Coprimality in Finite Models

Marcin Mostowski
Department of Logic
Institute of Philosophy, Warsaw University

Konrad Zdanowski
Institute of Mathematics
Polish Academy of Science

December 11, 2006

Abstract

We investigate properties of the coprimality relation within the family of finite models being initial segments of the standard model for coprimality, denoted by $\mathrm{FM}((\omega, \perp))$.

Within $\mathrm{FM}((\omega, \perp))$ we construct an interpretation of addition and multiplication on indices of prime numbers. Consequently, the first order theory of $\mathrm{FM}((\omega, \perp))$ is Π^0_1–complete (in contrast to the decidability of the theory of multiplication in the standard model). This result strengthens an analogous theorem of Marcin Mostowski and Anna Wasilewska, 2004, for the divisibility relation.

As a byproduct we obtain definitions of addition and multiplication on indices of primes in the model $(\omega, \perp, \leq_{P_2})$, where P_2 is the set of primes and products of two different primes and $\leq_X$ is the ordering relation restricted to the set X. This can be compared to the decidability of the first order theory of $(\omega, \perp, \leq_P)$, for P being the set of primes (Maurin, 1997) and to the interpretation of addition and multiplication in $(\omega, \perp, \leq_{P^2})$, for P^2 being the set of primes and squares of primes, given by Bès and Richard, 1998.

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

1 Introduction

This paper is devoted to the study of finite arithmetics, the research area concentrated on semantical and computational properties of arithmetical notions restricted to finite interpretations. Almost all computational applications of logic or arithmetic consider arithmetical notions in essentially finite framework. Therefore it is surprising that so little attention is directed to this area. This is particularly surprising when we observe that a few of classical papers in computer science (see e.g. Hoare [3], Gurevich [2]) postulate this research direction as particularly important.

Discussing the problem of analyzing algorithms in an implementation-independent way, Hoare essentially postulates proving their properties in appropriate axiomatic versions of finite arithmetic. We know that particular implementations of integers or unsigned integers (natural numbers) are essentially finite arithmetics with a distinguished upper bound.

By Trachtenbrot's theorem [17] we know that first order theories of non-trivial finite arithmetics cannot be axiomatizable. We know that the first order logic allowing arbitrary interpretations is axiomatizable. However, restricted to finite models it is axiomatizable only for poor vocabularies — for which it is recursive. Probably this was one of the reasons why Hoare's postulate did not motivate logicians to study the case of arithmetics with a finite bound. Nevertheless, let us observe that working in the standard infinite model of natural numbers is not easier in any way. The first order theory of this model is not arithmetical. On the other hand, the first order theory of any finite arithmetic is at most co-recursively enumerable, that is Π_1^0. Therefore we can expect much better axiomatic approximations in the finite case.

For this reason, we should firstly consider properties of finite arithmetics from the logical point of view. Only recently a few papers devoted mainly to this area have appeared, see [10], [14], [8], [12], [7].[1] Probably one of the reasons for the lack of interest in finite arithmetics in the past was the expectation that nothing surprising can be found under the restriction to a finite framework. Presently, we know that finite arithmetics have a lot of unexpected semantical and computational properties. Exponentiation is easier than multiplication [7], divisibility itself is as complicated as addition

[1] We do not claim that finite arithmetics were not considered in older papers at all, but not as the main topic.

and multiplication [12].

In this paper we give a solution of a problem presented at the Finite Model Theory Workshop Będlewo 2003. The problem is to determine the strength of coprimality in finite models. We show that, although semantically essentially weaker than the full arithmetic, it is recursively equally complicated.

The other source of our inspiration was the method of truth definitions in finite models proposed in [10] and further investigated in [11], [5] and [6]. The crucial problem there was finding a way of representing some non-trivial infinite relations in finite models. This motivated the notion of FM–representability.[2] It is known that a large class of arithmetical relations can be FM–represented. One of the motivating problems of our investigation is the question how much built-in arithmetic we need to apply the method of truth definitions. We characterize FM–representability for the finite arithmetic of coprimality. Our characterization — surprisingly — means that coprimality is sufficiently strong for the application of the truth definitions method in finite models.

Finally, as a byproduct of our research, we obtain an improvement of some theorems by Bès and Richard [1] characterizing the expressive power of coprimality in the standard infinite model equipped with some weak fragments of the standard ordering.

2 Basic notions

We start with the crucial definition of FM–domain.

Definition 1 *Let $\mathcal{R} = (R_1, \ldots, R_k)$ be a finite sequence of arithmetical relations on ω and let $\mathcal{A} = (\omega, \mathcal{R})$. We consider finite initial fragments of this model. Namely, for $n \geq 1$, by $\mathcal{A}_n$ we denote the following structure*

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

where, for $i = 1, \ldots, k$, the relation R_i^n is the restriction of R_i to the set $\{0, \ldots, n-1\}$.

The FM*–domain of $\mathcal{A}$, denoted by* FM($\mathcal{A}$)*, is the family $\{\mathcal{A}_n : n > 0\}$.*

[2] This notion was first considered in [10]. ("FM" stands for "Finite Models".) The paper [13] discusses some variants of the notion of FM–representability.

We assume that all considered models are in relational vocabularies. Thus, we think of addition or multiplication as ternary relations which describe graphs of corresponding functions. Nevertheless, we will write, e.g. $\varphi(x+y)$ with the intended meaning $\exists z\,(+(x,y,z)\wedge\varphi(z))$. Thus, the formula $\varphi(f(x))$ means that there exists z which is the value for $f(x)$ and φ is true about this z.

Definition 2 *We say that φ is true of $a_1,\ldots,a_r\in\omega$ in all sufficiently large finite models from* $\mathrm{FM}(\mathcal{A})$ *(shortly* $\mathrm{FM}(\mathcal{A})\models_{\mathrm{sl}}\varphi[a_1,\ldots,a_r]$*) if and only if*

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

Sometimes we also say that φ is true of $a_1,\ldots,a_r$ in almost all finite models from $\mathrm{FM}(\mathcal{A})$.

Of course, k as above should be chosen in such a way that $k>\max\{a_1,\ldots,a_r\}$.

Definition 3 *We say that $R\subseteq\omega^r$ is* FM*–represented in* $\mathrm{FM}(\mathcal{A})$ *by a formula $\varphi(x_1,\ldots,x_r)$ if and only if for each $a_1,\ldots,a_r\in\omega$ the following conditions hold:*

(i) $\mathrm{FM}(\mathcal{A})\models_{sl}\varphi[a_1,\ldots,a_r]$ *if and only if $R(a_1,\ldots,a_r)$,*

(ii) $\mathrm{FM}(\mathcal{A})\models_{sl}\neg\varphi[a_1,\ldots,a_r]$ *if and only if $\neg R(a_1,\ldots,a_r)$.*

The main characterization of the notion of FM–representability in $FM(\mathbb{N})$, for $\mathbb{N}=(\omega,+,\times)$, is given by the following theorem (see [10]).

Theorem 4 (FM**–representability theorem)** *Let $R\subseteq\omega^n$. R is* FM*–representable in* $\mathrm{FM}(\mathbb{N})$ *if and only if R is decidable with a recursively enumerable oracle.*

The first question related to FM–representability is the following: How weak arithmetical notions are sufficient for the FM–representability theorem? In [10] the theorem has been proven for addition, multiplication and concatenation. It is a straightforward observation that concatenation is superfluous. A few less trivial results in this direction were obtained in [7] and [12]. In particular, in the last paper it was proven that:

Theorem 5 *For each $R \subseteq \omega^r$, R is* FM*–representable in* FM$(\mathbb{N})$ *if and only if R is* FM*–representable in* FM*–domain of divisibility,* FM$((\omega, |))$*, where $a|b \equiv \exists x\ ax = b$.*

It is surprising that such a weak relation as divisibility is sufficient here. So, the following natural problem appears. Can this theorem be improved by replacing divisibility by some weaker notions? For example, coprimality, where the coprimality relation, $\perp$, is defined by the following equivalence:

$$a \perp b \equiv \forall x((x|a \wedge x|b) \Rightarrow \forall y\ x|y).$$

The answer is obviously negative. Let us consider the function f defined as

$$f(x) = \begin{cases} 4 & \text{if } x = 2, \\ 2 & \text{if } x = 4, \\ x & \text{otherwise.} \end{cases}$$

f is an automorphism of $(\omega, \perp)$. Moreover, f also preserves coprimality when it is restricted to initial segments $\{0, \ldots, n\}$, for $n \geq 4$,. Therefore, the set $\{2\}$ is not FM–representable in FM$((\omega, \perp))$. However, surprisingly, in a weaker sense coprimality is as difficult as addition and multiplication, see Theorems 10, 18, and 19.

Let us observe that in the standard model coprimality, and even multiplication, are relatively weak relations. Indeed, the first order theory of $(\omega, \times, \leq_P)$ is decidable, see [9], where P is the set of prime numbers and $\leq_P$ is the ordering relation restricted to this set.

We use the notion, $\leq_X$, for various sets $X \subseteq \omega$, with the analogous meaning. The complement of the predicate $\perp$ is denoted by $\not\perp$.

In our work, we use the notion of a first order interpretation. For details, see the paper by Szczerba [16], where the method was codified for the first time in the model-theoretic framework. We recall shortly the main ideas.

Let τ and σ be vocabularies and, for simplicity, let σ contain only one n-ary predicate R. A sequence $\bar{\varphi} = (\varphi_U, \varphi_\approx, \varphi_R)$ of formulae in the vocabulary τ is a first order interpretation of models of the vocabulary σ if the free variables of φ_U are $x_1, \ldots, x_r$, the free variables of $\varphi_\approx$ are $x_1, \ldots, x_{2r}$ and the free variables of φ_R are $x_1, \ldots, x_{rn}$. The sequence $\bar{\varphi}$ defines in a model $\mathcal{A}$ of the vocabulary τ a model of the vocabulary σ in the following sense. A universe U, defined by φ_U, is the set of n–tuples from $\mathcal{A}$:

$$U = \{(a_1, \ldots, a_r) : \mathcal{A} \models \varphi_U[a_1, \ldots, a_r]\}.$$

The equality relation is given by $\varphi_\approx$ which should define an equivalence relation on U. The interpretation of R is defined by

$$R(\mathbf{a}_1, \ldots, \mathbf{a}_n) \text{ if and only if}$$

$$\exists \bar{a}_1 \in \mathbf{a}_1 \ldots \exists \bar{a}_n \in \mathbf{a}_n \; \mathcal{A} \models \varphi_R[\bar{a}_1, \ldots, \bar{a}_n],$$

where $\mathbf{a}_1, \ldots \mathbf{a}_n$ are equivalence classes of the relation defined by $\varphi_\approx$ in U. The number r is called the width of the interpretation.

We write $I_{\bar{\varphi}}(\mathcal{A})$ for the model defined by $\bar{\varphi}$ in $\mathcal{A}$.

Definition 6 *We say that $\bar{\varphi}$ is an interpretation of* $\mathrm{FM}(\mathcal{A})$ *in* $\mathrm{FM}(\mathcal{B})$ *if there is a monotone, unbounded function $f : \omega \longrightarrow \omega$ such that for each $n \geq 1$,*

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

If $\bar{\varphi}$ is of width 1, φ_U defines an initial segment in each model from $\mathrm{FM}(\mathcal{B})$ *and the isomorphism between $\mathcal{A}_{f(n)}$ and $\mathcal{B}_n$ is just identity then we say that $\bar{\varphi}$ is an* IS*–interpretation.*

An IS–interpretation was used in [12] for proving Theorem 5. In our interpretation of $\mathrm{FM}(\mathbb{N})$ in $\mathrm{FM}((\omega, \perp))$ we define arithmetic on indices of prime numbers.

3 The main theorem

In what follows models of the form $(\omega, \perp)$ or $\mathrm{FM}((\omega, \perp))$ are called coprimality models.

Let $\{p_i : i \in \omega\}$ be the enumeration of primes, that is $p_0 = 2, p_1 = 3, \ldots$ For a natural number a we use the notion of the support of a, defined as $\mathrm{Supp}(a) = \{p_i : p_i | a\}$. We define the equivalence relation $\approx$ as follows:

$$a \approx b \iff \mathrm{Supp}(a) = \mathrm{Supp}(b).$$

For each a, the equivalence class of a is denoted by $[a]$. Let us observe, that in each model from $\mathrm{FM}((\omega, \perp))$ as well as in $(\omega, \perp)$ we cannot distinguish between elements being in the same equivalence class of $\approx$.

Definition 7 *A relation $R \subseteq \omega^r$ is coprimality invariant if $\approx$ is a congruence relation for R. This means that for all tuples $a_1, \ldots, a_r$ and $b_1, \ldots, b_r$ such that $a_i \approx b_i$, for $i = 1, \ldots, r$,*

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

We define relations R_+ and $R_\times$ by the following conditions:

$$R_+([p_i], [p_k], [p_m]) \text{ if and only if } i + k = m,$$

$$R_\times([p_i], [p_k], [p_m]) \text{ if and only if } ik = m.$$

We identify these relations with their coprimality invariant versions on elements of ω, instead of $\omega/_\approx$. R_+ and $R_\times$ give an interpretation of addition and multiplication on indices of prime numbers. Our main result is that they are interpretable in $\mathrm{FM}((\omega, \perp))$

For the proof of our main theorem we need some facts about the distribution of prime numbers.

Let $\pi(x)$ be a function defined as

$$\pi(x) = \sum_{\substack{p \leq x \\ p - \text{prime}}} 1.$$

The prime number theorem states that the limit $\pi(x)/(x/\ln(x))$ converges to 1 for x going to infinity. We need the following consequences of the prime number theorem.

Proposition 8 *For each $b \in \omega$ there is K such that for each $n \geq K$ and for each $i < b$ there is a prime q such that*

$$in \leq q < (i + 1)n.$$

Sierpiński has observed in [15] that $K = e^b$ suffices.

Proposition 9 *Let $0 < \varepsilon < 1$. There is N such that for all $x \geq N$ the interval $(x, x(1 + \varepsilon))$ contains a prime.*

Essentially, Proposition 9 is one of the corollaries of the prime number theorem mentioned in [4].

The main theorem of this section is the following.

Theorem 10 *There is an interpretation $\bar{\varphi}$ of width 1 of* $\mathrm{FM}(\mathbb{N})$ *in* $\mathrm{FM}((\omega, \perp))$ *such that for each k there is n such that $\bar{\varphi}$ defines in the model $(\{0, \ldots, n-1\}, \perp)$ the relations R_+ and $R_\times$ on an initial segment of $\{0, \ldots, n-1\}$ of size at least k.*

Moreover, the equality predicate is not used in the formulae from $\bar{\varphi}$.

Proof. We will prove the theorem through a sequence of lemmas.

Firstly, we define some auxiliary notions. Let $\varphi_\approx(x, y)$ be the formula

$$\forall z(z \perp x \equiv z \perp y).$$

Obviously, this formula defines the relation $\approx$ in $(\omega, \perp)$. Ambiguously, we denote relations defined by $\varphi_\approx(x, y)$ in models $(\omega, \perp)$ and $\mathrm{FM}((\omega, \perp))$ by $\approx$. In all these models $\approx$ is a congruence relation. (It means that $\approx$ is an equivalence and for all $a, b, a', b' \in \omega$ such that $a \approx a'$ and $b \approx b'$ we have $a \perp b$ if and only if $a' \perp b'$.) Therefore, in all considered models we cannot differentiate elements which are in the relation $\approx$. So, we can consider models $M_{/\approx}$ instead of M. The equivalence class of $a \in |M|$ with respect to $\approx$ is denoted by $[a]$. The elements of $M_{/\approx}$ which are of the form $[a]$ for $a \in |M|$, can be identified with finite sets of primes, $\mathrm{Supp}(a)$.

We define some useful predicates.

- $P(x) := \forall z, y(z \not\perp x \wedge y \not\perp x \Rightarrow z \not\perp y)$ — x is a power of prime,
- $x \in y := P(x) \wedge x \not\perp y$ — x is a power of prime dividing y.
- $\{p, q\}$ — a function denoting, for a pair of primes p, q, an element of an equivalence class of pq. We have no multiplication but elements a such that $a \approx pq$ are defined by the formula $\forall z(z \perp a \equiv (z \perp p \wedge z \perp q))$. Of course we cannot define the unique a with this property. Nevertheless, this element is unique up to $\approx$. So, when considering models of the form $M_{/\approx}$, it is simply unique.

We have some operations definable on the equivalence classes of $\approx$.

Lemma 11 *There are formulae in the coprimality language $\varphi_\cup(x, y, z)$, $\varphi_\cap(x, y, z)$, $\varphi_-(x, y, z)$ such that in each coprimality model M, the following conditions hold for each $a, b, c \in |M|$:*

- $M \models \varphi_\cup[a, b, c]$ *if and only if* $\mathrm{Supp}(a) \cup \mathrm{Supp}(b) = \mathrm{Supp}(c)$,

- $M \models \varphi_{-}[a,b,c]$ *if and only if* $\mathrm{Supp}(a) \setminus \mathrm{Supp}(b) = \mathrm{Supp}(c)$,
- $M \models \varphi_{\cap}[a,b,c]$ *if and only if* $\mathrm{Supp}(a) \cap \mathrm{Supp}(b) = \mathrm{Supp}(c)$.

Proof. As $\varphi_{\cup}(x,y,z)$ we can take

$$\forall w(w \perp z \equiv (w \perp x \wedge w \perp y)).$$

$\varphi_{-}(x,y,z)$ can be written as

$$\forall w(P(w) \Rightarrow (w \not\perp z \equiv (w \not\perp x \wedge w \perp y))).$$

$\varphi_{\cap}$ is expressible in terms of $\varphi_{\cup}$ and φ_{-}. □
□

It follows that in all coprimality models we can reconstruct a partial lattice of finite sets of primes. However, the operation $\cup$ is total only in the infinite model $(\omega, \perp)$.

The crucial fact is that in finite models from $\mathrm{FM}((\omega,\perp))$ we can compare small elements of a given model by the following formula $\varphi_{\prec}(x,y) :=$

$$\exists z(P(z) \wedge z \perp x \wedge z \perp y \wedge \exists w\ \varphi_{\cup}(x,z,w) \wedge \neg \exists w\ \varphi_{\cup}(y,z,w)).$$

By $\varphi_{\preceq}(x,y)$ we mean the formula $\varphi_{\prec}(x,y) \vee \varphi_{\approx}(x,y)$.

For a finite set $X \subseteq \omega$, we write ΠX for the product of all numbers in X.

Lemma 12 *For each c there is N such that for all $n \geq N$ and for all a, b with $1 \leq a, b \leq n$ and $\max\{\Pi\mathrm{Supp}(a), \Pi\mathrm{Supp}(b)\} \leq c$ the following holds*

$$(\{0,\ldots,n-1\}, \perp) \models \varphi_{\prec}[a,b] \quad \textit{if and only if} \quad \Pi\mathrm{Supp}(a) < \Pi\mathrm{Supp}(b)$$

Proof. Let $\mathcal{A} = (\{0,\ldots,n-1\}, \perp)$. The direction from left to right is simple. If $\mathcal{A} \models \varphi_{\prec}[a,b]$ then there is a prime $d \in |\mathcal{A}|$ such that $d\Pi\mathrm{Supp}(a) \leq n-1$ and $d\Pi\mathrm{Supp}(b) > n-1$. So, $\mathrm{Supp}(a) < \mathrm{Supp}(b)$.

To prove the other direction let us set $a_1 = \Pi\mathrm{Supp}(a)$ and $b_1 = \Pi\mathrm{Supp}(b)$ and let $a_1 < b_1$. Then, $\varphi_{\prec}$ is satisfied by a and b if and only if $(\frac{n-1}{b_1}, \frac{n-1}{a_1}]$ contains a prime. In the worst case $b_1 = a_1 + 1$ and in this case $(\frac{n-1}{b_1}, \frac{n-1}{b_1}(1+\frac{1}{a_1})]$ should contain a prime. Thus it suffices to take N from Proposition 9 for $\varepsilon = 1/a_1$. □
□

Now, our aim is to define in models from $\mathrm{FM}(\omega, \perp))$ the relations R_+, $R_\times$. We define these relations on an initial segment of the model $(\{0, \ldots, n-1\}, \perp)$.

Firstly, we introduce a tool for coding pairs of primes.

$\mathrm{Code}(p, x, y, q) \iff_{Def}$
$P(p) \wedge P(q) \wedge P(x) \wedge P(y) \wedge$ " q is the $\prec$–greatest prime less then $\{p, x, y\}$".

The statement in quotation marks can be written down as

$$\forall z \forall w[(\varphi_\cup(x, y, z) \wedge \varphi_\cup(p, z, w)) \Rightarrow \varphi_\prec(q, w)] \wedge$$

$$\forall r[(P(r) \wedge \varphi_\prec(q, r)) \Rightarrow \exists z \exists w(\varphi_\cup(x, y, z) \wedge \varphi_\cup(p, z, w) \wedge \varphi_\prec(w, r))].$$

In the above formula, the variable w plays the role of the set $\{p, x, y\}$. Then, with the help of $\varphi_\prec$ we easily express the maximality of q.

The intended meaning of the formula $\mathrm{Code}(p, x, y, q)$ is that q is a code of an unordered pair consisting of x and y. The prime q is determined uniquely up to the equivalence $\approx$. The prime p is called a base of a coding. Now, we define a formula which states that coding with the base p is injective below x.

$$\begin{aligned}
&\mathrm{GoodBase}(p, x) := \\
&P(p) \wedge \forall q_1 \ldots \forall q_4 \{[\bigwedge_{i \leq 4} (P(q_i) \wedge \varphi_\preceq(q_i, x)) \wedge \neg \varphi_\approx(\{q_1, q_2\}, \{q_3, q_4\})] \Rightarrow \\
&\qquad \exists c_1 \exists c_2 (\mathrm{Code}(p, q_1, q_2, c_1) \wedge \mathrm{Code}(p, q_3, q_4, c_2) \wedge \neg \varphi_\approx(c_1, c_2)\}.
\end{aligned}$$

The above formula states that p is a good base for our coding for primes which are less than x. Namely, for each pair of primes below x we obtain a different code q taking p as a base. The existence of a good base for each given x is guaranteed by Proposition 8. We subsume the above consideration in the following lemma.

Lemma 13 *For each k there is N and $p \leq N$ such that For all $n \geq N$, $\mathrm{Code}(p, x_1, x_2, z)$ defines an injective coding of pairs of primes less than k in each model $(\{0, \ldots, n-1\}, \perp)$.*

Proof. Let k be given and let K be chosen from Proposition 8 for $b = k^2$. Next, let p be a prime greater than K. By Proposition 8 p is a good base

for our coding in all models $(\{0,\ldots,n-1\},\perp)$, for $n \geq N = k^2p$. $\square$
$\square$

When the exact base for our coding of pairs of primes is inessential we write simply $\langle x,y\rangle$ for a prime coding a pair x, y. Of course, in such a case a proper base for our coding should be assured to exist. Nevertheless, since we always will be interested in coding pairs of primes from a given initial segment, the existence of a proper base follows in this case by Lemma 13.

The last lemma allows to turn recursive definitions of addition and multiplication on indices of primes into explicit ones. The first needed relation is the successor relation on indices of primes. It is defined as

$$S_{\prec}(x) = y \iff_{Def} \varphi_{\prec}(x,y) \wedge P(x) \wedge P(y) \wedge \forall z\,(P(z) \Rightarrow \neg(\varphi_{\prec}(x,z) \wedge \varphi_{\prec}(z,y))).$$

Let us observe that if $S_{\prec}(p_z)$ is defined in a given finite model then it is the case that $S_{\prec}(p_z) = p_{z+1}$. We have the following.

Lemma 14 *Partial functions on indices of primes* FM*–representable in coprimality models equipped with the relation $\prec$ are closed under the scheme of primitive recursion.*

Proof. Let $g : \omega^n \longrightarrow \omega$ and $h : \omega^{n+2} \longrightarrow \omega$ be functions on indices of primes FM–representable in coprimality models. We need to show that the function $f : \omega^{n+1} \longrightarrow \omega$ defined as

$$f(0,\bar{x}) = g(\bar{x}),$$
$$f(i+1,\bar{x}) = h(i+1,\bar{x},f(i,\bar{x})).$$

is FM–representable in coprimality models with $\prec$. For simplicity we assume that $n = 1$. Since we have $\prec$ and $\perp$, we can define, by Lemma 13, a function $\langle x,y\rangle$ coding pairs of primes as primes. The formula defining $f(p_i,p_x) = p_t$ states that there is a set which describes a recursive computation of $f(p_i,p_x)$ with the output p_t. It can be written as

$$\begin{aligned}&\exists X\{\langle p_0, g(p_x)\rangle \in X \wedge\\ &\forall p_z \forall p_w[\varphi_{\prec}(p_z,p_i) \Rightarrow (\langle p_{z+1},p_w\rangle \in X \iff\\ &\qquad \exists p_v(\langle p_z,p_v\rangle \in X \wedge p_w \approx h(p_{z+1},p_x,p_v)))] \wedge\\ &\qquad\qquad \langle p_i,p_t\rangle \in X\}.\end{aligned}$$

Let us observe that quantification over a set of primes X can be interpreted as first order quantification over numbers. Instead of X we can take a such that $X = \mathrm{Supp}(a)$. Thus, if we have formulas defining g and h, all the other notions can be defined in models for coprimality and $\prec$. □
□

Now, let φ_+ and $\varphi_\times$ be formulae, provided by means of Lemma 14, which define addition and multiplication on indices of primes. They define R_+ and $R_\times$ only on some initial segment of primes from a given finite model, but this segment grows with the size of a model.

We define the universe of our interpretation by the formula $\varphi_U(x_1)$ which states that φ_+ and $\varphi_\times$ define addition and multiplication on the set

$$\{y : P(y) \wedge (y \approx x_1 \vee y \prec x_1)\}.$$

Such a formula exists because there is a finite axiomatization of $\mathrm{FM}((\omega, +, \times))$ within the class of all finite models given explicitly in [11]. Thus, we have shown that $\mathrm{FM}((\omega, +, \times))$ is interpretable in finite models of coprimality even without equality. This ends the proof of Theorem 10. □
□

4 Some applications in finite models

As a corollary of Theorem 10, we obtain a partial characterization of relations which are FM–representable in $\mathrm{FM}((\omega, \perp))$.

Definition 15 *Let $R \subseteq \omega^r$. We define R^* as*

$$R^* = \{(x_1, \ldots, x_r) : \exists a_1 \ldots \exists a_r (\bigwedge_{i \leq r} (x_i \approx p_{a_i}) \wedge (a_1, \ldots, a_r) \in R\}.$$

Corollary 16 *Let $R \subseteq \omega^r$. R is* FM*–representable in* $\mathrm{FM}(\mathbb{N})$ *if and only if R^* is* FM*–representable in* $\mathrm{FM}((\omega, \perp))$.

Now we are going to characterize the complexity of the first order theory of $\mathrm{FM}((\omega, \perp))$ and of relations which are FM–represented in $\mathrm{FM}((\omega, \perp))$. Firstly, we need a partial result in this direction.

Let us define the relation $S \subseteq \omega^2$ such that

$$(x, y) \in S \text{ if and only if } \exists z(z \approx x \wedge y \approx p_z).$$

Lemma 17 *The relation S is* FM*–representable in* FM$((\omega, \perp))$.

Proof. To simplify the exposition we consider all the equivalences between formulae in the sense of being true in all sufficiently large models from FM$((\omega, \perp))$. They will be justified for fixed parameters a, b for which we want to decide whether $(a, b) \in S$. Thus, we may safely assume that $b \approx p$, for some prime p.

Let $x_0, x_1, \ldots$ be the enumeration of all consecutive products of different primes ordered according to $<$. This enumeration lists $\approx$–representatives of all $\approx$–equivalence classes. For $x \in \omega$ we define $\mathrm{ind}(x)$ as the unique i such that $x \approx x_i$. We define an auxiliary relation W such that

$$(x, y) \in W \iff y \approx p_{\mathrm{ind}(x)}.$$

Now, take $n = \mathrm{ind}(x)$ and let $a_0, \ldots, a_n$ be an initial segment of the above enumeration. By Proposition 8, there is a prime t such that each interval (ta_i, ta_{i+1}), for $i < n$, contains a prime. Let $q_0, \ldots, q_n$ be a sequence of primes such that

$$q_i = \min\{s : P(s) \wedge ta_i \prec q_i\}$$

and let $B = \Pi_{i \leq n} q_i$. Then, let $p_0, \ldots, p_k$ be a sequence of consecutive primes such that $p_k \approx y$ and let $C = \Pi_{i \leq k} p_i$. Let us observe that B and C are definable from x, t and y in terms of $\prec$ and $\perp$. Moreover, any t which allows this definition is good for our purpose. Thus, we can use B and C in our formulae.

Now, we show how to write a formula $\varphi_W(x, y)$ which, for any pair of fixed parameters as x and y, holds in almost all finite models from FM$((\omega, \perp))$ exactly when $(x, y) \in W$. The formula $\varphi_W(x, y)$ expresses the fact that sets coded by B and C, constructed as above, are equicardinal. This can be witnessed by a set X which is a set of pairs of primes from B and C determining a bijection between B and C. In the formula φ_W below we use $\exists^{=1} z$ for the quantifier "there exists exactly one z".

$$\exists X\{\forall q \in B\, \exists^{=1} p \in C\, \langle q, p\rangle \in X \wedge \forall p \in C\, \exists^{=1} q \in B\, \langle q, p\rangle \in X\}.$$

Of course, the existence of such an X proves that B and C are equicardinal. By the same argument as in the proof of Lemma 14 we can replace quantifying over X by first order quantification.

Now, we show how to define S from W. Let T be the following relation. For all $x, y \in \omega$,

$$(x, y) \in T \iff \mathrm{ind}(x) = y.$$

This relation is recursive, thus also FM–representable in $\mathrm{FM}((\omega, +, \times))$ and, by Corollary 16, the starred version of T is FM–representable in $\mathrm{FM}((\omega, \perp))$. T^* satisfies the following condition: for all x, y,

$$(x, y) \in T^* \iff \exists z(p_z \approx x \wedge p_{\mathrm{ind}(z)} \approx y).$$

So, let $\varphi_{T^*}(x, y)$ FM–represent T^*.

Let us also recall the definitions of S and W:

$$(x, y) \in S \iff \exists(z \approx x \wedge p_z \approx y),$$

$$(x, y) \in W \iff y \approx p_{\mathrm{ind}(x)}.$$

Let us observe that in all sufficiently large finite models an element w such that $\varphi_W(x, w)$ is just $p_{\mathrm{ind}(x)}$.

Now, the formula $\varphi_S(x, y)$ which FM–represents S can be written as

$$\exists w(\varphi_W(x, w) \wedge \varphi_{T^*}(y, w)).$$

Then, for all fixed parameters a and b, and for almost all finite models M from $\mathrm{FM}((\omega, \perp))$, the following equivalence holds:

$$M \models \varphi_S(a, b) \quad \iff \quad (a, b) \in S.$$

For the direction from left to right let us assume that for some t we have $\varphi_W(a, t)$ and $\varphi_{T^*}(b, t)$. This means that

$$t \approx p_{\mathrm{ind}(a)}$$

and that for some s we have

$$p_s \approx b \text{ and } p_{\mathrm{ind}(s)} \approx t.$$

This gives $p_{\mathrm{ind}(a)} \approx p_{\mathrm{ind}(s)}$ and $\mathrm{ind}(a) = \mathrm{ind}(s)$. Therefore, $s \approx a$ and $p_s \approx b$, which gives $(a, b) \in S$.

Now let us assume that $(a, b) \in S$. Then for some z we have

$$z \approx a \text{ and } p_z \approx b.$$

This gives that $\mathrm{ind}(z) = \mathrm{ind}(a)$, $p_z \approx b$ and $p_{\mathrm{ind}(z)} \approx t$, for $t = p_{\mathrm{ind}(z)}$. Then $\varphi_{T^*}(b, t)$. Additionally, $t \approx p_{\mathrm{ind}(a)}$ and $\varphi_W(a, t)$. Therefore, $\varphi_S(x, b)$. □
□

Theorem 18 *Let $R \subseteq \omega^r$. R is* FM*–representable in* $\mathrm{FM}((\omega, \perp))$ *if and only if R is* FM*–representable in* $\mathrm{FM}(\mathbb{N})$ *and R is coprimality invariant.*

Proof. All relations which are FM–representable in $\mathrm{FM}((\omega, \perp))$ are coprimality invariant. Therefore, the implication from left to right is obvious. So, we prove the converse.

For the sake of readability we consider only unary relations. Let us fix a coprimality invariant relation $R \subseteq \omega$ which is FM–representable in $\mathrm{FM}(\mathbb{N})$. By Corollary 16, let us take a formula $\xi(x)$ FM–representing R^* in the FM–domain of coprimality.

By Lemma 17, there is a formula $\psi(x, y)$, with coprimality as the only predicate, such that $\psi(x, y)$ FM–represents S in the FM–domain of coprimality. Then the formula $\varphi(x)$ defined as

$$\exists y(\psi(x, y) \wedge \forall z(\varphi_{\prec}(z, y) \Rightarrow \neg\psi(x, z)) \wedge \xi(y))$$

FM–represents R. □
□

Finally, let us consider the recursive complexity of the elementary theory of $FM((\omega, \perp))$. The classical Trachtenbrot theorem says that we can reduce the halting problem to the problem of satisfiability in finite models. By our interpretation, it suffices to consider only finite models for coprimality.

Theorem 19 (Trachtenbrot's theorem for coprimality FM**–domain)** *The first order theory of* $\mathrm{FM}((\omega, \perp))$ *is* Π^0_1*–complete. Moreover, the theorem remains valid even if we do not have equality in the language.*

5 An application in the standard model

Maurin has shown in [9] that the first order theory of $(\omega, \times, \leq_P)$, where $\leq_P$ is the standard ordering restricted to primes, is decidable. On the other hand, Bès and Richard have shown in [1] that adding the ordering on primes and squares of primes to coprimality allows an interpretation of addition and multiplication. In what follows, we prove a similar result for the structure $(\omega, \perp, \leq_{P_2})$, where P_2 is the set of primes and products of two different primes. Namely, we show that the relations R_+ and $R_\times$ are definable in $(\omega, \perp, \leq_{P_2})$. It follows that the first order theory of this model is as hard as the theory of $(\omega, +, \times)$. (Let us mention that it is not known whether R_+ and $R_\times$ are definable in the structure considered by Bès and Richard.)

Below, we show how to develop a coding for pairs of prime numbers below a given prime k. Then, the rest of the argument is the same as in the case of finite models. However, we cannot use coding of pairs of primes from the preceding sections since it uses a comparison of primes with products of three different primes. We defined such a coding there since it gives a simpler construction. Moreover, if one wants to estimate a fragment of a finite model on which we have definitions of R_+ and $R_\times$ then such a coding gives a better bound than the coding which we are going to present now. On the other hand, in the infinite model, we want to add to coprimality a relation as weak as possible to obtain our definability result.

Theorem 20 *R_+ and $R_\times$ are definable in $(\omega, \perp, \leq_{P_2})$, where $\leq_{P_2}$ is the ordering relation restricted to primes and products of two different primes.*

Proof. We only show how to define coding of pairs of primes by one prime, while the rest of the proof remains the same as in the finite case.

Let a prime k be given. We show how to code pairs of primes less or equal to k. Let ε be such that

$$(1+\varepsilon)^3 < k^2/(k^2-1), \qquad (*)$$

and let p be a prime such that for all $n \geq p$, the interval

$$(n, n(1+\varepsilon))$$

contains a prime number. Then, our new formula $\mathrm{Code}(p, x, y, r)$ is the following:

$$P(p) \wedge P(x) \wedge P(y) \wedge P(r) \wedge$$

$$\exists r_1 \exists r_2 (\text{“}r_1 \text{ is the smallest prime greater than } px\text{”} \wedge$$

“r_2 is the smallest prime greater than py”$\wedge$“r is the greatest prime less than $r_1 r_2$”).

All the notions needed in the above formula are definable in $(\omega, \perp, \leq_{P_2})$. Now, we only argue that the coding with p chosen as above is injective below k.

Let q, q' be two primes less or equal to k. By the choice of ε and p, there is a code r for this pair with the property

$$p^2(qq' - 1)(1 + \varepsilon)^2 < r < p^2 qq'(1 + \varepsilon)^2.$$

The first inequality follows from the fact that $pq < r_1$ and $pq' < r_2$. Thus, r is greater than any z such that $z(1 + \varepsilon) < p^2 qq'$. The maximal z with this property is greater than $p^2(qq' - 1)(1 + \varepsilon)^2$. Indeed,

$$\begin{aligned} p^2(qq' - 1)(1 + \varepsilon)^2(1 + \varepsilon) &\leq p^2 qq'(1 - 1/qq')(1 + \varepsilon)^3 \\ &\leq p^2 qq'(1 - 1/k^2)(1 + \varepsilon)^3 \\ &< p^2 qq', \end{aligned}$$

where the last strict inequality follows by (*).

The second inequality follows from the fact that $r_1 < pq(1 + \varepsilon)$, $r_2 < pq'(1 + \varepsilon)$, and $r < r_1 r_2$.

Therefore, for any pair of primes $q, q' \leq k$, the code r for this pair is in the interval $(p^2(qq' - 1)(1 + \varepsilon)^2, p^2 qq'(1 + \varepsilon)^2)$. However, since for any other pair of primes $t, t' \leq k$, qq' differs from tt' by at least one, these intervals are disjoint for different pairs of primes. This proves that our coding method with p as a base is injective below k. □

□

References

[1] Bès, A. and Richard, D., *Undecidable extensions of Skolem arithmetic*, **Journal of Symbolic Logic**, 63(1998), pp. 379–401.

[2] Gurevich, Y., *Logic and the Challenge of Computer Science*, in **Current Trends in Theoretical Computer Science** (ed. E. Börger) Computer Science Press, 1988, 1–7.p

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

[4] Jameson, G. J. O., **The prime number theorem**, Cambridge University Press, 2003.

[5] Kołodziejczyk, L. A. *Truth definitions in finite models*, **Journal of Symbolic Logic**, 69(2004), pp. 183–200.

[6] Kołodziejczyk, L. A. *A finite model-theoretical proof of a property of bounded query classes within PH*, **Journal of Symbolic Logic**, 69(2004), pp. 1105–1116.

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

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

[9] Maurin, F. *The theory of integer multiplication with order restricted to primes is decidable*, **Journal of Symbolic Logic**, 62(1997), pp. 123–130.

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

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

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

[13] Mostowski, M. and Zdanowski, K., FM*–representability and beyond*, Cooper, S. B., Löwe, B. and Torenvliet, L. (eds.), CiE 2005, LNCS 3526, Springer, pp. 358–367, 2005.

[14] Schweikardt, N., *Arithmetic, First-Order Logic, and Counting Quantifiers*, **ACM Transactions on Computational Logic**, 5(2004), pp. 1–35.

[15] Sierpiński, W., **Elementary Theory of Numbers**, PWN (Polish Scientific Publishers) – North Holland, 1964.

[16] Szczerba, L. W., *Interpretability of elementary theories*, in Proceedings 15th ICALP 88 **Logic, foundations of mathematics and computability theory**, eds. Butts, Hintikka, Reidel Publishing, 1977, pp. 129–145.

[17] Trachtenbrot, B., *The impossibility of an algorithm for the decision problem for finite domains*, in **Doklady Akademii Nauk SSSR**, 70(1950), pp. 569–572, in russian.