Warsaw University
Faculty of Mathematics, Informatics and Mechanics

Konrad Zdanowski

Arithmetics in finite but potentially infinite worlds

Arytmetyki w skończonych,
lecz potencjalnie nieskończonych światach

Ph.D. Thesis

Thesis Advisor:
Prof. Marcin Mostowski

$\forall\ \exists$
$\forall\ \exists$

28th February 2005

Abstract

Let $\mathrm{FM}(\mathcal{A})$, for $\mathcal{A} = (\omega, \bar{R})$, be the family of finite models being initial segments of $\mathcal{A}$. The thesis investigates logical properties of families of the form $\mathrm{FM}(\mathcal{A})$ for various arithmetics like arithmetic of addition and multiplication, Skolem arithmetic of multiplication, arithmetic of coprimality, of exponentiation and arithmetic of concatenation. We concentrate on questions such as decidability of various theories of $\mathrm{FM}(\mathcal{A})$; definability and interpretability of one arithmetic, $\mathrm{FM}(\mathcal{A})$ in another, $\mathrm{FM}(\mathcal{B})$; the problem of representing infinite relations in such families of models and on the spectrum problem for such arithmetics.

Following M. Mostowski ([31, 32]), we define some methods which one can use to represent infinite relations in finite models and some natural theories of families $\mathrm{FM}(\mathcal{A})$, such as the set of sentences true in almost all finite models from $\mathrm{FM}(\mathcal{A})$, $\mathrm{sl}(\mathrm{FM}(\mathcal{A}))$, or the set of sentences which are almost surely true in $\mathrm{FM}(\mathcal{A})$ (in a probabilistic sense). We show that for $\mathcal{A} = (\omega, +, \times)$, the first set is Σ_2–complete and the second one is Π_3–complete. We also characterize relations which can be represented in both theories as exactly Δ_2 relations (for the first theory such a characterization was obtained in [31]). We show that the above remains true even in the relatively weak arithmetic of multiplication.

We also consider various notions of definability and interpretability between arithmetics of finite models. We give the definition of $\mathrm{FM}((\omega, +, \times))$ in the finite models of arithmetic of concatenation. This is an analogous to the situation in the infinite models for these arithmetics but one should use a different method to give a suitable definition.

We show that, contrary to the infinite case, arithmetic of exponentiation, $\mathrm{FM}((\omega, \exp))$, is definable from arithmetic of multiplication only, $\mathrm{FM}((\omega, \times))$. We also give interpretations of $\mathrm{FM}((\omega, +, \times))$ in arithmetic of coprimality, $\mathrm{FM}((\omega, \perp))$, and in $\mathrm{FM}((\omega, \exp))$. The interpretations reveal that in finite models coprimality or exponentiation are as hard as the full arithmetic of addition and multiplication, which is especially surprising in the case of coprimality. We also describe the decidability border for finite model arithmetic of multiplication showing that the Σ_1–theory of $\mathrm{FM}((\omega, \times, \leq))$ is decidable while the Σ_2–theory of $\mathrm{FM}((\omega, \times))$ is undecidable. We close the thesis with a partial characterization of families of spectra for $\mathrm{FM}((\omega, \times))$ and $\mathrm{FM}((\omega, \exp))$.

Streszczenie

Praca poświęcona jest badaniu logicznych własności arytmetyki w skończonych modelach. Arytmetykę taką charakteryzujemy jako rodzinę modeli będących odcinkami początkowymi modelu $\mathcal{A} = (\omega, \bar{R})$ i oznaczamy przez $\mathrm{FM}(\mathcal{A})$. W szczególności zajmujemy się arytmetyką dodawania i mnożenia, samego mnożenia (znaną jako arytmetyka Skolema), arytmetyką konkatenacji, arytmetyką funkcji wykładniczej oraz arytmetyką relacji względnej pierwszości. Badamy stopień trudności teorii skończonych arytmetyk $\mathrm{FM}(\mathcal{A})$; definiowalność oraz interpretowalność pomiędzy takimi arytmetykami; jak można w nich reprezentować nieskończone relacje oraz problem spektrum dla takich rodzin.

Opierając sie na pracy Marcina Mostowskiego [31] definiujemy sposoby, na jakie można reprezentować w skończonych arytmetykach nieskończone relacje. Rozważamy FM–reprezentowalność (zdefiniowaną w [31]), słabą FM–reprezentowalność oraz reprezentowalność w sensie probabilistycznym. Rozważamy także teorie zdań prawdziwych w prawie wszystkich modelach z $\mathrm{FM}(\mathcal{A})$, oznaczaną $\mathrm{sl}(\mathrm{FM}(\mathcal{A}))$, oraz zdań, dla których prawdopodobieństwo prawdziwości w dostatecznie dużych modelach dąży do jedności. Pokazujemy, że dla $\mathcal{A} = (\omega, +, \times)$ pierwsza z teorii jest Σ_2 a druga Π_3–zupełna. Pokazujemy także, że w obu teoriach można reprezentować dokładnie relacje Δ_2. Co więcej, wyniki te pozostają prawdziwe również dla arytmetyki samego mnożenia, $\mathrm{FM}((\omega, \times))$.

Rozpatrujemy także związki pomiędzy skończonymi arytmetykami względem różnych pojęć interpretowalnośći. Podajemy definicje dodawania i mnożenia w skończonych modelach arytmetyki konkatenacji słów nad n elementowym alfabetem, dla $n \geq 2$. Pokazujemy także, że, w przeciwieństwie do sytuacji w nieskończonej dziedzinie, funkcja wykładnicza $\exp(x, y) = x^y$ jest definiowalna już w skończonej arytmetyce mnożenia. Podajemy także intereptacje $\mathrm{FM}((\omega, +, \times))$ w $\mathrm{FM}((\omega, \exp))$ a także w skończonej arytmetyce relacji względnej pierwszości, $\mathrm{FM}((\omega, \perp))$. Jako wniosek otrzymujemy, że obie z tych arytmetyk arytmetyki są w skończonych modelach równie trudne co $\mathrm{FM}((\omega, +, \times))$. Jest to szczególnie zaskakujące w przypadku arytmetyki względnej pierwszości.

Pokazujemy także rozstrzygalność Σ_1 teorii mnożenia i porządku oraz nierozstrzygalność Σ_2 teorii tej arytmetyki.

Pracę zamyka częściowa charakteryzacja spektr dla arytmetyk postaci $\mathrm{FM}(\mathcal{A})$.

Acknowledgements

Obviously, during all the years of writing this thesis it was influenced by many people. Here I will try to recall the most important ones.

In the first place I want to thank my thesis supervisor, Marcin Mostowski. He suggested investigating into the topic, was the source of inspiration and some parts of this work were done in cooperation with him. Then I want to thank Michał Krynicki. We started our joint work on finite arithmetics two years ago and since that time it has been one of the most stable scientific relationships that I had. The thesis has also profited from the comments made by Jurek Tomasik.

I spent many hours talking about arithmetic with Zosia Adamowicz and Henryk Kotlarski. Although we mainly talk about nonstandard models for Peano arithmetic and its subtheories, these conversations taught me a lot and made the universe of arithmetical structures more familiar to me.

I also thank Małgosia Maciejewska and Leszek Kołodziejczyk for correcting the English of some parts of the thesis.

Last but not least I want to thank to the people at Institute of Philosophy of Warsaw University for a good, friendly atmosphere. Among others, I am thinking about Cezary Cieśliński, Nina Gierasimczuk, Jakub Szymanik, Ania Wasilewska and Dominika Wojtyniak.

Contents

Hence this infinite is potential, never actual: the number of parts that can be taken always surpasses any assigned number. But this number is not separable from the process of bisection, and its infinity is not a permanent actuality but consists in a process of coming to be, like time and the number of time. [...]

Our account does not rob the mathematicians of their science, by disproving the actual existence of the infinite in the direction of increase [...]. In point of fact they do not need the infinite and do not use it. They postulate only that the finite straight line may be produced as far as they wish. It is possible to have divided in the same ratio as the largest quantity another magnitude of any size you like. Hence, for the purposes of proof, it will make no difference to them to have such an infinite instead, while its existence will be in the sphere of real magnitudes.

Aristotle "Physics", Book 3, part 7.
Translated by R. P. Hardie and R. K. Gaye.

Chapter 1

Introduction

1.1 Motivations

This work considers logical properties of arithmetical relations in finite but potentially infinite models. Intuitively, in such a model we can manipulate only with finitely many integers, but we always can enlarge the number of available entities. A mathematical framework capturing this intuition can be obtained by considering a family of finite approximations of an infinite model instead of considering just this infinite model.

This is similar to our situation in the real world. Without deciding whether the world is finite or infinite, when we consider our combinatorial abilities, we realize that we always deal with finitely many objects. There is no exact limit on the number of these objects but in each moment we can access only finitely many of them. In other words, while we agree that the successor operation can be always performed on a given integer n, we deny that this forces the actual infinity of the set of integers. While performing the successor operation on the maximal element of a model we may realize that we reached the limits of our actual world and we may try to enlarge it. This can be done either by incorporating new elements or new concepts like sets, or sets of sets of objects. These are the ways to make a step into a bigger but still finite model.

The motivation for investigating arithmetic in such a framework comes from three main sources. The first one is an attempt to give a description of computations which fits more closely to the computations which we carry out using our machines and which incorporates the limits of our computational abilities. In a very rough way, such a limit can be described by the condition that the number of integers we can manipulate with is finite, although potentially infinite.

Let us consider an example of computing the sequence of Fibbonaci numbers. The sequence of Fibonacci numbers $\{F_i\}_{i=0,1,2,\ldots}$ is defined by the following recursive equations:

$$F_0 = F_1 = 1,$$

$$F_{i+2} = F_i + F_{i+1}.$$

Let us see, what happens if we write a program for generating Fibonacci numbers based on the above equations. The author of this thesis has got the following results:

$$F_{44} = 1134903170,$$

$$F_{45} = 1836311903,$$

$$F_{46} = -1323752223.$$

These values were obtained using variables of the type **int** and programming language C. What happened here is, of course, an overflow.[1] The size of F_{46} is bigger than the size of variables of type **int**. The sequence of Fibonacci numbers grows so fast that we cannot compute numbers F_i for $i \geq 46$ using the arithmetic given by the type **int**. In a sense, we reached the limits of this finite arithmetic.

A remedy for this situation is to use a type of a bigger size e.g. **long int** or, better, **long unsigned int**, which may represent a bigger set of integers greater than zero. However, both of these arithmetics are still finite. Next, we may implement some data structures for manipulating even bigger numbers. Nevertheless, still we are limited by the finite size of the memory of our computer. We may buy some more memory chips ...

Whatever we do we see that the arithmetic we are using is the arithmetic of a finite world. This world may be enlarged but at each point of computation it is finite. Thus, our work describes properties of such arithmetics, arithmetics of computers we are using.

Our second motivation comes from descriptive complexity theory and an increasing importance of finite model theory in logic and complexity theory. The theorems of Fagin (see [11]), Immerman and Vardi (see [18], [19], [52]) show that there is a strict correspondence between the complexity of deciding a given problem and the logical formalism in which one can describe it. Thus, instead of machines and input strings one can equivalently consider formulas and finite models. Much of such, so called, feasible–descriptive correspondence depends on a "built in arithmetic"– a set of arithmetical relations available in finite models and treated as logical notions. For instance NLOGSPACE – transitive closure logic correspondence assumes that models

[1] A carefully written program should detect such an event and signal it to a user.

are equipped with standard linear ordering. When we consider weaker logics we need more arithmetic. So, alternating logarithmic time corresponds to first order logic with built in addition and multiplication. (For these results see [20].) Thus, investigating properties of various arithmetics in finite models also leads to a better understanding of the relation between logics and complexity classes.

Last but not least, there is a philosophical motivation for this work which is the old question of how we can justify the use of infinitistic methods in mathematics and their applicability to the real world. For example we treat time as a continuum isomorphic to the real line although there can be no evidence for time being not discrete. It seems that assuming actual infinity of the world is a bit risky. Especially now, when physicists try to estimate the actual number of particles in the world. So the question arises how we can ground our use of infinitistic methods in investigating properties of a finite world like ours. In the context of mathematical analysis such a question was successfully answered by Mycielski in [36] (see also [37]). He shows there how one can reinterpret the notations and tools of analysis when we do not assume the actual infinity of our world (which may be the real world situation) and when all values that we can measure are rational.

In this thesis we follow the work of Marcin Mostowski (see [31], [32]) and investigate the ways in which we are able to consider infinite relations when we are in a finite model. The aim of Mostowski was to transfer the methods from infinite model theory, such as truth definitions, into a finite model context (see also papers by Kołodziejczyk, [22] and [21]). Along these lines, we investigate which infinite families of relations can be represented in finite models and in what sense.

We open this thesis with a quotation from Aristotle with the intention to stress that infinity was a problem from the very beginings of science. The ways in which we approach infinite objects, as well as their mere existence, were questioned many times. Moreover, it is still not obvious how our use of infinity can be helpful in recognizing properties of our finite world. Although the present thesis does not solve these problems, it certainly contributes to better understing of the relation between the finite and the infinite.

1.2 Results

The results of this thesis can be organized around three main themes:

1. Which infinite relations can be represented in finite models and how?

2. What is the decidability border for arithmetics of finite models?

3. What are interpretability dependencies between finite arithmetics?

Ad. 1 Following the definition of FM–representability (meaning **F**inite **M**odel representability) given by M. Mostowski in [31], we define three methods of representing infinite relations in finite models: weak FM–representability, statistical representability and weak statistical representability. We show that the relations which can be represented by these methods are the Σ_2, Δ_2 and Π_3 relations, respectively. Thus, the second of these methods is no more powerful than the original FM–representability concept introduced by Mostowski while the first and the latter allow to represent some new relations, although the sense in which we can weakly statistically represent relations is rather poor from the epistemic point of view. These results are presented in [35]. The results related to statistical representability are of the author of this thesis. All other results are joint with Marcin Mostowski. The weakest known arithmetical notion sufficient for FM–representability of all Δ_2 relations is divisibility (see M. Mostowski and A. Wasilewska [33]).
Ad. 2 The second topic corresponds closely with the first. Indeed, a description of the class of relations representable in a given arithmetic allows to establish whether it is decidable or not. We show that if the standard ordering is definable in the infinite model version of a given arithmetic, then its finite model version can be interpreted in the infinite model. Thus, decidability results carry over from the infinite model to finite models. On the other hand, if ordering is not definable we show that even when the infinite model arithmetic has the decidable first order theory, its finite model version may become undecidable. The weakest arithmetic for which we know this happens is the arithmetic of coprimality. This was proven by the author of this dissertation and M. Mostowski, [34]. We also estimate the decidability border for the arithmetic of multiplication showing that the $\exists^*\forall^*$ finite model theory of multiplication is undecidable while the $\exists^*$ finite model theory of multiplication with ordering is decidable. The latter result is shown by estimating the size of a finite model for a $\exists^*$ formula. These results are joint with M. Krynicki, [25].

We consider also the set of sentences which are true in almost all finite models of a given arithmetic or almost surely true (in a probabilistic sense). We show that for arithmetic of addition and multiplication the first of these sets is Σ_2–complete (a joint result with M. Mostowski) while the latter is Π_3–complete in the arithmetical hierarchy. We also give a characterization of the first of these theories in terms of ultraproducts. Using this characterization we show that this theory has continuum many consistent extensions.
Ad. 3 We show that the finite model arithmetic of concatenation defines arithmetic of addition and multiplication. Thus, the former is as powerful as

the latter. This is a result of the author published in [25]. We also show that exponentiation is definable in finite models by means of multiplication only. This contrasts with the infinite model situation where exponentiation is as powerful as addition and multiplication while sole multiplication is strictly weaker. This is a joint result with M. Krynicki, [25].

We introduce various methods of interpreting one arithmetic of finite models into another, such as sl–interpretability and the stronger notion of IS–interpretability. We recall the result from M. Mostowski and Zdanowski [34] that even the relatively weak arithmetic of coprimality can sl–interpret addition and multiplication. We also show that multiplication or exponentiation can IS–interpret addition and multiplication. In the meantime a stronger result was obtained that divisibility relation instead of multiplication is sufficient, see M. Mostowski and A. Wasilewska [33]. As a corollary, we obtain equality between the classes of FM–representable relations in these arithmetics.

In principle all the theorems without references are firstly proven by the author of this dissertation.

1.3 An outline of the thesis

In the second chapter of the thesis we present basic notions like first order interpretations, Ehrenfeucht–Fraïsse games, and some concepts from recursion theory needed in this work.

The third chapter introduces three classical arithmetics: of addition and multiplication, of words with concatenation, and of hereditarily finite sets with the "belongs to" predicate. Then, for a given infinite model on natural numbers $\mathcal{A} = (\omega, \mathcal{R})$, we define the family, $\mathrm{FM}(\mathcal{A})$, of finite models which are finite initial segments of $\mathcal{A}$. The main result of this chapter is that the finite arithmetic of words with concatenation is as powerful in finite models as the two others classical arithmetics mentioned above.

In the fourth chapter we introduce the notion of FM–representability, following M. Mostowski [31, 32]. This concept was designed to enable expressing in finite models the notions which were originally used in infinite model theory, e.g. truth definitions. A (possibly infinite) relation $R \subseteq \omega^r$ is FM–represented in $\mathrm{FM}(\mathcal{A})$ by a formula φ if each finite fragment of R is correctly described by φ in almost all finite models from $\mathrm{FM}(\mathcal{A})$. It was shown in [31] that exactly the Δ_2 relations are FM–represented in $\mathrm{FM}((\omega, +, \times, \leq))$. Moreover, if the relation of truth between finite models from $\mathrm{FM}(\mathcal{A})$ and formulas is decidable, then no relation outside Δ_2 can be FM–represented in $\mathrm{FM}(\mathcal{A})$. At the end of the chapter we give a characterization of the set, $\mathrm{sl}(\mathrm{FM}(\mathcal{A}))$, of

sentences true in almost all models from $\mathrm{FM}(\mathcal{A})$ in terms of ultraproducts. Using this characterization we show that $sl(\mathrm{FM}(\mathcal{N}))$ has continuum many consistent extensions.

In the fifth chapter, we introduce some other methods of representing infinite relations in finite models: weak FM–representability and statistical representability. We describe the semantical power of these methods and, as a consequence, we characterize the complexity of some theories of the family $\mathrm{FM}((\omega, +, \times))$. Namely, we estimate the complexity of determining whether a given sentence is true in almost all models from $\mathrm{FM}((\omega, +, \times))$ or whether it is almost surely true (in a probabilistic sense).

The sixth chapter considers arithmetics which are weaker than the arithmetic of addition and multiplication, mainly arithmetics of multiplication, of exponentiation and of coprimality. We show that in finite models all of them can interpret addition and multiplication, although they are semantically weaker than $\mathrm{FM}((\omega, +, \times))$. As a consequence, we obtain that all of them have Π_1–complete sets of finite model tautologies, unlike in the infinite case where multiplication and coprimality are decidable. Further, we show that in finite models multiplication defines exponentiation. Then, we estimate the decidability border for multiplication with ordering. We show that the $\exists^*\forall^*$ theory of multiplication with ordering is undecidable in finite models and that this result is optimal. We end the chapter by proving strict inclusions between spectra of the above arithmetics. Nevertheless, the complexity of spectra of formulas with multiplication is equal to the complexity of spectra of formulas with addition and multiplication. This means that each set in the spectrum of $\mathrm{FM}((\omega, +, \times))$ is linearly reducible to a set in the spectrum of $\mathrm{FM}((\omega, \times))$.

Chapter 2

Basic notions and tools

In this chapter we fix logical background for our work. In the first section we discuss the basic logical notions. Then, we present the concept of interpretability which is one of the main tools in proving logical relations between various arithmetics. Finally, we discuss some recursion–theoretic notions which are used in some parts of our work in an essential way.

2.1 Formulas and models

We write ω for the set of natural numbers $\{0, 1, 2, \ldots\}$. For a function f $\mathrm{dom}(f)$ is the domain of f and $\mathrm{rg}(f)$ is the range of f. For a function $f\colon A \longrightarrow B$ and a sequence of elements $\bar{a} = a_1, \ldots, a_k \in A^k$ we write $\vec{f}(\bar{a})$ for the sequence $f(a_1), \ldots, f(a_k)$. We write $[a, b]$ for the set of integers $\{a, a+1, a+2, \ldots, b-2, b-1, b\}$.

By a vocabulary we mean a 4-tuple $(\mathbb{P}, \mathbb{F}, \mathbb{C}, \mathrm{ar})$, where $\mathbb{P}$ is the set of predicates, $\mathbb{F}$ is a set of functions symbols, $\mathbb{C}$ is the set of constants and $\mathrm{ar}\colon \mathbb{P} \cup \mathbb{F} \longrightarrow \omega$ is the arity function. We assume that all three sets: $\mathbb{P}$, $\mathbb{F}$ and $\mathbb{C}$ are disjoint. Vocabularies will be denoted by Greek characters σ, τ etc.

Each vocabulary $\sigma = (\{P_i\}_{i \leq s}, \{f_i\}_{i \leq t}, \{c_i\}_{i \leq r}, \mathrm{ar})$ determines the set of terms and formulas in σ. $\mathrm{Var} = \{x_1, x_2, x_3, \ldots\}$ is the set of variables. Variables are denoted also by: $x, y, z, \ldots$, possibly with indexes. The sets of terms, Trm_σ, and formulas, $\mathcal{F}_\sigma$, for a given vocabulary σ are defined inductively. All variables and constants belong to Trm_σ and for each function symbol f_i and $t_1, \ldots, t_{\mathrm{ar}(f_i)} \in \mathrm{Trm}_\sigma$, $f(t_1, \ldots, t_{\mathrm{ar}(f_i)}) \in \mathrm{Trm}_\sigma$. We call a term t simple if it has only one occurrence of a function symbol that is all its arguments are variables or a constants.

An atomic formula is an expression of the form $t = t'$ or $P_i(t_1, \ldots, t_{\mathrm{ar}(P_i)})$,

where $t, t', t_1, \ldots, t_{\mathrm{ar}(P_i)} \in \mathrm{Trm}_\sigma$ and $i \leq s$. The set of formulas $\mathcal{F}_\sigma$ includes all atomic formulas and for each $\varphi, \psi \in \mathcal{F}_\sigma$, $\ulcorner \neg\varphi \urcorner \in \mathcal{F}_\sigma$ and $\ulcorner (\varphi \Rightarrow \psi) \urcorner \in \mathcal{F}_\sigma$. Finally, for each variable x and $\varphi \in \mathcal{F}_\sigma$, $\ulcorner \forall x \varphi \urcorner \in \mathcal{F}_\sigma$. The other propositional connectives: $\wedge, \vee, \Leftrightarrow$, are introduced via their usual definitions in terms of negation and implication. The same convention is applied to the existential quantifier, $\exists$. We write Qx for a universal or existential quantifier binding the variable x.

If there is no occurrence of a quantifier in φ we say that φ is quantifier free. We define the quantifier rank of a formula by induction on the complexity of φ. For atomic formulas φ, $\mathrm{qr}(\varphi) = 0$. $\mathrm{qr}(\neg\varphi) = \mathrm{qr}(\varphi)$ and for $\varphi = \ulcorner \psi \circ \gamma \urcorner$, $\mathrm{qr}(\varphi) = \max(\mathrm{qr}(\psi), \mathrm{qr}(\gamma))$, where $\circ \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$. Finally, $\mathrm{qr}(\forall x\, \varphi) = \mathrm{qr}(\exists x\, \varphi) = \mathrm{qr}(\varphi) + 1$.

We write $\mathrm{Trm}_{\{X_1,\ldots,X_k\}}$ and $\mathcal{F}_{\{X_1,\ldots,X_k\}}$ for the set of terms and formulas, respectively, in the vocabulary consisting of $X_1, \ldots, X_k$ predicates, function symbols and constants. In this case the arity function should be obvious from the context or should not play an important role in a given reasoning.

We distinguish some subclasses of $\mathcal{F}_\sigma$. By Q^*, where $Q \in \{\exists, \forall\}$, we mean the set of quantifier prefixes of the form

$$Qz_1 \ldots Qz_k.$$

Then for two sets of such prefixes K_1 and K_2, K_1K_2 is the set of prefixes which can be formed by concatenation of a prefix from K_1 with a prefix from K_2. With each such class K we associate the class of formulas which begins with a prefix from K followed by a quantifier free formula. Thus, $\exists^*\forall^*$ is the set of prefixes of the form

$$\exists z_1 \ldots \exists z_k \forall y_1 \ldots \forall y_n$$

and the set of formulas of the form

$$\exists z_1 \ldots \exists z_k \forall y_1 \ldots \forall y_n\, \psi,$$

where ψ is a quantifier free formula. Later we introduce also Σ_n and Π_n families of arithmetical formulas, see subsection 3.2.1.

By an inductive construction of φ we mean a sequence of formulas $(\varphi_1, \ldots, \varphi_k)$ such that φ_k is φ and for each $i \leq k$, φ_i is an atomic formula or it is constructed from formulas occurring earlier in the sequence by application of a construction rule for a propositional connective or a quantifier. If a formula ψ occurs in every inductive construction of a formula φ we say that ψ is a subformula of φ. An occurrence of a variable x_i is bounded in φ if there is a subformula of φ of the form $Qx_i\psi$ and this occurrence of x_i is

within this $Qx_i\psi$. Otherwise, an occurrence of x_i is free in φ. A variable x_i is free in φ if it has a free occurrence in φ. The set of all free variables of φ will be denoted as $\mathrm{Free}(\varphi)$. If the formula φ has no free variables, ($\mathrm{Free}(\varphi) = \emptyset$) then it is called a sentence. We will write $\varphi(x_{i_1}, \ldots, x_{i_k})$ to indicate all free variables of φ. In this case $\mathrm{Free}(\varphi) \subseteq \{x_{i_1}, \ldots, x_{i_k}\}$.

A formula φ is in a relation–like form if all its atomic subformulas are of the form $P_i(z_1, \ldots, z_{\mathrm{ar}(P_i)})$, $f_i(z_1, \ldots, z_{\mathrm{ar}(f_i)}) = z_0$ or $z_1 = z_2$, where all the z's are variables or constants. It can be proven by induction on the complexity of a formula that for every formula $\varphi(z_1, \ldots, z_k)$ one can effectively find an equivalent formula $\psi(z_1, \ldots, z_k)$ in a relation–like form.

Now we fix some conventions concerning the semantic for first order logic. By a model $\mathcal{A}$ for a vocabulary σ as above we mean a tuple

$$\mathcal{A} = (A, \{R_i\}_{i \leq s}, \{F_i\}_{i \leq t}, \{a_i\}_{i \leq r}),$$

where A is a nonempty set — the universe of $\mathcal{A}$, denoted also by $|\mathcal{A}|$, $R_i \subseteq A^{\mathrm{ar}(P_i)}$ are relations on the universe of $\mathcal{A}$ interpreting the corresponding predicates of σ, $F_i \colon A^{\mathrm{ar}(f_i)} \longrightarrow A$ are operations on A interpreting corresponding function symbols and $a_i \in A$ are elements of universe which interpret constants of σ. The cardinality of $\mathcal{A}$ is the cardinality of its universe, i.e. $\mathrm{card}(\mathcal{A}) = \mathrm{card}(|\mathcal{A}|)$. The class of all models for σ is denoted by Mod_σ. We also extend the arity function ar from vocabularies to relations and functions of a model $\mathcal{A} \in \mathrm{Mod}_\sigma$. Namely, $\mathrm{ar}(R_i) = \mathrm{ar}(P_i)$, where R_i is the relation corresponding to the predicate P_i and, similarly, $\mathrm{ar}(F_i) = \mathrm{ar}(f_i)$.

For a relation $R \subseteq X^r$, the restriction of R to a set $Y \subseteq X$ is the relation

$$R_{|Y} = \{(a_1, \ldots, a_r) \in R : (a_1, \ldots, a_r) \in Y^r\}.$$

By the restriction of a function $F \colon X^r \longrightarrow X$ to a domain $Y \subseteq X$ we mean the function $F_{|Y} \colon Y^r \longrightarrow X$ such that $F_{|Y}(a_1, \ldots, a_r) = F(a_1, \ldots, a_r)$, for all $(a_1, \ldots, a_r) \in Y^r$.

By a submodel of $\mathcal{A}$ we denote the model $\mathcal{B}$ of the same vocabulary such that the universe of $\mathcal{B}$ is a subset of the universe of $\mathcal{A}$ and the relations (resp. operations) of $\mathcal{B}$ are restrictions of the corresponding relations (resp. operations) of $\mathcal{A}$ to $|\mathcal{B}|$. Moreover, interpretations for constants in $\mathcal{B}$ are the same as in $\mathcal{A}$. Let us observe that in this case $|\mathcal{B}|$ has to contain all the constants from $\mathcal{A}$ and has to be closed on the operations from $\mathcal{A}$. If $X \subseteq |\mathcal{A}|$ then by a restriction of $\mathcal{A}$ to X, $\mathcal{A}_{|X}$ we denote the submodel of $\mathcal{A}$ with the universe X, assuming that this restriction is properly defined.

A valuation $\mathbf{a}$ in a model $\mathcal{A}$ is a function from the set of variables of σ into the universe of $\mathcal{A}$. By $\mathbf{a}(x_i/b)$ we denote the valuation $\mathbf{a}'$ such that $\mathbf{a}'(x_j) = \mathbf{a}(x_j)$ for $j \neq i$ and $\mathbf{a}'(x_i) = b$.

We extend $\mathbf{a}$ to $\mathbf{a}$: $\mathrm{Trm}_\sigma \longrightarrow A$ denoted by the same symbol and defined by conditions:

- $\mathbf{a}(c_i) = a_i$, for all constants c_i from σ,
- $\mathbf{a}(f_i(t_1, \ldots, t_{\mathrm{ar}(f_i)}) = F_i(\mathbf{a}(t_1), \ldots, \mathbf{a}(t_{\mathrm{ar}(f_i)}))$, for all functions f_i from σ.

The satisfaction relation, $\models$, for a vocabulary σ is a relation between models, formulas and valuations. For a given $\mathcal{A} \in \mathrm{Mod}_\sigma$, $\varphi(x_{i_1}, \ldots, x_{i_k}) \in \mathcal{F}_\sigma$ and $\mathbf{a}$, a valuation in $\mathcal{A}$, $\mathcal{A} \models \varphi(x_{i_1}, \ldots, x_{i_k})[\mathbf{a}]$ is defined by induction on a construction of φ. The basic cases are:

- $\mathcal{A} \models (t = t')[\mathbf{a}]$ if $\bar{\mathbf{a}}(t) = \mathbf{a}(t')$,
- $\mathcal{A} \models P_i(t_1, \ldots, t_{\mathrm{ar}(P_i)})[\mathbf{a}]$ if $(\mathbf{a}(t_1), \ldots, \mathbf{a}(t_{\mathrm{ar}(P_i)})) \in R_i$.

For complex formulas we have:

- $\mathcal{A} \models \neg\varphi[\mathbf{a}]$ if $\mathcal{A} \not\models \varphi[\mathbf{a}]$,
- $\mathcal{A} \models (\varphi \Rightarrow \psi)[\mathbf{a}]$ if $\mathcal{A} \not\models \varphi[\mathbf{a}]$ or $\mathcal{A} \models \psi[\mathbf{a}]$.
- $\mathcal{A} \models \forall x(\varphi)[\mathbf{a}]$ if for all $b \in |A|$, $\mathcal{A} \models \varphi[\mathbf{a}(x/b)]$.

If $\mathcal{A} \models \varphi[\mathbf{a}]$ then we will say that φ holds in $\mathcal{A}$ under $\mathbf{a}$.

It can be proven by induction on a construction of a formula φ, that if two valuations $\mathbf{a}$ and $\mathbf{a}'$ agree on the free variables of φ then $\mathcal{A} \models \varphi[\mathbf{a}]$ if and only if $\mathcal{A} \models \varphi[\mathbf{a}']$. Thus, for $\varphi(x_{i_1}, \ldots, x_{i_k})$ it is meaningful to write $\mathcal{A} \models \varphi[a_1/x_{i_1}, \ldots, a_k/x_{x_{i_k}}]$, or just $\mathcal{A} \models \varphi[a_1, \ldots, a_k]$, for expressing that φ holds in $\mathcal{A}$ under any valuation which maps x_{i_j} to a_j for $j = 1, \ldots, k$. In this case we say that φ is satisfied in $\mathcal{A}$ by $a_1, \ldots, a_k$. When $\bar{a}$ and $\bar{z}$ are sequences of equal length of elements of $|\mathcal{A}|$ and variables respectively, we write also $\mathcal{A} \models \varphi[\bar{a}/\bar{z}]$ with the obvious meaning.

The set of all sentences true in $\mathcal{A}$ is the theory of the model $\mathcal{A}$ and is denoted by $\mathrm{Th}(\mathcal{A})$. By $\mathcal{A} \equiv \mathcal{B}$ we express that $\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$. Similarly, if $\mathcal{A}$ and $\mathcal{B}$ satisfy the same sentences in a relation-like form of a quantifier rank $\leq k$, we write $\mathcal{A} \equiv_k \mathcal{B}$.

Definition 2.1 *Let $\mathcal{A} = (A, \{R_i\}_{i \leq s}, \{F_i\}_{i \leq t}, \{a^{c_i}\}_{i \leq r})$ be a model, $\bar{x}$ and $\bar{y}$ sequences of pairwise distinct variables $x_1, \ldots, x_k$ and $y_1, \ldots, y_l$, respectively. Let $\varphi(\bar{x}, \bar{y})$ be a formula in the vocabulary of $\mathcal{A}$ such that $\mathrm{Free}(\varphi) \subseteq \{\bar{x}, \bar{y}\}$ and let $\bar{a} = a_1, \ldots, a_l$ be a sequence of elements from A. By $\varphi^{\mathcal{A}, \bar{a}, \bar{x}}$ we denote the set*

$$\varphi^{\mathcal{A}, \bar{a}, \bar{x}} = \{(b_1, \ldots, b_k) \in A^k : \mathcal{A} \models \varphi[b_1, \ldots, b_k, \bar{a}]\}.$$

$\varphi^{\mathcal{A},\bar{a},\bar{x}}$ is called the relation definable by $\varphi(\bar{x},\bar{y})$ in $\mathcal{A}$ with parameters $\bar{a}$, where we treat $\bar{a}$ as a finite valuation $\{(y_i,a_i) : i = 1,\dots,l\}$. When the sequence $\bar{x}$ is clear from the context or inessential for our considerations, and similarly the sequence $\bar{a}$, we write $\varphi^{\mathcal{A}}$.

Let us observe, that the relation 'definable by a formula φ' depends on variables $\bar{x}$. In particular some variables in $\bar{x}$ may not occur in φ.

Having defined semantics we describe what it means for two formulas to be equivalent. Formulas $\varphi(x_1,\dots,x_k)$ and $\psi(x_1,\dots,x_k)$ are equivalent if for each model $\mathcal{A}$ of the vocabulary containing all non logical symbols of both φ and ψ $\varphi^{\mathcal{A},\bar{x}} = \psi^{\mathcal{A},\bar{x}}$, where $\bar{x} = x_1,\dots,x_k$ is the sequence containing all free variables of φ and ψ.

Let $\mathcal{A} = (A, \{R_i^{\mathcal{A}}\}_{i\leq s}, \{F_i^{\mathcal{A}}\}_{i\leq t}, \{a^{c_i}\}_{i\leq r})$ and $\mathcal{B} = (B, \{R_i^{\mathcal{B}}\}_{i\leq s}, \{F_i^{\mathcal{B}}\}_{i\leq t}, \{b^{c_i}\}_{i\leq r})$ be models of the same vocabulary. An isomorphism between $\mathcal{A}$ and $\mathcal{B}$ is a bijection $f\colon |\mathcal{A}| \longrightarrow |\mathcal{B}|$ such that

- For each $i \leq s$ and for each $\bar{a} = a_1,\dots,a_{\mathrm{ar}(R_i^{\mathcal{A}})} \in |\mathcal{A}|$,
$$R_i^{\mathcal{A}}(\bar{a}) \iff R_i^{\mathcal{B}}(\vec{f}(\bar{a})).$$
- For each $i \leq t$ and for each $a \in |\mathcal{A}|$ and $\bar{a} = a_1,\dots,a_{\mathrm{ar}(F_i^{\mathcal{A}})}$,
$$F_i^{\mathcal{A}}(\bar{a}) = a \iff F_i^{\mathcal{B}}(\vec{f}(\bar{a})) = f(a).$$
- For each $i \leq r$, $f(a^{c_i}) = b^{c_i}$.

Let g be a partial injection between $|\mathcal{A}|$ and $|\mathcal{B}|$ and let $g' = g \cup \{(a^{c_i}, b^{c_i})\}_{i\leq r}$ fulfill the above three conditions restricted to the $\mathrm{dom}(g')$. Then we say that g is a partial isomorphism between $\mathcal{A}$ and $\mathcal{B}$.[1] If g is an isomorphism between $\mathcal{A}$ and the restriction of $\mathcal{B}$ to the $\mathrm{rg}(g)$ then g is an embedding of $\mathcal{A}$ into $\mathcal{B}$.

Let $\approx$ be an equivalence relation on X. We write $[a]_{/\approx}$ for an $\approx$–equivalence class of $a \in X$. When the equivalence relation is clear from the context we omit the subscript and write $[a]$. The set of all $\approx$–equivalence classes of elements in X is denoted by $X_{/\approx}$.

Let $\approx$ be an equivalence relation on an universe of a model $\mathcal{A} = (A, \{R_i\}_{i\leq s}, \{F_i\}_{i\leq t}, \{a^{c_i}\}_{i\leq r})$. We say that $\approx$ is a congruence relation on $\mathcal{A}$ if:

- for each $i \leq s$ and for each $\bar{a} = a_1,\dots,a_{arity(P_i)} \in |\mathcal{A}|$, $\bar{b} = b_1,\dots,b_{\mathrm{ar}(P_i)} \in |\mathcal{A}|$ such that $a_j \approx b_j$ for $j \leq \mathrm{ar}(P_i)$ we have:
$$(\bar{a}) \in R_i \text{ if and only if } (\bar{b}) \in R_i,$$

[1] Let us observe that in the second condition we have to require that the value of $F_i^{\mathcal{A}}(\bar{a})$ is in the domain of g'.

- for each $i \leq t$ and for each $\bar{a} = a_1, \ldots, a_{\mathrm{ar}(f_i)} \in |\mathcal{A}|$, $\bar{b} = b_1, \ldots, b_{\mathrm{ar}(f_i)} \in |\mathcal{A}|$,

$$\text{if } a_j \approx b_j \text{ for } j \leq \mathrm{ar}(f_i) \text{ then } F_i(\bar{a}) \approx F_i(\bar{b}).$$

Let us observe that equality is always a congruence relation for any model $\mathcal{A}$.

Definition 2.2 *Let $\mathcal{A} \in \mathrm{Mod}_\tau$ and let $\approx$ be a congruence relation on $\mathcal{A}$. Then we define the model*

$$\mathcal{A}_{/\approx} = (A_{/\approx}, \{R_{i/\approx}\}_{i \leq s}, \{F_{i/\approx}\}_{i \leq t}, \{[a^{c_i}]_{/\approx}\}_{i \leq r}),$$

where the universe of $\mathcal{A}_{/\approx}$ is the set of all $\approx$–equivalence classes,

$$R_{i/\approx} = \{([a_1]_{/\approx}, \ldots, [a_{\mathrm{ar}(R_i)}]_{/\approx}) : (a_1, \ldots, a_{\mathrm{ar}(R_i)}) \in R_i\},$$

and

$$f_{i/\approx}([a_1]_{/\approx}, \ldots, [a_{\mathrm{ar}(f_i)}]_{/\approx}) = [f_i(a_1, \ldots, a_{\mathrm{ar}(f_i)})]_{/\approx}.$$

The correctness of the above definition essentially depends on the second condition in the definition of the congruence relation.

2.1.1 Ehrenfeucht–Fraïsse games

In this section we describe one of the main tools in model theory, especially in finite model theory, namely, *Ehrenfeucht–Fraïsse games* or EF–games for short. Fraïsse defined this concept in an algebraic setting (see [13]), and later Ehrenfeucht presented a more intuitive and equivalent game–theoretic approach, see [10]. EF–games can be used for proving expressibility as well as non expressibility results for first order logic. For a detailed treatment of Ehrenfeucht–Fraïsse games we refer to [9].

An EF–game is played by two players which we call Ares and Eros[2] on two structures $\mathcal{A}_0, \mathcal{A}_1 \in \mathrm{Mod}_\tau$. Ares tries to show that $\mathcal{A}_0$ and $\mathcal{A}_1$ are different and Eros tries to show that they look alike. Each game has a predetermined number of rounds. In each round of the k-round game Ares chooses one structure, let it be $\mathcal{A}_0$, and an element $a \in |\mathcal{A}_0|$. Then, Eros chooses an element b from the other structure, that is $b \in |\mathcal{A}_1|$. The output of the round is the the ordered pair $\langle a, b\rangle \in |\mathcal{A}_0| \times |\mathcal{A}_1|$. After k rounds, we obtain the set

$$F = \{\langle a_1, b_1\rangle, \ldots, \langle a_k, b_k\rangle\} \subseteq |\mathcal{A}_0| \times |\mathcal{A}_1|.$$

[2]In the literature they are also called Abelard and Heloise, Adam and Eva, or Player I and Player II; or Player II and Player I.

We say that Eros wins the game if F is a partial isomorphism between $\mathcal{A}_0$ and $\mathcal{A}_1$.[3] Otherwise, Ares wins. Moreover, if Eros can win each k-round game on $\mathcal{A}_0$ and $\mathcal{A}_1$ then we say that he has a winning strategy in the k–round game and we express this fact by $\mathcal{A}_0 \sim_k \mathcal{A}_1$. The following theorem shows the relation between EF–games and first order logic.

Theorem 2.3 (Ehrenfeucht [10], Fraïsse [13]) *Let σ be a finite vocabulary and let $\mathcal{A}, \mathcal{B} \in \mathrm{Mod}_\sigma$. For each $r \in \omega$ the following are equivalent:*

1. $\mathcal{A} \sim_r \mathcal{B}$.
2. $\mathcal{A} \equiv_r \mathcal{B}$, *that is* $\mathcal{A}$ *and* $\mathcal{B}$ *satisfy exactly the same sentences in a relation–like form of quantifier depth* $\leq r$.

The next fact presents one of the most popular introductory examples of an application of Ehrenfeucht–Fraïsse games. We use it later in this section.

Fact 2.4 *Let $\leq_i$ be the standard ordering on natural numbers restricted to the set $\{0, \ldots, i\}$ and let $\mathcal{A} = (\{0, \ldots, m\}, \leq_m)$ and $\mathcal{B} = (\{0, \ldots, n\}, \leq_n)$. If $n, m \geq 2^r$, then $\mathcal{A} \equiv_r \mathcal{B}$.*

The proof of this fact is given usually by an explicit definition of a winning strategy for Eros and it can be found in many introductory textbooks, e.g. [9] or [17].

2.2 Interpretations, reductions and definability

In this section we introduce one of the basic tools used in our work, namely, interpretations. It was applied in the work of Tarski for proving decidability and undecidability of mathematical theories, see [30] or [50]. The method was codified by Szczerba in [48] and [49]. In his works a purely model–theoretic notion of interpretations was for the first time formulated in the general setting. Interpretations were later rediscovered by finite model theorists, see [7] or [27] for interpretative reductions and logical reductions, respectively. Let us stress an important difference between interpretations and reductions. An interpretation $\bar{\varphi}$ of one class of models $\mathcal{K}_1$ in antoher one $\mathcal{K}_2$ is a reduction of $\mathcal{K}_2$ to $\mathcal{K}_1$. In the finite model theory interpretations provide a natural and reasonably subtle method of reducing one class of finite models to another

[3] Let us remind that according to the definition of a partial isomorphism we have to consider F extended by a set of pairs of corresponding constants from two structures.

one. It turned out that many complete problems for various complexity classes such as LOGSPACE or NPTIME remain complete also under this form of reductions, see [20].

2.2.1 Interpretations

A first order interpretation of models for a vocabulary σ in models for a vocabulary τ is determined by a sequence of formulas of vocabulary τ in the following sense. Let $\sigma = (\{P_i\}_{i\leq s}, \{f_i\}_{i\leq t}, \{c_i\}_{i\leq r}, \mathrm{ar})$ and let

$$\bar{\varphi} = (\varphi_U, \varphi_\approx, \{\varphi_{P_i}\}_{i\leq s}, \{\varphi_{f_i}\}_{i\leq t}, \{\varphi_{c_i}\}_{i\leq r})$$

be the sequence of formulas from $\mathcal{F}_\tau$ such that $\mathrm{Free}(\varphi_U) \subseteq \{x_1, \ldots, x_n\}$, $\mathrm{Free}(\varphi_\approx) \subseteq \{x_1, \ldots, x_{2n}\}$, $\mathrm{Free}(\varphi_{R_i}) \subseteq \{x_1, \ldots, x_{n(\mathrm{ar}(R_i))}\}$, $\mathrm{Free}(\varphi_{f_i}) \subseteq \{x_1, \ldots, x_{n(\mathrm{ar}(f_i)+1)}\}$ and $\mathrm{Free}(\varphi_{c_i}) \subseteq \{x_1, \ldots, x_n\}$.[4]

Let $\mathcal{A} \in \mathrm{Mod}_\tau$. We write $\varphi_{P_i}^{\mathcal{A}}$ for a relation defined by φ_{P_i} in $\mathcal{A}$, with respect to variables $x_1, \ldots, x_{n(\mathrm{ar}(P_i))}$. A similar convention is applied for other formulas in $\bar{\varphi}$, e.g. $\varphi_U^{\mathcal{A}}$ is a subset of A^n.

At the first step, we construct a model $\mathcal{B}'$ in a relational vocabulary corresponding to σ,

$$\mathcal{B}' = (\varphi_U^{\mathcal{A}}, \{\varphi_{R_i}^{\mathcal{A}} \cap (\varphi_U^{\mathcal{A}})^{\mathrm{ar}(P_i)}\}_{i\leq s}, \{\varphi_{f_i}^{\mathcal{A}} \cap (\varphi_U^{\mathcal{A}})^{\mathrm{ar}(f_i)+1}\}_{i\leq t}, \{\varphi_{c_i}^{\mathcal{A}} \cap (\varphi_U^{\mathcal{A}})\}_{i\leq r}).$$

Now let us assume that the relation $\varphi_{\approx}^{\mathcal{A}}$ restricted to the universe of $\mathcal{B}'$ is a congruence relation in $\mathcal{B}'$. For brevity, we denote this relation by $\approx$. Then we define the model $\mathcal{B}$ as $\mathcal{B}'_{/\approx}$ with the modification that we treat $(\varphi_{c_i}^{\mathcal{A}} \cap \varphi_U^{\mathcal{A}})_{/\approx}$ not as one element sets but as elements of the universe. Thus, we have to require that $(\varphi_{c_i}^{\mathcal{A}} \cap \varphi_U^{\mathcal{A}})_{/\approx}$ is a singleton, for each $i \leq r$. Moreover, since we want $\mathcal{B}$ to be a model in a vocabulary σ, then $(\varphi_{f_i}^{\mathcal{A}} \cap \varphi_U^{\mathcal{A}})_{/\approx}$ should define a graph of a function, for each $i \leq t$.

More precisely,

$$\mathcal{B} = (B, \{R_i\}_{i\leq s}, \{F_i\}_{i\leq t}, \{d_i\}_{i\leq r}),$$

where

- $B = \varphi_{U/\approx}^{\mathcal{A}}$;
- for each $i \leq s$, $R_i = (\varphi_{R_i}^{\mathcal{A}} \cap (\varphi_U^{\mathcal{A}})^{\mathrm{ar}(P_i)})_{/\approx}$;

[4] We do not define here interpretations with parameters because we do not need them in our work.

- for each $i \leq t$, $F_i = (\varphi_{f_i}^{\mathcal{A}} \cap \varphi_U^{\mathcal{A}})^{\mathrm{ar}(f_i)+1})_{/\approx}$ is a graph of a function from $B^{\mathrm{ar}(f_i)}$ into B;

- for $i \leq r$, d_i is the unique $\approx$–equivalence class of elements in $\varphi_{c_i}^{\mathcal{A}} \cap \varphi_U^{\mathcal{A}}$.

We say that $\mathcal{B}$ constructed in this way is defined by $\bar{\varphi}$ in $\mathcal{A}$.

Since logic does not distinguish between isomorphic models, we say that $\mathcal{B}$ is defined by $\bar{\varphi}$ in $\mathcal{A}$ also when $\mathcal{B} \cong I_{\bar{\varphi}}(\mathcal{A})$.

Definition 2.5 (Interpretation) *Let τ, σ and $\bar{\varphi}$ be as above.* An interpretation $I_{\bar{\varphi}}$ of Mod_σ in Mod_τ *is a partial functor with the domain* $\mathrm{dom}(I_{\bar{\varphi}}) = \mathrm{Mod}_\tau$ *and the range* $\mathrm{rg}(I_{\bar{\varphi}}) \subseteq \mathrm{Mod}_\sigma$.

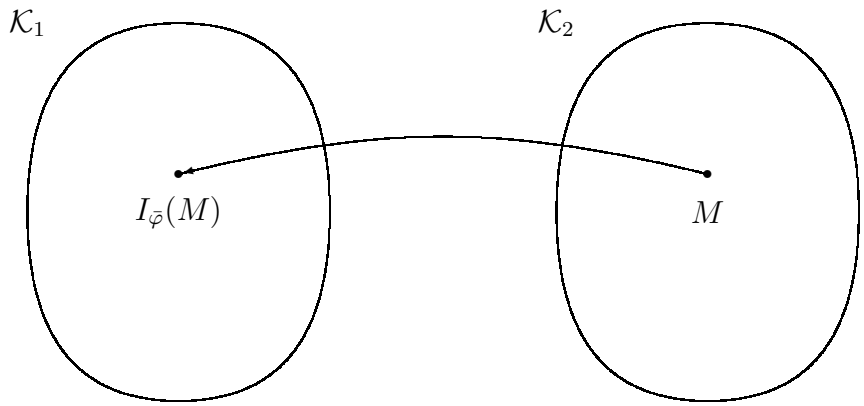
Then, $I_{\bar{\varphi}}(\mathcal{A})$ is the model defined by $\bar{\varphi}$ in $\mathcal{A}$.

The interpretation $I_{\bar{\varphi}}$ is determined by formulas in $\bar{\varphi}$; therefore we use the term interpretation also for $\bar{\varphi}$.

Let us observe that it may happen that $\bar{\varphi}$ does not define a model $I_{\bar{\varphi}}(\mathcal{A})$ in a given $\mathcal{A} \in \mathrm{Mod}_\tau$. Firstly, $\varphi_{\approx}^{\mathcal{A}}$ may not be a congruence relation in $\mathcal{B}'$. Secondly, the sets $\{F_i\}_{i \leq t}$ or $\{d_i\}_{i \leq r}$ may not be properly defined. Therefore, considering any property of models $\Psi(.)$, we interpret $\Psi(I_{\bar{\varphi}}(\mathcal{A}))$ as $\exists \mathcal{B}\, (\mathcal{B} = I_{\bar{\varphi}}(\mathcal{A}) \wedge \Psi(\mathcal{B}))$, where the assumption of existence of $I_{\bar{\varphi}}(\mathcal{A})$ is explicitly stated.

In the following picture we illustrate the interpretation $\bar{\varphi}$ of a family of models $\mathcal{K}_1$ in $\mathcal{K}_2$. The arrow indicates the direction in which the interpretation acts. It takes a model M from $\mathcal{K}_2$ and constructs a model from $\mathcal{K}_1$, $I_{\bar{\varphi}}(M)$. As we noted, the function given by the interpretation may be not total.

It is often convenient to consider an interpretation $\bar{\varphi}$ as acting from $\mathcal{K}_1$ into $\mathcal{K}_2$. Then for a given model $\mathcal{N}_1$ from $\mathcal{K}_1$ we look for a model $\mathcal{N}_2$ in $\mathcal{K}_2$ such that $\bar{\varphi}$ defines in $\mathcal{N}_2$ a model isomorphic to $\mathcal{N}_1$. In such a case, $\mathcal{N}_2$ may be not determined uniquely. However, in this thesis, we consider interpretations as acting from $\mathcal{K}_2$ into $\mathcal{K}_1$.



Picture 2.1 An interpretation $\bar{\varphi}$ of $\mathcal{K}_1$ in $\mathcal{K}_2$.

Now we define some variations of the original concept.

Definition 2.6 *Let σ, τ and $\bar{\varphi}$ be as above and assume that $\varphi_\approx$ is just the identity relation on n–tuples.*

An interpretation $\bar{\varphi}$ is simple if $n = 1$, otherwise it is n-cartesian. An interpretation is entire if φ_U is a tautology. If an interpretation is simple, entire and parameter free we say that it is exact.

Let $\mathcal{A} \in \mathrm{Mod}_\tau$ and $\mathcal{B} \in \mathrm{Mod}_\sigma$ and let $\bar{\varphi}$ define $\mathcal{B}$ in $\mathcal{A}$. If $\bar{\varphi}$ is simple we say that $\mathcal{B}$ is simply definable in $\mathcal{A}$. Similar convention applies for $\bar{\varphi}$ being a entire or exact interpretation.

2.2.2 Translation of formulas

Let $\bar{\varphi}$ be a sequence defining an n–cartesian interpretation of Mod_σ in Mod_τ and let $\mathcal{A} \in \mathrm{Mod}_\tau$.

We establish a correspondence between relations definable in models $I_{\bar{\varphi}}(\mathcal{A})$ and $\mathcal{A}$. Firstly, we define the translation function $\widehat{I}_{\bar{\varphi}} \colon \mathcal{F}_\sigma \longrightarrow \mathcal{F}_\tau$.

We introduce the following notation: for x_i by $\widetilde{x}_i$ we denote the sequence $x_{(i-1)n}, \ldots, x_{in}$. Similarly, for a constant c_i, $\widetilde{c_i}$ is $z_1^{c_i}, \ldots, z_n^{c_i}$, the sequence of new variables. If $\bar{z}$ is a sequence of variables and constants $z_1, \ldots, z_k$ and $Q \in \{\exists, \forall\}$, we write $Q\bar{z}$ for $Qz_1 \ldots Qz_k$.

We define an auxiliary operation * by induction on $\psi \in \mathcal{F}_\sigma$. We assume that ψ is in a relation–like form.

- If $\psi = \ulcorner x_l = x_j \urcorner$ then $\psi^\star = \ulcorner \varphi_\approx(\widetilde{x}_l, \widetilde{x}_j) \urcorner$.
- If $\psi = \ulcorner P_i(x_{j_1}, \ldots, x_{j_{\mathrm{ar}(P_i)}}) \urcorner$ then $\psi^\star = \ulcorner \varphi_{P_i}(\widetilde{x}_{j_1}, \ldots, \widetilde{x}_{j_{\mathrm{ar}(P_i)}}) \urcorner$.

- If $\psi = \ulcorner f_i(x_{j_1}, \ldots, x_{j_{\mathrm{ar}(f_i)}}) = x_l \urcorner$ then

$$\psi^\star = \ulcorner \exists \widetilde{x}_w(\varphi_{f_i}(\widetilde{x}_{j_1}, \ldots, \widetilde{x}_{j_{\mathrm{ar}(f_i)}}, \widetilde{x}_w) \wedge \varphi_\approx(\widetilde{x}_w, \widetilde{x}_l))\urcorner,$$

  where x_w is a new variable.

- If $\psi = \ulcorner(\gamma \Rightarrow \theta)\urcorner$ then $\psi^\star = \ulcorner(\gamma^\star \Rightarrow \theta^\star)\urcorner$.

- If $\psi = \ulcorner \neg\gamma \urcorner$ then $\psi^\star = \ulcorner \neg\gamma^\star \urcorner$.

- If $\psi = \ulcorner \forall x_j \gamma(x)\urcorner$ then $\psi^\star = \ulcorner \forall \widetilde{x}_j(\varphi_U(\widetilde{x}_j) \Rightarrow (\gamma(\widetilde{x}_j))^\star)\urcorner$.

In each point we make the following proviso:

> *If a variable x_i is free in ψ and some variables in $\widetilde{x}_i$ would be bounded in $\psi^\star$ by a quantifier in a formula φ from $\bar{\varphi}$ then we rename bounded variables in φ so that variables $\widetilde{x}_i$ remain free in $\psi^\star$.*

We obtain for a given $\psi(x_1, \ldots, x_k)$ a formula $\psi^\star(\widetilde{x}_1, \ldots, \widetilde{x}_k, \widetilde{c}_1, \ldots, \widetilde{c}_r)$, where $c_1, \ldots, c_r$ is the list of constants from σ. To finish the translation we need to quantify out these constants.

$$\widehat{I}_{\bar{\varphi}}(\psi) = \exists \widetilde{c}_1 \ldots \exists \widetilde{c}_r(\bigwedge_{1 \leq i \leq r}(\varphi_{c_i}(\widetilde{c}_i) \wedge \varphi_U(\widetilde{c}_i)) \wedge \psi^\star(\widetilde{x}_1, \ldots, \widetilde{x}_k, \widetilde{c}_1, \ldots, \widetilde{c}_r)).$$

The key property of the above translation is the following

Proposition 2.7 *Let $\bar{\varphi}$ be an interpretation of Mod_σ in Mod_τ, $\mathcal{A} \in \mathrm{Mod}_\tau$ and let $\psi(x_1, \ldots, x_k) \in \mathcal{F}_\sigma$. Then, for each $\mathbf{a}_1, \ldots, \mathbf{a}_k \in |I_{\bar{\varphi}}(\mathcal{A})|$,*

$$I_{\bar{\varphi}}(\mathcal{A}) \models \psi[\mathbf{a}_1, \ldots, \mathbf{a}_k] \iff \mathcal{A} \models \widehat{I}_{\bar{\varphi}}(\psi)[\mathbf{a'}_1, \ldots, \mathbf{a'}_k],$$

where $\mathbf{a'}_i$ is an arbitrary n–tuple from the equivalence class of $\mathbf{a}_i$.

The proof can be given by a straightforward induction on a construction of ψ (see e.g. [17]).

2.3 Some recursion theoretic notions

Now we describe briefly the recursion theoretic concepts used in this thesis. All the notions and facts stated in this section are fairly standard and can be find in many textbooks. We give the brief overview of them, without giving proofs, just to fix the notation.

We use in this section some concepts from subsection 3.2.1 concerning the Σ_n classes of arithmetical formulas and relations definable by such formulas.

2.3.1 Turing machines and computations

Let $A = \{a_1, \ldots, a_k\}$ be a finite alphabet. A word over the alphabet A is a finite sequence of elements from A. The unique empty word is denoted by λ and A^* will be the set of all words over A. By a language L we mean any subset of A^*.

A Turing machine H is a tuple $(Q, \Sigma, \Gamma, \delta, q_S, q_A)$, where Q is a finite set of states of H, q_S, q_A are the starting and accepting states, respectively, Σ and Γ are alphabets of the language of H and of the work tape, respectively and δ is a function (possibly partial) from $Q \setminus \{q_A\} \times \Gamma$ into $Q \times \Gamma \times \{L, S, R\}$.[5] We assume that the work tape of the machine is unbounded to the right and bounded to the left, $\Sigma \subseteq \Gamma$ and $\Gamma - \Sigma$ contains two special symbols: α which is written on the leftmost square of the tape, and β which is the blank symbol. We assume that H never tries to go to the left from α or to write on a square containing α.

The computation of H on a word $w \in \Sigma^*$ starts in the state q_S when w is written on the work tape next to α and the head of H reads the leftmost letter of w. The rest of the tape is filled with β's.

During the computation H makes moves according to the function δ, its present state and the symbol scanned on the working tape. If, for example, H is in the state q, reads the symbol c and $\delta(q, c) = (p, d, L)$ then H enters into the state p, writes d on the tape and moves its head one square to the left. If during the computation on the word w H is in a situation for which the transition function is not defined then we say that H halts of w. If H halts in the state q_A then we say that H accepts w. The set of all words from Σ^* accepted by H is called the language of H and is denoted by $L(H)$. Similarly, W_H is the set of all words on which H stops.

There are several possible variations in the definition of Turing machine. One can allow a two way unbounded working tape or several working tapes; also the function δ may take as values subsets of $Q \times \Gamma \times \{L, S, R\}$ etc. However, it turns out that all these modifications do not change the family of languages recognizable by Turing machines. Nevertheless, they play a significant role when we consider the amount of resources, such as space or time, which are used during a computation performed by a machine H.

We say that a set $X \subseteq \Sigma^*$ is decidable if there is a Turing machine H which halts on every input and which accepts exactly words from X. In such a case H is said to decide X. X is recursively enumerable (RE for short) if there is a Turing Machine which accepts exactly the words from X. There is

[5] The letters L, S, R code the move of the head of the machine with the mnemonic meaning: left, stop, right. Moreover, we assume that there is no further move when a Turing machine enters the accepting state.

a number of equivalent characterizations of RE sets. E.g. X is RE if and only if there is a Turing machine which halts exactly on the words from X. We can characterize decidable sets by the following property: X is decidable if and only if both X and $A^* \setminus X$ are RE.

Let $R \subseteq \omega^r$. We may code R as a language over a two letter alphabet $\{0,1\}$. Let $\mathrm{bin}(u)$ be the word being the binary representation of an integer u (without leading 0's) and let, for a word $v = v_1, \ldots, v_k$ with $v_i \in \{0,1\}$, $\mathrm{d}(v) := v_1 v_1 v_2 v_2 \ldots v_k v_k$. By $L(R)$ we mean the language

$$\{\mathrm{d}(\mathrm{bin}(u_1))010\mathrm{d}(\mathrm{bin}(u_2))010 \ldots 010\mathrm{d}(\mathrm{bin}(u_r)) : (u_1, \ldots, u_r) \in R\}.$$

Then by definition, $R \subseteq \omega^r$ is RE if $L(R)$ is RE and, similarly, R is decidable if $L(R)$ is decidable. In what follows when we talk about some computational properties of relations over natural numbers we always assume that these relations are given by some coding function. In particular, if we write that H accepts a tuple $(a_1, \ldots, a_k) \in \omega^k$, we mean that H accepts the code of this tuple in some fixed coding. The coding given above is suitable for all our purposes.

The coding of relations on ω we have just introduced allows us to connect the notions of decidability and recursive enumerability with the notion of arithmetical hierarchy, see subsection 3.2.1. Namely, $R \subseteq \omega^r$ is RE if and only if R is definable in $\mathcal{N}$ by a Σ_1 formula of arithmetic. Similarly, R is decidable if and only if R is definable in $\mathcal{N}$ by Σ_1 and Π_1 formulas.

2.3.2 Many–one reducibilities, complete sets

So far we considered machines which answer only yes or no on a given input. Now we modify our notion of computability to include machines which compute functions. Let f be a function, possibly partial, from ω^k into ω^m. We say that a Turing machine H computes f if for each $\mathbf{a} \in \omega^k$,

- H halts for the input $\mathbf{a}$ if and only if $\mathbf{a} \in \mathrm{dom}(f)$.
- If $\mathbf{a} \in \mathrm{dom}(f)$ then the word written on the work tape after the last step of the computation of H with the input $\mathbf{a}$ is the code of $f(\mathbf{a})$.

A function f is recursive if there is a Turing machine which computes f.

Now we can describe our first notion of relative computability. Let $R \subseteq \omega^k$, $S \subseteq \omega^r$. We say that R is many-one reducible to S, $R \leq_m S$, if there is a total recursive function f such that for each $\mathbf{a} \in \omega^k$, $\mathbf{a} \in R$ if and only if $f(\mathbf{a}) \in S$. The relation $\leq_m$ is reflexive and transitive. It follows that the relation defined as $R \leq_m S \wedge S \leq_m R$ is an equivalence relation. It

is denoted by $R \equiv_m S$. Let us observe that the empty set and ω form two distinct equivalence classes under $\equiv_m$.

Let $\mathcal{K} \subseteq \mathcal{P}(\omega)$ and $R \subseteq \omega$. We say that R is $\mathcal{K}$–complete via many-one reductions if $R \in \mathcal{K}$ and for each $S \in \mathcal{K}$, $S \leq_m R$. For each n, the families Σ_n and Π_n contain complete sets. Moreover, these sets can be described in a natural way as sets of indexes of Turing machines having some property, e.g. the set of Turing machines which compute functions with finite domain is Σ_2–complete.

Now we introduce sets complete for some classes of relations which will be usefull for us later.

Each Turing machine can be described by a finite word in a fixed alphabet, e.g. $\{0, 1\}$. Since we can identify such words with natural numbers, see section 3.2.2, it follows that we can identify a given Turing machine H with a natural number c_H which is called a code of a machine H. Subsequently, we write H to denote both: a Turing machine and its code. Indeed, for purposes of this thesis we can think of Turing machines just as they were natural numbers.

Definition 2.8 *By* Fin $\subseteq \omega$ *we denote the set of Turing machines which have finite domains i.e.*

$$\text{Fin} = \{H : W_H \text{ is finite}\}.$$

By CoInf $\subseteq \omega$ *we denote the set of all Turing machines H which have an infinite number of $n \in \omega$ such that H on the input n does not halt i.e.*

$$\text{CoInf} = \{H : (\omega \setminus W_H) \text{ is infinite}\}.$$

It is well known that the following holds, see e.g. [47].

Proposition 2.9 *1.* Fin *is a Σ_2–complete set in the arithmetical hierarchy.*

2. CoInf *is Π_3–complete.*

2.3.3 Turing degrees

Now we describe the concept of computations with an oracle.

An oracle Turing machine $H^?$ is a Turing machine which has one additional tape called oracle tape and three additional states $q_?$, q_{YES} and q_{NO}. A set $A \subseteq \Sigma^*$ is called an oracle and we write H^A for the machine $H^?$ with the oracle A. During the computation with the oracle A the machine can write

or read from the oracle tape. The only modification of the computation is when the machine enters in the state $q_?$. Let $w \in \Sigma^*$ be the word written at that time on the oracle tape. In the next step the content of the oracle tape is erased and if $w \in A$ then H^A enters in the state q_{YES}; if $w \notin A$ then H^A enters in the state q_{NO}. We say that the oracle answered positively or negatively. The notion of an accepting computation of H^A is the same as for an ordinary Turing machine.

Later we will need the following characterization of sets in arithmetical hierarchy by Turing machines with oracles.

Proposition 2.10 *Let $A \subseteq \omega^r$. The following conditions are equivalent:*

(i) A is Δ_2 in the arithmetical hierarchy,

(ii) A is decided by an oracle Turing machine H^X, where the oracle set X is recursively enumerable.

Chapter 3

Arithmetics, classical and finite models approaches

In the following sections we present some of the classical arithmetical domains determined by some sets of primitive notions, such as addition and multiplication, BIT relation or concatenation. Then we construct finite model domains of these arithmetics and we discuss some of their properties. Finally, as the main contribution of this chapter, we prove that in finite models concatenation is semantically equivalent to the arithmetic with addition and multiplication.

Here and later we use the word 'domain' to denote a model over some universe with a fixed set of relations, functions and constants. We assume that each element of such model has its name and, therefore, is distinguishable from any other. Moreover, each relation, function and constant in the domain has its own name. Therefore, we do not distinguish between the relation or function in the domain and the symbol in the language which is interpreted by it. E.g. $+$, $\times$ are both symbols from the language and the operations in the domain.

Since we have names for all elements in the domain we will subsequently give a stronger notion of interpretation, see definition 3.17. It requires that for two domains over the same universe, $\mathcal{A}$ and $\mathcal{B}$, the interpretation $\bar{\varphi}$ of $\mathcal{A}$ into $\mathcal{B}$ preserves also the elements from the first domain. In other words, the identity is the isomorphism between $\mathcal{A}$ and $I_{\bar{\varphi}}(\mathcal{B})$. Such an interpretation shows that everything we can express *about elements* of the domain in $\mathcal{A}$, we can also express in $\mathcal{B}$ while the previous notions preserve only structural properties of models.

In the present chapter for each model $\mathcal{A}$ of the form $(\omega, \mathcal{R})$ we define a family of finite models $\mathrm{FM}(\mathcal{A})$. We call this family a finite model domain (FM–domain). E.g. if $\mathcal{A}$ is a domain of addition, $(\omega, +)$, then $\mathrm{FM}(\mathcal{A})$ is

the FM–domain of addition – the family of all models determined by proper initial segments of natural numbers, see [33] where this terminology was introduced.

3.1 Arithmetics as determined by sets of primitive notions

In this section we briefly review what is known about properties of arithmetics with various sets of primitive notions. We assume in this section that the universe is the set of natural numbers, ω.

Considering various domains with the same universe we classify them according to their definability strength. Being more precise we ask for what $\mathcal{A}$ and $\mathcal{B}$, the notions from $\mathcal{B}$ are definable in $\mathcal{A}$. In particular, for what $\mathcal{A}$ one can define addition and multiplication in $\mathcal{A}$. The problem was extensively studied in the context of the infinite models for arithmetics. For a nice survey of these results we refer to [24]. Here, we present only the basic facts about definability of addition and multiplication in some, seemingly weaker, domains.

Definition 3.1 *Let $X \subseteq \omega$. $\leq_X$ is the ordering relation restricted to X. Consequently, $\leq_P$ and $\leq_\Pi$ are ordering relations restricted to the sets of primes and the powers of primes, respectively.* Neib *is a binary relation which holds between x and y if $|x - y| = 1$. $|$ is the divisibility relation and $\perp$ is the coprimality relation.*

We have the following.

Theorem 3.2 *In each of the following models one can define addition and multiplication:* $(\omega, \times, \leq_\Pi)$ *([4])*, $(\omega, \times, \text{Neib})$ *([23])*, $(\omega, |, S)$ *([41])*, $(\omega, +, \perp)$ *([53])*. (*The references give credits for the corresponding results.*)

It should be mentioned that both $(\omega, +)$ and $(\omega, \times)$ have decidable theories. The results are attributed to Presburger, [39], and Skolem, [44], respectively.[1] It follows that neither $(\omega, +)$ nor $(\omega, \times)$ can define the full arithmetic which has an undecidable theory.

In spite of the fact that we know a lot about various arithmetical relations defined on ω many questions remain open. One of the main open problems is whether the theory of $(\omega, \leq, P)$ is decidable. It is commonly conjectured

[1] It should be said that Skolem in his paper did not present a valid proof of decidability of the artihmetic with multiplication. The first proof appeared in a paper by Mostowski,[29]

that $\mathrm{Th}((\omega, \leq, P))$ is undecidable since the constructive proof of decidability would provide a method for resolving some questions about prime numbers like the twin prime conjecture which is expressible in $(\omega, \leq, P)$ by a sentence

$$\forall x \exists y_1 \exists y_2 \{P(y_1) \wedge P(y_2) \wedge x \leq y_1 \wedge y_1 \leq y_2 \wedge y_1 \neq y_2 \wedge$$

$$\forall z_1 \forall z_2 (\bigwedge_{1 \leq i \leq 2} (y_1 \leq z_i \leq y_2 \wedge z_i \neq y_1 \wedge z_i \neq y_2) \Rightarrow z_1 = z_2)\}.$$

In what follows we consider the questions concerning the finite model versions of the above problems. In particular, we examine what are the changes in dependencies between arithmetics when we step from infinite to finite models.

3.2 Three classical arithmetical domains

In the present section we discuss models with universes consisting of natural numbers, words over finite alphabet and hereditarily finite sets. Traditionally, arithmetic was considered as a structure with the universe consisting of natural numbers augmented with some basic arithmetical notions such as linear ordering, addition, multiplication, exponentiation or, in general, primitively recursive functions and relations. Since the work of Gödel ([14]) we know that in the presence of first order logic multiplication and addition are sufficient to define all of the above notions. Moreover, the arithmetics of concatenation and of hereditarily finite sets are semantically equivalent to the arithmetic of addition and multiplication which means that in each one of these arithmetic we can interpret any other.

Classically, the interpretations were given for infinite domains. Since we concentrate on finite models in what follows we recall or prove the finite model versions of these interpretations. These results show that being in a finite model with relations from one domain we can freely use the notions of any other domain because they are definable in this model. For example, if we consider a finite model of cardinality n for arithmetic of addition and multiplication we can treat the elements of this model as words over finite alphabet and we can define the concatenation operation on them. It should be mentioned that in most cases it is not possible to use interpretations which work in the infinite case. The main difference is that when we define in finite models a relation R on given elements $a_1, \ldots, a_k$ we cannot assume that we have an access to elements which are greater than $a_1, \ldots, a_k$. On the contrary, in an infinite model we can freely use elements which are greater than $a_1, \ldots, a_k$.

In what follows we give definitions of respective domains. Then we present in a uniform way their FM–versions.

Firstly, we consider the classical arithmetic of addition and multiplication.

Definition 3.3 *$\mathcal{N}$ is the model $(\omega, +, \times, S, \leq, 0, 1)$, where S, $+$ and $\times$ are the successor, addition and multiplication functions, respectively, $\leq$ is the ordering of natural numbers and 0 and 1 are its least element and the second elements, respectively.*

Let us observe that some of the operations and relations in the above model are easily definable from the others. So the successor function is definable from the ordering and ordering is definable from addition. Moreover, the constant 0 can be defined as the only element x such that for all z, $S(z) \neq x$ and 1 as $S(0)$. Therefore, addition allows us to define all the other notions of the model beside multiplication. If we were interested in taking a smaller set of operations we could take e.g. only exponentiation function, $\exp(x, y) = x^y$. Then one can easily define 0 and 1 using exp and then define multiplication as

$$xy = z \iff \exists w\, (w \neq 0 \wedge w \neq 1 \wedge \exp(\exp(w, x), y) = \exp(w, z)).$$

Similarly, having defined multiplication we can express addition as

$$x + y = z \iff \exists w\, (w \neq 0 \wedge w \neq 1 \wedge \exp(w, x) \exp(w, y) = \exp(w, z)).$$

In chapter 6 we show that the above is no longer possible in finite models, see corollary 6.28.

3.2.1 Δ_0 definability

Before discussing the other theories we will take a closer look at the definability in $\mathcal{N}$. Firstly, we define the arithmetical hierarchy of arithmetical formulas.

An occurrence of a quantifier $Q \in \{\exists, \forall\}$ is bounded in φ if it is of the form $Qx \leq t$, where t is a term and x does not occur in t. Bounded quantifier $\exists x \leq t\, \psi$ can be read as a shorthand for $\exists x(x \leq t \wedge \psi)$ and $\forall x \leq t\, \psi$ as $\forall x(x \leq t \Rightarrow \psi)$.

The basic level of arithmetical hierarchy is the family of Δ_0 formulas. It is the smallest set of formulas in the vocabulary $(+, \times, S, \leq, 0)$ such that it contains all quantifier free formulas and is closed on propositional connectives and bounded quantification. We denote this set also by Σ_0 and Π_0. Then we define the set Σ_{n+1} as the closure of Π_n under existential quantification and

Π_{n+1} as the closure of Σ_n under universal quantification. E.g. if φ is in Π_n, then the formula $\exists z_1 \ldots \exists z_k \, \varphi$ is in Σ_{n+1}. Thus, a formula is in Σ_n if it is of the form $\exists \bar{z}_1 \forall \bar{z}_2 \ldots Q \bar{z}_n \psi$, where Q is $\exists$ for odd n and $\forall$ otherwise and ψ is in Δ_0.

In some cases it is convenient to define the class Σ_n as the class of formulas of the form $\exists z_1 \forall z_2 \ldots Q z_n \psi$ with Q and ψ as above. Since in the infinite model we have a pairing function definable by a Δ_0 formula, these two notions are semantically equivalent in the infinite model. However, in a finite model we have no pairing function and we cannot reduce a homogeneous block of quantifiers to a single one.

A relation $R \subseteq \omega^r$ is Δ_0 (resp. Σ_n, Π_n) definable if there is a formula $\varphi(x_1, \ldots, x_r)$ in Δ_0 (resp. Σ_n, Π_n) such that $R = \varphi^{\mathcal{N}, \bar{x}}$ where $\bar{x}$ is $x_1, \ldots, x_r$. Thus, we can consider the arithmetical hierarchy as the hierarchy of relations definable by arithmetical formulas. According to the common convention we say that R is Σ_n when R is definable in $\mathcal{N}$ by a Σ_n formula.

Now our main interest is in Δ_0 definability. This is the most tractable class of relations in the arithmetical hierarchy. All relations in Δ_0 are decidable, unlike the relations in Σ_n for $n \geq 1$. In fact Δ_0 is exactly the class of relations in linear time hierarchy, see [15] for the precise definition.

The recognition of importance of Δ_0 definablity was initiated by Smullyan in [46]. There, the first systematic study of this and similarly defined classes was pursued. Moreover, besides the fact that Δ_0 relations are in linear time hierarchy (and, therefore, are decidable), they also have good properties with respect to axiomatization problems and definabilty. Namely, if we can define a relation $R \subseteq \omega^k$ in $\mathcal{N}$ by a Δ_0–formula, then this formula defines correctly R on the ω–initial segment in each model for Peano arithmetic. For us the importance of Δ_0 definability in $\mathcal{N}$ is based mainly on theorem 3.21.

Now we introduce some important arithmetical functions and relations. By $\exp(x, y)$ we denote the exponentiation function x^y. By $\mathrm{EXP}(x, y, z)$ we denote the graph of exp, i.e.

$$\mathrm{EXP}(x, y, z) \text{ if and only if } \exp(x, y) = z$$

By $\mathrm{BIT}(x, y)$ we denote the relation which holds if y has 1 on the x-th place in its binary representation. In other words, if $y = \Sigma_{i=0}^{i=n} a_i 2^i$ with $a_i \in \{0, 1\}$ then

$$\mathrm{BIT}(k, \Sigma_{i=0}^{i=n} a_i 2^i) \text{ if and only if } k \leq n \text{ and } a_k = 1.$$

$\mathrm{BITSUM}(x, y)$ is the relation expressing that y is equal to the number of ones in the binary representation of x that is

$$\mathrm{BITSUM}(\Sigma_{i=0}^{i=n} a_i 2^i, y) \text{ if and only if } y = \Sigma_{i=0}^{i=n} a_i.$$

We have the following lemma.

Lemma 3.4 *The following relations are Δ_0 definable in $\mathcal{N}$*

- $\mathrm{EXP}(x, y, z)$,
- $\mathrm{BIT}(x, y)$,
- $\mathrm{BITSUM}(x, y)$.

First part of the lemma was proven by Bennett in [3]. Having Δ_0 definition of $\mathrm{EXP}(x, y, z)$ it is easy to write a suitable formula for $\mathrm{BIT}(x, y)$ as

$$\exists z \leq x(\mathrm{EXP}(2, y, z) \wedge (x \text{ div } z \equiv 1(\text{mod } 2))),$$

where div is integer division defined by

$$x \text{ div } y = z \iff \exists u(\ 0 \leq u < z \wedge x = (yz) + u)$$

and $x \equiv y(\text{mod } z)$ is defined by

$$\exists u \exists u_1 \exists u_2 (0 \leq u < z \wedge x = u_1 z + u \wedge y = u_2 z + u).$$

The third part was of the lemma proven by Barrington, Immerman and Straubing in [1] in the finite models setting. A good presentation of the proof can be found in [15].

Later, in section 3.3, we present a general relation between Δ_0 definability and definability in finite models for arithmetic.

3.2.2 Arithmetics of hereditarily finite sets and of words

Now we present the other theories of arithmetics: the theory of hereditarily finite sets and the theory of words with concatenation.

Definition 3.5 *Let $V_0 = \emptyset$ and $V_{n+1} = \mathcal{P}(V_n)$, the power set of V_n. By V_ω we denote $\bigcup_{i \in \omega} V_i$. By HF we denote the structure $(V_\omega, \in)$.*

HF has as the universe all hereditarily finite sets and $\in$ as the only built-in relation. Whenever we need we use also the set theoretic operations such as sum ($\cup$), intersection ($\cap$) or set theoretical difference of y and x ($y \setminus x$).

Definition 3.6 *Let $\Gamma_t = \{a_1, \ldots, a_t\}$ be an alphabet.* A word *over Γ_t is a finite sequence of elements from Γ_t. We write λ for the empty word. By Γ_t^* we mean the set of all words over Γ_t, i.e.*

$$\Gamma_t^* = \{x_k \ldots x_0 : k \in \omega \wedge \forall i \leq k \, x_i \in \Gamma_t\} \cup \{\lambda\}.$$

FW^t *is the structure*

$$(\Gamma_t^*, *_t, \mathbf{a}_1, \ldots, \mathbf{a}_t)$$

where $*_t$ is the concatenation operation on words from Γ_t^* and $\mathbf{a}_i$ is the word consisting of one character a_i. In what follows we do not differentiate between a_i and $\mathbf{a}_i$.

The index t in FW^t and $*_t$ is omitted when the cardinality of the alphabet is not important or it is clear from the context. Let us also observe that FW^t is uniquely determined, up to isomorphism, by t.

Now we define ω-type orderings on V_ω and Γ_t^*. Firstly, we consider V_ω. We define the bijection f_ω from the set of natural numbers to V_ω. The ordering is expressed in terms of this bijection.

Let $\{k_i\}_{i\in\omega}$ be the sequence of natural numbers such that $k_0 = 0$ and $k_{i+1} = 2^{k_i}$. By induction on $n \in \omega$, we define the family of bijections $f_n \colon \{0, \ldots, k_n - 1\} \longrightarrow V_n$.

Firstly, we give an intuitive description of $\{f_n\}_{n\in\omega}$. f_0 is just the empty function and $f_1(0) = \emptyset$. Then, having defined $f_n \colon \{0, \ldots, k_n - 1\} \longrightarrow V_n$, we identify an element $x \in V_{n+1}$ with an $\{0, 1\}$ word $u_x = u_{k_n-1} \ldots u_0$ describing which elements of V_n belong to a. Namely, $u_i = 1$ if and only if the i-th element of V_n, $f_n(i)$, belongs to x. Such u_x can be interpreted as a binary representation of a number $k = \Sigma_{i=0}^{k_n-1} u_i 2^i$ and we put $f_{n+1}(k) = x$.

Now we give a precise definition of f_ω and $\{f_i\}_{i\in\omega}$. We have:

- $f_i \colon \{0, \ldots, k_i - 1\} \longrightarrow V_i$,
- $f_i \subseteq f_{i+1}$,
- $f_\omega = \bigcup_{i\in\omega} f_i$.

$f_0 \colon \emptyset \longrightarrow \emptyset$ can only be the empty set. Now let us assume that f_i is defined. We take f_{i+1} as

$$f_{i+1}(x) = \{f_i(y) \in V_i : \mathrm{BIT}(y, x)\}.$$

Let us observe that f_{i+1} is an extension of f_i.

Directly from the definition of the families V_i and f_i it follows that $f_\omega = \bigcup_{i\in\omega} f_i$ is a properly defined bijection.

The bijection f_ω allows us to define the ordering on V_ω. Namely, for $x, y \in V_\omega$,

$$x \leq y \iff f_\omega^{-1}(x) \leq f_\omega^{-1}(y).$$

The function f_ω establishes also the relation between HF and the predicate BIT. Therefore, we have proved the following proposition which is a part of the folklore. Other proofs of it can be found e.g. in Fitting, [12].

Proposition 3.7 *The structure* (ω, BIT) *is isomorphic to* HF *and* f_ω *as defined above is the unique isomorphism function.*

In the case of Γ_t^* we define the ordering relation directly without an additional definition of a bijection between ω and Γ_t^*. Let $w = a_{i_k} \dots a_{i_0}$ and $u = a_{j_n} \dots a_{j_0}$ be words in Γ_t^*. By $\mathrm{lh}(x)$ we denote the length of a word x, e.g. $\mathrm{lh}(w) = k+1$. For $0 \leq r < \mathrm{lh}(w)$, $w(r)$ is the r-th letter of w, a_{i_r}. Then the lexicographic ordering on words, $\leq_l$, is defined as

$$\begin{aligned} w \leq_l u \iff\ & w = u \vee \exists r\{r < \mathrm{lh}(w) \wedge r < \mathrm{lh}(u) \wedge \\ & \forall t < r(w(t) = u(t) \wedge (\textstyle\bigvee_{1 \leq l < m \leq t}(w(r) = a_l \wedge u(r) = a_m)))\} \vee \\ & \{\mathrm{lh}(w) < \mathrm{lh}(u) \wedge \forall r < \mathrm{lh}(w)(w(r) = u(r))\}. \end{aligned}$$

For $w, u \in \Gamma_t^*$ we define

$$w \leq u \iff (\mathrm{lh}(w) < \mathrm{lh}(u)) \vee (\mathrm{lh}(w) = \mathrm{lh}(u) \wedge w \leq_l u).$$

Let us observe that the ordering given above allows us to define the concatenation as an operation on natural numbers. If u, w, v are respectively the n_u-th, n_w-th and n_v-th elements of this ordering then

$$u *_t w = v \iff n_u t^{\lceil \log_t(n_w+1) \rceil} + n_w = n_v.$$

where $\lceil \log_t(n_w + 1) \rceil$ is the length of a word w. Thus, we write $*_t$ also for the operation on natural numbers corresponding to concatenation on words.

The above considerations can be subsumed as

Proposition 3.8 *The structure* $(\omega, *_t, 1, \dots, t)$*, where* $x *_t y = xt^{\lceil \log_t(y+1) \rceil} + y$*, is isomorphic to* FW^t*.*

It follows that we can treat the structures HF and FW^t as arithmetical structures. Therefore, from now on we treat HF as (ω, BIT) and FW^t as the model $(\omega, *_t, 1, 2, \dots, t)$.

There are classical results concerning the mutual interpretability of $\mathcal{N}$, HF and FW.

Theorem 3.9 *Each of the the following models is definable in any other by an exact interpretation*

(*i*) $\mathcal{N}$,

(*ii*) HF,

(*iii*) FW^t, *for any* $t \geq 2$.

The mutual interpretability of (*i*) and (*ii*) is a part of the mathematical folklore. A detailed proof of this fact can be found in [12]. The mutual interpretability of (*i*) and (*iii*) was shown in [40]. Let us observe that lemma 3.4 gives us an Δ_0 interpretation of HF in $\mathcal{N}$.

3.3 Finite arithmetics

Our aim in this section is to define, for a given countable model $\mathcal{A}$ with ω as its universe, a family of finite models, $FM(\mathcal{A})$, which are finite approximations of $\mathcal{A}$. We follow the approach presented by Krynicki and Zdanowski in [25].

Definition 3.10 *Let* $\mathcal{A} = (\omega, \{R_i\}_{i\leq s}, \{F_i\}_{i\leq t}, \{a_i\}_{i\leq r})$ *and let* $A_n = \{0, \ldots, n\}$. *By* $FM(\mathcal{A})$ *we define the family* $\{\mathcal{A}_i\}_{i\in\omega}$ *of the finite models of the form*

$$\mathcal{A}_n = (A_n, \{R_i^n\}_{i\leq s}, \{F_i^n\}_{i\leq t}, \{b_i\}_{i\leq r}, n),$$

where

- R_i^n *is the restriction of* R_i *to the set* A_n
- F_i^n *is defined as*

$$F_i^n(\bar{a}) = \begin{cases} F_i(\bar{a}) & \text{if } F(\bar{a}) \leq n \\ n & \text{if } F_i(\bar{a}) > n \end{cases}$$

- $b_i^n = a_i$ *if* $a_i \leq n$, *otherwise* $b_i^n = n$.

We extend the vocabulary by a constant MAX *for denoting* n *– the maximal element of a model* $\mathcal{A}_n$.

According to the above definition the n-th finite models from families $FM(\mathsf{HF})$ and $FM(\mathsf{FW}^t)$ are referred to as HF_n and FW_n^t.

Let us mention that the family FM($\mathcal{N}$) admits a finite axiomatization within a class of finite models.

Proposition 3.11 (M. Mostowski, [32]) *There exists a finite set of sentences F in the language of $(+, \times, S, \leq, 0, 1, \mathrm{MAX})$ such that for each finite model $\mathcal{A}$,*

$$\mathcal{A} \models F \quad \text{if and only if } \exists \mathcal{B} \in \mathrm{FM}(\mathcal{N})\ \mathcal{A} \cong \mathcal{B}.$$

The axioms given in [32] are the following:[2]

1. $\forall x(S(x) \neq 0 \vee \mathrm{MAX} = 0)$,
2. $S(0) = 1$,
3. $\forall x \forall y((S(x) = S(y) \wedge x \neq \mathrm{MAX} \wedge y \neq \mathrm{MAX}) \Rightarrow x = y)$,
4. $S(\mathrm{MAX}) = \mathrm{MAX}$,
5. $\forall x(x \leq x)$,
6. $\forall x \forall y((x \leq y \wedge x \neq y) \Rightarrow \neg(y \leq x))$,
7. $\forall x \forall y(x \leq S(y) \equiv (x = S(y) \vee x \leq y))$,
8. $\forall x(x + 0 = x)$,
9. $\forall x \forall y(x + S(y) = S(x + y))$,
10. $\forall x(x0 = 0)$,
11. $\forall x \forall y(xS(y) = (xy) + x)$.

Let us comment on possible ways of defining the family $\mathrm{FM}(\mathcal{A})$. The ambiguity follows from the way we deal with functions from $\mathcal{A}$. Namely, we have to make an arbitrary decision how to define $F^n(a)$, for $a \in \mathcal{A}_n$, when $F(a) > n$. We have assumed that $F^n(a) = n$. However, it is quite popular in the literature of the topic to treat functions of $\mathcal{A}$ as relations. Then in the n–th model the relation corresponding to F is the set $\{\langle a, b\rangle \in |\mathcal{A}_n|^2 : F(a) = b\}$. Consequently, we should think of constants from $\mathcal{A}$ as one element sets which are empty in $\mathcal{A}_n$ unless a given constant from $\mathcal{A}$ belongs to $|\mathcal{A}_n|$. Let us denote the family of finite models defined accordingly to the above modifications as $\mathrm{FM}^*(\mathcal{A})$ and let $\mathcal{A}^*_n$ be the n-th model from this family.

Now we compare these two approaches. Let us observe that within the family $\mathrm{FM}^*(\mathcal{A})$ we can express everything that we can say within $\mathrm{FM}(\mathcal{A})$.

[2]There are some minor changes due to the fact that we are dealing with $\leq$ relation while in [32] the strict ordering is used. According to a common convention we skip the symbol $\times$ in expresions of the form $\ulcorner t \times s \urcorner$.

Fact 3.12 *For each model $\mathcal{A}$ there is an exact interpretation of* $\mathrm{FM}(\mathcal{A})$ *in* $\mathrm{FM}^*(\mathcal{A})$.

Proof. It suffices only to describe for f being a function symbol a formula φ_f which, for each n, defines in $\mathcal{A}_n^*$ the graph of the function F^n from the model $\mathcal{A}_n$.

For simplicity let us assume that f is a one place function symbol and let P_f be the corresponding binary relation symbol in the vocabulary of $\mathrm{FM}^*(\mathcal{A})$. The formula $\varphi_f(x, y)$ can be taken as

$$P_f(x, y) \vee (\forall z \neg P_f(x, z) \wedge y = \mathrm{MAX}).$$

If $\mathcal{A}_n^* \models P_f(a, b)$ then $F(a) = b$ and the same fact holds in $\mathcal{A}_n$. On the other hand if $\mathcal{A}^* \not\models P_f[a, b]$, for all $b \in |\mathcal{A}_n^*|$, then $F(a) > n$ and, therefore, $\mathcal{A}_n \models f(a) = n$. Thus, the formula above defines in $\mathcal{A}_n^*$ the graph of F^n from $\mathcal{A}_n$. $\square$

In both families $\mathrm{FM}(\mathcal{A})$ and $\mathrm{FM}^*(\mathcal{A})$ we extend the language by the constant MAX. However, it is easy to see that if we could not define the maximal element of models in $\mathrm{FM}^*(\mathcal{A})$ then we could not, in general, give in $\mathrm{FM}^*(\mathcal{A})$ an exact interpretation of a family $\mathrm{FM}(\mathcal{A})$. To see this, let us consider the model $\mathcal{A} = (\omega, F)$, where

$$F(i) = \begin{cases} i + 2 & \text{if } i \text{ is even,} \\ i & \text{if } i \text{ is odd.} \end{cases}$$

The maximal element in models from $\mathrm{FM}(\mathcal{A})$ is definable by a formula

$$\exists x_1 \, \exists x_2 \, (x_1 \neq x_2 \wedge f(x_1) = x \wedge f(x_2) = x).$$

On the other hand, in models from $\mathrm{FM}^*(\mathcal{A})$ all odd elements are indistinguishable and therefore we can not define the maximal element in $\mathcal{A}_{2n+1}^*$ by a formula without MAX. Since we assumed to have the constant MAX which denotes the maximal element of a model, fact 3.12 implies that for each $\mathcal{A}$ the family $\mathrm{FM}^*(\mathcal{A})$ is semantically as powerful as $\mathrm{FM}(\mathcal{A})$. Indeed, there are situations in which $\mathrm{FM}^*(\mathcal{A})$ is strictly stronger than $\mathrm{FM}(\mathcal{A})$. However, before presenting an example let us define a concept which will be useful also in the other parts of our work.

Definition 3.13 (Spectrum) *Let $\mathcal{K}$ be a family of finite models in a vocabulary σ and let φ be a sentence in the vocabulary σ. By a $\mathcal{K}$–spectrum of φ we denote the set of cardinalities of models from $\mathcal{K}$ in which φ is satisfied,*

$$\mathrm{Spec}_{\mathcal{K}}(\varphi) = \{\mathrm{card}(\mathcal{A}) : \mathcal{A} \in \mathcal{K} \wedge \mathcal{A} \models \varphi\}.$$

By a spectrum of $\mathcal{K}$ we mean the set of all $\mathcal{K}$–spectra of sentences in the vocabulary σ,

$$\mathrm{Spec}(\mathcal{K}) = \{\mathrm{Spec}_{\mathcal{K}}(\varphi) : \varphi \in \mathcal{F}_\sigma\}.$$

we will usually consider spectra for families of the form $\mathrm{FM}(\mathcal{A})$.

Let us note that if $\mathcal{K}$ is a family of all finite models, Fin, for σ containing at least one binary relational symbol then the question whether Spec(Fin) is closed on the complement (known also, by the name of its author, as the Asser problem) is one of the main open problems in finite model theory. It is equivalent to the problem in complexity theory whether $\mathrm{NTIME}(2^{O(n)}) = co\mathrm{NTIME}(2^{O(n)})$.

When we consider a family of the form $\mathrm{FM}(\mathcal{A})$ then its spectrum is obviously closed on the complement. Simply for each φ,

$$(\omega \setminus \{0\}) \setminus \mathrm{Spec}_{\mathrm{FM}(\mathcal{A})}(\varphi) = \mathrm{Spec}_{\mathrm{FM}(\mathcal{A})}(\neg\varphi).^3$$

We have the following proposition.

Proposition 3.14 *Let $\mathcal{K}_\mathcal{A} = \{\mathcal{A}_n\}_{n\in\omega}$ and $\mathcal{K}_\mathcal{B} = \{\mathcal{B}_n\}_{n\in\omega}$ be two families of finite models in vocabularies σ and τ, respectively, such that* $\mathrm{card}(\mathcal{A}_n) = \mathrm{card}(\mathcal{B}_n) = n+1$. *If there is an exact interpretation of $\mathcal{K}_\mathcal{A}$ in $\mathcal{K}_\mathcal{B}$ then* $\mathrm{Spec}(\mathcal{K}_\mathcal{A}) \subseteq \mathrm{Spec}(\mathcal{K}_\mathcal{A})$.

Proof. Let $\bar{\varphi}$ be an exact interpretation of $\mathcal{K}_\mathcal{A}$ in $\mathcal{K}_\mathcal{B}$. Then for each model $\mathcal{B}_n$,

$$\mathrm{card}(I_{\bar{\varphi}}(\mathcal{B}_n)) = \mathrm{card}(\mathcal{B}_n).$$

It follows that for each n,

$$\mathcal{A}_n \cong I_{\bar{\varphi}}(\mathcal{B}_n).$$

Now let X be a $\mathcal{K}_\mathcal{A}$–spectrum of a sentence ψ and let $\widehat{I}_{\bar{\varphi}}$ be the translation function as defined in subsection 2.2.2. We have the following sequence of equivalent statements.

$$\begin{aligned} \mathcal{A}_n \models \psi &\iff I_{\bar{\varphi}}(\mathcal{B}_n) \models \psi \\ &\iff \mathcal{B}_n \models \widehat{I}_{\bar{\varphi}}(\psi), \end{aligned}$$

where the last equivalence follows from proposition 2.7. Therefore,

$$X = \mathrm{Spec}_{\mathcal{K}_\mathcal{B}}(\widehat{I}_{\bar{\varphi}}(\psi)).$$

□

Now let us come back to the comparison of various ways of defining the family of finite models for a countable model $\mathcal{A}$.

[3] Obviously, 0 does not belong to any set being a spectrum.

Proposition 3.15 *Let $\mathcal{A} = (\omega, \leq, f)$, where $\leq$ is the standard ordering and $f(i) = 2^k$, for $i \in \{2^{k-1} + 1, \ldots, 2^k\}$. Then there is no exact interpretation of $\mathrm{FM}^*(\mathcal{A})$ in $\mathrm{FM}(\mathcal{A})$.*

Proof. By proposition 3.14, it suffices to show that $\mathrm{Spec}(\mathrm{FM}^*(\mathcal{A}))$ is not contained in $\mathrm{Spec}(\mathrm{FM}(\mathcal{A}))$.

Let $\mathrm{Pow}_2 = \{2^k : k \in \omega\}$. It is easy to see that the formula $\forall x \, \exists y \, P_f(x, y)$ witnesses the fact that $\mathrm{Pow}_2 \in \mathrm{Spec}(\mathrm{FM}^*(\mathcal{A}))$. To show that Pow_2 is not in $\mathrm{Spec}(\mathrm{FM}(\mathcal{A}))$ it suffices to prove that, for each $n \geq 1$, Eros has a winning strategy in the n–moves game on models $\mathcal{A}_{2^{n+4}}$ and $\mathcal{A}_{2^{n+4}-1}$. Consequently, no first order sentence of quantifier rank $\leq n$ can define in $\mathrm{FM}(\mathcal{A})$ the spectrum Pow_2. Since n is arbitrary we conclude that $\mathrm{Pow}_2 \notin \mathrm{Spec}(\mathrm{FM}(\mathcal{A}))$.

Now let us describe a strategy for Eros in the n–moves game on $\mathcal{A}_{2^{n+4}}$ and $\mathcal{A}_{2^{n+4}-1}$. We divide universes of models into two parts such that $|\mathcal{A}_{2^{n+4}}| = A_1 \cup A_2$ and $|\mathcal{A}_{2^{n+4}-1}| = A_1 \cup A_3$, where $A_1 = \{0, \ldots, 2^{n+3} - 1\}$, $A_2 = \{2^{n+3}, \ldots, 2^{n+4}\}$ and $A_3 = A_2 - \{2^{n+4}\}$.

Now to make the life of Eros harder, let Ares choose in the first two extra moves the elements 2^{n+3} and 2^{n+4} from $\mathcal{A}_{2^{n+4}}$ and let Eros answer with elements 2^{n+3} and $2^{n+4} - 1$ from the other structure. Observe that Eros has to answer with the greatest element of the $\mathcal{A}_{2^{n+4}-1}$ since otherwise he would lose in the next step if Ares would choose the greatest element from $\mathcal{A}_{2^{n+4}-1}$.

It suffices to show now that Eros still wins the n-moves game on the structures with so chosen elements. The strategy for Eros is as follows. On the A_1–parts of the structures Eros can play according to the isomorphism between these parts, and on the parts defined by A_2 and A_3 Eros can use his winning strategy in the $(n + 2)$–move game between two orderings of length greater than 2^{n+2}, see fact 2.4. Let us observe that during the game between A_2 and A_3 the functions from both structures do not give Ares any opportunity to differentiate them. □

3.3.1 Δ_0 definability and definability in $\mathrm{FM}(\mathcal{N})$

In the present subsection we establish a relation between Δ_0 definability in $\mathcal{N}$ and definability in the family $FM(\mathcal{N})$. On the first sight it may appear that Δ_0 definability is a stronger notion. When we use a bounded quantifier of the form $Qx \leq t\varphi(\bar{a})$ the value of t may be greater than any parameter in $\varphi(\bar{a})$. Thus, one cannot expect that for each Δ_0 formula $\varphi(x)$ and for each model $\mathcal{N}_k \in \mathrm{FM}(\mathcal{N})$ and $\bar{a} \leq k$,

$$\mathcal{N} \models \varphi[\bar{a}] \text{ if and only if } \mathcal{N}_k \models \varphi[\bar{a}].$$

However, we will see that we can find another formula $\psi(x)$ with the above property, that is for each model $\mathcal{N}_k \in \mathrm{FM}(\mathcal{N})$ and $\bar{a} \leq k$,

$$\mathcal{N} \models \varphi[\bar{a}] \text{ if and only if } \mathcal{N}_k \models \psi[\bar{a}].$$

So, the Δ_0 definability and definability in $\mathrm{FM}(\mathcal{N})$ are, in some sense, equivalent notions.

Definition 3.16 *The family of finite models* $\mathrm{FM}(\mathcal{A})$ *is* cartesian closed *if for each* $k \in \omega$*,*

- *there is a* k*–cartesian interpretation* $\bar{\varphi}$ *such that, for each* n*,*

$$\mathcal{A}_{(n+1)^k-1} \cong I_{\bar{\varphi}}(\mathcal{A}_n),$$

- *there is a formula* $\psi(x, x_1, \ldots, x_k)$ *which defines in* $\mathcal{A}_n$ *the natural embedding of* $\mathcal{A}_n$ *into* $I_{\bar{\varphi}}(\mathcal{A}_n)$*, that is*

$\mathcal{A}_n \models \psi[a, a_1, \ldots, a_k]$ *if and only if* a *is the* i*-th element of* $\mathcal{A}_n$ *and* $(a_1, \ldots, a_k)$ *is the* i*-th element of* $I_{\bar{\varphi}}(\mathcal{A}_n)$ *for some* $i \leq n$*.*[4]

The property of being cartesian closed is in the background of many definability results in finite models, especially in establishing descriptive correspondence between logics and complexity classes, see e.g. [9] or [20].

If we were interested only in spectra for families $\mathrm{FM}(\mathcal{A})$ then we could skip the second requirement in definition 3.16. In this case only cardinality of a model is relevant and usually one does not need to bother about the internal structure of the interpretation. However, since we consider also definability problems within families $\mathrm{FM}(\mathcal{A})$, we want the interpretetation from definition 3.16 to be "well behaved". Due to the second requirement in definition 3.16, everything we can express about the elements from $\{0, \ldots, n\}$ in $\mathcal{A}_{(n+1)^k-1}$ can already be expressed in $\mathcal{A}_n$. In other words, we can use in $\mathcal{A}_n$ the polynomially bigger number of elements of the model $\mathcal{A}_{(n+1)^k-1}$. This will play an important role in the proof of theorem 3.21.

We need also to introduce a strengthening of the notion of interpretation. The main intuition for this is as follows. While we think of interpretability between two domains over the same universe what we want is not just to define in one of them a model isomorphic to the other one. We also want the defined model to be literally the same, that is, the isomorphism function should be just the identity. Moreover, the condition from the next definition, though quite strong, allows us to compare in a convenient way relations between definabilities in two domains.

[4]Because the universe of $\mathcal{A}$ is ω, we may say shortly that $(a_1, \ldots, a_k)$ is the a-th element of $I_{\bar{\varphi}}(\mathcal{A}_n)$.

Definition 3.17 *Let $\mathcal{A}$ and $\mathcal{B}$ be two models with ω as the universe and let $\bar{\varphi}$ be an interpretation of* FM($\mathcal{A}$) *in* FM($\mathcal{B}$). *We say that $\bar{\varphi}$ is order preserving if, for each n, the identity is an isomorphism between $\mathcal{A}_n$ and $I_{\bar{\varphi}}(\mathcal{B}_n)$.*

An order preserving and exact interpretation is called a full interpretation. If there is a full interpretation of FM($\mathcal{A}$) *in* FM($\mathcal{B}$) *we also say that* FM($\mathcal{A}$) *is definable in* FM($\mathcal{B}$).

We have the following useful proposition.

Proposition 3.18 *Let* FM($\mathcal{A}$) *and* FM($\mathcal{B}$) *be mutually definable one in the other. Then,* FM($\mathcal{A}$) *is cartesian closed if and only if* FM($\mathcal{B}$) *is cartesian closed.*

Proof. We assume, for simplicity, that models under consideration are in relational vocabularies. Let $\bar{\varphi}_{\mathcal{A}} = (\varphi_1^{\mathcal{A}}, \ldots, \varphi_s^{\mathcal{A}})$ and $\bar{\varphi}_{\mathcal{B}} = (\varphi_1^{\mathcal{B}}, \ldots, \varphi_t^{\mathcal{B}})$ be two full interpretations of FM($\mathcal{A}$) in FM($\mathcal{B}$) and FM($\mathcal{B}$) in FM($\mathcal{A}$), respectively. Let $\bar{\varphi} = (\varphi_1, \ldots, \varphi_s)$ be a k–cartesian interpretation such that, for each n, $\mathcal{A}_{(n+1)^k-1} \cong I_{\bar{\varphi}}(\mathcal{A}_n)$ and let $\psi(x, x_1, \ldots, x_k)$ be a formula which defines the natural embedding of $\mathcal{A}_n$ into $I_{\bar{\varphi}}(\mathcal{A}_n)$. Let $\mathcal{B}_n = (\{0, \ldots, n\}, R_1, \ldots, R_t)$. Then for $i \leq t$, we define a formula

$$\gamma_i = \widehat{I}_{\bar{\varphi}_{\mathcal{B}}}(\widehat{I}_{\bar{\varphi}}(\widehat{I}_{\bar{\varphi}_{\mathcal{A}}}(R_i(\bar{x})))).$$

It is straightforward to check that $\bar{\gamma} = (\gamma_1, \ldots, \gamma_t)$ is a k–cartesian interpretation of a family FM($\mathcal{B}$), that is

$$\mathcal{B}_{(n+1)^k-1} \cong I_{\bar{\gamma}}(\mathcal{B}_n).$$

Moreover, since interpretations $\bar{\varphi}_{\mathcal{A}}$ and $\bar{\varphi}_{\mathcal{B}}$ are full, the formula $\widehat{I}_{\bar{\varphi}_{\mathcal{A}}}(\psi)$ defines the embedding required in the second condition of definition 3.16. □

The next proposition was implicitly used e.g. in [16]. The detailed proof was given in [42].

Proposition 3.19 *Family* FM($\mathcal{N}$) *is cartesian closed, that is, for each k there is a k–cartesian interpretation $\bar{\varphi}$ such that for each model $\mathcal{N}_n \in FM(\mathcal{N})$*

$$I_{\bar{\varphi}}(\mathcal{N}_n) \cong \mathcal{N}_{(n+1)^k-1}.$$

Moreover, the formula which defines the embedding function h of $\mathcal{N}_n$ into $I_{\bar{\varphi}}(\mathcal{N}_n)$ is $\bigwedge_{i<k}(x_i = 0) \wedge x_k = x$. Then $h(i) = (\underbrace{0, \ldots, 0}_{k-1 \text{ times}}, i)$.

Lemma 3.20 *For each Δ_0–formula $\varphi(\bar{x})$ there exists k such that for all $n \geq 1$, all $\bar{a} \leq n$ and all $m \geq (n+1)^k - 1$,*

$$\mathcal{N} \models \varphi[\bar{a}] \quad \textit{if and only if} \quad \mathcal{N}_m \models \varphi[\bar{a}].$$

Proof. We may assume that $\varphi(\bar{x})$ is in relational like form, that is all terms in $\varphi(\bar{x})$ are of the form $S(0)$ or $z \circ y$, where $\circ \in \{+, \times\}$ and z, y are variables or the constant 0. If it is not so we can find a Δ_0 formula which is equivalent to $\varphi(\bar{x})$ in $\mathcal{N}$ and satisfies the above conditions.

The proof is by induction on the complexity of φ. For $\varphi(\bar{x})$ being quantifier free let $k = 3$. Then for each $n \geq 1$ and for each $\bar{a} \leq n$ the value of any term in φ is less then $(n+1)^3 - 1$. Therefore, for each $m \geq (n+1)^3 - 1$, the equivalence from the lemma holds.

Since the inductive steps for propositional connectives are trivial, we concentrate only on $\varphi(\bar{x})$ of the form $\exists z \leq t(\bar{x})\, \psi(\bar{x}, z)$, where for ψ there is k_0 satisfying the inductive condition. We take $k = 3k_0$. Let us assume that $n \geq 1$, $\bar{a} \leq n$ and that $m \geq (n+1)^k - 1$. We want to show that

$$\mathcal{N} \models \exists z \leq t(\bar{x})\psi[\bar{a}] \quad \text{if and only if} \quad \mathcal{N}_m \models \exists z \leq t(\bar{x})\psi[\bar{a}].$$

If $\mathcal{N} \models \exists z \leq t(\bar{x})\psi[\bar{a}]$ then there exists $b \leq t(\bar{a})$ such that $\mathcal{N} \models \psi[\bar{a}, b]$. Since t is a simple term, $b \leq (n+1)^2$. Then, by the inductive assumption for $m \geq (n+1)^k - 1 \geq ((n+1)^2 + 1)^{k_0} - 1$, we obtain that $\mathcal{N}_m \models \psi[\bar{a}, b]$ and $\mathcal{N}_m \models \varphi[\bar{a}]$. Conversely, if $\mathcal{N}_m \models \exists z \leq t(\bar{x})\psi[\bar{a}]$, there exists $b \leq t(\bar{a})$ such that $\mathcal{N}_m \models \psi[\bar{a}, b]$. Since $b \leq (n+1)^2$ and $m \geq ((n+1)^2+1)^{k_0} - 1$, we obtain, by the inductive assumption, that $\mathcal{N} \models \psi[\bar{a}, b]$ and, finally, that $\mathcal{N} \models \varphi[\bar{a}]$. $\square$

Now we can state a theorem which relates Δ_0 definability in $\mathcal{N}$ and definability in finite models.

Theorem 3.21 *Let $R \subseteq \omega^r$. Then R is Δ_0 definable in $\mathcal{N}$ if and only if $FM((\omega, R))$ is definable in $FM(\mathcal{N})$.*

Proof. First, we consider the implication from the right to the left. Let $\psi_R(x_1, \ldots, x_r, \mathrm{MAX})$ be a full interpretation of $\mathrm{FM}((\omega, R))$ in $\mathrm{FM}(\mathcal{N})$ and let t be the term $\Pi_{i \leq r}(x_i + 2)$. Additionally, let $\varphi_R(x_1, \ldots, x_r)$ be a formula constructed from ψ_r in the following way:

- replace each occurrence of MAX by t,
- bound each quantifier in ψ by t.

Of course φ_R is a Δ_0 formula and we claim that it defines R in $\mathcal{N}$. From the construction of φ_R we have the following equivalence: for each $\bar{a} = a_1, \ldots, a_r \in \omega$,

$$\mathcal{N} \models \varphi_R[\bar{a}] \text{ if and only if } \mathcal{N}_{t(\bar{a})} \models \psi_R[\bar{a}],$$

where the value of the term $t(\bar{a})$ is interpreted in $\mathcal{N}$. Since $\psi_R(x_1, \ldots, x_r)$ constitutes the full interpretation we also have that

$$\mathcal{N}_{t(\bar{a})} \models \psi_R[\bar{a}] \text{ if and only if } R(\bar{a}).$$

Combining these two equivalences we obtain that φ_R defines R in $\mathcal{N}$.

For the converse implication, let $\varphi_R(x_1, \ldots, x_r)$ define R in $\mathcal{N}$ and let k be chosen for φ_R by lemma 3.20. Let $\bar{\varphi}$ be the k–cartesian interpretation from proposition 3.19 and let $\tilde{0}$ be the sequence of $k-1$ zeros. Then for arbitrary $n \geq 1$ and arbitrary $a_1, \ldots, a_r \leq n$ we have the following sequence of equivalent formulas:

$$\begin{aligned} \mathcal{N} \models \varphi_R[\bar{a}] &\iff \mathcal{N}_{(n+1)^k-1} \models \varphi_R[\bar{a}] \\ &\iff I_{\bar{\varphi}}(\mathcal{N}_n) \models \varphi_R[(\tilde{0}, a_1), \ldots, (\tilde{0}, a_r)] \\ &\iff \mathcal{N}_n \models \widehat{I}_{\bar{\varphi}}(\varphi_R)[\tilde{0}, a_1, \ldots, \tilde{0}, a_r]. \end{aligned}$$

Let $\eta(x_1, x_2, \ldots, x_r)$ be $\widehat{I}_{\bar{\varphi}}(\varphi_R)(\tilde{0}, x_1, \ldots, \tilde{0}, x_r)$. Then, for $n \geq 1$, $\eta(x_1, \ldots, x_r)$ defines R restricted to the universe of $\mathcal{N}_n$. To finish the proof we should add to η a clause for the one element model $\mathcal{N}_0$. If $R(0, \ldots, 0)$ then the interpretation of $FM((\omega, R))$ is the formula

$$\exists^{=1} x(x = x) \vee (\exists^{\geq 2} x(x = x) \wedge \eta(x_1, \ldots, x_r)),$$

otherwise we should take

$$(\exists^{=1} x(x = x) \wedge (x_r \neq x_r)) \vee (\exists^{\geq 2}(x = x) \wedge \eta(x_1, \ldots, x_r)).$$

□

As a particular case of theorem 3.21 we obtain a theorem whose proof essentially uses Δ_0 definability of BIT in $\mathcal{N}$, see the second point of lemma 3.4. The theorem itslelf is a part of a mathematical folklore.

Theorem 3.22 *The family* FM(HF) *is definable in* FM($\mathcal{N}$).

Proof. Since $\mathsf{HF} = (\omega, \mathrm{BIT})$ it suffices to show that there is a formula $\varphi(x, y) \in \mathcal{F}_{\{S,+,\times,0\}}$ which in a finite model of cardinality n defines a restriction of BIT to the set $\{0, \ldots, n\}$. However, by lemma 3.4, BIT is Δ_0 definable in $\mathcal{N}$ and, by theorem 3.21, we can transfer this definition to finite models. □

3.3.2 Known relations between FM($\mathcal{N}$), FM(HF) and FM(FW)

In this subsection we present relations between the three domains above which were known prior to this work. Let us start with the theorem from [8]. It is the first step towards the interpretation of addition and multiplication in FM(HF). The following has been proven by Dawar et al.

Theorem 3.23 ([8]) FM($(\omega, \leq)$) *is definable in* FM(HF).

Barrington et el. extended this result in [1] by showing that BIT can express also BITSUM relation. (However, the proof in [1] essentially uses definability of the ordering relation from BIT.) It follows easily, see Immerman, [20], that BIT can express also addition and multiplication. We formulate this result in our terminology and we give a slightly stronger version of it which will be useful for us in section 3.4. Nevertheless, the proofs given in [1] and [20] carry over also to this stronger version.

Definition 3.24 *Let $t \geq 2$. By* $\mathrm{BIT}_t(x, y, k)$ *we denote the predicate which is true when $k < t$ and y has the digit k on the x-th place in its expansion in the base t. In other words, whenever $y = \Sigma_{i=0}^{i=r} a_i t^i$, with $a_i < t$ for $i \leq r$, then*

$$\mathrm{BIT}_t(x, \Sigma_{i=0}^{i=r} a_i t^i, k) \quad \textit{if and only if} \quad x \leq r \textit{ and } a_x = k.$$

When $t = 2$, $\mathrm{BIT}_2(x, y, 1)$ is equivalent to the predicate $\mathrm{BIT}(x, y)$ defined in subsection 3.2.1.

Theorem 3.25 ([1], see also [20]) *Let $t \geq 2$.* FM($\mathcal{N}$) *is definable in* FM((ω, BIT_t)).

In the next section, we use the full power of the the last theorem. Now we are mainly interested in the case when $t = 2$. As a corollary of the last theorem and proposition 3.18 we obtain the proposition which was proven directly by Schweikardt in [42].

Proposition 3.26 ([42]) *For each k, there is a k–cartesian interpretation $\bar{\varphi}$ such that for each model* $\mathsf{HF}_n \in$ FM(HF),

$$I_{\bar{\varphi}}(\mathsf{HF}_n) \cong \mathsf{HF}_{(n+1)^k - 1}.$$

Moreover, the embedding function h of HF_n *into* $I_{\bar{\varphi}}(\mathsf{HF}_n)$ *is defined as* $h(i) = (\underbrace{0, \ldots, 0}_{k-1 \textit{ times}}, i)$.

Proof. The thesis is a consequence of theorems 3.25, 3.22, 3.19 and proposition 3.18. The argument is as follows: each FM($\mathcal{N}$) and FM(HF) is exactly interpretable in the other one. Thus, since FM($\mathcal{N}$) is cartasian closed so is FM(HF). □

In both families, FM($\mathcal{N}$) and FM(HF), we can give a full interpretation of FM(FW^t). This allows us to treat the elements of a finite model in FM($\mathcal{N}$) as words augmented with the concatenation operation.

Theorem 3.27 *For each* $t \geq 1$, FM(FW^t) *is definable in* FM($\mathcal{N}$) *and* FM(HF).

Proof. Since the relation of definability between families of the form FM($\mathcal{A}$) is transitive, it suffices, by theorem 3.25, to give a full interepretation of FM(FW^t) in FM($\mathcal{N}$).

Let us recall that we can define in $\mathcal{N}$ the concatenation operation on words over the alphabet Γ_t by means of addition, multiplication and the graph of the exponentiation function. Since the graph of the exponentiation function is Δ_0 definable from addition and multiplication, therefore we can rewrite the definition of concatenation in $\mathcal{N}$ using only $+$ and $\times$. The definition so obtained is Δ_0. The thesis follows from theorem 3.21. □

3.4 Concatenation defines full arithmetic in finite models

The results from this section were published as a part of Krynicki and Zdanowski [25]. Nevertheless, it is based on the work of the author of this dissertation.

Unless explicitly stated, in this section we consider only alphabets with at least two different characters, that is we consider Γ_t for $t \geq 2$. This assumption follows from the fact that there is a straightforward characterization of FW^1. Namely, FW^1 is isomorphic to $(\omega, +)$ with an isomorphism function given by $f(\underbrace{a_1 \ldots a_1}_{n \text{ times}}) = n$.

In the case of interpretability of FM($\mathcal{N}$) in FM(FW^t) the first important result, according to our present interests, is the result of Bennett, [3]. Let $\Delta_0^{\{*_t, \leq\}}$ be the collection of bounded formulas defined as in section 3.2 but with concatenation as the only function symbol and with $\leq$ as the only

predicate.[5] The following theorem has been proven by Bennett in [3].

Theorem 3.28 ([3]) *Let $t \geq 2$. There are $\Delta_0^{\{*_t,\leq\}}$ formulas which define the addition and multiplication functions in $(\omega, *_t, \leq, 1, \ldots, t)$.*

In what follows we prove the finite model analog of Bennett's theorem. Namely, we show that FM($\mathcal{N}$) and FM(HF) have exact interpretations in FM(FW^t). However, contrary to the Bennett's result, we do not need the ordering relation. Indeed, we will define ordering in a finite model of concatenation.

One possible way of proving the main result of this section would be to show that $\Delta_0^{\{*_t,\leq\}}$ definability in the infinite model is captured by the definability in FM(FW^t). To do this one should prove for FM(FW^t) the analogs of proposition 3.19 and theorem 3.21.[6] However, the proof along this line would relay on relatively complicated and indirect constructions of [3]. Therefore, we decided to give the direct proof. Then, as a consequence of the results proven in previous sections, we obtain that FM(FW^t) is cartesian closed and that $\Delta_0^{\{*_t,\leq\}}$ definability in the infinite model is captured by the definability in FM(FW^t); exactly like in the case for $\mathcal{N}$ and FM($\mathcal{N}$).

As the first step towards the interpretation of the full arithmetic in FM(FW^t) we will show that the ordering relation is definable in finite models from FM(FW^t).

In what follows, we omitthe subscript t in $*_t$ since what is essential in our considerations is only that $t \geq 2$.

Lemma 3.29 *The graph of the concatenation function restricted to the elements of a finite model from* FM(FW^t) *is definable in* FM(FW^t). *We denote the formula which represents this graph by $\varphi_*(x, y, z)$.*

Proof. The formula $\varphi_*(x, y, z)$ can be written as

$$(z \neq \mathrm{MAX} \wedge x * y = z) \vee$$

$$(z = \mathrm{MAX} \wedge ((y = \mathrm{MAX} \wedge x = \lambda) \vee (y = \lambda \wedge x = \mathrm{MAX}))) \vee$$

[5] Bennett uses $\leq$ only in the context $Qx \leq t$ but he observes that $x \leq y$ can be defined as $\exists z \leq y(z = x)$.

[6] Let us observe that while interpreting the model for concatenation of cardinality $(n+1)^k - 1$ in a set of k–tuples from the model of cardinality $n+1$ one cannot propose that a tuple $(\alpha_1, \ldots, \alpha_k)$ corresponds to the element $\alpha_1 * \ldots * \alpha_k$. In this case, for the empty word λ and $\alpha \neq \lambda$, two different tuples $(\alpha, \lambda, \ldots, \lambda)$ and $(\lambda, \ldots, \lambda, \alpha)$ would correspond to the same word α.

$$\{z = \mathrm{MAX} \wedge \exists z'(z' \neq \mathrm{MAX} \wedge (\bigvee_{1 \leq i \leq t} [\mathrm{MAX} = z' * a_i \wedge \bigwedge_{1 \leq j < i} (\mathrm{MAX} \neq z' * a_i) \wedge$$
$$\forall z''((z'' \neq z' \wedge z'' * a_i = \mathrm{MAX}) \Rightarrow z'' * a_1 = \mathrm{MAX}) \wedge$$
$$\exists y'(y = y' * a_i \wedge z' = x * y')])\}.$$

The first two disjuncts of the above formula handle easy cases. If none of them is true then $x * y \geq \mathrm{MAX}$, $x \neq \mathrm{MAX}$ and $y \neq \mathrm{MAX}$. In this case $x \neq \lambda$ and $y \neq \lambda$. We should only exlude the case $x * y > \mathrm{MAX}$. To do this we find a_i such that $\mathrm{MAX} = z' * a_i$ for some minimal $z' < \mathrm{MAX}$. Then it suffices to check that a_i is the ending letter of $y = y' * a_i$ and that $z' = x * y'$. $\square$

Sometimes, when we compare the value of two terms in a given finite model $\mathcal{A}_n \in \mathrm{FM}(\mathcal{A})$ we may think that they are equal while in the infinite model $\mathcal{A}$ they have different values greater or equal to the maximal element of $\mathcal{A}_n$. In such a case values of s and t in $\mathcal{A}_n$ will be equal to the maximal element of $\mathcal{A}_n$. Now we define a formula which distinguishes such cases for models from $\mathrm{FM}(\mathsf{FW}^t)$.

Definition 3.30 *For two terms $s = s_1 * \ldots * s_k$ and $t = t_1 * \ldots * t_n$, were t_i and s_i are variables or constants, we write $t \mathrel{\mathring{=}} s$ for a formula*

$$\exists x_1 \ldots \exists x_k \, \exists y_1 \ldots \exists y_n \, (x_1 = s_1 \wedge y_1 = t_1$$
$$\bigwedge_{1 < i \leq k} \varphi_*(x_{i-1}, s_i, x_i) \wedge \bigwedge_{1 < i \leq n} \varphi_*(y_{i-1}, t_i, y_i) \wedge x_k = y_n).$$

Since φ_* defines in a given $\mathcal{A} \in \mathrm{FM}(FW^t)$ the restriction of the graph of the concatenation function from FW^t to the universe of $\mathcal{A}$, we have the following property of $\mathring{=}$.

Fact 3.31 *For each n and a valuation $\bar{a}$ in FW^t_n, for all terms t, s,*

$$\mathsf{FW}^t_n \models (s \mathrel{\mathring{=}} t)[\bar{a}] \quad \textit{if and only if}$$

$$\mathsf{FW}^t \models (s = t)[\bar{a}] \textit{ and values of } t \textit{ and } s \textit{ in } \mathsf{FW}^t \textit{ are less or equal to } n.$$

It follows that $\mathring{=}$ allows us to overcome the problem which arises when $\mathsf{FW}^t_n \models (t = s)[\bar{a}]$ merely because values of t and s in FW^t are greater or equal to the maximal element of FW^t_n and not necessarily equal one to the other in FW^t.[7]

[7]Let us observe that $s \mathrel{\mathring{=}} t$ is not a formula with two free variables for which we substitute terms t and s. It is the case because the form of $s \mathrel{\mathring{=}} t$ depends on the form of t and s.

Lemma 3.32 *Let $t \geq 1$ and let $\mathrm{lh}(x)$ be the length function for words in Γ_t^*.*

1. *$\mathrm{lh}(x) = \mathrm{lh}(y)$ and $\mathrm{lh}(x) < \mathrm{lh}(y)$ are definable in $\mathrm{FM}(\mathsf{FW}^t)$ by a formula with concatenation only.*

2. *There is a formula $\varphi_{\leq}(x, y)$ such that, for each n, $\varphi_{\leq}$ defines in $\mathsf{FW}_n^t \in \mathrm{FM}(\mathsf{FW}^t)$ the standard ordering relation restricted to the universe of FW_n^t.*

Proof. For $t = 1$ the proposition is obvious so we assume that $t \geq 2$. Let us observe that if we could use the predicates $\mathrm{lh}(x) < \mathrm{lh}(y)$ and $\mathrm{lh}(x) = \mathrm{lh}(y)$ then we could define the ordering by the following formula,

$$x = y \vee \mathrm{lh}(x) < \mathrm{lh}(y) \vee$$

$$[\mathrm{lh}(x) = \mathrm{lh}(y) \wedge \exists z_1, z_2, z_3 \, (\bigvee_{1 \leq i < j \leq t} (x \doteq z_1 * a_i * z_3 \wedge y \doteq z_2 * a_j * z_3))].$$

Since $\mathrm{lh}(x) = \mathrm{lh}(y)$ is easily definable from $\mathrm{lh}(x) < \mathrm{lh}(y)$, it suffices to define the latter predicate. As a first step we define $\psi(x, y)$ of the form

$$\exists z \, (x * z \neq \mathrm{MAX} \wedge y * z = \mathrm{MAX}).$$

with the following properties:

(i) If $\mathrm{lh}(x) + 2 \leq \mathrm{lh}(y)$ then $\psi(x, y)$.

(ii) If $\mathrm{lh}(x) - 1 \geq \mathrm{lh}(y)$ then $\neg\psi(x, y)$.

To show that ψ satisfy (i) and (ii) let us assume that $\mathrm{lh}(x) + 2 \leq \mathrm{lh}(y)$. Then let k be the minimal number such that $\mathrm{lh}(y * a_1^k) = \mathrm{lh}(\mathrm{MAX}) + 1$. Of course, we have $\mathsf{FW}_n \models (y * a_1^k = \mathrm{MAX})$. On the other hand $\mathrm{lh}(x * a_1^k) \leq \mathrm{lh}(y * a_1^k) - 2 \leq \mathrm{lh}(\mathrm{MAX}) + 1 - 2 < \mathrm{lh}(\mathrm{MAX})$. Thus, $\mathsf{FW}_n \models (x * a_1^k \neq \mathrm{MAX})$.

In a similar way we can show the second condition.

Using ψ, we may define the formula $\tilde{\varphi}_<(x, y) :=$

$$\tilde{\varphi}_<(x, y) := \psi(x * x * x, y * y * y) \wedge x * x \neq \mathrm{MAX} \wedge y * y \neq \mathrm{MAX}.$$

Then for all x, y,

$$\text{if } \mathrm{lh}(x) < \mathrm{lh}(y) < \left\lfloor \frac{\mathrm{lh}(\mathrm{MAX})}{3} \right\rfloor \text{ then } \tilde{\varphi}_<(x, y) \text{ and } \neg\tilde{\varphi}_<(y, x). \qquad (*)$$

The property $(*)$ of $\tilde{\varphi}_<$ follows from the fact that if $\mathrm{lh}(x) < \mathrm{lh}(y)$ then $\mathrm{lh}(x*x*x) + 2 < \mathrm{lh}(y*y*y)$ and $\mathrm{lh}(y*y*y) - 1 \geq \mathrm{lh}(x*x*x)$. Unfortunately,

$\tilde{\varphi}_<$ gives us no information when $\mathrm{lh}(x) = \mathrm{lh}(y)$. Nevertheless, the following formula $\tilde{\varphi}_=(x, y) :=$

$$x * x * x \neq \mathrm{MAX} \wedge y * y * y \neq \mathrm{MAX} \wedge$$

$$[x = y = \lambda \vee \exists x', y' \, (\bigvee_{1 \leq i,j \leq t} (x = x' * a_i \wedge y = y' * a_j \wedge \tilde{\varphi}_<(x', y) \wedge \tilde{\varphi}_<(y', x)))]$$

has the property that

$$\text{if } \mathrm{lh}(x), \mathrm{lh}(y) < \left\lfloor \frac{\mathrm{lh}(\mathrm{MAX})}{3} \right\rfloor \text{ then}$$
$$\mathrm{lh}(x) = \mathrm{lh}(y) \text{ if and only if } \tilde{\varphi}_=(x, y),$$

It is easy to see that when $\mathrm{lh}(x) = \mathrm{lh}(y) < \lfloor \frac{\mathrm{MAX}}{3} \rfloor$ then $\tilde{\varphi}_=(x, y)$. For the other direction let us assume that $\tilde{\varphi}_=(x, y)$. If $x = y = \lambda$ there is nothing to prove so let us assume that $x, y > \lambda$.[8] Then, $\psi(x' * x' * x', y * y * y)$, where $\mathrm{lh}(x') = \mathrm{lh}(x) - 1$. By the second property of ψ we obtain that $\mathrm{lh}(x' * x' * x') - 1 < \mathrm{lh}(y * y * y)$. In consequence we have that $\mathrm{lh}(x) \leq \mathrm{lh}(y)$. Similarly, we obtain that $\mathrm{lh}(y) \leq \mathrm{lh}(x)$. Thus, the only possibility is that $\mathrm{lh}(x) = \mathrm{lh}(y)$.

It is easy to write a formula for $\mathrm{lh}(x) < \mathrm{lh}(y)$ now. We simply divide x and y into four parts such that the first three have the same length and the last part of x is shorter than the last part of y. For each x, y we can do it in such a way that all parts will have lengths less than $\lfloor \frac{\mathrm{MAX}}{3} \rfloor$ and we will be able to use $\tilde{\varphi}_<$ and $\tilde{\varphi}_=$ for comparing their lengths. We should only add a finite disjunction for models in which $\mathrm{lh}(\mathrm{MAX}) \leq 3$. Therefore, the predicate $\mathrm{lh}(x) < \mathrm{lh}(y)$ can be expressed as

$$\exists x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \, \{x \doteq x_1 * x_2 * x_3 * x_4 \wedge y \doteq y_1 * y_2 * y_3 * y_4 \wedge$$

$$\bigwedge_{1 \leq i \leq 4} (x_i * x_i * x_i \neq \mathrm{MAX}) \wedge \bigwedge_{1 \leq i \leq 4} (y_i * y_i * y_i \neq \mathrm{MAX}) \wedge$$

$$\bigwedge_{i \leq 2} \tilde{\varphi}_=(x_i, y_i) \wedge \tilde{\varphi}_<(x_3, y_3) \wedge \neg \tilde{\varphi}_=(x_3, y_3)\} \vee$$

$$\bigvee_{0 \leq i < j \leq 3} \quad \bigvee_{\substack{u, v \in \Gamma_t^* \\ \mathrm{lh}(u) = i, \mathrm{lh}(v) = j}} (x \doteq u \wedge y \doteq v).$$

[8] Let us observe that $\tilde{\varphi}_=(x, y)$ cannot be true if one of x and y is the empty word and the other is not.

This ends the proof of the lemma. □

Below, instead of writing $\varphi_{\leq}(x, y)$ we simply write $x \leq y$ when x, y are words. As usual we write $x < y$ when $x \leq y$ and $x \neq y$.

As the next steps towards the interpretation of the full arithmetic in FM(FW^t) we show that in FM(FW^t) one can define the *graphs* of addition and exponentiation with the base t, that is $\exp_t(x) = t^x$.

Before going into details of lemmas, we will say a few more words on the representation of numbers as finite strings over t–letter alphabet, the, so called, t–adic representation. When $t = 2$ we call it a dyadic representation.

When we use the usual number representation, e.g binary or decimal, one number has infinitely many strings which represent it. Since we can always add leading zeros we can write, e.g. the number 2 in the decimal representation as $(2)_{10}$ or $(02)_{10}$. In the model of words with concatenation operation we have unambiguous representation of numbers according to the ordering of words we have defined in subsection 3.2.2. If we set, for $a_1, \ldots, a_t$ – characters in the alphabet – the function $\mathrm{ind}(a_i) = i$ then a word $u = u_k \ldots u_0$, with $u_i \in \Gamma_t^*$, represents the number $\Sigma_{i=0}^{i=k}\mathrm{ind}(u_i)t^i$ (here the empty sum is interpreted as 0). Let

$$\mathrm{num}_t(u) = \Sigma_{i=0}^{i=k}\mathrm{ind}(u_i)t^i$$

be the function which computes the number represented by u in t–adic notation.[9] It follows that for each word u and $a_i \in \Gamma^t$,

$$\mathrm{num}_t(u * a_i) = \mathrm{num}_t(u)t + \mathrm{ind}(a_i).$$

The following lemmas show that addition and $\exp_t$ are definable in finite models from FM(FW^t).

First, we present a lemma which shows how to express some useful properties of words in the language with concatenation.

Definition 3.33 *We define the following relations on the set of all words:*

- $x \subseteq y$, *x is a subword of y,*
- $x \preceq y$, *y begins with the word x, that is $y = x * z$ for some word z,*
- $x \prec y$, *y begins with the word x and it is a proper subword of y,*
- $a_i^* = \{x : x$ *consists only of letters* $a_i\}$, *for* $i \leq t$,

[9] Whenever it is inessential or clear from the context we omit the index t.

- Letter(x, p, a), *the* $\mathrm{lh}(p)$*-th letter of* x *is* a *or* $\mathrm{lh}(x) > \mathrm{lh}(p) + 1$ *and* $a = \lambda$, *that is*

$$x = x_n \dots x_0 \text{ with } x_i \in \Gamma_t \text{ and } (a_{\mathrm{lh}(p)} = a \vee (a = \lambda \wedge \mathrm{lh}(p) > n)).$$

- Interval(x, y, w_1, w_2), y *is a subword of* x *determined by the lengths of* w_1 *and* w_2, *that is,* $x = x_n \dots x_0$ *and* $y = x_{n-\mathrm{lh}(w_1)} \dots x_{n-\mathrm{lh}(w_1)-\mathrm{lh}(w_2)}$, *where* $x_i \in \Gamma_t$.

Lemma 3.34 *The following relations are expressible in finite models from* $\mathrm{FM}(\mathsf{FW}^t)$*:*

- $x \subseteq y$,
- $x \preceq y$,
- $x \prec y$,
- $x \in \{a_i\}^*$, *for* $1 \leq i \leq t$,
- $\mathrm{lh}(x) \geq 1$ *and* $\mathrm{lh}(x) = \max(\mathrm{lh}(y), \mathrm{lh}(z))$,
- Letter(x, p, a),
- Interval(x, y, w_1, w_2),

Proof. $x \subseteq y$ can be expressed as

$$\exists z_1 \, \exists z_2 \, (y \doteq z_2 * x * z_2)$$

Similarly, $x \preceq y$ is just

$$\exists z \, (y \doteq x * z).$$

Then, $x \prec y$ can be written as

$$x \preceq y \wedge x \neq y.$$

$\mathrm{lh}(x) \geq 1$ is just

$$\bigvee_{1 \leq i \leq t} a_i \subseteq x$$

and $\mathrm{lh}(x) = \max(\mathrm{lh}(y), \mathrm{lh}(z))$ can be expressed, by lemma 3.32, as

$$\mathrm{lh}(x) \geq \mathrm{lh}(y) \wedge \mathrm{lh}(x) \geq \mathrm{lh}(z) \wedge (\mathrm{lh}(x) \leq \mathrm{lh}(y) \vee \mathrm{lh}(x) \leq \mathrm{lh}(z)).$$

Letter(x, p, a) can be written as

$$(\mathrm{lh}(x) \leq \mathrm{lh}(p) \wedge a = \lambda) \vee$$

$$\exists z\, \exists y\, (x \stackrel{\circ}{=} y * a * z \wedge \mathrm{lh}(z) = \mathrm{lh}(p) \wedge \bigvee_{1 \leq i \leq t} (a = a_i)).$$

Finally, predicate Interval(x, y, w_1, w_2) can be expressed as

$$\exists x_1\, \exists x_2\, (\mathrm{lh}(x_1) = \mathrm{lh}(w_1) \wedge \mathrm{lh}(x_2) = \mathrm{lh}(w_1 * w_2) \wedge x_1 \preceq x \wedge x_2 \preceq x \wedge x_2 \stackrel{\circ}{=} x_1 * y).$$

□

Lemma 3.35 *There is a formula $\varphi_+(x, y, z)$ which, for each n, defines in $\mathsf{FW}^t_n \in \mathrm{FM}(\mathsf{FW}^t)$ the graph of the addition function restricted to $|\mathsf{FW}^t|$.*

Proof. We write a formula which describes the algorithm of adding two numbers in t–adic notation, say $x = x_n \dots x_0$ and $y = y_k \dots y_0$, where $x_i, y_j \in \Gamma^t$ for $i \leq n, j \leq k$. The algorithm is similar to the usual algorithm of addition, e.g. in binary or decimal notation. However, contrary to the standard case, during the process of addition of two numbers in t–adic notation we may encounter three types of carry: no carry, carry equals 1 and carry equals 2.

Adding $x = x_n \dots x_0$ to $y = y_k \dots y_0$ we guess two strings, c_1 and c_2. Let $c_1 = d_m \dots d_0$ and $c_2 = d'_m \dots d'_0$, where $m = \max(n, k)$. Then, $d_i = a_2$ if there is a carry generated on the i-th position and otherwise $d_i = a_1$. If $d_i = a_2$ then d'_i describes carry generated at this position, that is if the carry equals 1 then $d'_i = a_1$ and if the carry equals 2, then $d'_i = a_2$. With the help of c_1 and c_2 one can verify that a given word z is the result of adding x and y.

Now we write formulas which determine c_1 and c_2.[10] To shorten our formulas we assume convention that the empty word λ is denoted as a_0, just as it would be one more letter in our alphabet. Sometimes we also skip the concatenation sign, that is instead of $u * w$ we write uw. We do it often when one of the arguments of $*$ is a one letter word.

The formula $\mathrm{Carry}_1(x, z, c_1, c_2)$ which describes c_1 has the form

$$\bigwedge_{3 \leq i \leq t} a_i \not\preceq c_1 \wedge \mathrm{lh}(c_1) = \max(\mathrm{lh}(x), \mathrm{lh}(y)) \wedge$$

[10] Let us observe that both c_1 and c_2 are less than at least one of x and y.

$$\{\mathrm{Letter}(c_1,\lambda,a_2) \equiv [\bigvee_{\substack{i+j>t\\0\le i,j\le t}} (\mathrm{Letter}(x,\lambda,a_i)\wedge \mathrm{Letter}(y,\lambda,a_j))]\wedge$$

$$\forall w(\mathrm{lh}(w)<\mathrm{lh}(c_1)\Rightarrow (\mathrm{Letter}(c_1,wa_1,a_2) \iff \psi(x,y,w,c_1,c_2))\},$$

where ψ is a disjunction of three formulas

- $$\mathrm{Letter}(c_1,w,a_1)\wedge [\bigvee_{\substack{i+j>t\\0\le i,j\le t}} (\mathrm{Letter}(x,wa_1,a_i)\wedge \mathrm{Letter}(y,wa_1,a_j))],$$

- $$\mathrm{Letter}(c_1,w,a_2)\wedge \mathrm{Letter}(c_2,w,a_1)\wedge$$
  $$[\bigvee_{\substack{i+j+1>t\\0\le i,j\le t}} (\mathrm{Letter}(x,wa_1,a_i)\wedge \mathrm{Letter}(y,wa_1,a_j))],$$

- $$\mathrm{Letter}(c_1,w,a_2)\wedge \mathrm{Letter}(c_2,w,a_2)\wedge$$
  $$[\bigvee_{\substack{i+j+2>t\\0\le i,j\le t}} (\mathrm{Letter}(x,wa_1,a_i)\wedge \mathrm{Letter}(y,wa_1,a_j))].$$

Formula ψ uses the information coded in c_1 and c_2 about the carry generated at the position $\mathrm{lh}(w)$ and then determines whether there is a carry generated on the position $\mathrm{lh}(w)+1$. The carry at the 0-th position is computed in the second line of $\mathrm{Carry}_1(x,z,c_1,c_2)$.

$\mathrm{Carry}_2(x,y,c_1,c_2)$ can be written as

$$\bigwedge_{3\le i\le t} a_i \not\subseteq c_1 \wedge \mathrm{lh}(c_2)=\max(\mathrm{lh}(x),\mathrm{lh}(y))\wedge (\mathrm{Letter}(c_2,\lambda,a_1)\wedge$$
$$\forall w(\mathrm{lh}(w)<\mathrm{lh}(c_1)\Rightarrow$$
$$(\mathrm{Letter}(c_2,wa_1,a_2) \iff (\mathrm{Letter}(c_1,w,a_2)\wedge \psi'(x,y,w,c_1,c_2)))),$$

where ψ' is a disjunction of formulas

- $$\mathrm{Letter}(c_2,w,a_1)\wedge (\bigvee_{\substack{i+j\ge 2t\\0\le i,j\le t}} (\mathrm{Letter}(x,wa_1,a_i)\wedge \mathrm{Letter}(y,wa_1,a_j))),$$

•

$$\mathrm{Letter}(c_2, w, a_2) \wedge (\bigvee_{\substack{i+j \geq 2t-1 \\ 0 \leq i,j \leq t}} (\mathrm{Letter}(x, wa_1, a_i) \wedge \mathrm{Letter}(y, wa_1, a_j))).$$

In the second line of Carry_2 we use the fact that there can not be a carry equal 2 if there was no carry from the previous position what is expressed by $\mathrm{Letter}(c_1, w, a_2)$. We check this fact with the help of formula $\mathrm{Letter}(c_1, w, a_2)$. Then, in ψ' we compute what should be the value of a carry on the $\mathrm{lh}(wa_1)$-th position.

The formula $\psi'(x, y, w, c_1, c_2)$ describes the situations in which a carry on a given position $lh(wa_1)$ equals 2 when the carry from the position $\mathrm{lh}(w)$ equals 1 or 2.

The formulas above, $\mathrm{Carry}_1(x, y, c_1, c_2)$ and $\mathrm{Carry}_2(x, y, c_1, c_2)$, describe recursively properties of c_1 and c_2. To compute the k-th letter of c_1, Carry_1 uses the $(k-1)$-th letters of c_1 of c_2. The same fact holds also with respect to Carry_2 and c_2.

It can be proven by a simultaneous induction on the length of subwords of c_1 and c_2 that they are uniquely determined for given x and y. Namely, for $c_1 = d_m \ldots d_0$ and $c_2 = d'_m \ldots d'_0$ such that $\mathrm{Carry}_1(x, y, c_1, c_2)$ and $\mathrm{Carry}_2(x, y, c_1, c_2)$, the letters d_0 and d'_0 are determined uniquely for a given x, y. Then it holds that if d_i and d'_i, for $i < m$, are determined uniquely, then also d_{i+1} and d'_{i+1} are determined uniquely.

We define three formulas:

- $\mathrm{NoCarry}(c_1, w)$ for a formula which tells that there was no carry generated at the position $\mathrm{lh}(w)$,

$$\mathrm{Letter}(c_1, w, a_1),$$

- $\mathrm{Carry1}(c_1, c_2, w)$ for a formula which tells that carry generated at the position $\mathrm{lh}(w)$ is equal 1,

$$\mathrm{Letter}(c_1, w, a_2) \wedge \mathrm{Letter}(c_2, w, a_1),$$

- $\mathrm{Carry2}(c_1, c_2, w)$ which states that carry generated at the position $\mathrm{lh}(w)$ is equal 2,

$$\mathrm{Letter}(c_1, w, a_2) \wedge \mathrm{Letter}(c_2, w, a_2).$$

Now we can write a formula $\mathrm{Add}(x, y, z)$ which expresses that z is the result of addition of x and y (see below for a description of $\mathrm{Add}(x, y, z)$).

$$\exists c_1, c_2 \, \{\mathrm{Carry}_1(x, y, c_1, c_2) \wedge \mathrm{Carry}_2(x, y, c_1, c_2) \wedge$$

$$\exists z'[(\bigvee_{1\le i\le t}(z=z'a_i))\wedge((\mathrm{lh}(z)=\max(\mathrm{lh}(x),\mathrm{lh}(y))\wedge\mathrm{Letter}(c_1,z',a_1))\vee$$

$$(\mathrm{lh}(z)=\max(\mathrm{lh}(x),\mathrm{lh}(y))+1\wedge\mathrm{Letter}(c_1,z',a_2)))]\wedge$$

$$\bigwedge_{0\le i\le t}[\mathrm{Letter}(z,\lambda,a_i)\equiv(\bigvee_{r\in\{0,1\}}\bigvee_{\substack{j+k=rt+i\\0\le j,k\le t}}(\mathrm{Letter}(x,\lambda,a_j)\wedge\mathrm{Letter}(z,\lambda,a_k)))]\wedge$$

$$\forall w\,[\mathrm{lh}(w)\le\mathrm{lh}(z)\Rightarrow(\bigwedge_{0\le i\le t}(\mathrm{Letter}(z,wa_1,a_i)\equiv\psi_i))],$$

where $\psi_i(x,y,z,w,c_1,c_2)$ is the disjunction of the following formulas.

$$\mathrm{NoCarry}(c_1,w)\wedge\bigvee_{r\in\{0,1\}}\bigvee_{\substack{j+k=rt+i\\0\le j,k\le t}}(\mathrm{Letter}(x,wa_1,a_j)\wedge\mathrm{Letter}(z,wa_1,a_k)),$$

$$\mathrm{Carry1}(c_1,c_2,w)\wedge\bigvee_{r\in\{0,1,2\}}\bigvee_{\substack{j+k+1=rt+i\\0\le j,k\le t}}(\mathrm{Letter}(x,wa_1,a_j)\wedge\mathrm{Letter}(z,wa_1,a_k)),$$

$$\mathrm{Carry2}(c_1,c_2,w)\wedge\bigvee_{r\in\{0,1,2\}}\bigvee_{\substack{j+k+2=rt+i\\0\le j,k\le t}}(\mathrm{Letter}(x,wa_1,a_j)\wedge\mathrm{Letter}(z,wa_1,a_k)).$$

In the first line of $\mathrm{Add}(x,y,z)$ we guess the words c_1 and c_2 which describe carries in the proces of additions of x and y. The second and third lines determine, on the basis of the structure of c_1, whether the length of z is correct. Then, the fourth line describes that the first letter of z is the result of adding first letters of x and y. The last line of the formula does the same for the following letters of z. The correctness of $\mathrm{Add}(x,y,z)$ follows directly from the meaning of the previously constructed formulas. □

From now on, till the end of this chapter, when a and b are elements of a model FW_n we write $a+b$ to denote the sum of a and b, i.e. the element c such that $\mathsf{FW}_n\models\varphi_+[a,b,c]$.

Lemma 3.36 *Let* $\exp_t(x)=t^x$. *There is a formula* $\varphi_{\exp_t}(x,y)$ *which, for each* n, *defines in* FW_n^t *the graph of the exponentiation function* $\exp_t$ *restricted to the universe of* FW_n^t.

Proof. Since we assumed that our models have as universes initials segments of ω we write, for words w,u, expressions like $\exp_t(u)=w$ with the natural meaning.

For each $k > 0$, the word which corresponds in FW_n^t to the number t^k has the form $a_{t-1}^{k-1}a_t$:

$$\mathrm{num}(a_{t-1}^{k-1}a_t) = \sum_{i=1}^{k-1}(t-1)t^i + t = (\sum_{i=0}^{k-1}(t-1)t^i - (t-1)) + t = t^k.$$

The set of words u such that $u = \exp_t(v)$, for some v, is definable by the formula

$$\mathrm{Pow}_t(u) := \exists u_1\,(u_1 \in \{a_1\}^* \wedge u \doteq u_1 * a_2) \vee u \doteq a_1.$$

Now the proof of the lemma proceeds as follows. Firstly, we define the function $\exp_t$ on some initial segment of a model FW_n^t and then we extend this definition on the whole model. The general idea of the construction is to describe by some word from FW_n^t the polynomial algorithm for fast exponentiation. The algorithm uses the following recursive dependencies:

$$\exp_t(\lambda) = a_1,$$

$$\exp_t(a_i) = a_{t-1}^{i-1}a_t, \qquad \text{for } i = 1, \ldots, t,$$

$$\exp_t(ua_i) = a_{t-1}^{t(x+1)+i-1}a_t, \qquad \text{whenever } \exp_t(u) = a_{t-1}^x a_t.$$

For a one letter word a_i we use the expression $\exp_t(a_i)$ for the word $a_{t-1}^{i-1}a_t$.

By $\mathrm{RecExp}(a, y_1, y_2)$, where a is a one letter string, we mean the formula which states that whenever $y_1 = \exp_t(u)$, for some u, then $y_2 = \exp_t(ua)$. It can be written as

$$[y_1 \doteq a_1 \wedge (\bigvee_{1\le i\le t}(a \doteq a_i \wedge y_2 \doteq \exp_t(a_i)))] \vee \exists v \in \{a_{t-1}\}^*\,[y_1 \doteq v * a_t \wedge$$

$$(\bigvee_{1\le i\le t}(a \doteq a_i \wedge y_2 \doteq \underbrace{va_{t-1} * \ldots * va_{t-1}}_{t \text{ times}} * \underbrace{a_{t-1} * \ldots * a_{t-1}}_{(i-1) \text{ times}} * a_t))].$$

Now we can present the main construction. Let $u = u_n \ldots u_0$, with $u_i \in \Gamma_t$, be a word for which we want to compute $\exp_t(u)$. We construct three words x, y, z such that $x = x_n * x_{n-1} * \ldots * x_0$, $y = y_n * y_{n-1} * \ldots * y_0$, $z = z_n * z_{n-1} * \ldots * z_0$, which satisfy the following dependencies:

1. $\mathrm{lh}(x_i) = \mathrm{lh}(y_i) = \mathrm{lh}(z_i)$, we denote $\mathrm{lh}(x_i)$ by l_i,
2. $x_i = u_n \ldots u_i a_1^{l_i - i}$,
3. $y_i = a_{t-1}^{l_i - 1}a_t$,

4. $z_i = a_2^{i+1} a_1^{l_i - i - 1}$,

5. $\exp_t(u_n \dots u_i) = y_i$.

As it is expressed in point 5 we store the value $\exp_t(u_n \dots u_i)$ in y_i and the value $u_n \dots u_i$ in x_i. The sequence of $a_2's$ in z_i determines the length of $u_n \dots u_i$. If we could find x, y, z with the above properties then we could find $\exp_t(u) = y_0$. Thus, our aim is to write a formula $\mathrm{GoodSeq}(u, x, y, z)$ which states that x, y, z satisfy points $1 - 5$ for u.

Firstly, we write a formula $\mathrm{PowSeq}(y)$ which expresses that y is a concatenation of strings which are greater than 1 powers of t. It has the form

$$\forall w \subseteq y (a_{t-1} \subseteq w \vee a_t \subseteq w) \wedge y \neq \lambda.$$

Now we write a formula $\mathrm{Next}(y, w_1, w_2)$ which expresses that $w_1 \prec w_2 \preceq y$ and that w_2 is w_1 prolonged with a word being one of y_i.

$$w_1 \prec w_2 \wedge w_2 \preceq y \wedge [(w_1 \stackrel{\circ}{=} \lambda \wedge \mathrm{Pow}_t(w_2)) \vee$$

$$\exists s_1 \exists s_2 \, (\mathrm{Pow}_t(s_2) \wedge w_1 \stackrel{\circ}{=} s_1 * a_t \wedge w_2 \stackrel{\circ}{=} w_1 * s_2)].$$

Next, we write a formula $\mathrm{First}(u, x, y, z)$ which expresses that x_n, y_n, z_n satisfies dependencies 1 – 5.

$$\exists w \{\mathrm{Next}(y, \lambda, w) \wedge [\bigvee_{1 \leq i \leq t} (a_i \preceq u \Rightarrow$$

$$[w \stackrel{\circ}{=} \exp_t(a_i) \wedge \exists v \in \{a_1\}^* \, (\mathrm{lh}(a_1 v) = \mathrm{lh}(w) \wedge a_i v \preceq x \wedge a_2 v \preceq z)])]\}.$$

It would be difficult to express that a given triple (x_i, y_i, z_i) satisfies conditions $1 - 5$. Instead, we write a formula $\mathrm{CorrectStep}(u, x_{i+1}, y_{i+1}, z_{i+1}, x_i, y_i, z_i)$ which expresses that if x_i, y_i, z_i are the elements following $x_{i+1}, y_{i+1}, z_{i+1}$ in the sequence which forms x, y, z then x_i, y_i, z_i satisfy 1 – 5 provided $x_{i+1}, y_{i+1}, z_{i+1}$ satisfy 1 – 5. It has the form

$$\exists s_1 \in \{a_2\}^* \exists s_2 \in \{a_1\}^* \; \exists u_1 \preceq u \exists u_2 \preceq u \, [z_{i+1} \stackrel{\circ}{=} s_1 a_1 s_2 \wedge z_i \stackrel{\circ}{=} s_1 a_2 s_2 \wedge$$

$$\mathrm{lh}(u_1) = \mathrm{lh}(s_1) \wedge \mathrm{lh}(u_2) = \mathrm{lh}(s_1 a_2) \wedge x_{i+1} \stackrel{\circ}{=} u_1 a_1 s_2 \wedge x_i \stackrel{\circ}{=} u_2 s_2 \wedge$$

$$\bigvee_{1 \leq i \leq t} (u_1 a_i \stackrel{\circ}{=} u_2 \wedge \mathrm{RecExp}(a_i, y_{i+1}, y_i))].$$

The formula $\mathrm{CorrectStep}(u, x_{i+1}, y_{i+1}, z_{i+1}, x_i, y_i, z_i)$ checks the following dependencies.

- z_i begins with the sequence of a_2's which is one letter longer than the corresponding sequence in z_{i+1},

- x_{i+1} and x_i begin with the initial segments of u: u_1 and u_2, respectively, and the lengths of these sequences are determined by the lengths of a_2's sequences in z_{i+1}, z_i,
- if $y_{i+1} = \exp_t(w)$, then $y_i = \exp_t(wa)$, where a is the last letter in u_2.

Then we write a formula $\mathrm{Induct}(u, x, y, z)$ which states that, for all $i < n$, $\mathrm{CorrectStep}(u, x_{i+1}, y_{i+1}, z_{i+1}, x_i, y_i, z_i)$ holds. Since we know how to express that the triple x_n, y_n, z_n is correct and the whole sequence is finite it clearly suffices to assert correctness of the whole sequence. The formula $\mathrm{Induct}(u, x, y, z)$ has the form

$$\begin{aligned}\forall w_1, w_2, w_3\, \{&(\mathrm{Next}(y, w_1, w_2) \wedge \mathrm{Next}(y, w_2, w_3)) \Rightarrow \\ &\forall x_1, x_2\, ((\mathrm{Interval}(x, x_1, w_1, w_2) \wedge \mathrm{Interval}(x, x_2, w_2, w_3)) \Rightarrow \\ &\forall y_1, y_2\, ((\mathrm{Interval}(y, y_1, w_1, w_2) \wedge \mathrm{Interval}(y, y_2, w_2, w_3)) \Rightarrow \\ &\forall z_1, z_2\, (\mathrm{Interval}(z, z_1, w_1, w_2) \wedge \mathrm{Interval}(z, z_2, w_2, w_3)) \Rightarrow \\ &\qquad \mathrm{CorrectStep}(u, x_1, y_1, z_1, x_2, y_2, z_2))))\}.\end{aligned}$$

In the first four lines of the above formula we find the words x_i, y_i, z_i, for $i \in \{1, 2\}$, such that they are consecutive elements of the sequences forming x, y and z. We extract them from x, y, z on the basis of the structure of y using auxiliary words w_1 and w_2. In the last line we check that x_1, y_1, z_1 and x_2, y_2, z_2 satisfy the recursive dependencies.

The whole formula $\mathrm{GoodSeq}(u, x, y, z)$, which expresses that x, y, z satisfy the conditions 1 – 5 for u, has the form

$$\mathrm{lh}(x) = \mathrm{lh}(y) = \mathrm{lh}(z) \wedge \mathrm{PowSeq}(y) \wedge \mathrm{First}(u, x, y, z) \wedge$$

$$\mathrm{Induct}(u, x, y, z) \wedge \exists w(\mathrm{Next}(y, w, y) \wedge \mathrm{Interval}(x, u, w, x)).$$

The last conjunct of the above formula assures us that the last member of $x_n, x_{n-1}, \ldots, x_0$ is u. Thus, given u and x, y, z such that $\mathrm{GoodSeq}(u, x, y, z)$, the last member of the sequence $y = y_n * \ldots * y_0$, is equal to $\exp_t(u)$. We can define this element by the following formula

$$\mathrm{Last}(y, out) := \exists w\, (\mathrm{Next}(y, w, y) \wedge y \stackrel{\circ}{=} w * out).$$

Of course in general it is not true that if u and $\exp_t(u)$ are elements of a finite model FW_n, then also x, y, z satisfying $\mathrm{GoodSeq}(u, x, y, z)$ are in FW_n. However, the length of x, y, z is no more than two times longer than the length of $\exp_t(u)$. To see this it suffices to note that the length of y_0 is equal

to the length of $\exp_t(u)$ and that, for each $0 \leq i < \mathrm{lh}(u)$, $2\mathrm{lh}(y_{i+1}) \leq \mathrm{lh}(y_i)$. Since $\Sigma_{i=0}^{i=k} 2^i < 2^{k+1}$, we obtain that

$$\mathrm{lh}(x) = \mathrm{lh}(y) = \mathrm{lh}(z) < 2\mathrm{lh}(\exp_t(u)).$$

It follows that the formula $\tilde{\varphi}_{\exp_t}(u, w)$ of the form

$$(u = \lambda \wedge w = a_1) \vee \exists x, y, z\, (\mathrm{GoodSeq}(u, x, y, z) \wedge \mathrm{Last}(y, w))$$

defines the graph of $\exp_t$ restricted to the elements u such that $2\mathrm{lh}(u) < \mathrm{lh}(\mathrm{MAX})$.

To extend this definition on the whole model FW_n^t, one may use the following dependency:
if

- $y_1 = \exp_t(x_1) = a_{t-1}^{\mathrm{num}(x_1)-1} a_t$,
- $y_2 = \exp_t(x_2) = a_{t-1}^{\mathrm{num}(x_2)-1} a_t$,
- $y_3 = \exp_t(x_3) = a_{t-1}^{\mathrm{num}(x_3)-1} a_t$,

for $x_1, x_2, x_3 \geq 1$, then

$$y = \exp_t(x_1 + x_2 + x_3) = a_{t-1}^{(\mathrm{num}(x_1)-1)+(\mathrm{num}(x_2)-1)+(\mathrm{num}(x_3)-1)+2} * a_t,$$

where $x_1 + x_2 + x_3$ is the usual addition operation which was shown to be definable in FW_n^t in lemma 3.35.

So, let $\Gamma_t^{\leq 2}$ be the set of words of length ≤ 2. Then we can write the formula expressing that $w = \exp_t(u)$ as follows

$$\Big(\bigvee_{s \in \Gamma^{\leq 2}} (u \doteq s \wedge w \doteq \exp_t(s))\Big) \vee [\neg\varphi_{\leq}(a_t a_t, u) \wedge$$

$$\exists u_1, u_2, u_3\, \exists w_1, w_2, w_3\, \Big(\bigwedge_{i \leq 3} (\mathrm{lh}(u_i) \geq 1 \wedge \tilde{\varphi}_{\exp_t}(u_i, w_i)) \wedge u = u_1 + u_2 + u_3 \wedge$$

$$\exists s, s_1, s_2, s_3\, \Big(s \in \{a_{t-1}\}^* \wedge \bigwedge_{i \leq 3} s_i \in \{a_{t-1}\}^* \wedge$$

$$\bigwedge_{i \leq 3} (w_i \doteq s_i * a_t) \wedge s \doteq s_1 * s_2 * s_3 * a_{t-1} a_{t-1}\Big) \wedge w \doteq s * a_t)\Big].$$

The first disjunction of the above formula is finite and therefore can be easily written in the language of FW_n^t. In the next three lines we divide u into three words: u_1, u_2, u_3, for which we can find the value of $\exp_t$ using the formula

$\tilde{\varphi}_{\exp_t}$. Then we construct the value $\exp_t(u)$ from values $\exp_t(u_1)$, $\exp_t(u_2)$ and $\exp_t(u_3)$. The correctness of this formula follows from the fact that if u_i is a word such that $2\mathrm{num}(u_1) < \mathrm{num}(u)$ then $2\mathrm{lh}(\exp_t(u_1)) < \mathrm{lh}(\exp_t(u)) \leq \mathrm{lh}(\mathrm{MAX})$. Thus $\exp_t(u_1)$, $\exp_t(u_2)$ and $\exp_t(u_3)$ are short enough to find them by means of a formula $\tilde{\varphi}_{\exp_t}$. $\square$

As the final lemma we state

Lemma 3.37 $\mathrm{FM}((\omega, \mathrm{BIT}_t))$ *is definable in* $\mathrm{FM}(\mathsf{FW}^t)$.

Proof. Let us observe that the number t^k, for $k > 0$, is represented by a word $a_{t-1}^{k-1}a_t$ and that numbers it^k, for $1 < i < t$, are represented by $a_{i-1}a_{t-1}^{k-1}a_t$. Then we have that

- $\mathrm{num}(u)$ has the digit 1 on the k-th position in t–ary representation if and only if $a_{t-1}^{k-1}a_t \leq u < a_1a^{k-1}a_t$ or u ends with the word v such that $\mathrm{lh}(v) = k+1$ and $a_ta_{t-1}^{k-1}a_t \leq v < a_1a_{t-1}^{k-1}a_t$.

The dependencies for the digits $2, \ldots, t-1$ are a bit less complicated. For $i \in \{2, \ldots, t-1\}$,

- u has a digit i on the k–th position in its t–ary representation if and only if u ends with a word v such that $a_{i-1}a_{t-1}^{k-1}a_t \leq v < a_ia_{t-1}^{k-1}a_t$

and finally

- u has the digit 0 on the k–th position in its t–ary representation if and only if u ends with a word v such that $a_{t-1}a_{t-1}^{k-1}a_t \leq v < a_ta_{t-1}^{k-1}a_t$.

Therefore, we can express that u has 1 on the position w by a formula $\mathrm{Digit}_1(w, u)$ of the form

$$\exists s\,\{\exp_t(w) \doteq s \wedge [(s \leq u < a_1 * s) \vee \exists v \exists v'\,(v' * v \doteq u \wedge a_t * s \leq v < a_1 * s)]\}.$$

Formulas $\mathrm{Digit}_i(w, u)$, for $i \in \{2, \ldots, t-1\}$ expressing that u has i on the position w have the form,

$$\exists s \exists v \exists v'\,(\exp_t(w) \doteq s \wedge v' * v \doteq u) \wedge a_{i-1} * s \leq v < a_i * s).$$

Consequently, $\mathrm{Digit}_0(w, u)$, with the obvious meaning, is a formula

$$\exists s \exists v \exists v'\,(\exp_t(w) \doteq s \wedge v' * v \doteq u \wedge a_{t-1} * s \leq v < a_t * s).$$

The previous lemmas assure that all predicates used in formulas Digit_i can be expressed by means of concatenation.

Now we can write a formula for $\mathrm{BIT}_t(x, y, z)$. It has the form

$$(z = \lambda \wedge \mathrm{Digit}_0(x, y)) \vee (\bigvee_{0<i<t} (z = a_{i-1} \wedge \mathrm{Digit}_i(x, y)).$$

□

Now we are ready to state the main result of this section. Namely, that concatenation in finite models has the expressive power of the full arithmetic of addition and multiplication or the arithmetic of hereditarly finite sets.

Theorem 3.38 *For each $t \geq 2$, both* $\mathrm{FM}(\mathcal{N})$ *and* $\mathrm{FM}(\mathsf{HF})$ *are definable in* $\mathrm{FM}(\mathsf{FW}^t)$.

Proof. Let $t \geq 2$. By theorem 3.22, $\mathrm{FM}(\mathsf{HF})$ is definable in $\mathrm{FM}(\mathcal{N})$ and by theorem 3.25, $\mathrm{FM}(\mathcal{N})$ is definable in $\mathrm{FM}((\omega, \mathrm{BIT}_t))$. The relation of definability is transitive so, to prove the theorem, it suffices to note that, by lemma 3.37, $\mathrm{FM}((\omega, \mathrm{BIT}_t))$ is definable in $\mathrm{FM}(\mathsf{FW}^t)$. □

In the last section of Barrington, Immerman and Straubing [1], the authors put the question about relations other than BIT having the same expressive power in finite models as arithmetic of addition and multiplication. In this section we have shown that concatenation has the expressive power of the full arithmetic, too.

All three structures, $\mathcal{N}$, HF and FW^t, are considered as fundamental arithmetical structures and each of them was known to be definable in any other. Now we know that all these definability results carry over into the finite models framework.

Chapter 4

Representing concepts in finite models

4.1 Representing computations in finite models

One of the most fruitful ideas in logic was the description of computations in various logical formalisms. We can recall the formalism related to Turing machines as well as that of Δ_1–definable arithmetical functions or terms in lambda calculus. This idea was behind Church's proof of undecidability of first order logic and Trachtenbrot's proof of undecidability of tautologies of first order logic in finite models. We will present now the main concepts needed to carry out such a description and we will fix some conventions. The technical details of the description and the proofs of main lemmas will be given in the appendix, because they are not crucial for the following parts of the work. Though their development is very fascinating it may be safely skipped by a reader familiar with these notions.

4.1.1 Describing computations

Let $H = (Q, \Sigma, \Gamma, \delta, q_S, q_A)$ be a Turing machine, as in section 2.3. For simplicity we assume that $Q = \{q_1, \ldots, q_n\}$, $q_S = q_1$, $q_2 = q_A$, $\Sigma = \{0, 1\}$, $\Gamma = \{0, 1, \alpha, \beta\}$. Since H is a finite object, we can fully describe it by a finite word. With some ambiguity, we denote this description also by H.

A computation of H on a word w can be seen as the sequence of configurations, $C_0, \ldots, C_K$, where C_0 is the starting configuration and for each $i < K$, C_i and C_{i+1} describe the consecutive steps in the computation according to the function δ and C_K describes the final state of computation.

Each C_i can be written as

$$\alpha a_1 a_2 \dots a_{k-1} \mathrm{q} \underbrace{1 \dots 1}_{m \text{ times}} \mathrm{q} a_k \dots a_{r-1} a_r,$$

where $\alpha a_1 \dots a_r$ is the word written on the tape, H is in the state q_m and the string q1...1q indicates the position of the head of H. To make C_i unique we assume that $a_1 \dots a_r$ contains the word w and only those squares outside w which were earlier visited by H. Now if # is a new fixed symbol then we can describe a K–step computation of H on w by the following string

$$H\#\#C_0\#C_1\#\dots\#C_K\#.$$

Now we state the lemma which will be useful in the next chapters. It describes what can be said about computations in finite models. The main advantage of this lemma is that it allows to transfer the recursion–theoretic concepts into the context of finite models. Various versions of it can be found in many logical textbooks, e.g. [9].

In what follows we use the identification of words and natural numbers.

Lemma 4.1 *For each $r \in \omega$ there is an arithmetical formula* $\mathrm{Comp}(x, y)$ *such that for each Turing machine H and for each $\bar{w} = w_1, \dots, w_r$, c and $n \geq c$ the following holds*

$$c \text{ is a computation of } H \text{ with an input } \bar{w} \iff \mathcal{N}_n \models \mathrm{Comp}[H, \mathrm{code}(\bar{w}), c],$$

where $\mathcal{N}_n \in \mathrm{FM}(\mathcal{N})$ and code *is a Δ_0 definable function which codes r-tuples (see an example of such a coding on page 73, definition 4.25). In other words if $n \geq c$, we can correctly recognize the computation c in a finite model $\mathcal{N}_n$. Moreover, if $n < c$ then, for each $a \leq n$,*

$$\mathcal{N}_n \not\models \mathrm{Comp}[H, \mathrm{code}(\bar{w}), a].$$

Similarly, there is a formula $\mathrm{Accept}(x, y)$ *such that for each c, each Turing machine H and each $n \geq c$,*

$$c \text{ is an accepting computation of } H \iff \mathcal{N}_n \models \mathrm{Accept}[H, c].$$

The proof of the lemma is straightforward albeit technical and tedious. Since it does not affect our results we give it in the appendix.

The formalization of the concept of computation is the basis for many theorems in logic. We recall the one which is the most relevant for results presented in this chapter proven by Trachtenbrot in [51].

Theorem 4.2 ([51]) *The set of sentences true in all finite models in a vocabulary containing at least one binary predicate is co*RE*–complete.*

4.1.2 Describing computations with oracle

In formalizing the concept of a computation of an oracle Turing machine, $H^?$ ('?' stands for an oracle set which should be specified before the computation starts), one should add to the description of a configuration C_i the content of the oracle tape in the i–th step of the computation. This can be carried out in a straightforward way. Then the string $H\#\#C_0\#C_1\#\ldots\#C_K\#$ encodes the computation of H^A provided that it encodes the consecutive states of the computation and each oracle answer agrees with the set A.

In finite models, we represent the oracle set by an extension of an additional predicate or an extension of a formula. The problem which we encounter with this approach is that the oracle set can change from one finite model to the other one. We briefly describe a possible solution for this problem.

We want to describe in finite models the computation of a machine H^A, where A is an oracle set. Thus, in each finite model $\mathcal{N}_n$ we need one additional relation A_n (which can also be an extension of an arithmetical formula). The most natural condition we may put on sets A_n is that, for each n, $A_n = A \cap \{0,\ldots,n\}$. However, we will need a weaker condition.

Definition 4.3 *Let $R \subseteq \omega^r$. We say that the family of relations $\{R_n\}_{n\in\omega}$, such that $R_n \subseteq \{0,\ldots,n\}^r$,* approximates *$R$* in sufficiently large finite models*, or* sl–approximates*, if for each m there is a K such that whenever $k \geq K$ then R_k agrees with R on the set $\{0,\ldots,m\}$.*

Lemma 4.4 *Let A be an oracle set and let $\{A_n\}_{n\in\omega}$ be a family of finite relations which* sl*–approximates A. Then for each r there is an arithmetical formula* $\mathrm{OComp}(x,y,P)$ *such that for each Turing machine $H^?$ and for each c and $\bar{w} = w_1,\ldots,w_r$ there is N such that for all $n \geq N$ the following holds*

$$c \text{ is a } H^A\text{–computation with an input } \bar{w} \iff$$

$$(\mathcal{N}_n, A_n) \models \mathrm{OComp}[H^?, \mathrm{code}(\bar{w}), c, P],$$

where $(\mathcal{N}_n, A_n)$ is the n–th model from $\mathrm{FM}(\mathcal{N})$ *with additional set A_n interpreting P. In other words, if $n \geq N$ we can correctly represent the computation c in a finite model $\mathcal{N}_n$.*

Moreover, there is a formula $\mathrm{Accept}(x,y)$ *which expresses that y is an accepting computation of x.*

The second paragraph of the lemma follows from the fact that for detecting an accepting computation we only need to check the state of the machine at the end of the computation. Let us observe that we cannot demand, like

in lemma 4.1, that a minimal N equals c. It is caused by the fact that even if the model is big enough to include the code for the computation c the formula should also verify that the oracle answers agree with the set A. Therefore, N from the lemma should be chosen in such a way that for all $n \geq N$, A_n agrees with A on the set of words queried by H^A during the computation c.

4.2 Representing arbitrary notions in finite models

In this section we present the main ideas of Marcin Mostowski presented in [31] and [32]. He considered there the problem of representing infinite relations within the family FM($\mathcal{N}$). The question was motivated by an attempt to transfer some tools developed for infinite models into finite models theory. The goal was in particular to compare the semantical power of logics by means of truth definitions. As far as this last problem is concerned the reader can also consult the paper by Kołodziejczyk [22].

4.2.1 FM–representability

Definition 4.5 *Let $\mathcal{K} = \{\mathcal{K}_i\}_{i\in\omega}$ be a family of finite models in the same vocabulary such that $|\mathcal{K}_i| = \{0, \ldots, k_i\}$, for a monotone, unbounded sequence $\{k_i\}_{i\in\omega}$. We call $\mathcal{K}$ a good family of finite models.*

A formula $\varphi(x_1, \ldots, x_n)$ is satisfied by $a_1, \ldots, a_n$ in all sufficiently large finite models from $\mathcal{K}$, (or in almost all finite models from $\mathcal{K}$), $\mathcal{K} \models_{\mathrm{sl}} \varphi[a_1, \ldots, a_n]$, if

$$\exists N \forall \mathcal{A} \in \mathcal{K}(card(\mathcal{A}) \geq N \Rightarrow \mathcal{A} \models \varphi[a_1, \ldots, a_n]).$$

If the family $\mathcal{K}$ is clear from the context we write $\models_{\mathrm{sl}} \varphi[a_1, \ldots, a_n]$.

From now on, whenever we write $\mathcal{K}$ we assume that it is a good family of finite models. In most cases a family $\mathcal{K}$, from the above definitions, will be of the form FM($\mathcal{A}$).

Definition 4.6 *Let $\mathcal{K}$ be a good family of finite models and let F be a set of sentences in the vocabulary of $\mathcal{K}$.*

By $\mathrm{sl}_F(\mathcal{K})$ we denote the set of sentences from F true in all sufficiently large models from $\mathcal{K}$,

$$\mathrm{sl}_F(\mathcal{K}) = \{\varphi \in F : \mathcal{K} \models_{\mathrm{sl}} \varphi\}.$$

When F is the set of all sentences in a given vocabulary the subscript F will be omitted.

Now we state some basic properties of $\mathrm{Th}(\mathcal{K})$ and $\mathrm{sl}(\mathcal{K})$, which were observed in [31] and [32].

Let T be a set of sentences. By $\mathrm{Cn}(T)$ we denote the set of all first order consequences of T. T is closed on Cn if $\mathrm{Cn}(T) = T$. We have the following

Proposition 4.7 ([31]) *For each good family of finite models $\mathcal{K}$,* $\mathrm{Th}(\mathcal{K})$ *and* $\mathrm{sl}(\mathcal{K})$ *are consistent, closed on* Cn.

Proof. The statement is obvious for $\mathrm{Th}(\mathcal{K})$ so we prove only the case of $\mathrm{sl}(\mathcal{K})$.

To prove the consistency of $\mathrm{sl}(\mathcal{K})$, it suffices, by the compactness theorem, to prove that for every finite $F \subseteq \mathrm{sl}(\mathcal{K})$, F is consistent. However, if $F = \{\varphi_1, \ldots, \varphi_n\}$ then let N_i be such that for each $r \geq N_i$, $\mathcal{K}_r \models \varphi_i$. Such N_i exists since $\varphi_i \in \mathrm{sl}(\mathcal{K})$. Now if $N = \max\{N_i : i \leq n\}$ then for each $r \geq N$, $\mathcal{K}_r \models F$. Thus, F is consistent.

Next, if $\psi \in \mathrm{Cn}(\mathrm{sl}(\mathcal{K}))$, then there is a finite $F = \{\varphi_1, \ldots, \varphi_n\} \subseteq \mathrm{sl}(\mathcal{K})$ such that ψ follows from F. Now if N is as in the first part of the proof then for each $r \geq N$, $\mathcal{K}_r \models \psi$. Hence, $\psi \in \mathrm{sl}(\mathcal{K})$. It follows that $\mathrm{Cn}(\mathrm{sl}(\mathcal{K})) = \mathrm{sl}(\mathcal{K})$. □

We can reformulate the last fact in the following statement.

Fact 4.8 *Let $\mathcal{K}$ be a good family of finite models. For each sentence φ the following are equivalent:*

(i) φ is consistent with $\mathrm{sl}(\mathcal{K})$,

(ii) $\mathcal{K} \not\models_{\mathrm{sl}} \neg\varphi$,

(iii) for each N there is a $r \geq N$ such that $\mathcal{K}_r \models \varphi$.

Proof. The equivalence of last two points follows easily from the definition of $\models_{\mathrm{sl}}$. The equivalence of the first point with the second one follows from the fact that $\mathrm{sl}(\mathcal{K})$ is closed on the consequence operation. □

One of the motivations behind the idea of introducing the theory of sufficiently large finite models in M. Mostowski [31] was that it allows to describe infinite relations within the family of finite models. We present a definition given by M. Mostowski in [31] which formalizes a way in which one can think about infinity in finite models from a given family $\mathcal{K}$.

Definition 4.9 ([31]) *Let $\mathcal{K} = \{\mathcal{K}_i\}_{i\in\omega}$ be a good family of finite models. A formula $\varphi(x_1, \ldots, x_r)$* FM*–represents in $\mathcal{K}$ a relation $R \subseteq \omega^r$ if for all $a_1, \ldots, a_r \in \omega$*

$$(a_1, \ldots, a_r) \in R \iff \mathcal{K} \models_{\mathrm{sl}} \varphi[a_1, \ldots, a_r]$$

and

$$(a_1, \ldots, a_r) \notin R \iff \mathcal{K} \models_{\mathrm{sl}} \neg\varphi[a_1, \ldots, a_r].$$

A relation $R \subseteq \omega^r$ is FM*–representable in $\mathcal{K}$ if there is a formula $\varphi(x_1, \ldots, x_r)$ which* FM*–represents R in $\mathcal{K}$.*

In order to make the concept of FM–representability more flexible to work with, we recall some modifications or equivalent reformulations of the original definition given in [31] and [32]. Firstly, let us observe that we can weaken the equivalences in the last definition to implications.

Proposition 4.10 *Let $\varphi(x_1, \ldots, x_r)$ be a formula in the vocabulary of $\mathcal{K}$. Then φ* FM*–represents $R \subseteq \omega^r$ in $\mathcal{K}$ if and only if for all $a_1, \ldots, a_r \in \omega$,*

$$\text{if } (a_1, \ldots, a_r) \in R \text{ then } \mathcal{K} \models_{\mathrm{sl}} \varphi[a_1, \ldots, a_r]$$

and

$$\text{if } (a_1, \ldots, a_r) \notin R \text{ then } \mathcal{K} \models_{\mathrm{sl}} \neg\varphi[a_1, \ldots, a_r].$$

The proposition follows from the fact that for $a_1, \ldots, a_r \in \omega$ exactly one of the following holds: $(a_1, \ldots, a_r) \in R$ or $(a_1, \ldots, a_r) \notin R$.

Of course it is not the case that each formula FM–represents some relation. E.g. the formula $\exists z(z + z \neq \mathrm{MAX} \wedge z + z + 1 = \mathrm{MAX}) \wedge x = x$ is true about all elements x in models of even cardinality and is false about all elements x in models of odd cardinality. Therefore, it does not FM–represent anything. Later, we will estimate the complexity of deciding whether a given formula FM–represents some relation. Here, we define a notion from [31] which describes a condition under which a given formula FM–represents something.

Definition 4.11 *A formula $\varphi(x_1, \ldots, x_k)$ is determined in $\mathcal{K}$ if for each $a_1, \ldots, a_k \in \omega$, either $\mathcal{K} \models_{\mathrm{sl}} \varphi[a_1, \ldots, a_k]$ or $\mathcal{K} \models_{\mathrm{sl}} \neg\varphi[a_1, \ldots, a_k]$.*

The next fact follows directly from the definition of FM–representability.

Fact 4.12 *A formula $\varphi(x_1, \ldots, x_k)$* FM*–represents in $\mathcal{K}$ some relation if and only if $\varphi(x_1, \ldots, x_k)$ is determined in $\mathcal{K}$.*

If we know that a formula is determined then we can weaken the condition for FM–representability to only one equivalence. Indeed, it is straightforward to prove the following.

Proposition 4.13 *Let $\varphi(x_1, \ldots, x_r)$ be determined in $\mathcal{K}$. Then φ* FM–*represents $R \subseteq \omega^r$ in $\mathcal{K}$ if and only if for all $a_1, \ldots, a_r \in \omega$,*

$$(a_1, \ldots, a_r) \in R \iff \mathcal{K} \models_{\mathrm{sl}} \varphi[a_1, \ldots, a_r].$$

Now we will show an upper bound on the complexity of relations which can be FM–represented.

Definition 4.14 *Let $\mathcal{A} = (\omega, \bar{R})$. We say that $\mathcal{A}$ is recursive if each relation and operation in $\mathcal{A}$ has a recursive graph.*

Let us observe, that even if $\mathcal{A}$ is recursive the theory of $\mathcal{A}$ may be undecidable. E.g. $\mathcal{N}$ is a recursive model but the problem whether a given sentence holds in $\mathcal{N}$ is undecidable. Nevertheless, it is always the case that if $\mathcal{A}$ is recursive then for each finite model $\mathcal{A}_n \in \mathrm{FM}(\mathcal{A})$ the theory of $\mathcal{A}_n$ is decidable uniformly in n. It means that there is an algorithm which decides on an input (n, φ) whether $\mathcal{A}_n \models \varphi$.

Now we estimate an upper bound on the relations FM–representable in $\mathrm{FM}(\mathcal{A})$ for a recursive model $\mathcal{A}$.

Proposition 4.15 ([31]) *Let $\mathcal{A} = (\omega, \bar{R})$ be a recursive model. Then each* FM*–representable relation in* $\mathrm{FM}(\mathcal{A})$ *is Δ_2 in the arithmetical hierarchy.*

Proof. Let $R \subseteq \omega^r$ be FM–representable in $\mathrm{FM}(\mathcal{A})$. Then there is a formula $\varphi(x_1, \ldots, x_r)$ such that for each tuple $a_1, \ldots, a_r \in \omega$,

$$(a_1, \ldots, a_r) \in R \iff \mathrm{FM}(\mathcal{A}) \models_{\mathrm{sl}} \varphi[a_1, \ldots, a_r].$$

If we rewrite the right side of this equivalence we get a Σ_2–formula

$$\exists N \, \forall n \geq N \, \mathcal{A}_n \models \varphi[a_1, \ldots, a_r].$$

However, the same procedure can be repeated for the complement of R and $\neg\varphi$. Since both R and $\bar{R}$ have Σ_2 definitions, R is a Δ_2 relation. $\square$

In what follows we present the theorem from M. Mostowski [31] which states that Δ_2 is exactly the family of relations which are FM–representable in $\mathrm{FM}(\mathcal{N})$. Before we state the main theorem we need the following.

Lemma 4.16 *Let $R \subseteq \omega^r$. If R is recursively enumerable (*RE*) then R is* FM*–representable in* FM($\mathcal{N}$).

Proof. Let $R \subseteq \omega^r$ be RE and let H be a machine which accepts exactly tuples from R. Then let us consider a formula $\varphi(x_1, \ldots, x_r) :=$

$$\exists c\,(\mathrm{Comp}(H, \mathrm{code}(x_1, \ldots, x_r), c) \wedge \mathrm{Accept}(H, c)),$$

where Comp and Accept are formulas from lemma 4.1. We claim that φ FM–represents relation R. By proposition 4.10 we need to prove that for all $a_1, \ldots, a_r \in \omega$,

$$\text{if } (a_1, \ldots, a_r) \in R \text{ then } \mathrm{FM}(\mathcal{N}) \models_{\mathrm{sl}} \varphi[a_1, \ldots, a_r]$$

and

$$\text{if } (a_1, \ldots, a_r) \notin R \text{ then } \mathrm{FM}(\mathcal{N}) \models_{\mathrm{sl}} \neg\varphi[a_1, \ldots, a_r].$$

Let us observe that $(a_1, \ldots, a_r) \in R$ if and only if there exists an accepting computation c of H on $a_1, \ldots, a_r$. Thus, in each model $\mathcal{N}_n$, for $n \geq c$, φ is satisfied by $a_1, \ldots, a_r$.

If $(a_1, \ldots, a_r) \notin R$ then there is no accepting computation of H with the input $a_1, \ldots, a_r$. Thus, by properties of Comp stated in lemma 4.1, the formula φ is not satisfied by $a_1, \ldots, a_r$ in any model from FM($\mathcal{N}$). □

Now we are ready to state the theorem which describes exactly the family of FM–representable relations. The following theorem has been proven by M. Mostowski in [31].

Theorem 4.17 ([31]) *Let $R \subseteq \omega^r$. R is* FM*–representable in* FM($\mathcal{N}$) *if and only if R is Δ_2 in the arithmetical hierarchy.*

Proof. By proposition 4.15 we need only to prove that if $R \subseteq \omega^r$ is Δ_2 then it is FM–representable. Firstly, let us recall that, by proposition 2.10, a relation R is Δ_2 if and only if it is decidable by a Turing machine with a recursively enumerable oracle. Thus, let us assume that there exists a Turing machine $H^?$ and a recursively enumerable oracle A such that $L(H^A) = R$. By lemma 4.16 there is a formula $\varphi(x)$ such that it FM–represents the oracle set A. Then let $\psi(x_1, \ldots, x_r)$ be a formula

$$\exists c\,(\mathrm{OComp}(H, \mathrm{code}(x_1, \ldots, x_r), c, \varphi) \wedge \mathrm{Accept}(H, c)),$$

where $\mathrm{OComp}(x, y, z, \varphi)$ is the formula from lemma 4.4 where in place of P we substituted φ (renaming, if necessary, bound variables of OComp). Now we show that ψ FM–represents R.

Let $a_1, \ldots, a_r \in \omega$. Since H^A decides R, there is a H^A–computation c on the input $a_1, \ldots, a_r$. Thus,

$$(a_1, \ldots, a_r) \in R \text{ if and only if } c \text{ is an accepting computation}$$

and

$$(a_1, \ldots, a_r) \notin R \text{ if and only if } c \text{ is a rejecting computation.}$$

The family $\{\varphi^{\mathcal{N}_i,x}\}_{i\in\omega}$ sl–approximates A. Thus, by lemma 4.4, there is N such that for all $n \geq N$ and all d,

$$d \text{ is a } H^A\text{–computation on } a_1, \ldots, a_r \iff$$

$$\mathcal{N}_n \models \mathrm{OComp}(x, y, z, \varphi)[H, \mathrm{code}(a_1, \ldots, a_r), d],$$

Then for all $n \geq N$,

$$\mathcal{N}_n \models \psi[H, \mathrm{code}(a_1, \ldots, a_r)] \iff$$

$$\text{there is an accepting computation of } H^A \text{ on } a_1, \ldots, a_r$$

and

$$\mathcal{N}_n \models \neg\psi[H, \mathrm{code}(a_1, \ldots, a_r)] \iff$$

$$\text{there is a rejecting computation of } H^A \text{ on } a_1, \ldots, a_r.$$

Thus, ψ FM–represents R in $\mathrm{FM}(\mathcal{N})$. □

4.3 Characterization of $\mathrm{sl}(\mathrm{FM}(\mathcal{A}))$ in terms of ultraproducts

In this section we investigate the relations between theories of sufficiently large finite models and the ultraproduct construction. We show that each complete extension of the theory $\mathrm{sl}(\mathrm{FM}(\mathcal{A}))$ is the theory of a model being an ultraproduct of the family $\mathrm{FM}(\mathcal{A})$. Then at the and of this section, we obtain additionally that there is a continuum of complete extensions of $\mathrm{sl}(\mathrm{FM}(\mathcal{N}))$.

We need some definitions and facts from algebra which we briefly recall. For a complete presentation of these notions see e.g. [2].

Definition 4.18 *Let $\mathcal{F} = \{F_i\}_{i\in\omega}$ be a family of subsets of ω. We say that $\mathcal{F}$ has the finite intersection property (*fip*) if for each finite subset of $\mathcal{F}$, $\{F_1, \ldots, F_k\}$, the set $\bigcap_{i\leq k} F_i$ is not empty.*

Definition 4.19 *A nonempty family $\mathcal{F}$ of subsets of ω is a filter if*

- *for each $x, y \in \mathcal{F}$, $x \cap y \in \mathcal{F}$,*
- *for each $x \in \mathcal{F}$ and $y \subseteq \omega$, if $x \subseteq y$ then $y \in \mathcal{F}$,*
- *$\emptyset \notin \mathcal{F}$.*

A filter $\mathcal{F}$ is an ultrafilter if for each $x \subseteq \omega$, either $x \in \mathcal{F}$ or $\omega \setminus x \in \mathcal{F}$. An ultrafilter is nonprincipal if it does not contain any finite set. It can be shown (assuming the axiom of choice) that there is a continuum of nonprincipial ultrafilters.

We use the following important property of families with fip.

Fact 4.20 *Let $\mathcal{F}$ be a family with* fip. *Then there exists an ultrafilter containing $\mathcal{F}$.*

Definition 4.21 *Let $\mathcal{U}$ be an ultrafilter and let*

$$\Pi_{i\in\omega}\mathcal{A}_i = \{f\colon \omega \longrightarrow \bigcup_{i\in\omega} \mathcal{A}_i : \forall i\, f(i) \in |\mathcal{A}_i|\}.$$

Let $\sim$ be an equivalence relation on $\Pi_{i\in\omega}\mathcal{A}_i$ defined as

$$f \sim g \iff \{i : f(i) = g(i)\} \in \mathcal{U}.$$

An ultraproduct of $\{\mathcal{A}_i\}_{i\in\omega}$ and $\mathcal{U}$ *is the model $\Pi_{i\in\omega}\mathcal{A}_{i/\mathcal{U}}$ with the universe*

$$|\Pi_{i\in\omega}\mathcal{A}_{i/\mathcal{U}}| = \{[f]_\sim : f \in \Pi_{i\in\omega}\mathcal{A}_i\}$$

and in the vocabulary of family $\{\mathcal{A}_i\}_{i\in\omega}$. For a predicate R, a relation $R^{\Pi_{i\in\omega}\mathcal{A}_{i/\mathcal{U}}}$ is defined as

$$R^{\Pi_{i\in\omega}\mathcal{A}_{i/\mathcal{U}}}([f_i], \ldots, [f_r]) \iff \{i : R^{\mathcal{A}_i}(f_1(i), \ldots, f_r(i))\} \in \mathcal{U},$$

where $f_1, \ldots, f_r \in \Pi_{i\in\omega}\mathcal{A}_i$ and $R^{\mathcal{A}_i}$ is the corresponding relation from $\mathcal{A}_i$. A similar convention also applies in the case of function symbols and constants.

It follows from the properties of an ultrafilter that $\Pi_{i\in\omega}\mathcal{A}_{i/\mathcal{U}}$ is a well defined model.

We characterize the theory of $\Pi_{i\in\omega}\mathcal{A}_{i/\mathcal{U}}$ in terms of models $\mathcal{A}_i$ and an ultrafilter $\mathcal{U}$ in the following theorem.

Theorem 4.22 (Łoś theorem) *For all $\varphi(x_1, \ldots, x_k)$ and $f_1, \ldots, f_k \in \Pi_{i\in\omega}\mathcal{A}_i$ it holds that*

$$\Pi_{i\in\omega}\mathcal{A}_{i/\mathcal{U}} \models \varphi[[f_1], \ldots, [f_k]] \iff \{i : \mathcal{A}_i \models \varphi[f_1(i), \ldots, f_k(i)]\} \in \mathcal{U}.$$

The first step towards establishing a relation between $\mathrm{sl}(\mathrm{FM}(\mathcal{A}))$ and models constructed as ultraproducts is the following fact.

Fact 4.23 *For each* $\mathrm{FM}(\mathcal{A})$ *and for each nonpricipial ultrafilter* $\mathcal{U}$ *on* ω*,*

$$\mathrm{sl}(\mathrm{FM}(\mathcal{A})) \subseteq \mathrm{Th}(\Pi_{n\in\omega}\mathcal{A}_{n/\mathcal{U}}).$$

Proof. It suffices to note that each nonprincipial ultrafilter contains all sets $\{k \in \omega : k \geq N\}$, where $N \in \omega$ is fixed. Therefore, if $\varphi \in \mathrm{sl}(\mathrm{FM}(\mathcal{A}))$ then the set of indexes of models in which φ is true belongs to $\mathcal{U}$. □

One can obtain even more.

Proposition 4.24 *Let T be a complete, consistent extension of* $\mathrm{sl}(\mathrm{FM}(\mathcal{A}))$*. Then there is an ultrafilter $\mathcal{U} \subseteq \mathcal{P}(\omega)$ such that*

$$\Pi_{n\in\omega}\mathcal{A}_{n/\mathcal{U}} \models T.$$

Proof. Let $T = \{\varphi_0, \varphi_1, \varphi_2, \ldots\}$ and let $\psi_i = \bigwedge_{j\leq i}\varphi_j$, for $i \in \omega$. Consider a family $\{F_i\}_{i\in\omega}$ such that $F_i = \{k \in \omega : \mathcal{A}_k \models \psi_i\}$. We have that $\{F_i\}_{i\in\omega}$ is a family of infinite, descending subsets of ω, $F_0 \supseteq F_1 \supseteq F_2 \supseteq \ldots$ Since each ψ_i is consistent with $\mathrm{sl}(\mathrm{FM}(\mathcal{A}))$, it follows that each F_i is infinite. Moreover, for $i < j$, $\models (\psi_j \Rightarrow \psi_i)$, which implies $F_j \subseteq F_i$. It follows that $\{F_i\}_{i\in\omega}$ has the finite intersection property.

Now let $\mathcal{U}$ be a nonprincipial ultrafilter containing $\mathcal{F}$ and let $\mathcal{B} = \Pi_{n\in\omega}\mathcal{A}_{n/\mathcal{U}}$. We claim that $\mathcal{B} \models T$.

Since T is complete it suffices to prove that if $\varphi \in T$ then $\mathcal{B} \models \varphi$. Let $\varphi \in T$. Then $\varphi = \varphi_{i_0}$ for some i_0 and $F_{i_0} \subseteq \{k : \mathcal{A}_k \models \varphi\} \in \mathcal{U}$. It follows that $\mathcal{B} \models \varphi$. □

Now we show that there is a formula $\varphi(x)$ such that it can FM–represent any subset of ω in some complete extension of $\mathrm{sl}(\mathrm{FM}(\mathcal{N}))$. We can think about φ as a formula which is undetermined for any $a \in \omega$. Firstly, we need the following definition.

Definition 4.25 *The pairing function, $\langle\rangle_2 \colon \omega^2 \longrightarrow \omega$, is defined as*

$$\langle x, y\rangle_2 = \frac{(x+y)(x+y+1)}{2} + y.$$

By induction on $d \geq 2$, we define a d–ary function

$$\langle\rangle_d \colon \omega^d \longrightarrow \omega$$

which enumerates the set of d–tuples of integers.

If $\langle\rangle_d \colon \omega^d \longrightarrow \omega$ is defined then $\langle\rangle_{d+1} \colon \omega^{d+1} \longrightarrow \omega$ is defined as

$$\langle x_1, \ldots, x_{d+1}\rangle_{d+1} = \langle x_1, \langle x_2, \ldots, x_{d+1}\rangle_d\rangle_2.$$

Usually the index d will be omitted.

For each $d \geq 2$, $\langle\rangle_d \colon \omega^d \longrightarrow \omega$ is a bijection. Thus, we can think about $\langle\rangle_d$ as an enumeration od d-tuples of integers. E.g. $\langle\rangle_2$ enumerates pairs in the following order:

$$(0,0), (0,1), (1,0), (0,2), (1,1), (2,0), (0,3), (1,2), (2,1), (3,0), (0,4), \ldots$$

Let us observe that for each d the graph of the function $\langle\rangle_d$ is Δ_0 definable. It follows that there is a formula $\varphi_{\langle\rangle_d}$ such that in each finite model from $\mathrm{FM}(\mathcal{N})$ it defines a restriction of the graph of $\langle\rangle_d$ to the universe of this model.

Theorem 4.26 *There exists $\varphi(x)$ such that for each $A \subseteq \omega$ there is an ulrafilter $\mathcal{U}$ such that*

$$A = \{a \in \omega : \Pi_{n\in\omega}\mathcal{N}_{n/\mathcal{U}} \models \varphi[\mathbf{a}]\},$$

where $\mathbf{a}$ is defined as an equivalence class of the function

$$f_a(i) = \begin{cases} 0 & \text{if } i < a, \\ a & \text{otherwise.} \end{cases}$$

Proof. To start with, we define the family of sets $\{X_i\}_{i\in\omega}$ such that

- $X_i \subseteq \omega$,
- for each sequence $n_1, \ldots, n_{k+m}$ of pairwise different integers

$$\bigcap_{1\leq i\leq k} X_{n_i} \cap \bigcap_{1\leq i\leq m} (\omega \setminus X_{n_{k+i}})$$

  is infinite.

We take

$$X_i = \{x : \exists z_1 \leq x \exists z_2 \leq x (x = \langle z_1 p_i^{p_i}, z_2 \rangle)\},$$

where p_k is the k-th prime number. To see that $\{X_i\}_{i\in\omega}$ has the desired properties let $n_1, \ldots, n_{k+m}$ be a sequence of pairwise different integers. Then $\bigcap_{1\leq i\leq k} X_{n_i} \cap \bigcap_{1\leq i\leq m} (\omega \setminus X_{n_{k+i}})$ contains each number $\langle \Pi_{i\leq k} p_{n_i}^{p_{n_i}}, y\rangle$. This property of the family $\{X_i\}_{i\in\omega}$ guarantees that for each $\varepsilon\colon \omega \longrightarrow \{0,1\}$ the family $\{X_i^{\varepsilon(i)}\}_{i\in\omega}$, where

$$X_i^a = \begin{cases} X_i & \text{if } a = 1, \\ \omega \setminus X_i & \text{if } a = 0, \end{cases}$$

has the finite intersection property. Consequently, there is an ultrafilter in which this family is contained.

Now we construct the formula $\varphi(x)$. By $pr(x, y)$ we denote the functional relation $y = p_x^{p_x}$. pr is Δ_0 definable so its graph is uniformly definable in each finite model $\mathcal{N}_i$. By the time this thesis has been finished it is still unknown whether the relation "y is the x-th prime" is Δ_0. However, we can Δ_0 define p_x in the formula $pr(x, y)$ using $y = p_x^{p_x}$ as a bound for quantifiers.

Let $\widetilde{\varphi}(x, y)$ be the following formula

$$\exists z \exists z_1 \exists z_2 (pr(x + 1, z) \wedge y = \langle z_1 z, z_2 \rangle).$$

For each finite model $\mathcal{N}_k$,

$$\widetilde{\varphi}^{\mathcal{N}_k, x, y} = \{(a, b) : b \in X_a\} \cap |\mathcal{N}_k|.$$

As $\varphi(x)$ we take $\widetilde{\varphi}(x, \mathrm{MAX})$. Then for $a \in \omega$,

$$X_a = \{k \in \omega : \mathcal{N}_k \models \varphi[a]\}.$$

Now we show that φ satisfies the assertion of the theorem.

Let $A \subseteq \omega$ and let $\xi_A\colon \omega \longrightarrow \{0,1\}$ be the characteristic function of A,

$$\xi_A(i) = \begin{cases} 1 & \text{if } i \in A, \\ 0 & \text{otherwise.} \end{cases}$$

Then there exists a nonprincipial ultrafilter $\mathcal{U}$ containing the family $\{X_i^{\xi_A(i)}\}_{i\in\omega}$. For proving the theorem it suffices to observe that, for each $a \in \omega$, we have the following equivalence:

$$\begin{aligned} a \in A &\iff X_a^{\xi_A(a)} \in \mathcal{U} \\ &\iff \{k : \mathcal{A}_k \models \varphi[a]\} \in \mathcal{U} \\ &\iff \Pi_{i\in\omega}\mathcal{N}_{i/\mathcal{U}} \models \varphi[[f_a]]. \end{aligned}$$

□

Theorem 4.26 allows us also to show that there are as many complete extensions of sl(FM($\mathcal{N}$)) as it is possible.

Theorem 4.27 *There is a continuum complete, consistent extensions of* sl(FM($\mathcal{N}$)).

Proof. Let φ be as in theorem 4.26. Then for each $X \subseteq \omega$ there is an ultrafilter $\mathcal{U}_X$ such that φ defines X in $\Pi_{n\in\omega}\mathcal{N}_{n/\mathcal{U}_X}$. Of course, for different subsets X and Y theories of models $\mathcal{A}_X = \Pi_{n\in\omega}\mathcal{N}_{n/\mathcal{U}_X}$ and $\mathcal{A}_Y = \Pi_{n\in\omega}\mathcal{N}_{n/\mathcal{U}_Y}$ are different because φ defines X in $\mathcal{A}_X$ and Y in $\mathcal{A}_Y$. Since there is a continuum different subsets of ω, the theorem is proven. □

Chapter 5

Other methods of representing concepts

In this chapter we consider various weakenings of the concept of FM–representability. They allow to estimate the complexity of some families of formulas defined by their semantical properties in finite models. They also show how we can extend the family of relations representable in finite models if we weaken the constrains put on the way of representing them. Therefore, in some sense, we are able to describe in finite models not only Δ_2 relations but also relations which are Σ_2 or Π_3 in the arithmetical hierarchy.

The results presented in this section are published in M. Mostowski and Zdanowski [35].

5.1 Weak FM–representability

The first natural weakening of the concept of FM–representability is as follows.

Definition 5.1 *Let $\mathcal{K} = \{\mathcal{K}_i\}_{i\in\omega}$ be a family of finite models in the same vocabulary such that $|\mathcal{K}_i| = \{0, \ldots, i\}$.*

A formula $\varphi(x_1, \ldots, x_r)$ weakly FM*–represents in $\mathcal{K}$ a relation $R \subseteq \omega^r$ if for all $a_1, \ldots, a_r \in \omega$*

$$(a_1, \ldots, a_r) \in R \iff \mathcal{K} \models_{\mathrm{sl}} \varphi[a_1, \ldots, a_r].$$

A relation $R \subseteq \omega^r$ is weakly FM*–representable in $\mathcal{K}$ if there is a formula $\varphi(x_1, \ldots, x_r)$ which weakly* FM*–represents R in $\mathcal{K}$. We write* WFM($\mathcal{K}$) *for the family of relations which are weakly* FM*–representable in $\mathcal{K}$. In the most interesting case when $\mathcal{K} =$* FM($\mathcal{N}$) *we simply write* WFM*.*

It follows directly from definition 5.1 that if a relation is in WFM then it admits a Σ_2 definition. Below, we show that the converse of this fact also holds. In the first step, we write a formula which weakly FM–represents in FM($\mathcal{N}$) a Σ_2–complete set. In the second step, we show that the WFM family is closed on many–one Turing reducibilities.

It was stated in subsection 2.3.2 that the set of Turing machines which have a finite domain is Σ_2–complete.

Lemma 5.2 Fin *is weakly* FM*–representable.*

Proof. The formula $\varphi(x)$ which weakly FM–represents Fin can be taken as

$$\neg\exists y \ \mathrm{Comp}(x, y, \mathrm{MAX}),$$

where Comp is the formula from lemma 4.1. φ says that MAX is not a computation of a machine x. We use the properties of Comp stated in lemma 4.1 to show that the above formula weakly FM–represents Fin.

If $H \in$ Fin then there is a bound N on the size of a computation of H. Therefore, in each model $\mathcal{N}_n$, for $n > N$, MAX is not a code of a computation of H and $\mathcal{N}_n \models \varphi[H]$. On the other hand, if $H \notin$ Fin then there is a sequence $\{c_i\}_{i\in\omega}$ of computations of H such that $c_i < c_{i+1}$. Thus, for each $i \in \omega$, $\mathcal{N}_{c_i} \models \neg\varphi[H]$ and FM($\mathcal{N}$) $\not\models_{\mathrm{sl}} \varphi[H]$. $\square$

Now we can easily characterize the complexity of deciding whether a sentence φ holds in almost all finite models FM($\mathcal{N}$). The following theorem has been proven by M. Mostowski and Zdanowski in [35].

Theorem 5.3 ([35]) $sl(\mathrm{FM}(\mathcal{N}))$ *is* Σ_2^0*–complete.*

Proof. From the definition of $\models_{\mathrm{sl}}$ we have that $sl(\mathrm{FM}(\mathcal{N}))$ is Σ_2^0. To show that it is Σ_2^0–complete let $\varphi(x)$ be a formula which weakly FM–represents the Σ_2^0–complete set Fin. Then for each $H \in \omega$,

$$H \in \mathrm{Fin} \iff \varphi(H) \in sl(\mathrm{FM}(\mathcal{N})).$$

Hence, the mapping $H \mapsto \varphi(H)$ is a many–one reduction of Fin to $sl(\mathrm{FM}(\mathcal{N}))$. This proves that $sl(\mathrm{FM}(\mathcal{N}))$ is a Σ_2^0–complete set. $\square$

Let us observe that the above theorem can be used to prove the following variation on Trachtenbrot's theorem.[1]

[1]The theorem below is not a reformulation of Trachtenbrot's theorem. However, it has a smimilar aim of describing the complexity of some sets of first order formulas defined semantically in finite models.

Theorem 5.4 *The set of first order sentences which are true in all but finitely many finite models is Σ^0_2–complete.*

Proof. The set of first order sentences which are satisfied in almost all finite models is Σ^0_2. The Σ^0_2 definition of this set states that, for a given sentence γ, there is N such that in all finite models of cardinalities greater than N, γ is satisfied. So it suffices to prove that it is Σ^0_2–complete.

Let Ψ be a sentence which characterizes up to isomorphism finite models from $\mathrm{FM}(\mathcal{N})$ (see proposition 3.11). Then for each finite model M,

$$M \models \Psi \iff \exists \mathcal{A} \in \mathrm{FM}(\mathcal{N})\, M \cong \mathcal{A}.$$

Let $\varphi(x)$ be a formula which weakly FM–represents Fin. Then the mapping $H \mapsto \neg\Psi \vee \varphi(H)$ is a reduction of Fin to the problem from the theorem. Indeed, for each H, the formula $\neg\Psi \vee \varphi(H)$ is true in all models which do not belong to $\mathrm{FM}(\mathcal{N})$. Therefore, it is true in almost all finite models exactly when it is true in almost all finite models from $\mathrm{FM}(\mathcal{N})$. Since φ weakly FM–represents Fin, the latter is equivalent to $H \in \mathrm{Fin}$. $\square$

The next lemma is of a more general interest for us. It allows to show in a uniform way that certain classes of relations representable in finite models are closed on recursion theoretic reducibilities.

Lemma 5.5 *Let $f\colon \omega^k \longrightarrow \omega^m$ be a total function in Δ^0_2. Then for each formula $\varphi(x_1, \ldots, x_m)$ there exists a formula $\psi(z_1, \ldots, z_k)$ such that for each $\bar{a} = a_1, \ldots, a_k \in \omega$,*

$$\mathrm{FM}(\mathcal{N}) \models_{\mathrm{sl}} (\psi(z_1, \ldots, z_k) \equiv \varphi(x_1, \ldots, x_m))[\bar{a}/\bar{z}, \vec{f}(\bar{a})/\bar{x}].$$

Proof. We consider only the case for $\varphi(x)$ and $f\colon \omega \longrightarrow \omega$. The general case can be obtained by considering instead of a formula $\varphi(x_1, \ldots, x_m)$ a formula

$$\varphi'(x) := \exists x_1 \ldots \exists x_m (x = \langle x_1, \ldots, x_m \rangle_m \wedge \varphi(x_1, \ldots, x_m)).$$

Let $f\colon \omega \longrightarrow \omega$ be a total Δ^0_2 function. Thus, its graph $G_f = \{(a, b) : b = f(a)\}$ is FM–representable, say, by a formula $\varphi_f(x, y)$. Then let $\gamma(x, y)$ be the following formula

$$\varphi_f(x, y) \wedge \forall y' (y' < y \Rightarrow \neg\varphi_f(x, y')).$$

We claim that for all $a, b \in \omega$,

$$\models_{\mathrm{sl}} \gamma(x, y)[a, b] \iff b = f(a). \qquad (*)$$

To see the equivalence let N be such that in all models of cardinality at least N φ_f correctly represents G_f on the set $\{0, \ldots, \max\{a, f(a)\}\}$. Then for each $n \geq N$,

$$\mathcal{N}_n \models \varphi_f[a, f(a)] \text{ and for all } c < f(a), \mathcal{N}_n \models \neg\varphi_f[a, c].$$

It follows that in each model $\mathcal{N}_n$, where $n \geq N$, $f(a)$ is the minimal element b such that $\mathcal{N}_n \models \varphi_f[a, b]$. Hence, the equivalence holds.

Then let $\psi(z)$ be

$$\exists y(\gamma(z, y) \wedge \varphi(y)).$$

For all $a \in \omega$ we have the following sequence of equivalent statements

$$\begin{aligned} \models_{\text{sl}} \psi[a] &\iff \models_{\text{sl}} \exists y(\gamma(z, y) \wedge \varphi(y))[a], \text{ and by } (*), \\ &\iff \models_{\text{sl}} \varphi(y)[f(a)]. \end{aligned}$$

□

As a consequence of the last lemma we can state the following.

Lemma 5.6 *The family* WFM *is closed on many–one Turing reducibilities.*

Proof. For simplicity we consider only the case for relations of arity one. Let $R \subseteq \omega$ be weakly FM–representable by a formula $\varphi_R(x)$ and let S be many–one reducible to R. Thus, there is a recursive function $f\colon \omega \longrightarrow \omega$ such that for all $a \in \omega$,

$$a \in S \iff f(a) \in R.$$

The graph of f is recursive, so, by lemma 5.5, we can take a formula $\varphi_S(z)$ such that for each $a \in \omega$,

$$\models_{\text{sl}} (\varphi_S(z) \equiv \varphi_R(x))[a, f(a)].$$

Then for each $a \in \omega$,

$$\begin{aligned} \models_{\text{sl}} \varphi_S[a] &\iff \models_{\text{sl}} \varphi_R[f(a)] \\ &\iff f(a) \in R \\ &\iff a \in S. \end{aligned}$$

Hence, φ_S weakly FM–represents S. □

As a direct consequence of lemmas 5.2 and 5.6 we obtain the theorem which characterizes the family of weakly representable relations in FM($\mathcal{N}$). The following theorems were proven by M. Mostowski and Zdanowski in [35].

Theorem 5.7 ([35]) *A relation $R \subseteq \omega^r$ is weakly* FM*–representable if and only if R is Σ^0_2 in the arithmetical hierarchy.*

As a consequence of the relations between sets in the arithmetical hierarchy we obtain also

Theorem 5.8 ([35]) *Let $R \subseteq \omega^r$. R and the complement of R are weakly* FM*–representable if and only if R is* FM*–representable.*

5.2 Statistical representability

In this section we consider another possible weakening of the concept of representability in finite models. The results from this section were published as a part of M. Mostowski and Zdanowski [35]. Nevertheless, it is based on the work of the author of this dissertation while the other sections are joint with M. Mostowski.

Definition 5.9 *Let $\varphi(x_1, \ldots, x_r)$ be a formula in the vocabulary of* FM$(\mathcal{A})$ *and $a_1, \ldots, a_r \in \omega$. By the n-th density of $\varphi[a_1, \ldots, a_r]$ in* FM$(\mathcal{A})$*, $\mu_n(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A}))$, we mean*

$$\mu_n(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A})) = \frac{card\{i : i < n \wedge \mathcal{A}_i \models \varphi[a_1, \ldots, a_r]\}}{n},$$

By $\mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A}))$ we denote, if it exists,

$$\mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A})) = \lim_{n \to \infty} \mu_n(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A})).$$

When it does not lead to any misunderstandings we omit the second parameter in $\mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A}))$.

Definition 5.10 *The relation $R \subseteq \omega^r$ is statistically representable in* FM$(\mathcal{A})$ *if there is a formula $\varphi(x_1, \ldots, x_r)$ with all free variables among $x_1, \ldots, x_r$ such that for $a_1, \ldots, a_r \in \omega$,*

- *there exists $\mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A}))$,*
- $(a_1, \ldots, a_r) \in R \iff \mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A})) = 1$,
- $(a_1, \ldots, a_r) \notin R \iff \mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A})) = 0$.

The family of relations which are statistically representable in FM$(\mathcal{A})$ *is denoted as* SR(FM$(\mathcal{A})$).

We say that the set $R \subseteq \omega^r$ is weakly statistically representable in $\mathrm{FM}(\mathcal{A})$ *if there is a formula $\varphi(x_1, \ldots, x_r)$ with all free variables among $x_1, \ldots, x_r$ such that for all $a_1, \ldots, a_r \in \omega$,*

- *if $(a_1, \ldots, a_r) \in R$ then $\mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A}))$ exists,*
- *$(a_1, \ldots, a_r) \in R \iff \mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A})) = 1$.*

The family of relations which are weakly statistically representable in $\mathrm{FM}(\mathcal{A})$ *is denoted by* $\mathrm{WSR}(\mathrm{FM}(\mathcal{A}))$.

When $\mathcal{A} = \mathcal{N}$ we simply write SR *and* WSR.

Lemma 5.11 *Let $\mathcal{A} = (\omega, \bar{S})$ be a recursive model and let $R \subseteq \omega^r$. If R is statistically representable in* $\mathrm{FM}(\mathcal{A})$ *then it is Δ_2^0.*

Proof. Let us assume that $R \subseteq \omega^r$ is statistically represented by $\varphi(x_1, \ldots, x_r)$. We will give a Σ_2 definition of R. For each tuple $\bar{a}$,

$$(\bar{a}) \in R \iff \exists N \forall n \geq N \mu_n(\varphi(\bar{a})) > 1/2.$$

The formula on the right side of the equivalence is Σ_2, so it remains to show that it is indeed a good description of R. If the right side of the equivalence holds than of course $\mu(\varphi(\bar{a})) \geq 1/2$. But, by the definition of statistical representability, $\mu(\varphi[\bar{a}]) \in \{0, 1\}$. So $\mu(\varphi[\bar{a}]) = 1$ and $(\bar{a}) \in R$. On the other hand, if $(\bar{a}) \in R$ then $\mu(\varphi[\bar{a}]) = 1$ and if we choose N in such a way that for all $n \geq N$,

$$|1 - \mu_n(\varphi[\bar{a}])| < 1/4$$

then the right side of the equivalence will be satisfied.

In a similar way we can Σ_2^0–define the complement of R. Hence, $R \in \Delta_2^0$. □

As a consequence of lemma 5.11 and theorem 4.17 we obtain the following.

Theorem 5.12 ([35]) *Let $R \subseteq \omega^r$. R is statistically representable in* $\mathrm{FM}(\mathcal{N})$ *if and only if R is* FM*–representable in* $\mathrm{FM}(\mathcal{N})$.

Since the family SR coincides (over $\mathrm{FM}(\mathcal{N})$) with FM–representable relations one could expect that relations in WSR are exactly those which are weakly FM–representable in $\mathrm{FM}(\mathcal{N})$. On the other hand, the quantifier prefix in the expression $\mu(\varphi) = 1$ suggests that WSR relations are exactly relations which are Π_3 in the arithmetical hierarchy. We will show below that the second guess is correct. Additionally, we obtain also that the set of sentences φ such that $\mu(\varphi, \mathrm{FM}(\mathcal{N})) = 1$ is Π_3–complete.

Lemma 5.13 *Families* SR *and* WSR *are closed on many–one Turing reducibilities.*

Proof. Let $R \subseteq \omega^r$ be in one of the families mentioned in the lemma and let $\varphi(x_1, \ldots, x_r)$ be a formula which, in a suitable way, represents R. Then let $S \subseteq \omega^s$ be reducible to R via a recursive function $f\colon \omega^s \longrightarrow \omega^r$ and let $\psi(z_1, \ldots, z_s)$ be a formula from lemma 5.5. Then for each $\bar{a} = a_1, \ldots, a_s \in \omega$,

$$\mathrm{FM}(\mathcal{N}) \models_{\mathrm{sl}} (\psi(\bar{z}) \equiv \varphi(\bar{x}))[\bar{a}/\bar{z}, f(\bar{a})/\bar{x}].$$

Thus, on all but finite number of models from $\mathrm{FM}(\mathcal{N})$, ψ with parameters $\bar{a}$ behaves as φ with parameters $f(\bar{a})$. In particular,

- $\mu(\psi[\bar{a}])$ exists if and only if $\mu(\varphi[f(\bar{a})])$ exists,
- if $\mu(\psi[\bar{a}])$ exists then $\mu(\psi[\bar{a}]) = \mu(\varphi[f(\bar{a})])$.

Since f is the reduction of S to R, it follows that S belongs to the same class of represented relations as R. $\square$

It was stated in subsection 2.3.2 that the set

$$\mathrm{CoInf} = \{H : \omega \setminus W_H \text{ is infinite}\}.$$

is Π_3–complete. Now our aim is to show that this set is weakly statistically representable.

Before we present the lemma we define some auxiliary notions. We write $\sqrt{\mathrm{MAX}} < x$ for the formula $\forall z(xx \neq z)$. We write $\mathrm{Input}(c) = n$ for $\exists H < c\, \mathrm{Comp}(H, n, c)$ and $x \in W_H$ for $\exists c\, \mathrm{Comp}(H, x, c)$.

Lemma 5.14 *The set* CoInf *is weakly statistically representable in* $\mathrm{FM}(\mathcal{N})$.

Proof. We write the formula $\varphi(z) :=$

$$\begin{aligned}\forall n \forall c[\{\sqrt{\mathrm{MAX}} < c \wedge n = \mathrm{Input}(c) \wedge \forall c_1(\sqrt{\mathrm{MAX}} < c_1 \Rightarrow n \leq \mathrm{Input}(c_1))\} \Rightarrow \\ \forall x\{([(x \notin W_z \wedge x < n) \vee x = 1] \wedge \forall y((y \notin W_z \wedge y < n) \Rightarrow y \leq x)) \Rightarrow \\ \neg(x|\mathrm{MAX})\}]\end{aligned}$$

with the property that for all $H \in \omega$,

$$H \in \mathrm{CoInf} \text{ if and only if } \mu(\varphi, H) = 1. \qquad (*)$$

The formula φ in a model on $\{0, \ldots, m-1\}$ looks for a computation c greater than $\sqrt{m-1}$ with the smallest imput n. Then it takes the greatest $x < n$

which is not an input of any H–computation in the model (or it takes 1 if there is no such an x) and forces its own density close to $1 - 1/x$. If there is no such a computation c then φ is simply true. Now we show (*).

Let us assume that W_H is coinfinite and let $\varepsilon > 1/k$ such that $k \notin W_H$. Let $N = \max\{c^2 : \text{Input}(c) \leq k\} + 1$. We show that for all $m > N$, $|1 - \mu_m(\varphi, H)| < \varepsilon$. In the model $\mathcal{N}_m$ there is no computation c such that $\sqrt{m-1} < c$ and $\text{Input}(c) < k$. Thus, φ forces its density at least to $1 - 1/k$ in models greater than N.

Now let us assume that W_H is cofinite and let $k = \max(\omega \backslash W_H)$. Let us fix an arbitrary large N and $c_0 = \max\{c : \text{Input}(c) \leq N\}$. Starting from $\mathcal{N}_{c_0+1}$ up to $\mathcal{N}_{c_0^2}$, φ forces its density to $1-1/k$. In follows that $|1-\mu_{c_0^2}(\varphi, H)| \geq 1/2k$. □

As a direct consequence of last two lemmas we obtain the following.

Theorem 5.15 ([35]) *The family of relations which are weakly statistically representable in* $\text{FM}(\mathcal{N})$ *is exactly the family of* Π_3 *relations in the arithmetical hierarchy.*

The lemma 5.14 enables us to characterize the complexities of the set of sentences which has density 1 in $\text{FM}(\mathcal{N})$.

Theorem 5.16 ([35]) *The set* $\{\varphi : \mu(\varphi, \text{FM}(\mathcal{N})) = 1\}$ *is* Π_3*–complete.*

Chapter 6

Some arithmetics of finite models

As we have already seen the properties of finite models for arithmetic differ significantly from the properties of corresponding infinite models. In this chapter we investigate relations between various finite models arithmetics. Up to now, we considered arithmetics which are equivalent (via some exact interpretation) to the domain of addition and multiplication. Now we will also consider some weaker sets of basic notions like sole multiplication, coprimality or exponentiation.

The main results of this chapter are the following. We show that $\exists^*\forall^*$ theory of multiplication in finite models is undecidable while $\exists^*$ theory of multiplication with order is decidable (for families $\exists^*\forall^*$ and $\exists^*$ see the definition on page 12). We also show that the relations which are FM–representable in $\mathrm{FM}((\omega, \times))$ are exactly the same as in $\mathrm{FM}(\mathcal{N})$. Then we show that exponentiation in finite models is strictly weaker than multiplication. In particular, the former is definable from the latter. It can be contrasted with the situation in the infinite domain where exponentiation is semantically equivalent to addition and multiplication. Then we consider relations between sets of spectra for the above arithmetics and show strict inclusions between them.

These results can be seen also as finite models analogs of investigations on decidability and definability among various sets of arithmetical relations in the infinite model. The state of the knowledge in the classical case is presented e.g. in [24].

6.1 Arithmetics with the ordering relation

In this section we consider the situation when the standard ordering is definable in a model $\mathcal{A} = (\omega, \mathcal{R})$ from which we construct the family of finite models. We show that in this case $\mathrm{FM}(\mathcal{A})$ is easily interpretable in $\mathcal{A}$. As we see in the subsequent sections if it is not the case then the situation may change drastically.

The results of this section are standard although, as far as we know, they were never presented in a complete form.

Lemma 6.1 *For every formula $\varphi(x_1, \ldots, x_n)$ in the language of $\mathrm{FM}(\mathcal{A})$ there is a formula $\varphi^*(x_1, \ldots, x_n, y)$ in the language of $(\mathcal{A}, \leq)$, where y is a new variable, such that for each $a_1, \ldots, a_k \leq n$,*

$$\mathcal{A}_n \models \varphi[a_1, \ldots, a_k] \quad \textit{if and only if} \quad (\mathcal{A}, \leq) \models \varphi^*[a_1, \ldots, a_k, n].$$

Proof. A translation procedure is defined by induction on the complexity of φ. Let y be a variable which does not occur in φ. Firstly, we replace each occurrence of MAX in φ by y. We may assume that each atomic formula which occurs in φ is of the form: $P_j(t_1, \ldots, t_r)$, $F_k(t_1, \ldots, t_m) = t_0$ or $t_0 = t_1$, where $t_0, t_1, \ldots, t_{\max\{r,m\}}$ are variables or constants.

An atomic formula $P_j(t_1, \ldots, t_r)$ is translated into itself,

$$(P_j(t_1, \ldots, t_r))^* := P_j(t_1, \ldots, t_r).$$

Next we define

$$(F_k(t_1, \ldots, t_m) = t_0)^* :=$$
$$[(F_k(t_1, \ldots, t_m) \leq y \wedge F_k(t_1, \ldots, t_m) = t_0) \vee (y \leq F_k(t_1, \ldots, t_m) \wedge t_0 = y)]$$

and

$$(t = t')^* := (t \leq y \wedge t = t') \vee (y \leq t \wedge y \leq t').$$

The inductive step is as follows:

$$(\varphi \wedge \psi)^* := \varphi^* \wedge \psi^*,$$

$$(\neg\varphi)^* = \neg\varphi^*,$$

$$(\exists x \varphi)^* = \exists x \leq y \varphi^*.$$

A standard argument shows that the equivalence from the lemma holds. □

From lemma 6.1 we can conclude the following theorems proven by Krynicki and Zdanowski in [25].

Theorem 6.2 ([25]) $\mathrm{Th}(\mathrm{FM}((\mathcal{A},\leq)))$ *and* $sl(\mathrm{FM}((\mathcal{A},\leq)))$ *are recursively reducible to* $\mathrm{Th}((\mathcal{A},\leq))$. *In particular, if* $\mathrm{Th}((\mathcal{A},\leq))$ *is decidable then* $\mathrm{Th}(\mathrm{FM}((\mathcal{A},\leq)))$ *and* $sl(\mathrm{FM}((\mathcal{A},\leq)))$ *are decidable.*

Theorem 6.3 ([25]) *1. Every relation* FM*–representable in* $\mathrm{FM}(\mathcal{A})$ *is definable in* $(\mathcal{A},\leq)$.

2. If $\mathrm{Th}((\mathcal{A},\leq))$ *is decidable then each* FM*–representable relation in* $\mathcal{A}$ *is recursive.*

By theorem 6.3 we can give a large number of examples of arithmetics which are decidable in finite models. Let $k \geq 2$ and $V_k \colon \omega \longrightarrow \omega$ be a function which maps an integer a to the greatest power of k which divides a and $V_k(0) = 1$, e.g. $V_2(12) = 4$. We call the structure $(\omega, +, V_k)$ the Büchi arithmetic of base k. Büchi proved (see [5]) that for every $k \geq 2$, Büchi arithmetic of base k is decidable.

Let $\exp_n$ be the exponentiation function with a fixed base n, $\exp_n(x) = n^x$. It was proven by Semenov in [43] that $(\omega, +, \exp_n)$ has a decidable theory.

Theorem 6.4 ([25]) $\mathrm{Th}(\mathrm{FM}(\mathcal{A}))$ *and* $\mathrm{sl}(\mathrm{FM}(\mathcal{A}))$ *are decidable for* $\mathcal{A}$ *being one of the following models:* $\mathrm{FM}((\omega,<))$, $\mathrm{FM}((\omega,+))$, $\mathrm{FM}((\omega,+,\exp_n))$, $\mathrm{FM}((\omega,+,V_k))$, *for each natural number* $k \geq 2$.

6.2 Interpretability on initial segments

In this section we introduce some other notions of interpretation which are convenient for finite arithmetics. Our main aim is to have a suitable tool for transferring results, like e.g. the undecidability, from one FM–arithmetic, say $\mathrm{FM}(\mathcal{A})$, to the other one which interprets $\mathrm{FM}(\mathcal{A})$ in a suitable way.

Definition 6.5 $\mathrm{FM}(\mathcal{A})$ *is* sl*–interpretable in* $\mathrm{FM}(\mathcal{B})$ *if there exists a function* $f \colon \omega \longrightarrow \omega$ *and an interpretation* $\bar{\varphi}$ *of* $\mathrm{FM}(\mathcal{A})$ *in* $\mathrm{FM}(\mathcal{B})$ *such that:*

- $f[\omega]$ *is cofinite,*
- *for each* $i \in \omega$, $f^{-1}(\{i\})$ *is finite,*
- *for each* n, $\mathcal{A}_{f(n)} \cong I_{\bar{\varphi}}(\mathcal{B}_n)$.

If $\bar{\varphi}$ *is an order preserving interpretation of* $\mathcal{A}_{f(n)}$ *in* $\mathcal{B}_n$, *that is for each* n,

$$\mathcal{A}_{f(n)} = I_{\bar{\varphi}}(\mathcal{B}_n)$$

then we call $\bar{\varphi}$ *an order preserving* sl*–interpretation.*

A function f from the above definition tells us which model is interpreted in a given model $\mathcal{B}_n$, it is simply $\mathcal{A}_{f(n)}$. Thus, it is essentially the function $I_{\bar{\varphi}}$ described on picture 2.1 on page 20 for $\mathcal{K}_1 = \mathrm{FM}(\mathcal{A})$ and $\mathcal{K}_2 = \mathrm{FM}(\mathcal{B})$.

A similar notion of interpretation called IS–interpretability was formulated by M. Mostowski and A. Wasilewska in [33] and was also used implicitly in [25].

Definition 6.6 $\mathrm{FM}(\mathcal{A})$ *is* IS*–interpretable in* $\mathrm{FM}(\mathcal{B})$ *if there exists an interpretation* $\bar{\varphi}$ *and a monotonic, unbounded function* $f\colon \omega \longrightarrow \omega$ *such that for each* $n \in \omega$,

$$\mathcal{A}_{f(n)} = I_{\bar{\varphi}}(\mathcal{B}_n).$$

Let us observe that there may be sl–interpretations which are not IS–interpretions, and also IS–interpretations which are not sl–interpretations. In the present section we defined sl–interpretations because if there is such an interpretation of $\mathrm{FM}(\mathcal{A})$ in $\mathrm{FM}(\mathcal{B})$ then we can easily transfer properties of one family onto the other one, see theorems 6.10 and 6.11. Thus, the notion of sl–interpetation has an appeal of allowing quite general reasonings about families of the form $\mathrm{FM}(\mathcal{A})$.

On the other hand, it will often be convenient for us to give an IS–intepretation of $\mathrm{FM}(\mathcal{N})$ in $\mathrm{FM}(\mathcal{A})$. However, in such a case we will also be able to construct an sl–interpetation, see proposition 6.12. Thus, by proposition 6.12, we may profit from both notions and use the one which is more convenient for us.

Now we provide an example of an order preserving sl–interpretation (and also IS–interpretation) which will be useful for us in the next sections.

Lemma 6.7 *Let* $\mathcal{A} = (\omega, \leq)$, $\mathcal{B} = (\omega, \times)$ *and let*

$$\varphi_{\leq}(x, y) := \exists z(zx \neq \mathrm{MAX} \wedge zy = \mathrm{MAX}) \vee x = y.$$

For all n, *for all* $a, b < \sqrt{n}$,

$$a \leq b \quad \textit{if and only if} \quad \mathcal{B}_n \models \varphi_{\leq}[a, b].$$

Proof. If the right side of the equivalence holds then $a = b$ or a and b are differentiated by an element of $\mathcal{A}_n$, say z. Since $az < n \leq bz$, it follows that $a \leq b$.

In proving the other implication we may assume that $a \neq b$. Then let k be the smallest element of $\mathcal{A}_n$ such that $bk \geq n$. Since $b^2 < n$, $b < k$. It follows that

$$ak \leq (b-1)k \leq bk - k \leq bk - b \leq b(k-1) < n.$$

Therefore, k as above can be taken as a witness for z in $\varphi_{\leq}$. $\square$

For a further reference let us observe that the same property holds also for a $\forall^*$ formula $\varphi'_{\leq}(x,y)$ defined as

$$\forall z(zx = \mathrm{MAX} \Rightarrow zy = \mathrm{MAX}).$$

Thus, for a $\forall^*$ formula

$$\varphi_S(x,y) := x \neq y \wedge \forall z((\varphi_{\leq}(x,z) \wedge z \neq x) \Rightarrow \varphi'_{\leq}(y,z))$$

we have the following.[1]

Lemma 6.8 *For all n and $a, b < \sqrt{n}$,*

$$b = a + 1 \quad \textit{if and only if} \quad \mathcal{A}_n \models \varphi_S[a,b].$$

Proposition 6.9 *Let $\mathcal{A} = (\omega, \leq)$ and $\mathcal{B} = (\omega, \times)$. There is an interpretation $\bar{\varphi}$ of* FM($\mathcal{A}$) *in* FM($\mathcal{B}$) *such that $\bar{\varphi}$ is both: an order preserving* sl*–interpretation and an* IS*–interpretation.*

Proof. As a function f from definition 6.6 we take

$$f(n) = \left\lfloor \sqrt{n-1} \right\rfloor.$$

The interpretation is the sequence $(\varphi_U, \varphi_{\leq}, \varphi_{\mathrm{MAX}})$. As the formula defining the universe we take

$$\varphi_U(x) := xx \neq \mathrm{MAX}.$$

The formula defining the ordering $\varphi_{\leq}$ is the formula from lemma 6.7. $\varphi_{\mathrm{MAX}}(x)$ is

$$xx \neq \mathrm{MAX} \wedge \forall z(zz \neq \mathrm{MAX} \Rightarrow \varphi_{\leq}(z,x)).$$

The elements of $\mathcal{A}_n$ which satisfy φ_U are just elements $\{0, \ldots, f(n)\}$. It follows from lemma 6.7 that $\varphi_{\leq}$ defines the standard ordering on this set. Finally, φ_{MAX} chooses the maximal element of this set – $f(n)$. To sum up we defined an IS–interpretation of FM($\mathcal{A}$) in FM($\mathcal{B}$). The form of the function f assures that it is also an sl–interpretation. $\square$

The existence of an interpretation between two families of models should allow to infer some relations between these families. The next theorem fulfills this expectation.

[1] Of course φ_S is not a $\forall^*$–formula when we consider the form given above but it can be easily rewritten in such a form.

Theorem 6.10 *Let* $\mathcal{A}$ *and* $\mathcal{B}$ *be such that* $\mathrm{FM}(\mathcal{A})$ *is* sl*–interpretable in* $\mathrm{FM}(\mathcal{B})$. *Then* $\mathrm{sl}(\mathrm{FM}(\mathcal{A}))$ *is many–one reducible to* $\mathrm{sl}(\mathrm{FM}(\mathcal{B}))$ *and* $\mathrm{Th}(\mathrm{FM}(\mathcal{A}))$ *is many–one reducible to* $\mathrm{Th}(\mathrm{FM}(\mathcal{B}))$.

Proof. The proof uses standard techniques introduced in chapter 2.

Let $\mathrm{FM}(\mathcal{A})$ be sl–interpretable in $\mathrm{FM}(\mathcal{B})$ with an interpretation $\bar{\varphi}$ and let f be a function from definition 6.5. Then for any sentence ψ in the vocabulary of $\mathrm{FM}(\mathcal{A})$,

$$\psi \in sl(\mathrm{FM}(\mathcal{A})) \text{ if and only if } \widehat{I}_{\bar{\varphi}}(\psi) \in sl(\mathrm{FM}(\mathcal{B})).$$

One should be a bit more careful with $\mathrm{Th}(\mathrm{FM}(\mathcal{A}))$ and $\mathrm{Th}(\mathrm{FM}(\mathcal{B}))$. Let k be such that for all $n \geq k$ there exists i such that $f(i) = n$. In other words, any model $\mathcal{A}_n$, for $n \geq k$, is interpreted in some model from $\mathrm{FM}(\mathcal{B})$. Then let ψ be a sentence in the vocabulary of $\mathrm{FM}(\mathcal{A})$ and let

$$b(\psi, k) = \begin{cases} \bot & \text{if } \exists i < k,\ \mathcal{A}_i \not\models \psi, \\ \top & \text{otherwise.} \end{cases}$$

The following equivalence exhibits a many–one reduction from $\mathrm{Th}(\mathrm{FM}(\mathcal{A}))$ to $\mathrm{Th}(\mathrm{FM}(\mathcal{B}))$:

$$\psi \in \mathrm{Th}(\mathrm{FM}(\mathcal{A})) \text{ if and only if } \ulcorner \widehat{I}_{\bar{\varphi}}(\psi) \wedge b(\psi, k) \urcorner \in \mathrm{Th}(\mathrm{FM}(\mathcal{B})).$$

□

The existence of an order preserving sl–interpretation between $\mathrm{FM}(\mathcal{A})$ and $\mathrm{FM}(\mathcal{B})$ allows us to compare also the families of FM–representable relations in both families.

Theorem 6.11 *Let* $\mathcal{A}$ *and* $\mathcal{B}$ *be such that there is an order preserving* sl*–interpretation of* $\mathrm{FM}(\mathcal{A})$ *in* $\mathrm{FM}(\mathcal{B})$. *For each* $R \subseteq \omega^r$, *if* R *is* FM*–representable in* $\mathrm{FM}(\mathcal{A})$ *then* R *is* FM*–representable in* $\mathrm{FM}(\mathcal{B})$.

Proof. It is straightforward to see that if $\psi(\bar{x})$ FM–represents R in $\mathrm{FM}(\mathcal{A})$ and $\bar{\varphi}$ is an IS–interpretation of $\mathrm{FM}(\mathcal{A})$ in $\mathrm{FM}(\mathcal{B})$, then $\widehat{I}_{\bar{\varphi}}(\psi)$ FM–represents R in $\mathrm{FM}(\mathcal{B})$. □

To use theorems 6.10 and 6.11 we need to have an sl–interpretation. In the following sections it will often be often more convenient to give an IS–interpretation of $\mathrm{FM}(\mathcal{N})$ in a given arithmetic $\mathrm{FM}(\mathcal{A})$. As the following proposition states, in such a case the existence of an IS–interpretation is a sufficient condition to conlude the existence of an order preserving sl–interpretation.

Proposition 6.12 *Let $\bar{\varphi}$ be an* IS*–interpration of* FM($\mathcal{N}$) *in* FM($\mathcal{A}$)*. Then there is an order preserving* sl*–interpretation $\bar{\psi}$ of* FM($\mathcal{N}$) *in* FM($\mathcal{A}$)*.*

Proof. Let $\bar{\varphi}$ and f be as in definition 6.6. We find a function $g\colon \omega \longrightarrow \omega$ and an interpretation $\bar{\psi}$ such that

- g is monotonic and unbounded,
- $\forall n\, |g(n+1) - g(n)| \leq 1$,
- $\forall n\, \mathcal{N}_{g(n)} = I_{\bar{\psi}}(\mathcal{A}_n)$.

It follows, by the three conditions above, that $\bar{\psi}$ is an order preserving sl–interpretation of FM($\mathcal{N}$) in FM($\mathcal{A}$).

Now we construct g and $\bar{\psi}$. As an intermediate step we construct a function $h\colon \mathrm{rg}(f) \longrightarrow \omega$ such that

(i) h is monotonic and unbounded,

(ii) $\forall n\, |h(f(n+1)) - h(f(n))| \leq 1$,

(iii) the graph of h is Δ_0 definable.

Let us observe that if we have h as above then we can easily construct g and $\bar{\psi}$. To construct $\bar{\psi}$ we could take an interpretation $\bar{\gamma}$ of FM($\mathcal{N}$) in FM($\mathcal{N}$) such that for all n,

$$\mathcal{N}_{h(n)} = I_{\bar{\gamma}}(\mathcal{N}_n).$$

Such a $\bar{\gamma}$ exists since h is Δ_0 definable. Then $\bar{\psi}$ would be a composition of $\bar{\varphi}$ and $\bar{\gamma}$ and g would be a composition of f and h, that is $g(n) = h(f(n))$. So, we need only to show that the function h as above exists.

Let us observe that f is a recursive function. This follows from the fact that given n we can effectively check what is the cardinality of $I_{\bar{\varphi}}(\mathcal{N}_n)$. Thus, let H_f be a machine which computes f. Moreover, let us require that for each n, the computation of H_f on input n has a smaller code than the computation on input $n+1$. This can be achieved e.g. by forcing H_f to compute on input n all values $f(i)$, for $i \in \{0, \ldots, n\}$. Then let $c_{H_f}(n)$ be a computation of H_f on the input n. We can define h as

$$h(n) = \max\left\{k \,:\, c_{H_f}(k) \leq n\right\}.^2$$

Since being a code of a computation is Δ_0, the definition of h is also Δ_0. Obviously the properties (i) – (iii) that we put on h are fulfilled,which ends the proof. □

[2]Let us observe that our definition of h depends not only on f but also on the form of the machine H_f.

6.3 Undecidable arithmetics of finite models

In this section we consider various arithmetics which are weaker than addition and multiplication. Nevertheless, we show that in finite models some of them have the semantical power very close to the arithmetic of addition and multiplication.

6.3.1 Multiplication in finite models

In the first part of this section we show that the class $\mathrm{FM}((\omega,\times))$ is not finitely axiomatizable within the class of all finite models. It can be compared to the result of Marcin Mostowski from [32] on finite axiomatizability of the family $\mathrm{FM}(\mathcal{N})$ within the class of all finite models, see proposition 3.11. It may be mentioned that Patrick Cegielski showed in [6], using a different method, that the theory of $(\omega,\times)$ is not finitely axiomatizable.

Definition 6.13 *Let $\mathcal{A}=(\omega,\times)$ and $\mathcal{A}_n\in\mathrm{FM}(\mathcal{A})$, where $n>1$. By $\mathcal{A}'_n$ we denote a model $(\{0,\ldots,n\}\cup\{\alpha\},\otimes,n)$ such that*

- $\alpha\notin\omega$,
- $\otimes = \times_n\cup\{(0,\alpha,0),(\alpha,0,0),(1,\alpha,\alpha),(\alpha,1,\alpha)\}\cup\{(a,b,n) : a,b\notin\{0,1\}\wedge\alpha\in\{a,b\}\}$, *where $\times_n$ is the graph of multiplication from $\mathcal{A}_n$.*

It is easy to observe, that α behaves in $\mathcal{A}'_n$ like any other prime from $\{\lceil n/2\rceil,\ldots,n-1\}$.

Lemma 6.14 *Let $\mathcal{A}=(\omega,\times)$. For each $n>1$, for each $\mathcal{A}'_n$ and for each prime $p\in\{\lceil n/2\rceil,\ldots,n-1\}$ there is an automorphism f of $\mathcal{A}'_n$ such that*
$$f(a)=\begin{cases} a & \text{if } a\notin\{p,\alpha\},\\ p & \text{if } a=\alpha,\\ \alpha & \text{if } a=p.\end{cases}$$

Lemma 6.15 *Let $\mathcal{A}=(\omega,\times)$. For each n,*
$$\mathcal{A}'_n\cong\mathcal{A}_{n+1} \quad \text{if and only if } \ n \text{ is a prime.}$$

Proof. Let us observe that in any isomorphism between $\mathcal{A}'_n$ and $\mathcal{A}_{n+1}$ any prime from $\mathcal{A}'_n$ and α can be mapped only to a prime from $\mathcal{A}_{n+1}$. Therefore, if n is a prime then $f\colon|\mathcal{A}'_n|\longrightarrow|\mathcal{A}_{n+1}|$ defined as
$$f(a)=\begin{cases} a & \text{if } a<n,\\ n+1 & \text{if } a=n,\\ n & \text{if } a=\alpha.\end{cases}$$

is an isomorphism between $\mathcal{A}'_n$ and $\mathcal{A}_{n+1}$. On the other hand, if n is composite then there is too few number of primes in $\mathcal{A}_{n+1}$ to map onto them all primes from $\mathcal{A}'_n$ and α. $\square$

Let $\pi(x)$ be the following function

$$\pi(x) = \sum_{\substack{p < x \\ p \text{ is prime}}} 1.$$

The prime number theorem states that $\lim_{x\to\infty} \pi(x)/(x/\ln(x)) = 1$ (see e.g. [38]). We need an easy consequence of the prime number theorem.

Fact 6.16 *For all k there is n such that for all $s \geq n$ there are k primes in $\{s, \ldots, 2s\}$.*

Lemma 6.17 *Let $\mathcal{A} = (\omega, \times)$. Let n be such that there are k primes in $\{\lceil n/2 \rceil, \ldots, n-1\}$. Then $\mathcal{A}_n \equiv_k \mathcal{A}'_n$*

Proof. It suffices to show that Eros has a winning strategy in k–moves Ehrenfeucht–Fraïsse game between $\mathcal{A}_n$ and $\mathcal{A}'_n$. We split models $\mathcal{A}_n$ and $\mathcal{A}'_n$ into two parts. Let

$$P_1 = \{p : \text{ p is a prime and } p \in \{\lceil n/2 \rceil, \ldots, n-1\},$$

$$P_2 = P_1 \cup \{\alpha\}$$

and

$$B_1 = B_2 = (\{0, \ldots, n\} \setminus P_1.$$

Then $|\mathcal{A}_n| = B_1 \cup P_1$ and $|\mathcal{A}'_n| = B_2 \cup P_2$. We refer to B_1 and P_1 as subsets of the universe of $\mathcal{A}_n$ and to B_2 and P_2 as subsets of the universe of $\mathcal{A}'_n$. Then on sets B_1 and B_2 Eros's answers on Ares's moves are the same elements from the other structure. If Ares chooses a new element from P_i, $i \in \{0, 1\}$, then Eros can answer with an arbitrary element from P_{1-i} which has not been chosen. Since cardinalities of P_1 and P_2 are at least k, Eros can maintain this strategy during k moves of the Ehrenfeucht–Fraïsse game. Moreover, at each stage of the game the set of chosen pairs forms a partial isomorphism between $\mathcal{A}_n$ and $\mathcal{A}'_n$. Thus, Eros wins. $\square$

Theorem 6.18 *Let $\mathcal{A} = (\omega, \times)$. The family* $\mathrm{FM}(\mathcal{A})$ *is not finitely axiomatizable within the class of all finite models.*

Proof. We show that for each k there are two finite models $\mathcal{B}$ and $\mathcal{C}$ such that $\mathcal{B} \equiv_k \mathcal{C}$, $\mathcal{B} \in \mathrm{FM}(\mathcal{A})$ and there is no $\mathcal{D} \in \mathrm{FM}(\mathcal{A})$ such that $\mathcal{C} \cong \mathcal{D}$. It follows that no first order sentence of quantifier rank k axiomatizes $\mathrm{FM}(\mathcal{A})$ within the class of finite models. Since k is arbitrary, $\mathrm{FM}(\mathcal{A})$ is not finitely axiomatizable within finite models.

As $\mathcal{B}$ we choose $\mathcal{A}_{2n} \in \mathrm{FM}(\mathcal{A})$ such that, by fact 6.16, there are k primes in $\{n, \ldots, 2n\}$ and $\mathcal{C} = \mathcal{A}'_{2n}$. Then by lemma 6.17, $\mathcal{C} \equiv_k \mathcal{A}_n$ but there is no $\mathcal{D} \in \mathrm{FM}(\mathcal{A})$ such that $\mathcal{C} \cong \mathcal{D}$. By a cardinality argument, the only such $\mathcal{D}$ can be $\mathcal{A}_{2n+1}$. However, by lemma 6.15, there is no isomorphism between $\mathcal{A}_{2n+1}$ and $\mathcal{C}$. □

We need the following theorem proven by Lee in [26].

Theorem 6.19 ([26]) $\mathrm{FM}(\mathcal{N})$ *is definable in* $\mathrm{FM}((\omega, \times, \leq))$.

The following was observed by Schweikardt in [42].

Proposition 6.20 ([42]) $\mathrm{FM}((\omega, \leq))$ *is not definable in* $\mathrm{FM}((N, \times))$.

It can be observed that a stronger fact holds. Let us remind that $\leq_X$ is the ordering relation on ω restricted to the set $X \subseteq \omega$ and that P is the set of all primes.

Theorem 6.21 $\mathrm{FM}((\omega, \leq))$ *is not definable in* $\mathrm{FM}((N, \times, \leq_P))$.

Proof. Since addition is definable in finite models from multiplication and ordering (see theorem 6.19) it suffices to show that addition is not definable in $\mathrm{FM}((\omega, \times, \leq_P))$.

Let $k \in \omega$ be such that there are at least $2^{k+1} + 1$ primes in $\{\lceil n/2 \rceil, \ldots, n-1\}$ and let $\mathcal{A}_n \in \mathrm{FM}((\omega, \times, \leq_P))$, $\mathcal{B}_n \in \mathrm{FM}(\mathcal{N})$. Then let

$$S = \{p_i, \ldots, p_j\},$$

be the set of primes in $\{\lceil n/2 \rceil, \ldots, n-1\}$ and let p, q be the primes from the middle of this sequence, that is $p = p_{\lfloor (j-i)/2 \rfloor}$ and $q = p_{\lfloor (j-i)/2 \rfloor + 1}$. We show that no first order formula $\varphi(x)$ of quantifier rank less or equal k differentiates in $\mathcal{A}_n$ between p and q. That is, if $\mathrm{qr}(\varphi) \leq k$ then

$$\mathcal{A}_n \models \varphi[p] \text{ if and only if } \mathcal{A}_n \models \varphi[q].$$

On the contrary, for infinitely many of corresponding models $\mathcal{B}_n \in \mathrm{FM}(\mathcal{N})$ the primes p and q are differentiated by a fixed first order formula. Consequently, $\mathrm{FM}(\mathcal{N})$ is not definable in $\mathrm{FM}((\omega, \times, \leq_P))$.

To show the first claim we argue that Eros wins the k–moves game between $(\mathcal{A}_n, p)$ and $(\mathcal{A}_n, q)$, when we treat p and q as indicated elements. We split the universe of $\mathcal{A}_n$ into two parts: $S = \{p_i, \ldots, p_j\}$ and $T = |\mathcal{A}_n| \setminus S$. On T Eros answers for Ares moves with the same elements. Eros treats the part S as two linear orderings determined in both structures by the middle primes p and q. Eros can win a k–moves game between corresponding pairs of orderings in both structures, see fact 2.4. Combining these strategies Eros wins a k–moves game between $(\mathcal{A}_n, p)$ and $(\mathcal{A}_n, q)$. This is so because the only properties which differentiate the primes from S are the ordering properties.

To finish the proof we provide a formula $\psi(x)$ which differentiates between p and q in infinitely many models $\mathcal{B}_n$. It uses the ordering relation, the predicate for primes and the predicate $\mathrm{EXP}(x, y, z)$ which is interpreted as the graph of the exponentiation function. All these notions are definable in $\mathcal{B}_n$. $\psi(x)$ has the form

$$P(x) \wedge \exists z \exists y(\mathrm{EXP}(2, z, y) \wedge y \leq p \wedge \forall w(y \leq w \leq x \wedge w \neq p \Rightarrow \neg P(w))).$$

It states that x is the least prime greater than some power of two. Thus, for infinitely many n, $\mathcal{B}_n \models \psi[p]$. On the other hand no two consecutive primes satisfy $\psi(x)$. Thus, if $\mathcal{B}_n \models \psi[p]$ then $\mathcal{B}_n \not\models \psi[q]$. $\square$

Let us recall that we know from section 6.2 that there is an IS–interpretation of $\mathrm{FM}((\omega, \leq))$ in $\mathrm{FM}((\omega, \times))$.

Combining this result with theorem 6.19 we get the following theorem given by Krynicki and Zdanowski in [25].

Theorem 6.22 ([25]) *There is an* IS*–interpretation of* $\mathrm{FM}((\omega, +, \times))$ *in* $\mathrm{FM}((\omega, \times))$*. Moreover, as a function* f *from definition 6.6 one can take* $f(n) = \lfloor \sqrt{n-1} \rfloor$.

Proof. By lemma 6.7 there is an IS–interpretation of $\mathrm{FM}((\omega, \leq))$ in $\mathrm{FM}((\omega, \times))$ with function $f(n) = \lfloor \sqrt{n-1} \rfloor$. By theorem 6.19, once we have defined ordering, we can also define addition on the ordered part of a model $\mathcal{A}_n \in \mathrm{FM}((\omega, \times))$. Thus, we get an IS–interpretation as stated in the theorem. $\square$

By the above result, applying theorems 6.10, 6.11 and proposition 6.12, we obtain the following theorems.

Theorem 6.23 ([25]) *1.* $\mathrm{Th}((\omega, \times))$ *is* Π_1*–complete.*

2. $sl(\mathrm{FM}((\omega,\times)))$ *is* Σ_2*–complete.*

Theorem 6.24 ([25]) *The same relations are* FM*-representable in* $\mathrm{FM}((\omega,\times))$ *as in* $\mathrm{FM}((\omega,+,\times))$*.*

The last three theorems were proven in [25] although the term IS or sl–interpretation was not used there. Later, the analogous results were proven for the arithmetic of divisibility by M. Mostowski and A. Wasilewska in [33].

Theorem 6.25 ([33]) *There is an* IS*–interpretation of* $\mathrm{FM}((\omega,+,\times))$ *in* $\mathrm{FM}((\omega,|))$*, where* $|$ *is the divisibility relation. Moreover, as a function* f *from definition 6.6 one can take* $f(n)=\left\lfloor\sqrt[4]{n-1}\right\rfloor$*.*

Let us recall that by $\exists^*\forall^*$ we denote the class of formulas of the form

$$\exists x_1\ldots\exists x_k\forall z_1\ldots\forall z_n\psi,$$

where ψ is a quantifier free formula.

Now we are going to estimate the undecidability bound for multiplication in finite models. We show that $\exists^*\forall^*$–prefix gives the undecidable theory of multiplication. Later, in section 6.4, we show that this bound is optimal.

Theorem 6.26 ([25]) (i) *The set of* $\exists^*\forall^*$ *sentences of arithmetic of multiplication which are satisfiable in finite models is* Σ_1*–complete.*

(ii) *The set of* $\exists^*\forall^*$ *sentences of arithmetic of multiplication which are true in all sufficiently large finite models is* Σ_1*–hard.*

Proof. By Matijasevič theorem the set of sentences of the form

$$\exists\bar{x}f(\bar{x})=g(\bar{x}),$$

where f and g are terms of arithmetic which are true in the infinite model is Σ_1–complete.

Terms f and g may contain addition but it can be existentially defined from multiplication and successor by the identity due to Tarski: for all x, y, $z\neq 0$,

$$x+y=z \text{ if and only if } (xz+1)(yz+1)=z^2(xy+1)+1.$$

It follows that the problem whether the sentence of the form

$$\exists x_1\ldots\exists x_n\psi,$$

where ψ is quantifier free in a relational form with only positive occurrences of $\times$ and S, is true in the infinite model is Σ_1–complete. We reduce the last problem to the satisfiability of $\exists^*\forall^*$ sentences in $\mathrm{FM}((\omega,\times))$ and to $\mathrm{sl}_{\exists^*\forall^*}(\mathrm{FM}((\omega,\times)))$.

Let $\mathcal{A}=(\omega,\times)$ and let $\varphi_S(x,y)$ be a $\forall^*$ formula from lemma 6.8 which defines the graph of the successor function on $\{0,\ldots,\lceil\sqrt{n-1}\rceil\}$ part of a model $\mathcal{A}_n$. For a formula $\exists x_1\ldots\exists x_n\psi$ as above, let ψ' be the formula which is obtained from ψ by replacing equations $s(x_i)=x_j$ with $\varphi_S(x_i,x_j)$. Then let γ be

$$\exists x_1\ldots\exists x_n(\bigwedge_{i\leq n} x_ix_i\neq \mathrm{MAX}\wedge\psi').$$

It suffices to show that the following conditions are equivalent:

(i) $(\omega,\times,S)\models\exists x_1\ldots\exists x_n\psi$,

(ii) γ is satisfiable in $\mathrm{FM}(\mathcal{A})$,

(iii) $\mathrm{FM}(\mathcal{A})\models_{\mathrm{sl}}\gamma$.

If (i) then let $a_1,\ldots,a_n\in\omega$ be witnesses for $\exists x_1\ldots\exists x_n\psi$ in $(\omega,\times,S)$. Then in all models $\mathcal{A}_n$, where $n>(\max\{a_1,\ldots,a_n\})^2$, φ_S represents the successor function on $a_1,\ldots,a_n$ and $\mathcal{A}_n\models\psi'[a_1,\ldots,a_n]$. Thus, $\mathrm{FM}(\mathcal{A})\models_{\mathrm{sl}}\gamma$.

The implication from (iii) to (ii) is obvious. So, we assume (ii) and show (i). Let n be such that $\mathcal{A}_n\models\gamma$ and let $a_1,\ldots,a_n$ be witnesses in $\mathcal{A}_n$ for existential quantifiers in γ. Then $n>(\max\{a_1,\ldots,a_n\})^2$ and φ_S defines on $a_1,\ldots,a_n$ the successor function. Thus, by construction of ψ', $a_1,\ldots,a_n$ are also good witnesses for ψ in $(\omega,\times,S)$. □

Let us mention that we do not know whether $\mathrm{sl}_{\exists^*\forall^*}(\mathrm{FM}((\omega,\times))$ is a Σ_2–complete set.

6.3.2 Exponentiation in finite models

Now let us turn to the arithmetic with exponentiation. Let us recall that we define the exponentiation function as $\exp(x,y)=x^y$. We show that contrary to the infinite model, in finite models exponentiation is a rather weak function. It is known that in the infinite model sole exponentiation defines addition and multiplication. Here, we show that in finite models exponentiation can be defined by means of multiplication only. The following theorem was proven by Krynicki and Zdanowski in [25].

Theorem 6.27 ([25]) *Let* $\mathcal{A} = (\omega, \exp)$ *and* $\mathcal{B} = (\omega, \times)$. $\mathrm{FM}(\mathcal{A})$ *is definable in* $\mathrm{FM}(\mathcal{B})$.

Proof. A full interpretation of $\mathrm{FM}(\mathcal{A})$ in $\mathrm{FM}(\mathcal{B})$ is a sequence of formulas $(\varphi_U(x), \varphi_{\exp}(x,y,z), \varphi_{\mathrm{MAX}}(x))$. Since the interpretation is full we have to take for φ_U the formula $x = x$, and as φ_{MAX} we take $x = \mathrm{MAX}$. What is left is to write the formula $\varphi_{\exp}(x,y,z)$. Firstly, let us observe that there is a formula $\varphi_e(x,y,z)$ with multiplication only which defines exponentiation on $\{0, \ldots, \lfloor\sqrt{n-1}\rfloor\}$ part of a model $\mathcal{B}_n$. The existence of such a formula follows from the fact that there is a Δ_0 definition of exponentiation in the arithmetic of addition and multiplication (see lemma 3.4) and that any such definition can be rewritten in finite models (see theorem 3.21). We use in φ_e only multiplication because on $\{0, \ldots, \lfloor\sqrt{n-1}\rfloor\}$ part of a model for multiplication we can define addition (see theorem 6.22). Moreover, it can be easily checked that one can define exponentiation in $\mathcal{B}_n$, for $n \leq 10$. Therefore, we assume that the maximal element in $\mathcal{B}_n$ (which is just n) is greater than 10. We need the following property:

$$\text{for each } n \geq 10 \text{ and } a \text{ such that } a^2 \geq n \text{ and } b \geq 2,$$

$$b^a \geq n.$$

Thus, we should care mainly about elements a for which a^2 is less than the maximal element of a model.

We write the formula $\varphi_{\exp}$ as a disjunction of two formulas: $\varphi_1(x,y,z)$ and $\varphi_2(x,y,z)$. The first one detects and handles all easy cases and the second handles the only nontrivial one. We use a formula $\varphi_+(x,y,z)$ which defines addition on $\{0, \ldots, \lfloor\sqrt{n-1}\rfloor\}$ part of the model $\mathcal{B}_n$. Moreover, we freely use constants 0, 1 and 2 to denote first elements of the model $\mathcal{B}_n$ since they can be defined by means of multiplication.
$\varphi_1(x,y,z) :=$

$$(y = 0 \wedge z = 1) \vee (x = 1 \wedge z = 1) \vee (x = 0 \wedge y \neq 0 \wedge z = 0) \vee$$

$$(yy = \mathrm{MAX} \wedge x \neq 0 \wedge x \neq 1 \wedge z = \mathrm{MAX}),$$

$\varphi_2(x,y,z) :=$

$$yy \neq \mathrm{MAX} \wedge y \neq 0 \wedge y \neq 1 \wedge x \neq 0 \wedge x \neq 1 \wedge$$

$$\exists w_1 \exists w_2 \{\varphi_+(2w_1, w_2, y) \wedge (w_2 = 0 \vee w_2 = 1) \wedge$$

$$[\exists u(u^2 \neq \mathrm{MAX} \wedge \varphi_e(x, w_1, u) \wedge ((w_2 = 0 \wedge z = uu) \vee (w_2 = 1 \wedge z = uux))) \vee$$

$$(\neg \exists u(u^2 \neq \mathrm{MAX} \wedge \varphi_e(x, w_1, u)) \wedge z = \mathrm{MAX})]\}.$$

The first line of $\varphi_2(x,y,z)$ simply states that none of the easy cases holds. Then we find w_1, w_2 such that $y = 2w_1 + w_2$ and $w_2 \in \{0,1\}$. It is possible because y is in the part of the model on which $\varphi_+(x,y,z)$ defines addition. Then in the third line of φ_2, we find $u \leq \lfloor \sqrt{n-1} \rfloor$ such that $x^{w_1} = u$. It follows that

$$x^y = x^{2w_1} x^{w_2} = (x^{w_1})^2 x^{w_2} = u^2 x^{w_2}.$$

On the other hand, if such a u does not exist then $x^{w_1} > \lfloor \sqrt{n-1} \rfloor$ and

$$x^y \geq x^{2w_1} \geq (x^{w_1})^2 \geq (\lfloor \sqrt{n-1} \rfloor + 1)^2 \geq n$$

Thus z should be equal to the maximal element of the model. From the above analysis it follows that the disjunction of φ_1 and φ_2 defines exponentiation on the whole model from $\mathrm{FM}(\mathcal{A})$. $\square$

Since $\mathrm{FM}((\omega, \leq))$ is not definable in $\mathrm{FM}((\omega, \times))$ we obtain the following.

Corollary 6.28 $\mathrm{FM}((\omega, \leq))$ *is not definable in* $\mathrm{FM}((\omega, \exp))$.

Nevertheless, it is possible to give an IS–interpretation of $\mathrm{FM}((\omega, +, \times))$ in $\mathrm{FM}((\omega, \exp))$.

Theorem 6.29 ([25]) *Let* $\mathcal{A} = (\omega, \exp)$. $\mathrm{FM}(\mathcal{N})$ *is* IS*–interpretable in* $\mathrm{FM}(\mathcal{A})$.

Proof. In the interpretation we use the common definition of multiplication from exponentiation: for all x, y, z,

$$xy = z \iff \exp(\exp(2,x), y) = \exp(2,z).$$

It suffices now to observe that 2 is definable in all models $\mathrm{FM}(\mathcal{A})$ of cardinality greater than 5 by the following formula:

$$\exp(x,x) \neq x \wedge \exp(\exp(x,x), \exp(x,x)) \neq \exp(x,x) \wedge$$

$$\forall z((\exp(z,x) \neq z \wedge z \neq x) \Rightarrow \exists y(\exp(x,y) \neq \mathrm{MAX} \wedge \exp(z,y) = \mathrm{MAX})).$$

In the first line of the above formula we exlude the case of x being 0 or 1. In the second line we state that for any $z \notin \{0,1,x\}$ z can be proven to be less than x by a witness y.

Thus, a formula $\exp(\exp(2,x), y) = \exp(2,z)$ defines multiplication whenever z is less than logarithm of the maximal element of a model. Now the

exact forms of formulas in the interpretation can be written in a straightforward manner. □

The last theorem allows us to characterize the complexity of exponentiation in finite models. By proposition 6.12 we infer the existence of an order preserving sl–interpretation of FM($\mathcal{N}$) in FM($(\omega, \exp)$). Thus, by theorems 6.10 and 6.30, we have the following theorem proven by Krynicki and Zdanowski in [25].

Theorem 6.30 ([25]) *1.* Th($(\omega, \exp)$) *is* Π_1*–complete.*

2. sl(FM($(\omega, \exp)$)) *is* Σ_2*–complete.*

Then, by theorems 6.11 and 6.24, we can state the following.

Theorem 6.31 ([25]) *The same relations are* FM*-representable in* FM($(\omega, \exp)$) *as in* FM($(\omega, +, \times)$).

Let us mention that the definability of exponentiation in FM($(\omega, \times)$) can be seen as an example of the weakness of fast growing functions in finite models. It can also be shown that e.g. the facultet function or super exponential function are definable in FM($(\omega, \times)$). Both these functions grow so fast that for only small fractions of elements of a given finite model their value is not greater than the maximal element of the model. Thus, they are easily definable provided that we defined them on small elements of a model.

6.3.3 Coprimality in finite models

In this subsection we shortly discuss the results obtained by M. Mostowski and the author in [34]. We present them with the aim to complete the landscape of finite artihmetics.

Coprimality in the infinite model is one of the weakest natural arithmetical relations. We denote it with $\perp$. As we will see coprimality is surprisingly strong when considered in finite models. The results below were proven independently by the author and by Marcin Mostowski and are presented in [34].

We know that FM($\mathcal{N}$) is IS–interpretable in FM($(\omega, \times)$) or even in a semantically weaker class of finite models FM($(\omega, \exp)$), see theorems 6.22 and 6.29 respectively. After these results were proven, M. Mostowski and A. Wasilewska have shown that FM(N) is IS–intepretable in FM($(\omega, |)$), where $|$ is the divisibility relation (see [33]). The above results raise the

question: are there any relations essentially weaker than divisibility allowing an interpretation of $\mathrm{FM}(\mathcal{N})$ in their FM–domains? The answer is yes.

By means of coprimality relation we can not distinguish numbers which have the same set of prime divisors like e.g. 6 and 12. This is so because for each model $\mathcal{A} \in \mathrm{FM}((\omega, \perp))$ such that $6, 12 \in |\mathcal{A}|$, there is an automorphism f of $\mathcal{A}$ such that

$$f(x) = \begin{cases} 12, & \text{if } x = 6, \\ 6, & \text{if } x = 12, \\ x, & \text{if } x \in |\mathcal{A}| \setminus \{6, 12\}. \end{cases}$$

Nevertheless, even such a weak relation as coprimality can interpret in finite models the full arithmetic.

In our interpretation of $\mathrm{FM}(\mathcal{N})$ in $\mathrm{FM}((\omega, \perp))$ we define the arithmetic on indices of prime numbers. More precisely, we define the arithmetic on $\approx$–equivalence classes of the corresponding numbers. Let $\{p_i : i \in \omega\}$ be an enumeration of primes, that is $p_0 = 2, p_1 = 3, \ldots$ Let us define relations R_+ and $R_\times$ by the following:

$$R_+([p_i], [p_k], [p_m]) \text{ if and only if } i + k = m,$$

$$R_\times([p_i], [p_k], [p_m]) \text{ if and only if } ik = m.$$

The following theorem has been proven by M. Mostowski and Zdanowski in [34].

Theorem 6.32 ([34]) *There is an* sl*–interpretation* $\bar{\varphi}$ *of* $\mathrm{FM}(\mathcal{N})$ *in* $\mathrm{FM}((\omega, \perp))$*. The interpretation defines* R_+ *and* $R_\times$ *on the primes from an initial segment of a given model of* $\mathrm{FM}((\omega, \perp))$*.*

Moreover, the equality predicate is not used in formulas from $\bar{\varphi}$*.*

The proof of the above theorem uses essentially an estimation of the density of primes given by the prime number theorem.

As a corollary we obtain a characterization of relations which are FM–representable in $\mathrm{FM}((\omega, \perp))$ given by M. Mostowski and Zdanowski in [34].

Definition 6.33 *Let* $a \approx b$ *if* a *and* b *have the same prime divisors. A relation* $R \subseteq \omega^n$ *is coprimality invariant if* $\approx$ *is a congruence relation for* R*.*

Theorem 6.34 (FM**–representability theorem for** $\mathrm{FM}((\omega, \perp))$**)** *Let* $R \subseteq \omega^n$*.* R *is* FM*–representable in* $\mathrm{FM}((\omega, \perp))$ *if and only if* R *is* FM*–representable in* $\mathrm{FM}(\mathcal{N})$ *and* R *is coprimality invariant.*

The interpretation gives also the following theorem. Its first point can be seen as a variant of the Trachtebrot theorem for $\mathrm{FM}((\omega, \perp))$ family of finite models.

Theorem 6.35 ([34]) *1.* $\mathrm{Th}(\mathrm{FM}((\omega, \perp)))$ *is* Π_1*–complete,*
2. $sl(\mathrm{FM}((\omega, \perp)))$ *is* Σ_2*–complete.*

Moreover, the theorem remains valid even if we do not have equality in the language.

The methods used in [34] allows also to characterize the complexity of the coprimality relation with some parts of ordering in the infinite model.

Let

$$P_2 = \{p_i p_j \,:\, 0 \leq i < j\} \cup P,$$

for P being the set of primes.

Theorem 6.36 ([34]) *The relations* R_+ *and* $R_\times$ *are definable in* $(\omega, \perp, \leq_{P_2})$.

Let us observe that it was proven by Maurin in [28] that the theory of $(\omega, \times, \leq_P)$ is decidable. On the other hand, Bés and Richard proved in [4] that one can intepret the arithmetic of addition and multiplication in the model $(\omega, \perp, \leq_{P^2})$, where $P^2 = P \cup \{p^2 \,:\, p \in P\}$. In the view of this result the last theorem shows that another small extension of the structure $(\omega, \perp)$ by the ordering $\leq_{P_2}$ again gives an arithmetic so strong that it interprets addition and multiplication.

6.4 Decidable fragments of multiplication with order

The results presented in this section were achieved in cooperation with Michał Krynicki and are contained in our paper [25].

Let us fix $\mathcal{A}$ as the model $(\omega, \times, \leq)$. The main result of this section is the decidability of the existential fragment of multiplication with ordering in $\mathrm{FM}(\mathcal{A})$ as well as in $\mathcal{A}$. We also prove that $sl_{\exists^*}(\mathrm{FM}(\mathcal{A}))$ is decidable (see theorem 6.42). Morever, the proofs reveal some additional information on a size of the finite models for $\exists^*$ sentences.

Let us observe, that if we replaced ordering by the successor the corresponding theory becomes undecidable.

Fact 6.37 $\mathrm{Th}_{\exists^*}(\mathrm{FM}((\omega, \times, S)))$ *is* Π_1*–complete and* $sl_{\exists^*}(\mathrm{FM}((\omega, \times, S)))$ *is* Π_1*–hard.*

Proof. Analyzing the proof of theorem 6.26 one can see that if we replace the formula $\varphi_S(x,y)$ which defines the successor function with $S(x)=y$ we get $\exists^*$ formulas. Since we have the successor function in our vocabulary we get the result as in theorem 6.26 but for $\exists^*$ formulas. $\square$

We need the following fact from Krynicki and Zdanowski [25].

Fact 6.38 ([25]) *For any $\exists^*$ sentence φ, if φ is satisfiable in* $\mathrm{FM}(\mathcal{A})$ *then* $\mathrm{FM}(\mathcal{A}) \models_{\mathrm{sl}} \varphi$.

Proof. It suffices to show that for each k there is N such that for each $n \geq N$ there is a submodel of $\mathcal{A}_n$ which is isomorphic to $\mathcal{A}_k$. Therefore, if φ is $\exists^*$ and $\mathcal{A}_k \models \varphi$ then each model of cardinality greater or equal to N has a submodel in which φ is true. But for any $\exists^*$ formula ψ and $\mathcal{B} \subseteq \mathcal{A}$, if $\mathcal{B} \models \psi$ then $\mathcal{A} \models \psi$. Thus, φ has to be true also in $\mathcal{A}_n$ and, consequently, $\models_{\mathrm{sl}} \varphi$.

Let a model $\mathcal{A}_k$ be given. It has the universe $\{0,1,\ldots,k\}$. We define a function $\hat{}\colon |\mathcal{A}_k| \longrightarrow |\mathcal{A}_n|$ and then we prove that if n is sufficiently large, the image of $\hat{}$ defines a submodel of $\mathcal{A}_n$ isomorphic to $\mathcal{A}_k$.

Let $p_1,\ldots,p_m$ be all primes $< k$. For $i \leq m$ let

$$\hat{p}_i = \left\lceil n^{\log_k p_i} \right\rceil .$$

Each element $a \in \{2,\ldots,k-1\}$ has a unique representation of the form $p_1^{r_1}\cdots p_m^{r_m}$. To preserve multiplication we define $\hat{a}$ as $\hat{p}_1^{r_1}\cdots\hat{p}_m^{r_m}$.

Of course we put: $\hat{0}=0$, $\hat{1}=1$ and $\hat{k}=n$.

To prove that for a sufficiently large n the image of $\hat{}$ defines a submodel of $\mathcal{A}_n$ isomorphic to $\mathcal{A}_k$ it suffices to prove that for a sufficiently large n all $r_1,\ldots,r_m < k$ and all $a,b \in \{2,\ldots,k-1\}$,

1. $p_1^{r_1}\cdots p_m^{r_m} < k \iff \hat{p}_1^{r_1}\cdots\hat{p}_m^{r_m} < n$,
2. $a < b \iff \hat{a} < \hat{b}$.

Clearly, if all requirements of the form 1 and 2 are satisfied then $\hat{}$ is an injection of $\mathcal{A}_k$ into $\mathcal{A}_n$.

We will show only that for $a,b \in \{2,\ldots,k-1\}$ and for a sufficiently large n, the condition from point 2 is satisfied. The point 1 is proven in an analogous way.

Assume $a = p_1^{r_1} \cdots p_m^{r_m}$, $b = p_1^{s_1} \cdots p_m^{s_m}$ and $a < b$. Then

$$\begin{aligned}
\hat{a} &= \hat{p}_1^{r_1} \cdots \hat{p}_m^{r_m} \\
&= \left\lceil n^{\log_k p_1} \right\rceil^{r_1} \cdots \left\lceil n^{\log_k p_m} \right\rceil^{r_m} \\
&< (n^{\log_k p_1} + 1)^{r_1} \cdots (n^{\log_k p_m} + 1)^{r_m} \\
&\leq (n^{\log_k p_1 + \varepsilon'})^{r_1} \cdots (n^{\log_k p_m + \varepsilon'})^{r_m} \\
&\leq (n^{\log_k (p_1+\varepsilon)})^{r_1} \cdots (n^{\log_k (p_m+\varepsilon)})^{r_m}, \qquad \text{and for sufficiently large } n, \\
&\qquad\qquad \varepsilon' \text{ and } \varepsilon \text{ may be chosen arbitrarily small,} \\
&\leq n^{\log_k ((p_1+\varepsilon)^{r_1} \cdots (p_m+\varepsilon)^{r_m})} \\
&< n^{\log_k (p_1^{s_1} \cdots p_m^{s_m})}, \quad \text{for sufficiently small } \varepsilon, \\
&= (n^{\log_k p_1})^{s_1} \cdots (n^{\log_k p_m})^{s_m} \\
&\leq \hat{p}_1^{s_1} \cdots \hat{p}_m^{s_m} \\
&= \hat{b}.
\end{aligned}$$

By the same argument, if $a > b$ then $\hat{a} > \hat{b}$. Of course if $a = b$ then $\hat{a} = \hat{b}$. This finishes the proof of the equivalence from condition 2.

For each requirement of the form 1 and 2 we can choose N such that for each $n \geq N$ this requirement is satisfied in $\mathcal{A}_n$. To end the proof let us observe that there is a finite number of such requirements to satisfy. Therefore, if we choose N such that in all models of cardinalities greater than such N the image of $\hat{}$ defines a submodel isomorphic to $\mathcal{A}_k$. $\square$

As an immediate corollary we obtain

Corollary 6.39 ([25]) *Let φ be a $\exists^*$ sentence.*

$$\varphi \text{ is satisfiable in } \mathrm{FM}(\mathcal{A}) \quad \text{if and only if} \quad \mathrm{FM}(\mathcal{A}) \models_{\mathrm{sl}} \varphi.$$

Let us recall that the rank of a term t, $rk(t)$ is the number of occurrences of function symbols in t. We call a term t simple if $rk(t) \leq 1$. A formula ψ is simple if all terms in ψ are simple. Of course, each $\exists^*$ formula is effectively equivalent to a simple $\exists^*$ formula.

We estimate below the size of a model from $\mathrm{FM}(\mathcal{A})$ in which a given $\exists^*$ sentence in a relational form is satisfied, provided that it is satisfied in $\mathrm{FM}(\mathcal{A})$ at all. This result, combined with corollary 6.39, gives the decidability of $\mathrm{sl}_{\exists^*}(\mathrm{FM}(\mathcal{A}))$.

Before stating the next lemma we introduce three functions which are needed to express the lemma and we list their properties which are used during the proof.

For all $n, k \in \omega$,

$$G(n) = \exp(2, 2^n 2^{\frac{2}{3}(4^n - 1)}),$$

$$g(n,k) = \exp(2, 2^{\frac{2}{3}(4^{n-k}(4^k - 1))}),$$

$$h(n,k) = \exp(2, 2^{2(n-k)}).$$

It is easy to observe that

$$g(n,k) = \exp(2, \prod_{i=1}^{i=k} 2(h(n,i))^2)$$

and

$$G(n) = g(n,n).$$

During the proof of the next lemma we use the following inequalities which hold between h and g:

$\sigma_1 :\ 2(h(n,k+1))^2 \leq h(n,k)$,

$\sigma_2 :\ g(n,k+1) \geq (g(n,k))^{h(n,k+1)}$,

$\sigma_3 :\ g(n,k+1) \geq (g(n,k))^{h(n,k+1)+1}$,

$\sigma_4 :\ g(n,k+1) \geq (g(n,k))^{2(h(n,k+1))^2}$.

They can be verified by an easy calculation. Each time we use one of σ_i's in the proof of the next lemma we mention it by indicating a proper condition.

Lemma 6.40 ([25]) *Let P_2 be the set of powers of 2. For all $a_1, \ldots, a_n$ with $1 < a_1 < \ldots < a_n$ there exist $b_1, \ldots, b_n \in P_2 \cap \{2, \ldots, G(n)\}$ such that for all $i, j, m, l \leq n$*

$$a_i a_j < a_m a_l \iff b_i b_j < b_m b_l.$$

Proof.

We prove by induction on $k \leq n$ the following:

$$\forall k \leq n \exists b_1, \ldots, b_k \in P_2 \cap \{2, \ldots, g(n,k)\} \forall t_1(x_1, \ldots, x_k), t_2(x_1, \ldots, x_k)$$

$$\{\textstyle\bigwedge_{i\in\{1,2\}} rk(t_i) \leq h(n,k) \Rightarrow$$

$$[t_1(a_1, \ldots, a_k) < t_2(a_1, \ldots, a_k) \iff t_1(b_1, \ldots, b_k) < t_2(b_1, \ldots, b_k)]\}.$$

For $k = n$ we obtain the thesis.

We consider the following formula:

$$\forall t_1(x_1, \ldots, x_k), t_2(x_1, \ldots, x_k)\{ \bigwedge_{i\in\{1,2\}} rk(t_i) \leq h(n,k) \Rightarrow \qquad (*)$$

$$[t_1(a_1, \ldots, a_k) < t_2(a_1, \ldots, a_k) \iff t_1(b_1, \ldots, b_k) < t_2(b_1, \ldots, b_k)]\}.$$

We show that for each $k \leq n$ one can find a sequence $b_1, \ldots, b_k \leq g(n,k)$ which satisfy (*). Let us observe that if $b_1, \ldots, b_k$ satisfy (*) then, for each $m \geq 1$, the sequence $b_1^m, \ldots, b_k^m$ also satisfies (*).

For $k = 1$ we put $b_1 = 2$. Now let us assume that there exist $b_1, \ldots, b_k \leq g(n,k)$ which satisfy (*) for $k < n$ and we find proper $c_1, \ldots, c_{k+1}$, possibly with $c_i \neq b_i$ for $i \leq k$. We consider two cases.

For the first, let us assume that there exist $w \geq 1$ and $t(x_1, \ldots, x_k)$, $t'(x_1, \ldots, x_k)$ such that $rk(t) + w, rk(t') \leq h(n, k+1)$ and

$$t(a_1, \ldots, a_k)a_{k+1}^w = t'(a_1, \ldots, a_k). \qquad (**)$$

Then the new sequence $c_1, \ldots, c_{k+1}$ must satisfy the equation

$$t(c_1, \ldots, c_k)c_{k+1}^w = t'(c_1, \ldots, c_k).$$

Let r be such that

$$2^r = \frac{t'(b_1, \ldots, b_k)}{t(b_1, \ldots, b_k)}.$$

If $w|r$ we set $c_i = b_i$ for $i \leq k$ and set c_{k+1} to $2^{\frac{r}{w}}$. If $w \not| r$ then, for $i \leq k$, we take $c_i = b_i^w$ and as c_{k+1} we put 2^r. Observe that in both cases $c_i \leq g(n, k+1)$ for $i \leq k+1$ (by σ_2), the sequence $c_1, \ldots, c_k$ satisfies (*) and $c_{i+1}^w = t'(\bar{c})/t(\bar{c})$. Now we argue that our choice of $c_1, \ldots, c_{k+1}$ is suitable.

Since $h(n,k)$ is decreasing in k it suffices to show that if $s(x_1, \ldots, x_k)$, $s'(x_1, \ldots, x_k)$ and u are such that $rk(s) + u \leq h(n, k+1)$ and $rk(s') \leq h(n, k+1)$ then

$$s(a_1, \ldots, a_k)a_{k+1}^u < s'(a_1, \ldots, a_k) \iff s(c_1, \ldots, c_k)c_{k+1}^u < s'(c_1, \ldots, c_k)$$

and

$$s'(a_1, \ldots, a_k) < s(a_1, \ldots, a_k)a_{k+1}^u \iff s'(c_1, \ldots, c_k) < s(c_1, \ldots, c_k)c_{k+1}^u.$$

We show only the first equivalence. Let

$$s(a_1, \ldots, a_k)a_{k+1}^u < s'(a_1, \ldots, a_k).$$

Then

$$(s(a_1, \ldots, a_k))^w a_{k+1}^{uw} < (s'(a_1, \ldots, a_k))^w$$

and, by (**),

$$(s(a_1, \ldots, a_k))^w (t'(a_1, \ldots, a_k))^u < (s'(a_1, \ldots, a_k))^w (t(a_1, \ldots, a_k))^u.$$

We need the fact that $rk(s^w t'^u), rk(s'^w t^u) \leq h(n,k)$. Indeed,

$$\begin{aligned} rk(s^w t'^u) &\leq rk(s)w + (w-1) + 1 + rk(t')(h(n,k+1) - rk(s)) + \\ &\qquad + (h(n,k+1) - rk(s) - 1) \\ &\leq rk(s)h(n,k+1) + h(n,k+1) + \\ &\qquad + h(n,k+1)(h(n,k+1) - rk(s)) + \\ &\qquad + (h(n,k+1) - rk(s) - 1) \\ &\leq h(n,k+1)h(n,k+1) + h(n,k+1) + h(n,k+1) \\ &\leq (h(n,k+1))^2 + 2h(n,k+1) \\ &\leq 2(h(n,k+1))^2 \\ &\leq h(n,k). \end{aligned}$$

The last inequality is simply the condition (σ_1). The reasoning for $rk(s'^w t^u) \leq h(n,k)$ is perfectly parallel. Thus, by (*) applied to $c_1, \ldots, c_k$ we have,

$$(s(c_1, \ldots, c_k))^w (t'(c_1, \ldots, c_k))^u < (s'(c_1, \ldots, c_k))^w (t(c_1, \ldots, c_k))^u$$

and, since $c_{k+1}^w = t'(\bar{c})/t(\bar{c})$,

$$(s(c_1, \ldots, c_k))^w c_{k+1}^{uw} < (s'(c_1, \ldots, c_k))^w.$$

We finally obtain that

$$s(c_1, \ldots, c_k) c_{k+1}^u < s'(c_1, \ldots, c_k).$$

For the converse implication let us observe that we can reverse all steps in the above reasoning. The second equivalence is proven similarly.

Now let us assume that there are no $w \geq 1, t(x_1, \ldots, x_k), t'(x_1, \ldots, x_k)$ such that $rk(t)+w, rk(t') \leq h(n,k+1)$ and $t(a_1, \ldots, a_k) a_{k+1}^w = t'(a_1, \ldots, a_k)$. Then let $(t_1, t'_1, w_1), \ldots, (t_m, t'_m, w_m)$ be the list of all triples such that $rk(t_i) + w_i \leq h(n,k+1), rk(t'_i) \leq h(n,k+1)$, $w_i \geq 1$ and

$$t_i(a_1, \ldots, a_k) a_{k+1}^{w_i} < t'_i(a_1, \ldots, a_k)$$

and let $(s_1, s'_1, u_1), \ldots, (s_r, s'_r, u_r)$ be the list of all triples such that $rk(s_j) \leq h(n,k+1), rk(s'_j) + u_j \leq h(n,k+1)$, $u_j \geq 1$ and

$$s_j(a_1, \ldots, a_k) < s'_j(a_1, \ldots, a_k) a_{k+1}^{u_j}.$$

We should define $c_1, \ldots, c_{k+1}$ in a way that preserves all of the above inequalities.

If the first list is empty, we define c_{k+1} as $b_k^{h(n,k+1)+1}$ and, for $i \leq k$, $c_i = b_i$. By σ_3 the new sequence satisfies (*). Otherwise, for $i \leq m$, let us define ν_i such that

$$2^{\nu_i} = t'_i(b_1, \ldots, b_k)/t_i(b_1, \ldots, b_k).$$

Next, for $j \geq r$, we define μ_j such that if $s_j(b_1, \ldots, b_k) \geq s'_j(b_1, \ldots, b_k)$ then

$$2^{\mu_j} = s_j(b_1, \ldots, b_k)/s'_j(b_1, \ldots, b_k)$$

and $\mu_j = 0$, otherwise.

For each $i \leq m, j \leq r$

$$(t_i(a_1, \ldots, a_k))^{u_j}(s_j(a_1, \ldots, a_k))^{w_i} a_{k+1}^{w_i u_j} < (t'_i(a_1, \ldots, a_k))^{u_j}(s'_j(a_1, \ldots, a_k))^{w_i} a_{k+1}^{w_i u_j}$$

and therefore

$$(t_i(a_1, \ldots, a_k))^{u_j}(s_j(a_1, \ldots, a_k))^{w_i} < (t'_i(a_1, \ldots, a_k))^{u_j}(s'_j(a_1, \ldots, a_k))^{w_i}.$$

Again, $rk(t_i^{u_j} s_j^{w_i}) \leq h(n,k)$ and $rk(t'^{u_j}_i s'^{w_i}_j) \leq h(n,k)$ so, by the inductive assumption, we obtain that

$$(t_i(b_1, \ldots, b_k))^{u_j}(s_j(b_1, \ldots, b_k))^{w_i} < (t'_i(b_1, \ldots, b_k))^{u_j}(s'_j(b_1, \ldots, b_k))^{w_i}$$

and

$$\left(\frac{s_j(b_1, \ldots, b_k)}{s'_j(b_1, \ldots, b_k)}\right)^{w_i} < \left(\frac{t'_i(b_1, \ldots, b_k)}{t_i(b_1, \ldots, b_k)}\right)^{u_j}.$$

Thus,

$$(2^{\mu_j})^{w_i} < (2^{\nu_i})^{u_j}$$

and

$$2^{\frac{\mu_j}{u_j}} < 2^{\frac{\nu_i}{w_i}}.$$

Finally, we obtain that for each $i \leq m$, $j \leq r$

$$\frac{\mu_j}{u_j} < \frac{\nu_i}{w_i}.$$

We may assume that $\frac{\mu_1}{u_1}$ is maximal of all the fractions $\frac{\mu_j}{u_j}$ and $\frac{\nu_1}{w_1}$ is minimal of all the fractions $\frac{\nu_i}{w_i}$. If $\frac{\mu_1}{u_1} + 1 < \frac{\nu_1}{w_1}$ then the sequence $c_i = b_i$ for $i \leq k$ and $c_{k+1} = 2^{\left\lceil \frac{\mu_1}{u_1} \right\rceil}$ satisfy all relevant inequalities. However, that choice of $c_1, \ldots, c_{k+1}$ would be impossible if $\frac{\mu_1}{u_1} + 1 \geq \frac{\nu_1}{w_1}$. In this case let us define, for $i \leq k$, c_i as $b_i^{2w_1u_1}$. Now for the sequence $c_1, \ldots, c_k$, we can define ν'_j and μ'_i exactly in the same way as we did for $b_1, \ldots, b_k$. So

$$2^{\nu'_i} = t'_i(c_1, \ldots, c_k)/t_i(c_1, \ldots, c_k).$$

and

$$2^{\mu'_j} = s_j(c_1, \ldots, c_k)/s'_j(c_1, \ldots, c_k).$$

Then $\mu'_j = 2\mu_j w_1 u_1$ and $\nu'_i = 2\nu_i w_1 u_1$. Since $\frac{\mu'_1}{2u_1}, \frac{\nu'_1}{2w_1}$ are natural numbers such that $\frac{\mu'_1}{2u_1} < \frac{\nu'_1}{2w_1}$, we have that $\frac{\mu'_1}{u_1} + 1 < \frac{\nu'_1}{w_1}$. Thus, we can take c_{k+1} as $2^{\frac{\mu'_1}{u_1}+1}$ (here we use σ_4). It is straightforward to check that the sequence $c_1, \ldots, c_{k+1}$ satisfies (*) for $k+1$. □

Finally we obtain the estimation of the size of a model from $\mathrm{FM}((\omega, \times, \leq))$ for a purely existential formulas given by Krynicki and Zdanowski in [25].

Theorem 6.41 ([25]) *Let* $F(n) = \exp(2, 2^{n+1}2^{\frac{2}{3}(4^{n+1}-1)}) + 1$ *and let* $\varphi \in \mathcal{F}_{\{\times,\leq\}}$ *be an* $\exists^*$ *sentence in a relational like form with all variables among* $x_1, \ldots, x_n$. *If* φ *is satisfiable in* $\mathrm{FM}((\omega, \times, \leq))$ *then it has a model in* $\mathrm{FM}((\omega, \times, \leq))$ *of cardinality not greater than* $F(n)$.

Proof. Let us observe that $F(n) = G(n+1) + 1$, where G is a function from lemma 6.40.

Let $\mathcal{A} = (\omega, \times, \leq)$ and let $a_1, \ldots, a_n$ be witnesses for φ in a model $\mathcal{A}_{a_{n+1}} \in \mathrm{FM}(\mathcal{A})$ such that $\mathcal{A}_{a_{n+1}} \models \varphi$. Then by lemma 6.40, we can find $b_1, \ldots, b_{n+1}$ not greater than $G(n+1)$ such that for all $i, j \leq n+1$,

$$a_i < a_j \iff b_i < b_j$$

and, for all $i, j, k, l \leq n+1$,

$$a_i a_j < a_k a_l \iff b_i b_j < b_k b_l.$$

Since φ is in a relational like form, $\mathcal{A}_{b_{n+1}} \models \varphi$ and $\mathrm{card}(\mathcal{A}_{b_{n+1}}) \leq F(n)$. □

Theorem 6.42 ([25]) $\mathrm{sl}_{\exists^*}(\mathrm{FM}((\omega, \times, \leq)))$ *is decidable.*

Proof. By theorem 6.41 the satisfability problem for $\exists^*$ formulas is decidable in $\mathrm{FM}((\omega, \times, \leq))$. But then corollary 6.39 states that satisfiability in $\mathrm{FM}((\omega, \times, \leq))$ is equivalent to being true in almost all models from $\mathrm{FM}((\omega, \times, \leq))$. □

6.5 Spectra of arithmetics in finite models

In this section we examine spectra of some arithmetics. Let us recall that by an FM($\mathcal{A}$)–spectrum of a sentence φ, $\mathrm{Spec}_{\mathrm{FM}(\mathcal{A})}(\varphi)$, we define the set of the cardinalities of the models in FM($\mathcal{A}$) in which φ is true and Spec(FM($\mathcal{A}$)) is the set of all FM($\mathcal{A}$)–spectra, see definition 3.13.

It is not difficult to describe the spectrum of FM($(\omega, +)$). Indeed, for each sentence $\varphi \in \mathcal{F}_{\{+\}}$ there is a formula $\varphi^*(y)$ constructed in lemma 6.1 such that

$$Spec(\varphi) = \{n + 1 : (\omega, +) \models \varphi^*[n]\}.$$

This shows that there is a strict relation between elements of $Spec$(FM($(\omega, +)$)) and the sets of natural numbers definable in $(\omega, +)$. The theorem of Ginsburg and Spanier (for a proof see [45]) states that the sets definable in the infinite model for arithmetic with addition are exactly the ultimately periodic sets.[3] In consequence, $Spec$(FM($(\omega, +)$)) is just the family of ultimately periodic sets. Moreover, it follows from [42] that this is also a spectrum of arithmetic with addition in the language with counting quantifiers.

There is also a classical characterization of the spectrum for arithmetic of addition and multiplication given by Wrathall in [54].

Theorem 6.43 ([54]) *$Spec$(FM($(\omega, +, \times)$)) is the family of sets in linear time hierarchy.*

In her paper [54] Wrathall proved the equivalence of linear time hierarchy and the class of rudimentary sets. However, the latter can be easily shown to be contained, and indeed equal, to Spec(FM($(\omega, +, \times)$).

FM($(\omega, +, \times)$) is IS–interpretable in FM($(\omega, \times)$) but, as we will see later, Spec(FM($(\omega, \times)$) $\subsetneq$ Spec(FM($(\omega, +, \times)$)). However, the spectrum of FM($(\omega, \times)$) is not computationally easier than the spectrum of FM($(\omega, +, \times)$).

Proposition 6.44 ([25]) *Let X belong to the spectrum of arithmetic with addition and multiplication. Then the set*

$$\{r : \exists n \in X((n-1)^2 + 1 \leq r < n^2 + 1)\}$$

belongs to the spectrum of arithmetic with multiplication.

Proof. Let $\mathcal{A} = (\omega, \times)$ and $\mathcal{N} = (\omega, +, \times)$. Let $\bar{\varphi}$ be the IS–interpretation of FM($\mathcal{N}$) in FM($\mathcal{A}$) from theorem 6.22. Then, by the form of the function

[3] A set $X \subseteq \omega$ is ultimately periodic if there are a positive integer p and a natural number a such that $\forall n \geq a(n \in X \iff n + p \in X)$.

f from theorem 6.22 ($f(n) = \lfloor\sqrt{n-1}\rfloor$), it follows that for any sentence $\psi \in \mathcal{F}_{\{+,\times,\mathrm{MAX}\}}$, if $X = \mathrm{Spec}_{\mathrm{FM}(\mathcal{B})}(\psi)$ then

$$\{r : \exists n \in X((n-1)^2 + 1 \leq r < n^2 + 1)\} = \mathrm{Spec}_{\mathrm{FM}(\mathcal{A})}(\widehat{I}_{\bar{\varphi}}(\psi)).$$

The last equality follows from the fact that, for each $r \geq 1$,

$$\begin{aligned}
r \in \mathrm{Spec}_{\mathrm{FM}(\mathcal{A})}(\widehat{I}_{\bar{\varphi}}(\psi)) &\iff \mathcal{A}_{r-1} \models \widehat{I}_{\bar{\varphi}}(\psi) \\
&\iff \mathcal{B}_{f(r-1)} \models \psi \\
&\iff f(r-1)+1 \in \mathrm{Spec}_{\mathrm{FM}(\mathcal{B})}(\psi) \\
&\iff \exists n \in \mathrm{Spec}_{\mathrm{FM}(\mathcal{B})}(\psi)\ n = f(r-1)+1 \\
&\iff \exists n \in \mathrm{Spec}_{\mathrm{FM}(\mathcal{B})}(\psi)\ n = \lfloor\sqrt{r-1}\rfloor + 1 \\
&\iff \exists n \in \mathrm{Spec}_{\mathrm{FM}(\mathcal{B})}(\psi)\ (n \leq \sqrt{r-1}+1 < n+1) \\
&\iff \exists n \in \mathrm{Spec}_{\mathrm{FM}(\mathcal{B})}(\psi)\ ((n-1)^2 \leq r-1 < n^2 \\
&\iff \exists n \in \mathrm{Spec}_{\mathrm{FM}(\mathcal{B})}(\psi)\ ((n-1)^2 + 1 \leq r < n^2 + 1.
\end{aligned}$$

□

The next proposition is a slightly improved version of proposition from Krynicki and Zdanowski [25]. In that paper the proposition was given only for the family $\mathrm{FM}((\omega, \times))$.

Proposition 6.45 *The set* $\mathrm{Par} = \{2n : n \in \omega\}$ *does not belong to* $\mathrm{Spec}(\mathrm{FM}((\omega, \times, \leq_P)))$*, where* $\leq_P$ *is the ordering restricted to the set of primes.*

Proof. Let $\mathcal{A} = (\omega, \times, \leq_P)$. We show that for any sentence $\psi \in \mathcal{F}_{\{\times,\leq_P,\mathrm{MAX}\}}$, there are arbitrarily large finite models $\mathcal{A}_n, \mathcal{A}_{n+1} \in \mathrm{FM}(\mathcal{A})$ such that

$$\mathcal{A}_n \models \psi \text{ if and only if } \mathcal{A}_{n+1} \models \psi. \qquad (*)$$

Let ψ be a sentence of quantifier rank k and let n be a prime such that there are $2^{k+1}+1$ primes in $\{\lceil n/2\rceil, \ldots, n-1\}$ (by fact 6.16 there are such arbitrarily large primes). Then

$$\mathcal{A}_n \equiv_k \mathcal{A}_{n+1}.$$

The strategy for Eros to win the k–moves game on $\mathcal{A}_n$ and $\mathcal{A}'_n$ consists of the following rules:

1. He maps maximal element of $\mathcal{A}_n$ to the maximal element of $\mathcal{A}_{n+1}$.

2. He plays the set $\{\lceil n/2 \rceil, \ldots, n-1\} \cap P$ in $\mathcal{A}_n$ and $\{\lceil n/2 \rceil, \ldots, n\} \cap P$ in $\mathcal{A}_{n+1}$ just like between two linear orderings.

3. On the remaining parts of both models he plays usining identity function.

□

It is also easy to observe that $\mathrm{Spec}(\mathrm{FM}((\omega, \times))) \subseteq \mathrm{Spec}(\mathrm{FM}((\omega, \leq_P)))$ since P is not in the former spectrum.

Now we are going to separate $\mathrm{Spec}(\mathrm{FM}((\omega, \exp)))$ from $\mathrm{Spec}(\mathrm{FM}((\omega, \times)))$.

Fact 6.46 ([25]) *The set $\{n^2+1 : n \in \omega\}$ is in the spectrum of multiplication.*

Proof. Let $X = \{n^2+1 : n \in \omega\}$. Then X is the spectrum of the following sentence φ:

$$\exists x(xx \neq \mathrm{MAX} \wedge \forall z(zz \neq \mathrm{MAX} \Rightarrow \varphi_{\leq}(z,x)) \wedge$$

$$\exists^{=2} w(ww = \mathrm{MAX} \wedge xw \neq \mathrm{MAX})).$$

In the first line of φ we state that x is the maximal element such that $xx \neq \mathrm{MAX}$. In the second line it is claimed that there are exactly two elements, say w_1, w_2, greater than x such that $xw_i \neq \mathrm{MAX}$. Thus, $w_1 = x+1$ and $w_2 = x+2$. We obtain that $x(x+2) < \mathrm{MAX}$ and $(x+1)^2 \geq \mathrm{MAX}$. Combining the two equalities we obtain

$$x^2 + 2x < \mathrm{MAX} \leq x^2 + 2x + 1.$$

It follows that

$$(\{0, \ldots, n\}, \times_n) \models \varphi \text{ if and only if } \exists k \geq 1 n = k^2.$$

But then the cardinality of the model is exactly k^2+1. □

Fact 6.47 *$\{n^2+1 : n \in \omega\}$ does not belong to the spectrum of arithmetic of exponentiation.*

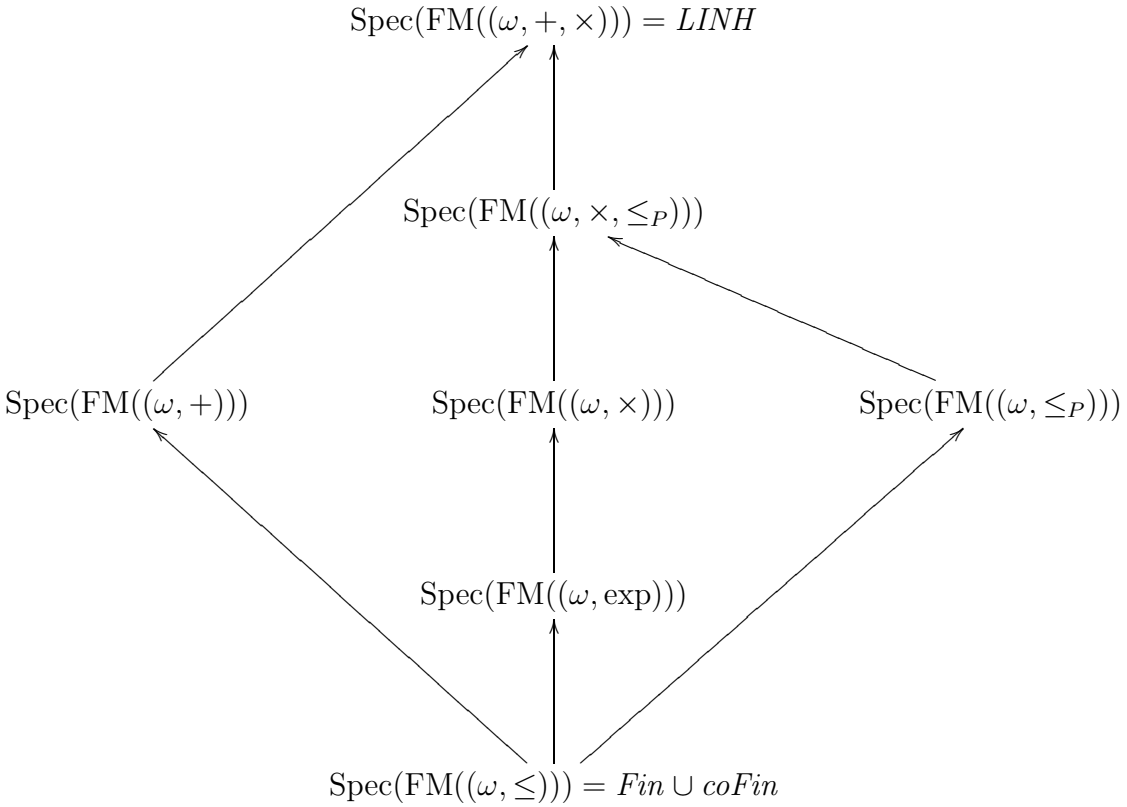
Proof. Let $\mathcal{B} = (\mathbf{N}, exp)$. By fact 6.46, to prove the thesis it suffices to show that there is no sentence φ of arithmetic with exponentiation such that for an arbitrary natural number n: $\mathcal{A}_{n^2-1} \not\models \varphi$ and $\mathcal{A}_{n^2} \models \varphi$. Indeed, let p be a "sufficiently large" prime number. Then p^2-1 behaves in

$\mathcal{B}_{p^2}$ in the same way as big prime numbers behave in models for multiplication. For all $x, y > 1$, $\exp(x, y) \neq p^2 - 1$ and both: $\exp(x, p^2 - 1)$ and $\exp(p^2 - 1, x)$ are greater than the maximal element of a model. Therefore, for all $x, y > 1$, if $\exp(x, y) \geq p^2 - 1$ then $\exp(x, y) \geq p^2$. It follows that we can play Ehrenfeucht–Fraïsse game between $\mathcal{B}_{p^2-1}$ and $\mathcal{B}_{p^2}$ treating $p^2 - 1$ in $\mathcal{B}_{p^2}$ like any other prime number from the upper half of $\mathcal{B}_{p^2}$. □

As a corollary we obtain the following.

Corollary 6.48 ([25]) $\mathrm{Spec}(\mathrm{FM}((\omega, \exp))) \subsetneq \mathrm{Spec}(\mathrm{FM}((\omega, \times)))$.

We can sum up presented relations in the following diagram where a path along the arrows indicates a proper inclusion and the lack of such a path indicates incomparability.



Pictrure 6.1. Inclusions between spectra of finite arithmetics.

Appendix A

Describing computations in finite models

In this appendix we present the proofs of theorems 4.1 and 4.4. We present them here because their proofs are quite tedious while their technical details do not affect our work. Readers familiar with the results of chapter 3 should have no difficulties with understanding them or just proving them by themselves.

As it was stated in sections 2.3 and 4.1 a Turing machine H is a tuple $(Q, \Sigma, \Gamma, \delta, q_S, q_A)$, where $Q = \{q_1, \ldots, q_n\}$ is a set of states of H, $q_S = q_1$ is a starting state, $q_A = q_2$ is an accepting state, $\Gamma = \{0, 1, \alpha, \beta\}$ and $\Sigma = \{0, 1\}$ are alphabets of the tape and of the machine, respectively, and $\delta\colon Q \times \Gamma \longrightarrow Q \times \Sigma \times \{L, S, R\}$ is a partial function called the transition function of H. We assume that the tape is unbounded to the right and that its leftmost square contains the character α which cannot be erased.

Now we will fix a coding of H by a finite word in a 10–letter alphabet $\{0, 1, \alpha, \beta, s, \#, \$, L, S, R\}$. For each transition of H, there is a tuple $(a, q_i, b, q_j, c) \in \Gamma \times Q \setminus \{q_A\} \times \Sigma \times Q \times \{L, S, R\}$ such that $\delta(a, q_i) = (b, q_j, c)$; we define its code as a word

$$\#a\#s^i\#b\#s^j\#c\#.$$

Let $e\colon \{0, \ldots, k\} \longrightarrow \Gamma \times Q \times \Sigma \times Q \times \{L, S, R\}$ be a fixed enumeration of all such codes for H. We can then describe H by a finite word of the form

$$\$\$\$s^n\$\$e(0)\$\ldots\$e(k)\$\$\$.$$

Let the word written on the tape by H during a computation of H be $u = u_1, \ldots, u_r$, with $u_1 = \alpha$, $u_i \in \Sigma$ for $1 < i < r$ and $u_r \in \Gamma$,[1] Then by a

[1]Only the last letter of u can be outside Σ since a machine can read the blank symbol

word

$$u_1 \dots u_{k-1} s^i u_k \dots u_r$$

we describe that the machine is in the state q_i and reads the square containing u_k. E.g. an initial configuration of the machine H on the input $w \in \{0,1\}^*$ is described by the word

$$\alpha s w.$$

If $C_1, \dots, C_N$ is a sequence of consecutive configurations during the computation of H with C_0 – a starting configuration and C_N – a final configuration then we describe the computation of H by a word

$$H\#\#C_0\# \dots \#C_N.$$

Now we can restate and prove lemma 4.1 from subsection 4.1.1.

Lemma A.1 *For each r there is an arithmetical formula* $\mathrm{Comp}(x,y)$ *such that for each code of a Turing machine H and for each $\bar{w} = w_1, \dots, w_r$, c and $n \geq c$ the following holds*

$$c \text{ is a computation of } H \text{ with an input } \bar{w} \iff \mathcal{N}_n \models \mathrm{Comp}[H, \mathrm{code}(\bar{w}), c],$$

where $\mathcal{N}_n \in \mathrm{FM}(\mathcal{N})$ and code *is the function which codes r-tuples (see an example of such a coding on page 23). In other words if $n \geq c$ then we can correctly represent the computation c in a finite model $\mathcal{N}_n$. Moreover, if $n < c$ then, for each $a \leq n$,*

$$\mathcal{N}_n \not\models \mathrm{Comp}[H, \mathrm{code}(\bar{w}), a].$$

Similarly, there is a formula $\mathrm{Accept}(x,y)$ *such that for each c and for each code H of a Turing machine and for each $n \geq c$,*

$$c \text{ is an accepting computation of } H \iff \mathcal{N}_n \models \mathrm{Accept}[H, c].$$

Proof. Although the lemma concerns the structure $\mathcal{N}$ in the proof we use the notions from arithmetic of words and we assume that the models are equipped with the concatenation operation. We can do this by the results of chapter 3 of the definability of concatenation in $\mathrm{FM}(\mathcal{N})$ (see theorem 3.27).

Let us recall the formula $s \mathrel{\mathring{=}} t$ from page 47 with the following property. For each n and a valuation $\bar{a}$ in FW^t_n, for all terms t, s,

$$\mathsf{FW}^t_n \models (s \mathrel{\mathring{=}} t)[\bar{a}] \text{ if and only if}$$

β when it moves its head to the right. We assume also that u always contains an input word.

$\mathsf{FW}^t \models (s = t)[\bar{a}]$ and values of t and s in FW^t are less or equal n.

Now we write several formulas which will be useful for us. The first one expresses the fact that H is a code of a Turing machine (for its description see below). Machine$(H) :=$

$$\exists u \in \{s\}^* \, \exists z \, \{H \mathrel{\hat{=}} \$\$\$u\$z\$\$\wedge$$

$$z \mathrel{\hat{=}} \$(\{\#\}\times\Gamma\times(Q\backslash\{ss\})\times\{\#\}\times\Sigma\times\{\#\}\times Q\times\{\#\}\times\{L,S,R\}\times\{\#\}\times\{\$\})^*\wedge$$

$$\forall y \in \{s\}^* \, (y \subseteq z \Rightarrow y \subseteq u)\wedge$$

$$\forall t_1 \, \forall t_2 \, \forall w[\$t_1\$ \subseteq z \wedge \$t_2\$ \subseteq z \wedge \$ \not\subseteq t_1 \wedge \$ \not\subseteq t_2 \wedge t_1 w t_2 \subseteq z \Rightarrow$$

$$\forall s_1 \, \forall s_2 \, \forall a_1 \, \forall a_2 \, (\#a_1\#s_1\# \preceq t_1 \wedge \#a_2\#s_2\# \preceq t_2 \Rightarrow a_1 \neq a_2 \vee s_1 \neq s_2)]\}.$$

The word u describes the number of states of the machine H and z is a word coding the transitions of H. The correct form of z is forced in the third line. The fourth line states that all states which appear in z are really states of H and the last line states that there are no repetitions in the transition function coded in z.

Then we write a formula which says that C is a word describing a temporary description of a computation of a Turing machine. GoodConf$(C) :=$

$$\exists u_1 \in \Sigma^* \, \exists u_2 \in \Sigma^* \, \exists w \in \{s\}^* \, (C \mathrel{\hat{=}} w\alpha u_1 u_2 \vee C \mathrel{\hat{=}} \alpha u_1 w u_2 \vee C \mathrel{\hat{=}} \alpha u_1 u_2 w\beta).$$

The disjunction in GoodConf(C) describes three possibilities which can occur during a computation: either the head of a machine reads the first symbol on the tape, α, or reads a symbol within the word written on the tape, or reads the blank symbol on the first of previously unvisited squares.

The next formula, InitConf(w, C) expresses that C is an initial configuration on the input w.

$$\text{InitConf}(w, C) := w \in \Sigma^* \wedge C \mathrel{\hat{=}} \alpha s w.$$

The last auxiliary formula states that two given configurations C, D of a machine H are the consecutive configurations of a computation of H. Next$(H, C, D) :=$

$$\text{GoodConf}(C) \wedge \text{GoodConf}(D)\wedge$$

$$\exists s_C \in \{s\}^* \, \exists s_D \in \{s\}^* \, (s_C \subseteq C \wedge s_C s \not\subseteq C \wedge s_D \subseteq D \wedge s_D s \not\subseteq D\wedge$$

$$\exists a \in \Gamma \, \exists b \in \Sigma \, \exists M \in \{L,S,R\} \, [s_C a \subseteq C \wedge \$a\$s_C\$b\$s_D\$M\$ \subseteq H \wedge \Psi]),$$

where Ψ is a disjunction of the following two formulas:

$$\exists w \, (C = s_C \alpha w \wedge ((M = S \wedge D = s_D \alpha w) \vee (M = R \wedge D = \alpha s_D w))),$$

$$\exists w_1\,\exists w_2\,\exists c_1 \in \Gamma\,\exists c_2 \in \Gamma\,\{C = w_1c_1s_Cc_2w_2 \wedge$$

$$((M = L \wedge D = w_1s_Dc_1bw_2) \vee (M = S \wedge D = w_1c_1s_Dbw_2) \vee$$

$$(M = R \wedge (w_2 \neq \lambda \Rightarrow D = w_1c_1bs_Dw_2) \wedge (w_2 = \lambda \Rightarrow D = w_1c_1bs_D\beta))]\}.$$

In the second line of $\mathrm{Next}(C, D)$ we find the states s_C and s_D of H in the configurations C and D, respectively. Then we find a character a which H reads in the configuration C and a tuple (a, s_C, b, s_D, M) describing a proper transition of H. The formula Ψ describes the relation between C and D depending on the form of the transition and the position of the head of H.

Finally, we can write a formula $\mathrm{Comp}(H, w, c)$ which states that c is a computation of H with the input w.

$$\mathrm{Machine}(H) \wedge \exists z\,\{c \doteq H\#z \wedge \exists z'(z \doteq \#z'\#) \wedge$$

$$\exists x\,\exists y\,[z \doteq \#x\#y \wedge \mathrm{InitConf}(H, w, x)] \wedge$$

$$\forall x_1 \forall x_2[(\#x_1\#x_2\# \subseteq z \wedge \bigwedge_{i\in\{1,2\}} \mathrm{GoodConf}(x_i)) \Rightarrow \mathrm{Next}(H, x_1, x_2)] \wedge$$

$$\exists x\,\exists y\,[z \doteq y\#x\# \wedge \mathrm{GoodConf}(x) \wedge \forall x'(\mathrm{GoodConf}(H, x') \Rightarrow \neg\mathrm{Next}(H, x, x'))]\}.$$

In the first line of $\mathrm{Comp}(H, w, c)$ we state that c begins with the code of the Turing machine H followed by $\#\#$. Moreover, we find a subword z of c which begins and ends with $\#$ and which is formed by removing from c a word consisting of the code of the Turing machine H and one $\#$. The word z should have the form $\#c_1\# \ldots \#c_j\#$, with $\# \not\subseteq c_i$ for $i \leq j$, where the consecutive c's are the consecutive configurations of H during the computation. This is stated in the third line of the formula. The second line forces c_1 to be an initial configuration of H and the fourth line establishes that c_j is a final configuration with no successor. All the above forces c to be the code of a computation of H with the input w. Moreover, since all the quantifiers in the above formulas could be bounded by c it follows that the formula $\mathrm{Comp}(H, w, c)$ correctly states that c is a computation of H whenever c appears in the finite model from $\mathrm{FM}(\mathcal{N})$.

It is relatively easy now to write a formula $\mathrm{Accept}(H, c)$ stating that c is an accepting computation of H. It has the form

$$\exists w \leq c\,\exists d \leq c\{\mathrm{Comp}(H, w, c) \wedge \mathrm{GoodConf}(H, d) \wedge \exists z(c \doteq z\#d\#) \wedge$$

$$s11s \subseteq d\}.$$

In the first line of the above formula we check that c is indeed a computation of H and we state that d is the last configuration of c. Then in the last line of Accept we check that H in this last configuration is in the accepting state

q_A which, by definition, is equal to q_2 and is coded by $s11s$. $\square$

Now we present lemma 4.4 from subsection 4.1.2. Let us recall that a family of relations $\{R_n\}_{n\in\omega}$, with $R_i \subseteq \{0,\ldots,n\}^r$, sl–approximates $R \subseteq \omega^r$ if for each m there is K such that whenever $k \geq K$ then R_k agrees with R on the set $\{0,\ldots,m\}$.

Lemma A.2 *Let A be an oracle set and let $\{A_n\}_{n\in\omega}$ be a family of finite relations which* sl*–approximates A. Then for each r there is an arithmetical formula* $\mathrm{OComp}(x,y,P)$ *such that for each Turing machine $H^?$ and for each c and $\bar{w} = w_1,\ldots,w_r$ there is N such that for all $n \geq N$ the following holds*

$$c \text{ is a } H^A\text{–computation with an input } \bar{w} \iff$$

$$(\mathcal{N}_n, A_n) \models \mathrm{OComp}[H^?, \mathrm{code}(\bar{w}), c, P],$$

where $(\mathcal{N}_n, A_n)$ is the n–th model from $\mathrm{FM}(\mathcal{N})$ *with an additional set A_n interpreting P.*

Moreover, there is the formula $\mathrm{Accept}(x,y)$ *which expresses that y is an accepting computation of x.*

Proof. Since the proof of this lemma is very similar to the proof of lemma A.1 we present only the description of necessary changes which should be made in the previous proof to obtain the proof of the present lemma.

First of all, the transition function of the machine with an oracle is more complex since it has to describe the moves of two heads. Then the notion of configuration should be changed to include the context of the oracle tape and the position on the second head.

The formulas $\mathrm{Machine}(H)$, $\mathrm{GoodConf}(C)$, $\mathrm{InitConf}(C)$ can be changed quite easily to fit in this new context. The formula $\mathrm{Next}(H,C,D)$ should be extended to handle also the oracle queries of H. That is, if w is a word written on the oracle tape, H is in the query state $q_?$ in a configuration C then the state s_D at the configuration D is determined by the answer of the oracle:

$$s_D = \begin{cases} s_{\mathrm{YES}} & \text{if } P(w), \\ s_{\mathrm{NO}} & \text{if } \neg P(w), \end{cases}$$

where P is an additional predicate whose denotation approximates, in a given finite model, an oracle set.

After such straightforward changes we obtain formulas which properly describe the computations of a given machine $H^?$ with the oracle A.

Now for a given $\bar{w}$, we should find N from the lemma. It suffices to observe that our formulas will correctly describe a computation c in a given

model $(\mathcal{N}_n, A_n)$ whenever $c \leq n$ and all oracle queries asked during the computation c are correctly decided by A_n. Thus, we should take such N that both conditions hold for all $n \geq N$. $\square$

Bibliography

[1] D. A. Mix Barrington, N. Immerman, and H. Straubing. On uniformity within NC^1. *Journal of Computer and System Science*, 41:274–306, 1990.

[2] J. L. Bell and A. B. Slomson. *Models and ultraproducts*. North Holland, 1971.

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

[4] W. Bés and D. Richard. Undecidable extensions of Skolem arithmetic. *Journal of Symbolic Logic*, 63(2):379–401, 1998.

[5] J. R. Büchi. Weak second–order arithmetic and finite automata. *Z. Math. Logik Grundl. Math.*, 6:66–92, 1960.

[6] Patrick Cegielski. Théorie élémentaire de la multiplication des entiers naturels. In *Model Theory and Arithmetic*, volume 890 of *Lecture Notes in Mathematics*, pages 44–89, 1981.

[7] E. Dahlhaus. Reduction to NP–complete problems by interpretations. In Rödding Börger and Hasenjaeger, editors, *Logic and machines: decision problems and complexity*, Lecture Notes in Computer Science 171, pages 357–365. Springer–Verlag, 1984.

[8] A. Dawar, K. Doets, S. Lindell, and S. Weinstein. Elementary properties of the finite ranks. *Mathematical Logic Quarterly*, 44:349–353, 1998.

[9] H.-D. Ebbinghaus and J. Flum. *Finite Model Theory*. Springer–Verlag, 1995.

[10] A. Ehrenfeucht. An application of games to completness problem for formalized theories. *Fundamenta Mathematicae*, 49:129–141, 1961.

[11] R. Fagin. Generalized first order spectra and polynomial–time recognizable sets. In *SIAM – AMS Proceedings*, volume 7, pages 43–73, 1974.

[12] M. Fitting. *Notes on Incompletness and Undecidability.* in manuscript, 1999. available at `http://comet.lehman.cuny.edu/fitting/bookspapers/unpublished.html`.

[13] R. Fraïsse. Sur quelques classifications des systèmes de relations. *Université d'Alger, Publications Scientifiques*, Serie A(1):35–182, 1954.

[14] K. Gödel. Über formal unentscheidbare Sätze der "Principia Mathematica" und verwandter Systeme. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.

[15] P. Hájek and P. Pudlák. *Metamathematics of First–Order Arithmetic.* Springer Verlag, 1993.

[16] K. Harrow. *Sub–elementary classes of functions and relations.* PhD thesis, New York University, 1973.

[17] W. Hodges. *Model theory.* Encyclopedia of mathematics and its applications. Cambridge University Press, 1993.

[18] N. Immerman. Relational queries computable in polynomial time. In *14th ACM STOC Symposium*, pages 147–152, 1982.

[19] N. Immerman. Languages which capture complexity classes. In *15th ACM STOC Symposium*, pages 347–354, 1983.

[20] N. Immerman. *Descriptive Complexity.* Springer Verlag, 1999.

[21] L. Kołodziejczyk. A finite model-theoretical proof of a property of bounded query classes within ph. *The Journal of Symbolic Logic*, 69:1105–1116, 2004.

[22] L. Kołodziejczyk. Truth definitions in finite models. *The Journal of Symbolic Logic*, 69:183–200, 2004.

[23] I. Korec. Definability of addition from multiplication and neighbourhood relation and some related results. In *Proceedings of the conference of analytic and elementary number theory, Vienna'96*, pages 137–148. Universät Wien, 1996.

[24] I. Korec. A list of arithmetical structures complete with respect to first–order definability. *Theoretical Computer Science*, 257:115–151, 2001.

[25] M. Krynicki and K. Zdanowski. Theories of arithmetics in finite models. *Journal of Symbolic Logic*, 70(1):1–28, 2005.

[26] T. Lee. Arithmetical definability over finite structures. *Mathematical Logic Quarterly*, 49:385–393, 2003.

[27] J. A. Makowsky and Y. B. Pnueli. Computable quantifiers and logics over finite structures. In M. Krynicki, M. Mostowski, and L. W. Szczerba, editors, *Quantifiers: Logics, Models and Computation, Volume I*, pages 313–357. Kluwer Academic Publishers, 1995.

[28] F. Maurin. The theory of integer multiplication with order restricted to prime numbers is decidable. *Journal of Symbolic Logic*, 62:123–130, 1997.

[29] A. Mostowski. On direct products of theories. *Journal of Symbolic Logic*, 17:1–31, 1952.

[30] A. Mostowski, R. M. Robinson, and A. Tarski. *Undecidable theories*. North Holland, 1953.

[31] M. Mostowski. On representing concepts in finite models. *Mathematical Logic Quarterly*, 47:513–523, 2001.

[32] M. Mostowski. On representing semantics in finite models. In A. Rojszczak†, J. Cachro, and G. Kurczewski, editors, *Philosophical Dimensions of Logic and Science*, pages 15–28. Kluwer Academic Publishers, 2003.

[33] M. Mostowski and A. Wasilewska. Arithmetic of divisibility in finite models. *Mathematical Logic Quarterly*, 50(2):169–174, 2004.

[34] M. Mostowski and K. Zdanowski. Coprimality in finite models. 2005. in manuscript.

[35] M. Mostowski and K. Zdanowski. FM–representability and beyond. In B. Cooper, B. Loewe, and L. Torenvliet, editors, *Proceedings of the conference Computability in Europe*, Lecture Notes in Computer Science. Springer, 2005. in printing.

[36] J. Mycielski. Analysis without actual infinity. *Journal of Symbolic Logic*, 46:625–633, 1981.

[37] J. Mycielski. Locally finite theories. *Journal of Symbolic Logic*, 51:59–62, 1986.

[38] M. B. Nathanson. *Elementary methods in number theory*. Springer, 2000.

[39] M. Presburger. Über die volständigkeit eines gewissen system der arithmetik ganzer zahlen, in welchem die addition als einzige operation hervortritt. In *C. R. 1er congrès des Mathématiciens des pays slaves, Varsovie*, pages 92–101, 1929.

[40] W. Quine. Concatenation as a basis for arithmetic. *Journal of Symbolic Logic*, 11:105–114, 1946.

[41] J. Robinson. Definability and decision problems in arithmetic. *Journal of Symbolic Logic*, 14:98–114, 1949.

[42] N. Schweikardt. *On the Expressive Power of First-Order Logic with Built-In Predicates*. PhD thesis, Johannes Gutenberg-Universität Mainz, 2001.

[43] A. L. Semenov. Logical theories of one–place functions on the set of natural numbers. *Izv. Akad. Nauk. SSSR ser. Mat.*, 47:623–658, 1983.

[44] T. Skolem. Über gewisse satzfunktionen in der arithmetik. *Skr. Norske Videnskaps–Akademie i Oslo*, 7:154–180, 1930.

[45] C. Smoryński. *Logical number theory I.* Springer, 1981.

[46] R. Smullyan. *Theory of formal systems.* Annals of Math. Stud. No. 47. Princeton Univ. Press, 1961.

[47] R. I. Soare. *Recursively enumerable sets and degrees.* Perspectives in Mathematical Logic. Springer, 1987.

[48] L. W. Szczerba. Interpretability of elementary theories. In Butts and Hintikka, editors, *Proceedings 15th ICALP 88*, Logic, foundations of mathematics and computability theory, pages 129–145. Reidel Publishing, 1977.

[49] L. W. Szczerba. Interpretaions with parameters. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 26:35–39, 1980.

[50] W. Szmielew and A. Tarski. Mutual interpretability of some essentially undecidable theories. In *Proceedings of the international congress of mathematicians, Cambridge Mass. 1950*, page 734. American Mathematical Society Providence, 1952.

[51] B. Trachtenbrot. The impossibility of an algorithm for the decision problem for finite domains. *Doklady Akademii Nauk SSSR*, 70:569–572, 1950. in russian.

[52] M. Vardi. Complexity of relational query languages. In *14th symposium on theory of computation*, pages 137–146, 1982.

[53] A. Woods. *Some problems in logic and number theory, and their connections*. PhD thesis, University of Manchester, 1981.

[54] C. Wrathall. Rudimentary predicates and relative computation. *SIAM Journal on Computing*, 7:194–209, 1978.

Index