# THEORIES OF ARITHMETICS IN FINITE MODELS

MICHAŁ KRYNICKI AND KONRAD ZDANOWSKI†

**Abstract.** We investigate theories of initial segments of the standard models for arithmetics. It is easy to see that if the ordering relation is definable in the standard model then the decidability results can be transferred from the infinite model into the finite models. On the contrary we show that the $\Sigma_2$–theory of multiplication is undecidable in finite models. We show that this result is optimal by proving that the $\Sigma_1$–theory of multiplication and order is decidable in finite models as well as in the standard model. We show also that the exponentiation function is definable in finite models by a formula of arithmetic with multiplication and that one can define in finite models the arithmetic of addition and multiplication with the concatenation operation.

We consider also the spectrum problem. We show that the spectrum of arithmetic with multiplication and arithmetic with exponentiation is strictly contained in the spectrum of arithmetic with addition and multiplication.

**§1. Introduction.** The world which is physically accessible for us is of a finite character. Even if our world is infinite we can experience only its finite fragments. The finite context occurs for example when we do a simple arithmetic of addition. To illustrate this let us try to add, using computer, two Fibonacci numbers: $F_{44} = 1\,134\,903\,170$ and $F_{45} = 1\,836\,311\,903$. The result obtained by one of the authors was $F_{46} = -1\,323\,752\,223$. This result was obtained using the programming language $C$ and the arithmetic on variables of type **int**. This overflow shows that our computer arithmetic is not the arithmetic of the standard model. Here we have only as many natural numbers, as the size of registers in our machine allows.

Our experience shows that infinite objects investigated in classical mathematics are only abstracts, which we do not meet in everyday live. Moreover, we can determine their properties only using finite proofs. Therefore, it is natural to think that to give a good description of our work we should concentrate on finite objects.

In our paper we investigate theories of finite initial segments of the standard model of arithmetic with various sets of primitive notions. Models under considerations have always finite universe but their cardinality is not bounded. One may say they are potentially infinite. In [13], Marcin Mostowski defined the concept of being true in sufficiently large finite models which is one of the basic

1991 *Mathematics Subject Classification.* Primary: 03C13, Secondary: 03C68, 68Q17.

*Key words and phrases.* finite models,arithmetic,definability, spectrum, complexity.

†During the preparation of this paper Konrad Zdanowski was supported by the Grant DFG LA630/10–2.

notions of our paper. In [14] he applied his idea to transform the classical results on nondefinability of truth to the context of finite models.

A similar idea was considered by Mycielski [17] (see also [18]). He showed how to reconstruct the analysis within the framework of the family of potentially infinite models. Although his results show how infinite objects can approximate the properties of the finite world, we show something opposite. Namely we show that some logical properties, as for example decidability or definability, are not preserved in finite structures.

In [21] Schweikardt considered theories of finite models of arithmetics. Some problems considered in [21] are complementary to the problems in our paper. Her definition of finite models for arithmetic is also slightly different than ours.

In the second section of the paper we introduce necessary notations and definitions. In the next section we show that some decidability results can be transferred from the standard infinite model to the finite models case. The main results of the fourth part are undecidability of the $\Sigma_2$–theory of arithmetic with multiplication and definability of exponentiation from multiplication in finite models. Here we prove also the undecidability of $\Sigma_2$–theory of arithmetic with exponentiation. In the fifth part we prove the optimality of the result in the fourth section. Namely, we prove that the $\Sigma_1$–theory of multiplication with ordering is decidable. In the next section we show that concatenation without ordering defines full arithmetic in finite models. The seventh section is devoted to the spectrum problem. Here we give a characterization of spectra of arithmetics with multiplication and exponentiation and describe their relation with the spectrum of full arithmetic.

**Acknowledgments.** We would like to thank Marcin Mostowski for discussions during the preparation of this paper and comments on the first draft. In particular his observation was the crucial argument in the proof of theorem 4.3. We want to thank also the members of Daniel Leivant's and Clemens Lautemann's seminars on which parts of this work were presented. In particular the second author thanks Nicole Schweikardt and Marcel Marquardt for a discussion of one problem from the paper. We also thank to Leszek Kołodziejczyk for allowing us to present his solution of one of the problem which arisen during the preparation of the paper. Finally, we specially thank to anonymous reviewer for numerous comments and corrections which greatly improved readability of the paper.

**§2. Basic definitions.** In this section we fix the notation and introduce the main concepts. We assume some background in a model theory and recursion theory. Any introductory textbooks, e.g. [8] and [23] should be sufficient.

By $\mathbf{N}$ we denote the set of natural numbers. By $\bar{n}$ we denote the numeral $n$. By $card(X)$ we denote the cardinality of $X$ and by $card(\mathcal{A})$, where $\mathcal{A}$ is a model, we denote the cardinality of the universe of $\mathcal{A}$. By $\lfloor a \rfloor$ and $\lceil a \rceil$ we denote the greatest integer $\leq a$ and the smallest integer $\geq a$, respectively. A logarithm without explicit base is always the logarithm with base 2. We use also a shorthand $\exists^{=1}$ for the quantifier "there exists exactly one element".

In this paper we will consider formulas of the first order logic. By $\Sigma_n$ we denote the set of formulas of a given vocabulary which begin with a block of

existential quantifiers and have $n-1$ alternations followed by a quantifier free formula. Similarly, $\varphi$ is in $\Pi_n$ if it begins with a block of universal quantifiers and has $n-1$ alternations followed by a quantifier free formula. We consider also the family of the bounded formulas denoted by $\Delta_0$. A formula is bounded if all quantifiers occurring in it are of the form $(Qx \leq t)$, where $Q \in \{\exists, \forall\}$ and $t$ is a term. Observe that according to our notation $\Sigma_0$ as well as $\Pi_0$ is not the same as $\Delta_0$. For a vocabulary $\theta$ by $\Sigma_n(\theta)$ and $\Delta_0(\theta)$ we denote the set of $\Sigma_n$-formulas and $\Delta_0$-formulas of the signature $\theta$. For a set of formulas $\mathcal{F}$, by $Bool(\mathcal{F})$ we denote the set of all boolean combinations of formulas from $\mathcal{F}$.

By $\Sigma_n^0$ and $\Pi_n^0$ we will denote the classes of relations in arithmetical hierarchy. A set is $\Delta_n^0$ if it is $\Sigma_n^0$ and $\Pi_n^0$. A set $R$ is $\Sigma_n^0$–hard if each set from $\Sigma_n^0$ is many–one reducible to $R$. A set $R$ is $\Sigma_n^0$–complete if it is $\Sigma_n^0$–hard and it belongs to $\Sigma_n^0$. For details of the above notions see [23].

For a given vocabulary $\sigma$ we write $\mathcal{F}_\sigma$ to denote the set of first order formulas in this vocabulary. Similarly, if $X$ is a set of predicates and functions (of known arities) we write $\mathcal{F}_X$ to denote the set of first order formulas with predicates and functions from $X$. E.g. $\mathcal{F}_{\{+\}}$ is the set of formulas with addition. Moreover, we always assume to have equality in our language.

In what follows, with each predicate we connect its intended meaning e.g. $+$ with addition, $\times$ with multiplication, etc. Therefore, we will not distinguish between the signature of the language (vocabulary) and relations in a model. The latter will be always either well known arithmetical relations or its finite models versions.

The rank of a formula $\varphi$, $rk(\varphi)$, is defined in a usual way, i.e. $rk(\varphi) = 0$ if $\varphi$ is atomic formula, $rk(\neg\varphi) = rk(\varphi)$, $rk(\varphi \wedge \psi) = max\{rk(\varphi), rk(\psi)\}$, and $rk(\exists x\varphi) = 1 + rk(\varphi)$.

By a rank of a term $t$, $rk(t)$ we mean a number of occurrences of function symbols in $t$. We call a term $t$ simple if $rk(t) \leq 1$. A formula $\psi$ is simple if all terms in $\psi$ are simple. Of course, each formula is effectively equivalent to a simple formula.

Let $\mathcal{A}$ be a model having as a universe the set of natural numbers, i.e. $\mathcal{A} = (\mathbf{N}, R_1, \ldots, R_s, f_1, \ldots, f_t, a_1, \ldots, a_r)$, where $R_1, \ldots, R_s$ are relations on $\mathbf{N}$, $f_1, \ldots, f_t$ are operations (not necessarily unary) on $\mathbf{N}$ and $a_1, \ldots, a_r \in \mathbf{N}$. We will consider finite initial fragments of these models. Namely, for $n \in \mathbf{N}$, by $\mathcal{A}_n$ we denote the following structure

$$\mathcal{A}_n = (\{0, \ldots, n\}, R_1^n, \ldots, R_s^n, f_1^n, \ldots, f_t^n, a_1^n, \ldots, a_r^n, n),$$

where $R_i^n$ is the restriction of $R_i$ to the set $\{0, \ldots, n\}$, $f_i^n$ is defined as

$$f_i^n(b_1, \ldots, b_{n_i}) = \begin{cases} f_i(b_1, \ldots, b_{n_i}) & \text{if } f(b_1, \ldots, b_{n_i}) \leq n \\ n & \text{if } f(b_1, \ldots, b_{n_i}) > n \end{cases}$$

and $a_i^n = a_i$ if $a_i \leq n$, otherwise $a_i^n = n$. We will denote the family $\{\mathcal{A}_n\}_{n \in \mathbf{N}}$ by $FM(\mathcal{A})$.

The signature of $\mathcal{A}_n$ is an extension of the signature of $\mathcal{A}$ by one constant. This constant will be denoted by $MAX$. We introduced it mainly for convenience reasons. In all theories we consider it will be definable.

Let $\varphi(x_1, \dots, x_p)$ be a formula and $b_1, \dots, b_p \in \mathbf{N}$. We say that $\varphi$ *is satisfied by* $b_1, \dots, b_p$ *in all finite models of* $FM(\mathcal{A})$ ($FM(\mathcal{A}) \models \varphi[b_1, \dots, b_p]$) if for all $n \geq max(b_1, \dots, b_p)$ $\mathcal{A}_n \models \varphi[b_1, \dots, b_p]$.

We say that $\varphi$ *is satisfied by* $b_1, \dots, b_p$ *in all sufficiently large finite models of* $FM(\mathcal{A})$, what is denoted by $FM(\mathcal{A}) \models_{sl} \varphi[b_1, \dots, b_p]$, if there is $k \in \mathbf{N}$ such that for all $n \geq k$ $\mathcal{A}_n \models \varphi[b_1, \dots, b_p]$.

When no ambiguity arises we will use $\models_{sl} \varphi[b_1, \dots, b_p]$ instead of $FM(\mathcal{A}) \models_{sl} \varphi[b_1, \dots, b_p]$.

Finally, a sentence $\varphi$ *is true in all finite models of* $FM(\mathcal{A})$ if $\mathcal{A}_n \models \varphi$ for all $n \in \mathbf{N}$. Similarly, a sentence $\varphi$ *is true in all sufficiently large finite models of* $FM(\mathcal{A})$ if there is $k \in \mathbf{N}$ such that for all $n \geq k$, $\mathcal{A}_n \models \varphi$.

Let $\mathcal{F}$ be a set of sentences of first order logic. By $Th_{\mathcal{F}}(\mathcal{A})$, where $\mathcal{A}$ is a model, we denote the set of all sentences from $\mathcal{F}$ true in $\mathcal{A}$. For a class of models $\mathcal{K}$, by $Th_{\mathcal{F}}(\mathcal{K})$ we denote the set of sentences from $\mathcal{F}$ true in all models from $\mathcal{K}$, that is $Th_{\mathcal{F}}(\mathcal{K}) = \bigcap_{\mathcal{A} \in \mathcal{K}} Th_{\mathcal{F}}(\mathcal{A})$.

By $sl_{\mathcal{F}}(FM(\mathcal{A}))$ we denote the set of sentences from $\mathcal{F}$ true in all sufficiently large finite models of $FM(\mathcal{A})$. So, we have

$$Th_{\mathcal{F}}(FM(\mathcal{A})) = \{\varphi \in \mathcal{F} \ : \forall n \in \mathbf{N} \ \mathcal{A}_n \models \varphi\},$$

$$sl_{\mathcal{F}}(FM(\mathcal{A})) = \{\varphi \in \mathcal{F} \ : \exists k \forall n \geq k \ \mathcal{A}_n \models \varphi\}.$$

When $\mathcal{F}$ is the set of all sentences of a given signature we will omit the subscript $\mathcal{F}$.

Our aim is to investigate the complexity of $Th_{\mathcal{F}}(FM(\mathcal{A}))$ and $sl_{\mathcal{F}}(FM(\mathcal{A}))$ for different models $\mathcal{A}$ and some special sets of sentences $\mathcal{F}$. We will also examine the representability problems for families of the form $FM(\mathcal{A})$.

The idea how to represent the relations on $\mathbf{N}$ in finite models was formulated in the article of Marcin Mostowski [13]. He defined there the notion of $FM$-representability. Relation $R \subseteq \mathbf{N}^r$ is $FM$–representable in $FM(\mathcal{A})$ if and only if there exists a formula $\varphi(x_1, \dots, x_r)$ such that for all $a_1, \dots, a_r \in \mathbf{N}$,

$$(a_1, \dots, a_r) \in R \text{ if and only if } FM(\mathcal{A}) \models_{sl} \varphi[a_1, \dots, a_r]$$

and

$$(a_1, \dots, a_r) \notin R \text{ if and only if } FM(\mathcal{A}) \models_{sl} \neg\varphi[a_1, \dots, a_r].$$

For the theory of finite models of arithmetic with addition and multiplication we have the following theorem.

THEOREM 2.1 ([13]). *Let $\mathcal{A}$ be the standard model of arithmetic with addition and multiplication. Relation $R \subseteq \mathbf{N}^r$ is $FM$–representable in $FM(\mathcal{A})$ if and only if $R$ is in $\Delta^0_2$.*

One can characterize the relations in $\Delta^0_2$ as those which are decidable by a Turing machine with recursively enumerable oracle (see e.g. [23]).

Later, Mostowski and Zdanowski in [16] proved that for the standard model of arithmetic $(\mathbf{N}, +, \times)$ the set $sl(FM((\mathbf{N}, +, \times)))$ is $\Sigma^0_2$–complete. We will show the same for arithmetic with multiplication only.

**§3. Decidable theories of finite arithmetics.** As we mentioned each considered infinite structure $\mathcal{A}$ has as a universe the set of natural numbers. So, $(\mathcal{A}, <)$ denotes the structure $\mathcal{A}$ extended by the usual ordering on $\mathbf{N}$. We start with the following general fact.

LEMMA 3.1. *For every formula $\varphi(x_1, \dots, x_k)$ of the language of $FM(\mathcal{A})$ there is a formula $\varphi^*(x_1, \dots, x_k, y)$ of the language of $(\mathcal{A}, <)$, where $y$ is a new variable, such that for each $n \in \mathbf{N}$ and $a_1, \dots, a_k \leq n$,*

$$\mathcal{A}_n \models \varphi[a_1, \dots, a_k] \text{ if and only if } (\mathcal{A}, <) \models \varphi^*[a_1, \dots, a_k, n].$$

*Moreover, $\varphi^*$ is a $\Delta_0$–formula.*

PROOF. A translation procedure is defined by the induction on the complexity of $\varphi$. First we replace each occurrence of $MAX$ in $\varphi$ by a variable which does not occur in $\varphi$, say $y$. Then, let $f$ be a function in the structure $\mathcal{A}$. We define in $\mathcal{A}$ the graph of the corresponding function from a finite structure by the following formula: $(F(x_1, \dots, x_k) = x_0 \wedge x_0 \leq y) \vee (F(x_1, \dots, x_k) \geq y \wedge x_0 = y)$. In a similar way we define relations from a finite structure. This gives us the starting point of the translation procedure. The rest of this procedure is standard. ⊣

Let $\forall\Delta_0$ ($\exists\forall\Delta_0$) denote the set of sentences of the form $\forall x\varphi$ ($\exists x\forall y\varphi$), where $\varphi$ is a $\Delta_0$ formula. From the last lemma we can conclude the following

PROPOSITION 3.2. *a) If $Th_{\forall\Delta_0}((\mathcal{A}, <))$ is decidable then $Th(FM(\mathcal{A}))$ is decidable.*

*b) If $Th_{\exists\forall\Delta_0}((\mathcal{A}, <))$ is decidable then $sl(FM(\mathcal{A}))$ is decidable.*

PROOF. It follows immediately from the lemma 3.1 that for arbitrary sentence $\varphi$ of the language $FM(\mathcal{A})$ we have:

$$\text{for all } n \in \mathbf{N}\,,\ \mathcal{A}_n \models \varphi \quad \text{if and only if} \quad (\mathcal{A}, <) \models \forall y\varphi^*,$$

where $\varphi^*$ is a formula from lemma 3.1.

Similarly,

$$\models_{sl} \varphi[a_1, \dots, a_n] \text{ if and only if } (\mathcal{A}, <) \models \exists z\forall y > z\varphi^*[a_1, \dots, a_n].$$

Therefore, the decidability of $Th(FM(\mathcal{A}))$ and $sl(FM(\mathcal{A}))$ follows from the decidability of $Th_{\forall\Delta_0}((\mathcal{A}, <))$ and of $Th_{\exists\forall\Delta_0}((\mathcal{A}, <))$, respectively. ⊣

As a corollary we obtain the following

COROLLARY 3.3. *Assume that $Th((\mathcal{A}, <))$ is decidable. Then $Th(FM(\mathcal{A}))$ and $sl(FM(\mathcal{A}))$ are decidable.*

From the lemma 3.1 follows also the following observation.

PROPOSITION 3.4. *a) Every relation FM–representable in $FM(\mathcal{A})$ is definable in $(\mathcal{A}, <)$.*

*b) If $Th((\mathcal{A}, <))$ is decidable then each FM–representable relation in $FM(\mathcal{A})$ is recursive.*

*c) If the standard ordering is definable in $\mathcal{A}$ and $Th(\mathcal{A})$ admits elimination of quantifiers then $sl(FM(\mathcal{A}))$ also admits elimination of quantifiers.*

In the proof of the point $c$) we use the fact that for each quantifier free formula $\varphi(\bar{x})$ and for each tuple $\bar{a}$ the following equivalence holds:

$$FM(\mathcal{A}) \models_{sl} \varphi[\bar{a}] \text{ if and only if } \mathcal{A} \models \varphi[\bar{a}].$$

Well known classical results allow to deduce from corollary 3.3 that theories $Th(FM((\mathbf{N},+)))$, $sl(FM((\mathbf{N},+)))$ are decidable. By the same way, using the result of Semenov in [22], we can deduce that for an arbitrary natural number $n$ theories $Th(FM((\mathbf{N},+,n^x)))$ and $sl(FM((\mathbf{N},+)))$ are decidable. Also results contained in [5], [22], [11] and [4] provide a large set of examples of theories of arithmetics decidable in finite models.

**§4. Undecidable theories of arithmetic in finite models.** In the present section we are going to describe the properties of a theory which has greater expressive power in finite models than in the standard case. We focus our attention to arithmetic with multiplication. Later we show that, contrary to the standard case, the exponentiation function (i.e. function $\exp(x,y) = x^y$) is definable in finite models from multiplication.[1]

Let us observe that in a finite model for arithmetic of multiplication the formula $\forall z(xz = x)$ defines zero and the formula $x \neq 0 \wedge \forall z \neq 0(xz = x)$ defines the maximal element (assuming that a model has at least 3 elements). Similarly we can define zero and the maximal element in arithmetic with exponentiation by formulas $\exp(x,x) \neq x \wedge \forall z \neq x(\exp(x,z) = x)$ and $x \neq 0 \wedge \forall z \neq 0(\exp(x,z) = x) \wedge \exp(x,0) \neq x$ (in the latter case assuming that a model has at least 3 elements).

Now our basic structures, everywhere denoted by $\mathcal{A}$ or $\mathcal{B}$, will be the standard model for arithmetic with addition and multiplication $(\mathbf{N},+,\times)$, the standard model for arithmetic with multiplication, $(\mathbf{N},\times)$, or the model with the exponentiation function, $(\mathbf{N},\exp)$. It will be always clear which one is considered.

First let us present the formula with multiplication defining the ordering relation on an initial segment of a given model $\mathcal{A}_n \in FM((\mathbf{N},\times))$. It has the form

$$\varphi_<(x,y) \;:=\; \exists z\ (zx \neq MAX \wedge zy = MAX).$$

We shall prove that the relation defined in this way is the standard ordering relation on an initial segment of the model $\mathcal{A}_n$. Moreover, we can define in the uniform way an initial segment of the structure $\mathcal{A}_n$ on which $\varphi_<$ defines the usual ordering.

LEMMA 4.1. *Let $a,b \in |\mathcal{A}_n|$ be such that $a^2, b^2 < n$. Then, $\mathcal{A}_n \models \varphi_<[a,b]$ if and only if $a < b$.*

PROOF. The implication from left to right is obvious. For the converse let us assume that $a < b$. Thus we can choose $k \in |\mathcal{A}_n|$ to be the smallest element of $\mathcal{A}_n$ such that $kb \geq n$. Since $b^2 < n$, $k$ must be greater than $b$. It follows that $n > (k-1)b = (kb-b) > (kb-k) = k(b-1) \geq ka$. Therefore $\mathcal{A}_n \models \exists z(zb = MAX \wedge za \neq MAX)$. ⊣

[1] We assume the convention that $\exp(0,0) = 1$.

It follows that the formula $xx \neq MAX$ defines an initial segment of $\mathcal{A}_n$ in which the formula $\varphi_<(x,y)$ defines the standard ordering.

From lemma 4.1 we get also the following

FACT 4.2. *For each $a, b \in \mathbf{N}$, $a < b$ if and only if $\models_{sl} \varphi_<[a,b]$.*

Now, we are going to show that the theory of sufficiently large finite models for multiplication has the same expressive power in sufficiently large finite models as arithmetic with addition and multiplication. For this aim we will present an interpretation of a model of cardinality $n$ for addition and multiplication in models for multiplication only of cardinalities between $(n-1)^2+1$ and $n^2$.

THEOREM 4.3. *For each formula $\varphi(x_1, \ldots, x_k) \in \mathcal{F}_{\{+,\times\}}$, there is a formula $\psi(x_1, \ldots, x_k) \in \mathcal{F}_{\{\times\}}$ with the same free variables as in $\varphi(x_1, \ldots, x_k)$ such that for each $a_1, \ldots, a_k \in \mathbf{N}$,*

$$\models_{sl} \varphi[a_1, \ldots, a_k] \text{ if and only if } \models_{sl} \psi[a_1, \ldots, a_k].$$

PROOF. To prove the theorem we need the following lemma.

LEMMA 4.4. *Let $\mathcal{A} = (\mathbf{N}, +, \times)$ and $\mathcal{B} = (\mathbf{N}, \times)$. There are formulas $\varphi_U(x)$, $\varphi_+(x,y,z)$, $\varphi_\times(x,y,z)$, $\varphi_0(x)$ and $\varphi_{MAX}(x)$ in the language of arithmetic with multiplication which define in a model $\mathcal{B}_r$ the model isomorphic to a model $\mathcal{A}_n$, whenever $n \geq 1$ and $r$ are such that $(n-1)^2 + 1 \leq r \leq n^2$. Moreover, the isomorphism function $f : |\mathcal{A}_n| \longrightarrow |\mathcal{B}_r|$ is as follows $f(a) = \begin{cases} a & \text{if } a < n \\ r & \text{if } a = n. \end{cases}$*

PROOF OF LEMMA 4.4. We will construct the formulas from the lemma. As a formula $\varphi_U(x)$ defining the universe of the model we take $x^2 \neq MAX \vee x = MAX$. The form of the isomorphism function forces us to take for $\varphi_0(x)$ and $\varphi_{MAX}(x)$ the formulas $x = 0$ and $x = MAX$. For the formula $\varphi_\times(x,y,z)$ we take $(xy = z \wedge z^2 \neq MAX) \vee ((xy)^2 = MAX \wedge z = MAX)$. Finally, we use results of Troy Lee from [12] stating that addition is definable in finite structures with multiplication and ordering. So, to write $\varphi_+(x,y,z)$ we take the appropriate formula from [12] defining addition from multiplication and ordering. ⊣

A straightforward consequence of the lemma 4.4 is the following.

LEMMA 4.5. *Let $\mathcal{A} = (\mathbf{N}, +, \times)$ and $\mathcal{B} = (\mathbf{N}, \times)$. For each formula $\varphi(\overline{x}) \in \mathcal{F}_{\{+,\times\}}$, there is a formula $\psi(\overline{x}) \in \mathcal{F}_{\{\times\}}$ with the same free variables as $\varphi(\overline{x})$, i.e. $\overline{x} = (x_1, \ldots, x_k)$ such that for each $a_1, \ldots, a_k \in \mathbf{N}$, and for each $n, r$ such that $\max\{a_1, \ldots, a_k\} < n$ and $(n-1)^2 + 1 \leq r \leq n^2$*

$$\mathcal{A}_n \models \varphi[a_1, \ldots, a_k] \text{ if and only if } \mathcal{B}_r \models \psi[a_1, \ldots, a_k].$$

Now, to prove the theorem 4.3 it suffices to take as $\psi$ the formula from the lemma 4.5. ⊣

As a consequence of the above results and the undecidability result from [13] we have that $sl((\mathbf{N}, \times))$ is undecidable. In what follows we are going to estimate $n$ such that $\Sigma_n$ theory of multiplication in finite models is undecidable.

Firstly, let us observe that for a model $\mathcal{B}_n \in FM(\mathcal{B})$, where $\mathcal{B} = (\mathbf{N}, \times)$, we can define the ordering relation on $\{0, \ldots, \lfloor\sqrt{n-1}\rfloor\}$ – segment of $\mathcal{B}_n$ by a $\Sigma_1$

as well as by a $\Pi_1$ formula. The $\Sigma_1$ formula $\exists z(xz \neq MAX \wedge yz = MAX)$ was given before. The corresponding $\Pi_1$ formula has the form

$$\forall z(xz = MAX \Rightarrow yz = MAX) \wedge x \neq y.$$

We have the fact analogous to lemma 4.1

LEMMA 4.6. *Let $\mathcal{A} = (\mathbf{N}, \times)$ and let $a, b \in |\mathcal{A}_n|$ be such that $a^2, b^2 < n$. Then, $\mathcal{A}_n \models \forall z(xz = MAX \Rightarrow yz = MAX \wedge x \neq y)[a, b]$ if and only if $a < b$.*

The proof of the last lemma is similar to the proof of lemma 4.1.

Therefore, if the conditions $a^2, b^2 < MAX$ are satisfied we may freely choose a $\Sigma_1$ or $\Pi_1$ formula to express the fact that $a < b$. In what follows we will write $\varphi_<(x, y)$ with the assumption that it has a $\Sigma_1$ or $\Pi_1$ form depending on what we need.

Now, let us consider a formula stating that $y$ is the successor of $x$ in the standard ordering of $\{0, \ldots, \lfloor\sqrt{n-1}\rfloor\}$. It has the form

$$\varphi_S(x, y) := \varphi_<(x, y) \wedge \forall z(\varphi_<(x, z) \wedge z \neq y \Rightarrow \varphi_<(y, z)).$$

Using the $\Pi_1$ and $\Sigma_1$ forms of the formula $\varphi_<$ we can write $\varphi_S$ as a $\Pi_1$ formula.

We have the following

THEOREM 4.7. *a) The set of $\Sigma_2$ sentences of arithmetic of multiplication which are satisfiable in finite models is $\Sigma_1^0$–complete.*

*b) The set of $\Sigma_2$ sentences of arithmetic of multiplication which are true in all sufficiently large finite models is $\Sigma_1^0$–hard.*

PROOF. First, let us remind the Tarski's identity. For each natural numbers $x, y$ and $z \neq 0$

$$x + y = z \quad \text{if and only if} \quad (xz + 1)(yz + 1) = z^2(xy + 1) + 1.$$

It follows that we can define addition in arithmetic with multiplication and successor function by a $\Sigma_1$ as well as by a $\Pi_1$ formula.

Let $D$ be the set of sentences of the form $\exists \bar{x}(f(\bar{x}) = g(\bar{x}))$ where $f, g$ are polynomials with coefficients in $\mathbf{N}$.

By *MDRP* (Matijasevič, Davis, Robinson, Putnam) theorem, see [6], the problem whether a given $\varphi \in D$ is true in the standard model is $\Sigma_1^0$–complete. We will give the reduction of this problem to the problems mentioned in the theorem.

Let $\varphi \in D$. We can construct a sentence $\exists y_1 \ldots y_k \psi$ such that it is equivalent to $\varphi$ in the standard model of arithmetic and $\psi$ is a conjunction of atomic formulas of the form: $w_i w_j = w_l$, $S(w_i) = w_j$ or $w_i = w_j$, where $w_i, w_j, w_l$ are variables or the constant 0. Such construction is possible by Tarski's identity and some logical transformations.

Now, when we replace subformulas of $\psi$ of the form $S(x) = y$ with $\varphi_S(x, y)$ we get $\gamma \in \Pi_1$ in the language of $FM((\mathbf{N}, \times))$ such that the following statements are equivalent:

(*i*) $(\mathbf{N}, \times, S) \models \exists y_1 \ldots y_k \psi$,
(*ii*) $FM((\mathbf{N}, \times)) \models_{sl} \exists y_1, \ldots, y_k(\bigwedge_{i \leq k} y_i^2 \neq MAX \wedge \gamma)$,
(*iii*) $\exists y_1, \ldots, y_k(\bigwedge_{i \leq k} y_i^2 \neq MAX \wedge \gamma)$ is satisfiable in $FM((\mathbf{N}, \times))$.

It suffices to prove only the implication from $(i)$ to $(ii)$ and from $(iii)$ to $(i)$.

If $(i)$ holds and $a_1, \ldots, a_k$ are witnesses for $\psi$ then in each model $\mathcal{A}_n$, where $n > (max_{i\leq k} a_i)^2$, the same sequence will witness for $\exists y_1, \ldots, y_k(\bigwedge_{i\leq k} y_i^2 \neq MAX \wedge \gamma)$.

Similarly, if $(iii)$ holds with $a_1, \ldots, a_k$ as witnesses for $y_1, \ldots, y_k$ then the condition $\bigwedge_{i\leq k} y_i^2 \neq MAX$ assures that $a_1, \ldots, a_k$ are also good witnesses for $\psi$ in the standard model.

The above equivalences show that the set of $\Sigma_2$ sentences of arithmetic of multiplication which are satisfiable in finite models as well as the set $sl(FM(\mathcal{A}))$ are $\Sigma_1^0$-hard. On the other hand the set of $\Sigma_2$ sentences of arithmetic of multiplication which are satisfiable in finite models is in $\Sigma_1^0$. $\dashv$

When we do not restrict the quantifier depth of sentences of $FM((\mathbf{N}, \times))$ we can give a more precise characterization of $sl(FM((\mathbf{N}, \times)))$, see theorem 4.11.

In section 5 we will show that the above result is optimal, see theorem 5.6.

Now, let us turn to the arithmetic with exponentiation. By $\mathcal{A}$ we will denote the structure $(\mathbf{N}, \exp)$ and by $\mathcal{B}$ the structure $(\mathbf{N}, \times)$.

It is well known that in the model $(\mathbf{N}, \exp)$ the addition and multiplication can be defined. So, in the case of the standard arithmetic, exponentiation is as strong as addition and multiplication. It was showed by Bennett in [3] that the graph of the exponentiation function is $\Delta_0$ definable from addition and multiplication (for the proof see [9]). Basing on this result one can construct a formula which, for each $n$, defines the graph of the exponentiation function in a finite model $\mathcal{B}_n$. Here, we show that in finite models the exponentiation function is definable from sole multiplication.

It can be observed (compare [21], section 2.4.2) that if $p$ and $q$ are prime numbers and $\frac{n}{2} < p < q < n$ then there is an automorphism $h$ of $\mathcal{B}_n$, such that $h(p) = q$. So, primes $p$ and $q$ are indiscernible in $\mathcal{B}_n$. This implies that it is not possible to define the ordering relation in finite models of arithmetic with multiplication only. Therefore, our result shows that, contrary to the standard case, in finite models, exponentiation is strictly weaker than addition and multiplication. Indeed, as we will see, exponentiation in finite models is even strictly weaker than sole multiplication.

THEOREM 4.8. *Let $\mathcal{A} = (\mathbf{N}, \exp)$ and $\mathcal{B} = (\mathbf{N}, \times)$. There exists a formula $\varphi_{\exp}(x, y, z) \in \mathcal{F}_{\{\times\}}$ such that, for each $n$, $\varphi_{\exp}$ defines in $\mathcal{B}_n$ the graph of the exponentiation function from $\mathcal{A}_n$.*

PROOF. By the remark preceding the theorem concerning the Bennett result, and by the fact that we can define addition from multiplication on the initial segment of a model $\mathcal{B}_n$ determined by $\lfloor\sqrt{n-1}\rfloor$, it follows that there is a formula $\psi_e(x, y, z)$ such that $\psi_e$ defines the graph of the exponentiation function on $\{0, \ldots, \lfloor\sqrt{n-1}\rfloor\}$ – fragment of a given model $\mathcal{B}_n$. Thus, we show how to extend the definition of the exponentiation function on the whole model $\mathcal{B}_n$. It is straightforward to check that for each $n < 10$ we can find a formula defining in $\mathcal{B}_n$ the graph of the exponentiation function from $\mathcal{A}_n$. So, let us assume that $n \geq 10$. The idea of the construction of $\varphi_{\exp}(x, y, z)$ is based on the following. If $y^2 \geq n \geq 10$ and $x \geq 2$, then $x^y \geq n$ and it suffices to check whether $z = n$. Otherwise, $y$ is in the segment on which we can define arithmetic in

$\mathcal{B}_n$ and we can find $w_1$ and $w_2$ such that $y = 2w_1 + w_2$ with $w_2 < 2$ Then, we compute $\exp(x, w_1) = u$. If the result does not lie in $\{0, \dots, \lfloor\sqrt{n-1}\rfloor\}$, then $\exp(x, y) \geq n$ and it suffices to check if $z = n$. Otherwise, we finish the computation of $\exp(x, y)$ by multiplying $u^2 x^{w_2}$. Since $w_2 < 2$ the latter can be described by a first order formula.

So, we define a formula $\varphi_{\exp}(x, y, z)$ as a disjunction of the following two formulas $\varphi_1(x, y, z)$ and $\varphi_2(x, y, z)$:

$$\begin{aligned}
\varphi_1(x,y,z) &= (y = 0 \wedge z = 1) \vee (x = 0 \wedge y \neq 0 \wedge z = 0) \vee (x = 1 \wedge z = 1) \vee \\
&\quad (y^2 = MAX \wedge x \neq 0 \wedge x \neq 1 \wedge z = MAX), \\
\varphi_2(x,y,z) &= y^2 \neq MAX \wedge y \neq 0 \wedge y \neq 1 \wedge x \neq 0 \wedge x \neq 1 \wedge \\
&\quad \exists w_1 \exists w_2 \{\varphi_+(2w_1, w_2, y) \wedge w_2 < \overline{2} \wedge \\
&\quad [\exists u(u^2 \neq MAX \wedge \psi_e(x, w_1, u) \wedge \\
&\quad ((w_2 = \overline{0} \wedge z = u^2) \vee (w_2 = \overline{1} \wedge z = u^2 x)) \vee \\
&\quad \neg\exists u(u^2 \neq MAX \wedge \psi_e(x, w_1, u) \wedge z = MAX)]\}.
\end{aligned}$$

As we can see $\varphi_1$ handles all the easy cases and $\varphi_2$ describes the most difficult case. It is easy to verify that $\varphi_{\exp}$ defines the exponentiation function from a model $\mathcal{A}_n$ whenever $n \geq 10$. ⊣

However, it can be mentioned that with respect to sufficiently large finite models, exponentiation have the same expressive power as arithmetic with addition and multiplication. Namely, we have an analogue of lemma 4.4

LEMMA 4.9. *Let $\mathcal{A} = (\mathbf{N}, \exp)$ and $\mathcal{B} = (\mathbf{N}, \times)$. There are formulas $\varphi_U(x)$, $\varphi_\times(x, y, z)$, $\varphi_0(x)$ and $\varphi_{MAX}(x)$ in the language of arithmetic with exponentiation which define in a model $\mathcal{A}_r$ the model isomorphic to a model $\mathcal{B}_n$ of arithmetic with multiplication, whenever $n \geq 4$ and $r$ are such that $2^{n-1} + 1 \leq r \leq 2^n$. Moreover, the isomorphism function $f : |\mathcal{B}_n| \longrightarrow |\mathcal{A}_r|$ is defined as follows* $f(a) = \begin{cases} a & \text{if } a < n \\ r & \text{if } a = n. \end{cases}$

PROOF. We use the fact that $(2^x)^y = 2^z$ if and only if $z = xy$. That allows us to define easily the multiplication in the standard model for exponentiation function. Of course, if we are in a finite model for exponentiation, we can define multiplication only on an initial segment of this model.

Firstly, let us remind (see beginning of this section) that in finite arithmetic with exponentiation we can define 0 and 1. Moreover, the formula

$$\forall z \forall y \neq 0, 1(\exp(z, x) = MAX \Rightarrow \exp(z, y) = MAX) \wedge x \neq 0 \wedge x \neq 1$$

defines 2 in all models of cardinalities greater than 5

Therefore, we will use the constant 2 in our formulas. We will present formulas which define model $\mathcal{A}_n$ of arithmetic with multiplication in models $\mathcal{A}_r$ for $n \geq 4$ and $r \in \{2^{n-1} + 1, \dots, 2^n\}$.

The formula defining a universe $\varphi_U(x)$ is $2^x \neq MAX \vee x = MAX$. The formula for equality relation $\varphi_=(x, y)$ is just $x = y$. For multiplication we take $\varphi_\times(x, y, z)$ defined as

$$\begin{aligned}
&((\exp(\exp(2, x), y) = \exp(2, z) \wedge \exp(2, z) \neq MAX) \vee \\
&(\exp(\exp(2, x), y)) = MAX \wedge z = MAX).
\end{aligned}$$

It is straightforward to check that these formulas define the model $\mathcal{B}_n$ in models $\mathcal{A}_r$ for $n, r$ as above. ⊣

As a consequence of lemma 4.9 and theorem 4.3 we have

THEOREM 4.10. *For each formula $\varphi(x_1, \dots, x_k) \in \mathcal{F}_{\{+,\times\}}$, there is formula $\psi(x_1, \dots, x_k) \in \mathcal{F}_{\{\exp\}}$ with the same free variables as in $\varphi(x_1, \dots, x_k)$ such that for each $a_1, \dots, a_k \in \mathbf{N}$,*

$$\models_{sl} \varphi[a_1, \dots, a_k] \text{ if and only if } \models_{sl} \psi[a_1, \dots, a_k].$$

We end this section with the description of complexity of $Th(FM(\mathcal{A}))$ and $sl(FM(\mathcal{A}))$ for $\mathcal{A}$ being a model for arithmetic with multiplication or exponentiation.

THEOREM 4.11. *Let $\mathcal{A}$ be $(\mathbf{N}, \times)$ or $(\mathbf{N}, \exp)$.*

*a) $Th(FM(\mathcal{A}))$ is $\Pi_1^0$–complete.*
*a) $sl(FM(\mathcal{A}))$ is $\Sigma_2^0$–complete.*

PROOF. The proof of part *a*) for $\mathcal{A} = (\mathbf{N}, \times)$ is a consequence of the first part of theorem 4.7 . The proof for $\mathcal{A} = (\mathbf{N}, \exp)$ relays on the fact that in finite models for exponentiation we can reconstruct the theory of multiplication in the sense of lemma 4.9.

The proof of the second part is a modified version of the proof of $\Sigma_2$–completeness of $sl(FM((\mathbf{N}, +, \times)))$ from [16]. In that article the reduction of a $\Sigma_2$–complete problem, $Fin$, to the $sl(FM((\mathbf{N}, +, \times)))$ was given (here $Fin$ is the set of indices of Turing machines with a finite domain). ⊣

Let us observe that the reduction from [16] uses formulas which do not belong to $\Sigma_2$ therefore we cannot state the last result for $sl_{\Sigma_2}(FM(\mathcal{A}))$.

**§5. Decidability of the existential theory of multiplication and order.** In the present section the vocabulary is fixed and contains the function symbol for multiplication, one binary predicate for order relation and constants 0, 1 and $MAX$.

Let us observe that if we consider the $\Sigma_1$ theory of arithmetic with multiplication then the presence of constants 0, 1 and $MAX$ in our language is inessential. In all models of cardinality greater than 3 we can define them by means of $\Sigma_1$ formulas with multiplication.

$$\begin{array}{lll} x = MAX & \text{if and only if} & \exists z_1, z_2(z_1 \neq x \wedge z_2 \neq x \wedge z_1 z_2 = x) \wedge xx = x, \\ x = 0 & \text{if and only if} & \exists z_1, z_2(z_1 \neq z_2 \wedge z_1 x = x \wedge z_2 x = x) \wedge x \neq MAX, \\ x = 1 & \text{if and only if} & \exists z_1, z_2(z_1 \neq z_2 \wedge z_2 \neq 0 \wedge z_1 \neq 0 \wedge \\ & & z_1 x = z_1 \wedge z_2 x = z_2). \end{array}$$

Therefore, we could quantify out the constants by adding new existential quantifiers.

Let us observe, that there are also equivalent definitions of all these constants by $\Pi_1$ formulas with multiplication. Namely

$$\begin{array}{lll} x = 0 & \text{if and only if} & \forall y(xy = x), \\ x = 1 & \text{if and only if} & \forall y(xy = y), \\ x = MAX & \text{if and only if} & \forall y(y = 0 \vee xy = x) \wedge x \neq 0. \end{array}$$

As we show in the third paragraph, $\Sigma_2$ theory of multiplication is undecidable with respect to sufficiently large finite models. Now, we are going to show that the $\Sigma_2$ lower bound for the undecidability of the theory of multiplication is optimal. Namely, we prove that the theory $sl_{Bool(\Sigma_1)}(FM((\mathbf{N}, \times, \leq))) = \{\varphi \in Bool(\Sigma_1) : \ FM((\mathbf{N}, \times, \leq)) \models_{sl} \varphi\}$ is decidable.

It is worth to note that the theory $sl_{\Sigma_1^*}(FM((N, \times, \leq)))$ is undecidable when $\Sigma_1^*$ denotes the class of formulas of the form $\exists x_1 \ldots \exists x_n \psi$ where in $\psi$ there may occur bounded quantifiers of the form: $\exists x \leq t, \forall x \leq t$. This fact can be easily seen from the Tarski's definition of addition and *MDRP* theorem. One can also observe that the set $sl_{\Sigma_1}(FM((\mathbf{N}, S, \times)))$, where $S$ is the successor function, is also undecidable.

To prove the main result of this section we will need the following.

FACT 5.1. *If $\varphi \in \Sigma_1$ and $\varphi$ is satisfiable in finite models then $\models_{sl} \varphi$.*

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 $\varphi \in \Sigma_1$ and $\mathcal{A}_k \models \varphi$ then each model of cardinality greater than or equal to $N$ has a submodel in which $\varphi$ is true. Since $\varphi$ is a $\Sigma_1$ formula it has to be true also in $\mathcal{A}_n$. Thus, $\models_{sl} \varphi$.

Let a model $\mathcal{A}_k$ be given. It has the universe $\{0, 1, \ldots, k\}$. We will define the function $\hat{}: |\mathcal{A}_k| \longrightarrow |\mathcal{A}_n|$ and then we prove that if $n$ is sufficiently large, the image of $\hat{}$ will define the 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

$$\hat{p_i} = \lceil n^{\log_k p_i} \rceil.$$

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 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 all 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 $a, b \in \{2, \ldots, k-1\}$ in all sufficiently large models $\mathcal{A}_n$, 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,

$$\begin{aligned}
\hat{a} &= \hat{p}_1^{r_1} \cdots \hat{p}_m^{r_m} \\
&= \lceil n^{\log_k p_1} \rceil^{r_1} \ldots \lceil n^{\log_k p_m} \rceil^{r_m} \\
&< (n^{\log_k p_1} + 1)^{r_1} \cdots (n^{\log_k p_m} + 1)^{r_m} \\
&\leq (n^{\log_k p_1 + \varepsilon'})^{r_1} \cdots (n^{\log_k p_m + \varepsilon'})^{r_m} \\
&\leq (n^{\log_k (p_1+\varepsilon)})^{r_1} \cdots (n^{\log_k (p_m+\varepsilon)})^{r_m}, \text{ and for sufficiently large } n, \varepsilon' \text{ and } \varepsilon \\
&\qquad \text{may be chosen arbitrary small,} \\
&\leq n^{\log_k ((p_1+\varepsilon)^{r_1} \cdots (p_m+\varepsilon)^{r_m})} \\
&< n^{\log_k (p_1^{s_1} \cdots p_m^{s_m})}, \text{ for sufficiently small } \varepsilon, \\
&= (n^{\log_k p_1})^{s_1} \cdots (n^{\log_k p_m})^{s_m} \\
&\leq \hat{p}_1^{s_1} \cdots \hat{p}_m^{s_m} \\
&= \hat{b}.
\end{aligned}$$

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 take the maximal $N$ in all models of cardinalities greater than such $N$ the image of $\hat{}$ will define a submodel isomorphic to $\mathcal{A}_k$. ⊣

As an immediate corollary of fact 5.1 we obtain

COROLLARY 5.2. *Let $\varphi \in \Sigma_1$. Then, $\varphi$ is satisfiable in finite models if and only if $\models_{sl} \varphi$.*

Observe that for an arbitrary sentence $\varphi \in \Sigma_1(\leq, \times)$,

$$\varphi \in Th_{\Sigma_1}(FM(\mathcal{A})) \text{ if and only if } \mathcal{A}_0 \models \varphi.$$

Therefore, $Th_{\Sigma_1}(FM((\mathbf{N}, \times, \leq)))$ is decidable. However, we can state more.

FACT 5.3.

$$T = \{(\varphi, k) : \varphi \in \Sigma_1(\times, \leq) \wedge \forall n \geq k \; \mathcal{A}_n \models \varphi\}$$

*is decidable.*

PROOF. By the proof of fact 5.1, for each $k$ we can compute $N(k)$ such that if a $\Sigma_1(\times, \leq)$ is satisfiable in $\mathcal{A}_k$ then it is satisfiable in all models $\mathcal{A}_n$ for $n \geq N(k)$. Therefore, to check whether $(\varphi, k)$ belongs to $T$ it suffices to compute $N(k)$ and then to check whether $\mathcal{A}_r \models \varphi$ for all $r$ such that $k \leq r < N(k)$. If the latter is true then $\varphi$ is true in all models of cardinality greater than or equal to $k$. ⊣

Now, we are going to prove the stronger result, namely, that the theory $sl_{\Sigma_1}(FM((\mathbf{N}, \times, \leq)))$ is decidable. In what follows by $P_2$ we denote the set of powers of 2. We will need the following

LEMMA 5.4. *Let $G(n) = 2^{z_n}$ where $z_n = 2^n 2^{\frac{2}{3}(4^n - 1)}$. For all $a_1, \ldots, a_n$ such that $1 < a_1 < \ldots < a_n$ there exists $b_1, \ldots, b_n \in P_2 \cap \{2, \ldots, G(n)\}$ such that for all $i, j, m, l \leq n$*

$$a_i a_j < a_m a_l \text{ if and only if } b_i b_j < b_m b_l.$$

PROOF. We will prove by induction on $k \leq n$ the following:

$$\forall k \leq n \exists b_1, \dots, b_k \in P_2 \cap \{2, \dots, g(n,k)\} \forall t_1(x_1, \dots, x_k), t_2(x_1, \dots, x_k)$$
$$\{\textstyle\bigwedge_{i\in\{1,2\}} rk(t_i) \leq h(n,k) \Rightarrow$$
$$[t_1(a_1, \dots, a_k) < t_2(a_1, \dots, a_k) \iff t_1(b_1, \dots, b_k) < t_2(b_1, \dots, b_k)]\},$$

where $h(n,k) = 2^{2^{2(n-k)}}$ and $g(n,k) = 2^{v_{nk}}$, $v_{nk} = 2^k 2^{\frac{2}{3}(4^{n-k}(4^k-1))}$.

For $k = n$ we obtain the thesis.

A few words should be said on the choice of functions $g$ and $h$. They satisfy the following recursive dependencies which will be used during the proof.

$\sigma_1 :\ 2(h(n,k+1))^2 \leq h(n,k)$,
$\sigma_2 :\ g(n,k+1) \geq (g(n,k))^{h(n,k+1)}$,
$\sigma_3 :\ g(n,k+1) \geq (g(n,k))^{h(n,k+1)+1}$,
$\sigma_4 :\ g(n,k+1) \geq (g(n,k))^{2(h(n,k+1))^2}$.

Of course, $h$ satisfies $(\sigma_1)$ and it suffices to show only $(\sigma_4)$. To do this it suffices to verify that $g$ satisfies the following equality

$$g(n,k) = 2^{\Pi_{i=1}^{i=k} 2(h(n,i))^2}.$$

Indeed, it is easy to see that $\sigma_4$ could be strengthen to equality.

Each time we will use one of $\sigma_i$ we will mention it by indicating a proper condition.

We consider the following formula:

$$(*)\ \forall t_1(x_1, \dots, x_k), t_2(x_1, \dots, x_k)\{ \bigwedge_{i\in\{1,2\}} rk(t_i) \leq h(n,k) \Rightarrow$$
$$[t_1(a_1, \dots, a_k) < t_2(a_1, \dots, a_k) \iff t_1(b_1, \dots, b_k) < t_2(b_1, \dots, b_k)]\}.$$

Let us observe that if $b_1, \dots, b_k$ satisfy $(*)$, then for each $m \geq 1$ the sequence $b_1^m, \dots, b_k^m$ also satisfies $(*)$.

For $k = 1$ we put $b_1 = 2$. Now, let us assume that there exists $b_1, \dots, b_k$ which satisfy the inductive assumption for $k < n$ and we will find proper $c_1, \dots, c_{k+1}$, possibly with $c_i \neq b_i$ for $i \leq k$. We will consider two cases.

Firstly, let us assume that there exists $t(x_1, \dots, x_k), t'(x_1, \dots, x_k), w$ such that $rk(t) + w, rk(t') \leq h(n,k+1)$ and

$$(**) \qquad t(a_1, \dots, a_k) a_{k+1}^w = t'(a_1, \dots, a_k).$$

Then, the new sequence $c_1, \dots, c_{k+1}$ must satisfy the equation $t(c_1, \dots, c_k) c_{k+1}^w = t'(c_1, \dots, c_k)$. Let $r$ be such that

$$2^r = \frac{t'(b_1, \dots, b_k)}{t(b_1, \dots, b_k)}.$$

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 $\sigma_2$) and the sequence $c_1, \dots, c_k$ satisfies $(*)$. Now, we should show that our choice of $c_1, \dots, c_{k+1}$, is suitable.

It suffices to show that if $s(x_1, \dots, x_k), s'(x_1, \dots, x_k)$ and $u$ are such that $rk(s) + u \leq h(n,k+1)$ and $rk(s') \leq h(n,k+1)$, then

$$s(a_1, \dots, a_k) a_{k+1}^u < s'(a_1, \dots, a_k) \iff s(c_1, \dots, c_k) c_{k+1}^u < s'(c_1, \dots, c_k)$$

and

$$s'(a_1,\dots,a_k) < s(a_1,\dots,a_k)a_{k+1}^u \iff s'(c_1,\dots,c_k) < s(c_1,\dots,c_k)c_{k+1}^u.$$

We will show the first equivalence. Let

$$s(a_1,\dots,a_k)a_{k+1}^u < s'(a_1,\dots,a_k).$$

Then

$$s^w(a_1,\dots,a_k)a_{k+1}^{uw} < s'^w(a_1,\dots,a_k)$$

and, by (**),

$$s^w(a_1,\dots,a_k)t'^u(a_1,\dots,a_k)a_{k+1}^{uw} < s'^w(a_1,\dots,a_k)t^u(a_1,\dots,a_k)a_{k+1}^{uw}.$$

It follows that

$$s^w(a_1,\dots,a_k)t'^u(a_1,\dots,a_k) < s'^w(a_1,\dots,a_k)t^u(a_1,\dots,a_k).$$

We need the fact that $rk(s^wt'^u), rk(s'^wt^u) \le h(n,k)$. Indeed,

$$\begin{aligned}
rk(s^wt'^u) &\le rk(s)w + (w-1) + 1 + rk(t')(h(n,k+1) - rk(s)) + \\
&\qquad + (h(n,k+1) - rk(s) - 1) \\
&\le rk(s)h(n,k+1) + h(n,k+1) + \\
&\qquad + h(n,k+1)(h(n,k+1) - rk(s)) + \\
&\qquad + (h(n,k+1) - rk(s) - 1) \\
&\le h(n,k+1)h(n,k+1) + h(n,k+1) + h(n,k+1) \\
&\le (h(n,k+1))^2 + 2h(n,k+1) \\
&\le 2(h(n,k+1))^2 \\
&\le h(n,k).
\end{aligned}$$

The last inequality is simply the condition $(\sigma_1)$. The reasoning for $rk(s'^wt^u) \le h(n,k)$ is perfectly parallel. So, by $(*)$ applied to $c_1,\dots,c_k$ we have,

$$s^w(c_1,\dots,c_k)t'^u(c_1,\dots,c_k) < s'^w(c_1,\dots,c_k)t^u(c_1,\dots,c_k)$$

and therefore

$$s^w(c_1,\dots,c_k)t'^u(c_1,\dots,c_k)c_{k+1}^{uw} < s'^w(c_1,\dots,c_k)t^u(c_1,\dots,c_k)c_{k+1}^{uw}.$$

By the choice of $c_{k+1}$ we obtain finally that

$$s(c_1,\dots,c_k)c_{k+1}^u < s'(c_1,\dots,c_k).$$

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 is no $t(x_1,\dots,x_k), t'(x_1,\dots,x_k), w$ such that $rk(t)+w, rk(t') \le h(n,k+1)$ and $t(a_1,\dots,a_k)a_{k+1}^w = t'(a_1,\dots,a_k)$.

Let $(t_1,t'_1,w_1),\dots,(t_m,t'_m,w_m)$ be the list of all triples such that $rk(t_i)+w_i \le h(n,k+1), rk(t'_i) \le h(n,k+1)$ and

$$t_i(a_1,\dots,a_k)a_{k+1}^{w_i} < t'_i(a_1,\dots,a_k)$$

and let $(s_1,s'_1,u_1),\dots,(s_r,s'_r,u_r)$ be the list of all triples such that $rk(s_j) < h(n,k+1), rk(s'_j)+u_j \le h(n,k+1)$ and

$$s_j(a_1,\dots,a_k) < s'_j(a_1,\dots,a_k)a_{k+1}^{u_j}.$$

We should define $c_1, \dots, c_{k+1}$ in a way that preserves all inequalities above.

If the first list is empty, we can define $c_{k+1}$ as $b_k^{h(n,k+1)+1}$ since $b_k$ is the largest of $b_i$'s and, for $i \leq k$, set $c_i = b_i$. By $\sigma_3$ the new sequence will satisfy $(*)$. Otherwise, for $i \leq m$, let us define $\nu_i$ such that

$$2^{\nu_i} = t'_i(b_1, \dots, b_k)/t_i(b_1, \dots, b_k).$$

Next, we define $\mu_j$ such that if $s_j(b_1, \dots, b_k) \geq s'_j(b_1, \dots, b_k)$, then

$$2^{\mu_j} = s_j(b_1, \dots, b_k)/s'_j(b_1, \dots, b_k)$$

and otherwise $\mu_j = 0$ for $j \leq r$.

For each $i \leq m, j \leq r$

$$t_i^{u_j}(a_1, \dots, a_k) s_j^{w_i}(a_1, \dots, a_k) a_{k+1}^{w_i u_j} < {t'}_i^{u_j}(a_1, \dots, a_k) {s'}_j^{w_i}(a_1, \dots, a_k) a_{k+1}^{w_i u_j}$$

and therefore

$$t_i^{u_j}(a_1, \dots, a_k) s_j^{w_i}(a_1, \dots, a_k) < {t'}_i^{u_j}(a_1, \dots, a_k) {s'}_j^{w_i}(a_1, \dots, a_k).$$

Again, $rk(t_i^{u_j} s_j^{w_i}) \leq h(n,k)$ and $rk({t'}_i^{u_j} {s'}_j^{w_i}) \leq h(n,k)$ so, by the inductive assumption, we obtain that

$$t_i^{u_j}(b_1, \dots, b_k) s_j^{w_i}(b_1, \dots, b_k) < {t'}_i^{u_j}(b_1, \dots, b_k) {s'}_j^{w_i}(b_1, \dots, b_k)$$

and

$$\left(\frac{s_j(b_1, \dots, b_k)}{s'_j(b_1, \dots, b_k)}\right)^{w_i} < \left(\frac{t'_i(b_1, \dots, b_k)}{t_i(b_1, \dots, b_k)}\right)^{u_j}.$$

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 $\frac{\mu_j}{u_j}$ and $\frac{\nu_1}{w_1}$ is minimal of all $\frac{\nu_i}{w_i}$. If $\frac{\mu_1}{u_1} + 1 < \frac{\nu_1}{w_1}$ then the sequence $c_i = b_i$ for $i \leq k$ and $c_{k+1} = 2^{\lceil \frac{\mu_1}{u_1} \rceil}$ will satisfy all relevant inequalities. However, that choice of $c_1, \dots, c_{k+1}$ 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 $c_1, \dots, c_k$, we can define $\mu'_j$ and $\nu'_i$ exactly in the same way as we did it for $b_1, \dots, b_k$. 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 $\sigma_4$). It is straightforward to check that the sequence $c_1, \dots, c_{k+1}$ will satisfy the condition $(*)$ for $k+1$. ⊣

Now, we are ready to prove the following proposition.

PROPOSITION 5.5. *Let $F(n) = 2^{z_n} + 1$ where $z_n = 2^{n+1} 2^{\frac{2}{3}(4^{n+1}-1)}$. Then, for each $\varphi \in \Sigma_1$, $\varphi$ simple with all variables $x_1, \dots, x_n$, if $\varphi$ has a finite model, then $\varphi$ has a model of cardinality less than or equal to $F(n)$.*

PROOF. Let $\varphi \in \Sigma_1$ satisfies the assumptions. If $x_1, \ldots, x_n$ is the list of all variables in $\varphi$ then, by lemma 5.4, if $\varphi$ has a model then it has a finite model of cardinality less than or equal to $G(n+1)$, where $G(i)$ is the function from lemma 5.4. We should take $n+1$ instead of $n$ because besides of the bound on witnesses for $x_1, \ldots, x_n$ we should also bound the witness for the size of the maximal element of a model in which $\varphi$ is satisfied. Now, the thesis follows from the fact that $F(n) = G(n+1)$. $\dashv$

From corollary 5.2 and proposition 5.5 the following theorem follows immediately.

THEOREM 5.6. *The theory* $sl_{\Sigma_1}(FM((\mathbf{N}, \times, \leq))) = \{\varphi \in \Sigma_1 : \models_{sl} \varphi\}$ *is decidable.*

Another consequence of lemma 5.4 is the following

THEOREM 5.7. *The existential theory of the standard model of arithmetic with multiplication and order is decidable. Moreover, the size of witnesses in the standard model for a simple sentence* $\varphi$ *with all variables* $x_1, \ldots, x_n$ *can be bounded by* $2^{z_n}$*, where* $z_n = 2^n 2^{\frac{2}{3}(4^n-1)}$.

The last theorem is a direct consequence of lemma 5.4. We obtained slightly better bound than in proposition 5.5 because we do not need to estimate the maximal element as it was the case for satisfiability in finite models.

**§6. Concatenation defines in finite models addition and multiplication.** In the present section we define the arithmetic of concatenation of finite words and show that in finite models it has the strength of the arithmetic of addition and multiplication.[2] This is a partial answer for a question from [2] about existing of other than *BIT* natural relations which define in finite models addition and multiplication.

The arithmetic of concatenation is one of the three classical theories of arithmetics, the others being the arithmetic of addition and multiplication and the arithmetic of hereditarily finite sets. The standard model for arithmetic of concatenation can be defined as follows.

DEFINITION 6.1. *Let* $\Gamma_t = \{a_1, \ldots, a_t\}$ *be an alphabet. A word over* $\Gamma_t$ *is a finite sequence of elements from* $\Gamma_t$*. The empty word is denoted by* $\lambda$*. By* $\Gamma_t^*$ *we denote the set of all words over* $\Gamma_t$*, i.e.*

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

*By* $FW^t$ *we denote the structure*

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

*where* $*_t$ *is the concatenation operation on words from* $\Gamma_t^*$ *and* $\mathbf{a}_i$ *is a word consisting of one letter* $a_i$*.*

Finite words in the universe of $FW^t$ can be identified with natural numbers via $t$–adic representation. It has an advantage over usual binary or decimal representation that each number is represented by exactly one word in $\Gamma_t^*$. The correspondence between finite words and natural numbers is established by a function $\mathrm{nr}_t : \Gamma_t^* \longrightarrow \omega$, where

[2]The section is based on [25].

- $\mathrm{nr}_t(\lambda) = 0$,
- $\mathrm{nr}_t(\mathbf{a}_i) = i$, for $1 \leq i \leq t$,
- $\mathrm{nr}_t(u_n \dots u_0) = \Sigma_{i=0}^{i=n} \mathrm{nr}_t(u_i)t^i$, for $u_i \in \Gamma_t$.

The function $\mathrm{nr}_t$ is one–to–one and onto and induces an $\omega$–type ordering on $\Gamma_t^*$ defined as

$$u \leq w \quad \text{if and only if} \quad \mathrm{nr}_t(u) \leq \mathrm{nr}_t(w).$$

In what follows we will implicitly treat elements of $\Gamma_t^*$ as natural numbers with the identification given by $\mathrm{nr}_t$. Moreover, we assume that $t \geq 2$. For the case $t = 1$ the model $FW^1$ is easily seen to be equivalent to arithmetic of addition. Indeed, when we identify words over one letter alphabet with natural numbers via $\mathrm{nr}_1$, $*_1$ is just the addition operation.

Let us also present the arithmetic of hereditarily finite sets. We define it in order to give a more complete description of the state of knowledge on various sets of built–in relations in finite models which are equivalent to addition and multiplication.

DEFINITION 6.2. *Let $\emptyset$ be the empty set and let $\mathcal{P}(x)$ be a power set of a set $x$. Let $V_0 = \emptyset$ and, for $i \in \mathbf{N}$, $V_{i+1} = \mathcal{P}(V_i)$. Furthermore, let $V_\omega = \bigcup_{i \in N} V_i$. The model of the arithmetic of hereditarily finite sets is defined as $HF = (V_\omega, \in)$.*

The relation $BIT \subseteq \mathbf{N}^2$ is defined as: $BIT(x, y)$ if and only if the $x$-th bit in the binary representation of $y$ is one. Thus, if $y = \Sigma_{i=0}^{i=n} a_i 2^i$, where $a_i \in \{0, 1\}$, then

$$BIT(x, y) \quad \text{if and only if} \quad a_x = 1.$$

It is not hard to prove that

THEOREM 6.3. *$HF$ is isomorphic to $(\mathbf{N}, BIT)$.*

The claimed isomorphism function can be defined by induction on $i$ for the family $\{V_i\}_{i \in \mathbf{N}}$. The function $f_0 : V_0 \longrightarrow \mathbf{N}$ is just the empty function and if we defined $f_i : V_i \longrightarrow \mathbf{N}$ then $f_{i+1} : V_{i+1} \longrightarrow \mathbf{N}$ can be defined for $y \in V_{i+1}$ as

$$f_{i+1}(y) = \Sigma_{x \in y} 2^{f_i(x)}.$$

It is straightforward to check that a function

$$f = \bigcup_{i \in \mathbf{N}} f_i$$

is a well defined function and that it is the unique isomorphism between $HF$ and $(\mathbf{N}, BIT)$.

Since we can identify elements of $FW^t$ and $HF$ with natural numbers we can easily extend our definition of $FM(\mathcal{A})$ to these models and talk about $FM(FW^t)$ and $FM(HF)$.

The class $FM(HF)$, or, equivalently, $FM((\mathbf{N}, BIT))$, is well examined. The following was proven in [2].

THEOREM 6.4 ([2]). *Operations of addition and multiplication are definable in $FM((\mathbf{N}, BIT, \leq))$.*

Later, Dawar et al. showed that

THEOREM 6.5 ([7]). *The standard ordering relation is definable in $FM(HF)$.*

Of course, the above two results give

THEOREM 6.6 ([2],[7]). *Operations of addition and multiplication are definable in $FM(HF)$.*

The family $FM(HF)$ was considered also by Asterias and Kolaits. Let us define $\Delta_0^{\in}$ as the class of $MAX$–free formulas $\varphi$ in $\mathcal{F}_{\{\in\}}$ such that all quantifiers occurring in $\varphi$ are of the form $Qx \in y$, where $Q \in \{\exists, \forall\}$. Therefore, contrary to the usual definition of $\Delta_0(\sigma)$, there is no $\leq$ predicate in formulas from $\Delta_0^{\in}$. It was shown in [1] that the least fixed point operator of arity 2 applied to a formula in $\Delta_0^{\in}$ is expressible on $FM(HF)$ in first order logic. Moreover, they observed that the analogous fact for the least fixed point of arbitrary arity implies that $PTIME \subseteq LINH$. Since $LINH \subsetneq PSPACE$, the separation of $PTIME$ from $PSPACE$ follows.

Now, let us turn to the standard model for arithmetic of concatenation, $FW^t$. (We assume that $t \geq 2$.) $FW^t$ was considered e.g. by Quine who showed in [20] how to define in it addition and multiplication. Later, Bennett in [3] considered the model $(\Gamma_t^*, *_t, \leq, \mathbf{a}_1, \ldots, \mathbf{a}_t)$. Let us denote the vocabulary of this model by $\sigma_{t-con}$. Bennett showed that we can define addition and multiplication by $\Delta_0(\sigma_{t-con})$ formulas. So, we have.

THEOREM 6.7 ([3]). *For each $t \geq 2$, the graphs of addition and multiplication are definable in $(\Gamma_t^*, *_t, \leq, \mathbf{a}_1, \ldots, \mathbf{a}_t)$ by $\Delta_0(\sigma_{t-con})$ formulas.*

In what follows, we show that in finite models from $FM(FW^t)$ we can define addition and multiplication. In particular, we do not need in finite models the ordering relation to define the full arithmetic from concatenation. Indeed, the ordering is definable in $FM(FW^t)$.

Let us observe that $\leq$ is definable from concatenation also in $FW^t$, see e.g. [20]. However, the known definitions of the relation $x \leq y$ use elements of $FW^t$ which are exponentially larger than $x$ and $y$. Thus, one cannot apply them in the finite models context. The definability of $\leq$ in finite models follows essentially from the fact that being in a finite model we can detect whether a value of a term $s$ is less than the maximal element or not.

LEMMA 6.8. *Let $t \geq 1$ and let $\mathrm{lh}(x)$ be the length function for words in $\Gamma_t^*$. Relations $\mathrm{lh}(x) = \mathrm{lh}(y)$, $\mathrm{lh}(x) < \mathrm{lh}(y)$ and $x \leq y$ are first order definable in $FM(FW^t)$.*

PROOF. For $t = 1$ the claim is obvious so let $t \geq 2$. Observe, that it suffices to define only the predicate $\mathrm{lh}(x) < \mathrm{lh}(y)$, the others being easily definable from it and concatenation. E.g. $x \leq y$ can be defined as follows:

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

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

Now, we will define $\mathrm{lh}(x) < \mathrm{lh}(y)$. As a first step we define $\psi(x, y)$ of the form

$$\exists z \, (x * z \neq MAX \wedge y * z = MAX)$$

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 see this, let $x, y \in |FW^t_n|$. If $\mathrm{lh}(x)+2 \leq \mathrm{lh}(y)$ then let $k = \mathrm{lh}(n)-\mathrm{lh}(x)-1$. We have that $\mathrm{lh}(x *_t a_1^k) < \mathrm{lh}(n)$ and $\mathrm{lh}(y *_t a_1^k) > \mathrm{lh}(n)$. Thus, $FW^t_n \models \psi[x,y]$. On the other hand, if $\mathrm{lh}(x)-1 \geq \mathrm{lh}(y)$, then for all words $z$, $\mathrm{lh}(x *_t z) > \mathrm{lh}(y *_t z)$. So, for all words $z$, if $y *_t z \geq n$ then $x *_t z \geq n$ and $FW^t_n \models \neg\psi[x,y]$.[3]

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

$$\psi(x * x, y * y) \wedge x * x \neq MAX \wedge y * y \neq MAX.$$

It holds in a given finite model from $FM(FW^t)$ that for all $x$, $y$

$$\text{if } \mathrm{lh}(x) < \mathrm{lh}(y) < \frac{\mathrm{lh}(MAX)}{2} \quad \text{ then } \ \tilde{\varphi}_<(x,y) \text{ and } \neg\tilde{\varphi}_<(y,x).$$

It can be easily proven by noting that if there is any difference in lengths of $x$ and $y$ then the difference between lengths of $x * x$ and $y * y$ will satisfy one of the conditions, $(i)$ or $(ii)$, for a formula $\psi(x,y)$.

Unfortunately, $\tilde{\varphi}_<$ gives us no information when $\mathrm{lh}(x) = \mathrm{lh}(y)$.[4] Nevertheless, the following formula $\tilde{\varphi}_=(x,y)$:=

$$x * x * x * x \neq MAX \wedge y * y * y * y \neq MAX \wedge [x = y = \lambda \vee$$

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

has the property that

$$\text{if } \mathrm{lh}(x), \mathrm{lh}(y) < \frac{\mathrm{lh}(MAX)}{4} \text{ then}$$
$$\mathrm{lh}(x) = \mathrm{lh}(y) \text{ if and only if } \tilde{\varphi}_=(x,y).$$

$\tilde{\varphi}_=(x,y)$ simply says that shortening one of the words: $x * x$ or $y * y$, by one letter results with a word which is shorter than the other one. Such a situation is possible only when $\mathrm{lh}(x) = \mathrm{lh}(y)$. If $y$ and $x$ have different lengths then the difference between $x * x$ and $y * y$ will be doubled. It follows that removing one letter from $x * x$ or $y * y$ will not make these words of equal length.

Now, we will define the predicate $\mathrm{lh}(x) = \mathrm{lh}(y)$ on a whole model. Let $\varphi'_=(x,y)$ be the following formula

$$\exists x_1, \ldots, x_6, y_1, \ldots, y_6 [x = x_1 * \ldots * x_6 \wedge y = y_1 * \ldots * y_6 \wedge$$

$$\bigwedge_{i \leq 6} (x_i * x_i * x_i * x_i * x_i \neq MAX \wedge y_i * y_i * y_i * y_i * y_i \neq MAX \wedge \tilde{\varphi}_=(x_i, y_i))].$$

$\varphi_=(x,y)$ holds if it is possible to divide $x$ and $y$ into six subwords which are so short that $\tilde{\varphi}_=$ can properly express the equality between their lengths.[5] In such a case lenghts of $x$ and $y$ are equal. However if the lenght of the maximal element is no greater than 25 such a division may be impossible even if $\mathrm{lh}(x) = \mathrm{lh}(y)$.

[3] Let us observe, that we cannot improve the condition in $(i)$ to $\mathrm{lh}(x)+1 \leq \mathrm{lh}(y)$. As a counterexample one can take a model $FW^2_4$, $x = a_2$ and $y = a_1 a_1$.

[4] E.g. for two elements alphabet and a model $FW^2_8$ we have, $FW^2_8 \not\models \tilde{\varphi}_<[\mathbf{a}_1, \mathbf{a}_1]$ and $FW^2_8 \models \tilde{\varphi}_<[\mathbf{a}_1, \mathbf{a}_2]$.

[5] Let us observe that we check in $\varphi_=$ a sufficient condition for $\mathrm{lh}(x_i), \mathrm{lh}(y_i) < \mathrm{lh}(MAX)/4$, for $i \leq 6$, to make $\tilde{\varphi}_=$ work properly.

So, finally the equality $\mathrm{lh}(x) = \mathrm{lh}(y)$ can be expressed by the following formula $\varphi_{=}(x, y)$:

$$\varphi'_{=}(x,y) \wedge \bigvee_{n=1}^{25} [n = MAX \wedge \bigvee_{\substack{u,v \in \Gamma_t^* \\ \mathrm{lh}(x) = \mathrm{lh}(y) \leq n}} (x = u \wedge y = v)].$$

Now, $\mathrm{lh}(x) < \mathrm{lh}(y)$ can be written as

$$\exists y_1, y_2 \, [y = y_1 * y_2 \wedge y_2 \neq \lambda \wedge \varphi_{=}(y_1, x)].$$

⊣

Now, we can state the main result of this section.

THEOREM 6.9. *For $t \geq 2$, the graphs of addition and multiplication are definable in $FM(FW^t)$.*

We only sketch two possible lines of proofs for the above theorem. Since the ordering relation is definable in $FM(FW^t)$, one can prove the theorem by transferring the proof of Bennett's theorem (theorem 6.7) to the finite model context. The only problem that should be overcome is that in the standard model one can use bounded quantification $Qx \leq s$, where $s$ is a term in the language of $FW^t$. However, in finite models the value of this term can exceed the maximal element of a finite model. Therefore, one should replace such quantification by quantification over tuples of elements of a given finite model.[6] However, instead of following quite general and involved constructions of [3] one can give the straightforward definition of addition and multiplication. Such definitions are given in [25].

**§7. Spectra of theories of arithmetics.** In this section we consider the spectrum problem for families of $FM(\mathcal{A})$. Usually the spectrum of a sentence is defined as the set of cardinalities of all finite structures being a model of this sentence. For our purpose we introduce a slightly different notion of spectrum.

DEFINITION 7.1. *By an $FM(\mathcal{A})$–spectrum of a sentence $\varphi$ we define the set of cardinalities of models from $FM(\mathcal{A})$ in which $\varphi$ is true, i.e.*

$$Spec_{FM(\mathcal{A})}(\varphi) = \{n + 1 : \mathcal{A}_n \models \varphi\}.$$

*By a spectrum of $FM(\mathcal{A})$, denoted by $Spec(FM(\mathcal{A}))$, we define the set of all $FM(\mathcal{A})$–spectra of sentences in the language of $FM(\mathcal{A})$. In what follows we will omit subscript $FM(\mathcal{A})$ in $Spec_{FM(\mathcal{A})}(\varphi)$.*

The above notion of spectrum has different properties than the classical one. Observe for example that the family $Spec(FM(\mathcal{A}))$ is closed not only on set-theoretical union and intersection but also on the set-theoretical complement.

[6] In the context of arithmetic of addition and multiplication there is a standard method of translating $\Delta_0$ formulas to formulas interpreted in finite models, see e.g. [21].

Moreover, if a structure $\mathcal{A}$ is a restriction of a structure $\mathcal{A}'$ to some subsignature, then $Spec(FM(\mathcal{A})) \subseteq Spec(FM(\mathcal{A}'))$. So, for example we have:

$$Spec((\mathbf{N},+)) \cup Spec((\mathbf{N},\times)) \subseteq Spec((\mathbf{N},+,\times))$$

It is not difficult to describe the spectrum of $FM((\mathbf{N},+))$. Indeed, for each sentence $\varphi \in \mathcal{F}_{\{+\}}$ there is a formula $\varphi^*(y)$ such that

$$Spec(\varphi) = \{n+1 : (\mathbf{N},+) \models \varphi^*[n]\}.$$

To construct $\varphi^*(y)$ one can take the formula from lemma 3.1 and replace the order predicate by its definition in $(N,+)$.

This shows that there is a connection between elements of $Spec(FM((\mathbf{N},+)))$ and sets of natural numbers definable in the structure $(\mathbf{N},+)$. The theorem of Ginsburg and Spanier (for a proof see [24]) states that sets definable in the standard model for arithmetic with addition are exactly the ultimately periodic sets. Note that a set $X \subseteq \mathbf{N}$ is ultimately periodic if there are a positive integer $p$ and a natural number $a$ such that $\forall n \geq a(n \in X \iff n+p \in X)$. In consequence, $Spec(FM((\mathbf{N},+)))$ is just the family of ultimately periodic sets. Moreover, it follows from [21] that this is also a spectrum of arithmetic with addition in the language with counting quantifiers.

Let us observe that $Spec(FM((\mathbf{N},<)))$ is the family of finite and cofinite subsets of $\mathbf{N}$.

It is known that $\Delta_0$–formulas define in $(\mathbf{N},+,\times)$ exactly the sets in the linear time hierarchy, $LINH$.[7] This allows to give a known characterization of the family $Sp(FM((\mathbf{N},+,\times)))$. Namely, $Sp(FM((\mathbf{N},+,\times))) = LINH$. The inclusion from right to left follows from the fact that if a set $X$ is $\Delta_0$ definable in $(\mathbf{N},+,\times)$ then there is a formula $\varphi_X$ such that in each finite model $\mathcal{A}_n \in FM((\mathbf{N},+,\times))$ $\varphi_X$ defines the set $X \cap \{0,\dots,n\}$. The other inclusion can be easily deduced from lemma 3.1. Indeed, lemma 3.1 allows us to state the following, more general fact.

FACT 7.2. *If $R_0,\dots,R_n$ are relations definable in the structure $(\mathbf{N},+,\times)$ by $\Delta_0$–formulas, then each set of $Spec((\mathbf{N},+,\times,R_0,\dots,R_n))$ is $\Delta_0$–definable in the standard model of arithmetic.*

From lemma 4.5 we may deduce that there is a close connection between $Spec(FM((\mathbf{N},\times)))$ and $Spec(FM((\mathbf{N},+,\times)))$.

PROPOSITION 7.3. *Let $X$ belong to the spectrum of arithmetic with addition and multiplication. Then the set*

$$Y = \{r+1 : \exists n \geq 2(n \in X \wedge (n-2)^2 + 1 \leq r \leq (n-1)^2)\}$$

*belongs to the spectrum of arithmetic with multiplication.*

PROOF. Let $\varphi$ be a sentence of the language of arithmetic with addition and multiplication such that $Spec(\varphi) = X$. Then $Y$ is the spectrum of the sentence which is constructed from $\psi$ occurring in lemma 4.5. The only modification is connected with including, or excluding, the one element model. ⊣

[7] For a definition of $LINH$ and for a proof of this fact see e.g. [9].

The following examples show that not all sets from $Spec((\mathbf{N}, \times))$ are of the form which occurs in the above proposition.

**Examples.**

Let $\varphi^{max}_{<}(x)$ denote the following formula $xx \neq MAX \wedge \forall y(yy \neq MAX \wedge y \neq x \Rightarrow \varphi_{<}(y, x))$, where $\varphi_{<}(x, y)$ is a formula defined at the beginning of the fourth section. It says that $x$ is a maximal element such that $xx \neq MAX$

**1.** Let $\Phi_0$ be the following sentence:

$$\exists x(\varphi^{max}_{<}(x) \wedge \exists^{=1} w(w^2 = MAX \wedge wx \neq MAX)).$$

If $x$ satisfies $\varphi^{max}_{<}(x)$ then an element $w$ mentioned in $\Phi_0$ is just $x+1$. Thus, $\Phi_0$ expresses that $x(x+1) < MAX$ and, by the uniqness of $w$, that $x(x+2) \geq MAX$. Therefore, for each $i$,

$$\mathcal{A}_i \models \Phi_0 \quad \text{if and only if} \quad \exists n \geq 1(n^2 + n < i \leq n^2 + 2n).$$

So, $Spec(\Phi_0) = \{i : \exists n \geq 1\ (n^2 + n + 1 < i \leq n^2 + 2n + 1)\}$.

**2.** Let $\Phi_1$ be the following sentence:

$$\exists x[\varphi^{max}_{<}(x) \wedge \exists y \exists^{=1} z(y \neq z \wedge y^2 = MAX \wedge z^2 = MAX \wedge$$
$$xy \neq MAX \wedge xz \neq MAX)]$$

Now, we expressed that if $x$ is as above then $x(x + 2) < MAX$ but, by the maximality of $x$, $(x + 1)^2 \geq MAX$. We obtain that for each $i$,

$$\mathcal{A}_i \models \Phi_1 \quad \text{if and only if} \quad \exists n \geq 1\,(i = n^2)$$

So, $Spec(\Phi_1) = \{n^2 + 1 \ : \ n \in \mathbf{N}\}$.

**3.** Let $\Phi_2$ be the following sentence:

$$\exists x[x^3 \neq MAX \wedge \forall y(\varphi_{<}(x, y) \rightarrow y^3 = MAX) \wedge \exists^{=1} z(\varphi_{<}(x, z) \wedge x^2 z \neq MAX)]$$

By an argument similar to that used above, for each $i$,

$$\mathcal{A}_i \models \Phi_2 \quad \text{if and only if} \quad \exists n \geq 1(n^3 + n^2 < i \leq n^3 + 2n^2).$$

So, $Spec(\Phi_2) = \{i \ : \ \exists n \geq 1(n^3 + n^2 + 1 < i \leq n^3 + 2n^2 + 1)\}$.

Using the equality $x^4 - 1 = (x^2 - 1)(x^2 + 1)$ one can easily show that also the set $\{n^4 + 1 : n \in N\}$ is in the spectrum of multiplication. The same fact holds also for a polynomial $x^4 - 2x^2 + 2$. The following question naturally arises. For which polynomials $p$ the range of $p$ is in the spectrum of multiplication? We give some comments concerning this question in the last section of the paper.

The proposition 7.3 shows that the spectrum of the arithmetic with addition and multiplication and the spectrum of the arithmetic with multiplication only are mutually interpretable. We will show that they are not equal.

Firstly we observe that the set of even natural numbers, let us denote it by $PAR$, belongs to the spectrum of the arithmetic with addition. Indeed, let $\varphi$ be the following sentence: $\exists x \exists y(y = x + x \wedge y + 1 \neq MAX \wedge y + 1 = MAX)$. Then $Spec(\varphi) = PAR$.

Our next result shows that $PAR$ does not belong to the spectrum of the arithmetic with multiplication.

For $n, c \in N$, by $I(n,c)$ we denote the interval $\langle \lceil \frac{n}{c+1} \rceil, \lfloor \frac{n-1}{c} \rfloor \rangle$. Then, for any element $a \in I(n,c)$, $ca < n$ and $(c+1)a \geq n$. In what follows we use the following consequence of the prime number theorem (see e.g. [19]).

THEOREM 7.4. *a) For arbitrary $k$ there exists $m$ such that for all $n > m$ there are at least $k$ primes between $n$ and $2n$.*

*b) For arbitrary $k$ and $c$ there is $m$ such that for all $n > m$, $I(n,c)$ contains at least $k$ prime numbers.*

We will consider structures from $FM(\mathcal{A})$, where $\mathcal{A} = (\mathbf{N}, \times)$.

The next construction was originally used by the second author in [25] to show that the family $FM((\mathbf{N}, \times))$ is not axiomatizable within the class of all finite models by any set of axioms with bounded quantifier depth.

For arbitrary $n$ we define the structure $\mathcal{A}'$ as follows: ${\mathcal{A}'}_n = (\{0, \ldots, n, \alpha\}, \otimes, n)$, where $\alpha$ is any object outside $|\mathcal{A}_n|$ (for instance any prime number greater than $n$) and $\otimes$ is defined as an extension of the operation $\times$ in $\mathcal{A}_n$ such that $0 \otimes \alpha = \alpha \otimes 0 = 0$, $1 \otimes \alpha = \alpha \otimes 1 = \alpha$, and for each element $b$ of ${\mathcal{A}'}_n$ different than 0 and 1, $b \otimes \alpha = \alpha \otimes b = n$.

An easy verification shows the following

FACT 7.5. *If $p \geq 2$ is a prime number then $\mathcal{A}_{p+1} \cong {\mathcal{A}'}_p$.*

As we noted earlier, every formula is equivalent to some simple formula. So, we can restrict ourselves to the formulas in that form.

The main observation is the following

LEMMA 7.6. *If $n$ is such that there exists at least $k$ primes between $n$ and $2n$ then for each simple sentence of the rank $k$ we have that*

$$\mathcal{A}_{2n+1} \models \varphi \text{ if and only if } {\mathcal{A}'}_{2n+1} \models \varphi.$$

PROOF. The proof is an application of the Ehrenfeucht–Fraïsse games. Note that EF–games can be adapted to the structures with functions. One way of this adaptation goes by a proper reformulation of the notion of the partial isomorphism and restriction of the language to simple formulas only.

To prove the lemma it is enough to show that in the EF–game with $k$ moves on structures $\mathcal{A}_{2n+1}$ and ${\mathcal{A}'}_{2n+1}$ the second player has a winning strategy. That strategy is as follows. As long as the first player does not choose from the structure ${\mathcal{A}'}_{2n+1}$ the element $\alpha$, the second player answers by the same element from the opposite structure. If the first player chooses the element $\alpha$ then the second player answers by choosing any prime number from the interval $(n, 2n)$ which was not taken. It is possible because there are at least $k$ primes between $n$ and $2n$. In the next steps the second player chooses the same element from the opposite structure with an exception for the case when the first player chooses a prime number corresponding to $\alpha$ or some chosen before prime number greater than $n$. In that cases the second player chooses some new prime number from the opposite structure belonging to the interval $(n, 2n)$. To see that such defined strategy is a winning strategy it is enough to observe that the prime numbers from the interval $(n, 2n)$ are indiscernible in both structures. $\dashv$

We obtain the following

COROLLARY 7.7. *For any set $X \in Sp(FM((\mathbf{N},\times)))$, there are only finitely many prime numbers $q$ such that $q+1 \in X$ and $q+2 \notin X$.*

PROOF. It follows from theorem 7.4 that for arbitrary $k$ there exists $m$ such that for all $n > m$ there exist at least $k$ primes between $n$ and $2n$. Moreover, taking $n$ such that $2n+1$ is a prime we obtain, by fact 7.5, that $\mathcal{A}_{2n+2} \cong \mathcal{A}'_{2n+1}$. Thus, by lemma 7.6 the same simple sentences of the rank $k$ are true in $\mathcal{A}_{2n+2}$ and $\mathcal{A}_{2n+1}$. ⊣

As a corollary we obtain

COROLLARY 7.8. *The set of even numbers, $PAR$, does not belong to the spectrum of arithmetic with multiplication.*

The last corollary shows that $Spec(FM((\mathbf{N},+))) \not\subseteq Spec(FM((\mathbf{N},\times)))$. On the other hand, from the proposition 7.3 follows that $Spec(FM((\mathbf{N},\times))) \not\subseteq Spec(FM((\mathbf{N},+)))$. During the preparation of this paper we conjectured that if $X \in Spec(FM((\mathbf{N},+))) \cap Spec(FM((\mathbf{N},\times)))$ then $X$ belongs to $Sp(FM((\mathbf{N})))$, where $(\mathbf{N})$ is the structure of the empty signature. Extending the method used in the proof of corollary 7.7 Leszek Kołodziejczyk proved the above conjecture.

Corollary 7.7 follows then from theorem 7.9. We decided to present both proofs separately to give properly the credits to the results and because the proof of corollary 7.7 is a good preparation for the proof of the next theorem.

By $Fin$ and $coFin$ we denote, respectively, the family of finite and cofinite subsets of $\mathbf{N}$.

THEOREM 7.9 ([10]). $Spec(FM((\mathbf{N},+))) \cap Spec(FM((\mathbf{N},\times))) = Fin \cup coFin$

PROOF. We will show that if $X \in Sp(FM((\mathbf{N},+)))$ and $X \notin Fin \cup coFin$ then $X$ does not belong to $Sp(FM((\mathbf{N},\times)))$. If $X$ is a nontrivial spectrum of addition then there are $d$, $n < d$ and $M$ such that for all $m \geq M$, $md+n \in X$ and $md+n+1 \notin X$. Let us fix such $d$, $n$ and $M$ and let $k$ be an arbitrary integer. We will show that no sentence $\varphi \in \mathcal{F}_{\{\times\}}$ with the quantifier rank $k$ can define the spectrum $X$. Obviously, that proves the theorem.

We need the following fact:

there exists $a$ such that for infinitely many prime numbers $q$

$$(*) \qquad aq+1 \in X \wedge aq+2 \notin X.$$

To prove $(*)$ let us define, for $0 \leq i < d$,

$$S_i = \{md+i \ : \ m \in \mathbf{N}\},$$

and let $i_0$ be such that $S_{i_0}$ contains infinitely many prime numbers. Obviously, $i_0$ is relatively prime with $d$. So, there exists $b$ such that $i_0 b \equiv 1 \mod d$. Then, we take $n'$ such that $n' \equiv n-1 \mod d$ and $0 \leq n' < d$. We define $a = bn'$. We have that for all $z = m_z d + i_0$, $z \in S_{i_0}$,

$$\begin{aligned} za &\equiv i_0 a \\ &\equiv (i_0 b)n' \\ &\equiv n-1 \mod d. \end{aligned}$$

Thus, for any prime $q \in S_{i_0}$, $q \geq M$,

$$aq + 1 \in X \text{ and } aq + 2 \notin X.$$

That proves $(*)$.

We will show that for each big enough prime number $q$, Duplicator has a winning strategy in the $k$–moves Ehrenfeucht–Fraïsse game on structures $\mathcal{A}_{aq}$ and $\mathcal{A}_{aq+1}$. So, for any sentence $\varphi \in \mathcal{F}_{\{\times\}}$ with the quantifier rank $k$, $X \neq Sp(\varphi)$.

Let us choose a prime $q$ such that $aq + 1 \in X$ and $aq + 2 \notin X$ and intervals $I(aq, a)$ and $I(aq, a - 1)$ (see the definition before theorem 7.4) contain more than $k$ prime numbers. Let us observe that prime numbers from $I(aq, a)$ have the same properties in $\mathcal{A}_{aq}$ as the prime numbers from $I(aq + 1, a)$ in $\mathcal{A}_{aq+1}$. Namely, for each $x \in I(aq, a)$,

$$(a + 1)x \geq aq \text{ and, for each } i \leq a,\ ix < aq.$$

Similarly, for each $x \in I(aq + 1, a)$,

$$(a + 1)x \geq aq + 1 \text{ and, for each } i \leq a,\ ix < aq + 1.$$

An analogous fact holds for primes from $I(aq, a - 1)$ in $\mathcal{A}_{aq}$ and primes from $I(aq + 1, a - 1)$ in $\mathcal{A}_{aq+1}$.

Let $\{\alpha, \beta\} = \{aq, aq + 1\}$. During a play of the Ehrenfeucht–Fraïsse game on the structures $\mathcal{A}_{aq}$ and $\mathcal{A}_{aq+1}$, if Spoiler picks up an element $sp$ from $\mathcal{A}_\alpha$, where $p \in I(\alpha, a)$ and $s \leq a$, then Duplicator can choose $sp'$ from $\mathcal{A}_\beta$, where $p' \in I(\beta, a)$. During the remaining part of the game Duplicator identifies the corresponding multiples of $p$ in $\mathcal{A}_\alpha$ and $p'$ in $\mathcal{A}_\beta$. A similar strategy is applied when Spoiler chooses an element $sp$ from $\mathcal{A}_\alpha$, where $p \in I(\alpha, a-1)$ and $s \leq a-1$.

For any other element different than $MAX$ Duplicator answers with the same element from the second structure.

The only prime number which has different properties in $\mathcal{A}_{aq}$ and $\mathcal{A}_{aq+1}$ is $q$. In $\mathcal{A}_{aq}$ it behaves like any other prime from $I(aq, a - 1)$ and in $\mathcal{A}_{aq+1}$ it behaves like primes from $I(aq + 1, a)$. Indeed, $I(aq, a) \cup \{q\} = I(aq + 1, a)$ and $I(aq, a - 1) \setminus \{q\} = I(aq + 1, a - 1)$. However, this fact cannot be detected in $k$ moves of an Ehrenfeucht–Fraïsse game because each of the intervals: $I(aq, a)$, $I(aq, a-1)$, $I(aq+1, a)$ and $I(aq+1, a-1)$ has more than $k$ primes. That shows that Duplicator has a winning strategy in the $k$–moves Ehrenfeucht–Fraïsse game on structures $\mathcal{A}_{aq}$ and $\mathcal{A}_{aq+1}$. ⊣

Now, we turn to the arithmetic with exponentiation. Similarly as we deduced the proposition 7.3 we can deduce from the theorem 4.9 the following.

PROPOSITION 7.10. *Let $X$ belong to the spectrum of arithmetic with multiplication. Then the set*

$$Y = \{r + 1 : \exists n \geq 4(n \in X \wedge 2^{n-2} + 1 \leq r \leq 2^{n-1})\}$$

*belongs to the spectrum of arithmetic with exponentiation.*

From theorem 4.8 immediately follows that $Spec((\mathbf{N}, exp)) \subseteq Spec((\mathbf{N}, \times))$. Now we prove that the above inclusion is strict. Let us denote $\mathcal{A} = (\mathbf{N}, \times)$ and $\mathcal{B} = (\mathbf{N}, exp)$. As we noted in the example 2 $Spec(\Phi_1) = \{n^2 + 1 \ : \ n \in \mathbf{N}\} \in Spec(FM(\mathcal{A}))$. We will show that $Spec(\Phi_1) \notin Spec(FM(\mathcal{B}))$. To prove this it suffices to show that there is no sentence $\varphi$ of arithmetic with exponentiation

such that for 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 $p^2-1 = (p+1)(p-1)$ behaves in $\mathcal{B}_{p^2}$ in a similar way like 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 others prime numbers from the upper half of $\mathcal{B}_{p^2}$.

Thus, we have proved the following theorem.

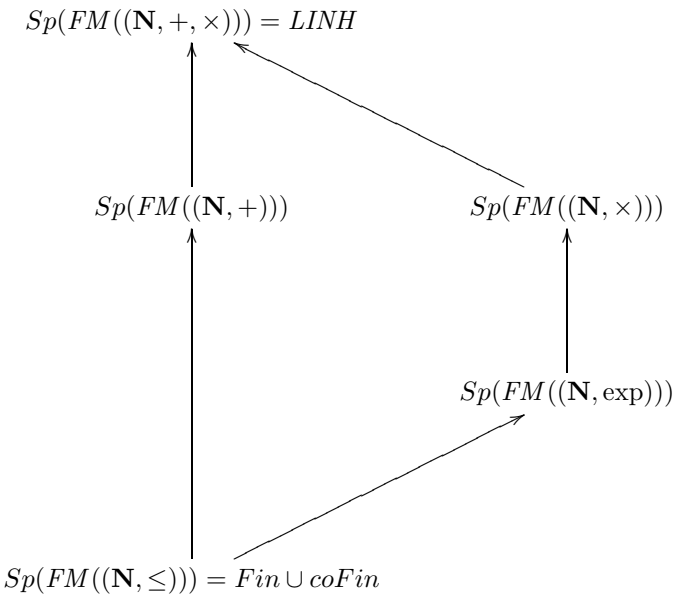
THEOREM 7.11. *The spectrum of arithmetic with exponentiation is strictly included in the spectrum of arithmetic with multiplication.*

As a consequence of this theorem we can deduce that the graph of the multiplication function is not definable in finite models of arithmetics with exponentiation. As a consequence of theorem 7.9 we have the following

COROLLARY 7.12. $Spec((\mathbf{N}, exp)) \cap Spec((\mathbf{N}, +)) = Fin \cup coFin.$

It is easy to give an example of a set in $Spec(FM((\mathbf{N}, \exp)))$ such that it is not ultimately periodic. Therefore, $Spec(FM((\mathbf{N}, +)))$ is not comparable with $Spec(FM((\mathbf{N}, \exp)))$.

We may subsume our considerations on spectra in the following diagram. If there is a way along the arrows from the spectrum of one arithmetic to the spectrum of another one then the first one is strictly included in the second one. The lack of such a way symbolizes incomparability.




Relations between spectra of finite arithmetics.

**§8. Conclusions and open problems.** The presented research investigated the arithmetic in a framework which is closer to the real world situation. Here we assumed that we have only finitely many natural numbers but we did not specify how many. In such approach arithmetics have significantly different properties than in the infinite case.

In the first part of the paper we presented the general conditions under which the definability in a finite arithmetic $FM(\mathcal{A})$ is not stronger than the definability in $\mathcal{A}$. This is the situation when we can define in $\mathcal{A}$ the ordering relation. When the ordering is not present, the arithmetics of finite models can be significantly stronger than in the standard model. That is the case of multiplication. We even saw that multiplication defines exponentiation in finite models. The reason for that is that exponentiation is a fast growing function. In consequence, for many elements $a, b$ the value of $\exp(a, b)$ is outside of a finite model. Of course, the same result can be proven for other fast growing functions like, e.g. $2^{x^y}$.

Both arithmetics: of multiplication and of exponentiation, are weaker than the arithmetic of addition and multiplication. On the other hand, we saw that with respect to $FM$–representability exponentiation is already equivalent to the full arithmetic. As a consequence we obtained the undecidability of $Th(FM(\mathcal{A}))$ and $sl(FM(\mathcal{A}))$, where $\mathcal{A}$ is $(\mathbf{N}, \times)$ or $(\mathbf{N}, \exp)$. Recently, the same results were proven by Mostowski and Wasilewska for the arithmetic of divisibility, see [15]. Also the arithmetic of coprimality can interpret in finite models addition and multiplication. An interpretation was given by Mostowski and Zdanowski in [16]. Thus, coprimality in finite models is as hard as addition and multiplication. Moreover, an interpretation given in [16] does not use the equality predicate.

Finally, we considered the spectrum problem. We have a partial characterization of the spectrum of the arithmetic with multiplication. We gave also some examples of polynomials which range is in $Sp(FM((\mathbf{N}, \times)))$. A natural question which arises is the following: for which polynomials their range is in $Sp(FM((\mathbf{N}, \times)))$?

As we observed in corollary 7.7, for any set $X \in Sp(FM((\mathbf{N}, \times)))$ it is impossible that there are infinitely many prime numbers $q$ such that $q + 1 \in X$ and $q + 2 \notin X$. This can be related to the following number theoretic problem.

Let $f$ be an irreducible polynomial satisfying the following conditions:

- $f$ has integer coefficients with a positive leading coefficient,
- there is no prime number $p$ such that for all $n$, $p$ divides $f(n)$.

It is conjectured that the range of $f$ contains infinitely many primes (see [19], section 8.4). If the latter is true then for no such polynomial $f$ of degree greater than one the set $\{f(n) + 1 : n \in \mathbf{N}\}$ is in $Sp(FM((\mathbf{N}, \times)))$. The last statement can be seen as a weaker version of the mentioned number theoretic conjecture. We can also ask whether there is an extension of the vocabulary of $FM((\mathbf{N}, \times))$ such that the above two conjectures are equivalent?

From Dirichlet's theorem follows that for relatively prime numbers $a$ and $b$ the set $\{an+b : n \in \mathbf{N}\}$ contains infinitely many primes numbers. So, our conjecture holds for such polynomials.

Rather than giving the complete description of arithmetics of finite models the present paper is only a rough approximation of that aim. Definitely, more should

be known on definability in finite models for various arithmetics. Moreover, the dependency between properties of a family $FM(\mathcal{A})$ and of the model $\mathcal{A}$ should be cleared. Little is known about the theories $sl(FM(\mathcal{A}))$, for various $\mathcal{A}$. Obviously, many such theories, which may be theories of the arithmetic of the physical world, have very different properties than the theory of the, so called, standard model.

## REFERENCES


[1] A. Atserias and Ph. Kolaitis, *First order logic vs. fixed point logic on finite set theory*, ***14th IEEE Symposium on Logic in Computer Science (LICS)***, vol. 14, 1999, pp. 275–284.

[2] D. A. Mix Barrington, N. Immerman, and H. Straubing, *On uniformity within $NC^1$*, ***Journal of Computer and System Science***, vol. 41 (1990), pp. 274–306.

[3] J. H. Bennett, *On spectra*, ***Ph.D. thesis***, Princeton University, 1962.

[4] W. Bés, *On pascal triangles modulo a prime power*, ***Annals of Pure and Applied Logic***, vol. 89 (1997), pp. 17–35.

[5] J. R. Büchi, *Weak second–order arithmetic and finite automata*, ***Z. Math. Logik Grundl. Math.***, vol. 6 (1960), pp. 66–92.

[6] M. Davis, *Hilbert's tenth problem is unsolvable*, ***American Mathematical Monthly***, vol. 80 (1973), pp. 233–269.

[7] A. Dawar, K. Doets, S. Lindell, and S. Weinstein, *Elementary properties of the finite ranks*, ***Mathematical Logic Quarterly***, vol. 44 (1998), pp. 349–353.

[8] H.-D. Ebbinghaus, J. Flum, and W. Thomas, ***Mathematical logic***, Springer–Verlag, 1994, second edition.

[9] P. Hájek and P. Pudlák, ***Metamathematics of first–order arithmetic***, Springer Verlag, 1993.

[10] L. A. Kołodziejczyk, Private communication.

[11] I. Korec, *Elementary theories of structures containing generalized pascal trangles modulo a prime*, ***Proc. of the 5th Conference on Discrete Mathematics and Applications, Blagoevgrad*** (S. Shtrakov and I. Marchev, editors), 1995, pp. 91–105.

[12] T. Lee, *Arithmetical definability over finite structures*, ***Mathematical Logic Quarterly***, vol. 49 (2003), pp. 385–393.

[13] M. Mostowski, *On representing concepts in finite models*, ***Mathematical Logic Quarterly***, vol. 47 (2001), pp. 513–523.

[14] ———, *On representing semantics in finite models*, ***Philosophical Dimensions of Logic and Science*** (A. Rojszczak†, J. Cachro, and G. Kurczewski, editors), Kluwer Academic Publishers, 2003, pp. 15–28.

[15] M. Mostowski and A. Wasilewska, *Elementary properties of divisibility in finite models*, ***Mathematical Logic Quaterly***, vol. 50 (2004), pp. 169–174.

[16] M. Mostowski and K. Zdanowski, *$FM$–representability and beyond*, in preparation.

[17] J. Mycielski, *Analysis without actual infinity*, ***The Journal of Symbolic Logic***, vol. 46 (1981), pp. 625–633.

[18] ———, *Locally finite theories*, ***The Journal of Symbolic Logic***, vol. 51 (1986), pp. 59–62.

[19] M. B. Nathanson, ***Elementary methods in number theory***, Springer, 2000.

[20] W. Quine, *Concatenation as a basis for arithmetic*, ***The Journal of Symbolic Logic***, vol. 11 (1946), pp. 105–114.

[21] N. Schweikardt, *On the expressive power of first-order logic with built-in predicates*, ***Ph.D. thesis***, Johannes Gutenberg-Universität Mainz, 2001.

[22] A. L. Semenov, *Logical theories of one–place functions on the set of natural numbers*, ***Izv. Akad. Nauk. SSSR ser. Mat.***, vol. 47 (1983), pp. 623–658.

[23] J. R. Shoenfield, ***Recursion theory***, Lectures Notes in Logic, Springer–Verlag, 1993.

[24] C. Smoryński, ***Logical number theory i***, Springer, 1981.

[25] K. Zdanowski, *Arithmetics in finite but potentially infinite worlds*, ***Ph.D. thesis***, Warsaw University, 2004.

MICHAŁ KRYNICKI,
CARDINAL STEFAN WYSZYŃSKI UNIVERSITY
WARSAW, POLAND
*E-mail*: krynicki@uksw.edu.pl

KONRAD ZDANOWSKI,
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCE
ŚNIADECKICH 8
00–956 WARSZAWA, POLAND
*E-mail*: konrad.zdanowski@wp.pl