An outline of the dissertation ,,Arithmetics in finite but potentially infinite worlds"

Konrad Zdanowski

31st July 2006

> *Our account does not rob the mathematicians of their science, by disproving the actual existence of the infinite in the direction of increase [...]. In point of fact they do not need the infinite and do not use it. They postulate only that the finite straight line may be produced as far as they wish.*
>
> Aristotle "Physics", Book 3, part 7.
> Translated by R. P. Hardie and R. K. Gaye.

In the dissertation we examine logical properties of finite arithmetics. Finite models with built-in arithmetical relations have gained an attention due to their ability to express concepts related to computational complexity. It was shown, for example, that the logic with the fixed point operator expresses on models with linear order exactly those properties which are computable in deterministic polynomial time. Similarly, the transitive closure operator corresponds on finite models with order to nondeterministic logarithmic space and just the first order logic, on finite models with addition and multiplication, describes the properties recognized by families of polynomial size, constant depth Boolean circuits constructed in logarithmic space (uniform AC^0). In the above results we need to enriched finite models with some arithmetical relations. And the weaker logic we consider, the stronger set of arithmetical relations we need. In our work we look into logical properties of such finite models arithmetics. As we will see they may be very different from that of the infinite model.

Now, we present the basic notion of our work, the family of finite models of a given arithmetic.

Definition 1 *Let* $\mathcal{A} = (\omega, \{R_i\}_{i\leq s}, \{F_i\}_{i\leq t}, \{a_i\}_{i\leq r})$ *and let* $A_n = \{0, \ldots, n\}$. *By* $FM(\mathcal{A})$ *we define the family* $\{\mathcal{A}_i\}_{i\in\omega}$ *of the finite models of the form*

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

where

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

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

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

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

Very often we identify an arithemtic with the set of its relations and operations. So, we will talk e.g. about finite arithmetic of addition and multiplication refering to the family $\mathrm{FM}((\omega, +, \times))$.

We use the following symbols $\leq, +, \times, \log_t, \exp$ for denoting the ordering, addition, multiplication, logarithm with the base t and two argument exponentiation operation, respectively. We write $\lceil x \rceil$ for the least integer not less than x.

We use also the well known arithmetical hierarchy of relations. So, we talk about Σ_n^0 (Π_n^0) relations which are relations definable in $(\omega, +, \times, 0, 1)$ by Σ_n^0 (Π_n^0) formulas.

In our work we consider the following questions.

1. Which infinite relations can be represented in finite models and how?
2. What are definability and interpretability dependencies between finite arithmetics?
3. What is the recursive complexity of various theories of finite arithmetics?

The first one of these questions is specific for our area of investigations that is for finite models. Questions 2 and 3 were often considered in the context of classical arithmetics of the infinite models. Thus, we may say that they are classical problems but put in a new context.

According to the first question the problem was raised initially by Marcin Mostowski in [Mos01] and [Mos03]. In the first of these papers M. Mostowski considered the question how one can represent infinite relations in finite models. He proposed there the following definitions.

Definition 2 *A formula* $\varphi(x_1, \ldots, x_n)$ *is satisfied by* $a_1, \ldots, a_n$ *in all sufficiently large finite models from* $\mathrm{FM}(\mathcal{A})$, *(or in almost all finite models from* $\mathrm{FM}(\mathcal{A})$*),* $\mathrm{FM}(\mathcal{A}) \models_{\mathrm{sl}} \varphi[a_1, \ldots, a_n]$, *if*

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

By $\mathrm{sl}(\mathrm{FM}(\mathcal{A}))$ *we denote the family of sentences true in almost all finite models from* $\mathrm{FM}(\mathcal{A})$*,*

$$\mathrm{sl}(\mathrm{FM}(\mathcal{A})) = \{\varphi : \mathrm{FM}(\mathcal{A}) \models_{\mathrm{sl}} \varphi\}\,.$$

Definition 3 *A formula* $\varphi(x_1, \ldots, x_r)$ FM*–represents in* $\mathrm{FM}(\mathcal{A})$ *a relation* $R \subseteq \omega^r$ *if for all* $a_1, \ldots, a_r \in \omega$

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

and

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

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

One may say that relations which are FM–representable in $\mathrm{FM}(\mathcal{A})$ are those, for which we have a good description in almost all finite models from $\mathrm{FM}(\mathcal{A})$. M. Mostowski proved the following characterization.

Theorem 4 ([Mos01]) *Let* $R \subseteq \omega^r$*.* R *is* FM*–representable in* $\mathrm{FM}(\mathcal{N})$ *if and only if* R *is* Δ_2 *in the arithmetical hierarchy (or, in the other words,* R *is recursive with some recursively enumerable oracle).*

Moreover, M. Mostowski proved the following result using his finite model version of the theorem on undefinability of truth.

Theorem 5 ([Mos01]) $\mathrm{sl}(\mathrm{FM}(\mathcal{N}))$ *is not* Δ_2^0*–definable.*

In our work we present the following methods of representing concepts in finite models.

Definition 6 *Let* $R \subseteq \omega^r$*.* R *is weakly* FM*–representable in* $\mathrm{FM}(\mathcal{A})$ *if there exists a formula* $\varphi(x_1, \ldots, x_r)$ *such that for all* $a_1, \ldots, a_r \in \omega$*,*

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

Definition 7 *Let* $\varphi(x_1, \ldots, x_r)$ *be a formula in the vocabulary of* $\mathrm{FM}(\mathcal{A})$ *and let* $a_1, \ldots, a_r \in \omega$*. By the* n*-th density of* $\varphi[a_1, \ldots, a_r]$ *in* $\mathrm{FM}(\mathcal{A})$*,* $\mu_n(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A}))$*, we mean*

$$\mu_n(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A})) = \frac{card\{i : i < n \wedge \mathcal{A}_i \models \varphi[a_1, \ldots, a_r]\}}{n},$$

By $\mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A}))$ *we denote, if it exists,*

$$\mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A})) = \lim_{n\to\infty} \mu_n(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A})).$$

When it does not lead to any misunderstandings we omit the second parameter in $\mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A}))$*.*

Definition 8 *A relation $R \subseteq \omega^r$ is statistically representable in* $\mathrm{FM}(\mathcal{A})$ *if there is a formula $\varphi(x_1, \ldots, x_r)$ with all free variables among $x_1, \ldots, x_r$ such that for all $a_1, \ldots, a_r \in \omega$,*

- *there exists $\mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A}))$,*
- $(a_1, \ldots, a_r) \in R \iff \mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A})) = 1$,
- $(a_1, \ldots, a_r) \notin R \iff \mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A})) = 0$.

We say that the set $R \subseteq \omega^r$ is weakly statistically representable in $\mathrm{FM}(\mathcal{A})$ *if there is a formula $\varphi(x_1, \ldots, x_r)$ with all free variables among $x_1, \ldots, x_r$ such that for all $a_1, \ldots, a_r \in \omega$,*

- *if $(a_1, \ldots, a_r) \in R$ then $\mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A}))$ exists,*
- $(a_1, \ldots, a_r) \in R \iff \mu(\varphi[a_1, \ldots, a_r], \mathrm{FM}(\mathcal{A})) = 1$.

For both of the above methods we present complete characterizations of the family of represented relations for finite arithmetic of addition and multiplication (the first characterization is a join result with M. Mostowski).

Theorem 9 ([MZ05b]) *Let $R \subseteq \omega^r$.*

1. *R is weakly* FM*–representable in* $\mathrm{FM}(\mathcal{N})$ *if and only if R is Σ^0_2 definable.*
2. *R statistically representable in* $\mathrm{FM}(\mathcal{N})$ *if and only if R is Δ^0_2 definable.*
3. *R is weakly statistically representable in* $\mathrm{FM}(\mathcal{N})$ *if and only if R is Π^0_3 definable.*

The condition for statistical representability is weaker than that for FM–representability. Nethertheless, as we see from the second point of the above theorem, both concepts are equivalent in $\mathrm{FM}(\mathcal{N})$.

The method of proving the above theorems allows also to estimate the complexity of some, semantically defined, theories of $\mathrm{FM}(\mathcal{N})$.

Theorem 10 ([MZ05b]) 1. *The set* $\mathrm{sl}(\mathrm{FM}(\mathcal{N}))$ *is Σ^0_2–complete.*

2. *The set $\{\varphi : \mu(\varphi, \mathrm{FM}(\mathcal{N})) = 1\}$ is Π^0_3–complete.*

It follows from point 1 of the above theorem that $\mathrm{sl}(\mathrm{FM}(\mathcal{N}))$ is not a complete theory. We show in our work, using an ultraproduct constructions, that there are continuum many complete consistent extensions of $\mathrm{sl}(\mathrm{FM}(\mathcal{N}))$.

Now, we will focus on the second of the presented questions about definability and interepratability dependecies between various finite arithmetics. The answers which we obtain will allow us to estimate the complexity of some subarithmetics of addition and multiplication.

There are three well known classical arithmetics: the arithmetic of addition and multiplication, the arithmetic of hereditarily finite sets with "in" relation and the arithmetic of finite words over a finite alphabet with concatenation operation. All of them we can treat as arithmetics with the universe ω consisting of the natural numbers. So, we can identify hereditarily finite sets, usually denoted by $(V_\omega, \in)$, with the model (ω, BIT), where $\mathrm{BIT}(x, y)$ holds when the x-th bit in the binary representation of y is one. Similarly, for an alphabet $\Gamma_t = \{a_1, \ldots, a_t\}$, the infinite model for finite words over Γ_t with concatenation operation can be identified with the model $(\omega, *_t, 1, \ldots, t)$, where i is the one letter word a_i and $*_t$ is defined as $x *_t y = xt^{\lceil \log_t(y+1) \rceil} + y$. We have the following theorem.

Theorem 11 *Let $t \geq 2$. Each of the following models is definable in any other:*

(i) $(\omega, +, \times, 0, 1)$,

(ii) (ω, BIT),

(iii) $(\omega, *_t, 1, \ldots, t)$.

Definability between $(\omega, +, \times, 0, 1)$ and $(\omega, *_t, 1, \ldots, t)$ was given by Quine. Definability between $(\omega, +, \times, 0, 1)$ and (ω, BIT) is considered as a part of logical folklore.

It turned out that the mutual definability between these arithmetics transfers also to finite models. Barrington et al. in [BIS90] showed the following theorem.

Theorem 12 ([BIS90]) $\mathrm{FM}((\omega, +, \times, 0, 1))$ *and* $\mathrm{FM}((\omega, \mathrm{BIT}))$ *are mutually definable one in the other.*

In our thesis we show that concatenation in finite models is as strong as the above two arithmetics.

Theorem 13 *Let $t \geq 2$.* $\mathrm{FM}((\omega, *_t, 1, \ldots, t))$ *and* $\mathrm{FM}((\omega, +, \times, 0, 1))$ *are mutually definable one in the other.*

We examine also some subarithmetics of addition and multiplication. In order to compare their strength we introduce the following notion.

Definition 14 *A sequence of formulas $\bar{\varphi}$ is an order preserving* sl*–interpretation of* $\mathrm{FM}(\mathcal{A})$ *in* $\mathrm{FM}(\mathcal{B})$ *if there exists a function $f\colon \omega \longrightarrow \omega$ such that*

- *the range of f is cofinite,*
- *for each $i \in \omega$, $f^{-1}(\{i\})$ is finite,*

- *for each $n \in \omega$, $\bar{\varphi}$ defines a model $\mathcal{A}_{f(n)}$ in a model $\mathcal{B}_n$.*

The existence of the interpretation as above allow us to transfer the properties of one family of the form $\mathrm{FM}(\mathcal{A})$ onto the other one, in which we can interpret $\mathrm{FM}(\mathcal{A})$. We show the following theorem (obtained with Michał Krynicki).

Theorem 15 ([KZ05]) *Let $\mathcal{N} = (\omega, +, \times, 0, 1)$ and let $\mathcal{A}$ be $(\omega, \times)$ or $(\omega, \exp)$. There exists an order preserving* sl*–interpretation of* $\mathrm{FM}(\mathcal{N})$ *in* $\mathrm{FM}(\mathcal{A})$.

The above theorem shows that in some way multiplication or exponentiation are as strong as the arithmetic of addition and multiplication. This is especially suprising for the case of multiplication which is strictly weaker than addition with multiplication in the infinite model. Nethertheless, we show that in finite models multiplication is a relatively strong operation. Moreover, the dependecies between arithmetics may be reversed in comparison to the infinite model.

Theorem 16 ([KZ05]) $\mathrm{FM}((\omega, \exp))$ *is definable in* $\mathrm{FM}((\omega, \times))$ *but not vice versa.*

Let us recall that in the infinite model $(\omega, \exp)$ defines addition and multiplication while in $(\omega, \times)$ one cannot define addition and the theory of $(\omega, \times)$ is decidable.

As a consequence of theorem 15 we obtained the following estimation on the complexity of theories of the families $\mathrm{FM}((\omega, \times))$ and $\mathrm{FM}((\omega, \exp))$ and on classes of representable relations in these families.

Theorem 17 ([KZ05]) *Let $\mathcal{N} = (\omega, +, \times, 0, 1)$, let $\mathcal{A}$ be $(\omega, \times)$ or $(\omega, \exp)$ and let $R \subseteq \omega^r$. R is* FM*–representable in* $\mathrm{FM}(\mathcal{A})$ *if and only if R is* FM*–representable in* $\mathrm{FM}(\mathcal{N})$.

Theorem 18 ([KZ05]) *Let $\mathcal{A}$ be $(\omega, \times)$ or $(\omega, \exp)$.*

1. *The theory of* $\mathrm{FM}(\mathcal{A})$ *is Π^0_1–complete.*
2. *The set* $\mathrm{sl}(\mathrm{FM}(\mathcal{A}))$ *is Σ^0_2–complete.*

After these results were obtained M. Mostowski and A. Wasilewska showed in [MW04] analogous results for arithmetic of divisibility. Moreover, the author of these thesis together with M. Mostowski gave in [MZ05a] an interpretation of $\mathrm{FM}((\omega, +, \times, 0, 1))$ in finite arithmetic of coprimality. This last result was presented in the thesis for information only without detailed proofs.

Together with M. Krynicki we estimated also the quantifier complexity of formulas with multiplication for which we get an undecidable finite model theory. Let $\exists^*$ be a class of formulas of the form $\exists x_1 \dots \exists x_n \psi$, where ψ is quantifier free and let $\exists^*\forall^*$ be a class of formulas of the form $\exists x_1 \dots \exists x_n \forall z_1 \dots \forall z_k \psi$, for ψ as above.

Theorem 19 ([KZ05]) *The set of $\exists^*\forall^*$–sentences which are satisfiable in $\mathrm{FM}((\omega, \times))$ is Σ_1^0–complete.*

Theorem 20 ([KZ05]) *Let $\mathcal{A} = (\omega, \times, \leq)$ and let $\varphi \in \exists^*$. Then, φ is satisfiable in $\mathrm{FM}(\mathcal{A})$ if and only if $\mathrm{FM}(\mathcal{A}) \models_{\mathrm{sl}} \varphi$.*

Theorem 21 ([KZ05]) *Let $\mathcal{A} = (\omega, \times, \leq)$. The problems of satisfiability in $\mathrm{FM}(\mathcal{A})$ and the problem of being true in almost all finite models from $\mathrm{FM}(\mathcal{A})$ are decidable for $\exists^*$–formulas.*

The proof of the above theorem is based on an estimation on the size of a model from $\mathrm{FM}(\mathcal{A})$ in which a given $\exists^*$–formula has to be true, if it is satisfiable in $\mathrm{FM}(\mathcal{A})$.

We say that a formula is in a relational form if all of its complex terms occur in the context $f(x_1, \dots, x_n) = z$. The following estimation was given in [KZ05].

Theorem 22 ([KZ05]) *Let $F(n) = \exp(2, 2^{n+1} 2^{\frac{2}{3}(4^{n+1}-1)}) + 1$ and let $\varphi \in \mathcal{F}_{\{\times, \leq\}}$ be an $\exists^*$ sentence in a relational form with all variables among $x_1, \dots, x_n$. If φ is satisfiable in $\mathrm{FM}((\omega, \times, \leq))$ then it has a model in $\mathrm{FM}((\omega, \times, \leq))$ of cardinality not greater than $F(n)$.*

We close our work with a partial characterization of sets of spectra for some finite arithmetics.

Definition 23 *By an $\mathrm{FM}(\mathcal{A})$–spectrum of the sentence φ we denote*

$$\mathrm{Spec}_{\mathrm{FM}(\mathcal{A})}(\varphi) = \{n + 1 : \mathcal{A}_{i+1} \models \varphi\}.$$

By a spectrum of $\mathrm{FM}(\mathcal{A})$ we denote the set of $\mathrm{FM}(\mathcal{A})$–spectra for all sentences,

$$\mathrm{Spec}(\mathrm{FM}(\mathcal{A})) = \left\{ \mathrm{Spec}_{\mathrm{FM}(\mathcal{A})}(\varphi) : \varphi \in \mathcal{F}_{\mathrm{FM}(\mathcal{A})} \right\}.$$

We show strict inclusions between spectra of the following arithmetics: $(\omega, \exp)$, $(\omega, \times)$, $(\omega, \times, \leq_P)$, $(\omega, +, \times)$, where $\leq_P$ is the ordering relation restricted to the set of prime numbers. The first one of these inclusions is from [KZ05].

Theorem 24

$$\mathrm{Spec}((\omega, \exp)) \subsetneq \mathrm{Spec}((\omega, \times)) \subsetneq \mathrm{Spec}((\omega, \times, \leq_P)) \subsetneq \mathrm{Spec}((\omega, +, \times)).$$

References

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

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

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

[Mos03] ———, *On representing semantics in finite models*, Philosophical Dimensions of Logic and Science (A. Rojszczak†, J. Cachro, and G. Kurczewski, eds.), Kluwer Academic Publishers, 2003, pp. 15–28.

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

[MZ05a] M. Mostowski and K. Zdanowski, *Coprimality in finite models*, Computer Science Logic: 19th International Workshop, CSL 2005 (Luke Ong, ed.), Lecture Notes in Computer Science, vol. 3634, Springer, 2005, pp. 263–275.

[MZ05b] ———, *FM–representability and beyond*, Proceedings of the conference Computability in Europe (B. Cooper, B. Loewe, and L. Torenvliet, eds.), Lecture Notes in Computer Science, vol. 3526, Springer, 2005, pp. 358–367.