Finite arithmetics

Michał Krynicki
Department of Mathematics and Exact Science
Uniwersity of Cardinal Stefan Wyszyński, Warsaw

Marcin Mostowski
Department of Logic
Institute of Philosophy, Warsaw University

Konrad Zdanowski
Institute of Mathematics
Polish Academy of Science

March 22, 2007

Abstract

The paper presents the current state of knowledge in the field of logical investigations of finite arithmetics. This is an attempt to summarize the ideas and results in this area. Some new results are presented — this are mainly genralizations of the earlier results related to properties of sl–theories and some nontrivial cases of FM–representability theorem.

keywords: finite models, arithmetic, finite arithmetic, interpretations, complete sets, FM–representability, truth definitions.

Contents

1 Introduction

Finite arithmetics were object of interest for deep practical reasons for many years in computer science and cryptography. In electronic computer technology we use essentially finite approximations of the set of natural numbers. In C terminology *long unsigned* numbers take 4 bytes of memory. It means that they can be represented in binary notation as numerals with 32 binary digits, from 0 to $2^{32} - 1$. For some purposes we use bigger natural numers representations by representing them as arrays of integers. In this way we obtain essentially larger numbers, but still only finitely many of them. Elaborating of algorithms for such restricted natural numbers we have to take into account that they are bound — oppositely to unbouded natural numbers in mathematics.[1]

Cryptographic algorithms are usually designed for carrying them out on electronic computers. They are based on representations of texts as natural numbers. Then by application of some suitable algorithm these numbers are represented by other numbers called encrypted messages. No wonder that such algorithms apply bounded natural numbers. However, independently of their implementations, these algorithms substantially apply natural numbers of bounded size. We can guess that future discoveries will not change this situation.

Our approch to finite arithmetics is from logical point of view. It is worth of noticing that practically all papers openly treating this subject as their main topic were published in XXI century. There are many results related to finite arithmetics in papers published earlier. Nevertheless no one of them was addressed to this area. Hoare in [Hoa69] considers some possible methods of proving properties of programs. He stresses there imortance of finite arithmetic approach. This paper has a lot of descendants, but no one of them takes into account of finite approach.

Our approach emanated from finite model theory. This is not accidental, because the main earlier results in this area were published in papers devoted to finite model theory.

[1]The term finite arithmetics is also used to computer representations of calculations on real numbers. We do not go in this direction. Nevertheless, it is worth to notice that some authors consider this case of finiteness as based on finteness of natural numbers, see [Myc81].

Moreover finite arithmetics as treated logically are essentially a subarea of finite model theory.

We discuss in this paper the basic ideas motivating some crucial concepts of our approach. These are mainly considerations related to an approach of transferring the tarskian method of truth definitions to finite case. The idea of FM truth definitions (from [Mos01]) motivated such notions as *truth in sufficiently large finite models* and *FM–representability*.

* * *

We give a survey of the results and methods related to logical approach to finite arithmetics. Obviously this reflects our mathematical and philosophical ideas. Nevertheless the problems considered seems to be of general significance.

We tried to make the paper self–contained — at least in the concepual sense — by explaining on the intuitive level everything what is not presented with all technical details. For all the main theorems we tries to supply at least sketchy proofs or some intuitive arguments. Of course in all these cases detailed proofs are given in the references.

2 Basic notions

Let $\mathcal{A}$ be a model having as a universe the set of natural numbers, i.e.

$$\mathcal{A} = (\mathbb{N}, R_1, \ldots, R_s, f_1, \ldots, f_t, a_1, \ldots, a_r),$$

where $R_1, \ldots, R_s$ are relations on $\mathbb{N}$, $f_1, \ldots, f_t$ are operations on $\mathbb{N}$ and $a_1, \ldots, a_r \in \mathbb{N}$. We will consider finite initial fragments of these models. Namely, for every positive $n \in \mathbb{N}$, by $\mathcal{A}_n$ we denote the following structure

$$\mathcal{A}_n = (\{0, \ldots, n-1\}, R_1^n, \ldots, R_s^n, f_1^n, \ldots, f_t^n, a_1^n, \ldots, a_r^n, n-1),$$

where R_i^n is the restriction of R_i to the set $\{0, \ldots, n-1\}$, f_i^n is defined as

$$f_i^n(b_1, \ldots, b_{n_i}) = \begin{cases} f_i(b_1, \ldots, b_{n_i}) & \text{if } f(b_1, \ldots, b_{n_i}) < n-1 \\ n-1 & \text{if } f(b_1, \ldots, b_{n_i}) \geq n-1 \end{cases}$$

and $a_i^n = a_i$ if $a_i < n$, otherwise $a_i^n = n-1$. We will denote the family $\{\mathcal{A}_{n+1}\}_{n \in \mathbb{N}}$ 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.

Let $\varphi(x_1, \ldots, x_p)$ be a formula and $b_1, \ldots, b_p \in \mathbb{N}$. We say that φ *is satisfied by* $b_1, \ldots, b_p$ *in all finite models of* $FM(\mathcal{A})$, what is denoted by $FM(\mathcal{A}) \models \varphi[b_1, \ldots, b_p]$, if for all $n > max(b_1, \ldots, b_p)$ $\mathcal{A}_n \models \varphi[b_1, \ldots, b_p]$. We say that φ *is satisfied by* $b_1, \ldots, b_p$ *in all sufficiently large finite models of* $FM(\mathcal{A})$, what is denoted by $\mathrm{FM}(\mathcal{A}) \models_{\mathrm{sl}} \varphi[b_1, \ldots, b_p]$, if there is $k \in \mathbb{N}$ such that for all $n \geq k$ $\mathcal{A}_n \models \varphi[b_1, \ldots, b_p]$.

When no ambiguity arises we will use $\models_{\rm sl} \varphi[b_1, \ldots, b_p]$ instead of $\mathrm{FM} \models_{\rm sl} \varphi[b_1, \ldots, b_p]$.

Finally, a sentence φ *is true in all finite models of* $FM(\mathcal{A})$ if $\mathcal{A}_n \models \varphi$ for all $n \in \mathbb{N}$. Similarly, a sentence φ *is true in all sufficiently large finite models of* $FM(\mathcal{A})$ if there is $k \in \mathbb{N}$ such that for all $n \geq k$, $\mathcal{A}_n \models \varphi$. By $sl(FM(\mathcal{A}))$ we denote the set of sentences true in all sufficiently large finite models of $FM(\mathcal{A})$. So, we have

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

A most typical structures strictly related to the arithmetic are standard models for arithmetic of addition, multiplication and the so called full arithmetic, i.e. structures $(\mathbb{N}, +)$, $(\mathbb{N}, \times)$, $(\mathbb{N}, +, \times)$, respectively. The last structure will be denoted by $\mathcal{N}$. However, from the computer science point of view some other arithmetical structures are important. These are the following:

- $(\mathbb{N}, \mathrm{BIT})$, where the relation BIT is defined as follows: $\mathrm{BIT}(x, y)$ if and only if the x-th bit in the binary representation of y is one. Thus, if $y = \Sigma_{i=0}^{\infty} a_i 2^i$, where $a_i \in \{0, 1\}$, then
$$\mathrm{BIT}(x, y) \ \text{ if and only if } \ a_x = 1.$$
The structure $(\mathbb{N}, \mathrm{BIT})$ is isomorphic to the domain of the hereditarily finite sets $\mathsf{HF} = (V_\omega, \in)$, where $V_\omega = \bigcup_{i \in N} V_i$, where $V_0 = \emptyset$ and, for $i \in \mathbb{N}$, $V_{i+1} = \mathcal{P}(V_i)$ – the powerset of V_i.

- $\mathsf{FW}^t = (\Gamma_t^*, *_t, \mathbf{a}_1, \ldots, \mathbf{a}_t)$, where Γ_t^* is the set of all words over $\Gamma_t = \{a_1, \ldots, a_t\}$, i.e. the set of finite sequence of elements from Γ_t, $*_t$ is the concatenation operation on words from Γ_t^* and $\mathbf{a}_i$ is a word consisting of one character a_i.

Finite words in the universe of FW^t can be identified with natural numbers via t–adic representation. The correspondence between finite words and natural numbers is established by a function $n_t \colon \Gamma_t^* \longrightarrow \omega$, where $n_t(\lambda) = 0$, $n_t(\mathbf{a_i}) = \mathbf{i}$, for $1 \leq i \leq t$, and $n_t(u_n \ldots u_0) = \Sigma_{i=0}^{i=n} n_t(u_i) t^i$, for $u_i \in \Gamma_t$.

Thus we simply ordered all finite words in such a way that shorter words always occur earlier and words of the same lenght are ordered lexicographicaly.

Also, it is not hard to prove that HF is isomorphic to $(\mathbb{N}, \mathrm{BIT})$. The claimed isomorphism function can be defined by induction on i for the family $\{V_i\}_{i \in \mathbb{N}}$. The function $f_0 \colon V_0 \longrightarrow \mathbb{N}$ is just the empty function and if we defined $f_i \colon V_i \longrightarrow \mathbb{N}$ then $f_{i+1} \colon V_{i+1} \longrightarrow \mathbb{N}$ 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 $f = \bigcup_{i \in \mathbb{N}} f_i$ is a well defined function and that it is the unique isomorphism between HF and $(\mathbb{N}, \mathrm{BIT})$.

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 $FM(\mathsf{FW}^t)$ and $FM(\mathsf{HF})$.

We use Σ_n^k, Π_n^k, Δ_n^k notation in three different meanings. Their meaning should be clear from the context. For example Δ_0-formula is an arithmetical formula with all quantifier

bounded. Σ_2^0 -formula is a formula of the form $\exists x_1 \ldots \exists x_n \forall y_1 \ldots \forall y_m \varphi$, where φ is a Δ_0 formula.

Σ_n^0-set (Π_n^0-set) is a set of natural numbers definable by an arithmetical Σ_n^0 (Π_n^0) formula. Recall that a set is Δ_n^0 if it is both Σ_n^0 and Π_n^0 set.

A set (class) of models is Σ_1^1 if there is a Σ_1^1 sentence φ (existential second order formula) such that this set (class) contains exactly these models in which φ is true.

Finally, let us describe the expressive power of arithmetic in finite models in terms of computational complexity.

Let $\mathrm{NLINTIME}_1$ be the class of relations which are computable on nondeterministic Turing machines which works in linear time. Then, $\mathrm{NLINTIME}_{i+1} = \mathrm{NLINTIME}_1^{\mathrm{NLINTIME}_i}$ is the class of relations which are computable on nondeterministic Turin machines which works in linear time and use the oracle from $\mathrm{NLINTIME}_i$. By the linear time hierarchy, LINH, we denote the union of all $\mathrm{NLINTIME}_i$.

It is known, from the results of Wrathall, [Wra78], and Bennett, [Ben62], that Δ_0 definable relations in the standard model are just relations in the linear time hierarchy. Now we formulate a version of this theorem for finite models.

Let $R \subseteq \omega^k$ be the relation in LINH. Then, there is a formula $\psi(x_1, \ldots, x_k)$ such that for each model $\mathcal{N}_i \in \mathrm{FM}(\mathcal{N})$ the following holds:

$$R \cap \{0, \ldots, i-1\}^k = \{(a_1, \ldots, a_k) : \mathcal{N}_i \models \psi[a_1, \ldots, a_k]\},$$

that is for each $i > 0$, ψ defines in $\mathcal{N}_i$ the relation R restricted to the universe of $\mathcal{N}_i$. It follows that in finite models the expressive power of arithmetical formulas is essentially the same as Δ_0 formulas in the standard model $\mathcal{N}$. Let us remark that this fact is not totally obvious because in the standard model we can bound quantifiers by arbitrary terms of our language. Thus, having a free variable x we can bound quantifiers by any polynomial in x. On the other hand in finite models we have no acces to elements which are greater than the maximal element of a given finite model. To show that we can replace the quantification bounded by terms with quantification bounded by variables only one should use the result by Paris and Dimitracopoulos from [PD82]. They show there (in proposition 1) that each Δ_0 formula (with terms) is equivalent to a Δ_0 formula in the relational arithmetical language with only variables as quantifiers bounds. (To be exact it should be said that Paris and Dimitracopoulos consider Δ_0 formulas with complex terms inside and only variables as bounds for quantifiers. However, it is easy to translate e.g. $Qx \leq z * z\varphi(x)$ as $Qx_1 \leq zQx_2 \leq z\varphi(x_1 z + x_2)$. Thus, this restriction is not essential in obtaining the theorem in the form which we present.)

3 Elementary properties of sl–theories

A basic logical properties of the set of sentences $\mathrm{sl}(\mathcal{A})$ are given in the following proposition.

Proposition 3.1 ([Mos01],[KTZ]) *For every structure $\mathcal{A}$ having as a universe the set of natural numbers we have*

a) $\mathrm{sl}(\mathcal{A})$ *have no finite models*

b) $\mathrm{sl}(\mathcal{A})$ *is closed under logical consequences, i.e. for every sentence φ we have: $\varphi \in \mathrm{sl}(\mathcal{A})$ if and only if $\mathrm{sl}(\mathcal{A}) \vdash \varphi$.*

c) $\mathrm{sl}(\mathcal{A})$ *is consistent*

d) A sentence φ is consistent with $\mathrm{sl}(\mathcal{A})$ *if and only if φ is true in infinitely many structures from $FM(\mathcal{A})$.*

e) $\mathrm{sl}(\mathcal{A})$ *is not finitely axiomatizable*

Proof. To prove *(a)* it is enough to observe that for every natural n the sentence "there exists at least n elements" holds in all structures $\mathcal{A}_k$, where $k \geq n$. The point *(b)* follows immediately from the definition of sl. Points *(c)* and *(d)* are immediate consequencies of *(b)*. To prove *(e)* assume that $\mathrm{sl}(\mathcal{A})$ is finitely axiomatizable. So, there exists a sentence φ which is an axiomatization of $\mathrm{sl}(\mathcal{A})$. This means that every model for φ is a model for $\mathrm{sl}(\mathcal{A})$. Thus by *(a)* every model for φ is infinite. But by *(b)* $\varphi \in \mathrm{sl}(\mathcal{A})$ what means that φ is true in structure $\mathcal{A}_n$ if n is enough big. So, φ has a finite model. Contradiction.

An easy verification shows that we have the following relation between the theory of a structure $\mathcal{A}$ and $\mathrm{sl}(\mathcal{A})$.

Proposition 3.2 ([KZ05]) *a) If $\mathcal{A} \models \varphi$ and φ is existential sentence then $\varphi \in \mathrm{sl}(\mathcal{A})$.*

b) If $\mathcal{A} \models \varphi$ and φ is a Σ^0_2–sentence without function symbols then $\varphi \in \mathrm{sl}(\mathcal{A})$.

By Łoś theorem (see e.g. [BS71]) we can easily deduce that for every ultrafilter F on $\mathbb{N}$ and every $\varphi \in \mathrm{sl}(\mathcal{A})$, $\Pi_{n\in\mathbb{N}}\mathcal{A}_n/F \models \varphi$. So, for every ultrafilter F on $\mathbb{N}$ the theory $Th(\Pi_{n\in\mathbb{N}}\mathcal{A}_n/F)$ is a complete extension of $\mathrm{sl}(\mathcal{A})$.

We can also characterize extensions of the theory $\mathrm{sl}(\mathcal{A})$ by an other way. For this aim we need to generalize the notion of sl-theory.

Let $X \subseteq \mathbb{N}$. By sl–*theory of $\mathcal{A}$ restricted to X* we mean the following set of sentences

$$\mathrm{sl}_X(\mathcal{A}) = \{\varphi \ : \ \exists k \forall n \geq k (n \in X \Rightarrow \mathcal{A}_n \models \varphi)\}.$$

When X is a cofinite set then $\mathrm{sl}_X(\mathcal{A})$ is just $\mathrm{sl}(\mathcal{A})$ but in general $\mathrm{sl}_X(\mathcal{A})$ could contain more sentences. Obviously, for an arbitrary infinite set of natural numbers X, the set of sentences $\mathrm{sl}_X(\mathcal{A})$ has similar logical properties as $\mathrm{sl}(\mathcal{A})$. In particular, it has the properties expressed in propositions 3.1 and 3.2. As we will see, any complete extension T of $\mathrm{sl}(\mathcal{A})$ can be characterized by a suitable X.

Theorem 3.3 ([KTZ]) *For $\mathcal{A}$ and any set of sentences $T \supseteq \mathrm{sl}(\mathcal{A})$ closed under first order consequencies one can choose an X such that $T = \mathrm{sl}_X(\mathcal{A})$.*

Proof. Let $T = \{\varphi_i\}_{i\in\mathbb{N}}$ be an extension of $\mathrm{sl}(\mathcal{A})$. Let $(\psi_i)_{i\in\mathbf{N}}$ be a sequence of all consistent with T sentences. Moreover, assume that every sentence which is consistent

with T occurs in $(\psi_i)_{i\in\mathbb{N}}$ infinitely many times. We construct a sequence of integers $(x_i)_{i\in\mathbb{N}}$ as follows:

$x_0 = 0$

$x_{i+1} = \min\{n \ : \ x_i < n \text{ and } \mathcal{A}_n \models \psi_i \wedge \bigwedge_{j\leq i+1} \varphi_i\}$.

Since T is a consistent extension of $\mathrm{sl}(\mathcal{A})$ and for each i, ψ_i, is a consistent with T sentence then for each i the sentence $\psi_i \wedge \bigwedge_{k\leq i} \varphi_k$ is consistent with $\mathrm{sl}(\mathcal{A})$. By the proposition 3.1(d) this sentence has arbitrary large finite models in $\mathrm{FM}(\mathcal{A})$. Therefore, $(x_i)_{i\in\mathbb{N}}$ is a well defined infinite sequence of integers. Moreover, we have:

- $x_i < x_{i+1}$, for $i \in \mathbb{N}$,
- for all $i \in \mathbb{N}$, for all $j \geq i$, $\mathcal{A}_{x_j} \models \varphi_i$,
- if ψ is a sentence consistent with T then for arbitrary i there is $j > i$ such that $\mathcal{A}_j \models \psi$.

From the above properties it follows that for $X = \{x_i\}_{i\in\mathbb{N}}$, $\mathrm{sl}_X(\mathcal{A}) = T$.

□

From the proof of the last teorem we can deduce the following.

Corollary 3.4 *For $\mathcal{A}$ and any complete extension T of $\mathrm{sl}(\mathcal{A})$ one can choose an X such that $T = \mathrm{sl}_X(\mathcal{A})$. Moreover, X is recursive in T.*

The following observation follows immediately from the definition and Łoś theorem.

Proposition 3.5 *For arbitrary infinite set $X \subseteq \mathbb{N}$ and nonprincipal ultrafilter U on $\mathbb{N}$ such that $X \in U$, $\mathrm{sl}_X(\mathcal{A}) \subseteq Th(\prod_{n\in\mathbb{N}} \mathcal{A}_n/U)$.*

Let us observe that if T is a complete extension of $\mathrm{sl}(\mathcal{A})$ and X is a set constructed in the proof of theorem 3.3 then for any nonprincipal ultrafilter U such that $X \in U$, $T = Th(\prod_{n\in\mathbb{N}} \mathcal{A}_n/U)$. So, we have the following.

Proposition 3.6 *For arbitrary complete extension T of $\mathrm{sl}(\mathcal{A})$ there exists a nonprincipal ultrafilter U such that $T = Th(\prod_{n\in\mathbb{N}} \mathcal{A}_n/U)$.*

From propositions 3.6 we have

Corollary 3.7 $\mathrm{sl}(\mathcal{A}) = \bigcap_U Th(\prod_{n\in\mathbb{N}} \mathcal{A}_n/U)$*, where the intersection is taken over all nonprincipal ultrafilters on $\mathbb{N}$.*

4 Representing concepts in finite models

One of the main questions[2] related to finite arithmetics is the problem of FM–representability in a given FM–domain.

Let an arithmetical model $\mathcal{A}$ be given, $K = \mathrm{FM}(\mathcal{A})$. Let us recall that a sentence φ is true in sufficiently large models from K ($K \models_{sl} \varphi$) if there is n, such that for all k greater than n, $\mathcal{A}_k \models \varphi$.

Let $\varphi(x_1, \ldots, x_n)$ be a formula and $S \subseteq \omega^n$. We say that $\varphi(x_1, \ldots, x_n)$ FM–represents S in K if for all $a_1, \ldots, a_n \in \omega$ the following two conditions are satisfied:

1. if $S(a_1, \ldots, a_n)$ then $K \models_{sl} \varphi(a_1, \ldots, a_n)$,
2. if $\neg S(a_1, \ldots, a_n)$ then $K \models_{sl} \neg\varphi(a_1, \ldots, a_n)$,

So, the idea of this definition is that a formula φ FM–represents a relation between natural numbers if for any given finite fragment of that relation φ correctly describes this fragment in all sufficiently large finite initial segments of $\mathcal{A}$ (for both positive and negative cases).

This notion and its basic properties was presented in the paper [Mos01]. Originally it was motivated by studying truth definitions in finite models (FM truth definitions).

4.1 FM truth definitions

For explaining the relation, firstly let us recall some historical facts about diagonal semantical arguments from papers by Gödel [Göd31] and Tarski [Tar33].

Gödel's first theorem is traditionally justified as follows: firstly we prove that all notions necessary for the diagonal lemma and proof theoretic relations are recursive.[3] Then we prove that all recursive notions are representable in the considered theory (e.g. PA), and combining this two ideas we construct a proper independent statement.

From our current point of view Tarski's contribution was mainly philosophical. At the begining of his historical paper Gödel essentially gives the proof of Tarski's theorem about undefinablity of truth — calling it an *informal argument* for his first main theorem.[4]

Tarski's undefinability of truth theorem can be justified according to the same scheme. Firstly we prove that all the notions required for the diagonal lemma are arithmetically definable. Then we have the lemma in the following form.

[2]This opinion is of course motivated by our methamathematical point of view.

[3]As a matter of fact Gödel considered primitively recursive relations. However, a few years later his idea was improved by observing that exactly recursive notions are representable in this way. Let us recall that Gödel's paper contains the first mathematical approximation of the notion of computability.

[4]It is known that the work by Tarski was independent from Gödel. The first version of his work was presented before publication of the paper by Gödel. Nevertheless all later presentations of ideas of Tarski are combined with the argument by Gödel.

Gödel's considerations were essentially more subtle from logical point of view. Proof theoretical approach assumed by Gödel gives better understanding assumptions, and — as a result — gives as a corollary another important theorem *the second Gödel theorem*. The main disadvantage of his approach is the lack of understanding semantics, and semantics was the main contribution of Tarski. Tarski's contribution allows to treat Gödel's *informal argument* as a correct easy proof of *the first Gödel theorem*.

Lemma 4.1 (The diagonal lemma) *For each arithmetical formula $\varphi(x)$ with one free variable x there is an arthmetical sentence ψ such that $\mathcal{N} \models (\psi \equiv \varphi(\ulcorner \psi \urcorner))$, where $\ulcorner \psi \urcorner$ is the Gödel number for ψ.*

For the notion of truth Tarski assumes very weak and basic condition. Particularly a formula $\varphi(x)$ with one free variable x defines arithmetical truth if $\mathcal{N} \models (\psi \equiv \varphi(\ulcorner \psi \urcorner))$, for each arithmetical sentence ψ.[5] Now we can easily justify the following.

Theorem 4.2 (The Tarski undefinability of truth theorem) *There is no arithmetical formula defining arithmetical truth.*

Proof. Let us assume the opposite. Then there is a formula $\varphi(x)$ with one free variable x such that $\mathcal{N} \models (\psi \equiv \varphi(\ulcorner \psi \urcorner))$, for each arithmetical sentence ψ. However — by the diagonal lemma — there is an arithmetical sentence ψ_0 such that $\mathcal{N} \models (\psi_0 \equiv \neg\varphi(\ulcorner \psi_0 \urcorner))$. Combaining these two statements we easily obtain the contradiction. □

Let us observe that in this reasoning we essentially use the fact that arithmetical formulae are closed on negations. Logics not closed on negations can contain its own truth definitions. One of the most important examples is so called Σ^1_1–logic.

This theorem gives a very powerfull tool for proving hierarchy theorems for second order logic — as well as for other logics. Having two logics L and L' we say that L' is stronger than L if each class of models definable by L–sentences is also definable by L'–sentences but not vice versa. The fact that L' is stronger than L can be justified by the Tarski method by proving that the logic L' have a formula defining truth for L–sentences. Another application of the method is proving that some logics are not closed on negations. For this purpose it suffices to show that the logic considered has a formula defining truth for all of its sentences. In this way we can easily justify that Σ^1_1–logic is not closed on negations.

We recall these ideas for explaining the idea of transferring the method to finite models. We know — by Fagin's theorem (see [Fag74]) — that Σ^1_1–logic on finite models capture NP complexity class. It means particularly that Σ^1_1–logic is equivalent to Π^1_1–logic on finite models. Because negations of Σ^1_1–formulae are eqivalent to Π^1_1–formulae then one of the most difficult open problems of computational complexity – whether $NP = coNP$ – is equivalent to the question whether Σ^1_1–logic is closed on negations on finite models. As we observed the method of truth definitions solves the question negatively for infinite models. The problem restricted to finite models seems to be very hard and remains open. Can we apply a similar methods in finite models for answering such questions? An attempt of transferring the method to finite models framework was made in [Mos93] (published later in [Mos01][6]).

[5]This definition — in english literature — is called *T—convention*. However, in polish version of the Tarski's work it is called *P—convention* and in german version of the Tarski's work it is called *W—convention*. The both names are taken from polish and german words for *truth* — correspondingly: *prawda* and *Warheit*.

[6]The paper [Mos93] circulated as a manuscript and its ideas and results were published only in conference abstracts, firstly it was published as a part of [Mos01].

The idea is based on the observation that for correct description of the required syntactict properties of a given formula we do not need all natural numbers but some sufficiently large initial segment of them would be enough. So, we say that a formula $\varphi(x)$ defines thruth in finite models (shortly FM truth) for a logic L if for each L–sentence ψ the sentence

$$\psi \equiv \varphi(\ulcorner \psi \urcorner)$$

is true in almost all finite models, where $\ulcorner \psi \urcorner$ is the Gödel number of ψ.

For the sake of a proper undefinability theorem we need a suitable version of the diagonal lemma.

Lemma 4.3 (The FM **diagonal lemma)** *For each arithmetical formula $\varphi(x)$ with one free variable x there is an arthmetical sentence ψ such that* $\mathrm{FM}(\mathcal{N}) \models_{sl} (\psi \equiv \varphi(\ulcorner \psi \urcorner))$, *where $\ulcorner \psi \urcorner$ is the Gödel number for ψ.*

Now the FM version of the Tarski undefiability theorem can be justified in almost the same way as the original one.

Theorem 4.4 (The FM **version of the Tarski undefinability of truth theorem)** *There is no arithmetical formula defining arithmetical* FM *truth.*

Let us observe that we did not yet prove our FM diagonal lemma. It easily follows from the FM representability theorem. It will be justified in the next subsection. Now let us observe that FM version of the Tarski theorem can be applied in a similar way as the original version. Similarly as in infinite case FM–truth definitions can be applied for comparing semantical power of some logics. Particularly if we can give FM–truth definition in L' for L then L' restricted to finite models is stronger than L. This method can be applied equally well for justifying "non closure on negations" properties.

These ideas were developped later in the papers [Mos03, Koł04a]. Leszek Kołodziejczyk successfully applied the method for computational complexity questions in [Koł04b, Koł05].

4.2 FM representability theorem

For successful applying the methods discussed above we need some representations of syntactical and semantical properties in finite models. We will use here introduced in the begining of this section the notion of the FM-representability.

The class of FM–representable relations essentially depends on on our choice of basic arithmetical notions. The maximal one (of course for recursive basic relations) we obtain by considering FM–domain of addition and multiplication.

Theorem 4.5 (The FM–**representability theorem, M. Mostowski 2001, [Mos01])** *Let S be a relation on natural numbers. Then the following are equivalent:*

1. *S is FM-representable (in $FM(\mathbb{N}, \times, +)$); (– in terms of expressibility in finite models)*

2. *S is recursive with recrsively enumerable oracle; (– in terms of oracle machines)*

3. *S is of degree $\leq \mathbf{0}'$; (– in terms of Turing degrees)*

4. *S is recursive in the limit; (– in terms of algorithmic learning theory, see [Gol65] and [Gol67])*

5. *S is Δ^0_2 in arithmetical hierarchy. (– in terms of arithmetical definability)*

Proof. Of course the FM–representability theorem is the equivalence of the first condition with all the remaining. The justifications of the equivalence of the conditions 2 — 5 can be found e.g. in [Sho93] and [Gol65].

Let us observe that both cases postive and negative for FM–representability are defined by Σ^0_2–formulae. It follows that all FM–representable relations are Δ^0_2–definable.

Following [Mos01] we will show that all relations recognized by by oracle Turing machines with recursively enumerable oracles are FM–representable. Let M_1 be an oracle deterministic Turing machine recognizing n–ary relation[7] R by using an oracle S, which is recognized by the halting condition by a deterministic Turing machine M_2. Our FM–representing formula $\varphi(x_1, \ldots, x_n)$ for R can be formulated as follows:

for a given input $x_1, \ldots, x_n$ if there is an accepting computation of M_1 such that all oracle questions are answered positively exactly if M_2 halts taking them as inputs.

For each given input $a_1, \ldots, a_n$ we can find a model of size sufficient to contain the unique M_1–computation c and all required witnesses for oracle questions put by c for accepting them correctly as members of S — all not accepted oracle questions will be rejected as members of S. □

If the relation satisfies one of the above equivalent conditions then we say that it is FM–representable.

4.3 FM–representability in other domains

Let us observe that if all the relations in a model $\mathcal{A}$ are recursive then the truth relation of models from FM($\mathcal{A}$) is also recursive. Thus from the definition of FM–representability we obtain the following.

Theorem 4.6 *Let $\mathcal{A}$ be a model on natural numbers having all relations recursive. Then the relations* FM*–representable in* FM($\mathcal{A}$) *are Δ^0_2 arithmetically definable.*

It means that the FM–representability theorem gives the upper bound for the FM–representability in a natural sense. However for some FM–domains essentially weaker classes of relations can be FM–represented. Particularly it was observed in [KZ05] that in the FM–domain of addition exactly semilinear relations are FM–representable. This and other interesting examples will be considered in section 7.

[7] In finite models we cannot restrict to sets of natural numbers because finite models are not closed on pairing function.

5 Specific finite arithmetics

The main interesting questions concerning sl-theories are connected with the fundamental arithmetical structures like $(\mathbb{N}, +)$, $(\mathbb{N}, \times)$, and $(\mathbb{N}, +, \times)$. Relations between theories of these structures as well as properties of these theories are subject of well known classical results (see e.g. a nice survey [Bes02]). Now, we put the following question: if a similar results hold for sl-theories of these structure or not? An answer for such question is connected with apriopriate notions of definability and interpretability of sl-theories and FM-domains.

5.1 Definability

Definition 5.1 *Let $\mathcal{A}$ be a model, let $\sigma = \{P_1, \ldots, P_m\}$ be a relational vocabulary and let $\bar{\varphi} = (\varphi_U, \varphi_1, \ldots, \varphi_m)$ be the sequence of formulae. Then, by $I_{\bar{\varphi}}(\mathcal{A})$ we denote the model of the vocabulary σ which is definable in $\mathcal{A}$ by $\bar{\varphi}$.*

We say that $\mathcal{B}$ is definable by $\bar{\varphi}$ in $\mathcal{A}$ if $\mathcal{B} = I_{\bar{\varphi}}(\mathcal{A})$.

We say that $\mathrm{FM}(\mathcal{B})$ *is definable in* $\mathrm{FM}(\mathcal{A})$ *if there is a sequence of formulae $\bar{\varphi}$ such that for each $n > 0$, $\mathcal{B}_n = I_{\bar{\varphi}}(\mathcal{A}_n)$.*

If $\mathrm{FM}(\mathcal{A})$ *is definable in* $\mathrm{FM}(\mathcal{B})$ *and* $\mathrm{FM}(\mathcal{B})$ *is definable in* $\mathrm{FM}(\mathcal{A})$ *then we say that* $\mathrm{FM}(\mathcal{A})$ *and* $\mathrm{FM}(\mathcal{B})$ *are mutually definable.*

In the case of nonrelational vocabulary the above definition can be formulated in a similar way, by treating k-ary functions as $k+1$-ary relation and constants as a unary relation.

Let us remaind that by $\mathcal{N}$ we denote the standard model for full arithmetic, i.e. $\mathcal{N} = (\mathbb{N}, +, \times)$. Now we will consider questions whether $\mathrm{FM}(\mathcal{N})$ is definable in $\mathrm{FM}(\mathcal{A})$, where $\mathcal{A}$ is a given structure. A natural way of proving that the answer for such a question is positive is an adaptation of a proof of the analogous results for infinite structure. However such adaptation usually is not easy because in finite structure we have a strict limitation for size of numbers which can be used. The situation is much easier if a needed definition is done by a Δ_0 formula, where quantifiers are bounded.

It is known that the relation BIT is definable in $\mathrm{FM}(\mathcal{N})$ and conversly, addition and multiplication are definable in $(\mathbb{N}, \mathrm{BIT})$. Formulas giving needed definitions are rather complicated and can not be used in the case of finite structures. However in the paper [BIS90] it is proved that $\mathrm{FM}(\mathcal{N})$ is definable in $\mathrm{FM}((\mathbb{N}, \mathrm{BIT}, \leq))$. In [DDLW98] it is proved that the standard ordering relation is definable in $\mathrm{FM}(\mathsf{HF})$, i.e. $\mathrm{FM}((\mathbb{N}, \leq))$ is definable in $\mathrm{FM}(\mathsf{HF})$. Using this definability it is also proved that addition and multiplication is definable in $\mathrm{FM}(\mathsf{HF})$. Thus we have

Theorem 5.2 ([DDLW98]) $\mathrm{FM}(\mathcal{N})$ *and* $\mathrm{FM}(\mathsf{HF})$ *are mutually definable.*

Quine in [Qui46] proved that in the structure FW it can be defined addition and multiplication. Later Bennett in [Ben62] observed that using ordering these definition can be written by Δ_0-formulas. Unfortunately this idea cannot be repeated in the finite models context because value of used here terms can exceed the maximal element of

a finite model. This concerns terms in the language of FW which occurs in bounded quantification.

Zdanowski, in [Zda05] shown that in FM(FW) one can define FM($\mathcal{N}$), even though we have no standard ordering relation in the language of FM(FW). In the first part of the proof in [Zda05] it is shown that the ordering relation is definable in FM(FW). Then, using this relation, it is quite straightforward, although tedious, to define addition and multiplication.

Theorem 5.3 ([Zda05], see also [KZ05]) FM($\mathcal{N}$) *and* FM(FW) *are mutually definable.*

Using the well known equivalence: $x + y = x \Leftrightarrow (xz + 1)(yz + 1) = z^2(xy + 1) + 1$ we can define addition using multiplication and successor function. However, this equivalence cannot be directly applied to define addition over finite structures. When $x, y < \frac{n}{2}$ then $x + y < n$. But if additionaly $\sqrt[4]{n} < x, y$ and $z = x + y$ then $(xz + 1)(yz + 1) > n$. So, the above equivalence does not hold in finite structure. However using a different method Troy Lee proved that addition can be defined over finite structures with multiplication and ordering. Moreover, he has show that the presence of ordering and coprimality is sufficient. So, we have the following.

Theorem 5.4 ([Lee03]) *The following FM-domains are mutually definable with* FM($\mathcal{N}$)*:* FM($(\mathbb{N}, \times, \leq)$), FM($(\mathbb{N}, |, \leq)$), FM($(\mathbb{N}, \perp, \leq)$).

We ilustrate a kind of arguments used in a proof of this theorem by showing how to define multiplication using addition and coprimality relation. At the first we observe that the followng formula

$$x \neq 0 \wedge x \neq 1 \wedge \forall y(0 < y < x \rightarrow y \perp x)$$

defines primality property "x is a prime number" (note that inequality is defined using addition). Now, we define multiplication over primes p_1 and p_2, as the smallest nonzero number not coprime to both p_1 and p_2. Finally, to define a multiplication over all natural numbers we use the number theoretical results claiming that every natural number greater than 1 is a sum of not more than 7 primes.

Let $\leq_P$ denotes usual inequality relation restricted to the set of all prime numbers. Using the method of Ehrenfeucht-Fraïssé games Zdanowski proved the following.

Theorem 5.5 ([Zda05]) FM($\mathcal{N}$) *is not definable in* FM($(\mathbb{N}, \times, \leq_P)$)*, in fact even* FM($(\mathbb{N}, \leq$ $))$ *is not definable in* FM($(\mathbb{N}, \times, \leq_P)$).

So, this result suggest that we cannot expect strong, or even any, strengthening of results of Troy Lee.

Using the exponentiation function x^y we can easily define in infinite structure addition and multiplication. For example we have $xy = z \Leftrightarrow \forall t((t^x)^y = t^z)$. But in finite structures

such equivalence does not hold. If n is the size of our finite model and $x, y < n$ are sufficiently big then it can happen that xy is in the model (i.e. $xy < n$) and $(2^x)^y$ is not in the model (i.e. $(2^x)^y \geq n$). Then the result of multiplication of x by y cannot be defined by the above formula. Moreover, surprisingly we have the following.

Theorem 5.6 ([KZ05]) $\mathrm{FM}((\mathbb{N}, \exp))$ *is definable in* $\mathrm{FM}((\mathbb{N}, \times))$*, and not vice versa.*

5.2 Interpretability

Another method which allows to compare theories is the method of interpretation. This method was applied in several model-theoretical achievements.

The interpretation notion is a generalization of the definability notion.

Definition 5.7 *Let $\mathcal{A}$ be a model, let $\sigma = \{P_1, \ldots, P_m\}$ be a relational vocabulary and let $\bar{\varphi} = (\varphi_U, \varphi_1, \ldots, \varphi_m)$ be the sequence of formulae.*

We say that $\mathrm{FM}(\mathcal{B})$ *is interpretable on initial segments (shortly IS-interpretable) in* $\mathrm{FM}(\mathcal{A})$ *if there is a sequence of formulae $\bar{\varphi}$ and unbounded and nondecreasing function $f : \mathbb{N} \longrightarrow \mathbb{N}$ such that for each $n > 0$, $\mathcal{B}_{f(n)} = I_{\bar{\varphi}}(\mathcal{A}_n)$.*

In an obvious way we can extend this definition to the case of nonrelational signature σ.

So, $\mathrm{FM}(\mathcal{B})$ is IS-interpretable in $\mathrm{FM}(\mathcal{A})$ if on initial segments of the structures of $\mathrm{FM}(\mathcal{A})$ the structures from $\mathrm{FM}(\mathcal{B})$ can be defined. The important thing is that the interpretability preserves FM-repesentability as well as undecidability of FM-theories. We have the following:

Theorem 5.8 ([MW04]) $\mathrm{FM}(\mathcal{N})$ *is* IS*–interpretable in* $\mathrm{FM}((\mathbb{N}, |))$.

The crucial point in the proof of the above theorem is the observation that using divisibility relation it can be defined the ordering restricted to some initial segment. Namely, let us consider the following formula $\varphi_<(x, y)$:

$$\exists z(z \perp x \wedge z \perp y \wedge \exists w(x \mid w \wedge z \mid w) \wedge \neg \exists w(y \mid w \wedge z \mid w)).$$

It can be proved that for arbitrary natural numbers a, b such that $(ab)^2 < n$ we have: $(\mathbb{N}, |) \models \varphi_<[a, b]$ if and only if $a < b$. So,the formula $\varphi_<$ defines the usual ordering in $(\mathbb{N}, |)_n$ on the initial segment of lenght $\sqrt[4]{n}$. This allows to define on such initial segment addition and multiplication what gives us needed IS-interpretability.

Obviously, in infinite as well as in finite structures the coprimality relation is definable by divisibility relation. Moreover, the divisibility relation can not be defined by coprimality relation. To see this it is enough to observe that using coprimality relation it is not possible to distinguish between different powers of the same prime number. However, using a more general notion of interpretation (for definition see [Szcz77] or [Hod93]) it can be proved the following.

Theorem 5.9 ([MZ05]) $\mathrm{FM}(\mathcal{N})$ *is interpretable in* $\mathrm{FM}((\mathbb{N}, \perp))$.

Roughly speaking the proof of the theorem goes by construction within $\mathrm{FM}((\mathbb{N}, \perp))$ an interpretation of addition and multiplication on indices of prime numbers.

6 Decidability of finite arithmetics

It is well known that the theory of addition as well as theory of multiplication (i.e $\mathrm{Th}((\mathbb{N},+))$ and $\mathrm{Th}((\mathbb{N},\times))$ is decidable. So, a natural question arise: what about a decidability of sl-theories of such structures? It is not to difficult to observe that some decidability results for infinite arithmetics implies the same results for finite arithmetic. It is enough to observe that using ordering relation we can define a translation of a formulas from the language of finite structures to formulas of the language of infinite structures in such a way that if a sentence $\bar{\varphi}$ is a translation of the sentence φ then $\bar{\varphi}$ is true in sufficiently large finite models if and only if φ is true in infinite model. Moreover, if the ordering relation is Δ_0-definable in infinite structure then the sentence $\bar{\varphi}$ is always Σ_2 sentence. Thus we have:

Proposition 6.1 *If Σ_2^0 theory of the structure $(\mathcal{A},<)$ is decidable then $sl(FM(\mathcal{A}))$ is decidable.*

From that results we obtain that the following theories are decidable: $\mathrm{sl}((\mathbb{N},\leq))$, $\mathrm{sl}((\mathbb{N},+))$, $\mathrm{sl}((\mathbb{N},+,k^x))$ for arbitrary fixed k.

We can not apply the last proposition to the theory of multiplication because the theory of the structure $(\mathbb{N},\times,<)$ is undecidable. Indeed, as it is proved in [KZ05] $\mathrm{FM}(\mathcal{N})$ is IS-interpretable in $(\mathbb{N},\times)$ what implies undecidability of the theory $\mathrm{sl}((\mathbb{N},\times))$. However, we have the following decidability result

Theorem 6.1 ([KZ05]) *The existential theory of* $\mathrm{sl}(\mathrm{FM}((\mathbb{N},\times,\leq)))$ *is decidable.*

Actually, the result on undecidability of the sl-theory of multiplication also follows from the mentioned above results contained in theorems 5.8 and 5.9. These give also the following conclusion

Theorem 6.2 (see [MZ05], [MW04],[Zda05], Trachtenbrot theorem) *The set of sentences true in all structures from* $\mathrm{FM}(\mathcal{A})$ *is Π_1^0-complete and therefore undecidable, for $\mathcal{A}$ being one of the following arithmetics:* $(\mathbb{N},+,\times)$, $(\mathbb{N},\times)$, $(\mathbb{N},|)$, $(\mathbb{N},\perp)$.

Theorem 6.3 (see [KZ05], [MZ05], [MW04],[Zda05],) *The theory* $\mathrm{sl}(\mathrm{FM}(\mathcal{A}))$ *is Σ_2^0–complete and therefore undecidable for $\mathcal{A}$ being one of the following arithmetics:* $(\mathbb{N},+,\times,\leq,0,1)$, $(\mathbb{N},\times)$, $(\mathbb{N},|)$, $(\mathbb{N},\perp)$.

7 FM–representability in poor arithmetics

In this section we consider the question for a given arithmetic $\mathcal{A}$, what is the family of relations which is FM–representable in $\mathrm{FM}(\mathcal{A})$. We saw that if $\mathcal{A}$ is a model with recursive relations then this family is contained in Δ_2^0–relations (see theorem 4.6.) On the other hand this upper bound is reached in the case of the arithmetic of addition and multiplication (see theorem 4.5). Now, we will consider some weaker arithmetics.

Firstly, we show how to compare the families of FM–representable relations in $\mathrm{FM}(\mathcal{A})$ and $\mathrm{FM}(\mathcal{B})$ if one family is interpretable in the other one.

Theorem 7.1 *Let* FM($\mathcal{A}$) *be* IS*–interpretable in* FM($\mathcal{B}$)*. Then, for each* $R \subseteq \mathbb{N}^r$*, if* R *is* FM*–representable in* FM($\mathcal{A}$) *then it is* FM*–representable in* FM($\mathcal{B}$)*.*

The proof of this theorem is based on a simple translation of a formula which FM–represents a given $R \subseteq \mathbb{N}^r$ in FM($\mathcal{A}$) into a formula which FM–represents R in FM($\mathcal{B}$). The translations just substitute the basic relations from FM($\mathcal{A}$) with their definitions in FM($\mathcal{B}$) given by an IS–interpretation.

From the above theorem together with FM–representability theorem for FM($\mathcal{N}$) (see theorem 4.5) and theorem 4.6 one can infer the following

Theorem 7.2 *If* $\mathcal{A}$ *is an arithmetic with decidable relations and such that* FM($\mathcal{N}$) *is* IS*–intepretable in* FM($\mathcal{A}$) *then the family of relations which are* FM*–representable in* FM($\mathcal{A}$) *is exactly the family of* Δ_2^0*–relations.*

In particular, $\mathcal{A}$ *can be one of the following arithmetics:* $(\mathbb{N}, \perp, \leq)$*,* $(\mathbb{N}, \times)$*,* $(\mathbb{N}, |)$*,* $(\mathbb{N}, \exp)$*.*

It follows that even relatively weak arithmetics of finite models FM–reprezent all that can be represented. Now, we characterize FM–representability in some arithmetics which are essentially weaker with respect to the class of FM–representable relations.

Firstly, we recall an observation from [KZ05].

Theorem 7.3 *Relations which are* FM*–representable in* FM($(\mathbb{N}, +)$) *are just the relations definable in* $(\mathbb{N}, +)$*.*

Now, we present an example of arithmetic which can FM–represent relations which are of arbitrary complexity below Δ_2^0 but which cannot represent all relations from this class.

Definition 7.4 *Let* $\sim$ *be an equivalence relation on* $\mathbb{N}$ *and let* $R \subseteq \mathbb{N}^r$*. We say that* $\sim$ *is a congruence relation for* R *if for all* $a_1, \ldots, a_r, b_1, \ldots, b_r \in \mathbb{N}$ *such that* $a_i \sim b_i$ *for,* $i = 1, \ldots, r$*,*

$$(a_1, \ldots, a_r) \in R \iff (b_1, \ldots, b_r) \in R.$$

Definition 7.5 *For* $a, b \in \mathbb{N}$*, we define* $a \approx b$ *if* a *and* b *have the same prime divisors. A relation* $R \subseteq \mathbb{N}^r$ *is coprimality invariant if* $\approx$ *is a congruence for* R*.*

The following characterization is from [MZ05].

Theorem 7.6 ([MZ05]) R *is* FM*–representable in* FM($(\mathbb{N}, \perp)$) *if and only if* R *is* FM*–representable in* FM($\mathcal{N}$) *and* R *is coprimality invariant.*

The methods used in [MZ05] can be generalized to characterize FM–representability for a bigger class of arithmetics.

Definition 7.7 *Let* $n \in \mathbb{N} - \{0\}$ *or* $n = \infty$*. We define the following relations on natural numbers:*

- *$x|_n y$ if and only if for each power of a prime q with an exponent not greater than n, if q divides x then q divides y.*
- *$x \approx_n y$ if and only if $x|_n y$ and $y|_n x$.*

The relation $|_\infty$ is just divisibility $|$ and $\approx_\infty$ is the identity. The relation $|_1$ is mutualy definable with coprimality.

The following theorem generalizes the above results on FM–representability in $\mathrm{FM}((\mathbb{N}, |))$ and in $\mathrm{FM}((\mathbb{N}, \perp))$.

Theorem 7.1 ([Mos07]) *For any $n > 0$ or $n = \infty$, a relation $R \subseteq \mathbb{N}^r$ is FM–representable in $\mathrm{FM}((\mathbb{N}, |_n))$ if and only if R is Δ_2^0–definable and the relation $\approx_n$ is a congruence for R.*

8 Spectra of finite arithmetics

Another way of comparing various arithmetics (and, in fact, even various logics) of finite models is to consider their spectra.

Definition 8.1 *Let $\mathcal{K}$ be a class of finite models in a vocabulary σ and let φ be sentence of the same vocabulary. The spectrum of φ in $\mathcal{K}$, $Spec(\varphi, \mathcal{K})$, is the set of cardinalities of models from $\mathcal{K}$ in which φ is true,*

$$Spec(\varphi, \mathcal{K}) = \{card(M) : M \in \mathcal{K} \wedge M \models \varphi\}.$$

The spectrum of a logic L in $\mathcal{K}$, $Spec_{\mathcal{K}}(L)$, is the set of spectra for all formulae of L, that is

$$Spec(L, \mathcal{K}) = \{Spec(\varphi, \mathcal{K}) : \varphi \text{ is a sentence of } L\}.$$

We skip L in $Spec(L, \mathcal{K})$ if L is just first order logic.

Sometime, we say the spectrum of arithmetic $\mathrm{FM}(\mathcal{A})$ for denoting the spectrum of the first order logic in $Spec(\mathrm{FM}(\mathcal{A}))$.

The importance of this notion in finite models comes, among other things, from its close relations with computational complexity. E.g. if Fin is a class of all finite models than the spectrum of first order logic is just the family of sets recognizable in nondeterministic time $2^{O(n)}$. Thus, the question whether Spec(Fin) is closed on the complement (known as Asser problem) is equivalent to the question whether NETIME = coNETIME.[8]

The situation we are interested in is when $\mathcal{K}$ is of the form $\mathrm{FM}(\mathcal{A})$, for $\mathcal{A}$ being a standard model for some arithmetic. In this case the following theorem is a classical one.

[8] NETIME is the class of problems which can be solved on nondeterministic Turing machines in time $2^{O(n)}$ and coNETIME is the class of problems whose complements are in NETIME.

Theorem 8.2 *Spec*(FM($\mathcal{N}$)) *is exactly the class of sets recognizable in linear time hierarchy.*

Of course from the definability results stated above it follows that arithmetics FM(HF) and FM(FW^t), for $t \geq 2$, have the same spectrum as FM($\mathcal{N}$). On the other hand there are examples of arithmetics which have quite easy spectra.

Theorem 8.3 *Let* $\mathcal{A} = (\mathbb{N}, \leq)$. Spec(FM($\mathcal{A}$)) *is the family of finite and cofinite sets.*

Proof. We only sketch the proof. Assume, for the sake of contradiction, that there is a sentence φ such that the sets Spec(φ, FM($\mathcal{A}$)) and Spec($\neg\varphi$, FM($\mathcal{A}$)) are infinite. Then, there are models $\mathcal{B}$ and $\mathcal{C}$ of the theory sl(FM($\mathcal{A}$)) such that $\mathcal{B} \models \varphi$ and $\mathcal{C} \models \neg\varphi$. But each model for sl(FM($\mathcal{A}$)) is an infinite linear discrete ordering with endpoints. It is well known that such theory is complete. Thus, it is impossible that $\mathcal{B} \models \varphi$ and $\mathcal{C} \models \neg\varphi$. □

The spectrum of finite arithmetic of addition only also poses a nice characterization.

Theorem 8.4 ([Sch01]) *Let* $\mathcal{A} = (\mathbb{N}, +)$. *Spec*(*MSO*, FM($\mathcal{A}$)) *are just semilinear sets (i.e. the sets definable in* $\mathcal{A}$*).*

Finally, we characterize the spectrum for full arithmetic of addition and multiplication.

Theorem 8.5 Spec(FM($\mathcal{N}$)) *are just sets in the linear time hierarchy.*

From the computational point of view the family Spec(FM($(\mathbb{N}, +)$) is easily recognizable. On the other hand the sets in Spec(FM($\mathcal{N}$)) are likely to be not recognizable in PTIME. If we consider the spectrum of FM($(\mathbb{N}, \times)$) then it was shown in [KZ05] that it is strictly included in Spec(FM($\mathcal{N}$)). Nevertheless, there is a close relation between the spectrum of FM($\mathcal{N}$) and the spectrum of FM($(\mathbb{N}, \times)$). The form of IS–interpretation of FM($\mathcal{N}$) in FM($(\mathbb{N}, \times)$) gives the following proposition.

Proposition 8.1 ([KZ05]) *Let* X *belong to the spectrum of arithmetic with addition and multiplication. Then the set*

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

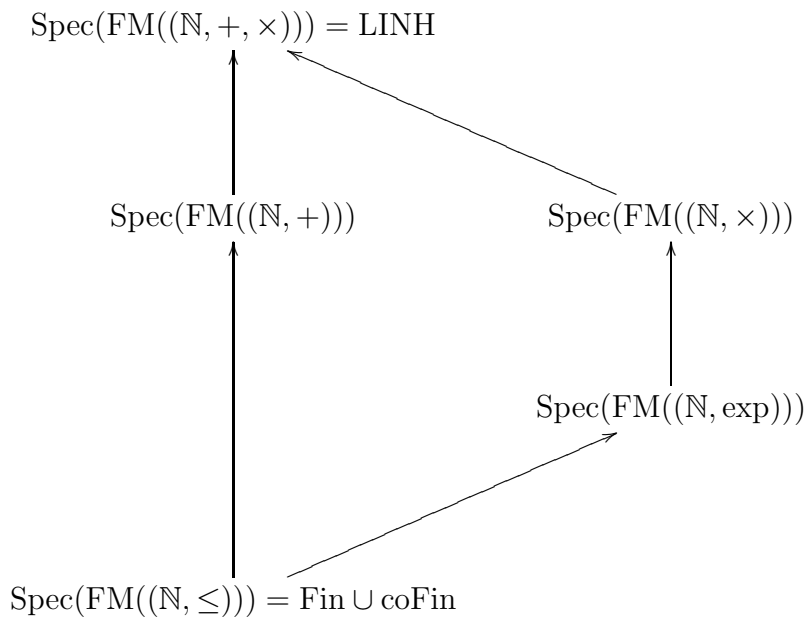
belongs to the spectrum of arithmetic with multiplication.

It follows that the spectra of FM($(\mathbb{N}, \times)$) are as hard as the spectra of FM($\mathcal{N}$) from the complexity point of view.

Both addition only and multiplication only have nontrivial spectra. The result by Kołodziejczyk which shows that the artimetics of addition only and of multiplication only are in a sense orthogonal with respect to spectra they define.

Theorem 8.6 (Kołodziejczyk, see [KZ05]) *If* X *is in the spectrum of* FM($(\mathbb{N}, \times)$) *and* FM($(\mathbb{N}, +)$) *then* X *is finite or cofinite.*

We end with the diagram which shows the inclusions between spectra of various arithmetic. 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.

9 Problems and questions

Finite arithmetic in general setting is relatively new research area. We attempted to give a general state of knowledge of this area. Nevertheless we have an impression that many interesting and important problems were not undertaken neither by us or by others. Therefore our list of open problems cannot be treated as a systematic presentation of the main open problems in the area.

1. What is definable in $\mathrm{FM}((\mathbb{N}, \perp, \leq_\Pi))$, where Π is the set of prime powers and $\leq_X$ is the ordering relation restricted to the set X. Let us note that in $(\mathbb{N}, \perp, \leq_\Pi)$ there are definable addition and multiplication (see [BR98]). However, definitions developed in [BR98] use essentially numbers which are of exponential size.

   If $\mathrm{FM}(\mathcal{N})$ is not definable in $\mathrm{FM}((\mathbb{N}, \perp, \leq_\Pi))$ it would be a natural example of an arithmetic which does not define $+$ and $\times$ in finite models although it does in the standard model.

2. Consider the spectrum problem for functions treated as relations. In this situation many results from subsection 8 do not hold.

3. Extend theorem 5.6 on the other classes of functions with various rates of growing, e.g. functions from the Grzegorczyk hierarchy.

4. What about (un)decidability of $\mathrm{FM}((\mathbb{N}, \leq, P))$, where P is the set of primes. In the standard model it is a long standing open problem. If $\mathrm{Th}((\mathbb{N}, \leq, P))$ is decidable it may be easier to prove it first for $\mathrm{Th}(\mathrm{FM}((\mathbb{N}, \leq, P))$. On the other hand, one can express e.g. twin prime conjecture by asking whether a certain sentence is in $\mathrm{sl}(\mathrm{FM}((\mathbb{N}, \leq, P)))$.

5. We concentrated in this survey on finite arithmetics with first order logic as underlying logic. It would be interesting to examine properties of various finite arithmetics in the framework of stronger logics like second order logic, logic with counting quantifiers etc. An analysis of fixed point logic over finite arithmetic of hereditarily finite sets is given in [AK99].

References

[AK99] A. Atserias and Ph. Kolaitis. First order logic vs. fixed point logic on finite set theory. In *14th IEEE Symposium on Logic in Computer Science (LICS)*, volume 14, pages 275–284, 1999.

[Ben62] J. H. Bennett. *On Spectra*. PhD thesis, Princeton University, 1962.

[Bes02] A. Bes. A survey of arithmetical definability. In A tribute to Maurice Boffa, Special Issue of Belg. Math. Soc., pages 1–54, 2002.

[BIS90] D. A. Mix Barrington, N. Immerman, and H. Straubing. On uniformity within NC^1. *Journal of Computer and System Science*, 41:274–306, 1990.

[BR98] W. Bés and D. Richard. Undecidable extensions of Skolem arithmetic. *Journal of Symbolic Logic*, 63(2):379–401, 1998.

[BS71] J. L. Bell and A. B. Slomson. *Models and ultraproducts*. North Holland, 1971.

[DDLW98] A. Dawar, K. Doets, S. Lindell, and S. Weinstein. Elementary properties of the finite ranks. *Mathematical Logic Quarterly*, 44:349–353, 1998.

[Fag74] R. Fagin. Generalized first order spectra and polynomial–time recognizable sets. In *SIAM – AMS Proceedings*, volume 7, pages 43–73, 1974.

[Göd31] K. Gödel. Über formal unentscheidbare Sätze der "Principia Mathematica" und verwandter Systeme. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.

[Gol65] E. M. Gold. Limiting recursion. *The Journal of Symbolic Logic*, 30:28–48, 1965.

[Gol67] E. M. Gold. Language identification in the limit. *Information and Control*, 10:447–474, 1967.

[Hoa69] C. A. R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12:576–583, 1969.

[Hod93] W. Hodges. *Model theory*. Encyclopedia of mathematics and its applications. Cambridge University Press, 1993.

[Koł04a] L. Kołodziejczyk. A finite model-theoretical proof of a property of bounded query classes within ph. *The Journal of Symbolic Logic*, 69:1105–1116, 2004.

[Koł04b] L. Kołodziejczyk. Truth definitions in finite models. *The Journal of Symbolic Logic*, 69:183–200, 2004.

[Koł05] L. A. Kołodziejczyk. *Truth definitions and higher order logics in finite models*. PhD thesis, Warsaw University, 2005.

[KTZ] M. Krynicki, J. Tomasik, and K. Zdanowski. Theory of initial segments of standard models of arithmetics and their complete extensions. in manuscript.

[KZ05] M. Krynicki and K. Zdanowski. Theories of arithmetics in finite models. *Journal of Symbolic Logic*, 70(1):1–28, 2005.

[Lee03] T. Lee. Arithmetical definability over finite structures. *Mathematical Logic Quarterly*, 49:385–393, 2003.

[Mos93] M. Mostowski. Truth–definitions in finite models. in manuscript, 1993.

[Mos01] M. Mostowski. On representing concepts in finite models. *Mathematical Logic Quarterly*, 47:513–523, 2001.

[Mos03] M. Mostowski. On representing semantics in finite models. In A. Rojszczak†, J. Cachro, and G. Kurczewski, editors, *Philosophical Dimensions of Logic and Science*, pages 15–28. Kluwer Academic Publishers, 2003.

[Mos07] M Mostowski. private communication, 2007.

[MW04] M. Mostowski and A. Wasilewska. Arithmetic of divisibility in finite models. *Mathematical Logic Quarterly*, 50(2):169–174, 2004.

[Myc81] J. Mycielski. Analysis without actual infinity. *Journal of Symbolic Logic*, 46:625–633, 1981.

[MZ05] M. Mostowski and K. Zdanowski. Coprimality in finite models. In Luke Ong, editor, *Computer Science Logic: 19th International Workshop, CSL 2005*, volume 3634 of *Lecture Notes in Computer Science*, pages 263–275. Springer, 2005.

[PD82] J. Paris and C. Dimitracopoulos. Truth definitions for Δ_0 formulae. In Logic and algorithmic, L'enseignement Mathematique No 30, Geneve, 1982.

[Qui46] W. Quine. Concatenation as a basis for arithmetic. *Journal of Symbolic Logic*, 11:105–114, 1946.

[Sch01] N. Schweikardt. *On the Expressive Power of First-Order Logic with Built-In Predicates*. PhD thesis, Johannes Gutenberg-Universität Mainz, 2001.

[Sho93] J. R. Shoenfield. *Recursion Theory*. Lectures Notes in Logic. Springer–Verlag, 1993.

[Szcz77] L. W. Szczerba. Interpretability of elementary theories. In Butts and Hintikka, editors, *Proceedings 15th ICALP 88*, Logic, foundations of mathematics and computability theory, pages 129–145. Reidel Publishing, 1977.

[Tar33] A. Tarski. *Pojęcie prawdy w językach nauk dedukcyjnych*. Nakładem Towarzystwa Naukowego Warszawskiego, 1933. English version in [**?**].

[Wra78] C. Wrathall. Rudimentary predicates and relative computation. *SIAM Journal on Computing*, 7:194–209, 1978.

[Zda05] K. Zdanowski. *Arithmetics in finite but potentially ifinite worlds*. PhD thesis, Warsaw University, 2005.