spectra.* PhD thesis, Princeton University, 1962.

S. R. Buss. *Bounded Arithmetic.* PhD thesis, Princeton University, 1985.

A. Church. A set of postulates for the foundation of logic. *Annals of Mathematics. Series 2.*, 33(2):346 – 366, 1932.

A. Church. A note on the Entscheidungsproblem. *Journal of Symbolic Logic*, 1: 40 – 41, 1936.

A. Cobham. *The intrinsic computational difficulty of functions*, pages 24 – 30. Studies in logic and the foundations of mathematics. North - Holland, 1965.

P. Hájek and P. Pudlák. *Metamathematics of first-order arithmetic.* Perspectives in Mathematical Logic. Springer-Verlag, 1993. ISBN 978-1107168411.

J. Håstad. *Computational limitations of small depth circuits.* PhD thesis, Massachusetts Institute of Technology, 1987.

G. O. H. Katona. A simple proof of the erdös-chao ko-rado theorem. *Journal of Combinatorial Theory, Series B*, 13(2):183 – 184, 1972.

R. Kaye. *Models of Peano Arithmetic.* Oxford Logic Guides. Oxford Science Publications, Oxford, 1991. ISBN 978-0198532132.

S. C. Kleene. Recursive predicates and quantifiers. *Transactions of the American Mathematical Society*, 53:41 – 73, 1943.

S. C. Kleene. *Introduction to Metamathematics*, chapter 71. North - Holland, 1952. ISBN 9780720421033.

J. Krajíček. *Bounded Arithmetic, Propositional Logic and Complexity Theory.* Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1995. ISBN 9780511529948.

J. Krajíček. *Proof Complexity.* Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 2019. ISBN 9781108242066.

J. Krajíček, P. Pudlák, and A. Woods. Exponential lower bound to the size of bounded depth frege proofs of the pigeonhole principle. *Random Structures and Algorithms*, 7:15 – 39, 1995.

Y. Matiyasevich. Hilbert's Tenth Problem. *MIT Press*, 1993.

V. Nepomnjascij. Rudimentary predicates and Turing calculations. In *Doklady AN SSSR*, page 195, 1970.

J. Parikh. Existence and feasibility in arithmetic. *J. Symbolic Logic*, 36:494 – 508, 1971.

J. Paris and A. J. Wilkie. Delta zero sets and induction. In *Proceeding of the Jadwisin Logic Conference, Poland*, pages 237 – 248, 1981.

J. Paris and A. J. Wilkie. Counting problems in bounded arithmetic. pages 332 – 334, 1985.

J. Paris and A. J. Wilkie. Counting Delta zero sets. *Fundamenta Mathematica*, 127:67 – 76, 1987.

J. Paris, A. J. Wilkie, and A. R. Woods. Provability of the pigeonhole principle and the existence of infinitely many primes. *J. Symbolic Logic*, 53:1235 – 1244, 1988.

J. B. Paris. O struktuře modelu omezené E_1 indukce (in Czech). *Časopis pěstování matematiky*, 109:372 – 379, 1984.

T. Pitassi, P. Beame, and R. Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Random Structures and Algorithms*, 7:15 – 39, 1995.

H. Rogers. *Theory of Recursive Functions and Effective Computability*, chapter 9.6. Fifth Edition. The MIT Press, Massachusetts, 1967. ISBN 978-0262680523.

L. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3:1 – 22, 1977.

S. Tennenbaum. Non-archimedean models of arithmetic. *Notices of the A.M.S.*, 6:270, 1959.

A. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society. 2.*, 42:230 – 265, 1936.

A. Wilkie. On sentences interpretable in systems of arithmetic. In *Logic Colloquim '84*, pages 329 – 342, 1986.

C. Wrathall. Rudimentary predicates and relative computation. *SIAM Journal on computations*, 7(2):149 – 209, 1978.