Undecidable extensions of Skolem arithmetic

Alexis Bès , Denis Richard

Published in J.Symb.Logic 63(2), 379–401 (1998)

Abstract

Let $<_{P_2}$ be the restriction of usual order relation to integers which are primes or squares of primes, and let $\perp$ denote the coprimeness predicate. The elementary theory of $\langle \mathbb{N}; \perp, <_{P_2} \rangle$ is undecidable. Now denote by $<_\Pi$ the restriction of order to primary numbers. All arithmetical relations restricted to primary numbers are definable in the structure $\langle \mathbb{N}; \perp, <_\Pi \rangle$. Furthermore, the structures $\langle \mathbb{N}; |, <_\Pi \rangle$, $\langle \mathbb{N}; =, \times, <_\Pi \rangle$ and $\langle \mathbb{N}; =, +, \times \rangle$ are interdefinable.

Résumé

Soit $<_{P_2}$ la restriction de l'ordre usuel aux entiers qui sont premiers ou carrés de premiers, et soit $\perp$ le prédicat de coprimarité. La théorie élémentaire de $\langle \mathbb{N}; \perp, <_{P_2} \rangle$ est indécidable. Soit maintenant $<_\Pi$ l'ordre restreint aux entiers primaires. Toute relation arithmétique restreinte aux entiers primaires est définissable dans la structure $\langle \mathbb{N}; \perp, <_\Pi \rangle$. De plus, les structures $\langle \mathbb{N}; |, <_\Pi \rangle$, $\langle \mathbb{N}; =, \times, <_\Pi \rangle$ et $\langle \mathbb{N}; =, +, \times \rangle$ sont interdéfinissables.

1. Introduction

This paper is concerned with questions of definability and decidability related to several sublanguages of arithmetic. For every $X \subseteq \mathbb{N}$, let $<_X$ be the restriction of usual order relation to elements of X. In [Mau95], F.Maurin proved that the elementary theory of the structure $\langle \mathbb{N} \setminus \{0\}; =, \times, <_P \rangle$, where P denotes the set of prime numbers, is decidable. On the other hand, according to Tarski's equivalence

$$[z = 0 \ \vee z = x + y] \Longleftrightarrow (xz + 1)(yz + 1) = z^2(xy + 1) + 1$$

it is easily shown that addition is first-order definable in the structure $\langle \mathbb{N}; =, \times, < \rangle$, which implies the undecidability of its elementary theory.

A natural question that arises from the above results is to determine, among fragments of order "richer" than $<_P$, those which, associated with multiplication, lead to undecidable theories. In particular, F.Maurin asks whether the structure $\langle \mathbb{N}; =, \times, <_\Pi \rangle$, where Π denotes the set of primary numbers (i.e. powers of primes), has a decidable theory or not. We show in this paper that even more restrictive fragments of order, in association with predicates weaker than multiplication, suffice to obtain undecidability.

In Section 2 we study structures associated with $<_{P_2}$, where P_2 denotes the set of integers which are primes or squares of primes. Let $\perp$ be the coprimeness symbol (i.e. $x \perp y$ if and only if x and y have no common prime divisor); we show that the elementary theory of the structure $\langle \mathbb{N}; \perp, <_{P_2} \rangle$ is undecidable. This result leads, in particular, to the undecidability of $Th(\mathbb{N}; =, \times, <_\Pi)$, which answers Maurin's question. Using similar ideas, we improve a non-definability result obtained in [CMR95] for the structure $\langle \mathbb{N} \setminus \{0\}; | \rangle$. Furthermore, we prove that addition is not definable in the structure $\langle \mathbb{N}; =, \times, <_{P_2} \rangle$, and settle for every $X \subseteq \Pi$ a necessary condition for the synonymy of $\{=, \times, <_X\}$ and $\{=, \times, +\}$.

Section 3 is devoted to structures associated with $<_\Pi$. Let S denote the successor function. Up to now, it is not known whether the languages $\{\perp, S\}$ and $\{=, \times, +\}$ are synonymous. The second author specified in [Ric85] the power of expression of $\{\perp, S\}$ by showing that

every arithmetical relation restricted to the set of primary numbers is definable *(P)*

in the structure $\langle \mathbb{N}; \perp, S\rangle$. This result ensures us that $\{\perp, <_\Pi\}$ is a sublanguage of $\{\perp, S\}$. We show that it is a strict sublanguage, and that the structure $\langle \mathbb{N}; \perp, <_\Pi\rangle$ satisfies property *(P)*. Finally, it is proved that the structures $\langle \mathbb{N}; |, <_\Pi\rangle$, $\langle \mathbb{N}; =, \times, <_\Pi\rangle$ and $\langle \mathbb{N}; =, \times, +\rangle$ are interdefinable.

The following table emphasizes the relationship between some "classical" structures and the ones we investigate in the present paper; the direction of arrows corresponds to an increasing power of expression.

$$\left.\begin{array}{ccccc}
\langle \mathbb{N}; \perp, <\rangle & \rightarrow & \langle \mathbb{N}; |, <\rangle & \rightarrow & \langle \mathbb{N}; =, \times, <\rangle \\
\text{Woods [Woo81]} & & & & \\
\uparrow & & \uparrow & & \uparrow \\
\langle \mathbb{N}; \perp, S\rangle & \rightarrow & \langle \mathbb{N}; |, S\rangle & \rightarrow & \langle \mathbb{N}; =, \times, S\rangle
\end{array}\right\} \textbf{Undecidable theories}$$

$$\begin{array}{ccccc}
\text{Woods [Woo81]} & & \text{Robinson [Rob49]} & & \\
\text{Richard [Ric85]} & & & & \\
\uparrow & & \uparrow & & \uparrow \\
\langle \mathbb{N}; \perp, <_\Pi\rangle & \rightarrow & \langle \mathbb{N}; |, <_\Pi\rangle & \rightarrow & \langle \mathbb{N}; =, \times, <_\Pi\rangle \\
\uparrow & & \uparrow & & \uparrow \\
\langle \mathbb{N}; \perp, <_{P_2}\rangle & \rightarrow & \langle \mathbb{N}; |, <_{P_2}\rangle & \rightarrow & \langle \mathbb{N}; =, \times, <_{P_2}\rangle \\
 & & & & \uparrow
\end{array}$$

$$\left.\begin{array}{c}
\langle \mathbb{N}; =, \times, <_P\rangle \\
\text{Maurin [Mau95]} \\
\uparrow \\
\langle \mathbb{N}; =, \times, (\underline{n})_{n\in\mathbb{N}}\rangle
\end{array}\right\} \textbf{Decidable theories}$$

$$\text{Skolem [Sko30]}$$

Definitions and notations : Let $\mathcal{L}$ be a first-order language, not necessarily containing equality, and let $\mathcal{M}$ be a $\mathcal{L}$-structure with domain M. Recall that a n-ary relation R on M is definable in $\mathcal{M}$ if and only if there exists a first-order $\mathcal{L}$-formula φ with n free variables such that for all $a_1, \ldots, a_n \in M$, $R(a_1, \ldots, a_n)$ holds if and only if $\mathcal{M} \models \varphi[a_1, \ldots, a_n]$. The set of all relations and functions definable within $\mathcal{M}$ will be denoted by $DEF(\mathcal{M})$, and the elementary theory of $\mathcal{M}$ will be denoted by $Th(\mathcal{M})$.

Let $\mathbb{N}$ denote the set of non-negative integers, and let $S, +, \times$ respectively denote the usual operations of successor, addition and multiplication. A relation is said to be *arithmetical* if it is definable in the structure $\langle \mathbb{N}; =, +, \times\rangle$.

Let $\mathcal{L}$ and $\mathcal{L}'$ be two first-order languages, and let $\mathcal{M} = \langle \mathbb{N}; \mathcal{L} \rangle$ and $\mathcal{M}' = \langle \mathbb{N}; \mathcal{L}' \rangle$. We say that $\mathcal{L}$ is a *sublanguage* (resp. *strict sublanguage*) of $\mathcal{L}'$ if $DEF(\mathcal{M}) \subseteq DEF(\mathcal{M}')$ (resp. $DEF(\mathcal{M}) \subset DEF(\mathcal{M}')$). The languages $\mathcal{L}$ and $\mathcal{L}'$ are said to be *synonymous* if $DEF(\mathcal{M}) = DEF(\mathcal{M}')$; in this case we say that $\mathcal{M}$ and $\mathcal{M}'$ are *interdefinable*.

We say that a structure $\mathcal{M} = \langle \mathbb{N}; \mathcal{L} \rangle$ has the *Isomorphic Reinterpretation Property* if there is a structure definable in $\mathcal{M}$ and isomorphic to $\langle \mathbb{N}; =, \times, + \rangle$. If $\mathcal{M}$ satisfies such a property then $Th(\mathcal{M})$ is undecidable (see e.g. [Ric85]).

We shall use the following notations:
- P for the set of primes;
- P_n for $P \cup \{p^n : p \in P\}$ $(n \geq 2)$;
- $\pi(n)$ for the numbers of primes less or equal to n;
- π_n for the n-th prime ($\pi_0 = 2, \pi_1 = 3, \ldots$);
- $p^{\mathbb{N}}$ for the set of powers of p;
- Π for the set of primary numbers (powers of primes);
- ρ_n for the n-th primary number;
- $Supp(x)$ for the set of prime divisors of x (also called *support* of x).

Throughout the paper we shall use the following corollary of Chebychev Theorem :

Proposition 1.1. *For every integer $n \geq 2$ there exists a prime p such that $n \leq p \leq \frac{7}{5}n$.*

Proof. It is proved in [EMF75,p.23] that there exists a constant $A > 0$ such that for every integer $n \geq 30$ the following holds :

$$\frac{A \cdot n}{\log n} \leq \pi(n) \leq \frac{6}{5} \cdot \frac{A \cdot n}{\log n}$$

We can deduce from it that for every integer $n \geq 30$

$$\pi(\frac{7}{5} \cdot n) - \pi(n) \geq \frac{7}{5} \cdot \frac{A \cdot n}{\log(\frac{7}{5} \cdot n)} - \frac{6}{5} \cdot \frac{A \cdot n}{\log n}$$

$$\geq \frac{A \cdot n}{5 \cdot (\log n) \cdot (\log n + \log \frac{7}{5})}[7 \cdot \log n - 6 \cdot (\log n + \log \frac{7}{5})]$$

The previous expression is strictly positive whenever $n > (\frac{7}{5})^6$. Since $(\frac{7}{5})^6 < 30$, this proves that for every $n \geq 30$ there exists a prime p such that $n \leq p \leq \frac{7}{5}n$. The cases $n = 2, \ldots, 29$ are easily checked. ■

We first specify the expressive power of the six structures which are studied in this paper.

Proposition 1.2. *The following inclusions hold:*

$$\begin{array}{ccccc} DEF(\mathbb{N}, \perp, <_{\Pi}) & \subseteq & DEF(\mathbb{N}, |, <_{\Pi}) & \subseteq & DEF(\mathbb{N}; =, \times, <_{\Pi}) \\ \cup\!| & & \cup\!| & & \cup\!| \\ DEF(\mathbb{N}, \perp, <_{P_2}) & \subseteq & DEF(\mathbb{N}, |, <_{P_2}) & \subseteq & DEF(\mathbb{N}; =, \times, <_{P_2}) \end{array}$$

Proof. The horizontal inclusions are obvious. In order to obtain the vertical ones, it suffices to give a $\{\perp, <_{\Pi}\}$-definition of $x <_{P_2} y$ in $\mathbb{N}$. A convenient one is:

$$\neg[\exists x_1 \exists x_2 (x_1 <_\Pi x_2 \wedge x_2 <_\Pi x \wedge \neg x_1 \perp x \wedge \neg x_2 \perp x)]$$
$$\wedge \neg[\exists y_1 \exists y_2 (y_1 <_\Pi y_2 \wedge y_2 <_\Pi y \wedge \neg y_1 \perp y \wedge \neg y_2 \perp y)]$$
$$\wedge\ x <_\Pi y.$$

■

Thanks to the previous inclusions, the undecidability of $Th(\mathbb{N}, \perp, <_{P_2})$ will imply in turn the undecidability of the elementary theories of the five other structures. Moreover, Proposition 1.2 will be sharpened along the paper: we will prove (Th.3.11) that

$$DEF(\mathbb{N}, |, <_\Pi) = DEF(\mathbb{N}; =, \times, <_\Pi)$$

and all other inclusions will turn out to be strict ones (Prop.2.2.1, Th.2.3.1 and 2.3.2, Prop.3.3).

2. Structures associated with $<_{P_2}$

We first consider the "weakest" structure of Prop.1.2, namely $\langle \mathbb{N}; \perp, <_{P_2} \rangle$. Our aim is to show that this structure has the Isomorphic Reinterpretation Property, which will yield the undecidability of its elementary theory, as well as those of the five "richer" structures. For this purpose we introduce the notion of P_2*-representative* of a prime, and prove several properties related to this notion. We then define a special sequence $(q_n)_{n\geq 0}$ of primes, the elements of which will constitute the base set Q of our internal $\{\perp, <_{P_2}\}$-structure.

2.1 Some arithmetical devices

Definition 2.1.1. Let p be a prime number; we associate to p the sequence $(r_{p,n})_{n\geq 0}$ defined as follows:

$$\begin{cases} r_{p,0} = p \\ \text{For every } n \in \mathbb{N}, r_{p,n+1} = \min\{q \mid q \text{ prime and } q > r_{p,n}^2\} \end{cases}$$

The elements of this sequence will be called P_2*-representatives* of p.

Lemma 2.1.2. *For all primes p, q and all $i, j \in \mathbb{N}$, the following holds:*

(i) If $r_{p,i} > r_{q,j}$ then $r_{p,i+1} \geq r_{q,j+1}$

(ii) If $r_{p,i+1} > r_{q,j+1}$ then $r_{p,i} > r_{q,j}$

(iii) For every $n \in \mathbb{N}$, $r_{p,n}^2 < r_{p,n+1} \leq \frac{7}{5} r_{p,n}^2$

Proof. (i) and (ii) follow from the very definition, and Proposition 1.1 yields (iii). ■

We now intend to define an infinite sequence of primes such that no two of its elements have common $<_{P_2}$-representatives. In this respect, the large inequality of point (i) in the previous lemma seems to go against our wishes[1]; the following lemma shows how to overcome the difficulty.

[1] The question of whether the strict inequality holds can be stated in the following terms: does there exist a prime between the squares of two consecutive primes ? As far as we know this question is still open.

Lemma 2.1.3. *Let $m \in \mathbb{N}$, and let $p_0, p_1, \ldots, p_m$ be a set of primes such that*

$$p_0 < p_1 < \ldots < p_m$$

and no two of $p_0, p_1, \ldots, p_m$ have common P_2-representatives. There exists a prime q greater than p_m such that no two of $p_0, p_1, \ldots, p_m, q$ have common P_2-representatives.

Proof. Let $A = \{r_{p_i,j} \mid i \in \{0,1,\ldots m\}, j \in \mathbb{N}\}$ be the set of P_2-representatives of $p_0, p_1, \ldots, p_m$, and let $(s_n)_{n\in\mathbb{N}}$ be the strictly increasing sequence of elements of A.

Fact 2.1.3.1. *There exists an integer k such that $s_k \geq p_m$ and $\dfrac{s_{k+1}}{s_k} \geq 8$.*

Proof . Let $s_n = r_{p_i,j}$ be an element of A such that $s_n > \max(p_m, 8^{m+1})$, and let $s_{n'} = r_{p_i,j+1}$. By Lemma 2.1.2 (iii) we have

$$\frac{s_{n'}}{s_n} = \frac{r_{p_i,j+1}}{r_{p_i,j}} > r_{p_i,j} > 8^{m+1}.$$

If we prove that there exist at most $m+1$ elements of A between s_n and $s_{n'}$, then the fact that $\dfrac{s_{n'}}{s_n} > 8^{m+1}$ will imply the existence of an integer k such that $n \leq k < n'$ and $\dfrac{s_{k+1}}{s_k} > 8$.

Assume that there exist at least $m+2$ elements $s_{i_1} < s_{i_2} < \ldots < s_{i_{m+2}}$ of A between s_n and $s_{n'}$. Every element of A is the P_2-representative of a single prime among $p_0, p_1, \ldots, p_m$; therefore there exist at least, among the $m+2$ integers $s_{i_1}, s_{i_2}, \ldots, s_{i_{m+2}}$, two distinct elements s_{j_1}, s_{j_2} which are P_2-representatives of a single prime p_c. Assume that $s_{j_1} < s_{j_2}$. There exist $l_1, l_2 \in \mathbb{N}$ such that $s_{j_1} = r_{p_c,l_1}$ and $s_{j_2} = r_{p_c,l_2} \geq r_{p_c,l_1+1}$. We have $r_{p_i,j} < r_{p_c,l_1}$; it follows from Lemma 2.1.2 (i) that $r_{p_i,j+1} \leq r_{p_c,l_1+1} \leq s_{j_2}$, which contradicts the fact that $s_{j_2} < s_{n'}$. ☐

Let k be an integer satisfying the inequalities of Fact 2.1.3.1. By Prop.1.1 there exists a prime q such that $2s_k \leq q \leq 4s_k$.

Fact 2.1.3.2. *q has no common P_2-representative with any of the primes $p_0, p_1, \ldots, p_m$.*

Proof . We must prove that $\{s_n \mid n \in \mathbb{N}\} \cap \{r_{q,n} \mid n \in \mathbb{N}\} = \emptyset$. Let $s_k = r_{p_{i_1},j_1}$ and $s_{k+1} = r_{p_{i_2},j_2}$. Let us first show that for every $n \in \mathbb{N}$, $r_{p_{i_1},j_1+n}$ and $r_{p_{i_2},j_2+n}$ are consecutive elements of the sequence $(s_n)_{n\in\mathbb{N}}$, by induction on n :

- From the very definitions $r_{p_{i_1},j_1+0} = s_k$ and $r_{p_{i_2},j_2+0} = s_{k+1}$ are consecutive elements of $\{s_n\}_{n\in\mathbb{N}}$.
- Assume that $r_{p_{i_1},j_1+n}$ and $r_{p_{i_2},j_2+n}$ are consecutive elements of the sequence $(s_n)_{n\in\mathbb{N}}$; suppose for a contradiction that there exists x in A such that

$$r_{p_{i_1},j_1+n+1} < x < r_{p_{i_2},j_2+n+1}$$

then $x = r_{p_{i_3},j_3}$ for some $j_3 \geq 1$ (since $r_{p_{i_1},j_1+n+1} > p_m$). From Lemma 2.2 (ii) we get

$$r_{p_{i_1},j_1+n} < r_{p_{i_3},j_3-1} < r_{p_{i_2},j_2+n}$$

which contradicts the consecutivity of $r_{p_{i_1},j_1+n}$ and $r_{p_{i_2},j_2+n}$ (assumed by induction).

We shall now prove that

$$\forall\, n \in \mathbb{N} \quad r_{p_{i_1},j_1+n} < r_{q,n} < r_{p_{i_2},j_2+n} \tag{1}$$

which will ensure us, from the consecutivity of $r_{p_{i_1},j_1+n}$ and $r_{p_{i_2},j_2+n}$, that no P_2-representative of q belongs to A.

We show, by induction, that

$$\forall\, n \in \mathbb{N} \quad 2r_{p_{i_1},j_1+n} \leq r_{q,n} \leq \frac{r_{p_{i_2},j_2+n}}{2}$$

which will imply (1).
- From the very definition $2r_{p_{i_1},j_1} \leq q \leq 4r_{p_{i_1},j_1}$ and $\dfrac{r_{p_{i_2},j_2}}{r_{p_{i_1},j_1}} = \dfrac{s_{k+1}}{s_k} > 8$, hence $q \leq \dfrac{r_{p_{i_2},j_2}}{2}$.
- Assuming by induction

$$2 \cdot r_{p_{i_1},j_1+n} \leq r_{q,n} \leq \frac{r_{p_{i_2},j_2+n}}{2}$$

leads with Lemma 2.1.2 (iii) to

$$2 \cdot r_{p_{i_1},j_1+n+1} \leq 2 \cdot \frac{7}{5} \cdot r^2_{p_{i_1},j_1+n} \leq 2 \cdot \frac{7}{5} \cdot \frac{r^2_{q,n}}{4} \leq \frac{7}{10} r_{q,n+1} \leq r_{q,n+1}$$

and

$$r_{q,n+1} \leq \frac{7}{5} \cdot r^2_{q,n} \leq \frac{7}{5} \cdot \frac{1}{4} \cdot r^2_{p_{i_2},j_2+n} \leq \frac{7}{20} \cdot r_{p_{i_2},j_2+n+1} \leq \frac{r_{p_{i_2},j_2+n+1}}{2}.$$

□

This proves lemma 2.1.3. ■

Corollary 2.1.4. *We define inductively the sequence $(q_n)_{n\geq 0}$ as follows:*
- $q_0 = 2$
- *For every $n \in \mathbb{N}$, assuming $q_0, q_1, \ldots q_n$ already defined, lemma 2.1.3 allows us to set q_{n+1} as the least prime greater than q_n and without common P_2-representative with any of the primes $q_0, q_1, \ldots q_n$.*

2.2 Undecidability of $Th(\mathbb{N}, \perp, <_{P_2})$

We now come to the expressive power of $\{\perp, <_{P_2}\}$. At first, let us sharpen two inclusions of Prop.1.2.

Proposition 2.2.1. *The language $\{\perp, <_{P_2}\}$ is a strict sublanguage of arithmetic; furthermore we have*
(i) $DEF(\mathbb{N}, \perp, <_{P_2}) \subset DEF(\mathbb{N}, |, <_{P_2})$
(ii) $DEF(\mathbb{N}, \perp, <_{P_2}) \subset DEF(\mathbb{N}, \perp, <_{\Pi})$.

Proof. One can verify easily that the mapping $f : \mathbb{N} \to \mathbb{N}$ defined by

$$\begin{cases} f(2^3) = 2^4 \\ f(2^4) = 2^3 \\ f(x) = x \quad \text{otherwise} \end{cases}$$

is an automorphism of the structure $\langle \mathbb{N}; \perp, <_{P_2} \rangle$, and preserves neither division nor order on primary numbers. ■

The following definition introduces the internal structure to be defined in $\langle \mathbb{N}; \perp, <_{P_2} \rangle$.

Definition 2.2.2. Let $\langle Q; =_Q, \oplus_Q, \otimes_Q \rangle$ be the structure such that
$Q(x)$ means that $x \in \{q_n \mid n \in \mathbb{N}\}$;
$=_Q$ denotes the equality relation restricted to Q;
$z = x \oplus_Q y$ holds if and only if [*there exist $a, b \in \mathbb{N}$ such that $x = q_a$, $y = q_b$ and $z = q_{a+b}$*];

$z = x \otimes_Q y$ holds if and only if [*there exist* $a, b \in \mathbb{N}$ *such that* $x = q_a$, $y = q_b$ *and* $z = q_{a \cdot b}$].

It can be easily shown that this structure is isomorphic to $\langle \mathbb{N}; =, +, \times \rangle$. It remains to show that Q, $=_Q$, $\oplus_Q$ and $\otimes_Q$ are definable in the structure $\langle \mathbb{N}; \perp, <_{P_2} \rangle$, which will prove that this structure has the Isomorphic Reinterpretation Property.

We first define several relations which will be used throughout the paper.

Lemma 2.2.3. *The constants* $0, 1, 2$ *and the relations*
[*x is prime*] denoted by $P(x)$;

[*x is prime and $x = y$*] denoted by $EQPRIM(x, y)$;

[$p \in$ *Supp*(x)] denoted by $SUPP(p, x)$;

[*p is the least prime of Supp(x)*] denoted by $INISUPP(p, x)$;

[*p is the greatest prime of Supp(x)*] denoted by $FINSUPP(p, x)$;

[*$p \in$ Supp(x) and q is the least prime of Supp(x) greater than p*] denoted by $NEXTSUPP(p, q, x)$ *are definable in the structure* $\langle \mathbb{N}; \perp, <_{P_2} \rangle$.

Proof. Convenient definitions are the following:

$$\forall y \; x \perp y$$
for $x = 1$;

$$\forall y \; (x \perp y \Longrightarrow y = 1)$$
for $x = 0$;

$$(\exists y) \; x <_{P_2} y \wedge (\forall z) \neg z <_{P_2} x$$
for $x = 2$;

$$\exists y [x <_{P_2} y \wedge \forall z (z <_{P_2} x \Longrightarrow z \perp x)]$$
for $P(x)$;

$$P(x) \wedge (\forall z)(z <_{P_2} x \Longleftrightarrow z <_{P_2} y)$$
for $EQPRIM(x, y)$;

$$P(p) \wedge \neg p \perp x$$
for $SUPP(p, x)$;

$$SUPP(p, x) \wedge (\forall q)\big(SUPP(q, x) \Longrightarrow \neg q <_{P_2} p\big)$$
for $INISUPP(p, x)$;

$$SUPP(p, x) \wedge (\forall q)\big(SUPP(q, x) \Longrightarrow \neg p <_{P_2} q\big)$$
for $FINSUPP(p, x)$;

$$SUPP(p, x) \wedge SUPP(q, x) \wedge \neg(\exists r (p <_{P_2} r \wedge r <_{P_2} q \wedge SUPP(r, x)))$$
for $NEXTSUPP(p, q, x)$.

∎

Let us now begin to define our internal $\{\perp, <_{P_2}\}$-structure.

Lemma 2.2.4. *The relations* Q *and* $=_Q$ *are definable in* $\langle \mathbb{N}; \perp, <_{P_2} \rangle$.

Proof. We first define the relation

[*p is prime and q is the least prime greater than* p^2] denoted by $NEXTP_2REP(p,q)$, by the formula

$$\exists x[p <_{P_2} x \wedge \neg p \perp x \wedge x <_{P_2} q \wedge P(q) \wedge \neg\exists q'(x <_{P_2} q' \wedge q' <_{P_2} q \wedge P(q'))].$$

Thus we can define the relation
[*p is prime and q is a* P_2*-representative of* x] denoted by $P_2REP(p,q)$,
by the following formula

$$\exists x\Big(INISUPP(p,x) \wedge \forall q \forall q'[NEXTSUPP(q',q'',x) \Longrightarrow NEXTP_2REP(q',q'')] \wedge SUPP(q,x)\Big)$$

where the variable x corresponds to an integer the support of which contains successive P_2-representatives of the prime p.

In order to define the set $\{q_n \mid n \in \mathbb{N}\}$, we introduce the relation
[*p and q are two primes without common* P_2*-representative*] denoted by $DISTP_2REP(p,q)$ for which a suitable definition is

$$P(p) \wedge P(q) \wedge \neg(\exists r)[P_2REP(p,r) \wedge P_2REP(q,r)].$$

Now we intend to code by some y an initial segemnt I of the sequence $(q_n)_{n \geq 0}$, in such a way that I will be determined by its maximal element p. In order to do this, let us define [*There exists i such that* $p = q_i$ *and* $Supp(y) = \{q_0, q_1, \ldots q_i\}$] denoted by $COD(p,y)$.

In the defining formula for $COD(p,y)$, the "construction" of y exactly describes the inductive definition of the sequence $(q_n)_{n \geq 0}$: 2 is the least prime of $Supp(y)$, and every element of $Supp(y)$ distinct from 2 is the least prime q without any common P_2-representative with the primes of $Supp(y)$ less than q. A correct definition for $COD(p,y)$ is

$$\begin{gathered} INISUPP(2,y) \wedge \\ \forall q\{SUPP(q,y) \Longrightarrow \forall r[SUPP(r,y) \wedge r <_{P_2} q \Longrightarrow DISTP_2REP(q,r)] \wedge \\ \neg(\exists s[P(s) \wedge s <_{P_2} q \wedge \exists t\ NEXTSUPP(t,q,y) \wedge t <_{P_2} s \wedge \\ \forall u\ SUPP(u,y) \wedge u <_{P_2} s \Longrightarrow DISTP_2REP(u,s)])\} \\ \wedge\ FINSUPP(p,y). \end{gathered}$$

Now we can define $Q(x)$ by the formula

$$\exists y\ COD(x,y)$$

We immediately obtain a definition for $x =_Q y$ by the formula

$$Q(x) \wedge EQPRIM(x,y)$$

■

The following lemma introduces an auxiliary relation which will allow us to define $\oplus_Q$ and $\otimes_Q$.

Lemma 2.2.5. *The relation*
[$Supp(x) \cup Supp(y) \subset (q_n)_{n\in\mathbb{N}}$ *and* $Card(Supp(x)) = Card(Supp(y))$] *denoted by* $SUPPEQUI_Q(x,y)$ *is definable in* $\langle \mathbb{N}; \perp, <_{P_2} \rangle$.

Proof. Let x and y be two integers such that $\mathrm{Supp}(x) \cup \mathrm{Supp}(y) \subset \{q_n \mid n \in \mathbb{N}\}$. We first introduce two integers x' and y' such that

$$Supp(x') = Supp(x) \setminus Supp(y) \quad \text{and} \quad Supp(y') = Supp(y) \setminus Supp(x).$$

Obviously

$$Supp(x') \cup Supp(y') \subseteq \{q_n \mid n \in \mathbb{N}\}$$

and

$$Card(Supp(x)) = Card(Supp(y)) \quad \text{iff} \quad Card(Supp(x')) = Card(Supp(y')).$$

Now we show that the equipotence of $Supp(x')$ and $Supp(y')$ can be described within $\langle \mathbb{N}; \perp, <_{P_2} \rangle$ through the existence of an integer z such that $Supp(z) = \{r_1, \ldots, r_n\}$ and:

(i) $r_1 < r_2 < \ldots < r_n$

(ii) Every prime of $Supp(z)$ is a P_2-representative of a prime in $\mathrm{Supp}(x') \cup \mathrm{Supp}(y')$, and every prime of $\mathrm{Supp}(x') \cup \mathrm{Supp}(y')$ has a single P_2-representative in $Supp(z)$.

(iii) For every $j \in \{1, 2, \ldots, n-1\}$, if r_j is a P_2-representative of a prime in $\mathrm{Supp}(x')$ (resp $\mathrm{Supp}(y')$) then r_{j+1} is a P_2-representative of a prime in $\mathrm{Supp}(y')$ (resp $\mathrm{Supp}(x')$).

(iv) r_1 is a P_2-representative of a prime in $\mathrm{Supp}(x')$, and r_n is a P_2-representative of a prime in $\mathrm{Supp}(y')$.

Assume first that such a z exists. Recall that two distinct elements of Q don't have any common P_2-representative; it follows that every prime of $Supp(z)$ is a P_2-representative of a *single* prime in $\mathrm{Supp}(x') \cup \mathrm{Supp}(y')$. Thus condition (ii), and the fact that $\mathrm{Supp}(x')$ and $\mathrm{Supp}(y')$ are disjoint, yield $Card(Supp(z)) = Card(Supp(x')) + Card(Supp(y'))$. Then (iii) and (iv) lead to $Card(Supp(x')) = Card(Supp(y'))$.

Conversely, if $Card(Supp(x')) = Card(Supp(y')) = k$, with $Supp(x') = \{p_1, \ldots, p_k\}$ and $Supp(y') = \{p'_1, \ldots, p'_k\}$, then using the fact that every prime has infinitely many P_2-representatives, one can construct an increasing sequence of primes $r_1 < \ldots < r_{2k}$ such that for every $j \in \{1, 2, \ldots, k\}$, r_{2j-1} is a P_2-representative of p_j and r_{2j} is a P_2-representative of p'_j . Then every integer z such that $Supp(z) = \{r_1, \ldots, r_{2k}\}$ satisfies conditions (i) to (iv).

Thus $SUPPEQUI_Q(x, y)$ can be defined by the following $\{\perp, <_{P_2}\}$-formula:

$$\forall a[SUPP(a, x) \vee SUPP(a, y)] \Longrightarrow Q(a)$$

$$\wedge$$

$$\Big[\forall b(b \perp x \Longleftrightarrow b \perp y)$$

$$\vee$$

$$\exists x' \exists y' \exists z' \Big[$$

$$\forall t\{[t \perp x' \Longleftrightarrow (t \perp x \vee \neg t \perp y)] \wedge [t \perp y' \Longleftrightarrow (t \perp y \vee \neg t \perp x)]\}$$

$$\wedge$$

$$\text{translation of (ii)} \quad \begin{cases} \forall q[SUPP(q, z) \Longrightarrow \exists r\{[SUPP(r, x') \vee SUPP(r, y')] \wedge P_2REP(r, q)\}] \\ \wedge \forall s\{[SUPP(s, x') \vee SUPP(s, y')] \Longrightarrow \exists t[SUPP(t, z) \wedge P_2REP(t, s)]\} \end{cases}$$

$$\wedge$$

$$\text{translation of (iii)} \quad \begin{cases} \wedge \forall u_1 \forall u_2[NEXTSUPP(u_1, u_2, z) \Longrightarrow \exists v_1 \exists v_2 SUPP(v_1, x') \wedge SUPP(v_2, y') \\ \wedge\{[P_2REP(v_1, u_1) \wedge P_2REP(v_2, u_2)] \vee [P_2REP(v_1, u_2) \wedge P_2REP(v_2, u_1)]\} \end{cases}$$

$$\wedge$$

translation of (iv) $\left\{ \begin{array}{l} \exists r_1 \exists r_2 \exists w_1 \exists w_2 [INISUPP(r_1, z) \wedge SUPP(w_1, x') \wedge P_2REP(w_1, r_1) \\ \wedge FINSUPP(r_2, z) \wedge SUPP(w_2, y') \wedge P_2REP(w_2, r_2)]]\Big]\Bigg] \end{array} \right.$

■

Lemma 2.2.6. *The function $\oplus_Q$ is definable in the structure $\langle \mathbb{N}; \perp, <_{P_2} \rangle$.*

Proof. From $x = q_a$ and $y = q_b$ we shall characterize $z = q_{a+b}$. We begin, using the relation COD introduced in Lemma 2.2.4 , by associating to x and y two integers x' and y' such that $Supp(x') = \{q_0, \dots, q_a\}$ and $Supp(y') = \{q_0, \dots, q_b\}$. We then observe that every integer z' such that $Supp(z') = \{q_0, \dots, q_{a+b}\}$ satisfies

$$Supp(z') = Supp(x') \cup \{q_a, q_{a+1} \dots, q_{a+b}\}.$$

Thus, among integers whose support is an initial segment of $(q_n)_{n \in \mathbb{N}}$, the integers z' such that $Supp(z') = \{q_0, \dots, q_{a+b}\}$ can be characterized by the following property:

There exists $t \in \mathbb{N}$ such that

(i) $Supp(z') = Supp(x') \cup Supp(t)$

(ii) $Supp(x') \cap Supp(t) = \{q_a\}$

(iii) $Card(Supp(t)) = Card(Supp(y'))$

Conditions (i) and (ii) are easily expressible in the language $\{\perp, <_{P_2}\}$, and the relation $SUPPEQUI_Q$ which was defined in the previous lemma enables us to express the last condition. A convenient definition for $z = x \oplus_Q y$ is :

$$\exists x' \ \exists y' \ \exists z' \ \exists t \ COD(x, x') \wedge COD(y, y') \wedge COD(z, z') \wedge$$

$$\wedge \forall u \ [u \perp z' \iff (u \perp x' \wedge u \perp t)]$$

$$\wedge \forall v \ [v \perp x \iff (v \perp x' \vee v \perp t)]$$

$$\wedge SUPPEQUI(t, y').$$

■

Lemma 2.2.7 *The function $\otimes_Q$ is definable in the structure $\langle \mathbb{N}; \perp, <_{P_2} \rangle$.*

Proof. Let $x = q_a$, $y = q_b$ with $a, b \neq 0$. The integer $z = q_{a \cdot b}$ can be characterized as the greatest prime divisor of an integer u which satisfies the two following conditions :

(i) $Supp(u)$ has the form $\{q_0, q_a, q_{2 \cdot a}, \dots, q_{n \cdot a}\}$ for some $n \in \mathbb{N}$.

(ii) $Card(Supp(u)) = Card(\{q_0, q_1, q_2, \dots, q_b\})$.

Using $\oplus_Q$ and $SUPPEQUI_Q$, one can express these two conditions in the language $\{\perp, <_{P_2}\}$; a suitable definition for $z = x \otimes_Q y$ is

$$Q(x) \wedge Q(y) \wedge \exists t \exists u \{$$

$$COD(y, t) \wedge INISUPP(2, u)$$

$$\wedge \forall p_1 \forall p_2 [NEXTSUPP(p_1, p_2, u) \Longrightarrow p_2 = p_1 \oplus_Q x]$$

$$\wedge SUPPEQUI_Q(t,u)\}.$$

■

Lemmas 2.2.4 , 2.2.6 and 2.2.7 directly yield

Proposition 2.2.8. *The structure $\langle \mathbb{N}; \perp, <_{P_2}\rangle$ has the Isomorphic Reinterpretation Property.*

From Prop.1.2 and the previous proposition we get:

Theorem 2.2.9. *The elementary theories of $\langle \mathbb{N}; \perp, <_{P_2}\rangle$, $\langle \mathbb{N}; |, <_{P_2}\rangle$, $\langle \mathbb{N}; =, \times, <_{P_2}\rangle$, $\langle \mathbb{N}; \perp, <_{\Pi}\rangle$, $\langle \mathbb{N}; |, <_{\Pi}\rangle$ and $\langle \mathbb{N}; =, \times, <_{\Pi}\rangle$ are undecidable.*

Replacing each "P_2 notion" by the corresponding "P_n notion", the undecidability of $\mathrm{Th}(\mathbb{N}; \perp, <_{P_2})$ can be generalized in the following way:

Theorem 2.2.10. *For every $n \geq 2$ the elementary theory of $\langle \mathbb{N}; \perp, <_{P_n}\rangle$ is undecidable.*

As an interlude, we now consider a definability question for which the previous construction can be used in an efficient way. Consider the binary relation $SUPPEQUI(x,y)$ which holds if and only if $[Card(Supp(x)) = Card(Supp(y))]$. In [CMR95], the authors prove that $SUPPEQUI$ is not definable in the structure $\langle \mathbb{N} \setminus \{0\}; |\rangle$. This result can be strengthened as follows:

Proposition 2.2.11. *The relation $SUPPEQUI$ is not definable in the structure $\langle \mathbb{N} \setminus \{0\}; =, \times, <_P\rangle$.*

Proof. Assume for a contradiction that $SUPPEQUI$ is definable in the structure $\langle \mathbb{N} \setminus \{0\}; =, \times, <_P\rangle$. Now consider the structure $\langle P; =_P, \otimes_P, \oplus_P\rangle$ where
$P(x)$ means [*x is a prime number*]
$=_P$ denotes the equality relation restricted to primes
$z = x \oplus_P y$ means [$x = \pi_a$, $y = \pi_b$ *and* $z = \pi_{a+b}$ *for some* $a, b \in \mathbb{N}$]
$z = x \otimes_P y$ means [$x = \pi_a$, $y = \pi_b$ *and* $z = \pi_{a \cdot b}$ *for some* $a, b \in \mathbb{N}$]

This structure is clearly isomorphic to $\langle \mathbb{N}; =, \times, +\rangle$. The predicates P and $=_P$ are easily definable in $\langle \mathbb{N} \setminus \{0\}; =, \times, <_P\rangle$. Using previous ideas, one can define $\oplus_P$ and $\otimes_P$ from $SUPPEQUI$. It follows that $\langle \mathbb{N} \setminus \{0\}; =, \times, <_P\rangle$ has the Isomorphic Reinterpretation Property, which contradicts the decidability of its elementary theory [Mau95]. ■

2.3 Non-definability within $\langle \mathbb{N}; |, <_{P_2}\rangle$ and $\langle \mathbb{N}; =, \times, <_{P_2}\rangle$

By virtue of Theorem 2.2.9 the elementary theories of $\langle \mathbb{N}; |, <_{P_2}\rangle$ and $\langle \mathbb{N}; =, \times, <_{P_2}\rangle$ are undecidable. We now specify the limits of the expressive power of these two structures.

Theorem 2.3.1. *Multiplication is not definable in the structure $\langle \mathbb{N}; |, <_{P_2}\rangle$.*

Proof. Let $\mathcal{M}$ be a non-standard model of PA. Due to the fact that $|$ and $<_{P_2}$ are arithmetical relations, we can look at $\mathcal{M}$ as a model of $\mathrm{Th}(\mathbb{N}; |, <_{P_2})$. Now consider the mapping $f : |\mathcal{M}| \to |\mathcal{M}|$ defined by

$$\begin{cases} f(0) = 0 \\ f(2^a \cdot b) = 2^a \cdot b \ \text{ for all } \ a \in \mathbb{N} \ , \ b \perp 2 \\ f(2^a \cdot b) = 2^{a-1} \cdot b \ \text{ for all } \ a \notin \mathbb{N} \ , \ b \perp 2 \end{cases}$$

f is 1-1 and preserves $|$ and $<_{P_2}$. However f does not preserve multiplication, since if $x = 2^a$ with a non-standard, then $f(x^2) = 2^{2 \cdot a - 1} \neq f^2(x)$. ■

Theorem 2.3.2. *Addition is not definable in the structure* $\langle \mathbb{N}; =, \times, <_{P_2} \rangle$.

Proof. Let $<_{P_2'}$ denote the order restricted to $P_2' = P_2 \setminus \{2, 3, 2^2\}$, and let $\bullet$ denote the graph of multiplication. It is easily seen that the structures $\langle \mathbb{N}; =, \times, <_{P_2} \rangle$ and $\langle \mathbb{N}; \bullet, <_{P_2'} \rangle$ are interdefinable. Assume for a contradiction that addition is definable in the former structure; it is definable in the latter too. In this case all arithmetical sets are definable in $\langle \mathbb{N}; \bullet, <_{P_2'} \rangle$; in particular, the set $A = \{2^{n^2} : n \in \mathbb{N}\}$ is definable in this structure. Our aim is to show that A is actually definable in the structure $\langle \mathbb{N}; \bullet, \{\underline{n}\}_{n \in \mathbb{N}} \rangle$, which will lead to a contradiction (to be precised below).

Let V_2 and $\tilde{V_2}$ be the mappings on $\mathbb{N}$ defined as follows:
- $V_2(0) = \tilde{V_2}(0) = 0$
- For every integer $x \neq 0$, $V_2(x)$ is the greatest power of 2 which divides x, and $\tilde{V_2}(x) = \dfrac{x}{V_2(x)}$.

The functions V_2 and $\tilde{V_2}$ are definable in $\langle \mathbb{N}; \bullet, <_{P_2'} \rangle$ in the following way:

$$(x = 0 \wedge y = 0) \vee \{x \neq 0 \wedge \exists t[x = t \bullet y \wedge \neg SUPP(2, y) \wedge \forall p SUPP(p, t) \Longrightarrow EQPRIM(p, 2)]\}$$

$$\text{for } \ y = \tilde{V_2}(x);$$

$$(x = 0 \wedge y = 0) \vee \exists z (z = \tilde{V_2}(x) \wedge x = y \bullet z)$$

$$\text{for } \ y = V_2(x);$$

The constant 2 is definable in $\langle \mathbb{N}; \bullet, \{\underline{n}\}_{n \in \mathbb{N}} \rangle$; therefore V_2 and $\tilde{V_2}$ are definable in $\langle \mathbb{N}; \bullet, \{\underline{n}\}_{n \in \mathbb{N}} \rangle$ too.

We shall work within the structure $\mathcal{N} = \langle \mathbb{N}; \bullet, <_{P_2'}, V_2, \tilde{V_2}, 0, 1 \rangle$, and proceed to transform the $\{\bullet, <_{P_2'}\}$-formula $\phi(x)$ defining A into a logically equivalent $\{\bullet, <_{P_2'}, V_2, \tilde{V_2}, 0, 1\}$-formula $\psi(x)$ having adequate syntaxical properties. We do this in several steps.

First observe that from the above definitions, for every $t, u, v \in \mathbb{N}$ the following holds:

$$\mathcal{N} \models \ t = u \bullet v \Longleftrightarrow [V_2(t) = V_2(u) \bullet V_2(v) \wedge \tilde{V_2}(t) = \tilde{V_2}(u) \bullet \tilde{V_2}(v)] \tag{1}$$

Furthermore, since no multiple of 2 belongs to P_2', we have:

$$\mathcal{N} \models \ t <_{P_2'} u \Longleftrightarrow [V_2(t) = 1 \wedge V_2(u) = 1 \wedge \tilde{V_2}(t) <_{P_2'} \tilde{V_2}(u)] \tag{2}$$

Using these two facts, we construct the formula $\phi_1(x)$ from $\phi(x)$ by replacing each atomic formula of $\phi(x)$ having the form $t = u \bullet v$ (respectively $t <_{P_2'} u$) by the right member of equivalence (1) (respectively (2)). Obviously ϕ and ϕ_1 are equivalent formulas. Besides, every variable y of ϕ_1 occurs only in the form $V_2(y)$ or $\tilde{V_2}(y)$.

Now, if x is a power of 2, then $\tilde{V_2}(x) = 1$ and $x = V_2(x)$. Since $\phi_1(x)$ defines A which is a subset of $2^{\mathbb{N}}$, we can "relativize" $\phi_1(x)$ to $2^{\mathbb{N}}$ by replacing each term $V_2(x)$ (respectively $\tilde{V_2}(x)$) by x (respectively 1). Doing this we obtain a formula $\phi_2(x)$ which is equivalent to $\phi_1(x)$. In $\phi_2(x)$ can be distinguished two groups of terms, the first one consisting of x and all terms $V_2(y)$ (y variable), the second one of all terms $\tilde{V_2}(y)$ (y variable). Terms of the first group do not occur in atomic formulas involving $<_{P_2'}$, and in each atomic formula all terms belong to the same group.

Assume that $\phi_2(x)$ is in prenex form, say

$$\phi_2(x) \equiv Q_1 y_1 \dots Q_n y_n \ \theta(x, y_1, \dots, y_n)$$

(the Q_i's are quantifiers,θ is a formula without quantifier). The next transformation consists in splitting gradually each variable y_i in two new variables y_i^1 and y_i^2, in such a way that y_i^1 and y_i^2 respectively correspond to $V_2(y_i)$ and $\tilde{V}_2(y_i)$.

Let us consider the formula $\varphi_n(x, y_1, \dots, y_{n-1}) \equiv Q_n y_n \theta(x, y_1, \dots, y_n)$. Assume first that Q_n is $\exists$. We define the formula

$$\varphi_n^\star(x, y_1, \dots, y_{n-1}) \equiv \exists y_n^1 \exists y_n^2 \{[(y_n^1 = 0 \wedge y_n^2 = 0) \vee (\tilde{V}_2(y_n^1) = 1 \wedge V_2(y_n^2) = 1] \wedge$$
$$\theta_n^\star(x, y_1, y_2, \dots, y_{n-1}, y_n^1, y_n^2)\}$$

where $\theta_n^\star$ is obtained from θ_n by replacing each term $V_2(y_n)$ (respectively $\tilde{V}_2(y_n)$) by y_n^1 (resp. y_n^2).

Let us prove that φ_n and $\varphi_n^\star$ are equivalent. Fix the n-tuple $(x, y_1, \dots, y_{n-1})$, and suppose that $\varphi_n(x, y_1, \dots, y_{n-1})$ holds in $\mathcal{N}$; by assumption on Q_n there exists y_n such that $\theta(x, y_1, \dots, y_n)$ holds in $\mathcal{N}$ too. Then if we set $y_n^1 = V_2(y_n)$ and $y_n^2 = \tilde{V}_2(y_n)$, $\theta_n^\star(x, y_1, y_2, \dots, y_{n-1}, y_n^1, y_n^2)\}$ holds in $\mathcal{N}$, hence $\mathcal{N} \models \varphi_n^\star(x, y_1, \dots, y_{n-1})$. For the converse, assume that there exists y_n^1 and y_n^2 such that

$$\mathcal{N} \models [(y_n^1 = 0 \wedge y_n^2 = 0) \vee (\tilde{V}_2(y_n^1) = 1 \wedge V_2(y_n^2) = 1] \wedge$$
$$\theta_n^\star(x, y_1, y_2, \dots, y_{n-1}, y_n^1, y_n^2) \tag{3}$$

Then if we set $y_n = y_n^1 \cdot y_n^2$, the conditions imposed on y_n^1 and y_n^2 by the subformula in brackets in (3) ensure that $y_n^1 = V_2(y_n)$ and $y_n^2 = \tilde{V}_2(y_n)$, which yields $\mathcal{N} \models \theta(x, y_1, \dots, y_n)$. Thus φ_n and $\varphi_n^\star$ are equivalent. In the case where Q_n is $\forall$, we use the classical equivalence

$$\forall y_n \theta(x, y_1, \dots, y_n) \Longleftrightarrow \neg \exists y_n \neg \theta(x, y_1, \dots, y_n)$$

and apply the transformation to

$$\exists y_n \neg \theta(x, y_1, \dots, y_n).$$

For $i = n-1, n-2, \dots, 1$ we repeat this process with $\varphi_i(x, y_1, \dots, y_{i-1}) \equiv Q_i y_i \varphi_{i+1}^\star(x, y_1, \dots, y_i)$, and finally obtain a formula

$$\varphi_1(x) \equiv Q_1 y_1^1 Q_1 y_1^2 \dots Q_n y_n^1 Q_n y_n^2 \ \theta_1^\star(x, y_1^1, y_1^2, \dots, y_n^1, y_n^2)$$

which is equivalent with $\varphi_2(x)$.

From the two groups of terms in $\varphi_2(x)$ we obtain two groups of variables in $\varphi_1(x)$: the first one is formed with x and all y_i^1 $(i = 1, \dots, n)$; variables of this group do not occur in atomic formulas involving $<_{P_2'}$. The second group consists of all variables y_i^2 $(i = 1, \dots, n)$. Once again, in each atomic formula of $\varphi_1(x)$ occur variables of only one group. This property enables us to distribute the quantifiers of $\varphi_1(x)$, in such a way that we obtain a formula $\psi(x)$ (logically equivalent with $\varphi_1(x)$) which is a disjunction of conjunction of formulas which can be either close formulas (in which occur variables of a same group), or formulas with x as unique free variable and only involving variables of the first group. Denote by $F_i(x)$ $(i = 1, \dots, k)$ the formulas only involving variables of the first group. Now the close subformulas of $\Psi(x)$ are equivalent either to $0 = 0$ or $0 = 1$; therefore there exists a formula $\beta(x)$ equivalent with $\psi(x)$, and such that its subformulas are the $F_i(x)$'s $(i = 1, \dots, k)$ and maybe subformulas of the form $0 = 0$ or $0 = 1$.

Now the $F_i(x)$'s only involve variables of the first group, which do not occur in atomic formulas involving $<_{P_2'}$. Thus $\beta(x)$ is a $\{\bullet, V_2, \tilde{V}_2, 0, 1\}$-formula. Since V_2 and $\tilde{V}_2$ were proved to be definable in $\langle \mathbb{N}; \bullet, \{\underline{n}\}_{n\in\mathbb{N}}\rangle$, there exists a $\{\bullet, \{\underline{n}\}_{n\in\mathbb{N}}\}$-formula $\lambda(x)$ which is equivalent to $\beta(x)$. All of our syntactical transformations preserving logical equivalence, $\lambda(x)$ defines the set A. Therefore we proved that the set $\{2^{n^2} : n \in \mathbb{N}\}$ is definable in $\langle \mathbb{N}; \bullet, \{\underline{n}\}_{n\in\mathbb{N}}\rangle$. Consider the structure $\langle 2^{\mathbb{N}}; =_{[2]}, TIMES_2, \lambda\rangle$ where $=_{[2]}$ and $TIMES_2$ respectively denote equality relation and multiplication function restricted to $2^{\mathbb{N}}$. This structure is easily definable in $\langle \mathbb{N}; \bullet, \{\underline{n}\}_{n\in\mathbb{N}}\rangle$, and is isomorphic with $\langle \mathbb{N}; =, +, Sq\rangle$ where Sq denotes the unary relation that defines the set of squares. The elementary theory of the latter structure was shown to be undecidable ([Put57]). This implies that Th$(\mathbb{N}; \bullet, \{\underline{n}\}_{n\in\mathbb{N}})$ is undecidable too, which contradicts the classical result of Skolem ([Sko30]). ■

The previous result can be generalized in the following way.

Theorem 2.3.3. *Let $X \subset \Pi$ be a subset satisfying the following property:*
There exist a prime p such that only a finite number of powers of p belong to X.
Then addition is not definable in the structure $\langle \mathbb{N}; =, \times, <_X\rangle$.

Proof. The previous proof can be used with slight modifications. Let q be the least element of X such that no power of p greater than q belongs to X. Consider the set

$$X' = \{x : x \in X \wedge x \geq q\},$$

and the structure

$$\mathcal{N}' = \langle \mathbb{N}; \bullet, <_{X'}, V_p, \tilde{V_p}, 0, 1, \{\underline{c}\}_{c\in C}\rangle$$

where $C = X \setminus X'$. This time $\langle \mathbb{N}; =, X, <_X\rangle$ and $\mathcal{N}'$ are not necessarily interdefinable: for instance, if $X \cap p^{\mathbb{N}} = \emptyset$ and if furthermore there exists another prime p' such that $X \cap p'^{\mathbb{N}} = \emptyset$ then using an automorphism argument one can prove that the constant $\underline{p}$ (and *a fortiori* V_p and $\tilde{V_p}$) is not definable in $\langle \mathbb{N}; =, X, <_X\rangle$. However by an explicit extension of $<_{X'}$, it is easily checked that $\mathcal{N}'$ is at least as expressive as $\langle \mathbb{N}; =, X, <_X\rangle$. Using the same method one proves that the definability in $\mathcal{N}'$ of the set $A' = \{p^{n^2} \mid n \in \mathbb{N}\}$ leads to a contradiction. ■

3. Structures associated with $<_\Pi$

We first review some results connected to the coprimeness predicate. In [Rob49], J.Robinson proved the equality between $DEF(\mathbb{N}; |, S)$ and $DEF(\mathbb{N}; =, \times, +)$, and asked whether the languages $\{\perp, S\}$ and $\{=, \times, +\}$ are synonymous. This question is still open. A.R.Woods proved in [Woo81] the equality $DEF(\mathbb{N}; \perp, <) = DEF(\mathbb{N}; =, \times, +)$, and provided a partial answer to Robinson's question by showing that

(i) Th$(\mathbb{N}; \perp, S)$ is undecidable.

(ii) The synonymy of $\{\perp, S\}$ and $\{=, \times, +\}$ is equivalent to the following statement (usually called *Erdös-Woods conjecture*):
there exists an integer k such that for all integers x, y:

$$x = y \iff [Supp(x+i) = Supp(y+i) \quad \text{for} \quad i = 0, 1, \ldots, k]$$

In [Ric85], the second author of the present paper gave another proof of undecidability of Th $(\mathbb{N}; \perp, S)$ and specified the expressive power of $\{\perp, S\}$ by showing that every arithmetical relation restricted to Π is definable in $\langle \mathbb{N}; \perp, S\rangle$; moreover, it was proved that the languages

$\{\perp, S, EXP_p\}$ (where EXP_p denotes the function $x \mapsto p^x$ for any fixed prime x) and $\{=, \times, +\}$ are synonymous.

The following theorem states several arguments of [Ric85] which we shall use in the sequel.

Theorem 3.1 (Richard). *let $\mathcal{M} = \langle \mathbb{N}; \mathcal{L} \rangle$ be a first-order $\mathcal{L}$-structure which satisfies the property:*

(i) There exists a prime p such that the structure $\langle p^{\mathbb{N}}; =_{[p]}, \otimes_p, \oplus_p \rangle$, where
$=_{[p]}$ denotes the equality relation restricted to $p^{\mathbb{N}}$,
$z = x \otimes_p y$ means $[x = p^a,\ y = p^b$ and $z = p^{a \cdot b}$ for some $a, b \in \mathbb{N}]$, and
$z = x \oplus_p y$ means $[x = p^a,\ y = p^b$ and $z = p^{a+b}$ for some $a, b \in \mathbb{N}]$,

is definable in $\mathcal{M}$. Then the following holds:

(a) if the mapping $f : x \mapsto p^x$ with domain Π is definable in $\mathcal{M}$ then for every arithmetical set $X \subseteq \mathbb{N}^k$ the set $X_\Pi = X \cap \Pi^k$ is definable in $\mathcal{M}$.

(b) if the mapping $g : x \mapsto p^x$ with domain $\mathbb{N}$ is definable in $\mathcal{M}$ then

$$DEF(\mathcal{M}) = DEF(\mathbb{N}; =, \times, +)$$

(in this case we say that $\mathcal{M}$ has the Definable Isomorphic Reinterpretation Property).

We prove below that the structure $\langle \mathbb{N}; \perp, <_\Pi \rangle$ satisfies (i) and (a) for $p = 2$. Furthermore, it is shown that $\langle \mathbb{N}; |, <_\Pi \rangle$ satisfies (b) in addition, as well as $\langle \mathbb{N}; =, \times, <_\Pi \rangle$.

Let us start with $\langle \mathbb{N}; \perp, <_\Pi \rangle$. First observe that in the previous section, the key-argument in the construction of the internal structure $\langle Q; =_Q, \otimes_Q, \oplus_Q \rangle$ was the ability to define the relation $SUPPEQUI_Q(x, y)$ which means
$[Supp(x) \cup Supp(y) \subset \{q_n\}_{n \in \mathbb{N}}$ and $Card(Supp(x)) = Card(Supp(y))$].
Using this predicate, we could obtain, from two integers with respective support $\{q_0, q_1, \ldots, q_a\}$ and $\{q_0, q_1, \ldots, q_b\}$, an integer with support $\{q_0, q_1, \ldots, q_{a+b}\}$, and thus define $\oplus_Q$, which in turn led us quite easily to a definition for $\otimes_Q$.

We shall use similar arguments to prove that $\langle \mathbb{N}; \perp, <_\Pi \rangle$ satisfies property (i) of Th.3.1. Let φ be the mapping with domain Π which maps every primary number x to the least prime number greater than x. Fix a prime number p, and consider two powers of p, p^a and p^b. Encoding p^a and p^b by two integers with respective support $\{\varphi(p), \varphi(p^2), \ldots, \varphi(p^a)\}$ and $\{\varphi(p), \varphi(p^2), \ldots, \varphi(p^b)\}$, the characterization of integers that have $\{\varphi(p), \varphi(p^2), \ldots, \varphi(p^{a+b})\}$ for support will rely on the definability in $\langle \mathbb{N}; \perp, <_\Pi \rangle$ of the relation
$[Supp(x) \cup Supp(y) \subset \{\phi(p^n) \mid n \geq 1\}$ and $Card(Supp(x)) = Card(Supp(y))]$
denoted by $SUPPEQUI_\Pi(x, y, p)$.

In order to define this predicate, we need a new notion of representative.

Definition 3.2. let p be a prime number. For every integer i we call *p-representative* of $\varphi(p^i)$ every integer of the form $\varphi(p^{(2i+1) \cdot 2^j})$ $(j \in \mathbb{N})$.

Every $\varphi(p^i)$ has infinitely many p-representatives; furthermore if $i_1 \neq i_2$ then $\varphi(p^{i_1})$ and $\varphi(p^{i_2})$ have no common p-representative, since for all $a, a', b, b' \in \mathbb{N}$, $p^{(2a+1) \cdot 2^b} = p^{(2a'+1) \cdot 2^{b'}}$ implies $(a = a'$ and $b = b')$. These remark ensure us that our notion is convenient.

Let F be a formula with n free variables. In the sequel we will use the notation

$$y = \min_{\Pi}\{t : F(t, x_2, \ldots, x_n)\}$$

as an abbreviation for the formula

$$\exists z \; y <_\Pi z \wedge F(y, x_2, \ldots, x_n) \wedge \forall t\{[F(t, x_2, \ldots, x_n) \wedge \exists z'(t <_\Pi z')] \Longrightarrow \neg t <_\Pi y\}.$$

Proposition 3.3. *The following inclusions hold:*
(i) $DEF(\mathbb{N}, \perp, <_\Pi) \subset DEF(\mathbb{N}, \perp, S)$
(ii) $DEF(\mathbb{N}, \perp, <_\Pi) \subset DEF(\mathbb{N}, |, <_\Pi)$.

Proof. Since every arithmetical relation restricted to Π is definable in $\langle \mathbb{N}, \perp, S\rangle$, the relation $<_\Pi$ is definable in this structure, which yields $DEF(\mathbb{N}, \perp, <_\Pi) \subseteq DEF(\mathbb{N}, \perp, S)$. Now consider the mapping $h : \mathbb{N} \mapsto \mathbb{N}$ which only permute 6 and 12. Clearly h is an automorphism of $\langle \mathbb{N}, \perp, <_\Pi\rangle$; however h preserves neither S nor $|$. ∎

Lemma 3.4. *The relations*
$=_\Pi$ *which denotes the equality relation restricted to* Π*;*

[p is prime and x is a power of p] denoted by $POW(x, p)$*;*

[there exists a prime p and an integer a such that $x = p^a$ and $y = p^{a+1}$] denoted by $NEXTPOW(x, y)$*;*

the function $\phi : \Pi \to \mathbb{N}$ which maps every primary number x to the least prime greater than x;

and the relation
[there exists a prime p and an integer $a \geq 1$ such that $x = p^a$ and $Supp(y) = \{\phi(p), \phi(p^2), \ldots, \phi(x)\}$] denoted by $\Pi COD(x, y)$

are definable in the structure $\langle \mathbb{N}; \perp, <_\Pi\rangle$.

Proof. Convenient definitions are the following:

$$\exists z(x <_\Pi z) \wedge \forall t(x <_\Pi t \Longleftrightarrow y <_\Pi t)$$
for $x =_\Pi y$;

$$P(p) \wedge (x =_\Pi p \vee p <_\Pi x)$$
for $POW(x, p)$;

$$x <_\Pi y \wedge y = \min_\Pi\{t : x <_\Pi t \wedge \neg x \perp t\}$$
for $NEXTPOW(x, y)$;

$$P(y) \wedge y = \min_\Pi\{t : P(t) \wedge (x =_\Pi t \vee x <_\Pi t)\}$$
for $y = \varphi(x)$;

$$\begin{gathered}\exists p[POW(x,p) \wedge INISUPP(p,y) \wedge FINSUPP(\varphi(x), y) \wedge \\ \forall p \forall q\{NEXTSUPP(q, q', y) \Longrightarrow [\exists r \exists r' POW(r, p) \wedge \\ NEXTPOW(r, r') \wedge q =_\Pi \varphi(r) \wedge q' =_\Pi \varphi(r')]\}]\end{gathered}$$
for $\Pi COD(x, y)$.

∎

Lemma 3.5. *The ternary relation*
[p is prime and there exists $a \geq 1, b \geq 0$ such that $x = \phi(p^a)$ and $y = \phi(p^{(2a+1)\cdot 2^b})$] denoted by $\Pi REP(x, y, p)$*, is definable in the structure* $\langle \mathbb{N}; \perp, <_\Pi\rangle$.

Proof. We first observe that for every $a \geq 1$, by Prop.1.1 we have

$$p^a < \phi(p^a) \leq \frac{7}{5} \cdot p^a$$

which implies

$$p^{2a} < [\phi(p^a)]^2 \leq \frac{49}{25} \cdot p^{2a} \leq p^{2a+1}.$$

Thus p^{2a} can be characterized as the greatest power of p less than $[\phi(p^a)]^2$. This remark enables us to define the relation

[*p is prime and there exists* $a \geq 1$ *such that* $x = \phi(p^a)$ *and* $y = \phi(p^{2a})$]

denoted by $\Pi SQ(x, y, p)$, by the formula

$$\exists q \exists r \exists q' \{POW(q, p) \wedge POW(q', p) \wedge x =_\Pi \phi(q) \wedge NEXTPOW(\phi(q), r) \wedge$$

$$\wedge \exists s[NEXTPOW(q', s) \wedge q' <_\Pi r \wedge r <_\Pi s] \wedge y =_\Pi \phi(q')\}.$$

From this predicate we define $JUMP(x, y, p)$ which means

[*p is prime and there exists* $a \geq 1$ *such that* $x = \varphi(p^a)$ *and* $y = \varphi(p^{2 \cdot a+1})$]

by the formula

$$\exists z \exists q \exists q'[POW(q, p) \wedge \Pi SQ(x, z, p) \wedge z =_\Pi \varphi(q) \wedge NEXTPOW(q, q') \wedge y =_\Pi \varphi(q')].$$

Now we are able to define $\Pi REP(x, y, p)$ by observing that there exist $a \geq 1$,$b \geq 0$ such that $x = \phi(p^a)$ and $y = \phi(p^{(2a+1) \cdot 2^b})$ if and only if there exists an integer z the support of which satisfies

$$Supp(z) = \{\phi(p^{2a+1}), \phi(p^{(2a+1) \cdot 2}), \phi(p^{(2a+1) \cdot 2^2}), \ldots, y\}$$

Therefore a suitable formula for $\Pi REP(x, y, p)$ is

$$\exists t \exists z \{JUMP(x, p, t) \wedge INISUPP(t, z) \wedge FINSUPP(y, z) \wedge$$

$$\forall q \forall q'[NEXTSUPP(q, q', z) \Longrightarrow \Pi SQ(q, q', p)]\}.$$

■

Lemma 3.6. *The relation*

[$Supp(x) \cup Supp(y) \subset \{\phi(p^n) : n \geq 1\}$ *and* $Card(Supp(x)) = Card(Supp(y))$],

denoted by $SUPPEQUI_\Pi(x, y, p)$*, is definable in* $\langle \mathbb{N}; \perp, <_\Pi \rangle$.

Proof. We use the same arguments as in the proof of Lemma 2.2.5. Let p be a prime number, and let x and y be two integers such that

$$Supp(x) \cup Supp(y) \subset \{\phi(p^n) \mid n \geq 1\}.$$

In the defining formula for $SUPPEQUI_\Pi(x, y, p)$ we use two integers x' and y' such that $Supp(x') = Supp(x) \setminus Supp(y)$ and $Supp(y') = Supp(y) \setminus Supp(x)$. Then we can describe the equipotence of $Supp(x')$ and $Supp(y')$ through the existence of an integer z which satisfies conditions (i) to (iv) of Lemma 2.2.5 , where "P_2-representative" is replaced by "p-representative ".

Finally a suitable formula for $SUPPEQUI_\Pi(x, y, p)$ is

$$\forall a[SUPP(a, x) \vee SUPP(a, y)] \Longrightarrow Q(a)$$

$$\wedge$$

$$\Bigg[\forall b(b\perp x \iff b\perp y)$$

$$\vee$$

$$\exists x'\exists y'\exists z'\Bigg[$$

$$\forall t\{[t\perp x' \iff (t\perp x \vee \neg t\perp y)] \wedge [t\perp y' \iff (t\perp y \vee \neg t\perp x)]\}$$

$$\wedge$$

$$\text{translation of (ii)} \quad \begin{cases} \forall q[SUPP(q,z) \Longrightarrow \exists r\{[SUPP(r,x') \vee SUPP(r,y')] \wedge \Pi REP(r,q)\}] \\ \wedge\forall s\{[SUPP(s,x') \vee SUPP(s,y')] \Longrightarrow \exists t[SUPP(t,z) \wedge \Pi REP(t,s)]\} \end{cases}$$

$$\wedge$$

$$\text{translation of (iii)} \quad \begin{cases} \wedge\forall u_1\forall u_2[NEXTSUPP(u_1,u_2,z) \Longrightarrow \exists v_1\exists v_2 SUPP(v_1,x') \wedge SUPP(v_2,y') \\ \quad \wedge\{[\Pi REP(v_1,u_1) \wedge \Pi REP(v_2,u_2)] \vee [\Pi REP(v_1,u_2) \wedge \Pi REP(v_2,u_1)]\} \end{cases}$$

$$\wedge$$

$$\text{translation of (iv)} \quad \begin{cases} \exists r_1\exists r_2\exists w_1\exists w_2[INISUPP(r_1,z) \wedge SUPP(w_1,x') \wedge \Pi REP(w_1,r_1) \\ \qquad \wedge FINSUPP(r_2,z) \wedge SUPP(w_2,y') \wedge \Pi REP(w_2,r_2)]\Bigg]\Bigg] \end{cases}$$

■

Lemma 3.7. *The relation*
[*x and y are powers of the same prime and $z = x \cdot y$*]
denoted by $MULT\Pi(x,y)$, is definable in $\langle \mathbb{N}; \perp, <_\Pi\rangle$.

Proof. The arguments used below are very close to those for Lemma 2.2.6 . Let p be a prime, and let $x = p^a$, $y = p^b$, with a and b different from 0. Using the relation ΠCOD previously introduced, we associate to x and y two integers x' and y' such that $Supp(x') = \{\phi(p), \phi(p^2), \ldots, \phi(p^a)\}$ and $Supp(y') = \{\phi(p), \phi(p^2), \ldots, \phi(p^b)\}$. Now, among integers whose support is of the form $\{\phi(p), \phi(p^2), \ldots, \phi(p^i)\}$, the integers z' whose greatest prime divisor is $\phi(p^{a+b})$ can be characterized by the following property:

There exists $t \in \mathbb{N}$ such that

(i) $Supp(z') = Supp(x') \cup Supp(t)$

(ii) $Supp(x') \cap Supp(t) = \emptyset$

(iii) $Card(Supp(t)) = Card(Supp(y'))$

These conditions are expressible in the structure $\langle \mathbb{N}; \perp, <_\Pi\rangle$, and a convenient $\{\perp, <_\Pi\}$-definition for for $MULT\Pi(x,y,z)$ is

$$\exists p[POW(x,p) \wedge POW(y,p)] \wedge [x = 1 \Longrightarrow z = y] \wedge [y = 1 \Longrightarrow z = x]$$

$$\wedge(\neg x = 1 \wedge \neg y = 1) \Longrightarrow$$

$$\big[\exists x'\exists y'\exists z'\exists t[\Pi COD(x,x') \wedge \Pi COD(y,y') \wedge \Pi COD(z,z') \wedge$$

$$\forall u\ [u\perp z' \iff (u\perp x' \ \wedge\ u\perp t)]$$

$$\wedge x'\perp t \wedge SUPPEQUI_\Pi(t,y')\big].$$

■

Lemma 3.8. *The relation*

[*There exist a prime* p *and* $a, b \in \mathbb{N}$ *such that* $x = p^a$, $y = p^b$ *and* $z = p^{a \cdot b}$]
denoted by $EXP\Pi(x, y, z)$, *is definable in* $\langle \mathbb{N}; \perp, <_\Pi \rangle$.

Proof. The defining formula rests on the following fact: let $x = p^a$, $y = p^b$ for a prime p and $a, b \geq 1$. The integer $z = p^{a \cdot b}$ can be characterized as the greatest prime divisor of an integer t the support of which has the form $\{\varphi(p^a), \varphi(p^{2 \cdot a}), \ldots, \varphi(p^{n \cdot a})\}$ and

$$Card(Supp(t)) = Card(\{\varphi(p), \varphi(p^2), \ldots, \varphi(p^b)\}).$$

This provides the following definition for $EXP\Pi(x, y, z)$:

$$[(x = 1 \vee y = 1) \Longrightarrow z = 1] \wedge$$
$$\exists p \exists t \exists u \big[POW(x, p) \wedge POW(y, p) \wedge POW(z, p) \wedge INISUPP(\varphi(x), t) \wedge$$
$$\forall q \forall q' \{ NEXTSUPP(q, q', t) \Longrightarrow \exists r \exists r' [POW(r, p) \wedge q =_\Pi \varphi(r) \wedge$$
$$MULT\Pi(r, x, r') \wedge q' =_\Pi \varphi(r')]\}$$
$$\wedge FINSUPP(\varphi(z), t) \wedge \Pi COD(y, u) \wedge SUPPEQUI_\Pi(t, u) \big].$$

■

Lemma 3.9. *The mapping* $f : x \mapsto 2^x$ *with domain* Π *is definable in* $\langle \mathbb{N}; \perp, <_\Pi \rangle$.

Proof. Let $x = \rho_n$. The basic idea is to use the equipotence of the sets $A = \{\rho_0, \rho_1, \ldots, \rho_n\}$ and $B = \{2^{\rho_0}, 2^{\rho_1}, \ldots, 2^{\rho_n}\}$. Since we only have a restricted relation of equipotence $SUPPEQUI_\Pi$, we shall define from A and B two sets A' and B' such that $Card(A') = Card(A)$, $Card(B') = Card(B)$ and $A' \cup B' \subset \{\varphi(2^i) \quad i \geq 0\}$. A' will be a set connected to $\{\rho_0^d, \rho_1^d, \ldots, \rho_n^d\}$ and B' will have the form $\{\varphi(2^{\rho_0}), \varphi(2^{\rho_1}), \ldots, \varphi(2^{\rho_n})\}$.

If $x \in \Pi$ then there exists a power of 2 between all consecutive powers of x. This remark enables us to encode each finite set $\{x, x^2, \ldots, x^d\}$ by a set with the same cardinality, and formed only with $\varphi(2^i)$'s. We introduce the relation

[$x \in \Pi$, $y = x^d$ *for a* $d \geq 1$, *and* $Supp(c)$ *has the form* $\{\varphi(2^{k_1}), \varphi(2^{k_2}), \ldots, \varphi(2^{k_d})\}$ *where* 2^{k_i} *is the least power of two greater than or equal to* x^i $(i = 1, 2, \ldots, d)$.]
denoted by $CODPOW(x, y, c)$, for which a suitable definition is

$$\exists a \big[INISUPP(\varphi(a), c) \wedge a = \min_\Pi \{t : POW(t, 2) \wedge (x =_\Pi t \vee x <_\Pi t)\} \big] \wedge$$
$$\forall q \forall q' \big\{ NEXTSUPP(q, q', c) \Longrightarrow \exists r \exists r' \exists b \exists b' \big[=_\Pi \varphi(r) \wedge q' =_\Pi \varphi(r') \wedge MULT_\Pi(b, x, b')$$
$$\wedge r = \min_\Pi \{t : POW(t, 2) \wedge (b =_\Pi t \vee b <_\Pi t)\}) \wedge$$
$$\wedge r' = \min_\Pi \{t : POW(t, 2) \wedge (b' =_\Pi t \vee b' <_\Pi t)\}) \wedge$$
$$\exists a' (FINSUPP(\varphi(a'), c) \wedge a' = \min_\Pi \{t : POW(t, 2) \wedge (y =_\Pi t \vee y <_\Pi t)\}) \big] \big\}.$$

Now let x_1 and x_2 be primary numbers. For all $y_1, y_2 \in \Pi$, $y_1 = x_1^d$ and $y_2 = x_2^d$ for a $d \geq 1$ if and only if y_1 and y_2 respectively are powers of x_1 and x_2, and furthermore if the sets $\{x_1, x_1^2, \ldots, y_1\}$ and $\{x_2, x_2^2, \ldots, y_2\}$ are equipotent. The latter condition can be expressed using $CODPOW$, and one obtains a definition for the relation

[$x_1, x_2 \in \Pi$ *and there exists* $d \geq 1$ *such that* $y_1 = x_1^d$ *and* $y_2 = x_2^d$]
denoted by $SAMEPOW(x_1, x_2, y_1, y_2)$ with the formula

$$\exists c_1 \exists c_2 [CODPOW(x_1, y_1, c_1) \wedge CODPOW(x_2, y_2, c_2) \wedge SUPPEQUI_\Pi(c_1, c_2, 2)].$$

Let $j \in \mathbb{N}$. Set $\alpha = \min\{\frac{\rho_{i+1}}{\rho_i} \ : \ 0 \leq i \leq j-1\}$, and assume that d is an integer greater than $\frac{\log 2}{\log \alpha}$. For every $i \in \{0, \ldots, j-1\}$ we have $\frac{\rho_{i+1}^d}{\rho_i^d} \geq \alpha^d \geq 2$. Therefore there exists a power of 2 between ρ_i^d and ρ_{i+1}^d for every $i \in \{0, \ldots, j-1\}$. This means that for d great enough one can encode the set $\{\rho_0, \rho_1, \ldots, \rho_j\}$ by the set $\{\varphi(2^{k_0}), \varphi(2^{k_1}), \ldots, \varphi(2^{k_j})\}$ where 2^{k_i} is the least power of 2 greater than or equal to ρ_i^d $(i = 0, 1, \ldots, j)$. So we introduce the relation
[$x = \rho_j$ *for a* $j \in \mathbb{N}$, *and there exists* $d \geq 1$ *such that*
(i) there exists a power of 2 between ρ_i^d *and* ρ_{i+1}^d *for every* $i \in \{0, \ldots, j-1\}$
(ii) $Supp(c) = \{\varphi(2^{k_0}), \varphi(2^{k_1}), \ldots, \varphi(2^{k_j})\}$ *where* 2^{k_i} *is the least power of 2 greater than or equal to* ρ_i^d $(i = 0, 1, \ldots, j)$]
denoted by $CODSEQ\Pi(x, c)$ and for which a convenient definition is

$$\exists y \exists x' \exists v \{INISUPP(\varphi(y), c) \wedge FINSUPP(\varphi(v), c) \wedge SAMEPOW(2, x, y, y')$$

$$\wedge v = \min_{\Pi}\{t : POW(t, 2) \wedge x' <_{\Pi} t\} \wedge$$

$$\forall q \forall q' \ NEXTSUPP(q, q', c) \Longrightarrow$$

$$\exists r \exists r' \exists z_1 \exists z_2 \exists z_1' \exists z_2' [q =_{\Pi} \varphi(r) \wedge q' =_{\Pi} \varphi(r') \wedge SAMEPOW(2, z_1, y, z_1') \wedge$$

$$SAMEPOW(2, z_2, y, z_2') \wedge \neg \exists u (z_1 <_{\Pi} u \wedge u <_{\Pi} z_2) \wedge$$

$$r = \min_{\Pi}\{t : POW(t, 2) \wedge z_1' <_{\Pi} t\} \wedge r' = \min_{\Pi}\{t : POW(t, 2) \wedge z_2' <_{\Pi} t\}]\}.$$

One should note that condition (i) in the definition of $CODSEQ\Pi(x, c)$ is necessary to get $Card(Supp(c)) = Card(\{\rho_0, \rho_1, \ldots, \rho_j\})$.

We now want to define $CODSEQ\Pi EXP(c)$ which means
[$Supp(c) = \{\varphi(2^{\rho_0}), \varphi(2^{\rho_1}), \ldots, \varphi(2^{\rho_j})\}$ *for a* $j \in \mathbb{N}$].
We need the auxiliary relation
[*there exists* $q \in \Pi$ *such that* $z = \varphi(2^q)$]
denoted by $COD\Pi EXP(z)$, and which can be defined by

$$\exists v \{POW(v, 2) \wedge z =_{\Pi} \varphi(v) \wedge \forall y_1 \forall y_2 [(EXP\Pi(y_1, y_2, v) \wedge \neg y_1 = 1 \wedge \neg y_2 = 1) \Longrightarrow$$

$$\exists u \exists z_1 \exists z_2 (\neg u = 1 \wedge \neg z_1 = 1 \wedge \neg z_2 = 1 \wedge EXP\Pi(u, z_1, y_1) \wedge EXP\Pi(u, z_2, y_2)]\}.$$

Then a convenient definition for $CODSEQ\Pi EXP(c)$ is

$$\exists q [POW(q, 2) \wedge INISUPP(\varphi(q), c)] \wedge$$

$$\forall r \forall r' \{NEXTSUPP(r, r', c) \Longrightarrow [COD\Pi EXP(r) \wedge r' = \min_{\Pi}\{t : COD\Pi EXP(t) \wedge r <_{\Pi} t\}]\}.$$

We now are able to define $y = f(x)$ by the formula

$$\exists c_1 \exists c_2 [CODSEQ\Pi(x, c_1) \wedge CODSEQ\Pi EXP(c_2) \wedge SUPPEQUI_{\Pi}(c_1, c_2, 2) \wedge$$

$$FINSUPP(\varphi(y), c)].$$

■

Remark. With slight modifications, the previous coding device can be used to define the relation $SUPPEQUI$.

At this step we can state the main theorem.

Theorem 3.10. *For every arithmetical set $X \subseteq \mathbb{N}^k$ the set $X_\Pi = X \cap \Pi^k$ is definable in $\langle \mathbb{N}; \perp, <_\Pi \rangle$.*

Proof. We show that $\langle \mathbb{N}; \perp, <_\Pi \rangle$ satisfies properties (i) and (a) of Th.3.1 for $p = 2$. Lemma 3.9 corresponds to (a), thus it remains to show that the structure $\langle 2^{\mathbb{N}}; =_{[2]}, \otimes_2, \oplus_2 \rangle$ is definable in $\langle \mathbb{N}; \perp, <_\Pi \rangle$. The domain $2^{\mathbb{N}}$ is definable by the formula $POW(x, 2)$; then $=_{[2]}$, $\otimes_2$ and $\oplus_2$ can easily be defined by the following formulas:

$$(POW(x,2) \wedge POW(y,2) \wedge x =_\Pi y)$$
for $x =_{[2]} y$;

$$(POW(x,2) \wedge EXP_\Pi(x,y,z))$$
for $z = x \otimes_2 y$;

$$(POW(x,2) \wedge MULT_\Pi(x,y,z)$$
for $z = x \oplus_2 y$.

■

Theorem 3.11. *The sets DEF$(\mathbb{N}; |, <_\Pi)$, DEF$(\mathbb{N}; =, \times, <_\Pi)$ and DEF$(\mathbb{N}; =, \times, +)$ are equal.*

Proof. According to Lemma 3.7, the restriction of multiplication to powers of the same prime, denoted by $MULT\Pi$, is $\{\perp, <_\Pi\}$-definable, so it is also $\{|, <_\Pi\}$-definable. This predicate allows us to define multiplication in the structure $\langle \mathbb{N}; |, <_\Pi \rangle$, which will ensure us that DEF$(\mathbb{N}; |, <_\Pi)$ and DEF$(\mathbb{N}; =, \times, <_\Pi)$ are equal. We need the auxiliary relation

[$x \neq 0$, *p is prime, and t is the greatest power of p which divides x*]

which is denoted by $COMP(x, p, t)$, and can be defined by

$$\neg(x = 0) \wedge P(p) \wedge \forall z[(Pow(z,p) \wedge z \mid x) \Longleftrightarrow z \mid t]$$

Then a suitable defining formula for $x \times y = z$ is the following:

$$[(x = 0 \vee y = 0) \Longrightarrow z = 0] \wedge$$
$$\forall p \forall t_1 \forall t_2 \forall t_3 \Big\{ [COMP(x,p,t_1) \wedge COMP(y,p,t_2) \wedge COMP(z,p,t_3)] \Longrightarrow MULT\Pi(t_1,t_2,t_3) \Big\}$$

Let us now show that DEF$(\mathbb{N}; =, \times, <_\Pi)$ = DEF$(\mathbb{N}; =, \times, +)$. By Th.3.1 (b), it suffices to define the mapping $g : x \mapsto 2^x$ with domain $\mathbb{N}$. The possibility to define g relies on the following observation: for every non-zero integer $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ (the p_i's being distinct primes), 2^n is the least power of 2 which is a positive power of $2^{p_i^{\alpha_i}}$ for every $i \in \{1, 2, \ldots k\}$. Thus a suitable definition for $y = g(x)$ is

$$y = \min_\Pi \{t : POW(t,2) \wedge \forall p \forall u [COMP(x,p,u) \Longrightarrow \exists v(\neg v = 1 \wedge EXP_\Pi(f(u), v, t))]\}.$$

■

References

[CMR95] P.Cegielski, Y. Matiyasevich, D.Richard, *Definability and decidability issues in extensions of the integers with the divisibility predicate*, **Journal of Symbolic Logic** 61(2), 1996, 515–540.

[EMF75] W.J.Ellison, M.Mendès-France, *Les nombres premiers*, Ed.Hermann, Paris, 1975.

[Mau95] F.Maurin, *The theory of integer multiplication with order restricted to primes is decidable*, **Journal of Symbolic Logic** 62(1), 1997, 123–130 .

[Put57] H.Putnam, *Decidability and essential undecidability*, **Journal of Symbolic Logic** 22, 1957, 39–54.

[Ric85] D.Richard, *All arithmetical sets of powers of primes are first-order definable in terms of the successor function and the coprimeness predicate* , **Discrete Mathematics**, vol.53, 1985, 221–247.

[Rob49] J.Robinson, *Definability and decision problems in arithmetic*, **Journal of Symbolic Logic** 14, 1949, 98–114.

[Sko30] T.Skolem, *Über gewisse Satzfunktionen in der Arithmetik*, **Skr. Norske Videnskaps-Akademie i Oslo**, 7 , 1930.

[Woo81] A.R.Woods, *Some problems in logic and number theory and their connections, Thesis*, University of Manchester, 1981.

Alexis Bès
Equipe de Logique
Université Paris 7
2, Place Jussieu
75251 Paris Cedex 05
France
e-mail: **bes@logique.jussieu.fr**

Denis Richard
Laboratoire de Logique, Algorithmique et Informatique de Clermont I (LLAIC 1)
I.U.T. Informatique
B.P. 86
F-63172 Aubière Cedex
France
e-mail: **richard@llaic.univ-bpclermont.fr**