A Survey of Arithmetical Definability

Alexis Bès

Abstract

We survey definability and decidability issues related to first-order fragments of arithmetic, with a special emphasis on Presburger and Skolem arithmetic and their (un)decidable extensions.

Contents

1991 *Mathematics Subject Classification :* Primary 03-02. Secondary 03F30, 03B25, 03D05, 11U05.

Key words and phrases : decidability, definability, Presburger arithmetic, finite automata, numeration systems, Skolem arithmetic, Feferman-Vaught technique, Erdös-Woods conjecture.

1 Introduction

This paper deals with arithmetical definability, which aims to study the expressive power of first-order fragments of arithmetic. A classical example is Presburger arithmetic, which is the elementary theory of $\langle \mathbb{N}; +, = \rangle$. More generally arithmetical definability deals with theories of structures $\langle \mathbb{N}; \mathcal{R} \rangle$ where $\mathcal{R}$ denotes a set of functions, relations, constants, which are *arithmetical*, i.e. elementary definable in $\langle \mathbb{N}; +, \times, = \rangle$. Some examples of arithmetical relations and functions are: order relation $<$, successor function $S : x \mapsto x + 1$, the function π which enumerates prime numbers, the divisibility relation $|$, the relations "*to be a prime*", "*to be a square*", etc...

The subject is obviously related to the study of decidability of logical theories, as one often proves (un)decidability of a theory by means of definability arguments; let us also note that (un)decidability results *in the context of logical theories* are usually considered for definability (and more generally model-theoretical) properties they imply rather than for practical purposes.

Some classical examples:

- Presburger's proof of decidability for the elementary theory of $\langle \mathbb{N}; =, + \rangle$ implies that a set $X \subseteq \mathbb{N}$ is definable in $\langle \mathbb{N}; =, + \rangle$ if and only if X is ultimately periodic (see next section);
- a key-argument in Gödel's proof of undecidability of $\mathrm{Th}(\mathbb{N}; =, +, \times)$ is the definability of exponentiation function;
- in the same way the negative solution given by Matiyasevich to Hilbert's Tenth Problem relies on the fact that exponentiation function is *existentially* definable in $\langle \mathbb{N}; =, +, \times \rangle$.

In spite of the first two examples, which come respectively from the 20's and 30's, one can consider that arithmetical definability was initiated by Julia Robinson's 1949 paper [Rob49], in which she proved that $+$ and $\times$ are definable in $\langle \mathbb{N}; S, | \rangle$, and proposed several related questions, among which stands one of the most famous open problems in the field, namely whether one can define $+$ and $\times$ in the structure $\langle \mathbb{N}; S, \perp \rangle$, where $\perp$ is interpreted as the relative primeness relation (i.e. $x \perp y$ iff $\gcd(x, y) = 1$); this question received considerable attention in the 80's, and the partial answers given by Woods and Richard showed nice connections between arithmetical definability and number theory. Another recent achievements in the field are the results of Muchnik, and Michaux-Villemaire, who exploit the strong connection (discovered by Büchi in the late fifties) between definability in Presburger arithmetic and recognizability of sets of natural numbers by finite automata.

Our aim here is to present classical results and techniques in the field, as well as less known results and proofs (in particular Woods' proofs of results related to $\langle \mathbb{N}; S, \perp \rangle$). We shall consider various sets $\mathcal{R}$ of arithmetical relations and functions, and address the following questions: can we describe relations definable in $\langle \mathbb{N}; \mathcal{R} \rangle$? In particular, can we define $+$, and $\times$? Is the elementary theory of $\langle \mathbb{N}; \mathcal{R} \rangle$ decidable ? Starting from the language of arithmetic $\mathcal{R} = \{=, +, \times\}$, it is quite natural to consider then the languages $\{=, +\}$ and $\{=, \times\}$. We concentrate on these two languages and their extensions.

We will focus on "full" definability and only mention a few existential definability related results and questions; we refer the interested reader to the survey paper [Phe94].

The papers [Rab77], [Gri91], [Ceg96], [Res00], [Kor97], and the book [Smo91], are closely related to the subject treated here - and allow to escape from the rather monomaniac viewpoint adopted in the present paper.

The first section deals with *Presburger Arithmetic*, namely the (first-order) theory of $\langle \mathbb{N}; =, + \rangle$. We recall Presburger's quantifier elimination result and its consequences. We then consider extensions of Presburger arithmetic obtained by adding a unary predicate which is interpreted as the range of a polynomial function, or by adding a "weakening" of multiplication, e.g. the relative primeness predicate, or the set of prime numbers (i.e. the unary relation interpreted as "to be a prime number"). Then we recall the main results of Semënov, who described a large class of decidable extensions of $\langle \mathbb{N}; =, + \rangle$ (an example: $\langle \mathbb{N}; +, =, f \rangle$, with $f(x) = 2^x$). The last part of the section deals with connections between definability in (extensions of) Presburger arithmetic, finite automata and numeration systems; this is the place to present some recent successful applications of definability due to Muchnik, as well as Michaux and Villemaire.

The next section deals with *Skolem Arithmetic*, i.e. the multiplicative theory of integers, and its extensions. We recall Mostowski's proof of decidability of $\mathrm{Th}(\mathbb{N}; \times, =)$, then explain Feferman-Vaught composition theorem, which consists in a refinement of Mostowski's notion of products of structures, and appears as a nice tool for constructing decidable extensions of $\langle \mathbb{N}; \times, = \rangle$. An example, due to Maurin, is the (decidable) theory of $\langle \mathbb{N}; \times, =, <_P \rangle$ where $<_P$ denotes order relation restricted to prime numbers. We then use the automata techniques that were introduced in the previous sections to give an alternative proof for decidability of the latter theory. We also state some undecidability results for extensions of Skolem arithmetic, such as $\langle \mathbb{N}; \times, =, <_\Pi \rangle$ where $<_\Pi$ denotes order restricted to primary numbers (a result due to D.Richard and the author), and the result of Cegielski, Matiyasevich and Richard about structures $\langle \mathbb{N}; \times, =, p \rangle$ where p denotes any injection from $\mathbb{N}$ to the set of primes.

The last section is devoted to Julia Robinson's famous open problem, which we already mentioned: can we define $+$ and $\times$ in $\langle \mathbb{N}; S, \perp \rangle$, where S denotes successor function and $x \perp y$ iff $gcd(x, y) = 1$? As shown by Woods, this question turns out to be equivalent with a difficult number-theoretic problem, known as *Erdös-Woods Conjecture*. We first recall Julia Robinson's proof of undecidability of $\mathrm{Th}(\mathbb{N}; S, |)$, then detail Woods' main results on $\langle \mathbb{N}; S, \perp \rangle$ (as far as we know, until now the proofs could only be found in Woods' PhD Thesis). We finally state related definability results obtained by Richard.

Let us specify our logical conventions and notations. We work within first-order predicate calculus *without* equality[1]. We will confuse formal symbols and their interpretations. The symbols $<, +, |, \times, \ldots$ are interpreted in their usual way.

[1]Most structures considered in the paper will have equality relation $=$ in their language, but $=$ is considered as a non-logical symbol.

Given a $\mathcal{L}-$structure $\langle M;\mathcal{L}\rangle$, and a $n-$ary relation R over M, recall that R is elementary definable (shortly: *definable*) in $\langle M;\mathcal{L}\rangle$ if there exists a first-order $\mathcal{L}-$formula φ with n free variables such that $R=\{(a_1,\ldots,a_n):\langle M;\mathcal{L}\rangle\models\varphi(a_1,\ldots,a_n)\}$. We will say that a function is definable in a structure if its graph is definable.

Examples :

- the order relation on $\mathbb{N}$ is definable in $\langle\mathbb{N};=,+\rangle$, since $x<y$ iff

$$\exists z\ \Big(\neg(z+z=z)\ \wedge\ x+z=y\Big);$$

- the unary relation *"x is prime"* is definable in $\langle\mathbb{N};=,\times\rangle$ by the formula

$$\forall y\forall z\ \Big(x=yz\Longrightarrow[(\forall t\ t=ty)\ \vee\ (\forall t\ t=tz)]\Big)$$

(we will simply say that the set of primes is definable in the structure).

We shall only use this basic notion of definability; more advanced definability notions and techniques can be found e.g. in [Ceg96] (non-definability techniques, in particular).

Given a structure $\mathcal{M}$, we denote by $\mathrm{Def}(\mathcal{M})$ the set of relations definable in $\mathcal{M}$, and by $\mathrm{Th}(\mathcal{M})$ the elementary theory of $\mathcal{M}$.

The main symbols and notations used in the paper can be found in the table at the end of the paper.

2 Presburger Arithmetic and extensions

2.1 Presburger Arithmetic

Presburger proved in [Pre29] the decidability of the theory of $\langle\mathbb{N};=,+\rangle$ by means of quantifier elimination. We only state the result, whose proof can be found in many introductive textbooks on mathematical logic (see e.g. [End72]).

As usual with quantifier elimination, we have to extend the language: we add constant symbols for 0 and 1, and an infinite set of binary relations $<_n$ for $n\geq 1$ defined by: for all $x,y\in\mathbb{N}$,

$x<_n y$ holds iff $(x<y$ and $x\equiv y\pmod n)$.

Theorem 1. *The theory* $Th(\mathbb{N};=,+,0,1,(<_n)_{n\geq 1})$ *admits quantifier elimination.*

Let us state two important corollaries of Presburger's result.

Corollary 2. *The elementary theory of* $\langle\mathbb{N};=,+\rangle$ *is decidable.*

We will state another proof of this result in paragraph 2.5, using arguments from automata theory.

Theorem 1 allows to describe definable subsets of $\mathbb{N}$.

Corollary 3. *A subset $X \subseteq \mathbb{N}$ is definable in $\langle \mathbb{N}; =, + \rangle$ iff X is* ultimately periodic*, i.e. if there exist $M, p \geq 1$ such that for every $n \geq M$, $n \in X \iff n + p \in X$*

This characterization was generalized by Ginsburg and Spanier [GS66] as follows.

Theorem 4. *For every $n \geq 1$, a subset $X \subseteq \mathbb{N}^n$ is definable in $\langle \mathbb{N}; +, = \rangle$ if and only if X is* semilinear*, i.e if X is definable by a finite disjunction of formulas $\varphi(\overrightarrow{x})$ of the form*

$$\exists y_1 \ldots \exists y_n \ (\overrightarrow{x} = \overrightarrow{a}_0 + \overrightarrow{a}_1 \cdot y_1 + \cdots + \overrightarrow{a}_j \cdot y_j)$$

where $\overrightarrow{x}$ is the $n-$tuple $(x_1, \ldots, x_n)$, $\overrightarrow{a}$, $\overrightarrow{a}_0$, $\ldots$ $\overrightarrow{a}_j \in \mathbb{N}^n$ are constants, and $\overrightarrow{a} \cdot y$ stands for the product $(a_1 y, \ldots, a_n y)$.

Two alternative (recent) characterizations of definable relations in $\langle \mathbb{N}; +, = \rangle$, and their applications, will be stated in paragraph 2.5.

2.2 Addition and polynomials

A straightforward consequence of Corollary 3 is that, among polynomial functions in one variable (with coefficients in $\mathbb{N}$), only the linear ones are definable in $\langle \mathbb{N}; =, + \rangle$. In other words, adding a linear function f (or the range of f) to the language $\{=, +\}$ does not increase the expressive power. As the next results show, the situation is quite different for non-linear polynomials. The first result is due to Putnam [Put57].

Let $\times$ denote the multiplication function.

Proposition 5. *Let C denote the set of squares. The function $\times$ is definable in $\langle \mathbb{N}; =, +, C \rangle$; therefore $Th(\mathbb{N}; =, +, C)$ is undecidable.*

Proof. First define the constants 0 and 1. Then the relation $y = x^2$ is definable by the formula

$$C(y) \wedge C(y + x + x + 1) \wedge \neg \exists z [C(z) \wedge y < z < y + x + x + 1].$$

Finally one defines $z = x \times y$ by the formula $(x + y)^2 = x^2 + z + z + y^2$.

■

The result was generalized by Büchi [Buc60].

Proposition 6. *Let $P(x)$ be a polynomial with coefficients in $\mathbb{N}$, with degree ≥ 2, and let $X_P = \{P(n) : \ n \in \mathbb{N}\}$. Then $\times$ is definable in $\langle \mathbb{N}; =, +, X_P \rangle$.*

Proof. by induction on the degree $deg(P)$ of P. The case $deg(P) = 2$ follows from the same idea as in the previous proof. For the induction step, observe that the range of the polynomial $Q(n) = P(n + 1) - P(n)$ is definable in $\langle \mathbb{N}; =, +, X_P \rangle$, and that Q has degree $deg(P) - 1$. ■

It is not known whether the *existential* theory of $\langle \mathbb{N}; =, +, C \rangle$ is decidable. As shown by Büchi (see [Buc90, Section 8, p.677]) this question is connected with the following one :

Is there some $n \geq 2$ such that for all integers $a_0 < a_1 < \cdots < a_n$ if
$a_{i+2}^2 + a_i^2 = 2a_{i+1}^2 + 2$ *for every $i \leq n-2$, then $a_0, a_1, \ldots, a_n$ are consecutive integers ?*

Indeed if this question had a positive answer then one could define existentially the relation "*x, y are consecutive squares*", then the squaring function, and finally $\times$ as above. Now by Matiyasevich-Davis-Robinson-Putnam theorem [Mat70], the existential theory of $\langle \mathbb{N}; +, \times, = \rangle$ is undecidable, thus the existential theory of $\langle \mathbb{N}; +, C, = \rangle$ would be undecidable too. We refer to the survey paper [Maz94] where the question is discussed (up to now it is known that n must be ≥ 3).

We saw that extending Presburger arithmetic by a predicate for the range X_P of a polynomial function P of degree ≥ 2 suffices to define full arithmetic and obtain undecidability for the corresponding theory. A nice related result due to Korec [Kor00] is that there are polynomials in two variables which alone suffice to define both $+$ and $\times$. Let us state one of the examples he gave (the proof uses a result from section 3).

Theorem 7. *Let $f : \mathbb{N}^2 \to \mathbb{N}$ be defined by $f(x, y) = x^2 + y^2$. We have*

$$\mathrm{Def}(\mathbb{N}; f, =) = \mathrm{Def}(\mathbb{N}; +, \times, =).$$

Proof. The first step is to define the function $g(x) = 2x$. This can be done by defining the constants 0 and 1 (easy), then intermediate polynomial functions (in x) that are listed below:

$$x^2, 2x^2, 4x^4, 5x^4, 8x^4, 3x^4, 7x^4, 34x^8, 9x^8, 12x^8$$

$$36x^8, 6x^4, 9x^4, 3x^2, 18x^4, 17x^4, 16x^4, 4x^2, 2x.$$

For example one defines $y = x^2$ thanks to the equivalence $(y = x^2 \iff y = f(x, 0))$, then we use $(y = 2x^2 \iff y = f(x, x))$, then $(y = 4x^4 \iff y = (2x^2)^2)$, then $(y = 5x^4 \iff y = f(2x^2, x^2))$ and so on.

Once $x \mapsto 2x$ is defined, the function $h(x, y) = |x^2 - y^2|$, and then $\times$, can be defined by

$$z = h(x, y) \iff f(z, f(x, y)) = 2f(x^2, y^2)$$

$$z = xy \iff f(h(x, y), 2z) = ((f(x, y))^2$$

Then one defines the binary relation $\mathrm{Neib}(x, y)$, interpreted as $|x - y| = 1$, by the formula

$$(x = 0 \ \wedge \ y = 1) \ \vee \ (x = 1 \ \wedge \ y = 0) \vee$$

$$\exists z \ (h(y, z) = 4x \ \wedge \ f(y, z) = 2f(x, 1))$$

Now by Theorem 46 (see Section 3) we have

$$\mathrm{Def}(\mathbb{N}; =, \mathrm{Neib}, \times) = \mathrm{Def}(\mathbb{N}; =, +, \times).$$

■

2.3 Extending $\langle \mathbb{N}; =, + \rangle$ with "fragments" of multiplication

It is rather natural to consider, among languages laying between $\{=, +\}$ and $\{=, +, \times\}$, those having the form $\{=, +, R\}$ where R is definable in $\langle \mathbb{N}; =, \times \rangle$. Some natural candidates for R are: divisibility relation $|$, coprimeness relation $\perp$ (recall that $x \perp y$ iff $\gcd(x, y) = 1$), and the set P of primes (i.e. the unary relation "to be a prime").

The following proposition is left as an exercise.

Proposition 8. *(i) $\perp$ and P are definable in $\langle \mathbb{N}; | \rangle$;*
(ii) $|$ is definable in $\langle \mathbb{N}; =, \times \rangle$.

We shall study the structures $\langle \mathbb{N}; =, +, \perp \rangle$ and $\langle \mathbb{N}; =, +, P \rangle$.

2.3.1 Addition and relative primeness

The question of whether $\mathrm{Th}(\mathbb{N}; +, \perp, =)$ is decidable was asked by J.Robinson [Rob49].

Theorem 9. $\mathrm{Def}(\mathbb{N}; =, +, \perp) = \mathrm{Def}(\mathbb{N}; =, +, \times)$*, thus* $Th(\mathbb{N}; =, +, \perp)$ *is undecidable.*

We shall give two proofs of this result, as an illustration of classical techniques used in the field. The first one is due to Woods [Woo81] and has been independently found by J.Robinson (unpublished). It rests on a strong number-theoretical result.

Proof. The constants $0, 1, 2$ are easily definable in $\langle \mathbb{N}; =, +, \perp \rangle$ (even in $\langle \mathbb{N}; =, + \rangle$).

The relation "x is prime", denoted by $P(x)$, is definable by the formula

$$(x \neq 0) \wedge (x \neq 1) \wedge \forall y[(y \neq 0 \wedge y < x) \Longrightarrow y \perp x].$$

Now consider the ternary relation "x and y are prime integers, and $z = x \times y$", denoted by $MULTP(x, y, z)$ (a restriction of the graph of multiplication). Note that if x and y are two distinct primes, then xy is the least positive integer which is not prime to both x and y. Moreover if x is prime then x^2 is the least integer greater than x which has the same prime divisors as x. These facts lead to the following definition for $MULTP(x, y, z)$:

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

$$\{x \neq y \Longrightarrow [\neg z \perp x \wedge \neg z \perp y \wedge \forall t((\neg t \perp x \wedge \neg t \perp y) \Longrightarrow (t = 0 \vee z \leq t))]\} \wedge$$

$$\{x = y \Longrightarrow [\forall t(t \perp x \iff t \perp z) \wedge \forall u \forall v[(v \perp x \iff v \perp u) \Longrightarrow (u = x \vee u \geq z]]\}.$$

We now use Schnirelmann-Vaughan [RV83] theorem which asserts that there exists a constant c such that any integer greater than 1 can be written as the sum of at most c primes. Multiplication of two integers, thanks to this theorem, reduces to the addition of a bounded number of products of two primes. This allows to define $z = xy$ in $\langle \mathbb{N}; =, +, \perp \rangle$ by the formula

$$[(x = 0 \vee y = 0) \Longrightarrow z = 0] \wedge [x = 1 \Longrightarrow z = y] \wedge [y = 1 \Longrightarrow z = x] \wedge$$

$$\{(x \geq 2 \wedge y \geq 2) \Longrightarrow \bigvee_{1 \leq\ i,j\ \leq c} \exists x_1 \ldots \exists x_i\ \exists y_1 \ldots \exists y_j\ \exists z_{1,1} \ldots \exists z_{i,j}$$

$$[(x = \sum_{k=1}^{i} x_k) \wedge (y = \sum_{l=1}^{j} y_l) \wedge (\bigwedge_{\substack{1 \leq k \leq i \\ 1 \leq l \leq j}} MULTP(x_k, y_l, z_{k,l})) \wedge (z = \sum_{k=1}^{i} \sum_{l=1}^{j} z_{k,l})]\}.$$

■

Reisel and Vaughan proved that a convenient value for the constant c of the previous proof (known as *Schnirelmann's constant*) is 19. Since then the value has been reduced to 7 (Ramare [Ram95]). It is conjectured that 3 is the best possible value.

The second proof of Theorem 9 is partly inspired by Richard's proof [Ric89]. This time we use the classical technique of encoding finite sequences of integers.

Second proof. By Theorem 5 it suffices to define the set of squares C in $\langle \mathbb{N}; =, +, \perp \rangle$. One defines, as it was done in the previous proof, the set of primes P, the constants $0, 1, 2$, the relation $<$, and then the function $F : \mathbb{N} \times P \to \mathbb{N}$ which maps $(n, p) \in \mathbb{N} \times P$ to the (non-negative) integer $m < p$ congruent to n modulo p.

Now $x \geq 1$ is a square iff x satisfies the following property: there exist integers c, m, t, $t \geq 1$ such that

- $F(c, \pi(m)) = 0$;
- $F(c, \pi(m+1)) = 1$;
- $F(c, \pi(m+k+2)) - F(c, \pi(m+k+1)) = F(c, \pi(m+k+1)) - F(c, \pi(m+k)) + 2$ for every k such that $0 \leq k \leq t-2$;
- $F(c, \pi(m+t)) = x$

(the integer c encodes the sequence of consecutive squares 0,1,4,... up to x). On one hand it is clear that if x satisfies the above property then it is a square, and conversely if x is a square, say $x = y^2$, then x satisfies the above property if we take $m \geq x$, $t = y$, and c such that $c \equiv i^2 \pmod{\pi(m+i)}$ whenever $i \leq t$ (such a c exists by Chinese Remainder Theorem). ■

Remark. From the decidability of the existential theory of $\langle \mathbb{N}; =, +, | \rangle$, independently proved by Beltyukov [Bel76] and Lipshitz [Lip78], one can infer decidability of the existential theory of $\langle \mathbb{N}; =, +, \perp \rangle$.

The additive theory of primes.

We now turn to the theory of $\langle \mathbb{N}; =, +, P \rangle$. The language $\{=, +, P\}$ allows to express famous open problems of number theory, such as the twin-prime conjecture, or Goldbach' conjecture. Thus a decidability result for $\mathrm{Th}(\mathbb{N}; =, +, P)$ would be rather surprising.

Up to now the only result on $\langle \mathbb{N}; =, +, P\rangle$ rests on a strong number-theoretical hypothesis known as *Dickson's Hypothesis* [Dic04]:

(D) Let $P_i(x) = a_i x + b_i$, with $a_i, b_i \in \mathbb{N}$ and $a_i \geq 1$, for $i = 1, \ldots, k$. Assume that there is no prime p which divides all products $P_1(n) \cdot P_2(n) \cdot \cdots \cdot P_k(n)$ for $n \in \mathbb{N}$. Then there is infinitely many positive integers n such that $P_1(n), P_2(n), \ldots, P_k(n)$ are simultaneously prime.

Dickson's hypothesis is true for case $k = 1$: this is nothing but Dirichlet's Theorem. (D) implies e.g. the twin-prime conjecture. We refer to [Rib96] for a discussion of (D) and related conjectures (such as Schinzel's hypothesis).

The following result was proved by Woods [Woo81], and appeared in a paper by Bateman, Jockusch and Woods [BJW93].

Theorem 10 (assuming (D)). *Multiplication is definable in $\langle \mathbb{N}; =, +, P\rangle$. Therefore $Th(\mathbb{N}; =, +, P)$ is undecidable.*

We first need the following consequence of (D):

Lemma 11 (assuming (D)). *Let $b_0, \ldots, b_n$ be positive integers such that $b_0 < \cdots < b_n$, and assume that for every prime p the set $\{b_0, \ldots, b_n\}$ is not a complete residue system modulo p. Then there exist infinitely many $a \in \mathbb{N}$ such that $a + b_0, \ldots, a + b_n$ are* consecutive *primes.*

Proof. Let $a_1, \ldots, a_r$ be the integers between b_0 and b_n which are not of the form b_i (with $a_1 < \cdots < a_r$). We shall apply (D) to the polynomials $f_j(x) = cx + a_0 + b_j$ $(j = 0, \ldots, n)$, where $c = \prod_{i=0}^{b_n+r} \pi(i)$ (recall that $\pi(i)$ is the $i-$th prime number) and a_0 is chosen such that

(i) a_0 is not congruent to any element of $\{-b_0, -b_1, \ldots, -b_n\}$ modulo $\pi(i)$ $(i = 0, \ldots, b_n)$.

(ii) $a_0 \equiv -a_i \pmod{\pi(b_n + i)}$ $(i = 1, \ldots, r)$.

Such a choice is possible by Chinese Remainder Theorem and our assumptions on $b_0, \ldots, b_n$.

Let us show that $f_1, \ldots, f_n$ satisfy the assumptions of (D).

Assume for a contradiction that some prime p is such that for every x we have $p | f_j(x)$ for some j.

First we must have $p \leq \pi(b_n + r)$. Indeed if $p > \pi(b_n + r)$, then let x be such that $cx + a_0 \equiv 1 \pmod{p}$ (such a x exists since $c \perp p$). Let j be such that $p | f_j(x)$, then we have $p | cx + a_0 + b_j - (cx + a_0 - 1)$, that is $p | b_j + 1$, which implies $p \leq b_n + 1 \leq \pi(b_n + 1)$, from which we get a contradiction.

Therefore we have $p \leq \pi(b_n + r)$. If $p = \pi(i)$ for some $i \leq b_n$ then p divides $f_j(x)$ iff $p | a_0 + b_j$, which is impossible by our assumption on a_0. Now if $p = \pi(b_n + i)$ with $1 \leq i \leq r$ then $p | f_j(x)$ iff $p | a_0 + b_j$ iff $p | -a_i + b_j$, which is impossible since

$$0 < |-a_i + b_j| < b_n < \pi(b_n + i).$$

We have shown that the f_i's satisfy the assumptions of (D), thus there are infinitely many $x \geq 1$ such that $f_1(x), \ldots, f_n(x)$ are simultaneously prime; for those x the integers $f_1(x), \ldots, f_n(x)$ are actually *consecutive* primes, since $cx + a_0 + a_i$ is always divisible by $\pi(b_n + i)$ (by our assumptions on c and a_0) and greater than $\pi(b_n + i)$ (since $x \geq 1$). Taking $a = cx + a_0$ yields the required result. ∎

Proof of Theorem 10. We shall define the range X_g of $g(n) = n^2 + n$ which will yield the result by Proposition 6. Take $n \in \mathbb{N}$, and $b_i = g(i)$ for every $i \leq n$. The b_i's satisfy the assumptions of the previous Lemma, since $g(0) \equiv g(-1) \pmod{p}$ for every prime p. Consider the binary relation $T(x, y)$ which holds iff x is prime, $x \leq y$, and the only primes lying in $[x, y]$ are $x+b_0, \ldots, x+b_n = y$, for some $n \geq 1$. The fact that the second differences of consecutive elements of X_g are all equal to 2 allows to show that the relation T is definable in $\langle \mathbb{N}; =, +, P \rangle$. Now $X_g(y)$ is definable by the formula $y = 0 \vee \exists x T(x, x + y)$. Indeed if this formula holds then obviously $x \in X_g$, and conversely if $x = g(n)$ for some $n \geq 1$ then the formula holds by the previous Lemma (with $b_i = g(i)$ for $i = 0, \ldots, n$). ∎

Boffa recently proved ([Bof98], see also [LM00]), again assuming (D), that Theorem 10 still holds if we replace $\langle \mathbb{N}; =, +, P \rangle$ by $\langle \mathbb{N}; =, +, P_{m,r} \rangle$, where $P_{m,r} = \{p \in P : p \equiv r \pmod{m}\}$, where $m > 2$ and $r \perp m$; note that Dirichlet's Theorem implies that $P_{m,r}$ is infinite.

Up to now nothing is known about $\langle \mathbb{N}; =, +, P \rangle$ in the absence of a special hypothesis. The same is true for $\langle \mathbb{N}; <, P \rangle$, whose expressive power is weaker than the one of $\langle \mathbb{N}; =, +, P \rangle$[2], but already allows to express difficult open problems such as the twin-prime conjecture. Bateman, Jockusch and Woods [BJW93] show that (D) implies not only undecidability of $\mathrm{Th}(\mathbb{N}; =, +, P)$, but also *decidability* of $\mathrm{Th}(\mathbb{N}; <, P)$.

The decidability question still is open for the theory of $\langle \mathbb{N}; =, +, \pi \rangle$ (recall that $\pi(n)$ is the $n-$th prime), which is *a priori* stronger than $\langle \mathbb{N}; =, +, P \rangle$ in terms of definability. A partial answer was given by Cegielski, Richard and Vsemirnov who proved [CRV00] that $\times$ is definable in $\langle \mathbb{N}; =, +, f \rangle$ for a class of functions f which asymptotically behave like π.

2.4 Semënov's work on decidable extensions of $\langle \mathbb{N}; =, + \rangle$

Semënov gave in [Sem79] a criterium for decidability of theories of the form $\langle \mathbb{N}; =, +, R \rangle$, where $R \subseteq \mathbb{N}$. It applies e.g. when R denotes the set of factorials, or the set of Fibonacci numbers, or the set $\{\lfloor e^n \rfloor : n \in \mathbb{N}\}$ (where $\lfloor x \rfloor$ denotes the integral part of x). We shall only state this criterium and omit all proofs; see [Mae00b] for a detailed presentation of Semënov' ideas.

Given a finite alphabet Σ, we denote by Σ^* the set of finite words over Σ, and by Σ^ω the set of infinite words over Σ (i.e. the set of functions $f : \mathbb{N} \to \Sigma$). The *finite factors* of a word $W \in \Sigma^\omega$ are the finite words (over Σ) obtained by restricting W to a finite segment. We denote by W_X the characteristic function of a set $X \subseteq \mathbb{N}$; we have $W_X \in \{0, 1\}^\omega$.

Definition 12. *An infinite word $W \in \Sigma^\omega$ is said to be* almost-periodic *if for every finite factor u of W*

- *either the factor u does not occur after some position Δ;*

[2] It can be shown that $+$ (and even a function like $x \mapsto 2x$) is not definable in $\langle \mathbb{N}; <, P \rangle$, and more generally in any structure $\langle \mathbb{N}; <, R \rangle$, with R unary. See e.g. [Tho79].

- *or u occurs infinitely many times in W, and there is a bound Δ between two consecutive occurrences of u in W.*

Moreover, if there is an algorithm which decides for every u which case holds, and produces a convenient value for Δ, then W is said to be effectively almost periodic[3].

Examples (see [Mae00b]):

- if $X \subseteq \mathbb{N}$ is ultimately periodic then W_X is almost periodic.
- a classical example of an almost-periodic word which is not ultimately periodic is the Thue-Morse word $W \in \{0,1\}^\omega$ whose $i-$th letter is a 1 iff i has an even number of non-zero digits in its binary expansion

$$W = 100101100\ldots$$

- if X is the set of powers of 2 then the word W_X is not almost-periodic: e.g. $u = 1$ occurs infinitely many times in W_X but obviously there is no bound between two consecutive occurrences of u in W_X.

  The argument still holds for any infinite set $X \subseteq \mathbb{N}$ such that the set of differences between consecutive elements of X is unbounded (such a set is said to be *expanding*, see next subsection).

Given $R \subseteq \mathbb{N}$, let $e_R : \mathbb{N} \to R$ enumerate the elements of R in increasing order. For all $c, m \in \mathbb{N}$, $m \geq 2$, we set

$$R_{c,m} = \{n \in \mathbb{N} : \ e_R(n) \equiv c \pmod{m}\}.$$

As an example, if $R = P_2$ then we have we have e.g. $W_{R_{1,2}} = 100000\ldots$, $W_{R_{0,2}} = 0111111\ldots$, $W_{R_{1,3}} = 1010101\ldots$, etc...

We can stack up $W_{R_{0,2}}$ and $W_{R_{1,3}}$, forming the infinite word $\begin{matrix} 0 & 1 & 1 & 1 & 1 & \ldots \\ 1 & 0 & 1 & 0 & 1 & \ldots \end{matrix}$ over the alphabet $\{0,1\} \times \{0,1\}$. The process of stacking up n infinite words ($n \geq 2$) is defined in a similar way.

We set

$$\mathcal{E}_R = \{W_{R_{c,m}} : \ c \geq 0, m \geq 2\}.$$

We say that $\mathcal{E}_R$ is *almost-periodic* (respectively *effectively almost-periodic*) if every word of $\mathcal{E}_R$, or which can be obtained by stacking up a finite number of words of $\mathcal{E}_R$, is almost-periodic (respectively effectively almost-periodic).

It can be shown for example that if R denotes the set of power of 2 then $\mathcal{E}_R$ is effectively almost-periodic.

Definition 13. ([Sem79, section 3]) *Let $R \subseteq \mathbb{N}$; we call* operator *on R any function $A^R : R \to \mathbb{Z}$ for which there exist $t \in \mathbb{N}$ and $a_0, \ldots, a_t \in \mathbb{Z}$ such that*

$$A^R(e_R(n)) = a_t e_R(n+t) + a_{t-1} e_R(n+t-1) + \cdots + a_0 e_R(n)$$

for every $n \in \mathbb{N}$.

[3] Semënov proves that there exist almost-periodic words which are not effectively almost-periodic [Sem79].

Definition 14. ([Sem79, section 3]) *We say that a set $R \subseteq \mathbb{N}$ is* sparse *if every operator A^R on R satisfies the following conditions:*

(i) either $A^R = 0$, or one of the sets $\{n : \ A^R(n) \leq 0\}$, $\{n : \ A^R(n) \geq 0\}$ is finite.

(ii) if $\{n : \ A^R(n) \leq 0\}$ is finite, then there exists $\Delta \in \mathbb{N}$ such that $A^R(y+\Delta) - e_R(y) > 0$ for every $y \in \mathbb{N}$.

The set R is said to be effectively sparse *if it is sparse, and if*

- *there is an algorithm which tells, for every operator A_R, which condition of (i) holds;*
- *in case $\{n : \ A^R(n) \leq 0\}$ is finite, this algorithm provides a value of Δ for which (ii) holds.*

Examples ([Sem79, section 3], see also [Mae00b]):

- if R is the set of powers of 2 then an operator A^R on R has the form

$$A^R(2^n) = a_t 2^{n+t} + a_{t-1} 2^{n+t-1} + \cdots + a_0 2^n = 2^n(a_t 2^t + \cdots + a_0)$$

  The sign of A^R depends on the expression in parenthesis. Moreover if $\{n : A^R(n) \leq 0\}$ is finite then $\Delta = 1$ is a convenient value. Thus R is effectively sparse.

- if R is the set of factorials, then the sign of an operator A^R of the form

$$A^R(n!) = a_t((n+t)!) + a_{t-1}((n+t-1)!) + \cdots + a_0(n!)$$

  ultimately depends on the sign of a_t. Moreover if case (ii) holds, which occurs iff $a_t \geq 1$, then a convenient value for Δ can be recursively computed from the coefficients $a_0, \ldots, a_t$. Thus R is effectively sparse.

  More generally if R satisfies $\lim_{n\to\infty} e_R(n+1)/e_R(n) = \infty$ then R is sparse, and it is effectively sparse if in addition the limit is effective (i.e if there is a computable function $f : \mathbb{N} \to \mathbb{N}$ such that for every m, $e_R(n+1)/e_R(n) > m$ whenever $n > f(m)$).

- the Fibonacci sequence $(U_n)_{n\in\mathbb{N}}$ defined by $U_0 = 1$, $U_1 = 2$ and $U_{n+2} = U_{n+1} + U_n$ for every n, forms an effectively sparse set.

Theorem 15 (Semënov). *Let $R \subseteq \mathbb{N}$ be sparse. Then $Th(\mathbb{N}; =, +, R)$ is decidable if and only if R is effectively sparse and $\mathcal{E}_R$ is effectively almost periodic.*

Semënov's proof consists in showing (in a syntactic way) that some extension by definition of the theory is existential. Point [Poi00a],[Poi00b] recently gave a model-theoretic proof of Theorem 15, and exhibited a new class of sparse predicates for which the above theorem holds.

In the paper [Sem83], Semënov then gave a criterium for decidability of $\mathrm{Th}(\mathbb{N}; =, +, f)$, where f denotes a unary function. Again we only state the result.

Definition 16. ([Sem83, section 2]) *We call* $f-$sum *any function* $A : \mathbb{N} \to \mathbb{Z}$ *of the form*

$$A(x) = \sum_{i=1}^{n} a_i f(x + b_i)$$

where $n \in \mathbb{N}$ *and* $a_i, b_i \in \mathbb{Z}$.

We say that the function f *is* compatible with addition *if the two following conditions hold:*

- *for every* m*, the values of* f *are periodic modulo* m*,*
- *for every* $f-$*sum* A*, one of the following conditions hold:*
  (1) $A(x)$ *is bounded;*
  (2) there exists Δ *such that* $A(x + \Delta) > f(x)$ *holds for all* x*;*
  (3) there exists Δ *such that* $-A(x + \Delta) > f(x)$ *holds for all* x*.*

Moreover if there is an algorithm which tells, for every $f-$*sum* A*, which one of the above condition holds, and produces a convenient value for* Δ *in case (2) or (3) holds, then we say that* f *is* effectively compatible with addition.

Examples :

- $f(x) = 2^x$ (and more generally $f(x) = c^x$ with $c \geq 2$) is compatible with addition;
- if the values of f are periodic modulo m for every m, and if f satisfies $\lim_{x\to\infty} \frac{f(x+1)}{f(x)} = \infty$ then f is also compatible with addition
- $f(x) = x^2$ is not compatible with addition. Consider indeed $A(x) = f(x + 1) - f(x) = 2x + 1$. Then A does not fulfill any of the conditions (1),(2),(3).

  More generally a non-linear polynomial function (with coefficients in $\mathbb{N}$) is not compatible with addition.

Theorem 17 (Semënov). *If* f *is effectively compatible with addition then* $Th(\mathbb{N}; =, +, f)$ *is decidable.*

Semënov's proof is a syntactic one. Cherlin and Point [CP86] gave an alternative proof by constructing an axiom system for the theory and proving that it admits quantifier-elimination. The paper [Poi00b] (already mentioned) describes a whole class of new examples of functions f for which the above theorem holds.

2.5 Presburger Arithmetic and finite automata

The connection between definability and finite automata was first explored in Büchi's paper [Buc60], in which he considered the theory now known as WS1S, the weak monadic second-order theory of one successor function, i.e. of $\langle \mathbb{N}; S \rangle$ (where S denotes successor function). Recall that the weak monadic second-order theory of a

structure $\mathcal{M} = \langle M; \dots \rangle$ arises from its first-order theory by allowing quantification over *finite* subsets of M. Büchi proved decidability of WS1S by showing that definable relations in WS1S correspond (in a natural way) to languages recognizable by finite automata; this correspondence allowed him to reduce the decision problem for WS1S to the emptiness problem for regular languages, which is known to be decidable.

Büchi's decidability technique was extended during the sixties to other monadic second-order theories, up to Rabin's celebrated result [Rab69] on the decidability of S2S, the monadic second-order theory of the binary tree, which is one of the major results regarding decidability of logical theories (see [Tho97]).

In a more general viewpoint, Büchi opened up the way to *descriptive complexity theory*, a very active research area which provides logical characterizations (in terms of definability) of complexity classes, such as Fagin's characterization [Fag75] of the class NP with existential second-order logic (see the survey paper [Pin96]) .

Consider the function that maps any finite set X to the integer $n_X = \sum_{i \in X} 2^i$. This function establishes a natural correspondence between weak monadic second-order theories and first-order theories over the natural numbers, which allowed Büchi to give a new proof of decidability for the *first-order* theory of $\langle \mathbb{N}; =, + \rangle$, i.e. Presburger Arithmetic [4]. In this paragraph we explain the essence of Büchi's technique in the framework of first-order theories. This viewpoint turns to be quite fruitful, as it allows to construct substantial decidable extensions of Presburger arithmetic and offers powerful tools in the study of numeration systems. We discuss some recent related achievements due to Muchnik, as well as Michaux and Villemaire. Finally we deal with Bruyère-Hansel extension of Büchi's result to non-classical numeration systems.

We only touch on the subject, and omit most proofs. We refer the interested reader to the expository paper [BHMV94] and the survey papers [Bru95],[MV96b].

Finite automata and $k-$recognizable sets

Let us recall at first some useful notions about regular languages (a serious presentation of the subject can be found in [Per90]).

Let Σ be a finite alphabet. Recall that Σ^* denotes the set of finite words over Σ, including the empty word which is denoted by λ. The set Σ^* equipped with the concatenation operation $\cdot$ is a free monoid.

We call *language* any subset of Σ^*. Given $L, L' \subseteq \Sigma^*$, let

$$L \cdot L' = \{u \cdot u' : \ u \in L, u' \in L'\}$$

and L^* be the set of words that can be written as a (finite) product of words of L (with the convention $\lambda \in L^*$). The class of *regular languages* (over Σ) is the smallest class of languages containing finite languages and closed under the operations $\cup, \cdot$ and *.

Examples with $\Sigma = \{a, b\}$*:*

[4] R.Robinson proved that the weak monadic second-order theory of $\langle \mathbb{N}; +, = \rangle$ is undecidable [Rob58].

- The set L of words having an even number of a is regular, since $L = (b^*ab^*ab^*)^*$.
- On the other hand it can be shown that the set of words having the same number of a's and b's is not regular.

Regular languages can be described in terms of finite automata. Recall that a (deterministic) finite $\Sigma-$automaton is a quadruple $\mathcal{A} = (Q, q_0, \delta, Q')$ where Q is a finite set (the *set of states*), $q_0 \in Q$ is the *initial state*, $Q' \subseteq Q$ is the set of *final states*, and $\delta : Q \times \Sigma \to Q$ is the *transition function*.

The function δ is inductively extended to a function $\delta^* : Q \times \Sigma^* \to Q$ as follows:

$$\delta^*(q, a) = \delta(q, a) \text{ for all } q \in Q,\ a \in \Sigma;$$
$$\delta^*(q, aw) = \delta(\delta^*(q, w), a) \text{ for all } a \in \Sigma,\ w \in \Sigma^*.$$

A word $w \in \Sigma^*$ is *accepted* by the Σ-automaton $\mathcal{A} = (Q, q_0, \delta, Q')$ if $\delta^*(q_0, w) \in Q'$.

A subset X of Σ^* is said to be *recognizable* if X is the set of accepted words of some finite Σ-automaton.

Example with $\Sigma = \{a, b\}$ *:* the set L of the previous example can be recognized by the automaton $\mathcal{A} = (Q, q_0, \delta, Q')$ defined by $Q = \{q_0, q_1\}$, $\delta(q_0, a) = \delta(q_1, b) = q_1$, $\delta(q_0, b) = \delta(q_1, a) = q_0$ and $Q' = \{q_0\}$.

Kleene's theorem (see [Per90]) asserts the equivalence between regularity and recognizability.

The notion of k-recognizability has to do with the k-ary expansion of integers. For every integer $k \geq 2$, let $\Sigma_k = \{0, 1, \ldots, k-1\}$. For every nonzero integer n, if $n = \sum_{i=0}^{t} \lambda_i k^i$ with $\lambda_i \in \{0, 1, \ldots, k-1\}$ and $\lambda_t \neq 0$, then $[n]_k$ is the word of Σ_k^* defined by $[n]_k = \lambda_t \lambda_{t-1} \ldots \lambda_0$. We set $[0]_k = \lambda$. For every $M \subseteq \mathbb{N}$ we shall denote by $[M]_k$ the set $\{[n]_k : \ n \in M\}$.

Example 1. If $k = 2$, we have e.g. $[5]_2 = 101$, $[8]_2 = 1000$; for the set P_2 of powers of 2 we have $[P_2]_2 = 10^*$, i.e. $[P_2]_2$ is the set of words consisting of a "1" followed by any number of "0".

Definition 18. *A set $M \subseteq \mathbb{N}$ is said to be $k-$recognizable if $[M]_k$ is regular.*

Examples :

- The set P_2 is $2-$recognizable;
- The set of even numbers is $2-$recognizable (more generally Büchi [Buc60] proved that any ultimately periodic set is $k-$recognizable for every $k \geq 2$);
- The set $\{2^{n!} : n \in \mathbb{N}\}$ is not $2-$recognizable.

The previous notion can be extended to subsets of $\mathbb{N}^n$. For every $u \in \Sigma^*$ we shall denote by $|u|$ the length of u. Given a $n-$tuple
$x = (x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ we define $[x]_k$ as the word (of $n-$tuples)

$$(0^{m-m_1}[x_1]_k, 0^{m-m_2}[x_2]_k, \ldots, 0^{m-m_n}[x_n]_k)$$

over Σ_k^n, where $m_i = |x_i|$ and $m = \max\{m_1, \ldots, m_n\}$.

We have e.g.

$$[(5,8)]_2 = \binom{0}{1}\binom{1}{0}\binom{0}{0}\binom{1}{0}$$

For every $M \subseteq \mathbb{N}^n$ we set $[M]_k = \{[a]_k : \ a \in M\}$.

Definition 19. *A set $M \subseteq \mathbb{N}^n$ is said to be $k-$recognizable if $[M]_k$ is regular.*

Examples :

- The graph of addition is $k-$recognizable for every $k \geq 2$;
- For every $k \geq 2$, the graph of multiplication is not $k-$recognizable.

Büchi Arithmetic.

For every integer $k \geq 2$, we call *Büchi Arithmetic of base k* the structure $\langle \mathbb{N}; =, +, V_k \rangle$, where V_k denotes the function which maps every non-zero integer to the greatest power of k dividing it (and $V_k(0) = 1$). The following theorem was stated (in an incorrect form) by Büchi [Buc60] and proved by Bruyère [Bru85].

Theorem 20. *Let $k \geq 2$, $n \geq 1$. A subset $X \subseteq \mathbb{N}^n$ is $k-$recognizable if and only if it is definable in the structure $\langle \mathbb{N}; =, +, V_k \rangle$.*

For a detailed proof see [BHMV94]. The part "definable $\rightarrow$ $k-$recognizable" goes by induction on the number of quantifiers of a prenex formula defining X. The fact that $\mathbb{N}$, as well as the graph of $+$ and V_k, are $k-$recognizable, allows to initialize the induction. For the converse "$k-$recognizable$\rightarrow$definable", assume that the set $[X]_k$ is recognized by a finite automaton $\mathcal{A}$ with n states, say $q_1, \ldots, q_n$. Then the formula $\varphi(\overrightarrow{x})$ which defines X expresses that there exist n integers $y_1, \ldots, y_n$ which encode a successful run of $\mathcal{A}$ for $[\overrightarrow{x}]_k$. The integers $y_1, \ldots, y_n$ are chosen such that the automaton $\mathcal{A}$ reaches the state q_i after reading the $j-$th letter of $[\overrightarrow{x}]_k$ iff the $j-$th letter of $[(y_1, \ldots, y_n)]_k$ has the form $(0, \ldots, 0, 1, 0, \ldots, 0)$ where the "1" is in $i-$th position.

Theorem 20 yields a decision procedure for $\mathrm{Th}(\mathbb{N}; =, +, V_k)$. Consider indeed a sentence ψ, say e.g. of the form $\exists x \ \varphi(x)$. The previous theorem allows to find (in an effective way) a regular language $L_\varphi \subseteq \Sigma_k^*$ such that for every integer n,

$$\langle \mathbb{N}; =, +, V_k \rangle \models \varphi(n)$$

iff $[n]_k \in L_\varphi$. Therefore deciding whether ψ holds in $\langle \mathbb{N}; +, V_k \rangle$ amounts to decide whether L_φ is empty. Now the latter problem has been show to be decidable by Kleene (see [Per90]).

Thus we have the following result (essentially due to Büchi [Buc60]):

Theorem 21. *$Th(\mathbb{N}; =, +, V_k)$ is decidable for every $k \geq 2$.*

Theorems 20 and 21 provide useful tools in the study of $k-$recognizable sets. Let us mention some easy applications to decision problems.

1. The subsequent problem was first proved decidable by Honkala [Hon86] in a combinatorial way.

   Instance: $k \geq 2$, and $X \subseteq \mathbb{N}$ a $k-$recognizable set;

   Question: Is X ultimately periodic ?

   Indeed X is ultimately periodic iff the following sentence holds in $\langle \mathbb{N}; =, \leq, +, X \rangle$:

   $$\psi : \quad \exists m \; \exists p \; \forall n \; (n \geq m \Longrightarrow [X(n) \Longleftrightarrow X(n+p)])$$

   Now X is $k-$recognizable thus by Theorem 20 it is definable in $\langle \mathbb{N}; =, +, V_k \rangle$. Moreover $\leq$ is definable in $\langle \mathbb{N}; =, + \rangle$, thus ψ can be transformed in a formally equivalent sentence ψ' in the language $\{=, +, V_k\}$. Then we use Theorem 21 to decide whether ψ' holds.

   The same result holds if we consider the question *"is X almost-periodic ?"*.

   It still holds too if we consider $X \subseteq \mathbb{N}^n$, for some $n \geq 2$, and ask whether X is definable in $\langle \mathbb{N}; =, + \rangle$; this is the consequence of a non-trivial result of Muchnik which is discussed below.

2. (from [Fagn97]) Given an infinite word $W \in \Sigma^\omega$, let $\mathrm{Fact}(W)$ denote the set of finite factors of W. Recall that, given $X \subseteq \mathbb{N}$, W_X denotes the infinite word over $\{0, 1\}$ naturally associated with the characteristic function of X.

   The following problem is decidable:

   Instance: $k \geq 2$, and X, Y two $k-$recognizable subsets of $\mathbb{N}$;

   Question: $\mathrm{Fact}(W_X) \subseteq \mathrm{Fact}(W_Y)$?

   We use the same idea as in the previous example. The main observation is that we have $\mathrm{Fact}(W_X) \subseteq \mathrm{Fact}(W_Y)$ iff the following sentence holds in $\langle \mathbb{N}; =, \leq, +, X, Y \rangle$:

   $$\forall m \; \forall n \; \exists m' \; \forall i \; (i \leq n \Longrightarrow [X(m+i) \Longleftrightarrow Y(m'+i)]).$$

Theorem 20 provides an alternative approach to questions regarding $k-$recognizable sets (and more generally regular languages). The next paragraph about the Cobham-Semënov Theorem will deal with one of the main related achievements. A typical kind of problems where definability techniques appear to be very efficient is when one wants to show that a given operation preserves $k-$recognizability, or regularity. In such situations simple definability arguments can replace long and tedious automata constructions.

Let us give an example. Consider a $k-$recognizable set $X \subseteq \mathbb{N}$, and let $f : \mathbb{N} \to \mathbb{N}$ map every $n \in \mathbb{N}$ to the least integer m such that all distinct finite factors of W_X of length n occur at least once before position m (this kind of function occurs quite often in the study of combinatorics of infinite words). Then the range of f is $k-$recognizable. In order to prove this, it suffices to show that f is definable in $\langle \mathbb{N}; =, +, X\rangle$, which ensures together with Theorem 20 that (the range of) f is also definable in $\langle \mathbb{N}; =, +, V_k\rangle$, and thus $k-$recognizable by virtue of the same theorem.

Büchi's automata technique for proving decidability led to the notion of *automatic structure*, which was introduced by Hodgson [Hod83]. Consider a relational structure $\mathcal{M} = \langle M; R_1, \ldots, R_k\rangle$, and assume you have a correspondance $c : M \to \Sigma^*$ between elements of the domain M and words over a finite alphabet Σ. The structure is said to be automatic (for c) if $c(M)$, and $c(R_1), \ldots, c(R_k)$, are regular languages (one encodes $n-$tuples in a similar way as before). Under these conditions, one proves that $c(X)$ is regular for every relation $X \subseteq M^n$ definable in $\mathcal{M}$, and that $\mathrm{Th}(\mathcal{M})$ is decidable.

Blumensath and Grädel recently studied a similar notion of automatic structure [BG00].

Let us state now some results about extensions of Büchi arithmetic. Cherlin and Point proved the following [CP86].

Proposition 22. *For every $k \geq 2$ we have*

$$\mathrm{Def}(\mathbb{N}; =, +, V_k, x \mapsto k^x) = \mathrm{Def}(\mathbb{N}; =, +, \times)$$

Proof (sketch). By Theorem 5 it is sufficient to define the set of squares. In order to do this one translates the property *"x is a square"* by the existence of an integer c of the form $c = k^{0^2} + k^{1^2} + k^{2^2} + \cdots + k^{n^2}$, such that the greatest power of k appearing in the $k-$ary expansion of c is equal to k^x. ∎

Note that the theories of $\langle \mathbb{N}; =, +, V_k\rangle$ and $\langle \mathbb{N}; =, +, x \mapsto k^x\rangle$ both are decidable (by Theorems 21 and 17, respectively).

Another related problem is to consider the theory of $\langle \mathbb{N}; =, +, V_k, V_l\rangle$ for $k \neq l$. Note that $\mathrm{Def}(\mathbb{N}; =, +, V_k, V_l)$ is (by Theorem 20) the smallest class of relations over $\mathbb{N}$ which contains both $k-$ and $l-$recognizable relations and which is closed under boolean operations and projection. On one hand Büchi [Buc60] proved that if k and l are multiplicatively dependent (i.e. they have a non-trivial common power) then $k-$ and $l-$recognizability are equivalent, thus the graph of V_l, which is $l-$recognizable, is also $k-$recognizable, therefore it is definable in $\langle \mathbb{N}; =, +, V_k\rangle$ by Theorem 20, which finally implies that $\mathrm{Th}(\mathbb{N}; =, +, V_k, V_l)$ is decidable as it is reducible to the decidable theory $\mathrm{Th}(\mathbb{N}; =, +, V_k)$.

Villemaire proved ([Vil92a], see also [Vil92b]) that the situation is different when one considers multiplicatively independent bases.

Theorem 23. *If $k, l \geq 2$ are multiplicatively independent then multiplication is definable in the structure $\langle \mathbb{N}; +, V_k, V_l\rangle$. Therefore Th$(\mathbb{N}; =, +, V_k, V_l)$ is undecidable.*

We will state below a significant improvement of this theorem.

Logic and Cobham-Semënov theorem.

One of the most striking applications of definability has to do with Cobham-Semenov theorem, which states the base-dependence of the notion of $k-$recognizability.

We mentioned Büchi's result [Buc60] that if k, l are multiplicatively dependent then $k-$recognizability is equivalent to $l-$recognizability. Moreover he proved that an ultimately periodic set is $k-$recognizable for every $k \geq 2$. One can ask whether there are other subsets of $\mathbb{N}$ which are $k-$ and $l-$recognizable for k, l multiplicatively independent. Cobham answers negatively this question in [Cob69].

Theorem 24 (Cobham's theorem). *Let $k, l \geq 2$ be multiplicatively independent integers. Every subset $X \subseteq \mathbb{N}$ which is $k-$ and $l-$recognizable is ultimately periodic.*

Therefore such a X is $m-$recognizable for any $m \geq 2$.

Using Corollary 3 and Theorem 20 we can re-formulate Cobham's Theorem as follows: *if $k, l \geq 2$ are multiplicatively independent, then every subset $X \subseteq \mathbb{N}$ which is definable both in $\langle \mathbb{N}; =, +, V_k \rangle$ and $\langle \mathbb{N}; =, +, V_l \rangle$ is actually definable in $\langle \mathbb{N}; =, + \rangle$.*

Cobham's theorem splits subsets of $\mathbb{N}$ into three categories:

- ultimately periodic subsets, which are $k-$recognizable for every $k \geq 2$;
- subsets which are $k-$recognizable for some $k \geq 2$, and $l-$recognizable only for l multiplicatively dependent with k;
- subsets which are not $k-$recognizable for any $k \geq 2$ (e.g. the set of prime numbers –see [Eil74]– or the set of squares[5]).

Semënov [Sem77] extended Cobham's result to relations of any arity :

Theorem 25 (Cobham-Semënov theorem). *For any $n \geq 1$, and all multiplicatively independent integers $k, l \geq 2$, every subset of $\mathbb{N}^n$ which is $k-$ and $l-$recognizable is definable in $\langle \mathbb{N}; =, + \rangle$.*

Cobham's proof is quite intricate, and Semënov's one very hard to follow. Hansel ([Han82], see [Per90]) gave a simpler combinatorial proof of Cobham's result. Muchnik [Muc91] used the logical characterization of $k-$recognizable sets to give an alternative proof of Cobham-Semënov Theorem. We only state here the main result on which Muchnik's proof rests (see [BHMV94] for a detailed proof). This result is a criterium for definability of subsets of $\mathbb{N}^n$ in $\langle \mathbb{N}; =, + \rangle$, which generalizes in all dimensions the fact that the subsets of $\mathbb{N}$ that are definable in $\langle \mathbb{N}; =, + \rangle$ are ultimately periodic (Corollary 3).

Let $n \geq 1$, and $X \subseteq \mathbb{N}^n$. A *section* of X is a subset of $\mathbb{N}^{n-1}$ of the form

$\{(x_1, \ldots, x_i, x_{i+2}, \ldots, x_n) \ : \ ((x_1, \ldots, x_i, c, x_{i+2}, \ldots, x_n) \in X\}$, for some fixed integer c.

[5] if C was definable in $\langle \mathbb{N}; =, +, V_k \rangle$ for some $k \geq 2$ then $\mathrm{Th}(\mathbb{N}; =, +, C)$, undecidable by Theorem 5, would be reducible to $\mathrm{Th}(\mathbb{N}; =, +, V_k)$, decidable by Theorem 21, which is impossible.

For every $\overrightarrow{x} = (x_1, \ldots, x_n) \in \mathbb{N}^n$, let $||\overrightarrow{x}|| = \max(x_1, \ldots, x_n)$. For $\overrightarrow{x}, \overrightarrow{y} \in \mathbb{N}^n$, we denote by $\overrightarrow{x} + \overrightarrow{y}$ the componentwise addition of $\overrightarrow{x}$ and $\overrightarrow{y}$.

For any $X \subseteq \mathbb{N}^n$ and $\overrightarrow{x} \in \mathbb{N}^n$, let us call *$X-$neighbourhood of $\overrightarrow{x}$ of size m* the set

$$U_X(\overrightarrow{x}, m) = \{\overrightarrow{y} \in \mathbb{N}^n \mid \overrightarrow{x} + \overrightarrow{y} \in X \text{ and } ||\overrightarrow{y}|| \leq m\}.$$

Muchnik proved the following.

Theorem 26. *Let $n \geq 1$ and $X \subseteq \mathbb{N}^n$. The set X is definable in $\langle \mathbb{N}; =, + \rangle$ iff the two following conditions are fulfilled:*

- *every section of X is definable in $\langle \mathbb{N}; =, + \rangle$;*
- *there exists $s \in \mathbb{N}$ such that for every $k \in \mathbb{N}$, there is $l \in \mathbb{N}$ such that for every $\overrightarrow{x} \in \mathbb{N}^n$ satisfying $||\overrightarrow{x}|| > l$, we have*

$$U_X(\overrightarrow{x}, k) = U_X(\overrightarrow{x} + \overrightarrow{t}, k)$$

for some $\overrightarrow{t} \in \mathbb{N}^n$ such that $||\overrightarrow{t}|| < s$.

This result allows to give an alternative proof of the Cobham-Semënov theorem but also implies the following.

Corollary 27 (Muchnik). *The question whether a given $k-$recognizable set $X \subseteq \mathbb{N}^n$ is definable in $\langle \mathbb{N}; =, + \rangle$, is decidable.*

The main idea for the proof, is that the two conditions of Theorem 26 can be expressed as sentences in the language $\{=, +, X\}$ [6]. Note that in case $n = 1$, The first condition vanishes and the second one is equivalent to "X is ultimately periodic", a property which is expressible in $\langle \mathbb{N}; =, +, X \rangle$ (see above). The general case can be proved by induction over n. Finally we get a sentence ϕ in the language $\{=, +, X\}$ such that $\langle \mathbb{N}; =, +, X \rangle$ satisfies ϕ iff X is definable in $\langle \mathbb{N}; =, + \rangle$. Now X is $k-$recognizable, thus by Theorem 20 it is definable in $\langle \mathbb{N}; =, +, V_k \rangle$, and it follows from Corollary 21 that $\mathrm{Th}(\mathbb{N}; =, +, X)$ is decidable. Thus it is decidable whether ϕ holds in $\langle \mathbb{N}; =, +, X \rangle$.

The second alternative proof of the Cobham-Semënov Theorem is due to Michaux and Villemaire [MV93, MV96a]. Their proof also rests on a fine study of definability in Presburger Arithmetic.

Recall that an infinite set $X \subseteq \mathbb{N}$ is said to be *expanding* if the set of differences between consecutive elements of X is infinite. Note that Corollary 3 implies that expanding sets are not definable in $\langle \mathbb{N}; =, + \rangle$.

Michaux and Villemaire proved the following.

Theorem 28. *A set $L \subseteq \mathbb{N}^n$ is definable in $\langle \mathbb{N}; =, + \rangle$ if and only if every subset of $\mathbb{N}$ which is definable in $\langle \mathbb{N}; =, +, L \rangle$ is definable in $\langle \mathbb{N}; =, + \rangle$.*

Or, in other words: *If $L \subseteq \mathbb{N}^n$ is not definable in $\langle \mathbb{N}; =, + \rangle$ then there exists $M \subseteq \mathbb{N}$ which is definable in $\langle \mathbb{N}; =, +, L \rangle$ but not in $\langle \mathbb{N}; =, + \rangle$.*

[6] it is therefore a *definable* criterium for definability in Presburger Arithmetic

Theorem 29. *Let $M \subseteq \mathbb{N}$. If M is not definable in $\langle \mathbb{N}; =, + \rangle$ then there exists an expanding set $M' \subseteq \mathbb{N}$ which is definable in $\langle \mathbb{N}; =, +, M \rangle$.*

Note that the two above results do not involve any automata notion.

In addition Michaux and Villemaire gave an alternative proof of the following useful lemma, which appeared in Hansel's proof [Han82] of Cobham's Theorem.

Lemma 30 ([Han82, MV96a]). *For all multiplicatively independent integers $k, l \geq 2$, if A is $k-$ and $l-$recognizable then A is not expanding.*

Now we can state the Michaux-Villemaire proof of the Cobham-Semënov Theorem.

Proof of the Cobham-Semënov theorem [MV96a]. Suppose there exists $L \subseteq \mathbb{N}^n$ not definable in $\langle \mathbb{N}; =, + \rangle$, and $k-$ and $l-$recognizable for multiplicatively independent integers $k, l \geq 2$.

It follows from Theorem 28 that there exists $M \subseteq \mathbb{N}$ definable in $\langle \mathbb{N}; =, +, L \rangle$ but not definable in $\langle \mathbb{N}; =, + \rangle$. Now Theorem 29 implies the existence of an expanding set $M' \subseteq \mathbb{N}$ definable in $\langle \mathbb{N}; =, +, M \rangle$; this set is *a fortiori* definable in $\langle \mathbb{N}; =, +, L \rangle$. Now L is $k-$ and $l-$recognizable from our very hypothesis, thus L is definable in $\langle \mathbb{N}; =, +, V_k \rangle$ and $\langle \mathbb{N}; =, +, V_l \rangle$ by Theorem 20. It follows that M' is also definable in $\langle \mathbb{N}; =, +, V_k \rangle$ and $\langle \mathbb{N}; =, +, V_l \rangle$, and therefore M' is also $k-$ and $l-$recognizable by virtue of the same Theorem. This contradicts Lemma 30. ∎

We proposed a third alternative proof of the Cobham-Semënov theorem, which uses a decidability argument. It rests on the following improvement of Villemaire's Theorem 23.

Theorem 31 ([Bes97b]). *Let $k, l \geq 2$ be two multiplicatively independent integers . For every $n \geq 1$, if $L \subseteq \mathbb{N}^n$ is $l-$recognizable and not definable in $\langle \mathbb{N}; =, + \rangle$ then $\times$ is definable in $\langle \mathbb{N}; =, +, V_k, L \rangle$. The theory of this structure is therefore undecidable.*

The proof uses Michaux-Villemaire Theorems 28 and 29.

A third proof of the Cobham-Semënov Theorem. Suppose there exists $L \subseteq \mathbb{N}^n$ not definable in $\langle \mathbb{N}; =, + \rangle$, and $k-$ and $l-$recognizable for multiplicatively independent integers $k, l \geq 2$. Then the previous theorem implies that $\mathrm{Th}(\mathbb{N}; =, +, V_k, L)$ is undecidable. Now L is also $k-$recognizable, thus by Theorem 20, $\mathrm{Th}(\mathbb{N}; =, +, V_k, L)$ reduces to $\mathrm{Th}(\mathbb{N}; =, +, V_k)$, which is decidable by Theorem 21, from which we get a contradiction. ∎

Non-classical numeration systems.

Bruyère and Hansel extended Theorem 20 to a class of non-classical numeration systems [BH97]. We describe below their result and refer the reader to [Bru95, Fra85, Fro00] for a nice introduction to numeration systems and links with automata theory.

The $k-$ary numeration system allows to express every integer as a sum of elements of the sequence $(k^n)_{n\in\mathbb{N}}$. One can generalize this idea as follows : let us call *numeration system* any strictly increasing sequence of integers $U = (U_n)_{n\in\mathbb{N}}$ such that $U_0 = 1$ and $\{\frac{U_{n+1}}{U_n} : n \in \mathbb{N}\}$ is bounded. Every positive integer x can be represented as

$$x = a_n U_n + a_{n-1}U_{n-1} + \cdots + a_0 U_0$$

using the Euclidian algorithm: let n be such that $U_n \leq x < U_{n+1}$, and let $x_n = x$. For $i = n, n-1, \ldots, 1$ we compute the Euclidean division $x_i = a_i U_i + x_{i-1}$. Finally we get a word (called *normalized U-representation* of x), $\rho_U(x) = a_n a_{n-1} \ldots a_0$ over the *canonical alphabet* $\Sigma_U = \{0, 1, \ldots, c\}$, where c is the greatest integer less than $\sup\{\frac{U_{n+1}}{U_n} : n \in \mathbb{N}\}$.

A classical example is the Fibonacci numeration system defined by $U_0 = 1, U_1 = 2$ and $U_{n+2} = U_{n+1} + U_n$ for every $n \geq 0$; we have e.g. $14 = U_4 + U_3 + U_0$, that is $\rho_U(14) = 11001$.

One can extend the notion of $k-$recognizability to these numeration systems: let us say that $X \subseteq \mathbb{N}$ is $U-$recognizable if $\rho_U(X)$ is regular (this definition is extended to relations $X \subseteq \mathbb{N}^n$ in a similar way as in the classical case).

One shows for example that for Fibonacci number system, $\rho_U(\mathbb{N})$ is the set of words over $\{0, 1\}$ that do not begin with a 0 and do not contain the factor 11 (it is a regular language).

Some difficulties arise when one deals with non-classical numeration systems. A first observation is that whereas any integer (essentially) admits a single representation in classical numeration systems, this does not hold any longer in the general case. In the Fibonacci numeration system, we have e.g. $14 = U_4 + U_2 + U_1 + U_0$, i.e. the word 10111 is also a representation of the integer 14.

The situation can even be worse, as there exist numeration systems U for which the set $\rho_U(\mathbb{N})$ of all normalized representations of integers is not regular (see [Bru95]) – a quite disturbing situation, when one recalls that one of the essential arguments in the proof of Büchi-Bruyère Theorem is that $\mathbb{N}$ is $k-$recognizable.

From the work of Frougny and Solomyak [FS94] on normalization [7] emerged a class of numeration systems which behave closely to the classical ones: these are the linear numeration systems whose characteristic polynomial is the minimal polynomial of a Pisot number.

Recall that a *linear numeration system* is a numeration system $U = (U_n)_{n\in\mathbb{N}}$ defined by a linear recurrence relation

$$U_n = d_{k-1}U_{n-1} + \cdots + d_0 U_{n-k}$$

for all $n \geq k$, with $d_i \in \mathbb{Z}$ for $i = 0, 1, \ldots, k-1$, and $d_0 \neq 0$. The polynomial

$$P_U(X) = X^k - d_{k-1}X^{k-1} - \cdots - d_1 X - d_0$$

[7] Normalization consists in mapping any word w over an alphabet A to a word $\nu(w)$ over an alphabet B in such a way that w and $\nu(w)$ are representing the same integer. In the Fibonacci numeration system for example (with $A = B = \{0, 1\}$) this function maps 10111 to 11001.

The process of addition can also be seen through normalization. Consider e.g. the classical binary number system. A possibility to compute the sum of 3 and 5 from their respective binary representation 11 and 101 is to work momentaneously with the extended alphabet of digits $\{0, 1, 2\}$, perform an addition digit by digit without carry, here from 011 and 101 we get 112, and then normalize the result, i.e. map 112 to 1000 (this time we have $A = \{0, 1, 2\}$ and $B = \{0, 1\}$).

is called the *characteristic polynomial* of the system U.

A *Pisot number* is an algebraic integer $\theta > 1$ such that the roots of its minimal polynomial, distinct from θ, have modulus less than 1.

As an example, for the Fibonacci numeration system we have $P_U(x) = X^2 - X - 1$, and $\theta = \frac{1+\sqrt{5}}{2}$ (the golden ratio).

Bruyère and Hansel [BH97] proved that Theorem 20 can be extended to the previous class of numeration systems.

For any numeration system $U = (U_n)_{n\in\mathbb{N}}$, one defines the function $V_U : \mathbb{N} \to \mathbb{N}$ as follows: $V_U(0) = 1$, and if $x \geq 1$ then $V_U(x)$ is the least U_i appearing in the normalized $U-$representation of x with a non-zero coefficient.

Theorem 32 (Bruyère, Hansel). *Let U be a linear numeration system whose characteristic polynomial is the minimal polynomial of a Pisot number. For every $n \geq 1$ a set $X \subseteq \mathbb{N}^n$ is $U-$recognizable if and only if X is definable in the structure $\langle \mathbb{N}; =, +, V_U \rangle$.*

One of the main arguments that allow the authors to adapt Büchi's proof is that both $\mathbb{N}$ and the graph of $+$ are $U-$recognizable under those conditions over U.[8]

Corollary 33. *Under the previous assumptions the theory of $\langle \mathbb{N}; =, +, V_U \rangle$ is decidable.*

There have been many attempts to generalize the Cobham-Semënov theorem to non-classical numeration systems – see [Fab94], [PB97], [Dur98], [Fagn00], [Han98], [Bes00]. The three last references use Theorem 32, together with the very general theorems 28 and 29. Indeed Michaux-Villemaire results are independent of any notion of recognizability, and therefore can be used again in this context: while Theorem 28 allows to reduce the case of relations over $\mathbb{N}$ to the case of subsets of $\mathbb{N}$ (i.e. "Semënov's part" to "Cobham's part"), Theorem 29 reduces then the difficulty to the case of expanding subsets of $\mathbb{N}$.

2.6 Notes

• *Pascal triangles modulo n.* Korec studied theories of structures $\langle \mathbb{N}; =, +, B_n \rangle$, where $B_n(x, y)$ equals the remainder modulo n of the binomial coefficient $\binom{x+y}{x}$. In [Kor95] it is shown that $\langle \mathbb{N}; =, +, B_n \rangle$ is decidable whenever n is prime. The proof proceeds by interpretation into WS1S, and uses Lucas' theorem (1861): for p prime, if $x = \sum_{i=0}^{t} x_i p^i$ and $z = \sum_{i=0}^{t} z_i p^i$, then

$$\binom{z}{x} \equiv \prod_{i=0}^{t} \binom{z_i}{x_i} \pmod{p}$$

(in fact Lucas' theorem essentially tells that the graph of B_p is $p-$recognizable). In [Bes97a] it is shown that Korec's result still holds in case n is a prime power; however [Kor93] shows that $+$ and $\times$ are definable in $\langle \mathbb{N}; =, B_n \rangle$ if n is not a prime power (e.g. $\mathrm{Def}(\mathbb{N}; =, B_6) = \mathrm{Def}(\mathbb{N}; =, +, \times)$).

[8] Bruyère and Hansel prove these two facts in a direct way; note they are also consequences of Frougny-Solomyak results [FS94].

• For recent developments in the study of almost-periodic words and decidability we refer to [Mae98] and [Mae00a].

• *Around Theorem 28.* Let us say that a structure $\mathcal{M} = \langle M; \mathcal{L} \rangle$ has the *1-witness property* if the following holds:

for every $n \geq 1$, a relation $X \subseteq M^n$ is definable in $\mathcal{M}$ iff every set $Y \subseteq M$ which is definable in $\langle M; \mathcal{L}, X \rangle$ is definable in $\mathcal{M}$.

Theorem 28 simply expresses that Presburger Arithmetic has the 1-witness property. It can be shown that $\langle \mathbb{N}; =, +, \times \rangle$, as well as $\langle \mathbb{N}; < \rangle$, enjoy this property, while $\langle \mathbb{N}; =, S \rangle$ does not [9] . Let us consider now a stronger property, namely the *1-encoding* property. We say that $\mathcal{M} = \langle M; \mathcal{L} \rangle$ has the *1-encoding property* if for every $X \subseteq M^n$ there exists some $Y \subseteq M$ such that $\mathrm{Def}(M; \mathcal{L}, X) = \mathrm{Def}(M; \mathcal{L}, Y)$. Observe that if $\mathrm{Def}(M; \mathcal{L}) \subseteq \mathrm{Def}(M; \mathcal{L}')$ and $\langle M; \mathcal{L} \rangle$ has the 1-encoding property then $\langle M; \mathcal{L}' \rangle$ does. The structures $\langle \mathbb{N}; =, +, \times \rangle$ and $\langle \mathbb{N}; =, +, x \mapsto 2^x \rangle$ have the 1-encoding property (easy), while one proves that $\langle \mathbb{N}; < \rangle$ does not[10]. Michaux and Villemaire ask in [MV96b] whether $\langle \mathbb{N}; =, + \rangle$ has the 1-encoding property.

Applications of Theorem 28 to $o-$minimality can be found in [PW00], [BPW00].

• *Extensions of* $\langle \mathbb{N}; =, +, V_k \rangle$. The function which maps any finite set $X \subseteq \mathbb{N}$ to $\sum_{i \in X} 2^i$ allows to transfer any (un)decidability result for the weak monadic second-order theory of $\langle \mathbb{N}; =, S, R \rangle$ (where R is a predicate of arity k) to the first-order theory of

$\langle \mathbb{N}; +, V_2, \{(2^{n_1}, \ldots, 2^{n_k}) : (n_1, \ldots, n_k) \in R\}, = \rangle$. As an example from the decidability of the weak monadic second-order theory of $\langle \mathbb{N}; =, S, \{n! : n \in \mathbb{N}\} \rangle$ (due to Elgot and Rabin [ER66]) one can derive decidability for the first-order theory of $\langle \mathbb{N}; =, +, V_2, \{2^{n!} : n \in \mathbb{N}\} \rangle$.

Both Theorems 23 and 31 involve a Thomas' result [Tho76] about weak monadic second-order theories of $\langle \mathbb{N}; =, S, f \rangle$, where f denotes a unary function.

• The question (attributed to Van den Dries) of whether $\mathrm{Th}(\mathbb{N}; =, +, P_2, P_3)$ is decidable is still open. From Theorems 21 and 31 we can infer, on one hand, decidability of $\mathrm{Th}(\mathbb{N}; =, +, P_2)$ and $\mathrm{Th}(\mathbb{N}; =, +, P_3)$, on the other hand undecidability of $\mathrm{Th}(\mathbb{N}; =, +, V_2, P_3)$.

3 Skolem Arithmetic and extensions

We now consider the multiplicative theory of integers, which is usually called *Skolem arithmetic*, and its extensions.

Skolem claimed decidability for the theory of $\langle \mathbb{N}; \times, = \rangle$ in [Sko30], using quantifier elimination technique; however the paper provided some examples but no real proof. The first decidability proof appeared in Mostowski's work [Mos52] on products of theories. It rests on the notion of weak (direct) power of a structure, which allows the reduction of $\mathrm{Th}(\mathbb{N}; \times, =)$ to $\mathrm{Th}(\mathbb{N}; +, =)$. Alternative proofs were proposed later by Cegielski who axiomatized the theory and proved quantifier elimi-

[9] $<$ is not definable in $\langle \mathbb{N}; =, S \rangle$, but every subset of $\mathbb{N}$ which is definable in $\langle \mathbb{N}; =, S, < \rangle$ is actually definable in $\langle \mathbb{N}; =, S \rangle$ –both structures define only finite or co-finite subsets of $\mathbb{N}$, see [End72].

[10] Note that $\mathrm{Th}(\mathbb{N}; +, x \mapsto 2^x)$ is decidable by Theorem 17.

nation ([Ceg81], see also [Smo91]), and by Hodgson using a mix of automata and weak powers [Hod82] (we follow a similar viewpoint in paragraph 3.3). We focus here on Mostowski's approach (first paragraph) as it introduces key notions for the subsequent study of decidable extensions of Skolem arithmetic.

In the fifties, the study of the decision problem for the theory of ordinal addition led Feferman and Vaught [FV59] to introduce a notion of generalized product of theories extending Mostowski's one. The results (often called *composition theorems* now), while not leading their authors to the solution of the original problem[11], provide however a very helpful method for proving decidability. In our context, they allow to deal with extensions of Skolem arithmetic for which Mostowski's method seem to fail. Feferman and Vaught gave an example in their original paper by proving decidability for $\mathrm{Th}(\mathbb{N}; \times, =, \sim)$, where $x \sim y$ hold iff x and y have the same number of distinct prime divisors. As shown by Maurin [Mau97], the method also applies to $\mathrm{Th}(\mathbb{N}; \times, =, <_P)$, where $<_P$ denotes order relation restricted to prime numbers. These results are detailed in the second paragraph.

In the next one, we stay with $\langle \mathbb{N}; \times, =, <_P \rangle$ and give an alternative (and simpler) proof of decidability for the theory, using the automata techniques that were introduced in the previous section.

In the final paragraph we turn to undecidable extensions of Skolem arithmetic. We recall the easy cases of $\langle \mathbb{N}; \times, S, = \rangle$ and $\langle \mathbb{N}; \times, <, = \rangle$, then detail Korec's proof for $\langle \mathbb{N}; \times, \mathrm{Neib}, = \rangle$, where $\mathrm{Neib}(x, y)$ holds iff $|x - y| = 1$.

We then state results of Cegielski, Matiyasevich and Richard for structures $\langle \mathbb{N}; \times, =, p \rangle$ where p denotes any injection from $\mathbb{N}$ to the set P of prime numbers. Finally we answer Maurin's question about the structure $\langle \mathbb{N}; =, \times, <_\Pi \rangle$, where Π denotes the order relation restricted to primary numbers.

Remark. All decidability results mentioned in this section about $\mathrm{Th}(\mathbb{N} \setminus \{0\}; \dots)$ still hold if we replace the domain $\mathbb{N} \setminus \{0\}$ by $\mathbb{N}$. They still hold too if we add to the language a constant symbol for each $n \in \mathbb{N}$ (note that an automorphism argument shows that the only definable constants in $\langle \mathbb{N}; \times, = \rangle$ are 0 and 1).

3.1 Skolem Arithmetic

We recall in this paragraph Mostowski's proof [Mos52] of decidability of $\mathrm{Th}(\mathbb{N} \setminus \{0\}; \times, =)$. It relies on the notion of *weak power* of a structure, which allows to reduce the decidability question for $\mathrm{Th}(\mathbb{N} \setminus \{0\}; =, \times, 1)$ to the one for $\mathrm{Th}(\mathbb{N}; =, +)$.

Let A be a nonempty set, and let $e \in A$. We denote by $S^+(\mathbb{N})$ (respectively $S^*(\mathbb{N})$) the set of finite (resp. finite or cofinite) subsets of $\mathbb{N}$. We denote by $A_e^{(\mathbb{N})}$ the set of functions $f : \mathbb{N} \to A$ such that $\{n \in \mathbb{N} \ : \ f(n) \neq e\}$ is finite.

Definition 34. *Let $\mathcal{A} = \langle A; \mathcal{R}_A, e \rangle$, be a structure in the language $\mathcal{L}_A = \{\mathcal{R}_A, e\}$ where e is a constant and $\mathcal{R}_A = \{R_1, \dots, R_k\}$ is a finite set of relations over A ($\mathcal{A}$ is the "factor structure"). The* weak power *of $\mathcal{A}$ is the structure $\mathcal{A}^* = \langle A_e^{(\mathbb{N})}, R_1^*, \dots, R_k^*, f \rangle$ where*

- *f is the element of $A_e^{(\mathbb{N})}$ s.t. for every $i \in \mathbb{N}$, $f(i) = e$;*

[11] The decidability of the theory of ordinal addition was proved by Büchi [Buc65] using automata techniques.

- *for every $i \in \{1, 2, \ldots, k\}$, if a_i denotes the arity of R_i, then for every a_i-tuple $(f_1, \ldots, f_{a_i})$ of elements of $A_e^{(\mathbb{N})}$,*

$$\mathcal{A}^* \models R_i^*(f_1, \ldots, f_{a_i})$$

iff

$$\text{for every } n \in \mathbb{N}, \quad \mathcal{A} \models R_i(f_1(n), \ldots, f_{a_i}(n)).$$

The main result of [Mos52] for our purpose is the following one.

Theorem 35. *If Th($\mathcal{A}$) is decidable then so is Th($\mathcal{A}^*$).*

Let us note that Mostowski's proof of this result rests on the decidability of the theory of $\langle S^*(\mathbb{N}); \subseteq\rangle$, the "index structure". We shall consider this structure with more attention in the next paragraph.

Let $+_g$ and $\times_g$ respectively denote the graph of addition and multiplication (over $\mathbb{N}$).

As an application of the previous theorem, Mostowski considers Skolem arithmetic and proves the following.

Theorem 36. *The theory of $\langle \mathbb{N} \setminus \{0\}; \times, =\rangle$ is decidable.*

Proof. The decision problem for $\mathrm{Th}(\mathbb{N} \setminus \{0\}; \times, =)$ obviously reduces to the one for $\mathrm{Th}(\mathbb{N} \setminus \{0\}; \times_g, 1)$. Now consider the function $\psi : \mathbb{N} \setminus \{0\} \to \mathbb{N}_0^{(\mathbb{N})}$ which maps every positive integer x to the function $f_x : \mathbb{N} \to \mathbb{N}$ such that $f_x(n)$ is the exponent of the $n-$th prime in the decomposition of x as a product of prime factors. It is quite easy to check that ψ is one-one and induces an isomorphism between $\langle \mathbb{N} \setminus \{0\}; \times_g, 1\rangle$ and the weak power of $\langle \mathbb{N}; +_g, 0\rangle$. Now $\mathrm{Th}(\mathbb{N}; +_g, 0)$ is decidable as it reduces to $\mathrm{Th}(\mathbb{N}; =, +)$ (Theorem 2), which together with Theorem 35 gives the required result. ∎

We add a word on complexity: J.Ferrante and C.Rackoff proved in [FeRa79] that a lower complexity bound for deciding the truth of a sentence of length n in $\langle \mathbb{N} \setminus \{0\}; \times, =\rangle$ is $2^{2^{2^{cn}}}$ for some constant c, to be compared with the lower bound $2^{2^{cn}}$ for Presburger arithmetic given by Fischer and Rabin [FiRa74].

3.2 The Feferman-Vaught technique

We now describe Feferman-Vaught notion of generalized weak power of a structure [FV59], and its application to extensions of Skolem arithmetic.

Mostowski's notion of weak power involves the factor "structure" $\mathcal{A}$ and the "index structure" $\langle S^*(\mathbb{N}); \subseteq\rangle$. Feferman and Vaught generalize this idea by allowing a more general kind of composition that may use extensions of $\langle S^*(\mathbb{N}); \subseteq\rangle$. In case this extended "index structure", as well as the "factor structure", have a decidable theory, then the structure resulting from the composition has a decidable theory too. This will allow to construct extensions of Skolem arithmetic by composing $\langle \mathbb{N}; +_g, 0\rangle$ "through" decidable extensions of $\langle S^*(\mathbb{N}); \subseteq\rangle$.

Let us now state precisely the above notions and results. We keep the notations of the previous paragraph.

Let $\mathcal{A} = \langle A; \mathcal{R}_A, e\rangle$, be a structure in the language $\mathcal{L}_A = \{\mathcal{R}_A, e\}$ where e is a constant and $\mathcal{R}_A$ is a finite set of relations over A.

Let $\mathcal{B} = \langle S^*(\mathbb{N}); \subseteq, \mathrm{FIN}, \mathcal{R}_B\rangle$ be a structure in the language $\mathcal{L}_B = \{\subseteq, \mathrm{FIN}, \mathcal{R}_B\}$, where $\subseteq$ and FIN are interpreted respectively as the inclusion relation and the relation "to be a finite set", and $\mathcal{R}_B$ is a set of relations over $S^*(\mathbb{N})$.

Definition 37. *Let R be a $k-$ary relation over $A_e^{(\mathbb{N})}$; we say that R is accessible in $(\mathcal{A}, \mathcal{B})$ if and only if there exist a $\mathcal{L}_B$-formula $G(X_1, \ldots, X_l)$, and l $\mathcal{L}_A$-formulas with k free variables $F_1, \ldots, F_l$ such that for every k-tuple $(f_1, \ldots, f_k)$ of elements of $A_e^{(\mathbb{N})}$, $R(f_1, \ldots, f_k)$ holds if and only if*

$$\mathcal{B} \models G(T_1, \ldots, T_l)$$

where

$$T_i = \Big\{x \in \mathbb{N} : \mathcal{A} \models F_i(f_1(x), \ldots, f_k(x))\} \quad \text{for every} \quad i \in \{1, \ldots, l\Big\}.$$

Example 2. Take $\mathcal{A} = \langle \mathbb{N}; +_g, 0\rangle$ and $\mathcal{B} = \langle S^*(\mathbb{N}); \subseteq, \mathrm{FIN}\rangle$ (i.e. $\mathcal{R}_B$ is empty). Let M be the ternary relation on $\mathbb{N}_0^{(\mathbb{N})}$ defined by

$$M = \{(f, g, h) : \ f(n) + g(n) = h(n) \quad \text{for every } n \in \mathbb{N}\}.$$

This relation is accessible in $(\mathcal{A}, \mathcal{B})$: indeed $M(f, g, h)$ holds iff the set $\{n : f(n) + g(n) \neq h(n)\}$ is empty, or in other words iff

$$\langle S^*(\mathbb{N}); \subseteq, \mathrm{FIN}\rangle \models \ \forall X \ T \subseteq X$$

where

$$T = \{x \in \mathbb{N} : \langle \mathbb{N}; +_g, 0\rangle \models \neg(+_g(f(x), g(x), h(x)))\}.$$

Definition 38. *With the above notations, if $\mathcal{R}$ is a set of relations over $A_e^{(\mathbb{N})}$, we say that the structure $\langle A_e^{(\mathbb{N})}; \mathcal{R}\rangle$ is a generalized weak power of $\mathcal{A}$ relative to $\mathcal{B}$ if every relation of $\mathcal{R}$ is accessible in $(\mathcal{A}, \mathcal{B})$* [12] *.*

Example 2 (continued) : The structure $\langle \mathbb{N}_0^{(\mathbb{N})}; T\rangle$ is a weak generalized power of $\langle \mathbb{N}; +_g, 0\rangle$ relative to $\langle S^*(\mathbb{N}); \subseteq, \mathrm{FIN}\rangle$.

Mostowski's notion of weak power corresponds to the case $\mathcal{B} = \langle S^*(\mathbb{N}); \subseteq, \mathrm{FIN}\rangle$, i.e. to the simplest index structure.

Theorem 39 ([FV59]). *(i) With the above notations, if Th($\mathcal{A}$) and Th($\mathcal{B}$) are decidable and $\mathcal{C}$ is a generalized weak power of $\mathcal{A}$ relative to $\mathcal{B}$ then the elementary theory of $\mathcal{C}$ is decidable.*

(ii) The decision problem for Th($\mathcal{B}$) reduces to the one for Th($S^+(\mathbb{N}); \subseteq, \mathcal{R}'_B$), where $\mathcal{R}'_B$ consists in all relations of $\mathcal{R}_B$ restricted to $S^+(\mathbb{N})$.

[12] Feferman-Vaught' original definition allows any set B in place of $\mathbb{N}$. Moreover they define *the* generalized weak power of $\mathcal{A}$ relative to $\mathcal{B}$ as the structure $\langle A_e^{(B)}; \mathcal{R}\rangle$ where $\mathcal{R}$ denotes the set of *all* accessible relations.

As an example Feferman and Vaught prove the following.

Proposition 40. *The structure* $\langle \mathbb{N} \setminus \{0\}; \times_g, \sim \rangle$ *where* $x \sim y$ *holds iff* x *and* y *have the same number of distinct prime factors, is isomorphic with a generalized weak power of* $\langle \mathbb{N}; +_g, 0 \rangle$ *relative to* $\langle S^*(\mathbb{N}); \subseteq, \mathrm{FIN}, \approx \rangle$*, where* $X \approx Y$ *holds iff* X, Y *are finite and* $\sharp X = \sharp Y$*.*

Proof. Consider again the function $\psi : \mathbb{N} \setminus \{0\} \to \mathbb{N}_0^{(\mathbb{N})}$ defined in the proof of Theorem 36. This function is one-one and induces an isomorphism between $\langle \mathbb{N} \setminus \{0\}; \times_g, \sim \rangle$ and $\langle \mathbb{N}_0^{(\mathbb{N})}; M, E \rangle$, where $M(f, g, h)$ holds iff $f(n) + g(n) = h(n)$ for every $n \in \mathbb{N}$, and $E(f, g)$ holds iff

$$\sharp\{n : f(n) \neq 0\} = \sharp\{n : g(n) \neq 0\}.$$

We only have to show that M and E are accessible in $(\langle \mathbb{N}; +_g, 0 \rangle, \langle S^*(\mathbb{N}); \subseteq, \mathrm{FIN}, \approx \rangle)$.

The case of M is treated in Example 2. Moreoever $E(f, g)$ holds iff

$$\langle S^*(\mathbb{N}); \subseteq, \mathrm{FIN}, \approx \rangle \models\ X \approx Y$$

where

$$X = \{x \in \mathbb{N} : \langle \mathbb{N}; +_g, 0 \rangle \models \neg(+_g(f(x), 0, 0))\}$$

and

$$Y = \{x \in \mathbb{N} : \langle \mathbb{N}; +_g, 0 \rangle \models \neg(+_g(g(x), 0, 0))\}.$$

■

Theorem 41. *The theory of* $\langle \mathbb{N} \setminus \{0\}; \times, \sim, = \rangle$ *is decidable.*

Proof (main ideas). The theory of $\langle \mathbb{N} \setminus \{0\}; \times, \sim, = \rangle$ clearly reduces to the one of $\langle \mathbb{N} \setminus \{0\}; \times_g, \sim \rangle$. Thus by Proposition 40 and Theorem 39 we only have to show that $\langle \mathbb{N}; +_g, 0 \rangle$ and $\langle S^+(\mathbb{N}); \subseteq, \approx \rangle$ have decidable theories.

For $\langle \mathbb{N}; +_g, 0 \rangle$, one uses (again) the reduction to Presburger arithmetic. One shows that $\mathrm{Th}(S^+(\mathbb{N}); \subseteq, \approx)$ also reduces to Presburger arithmetic. The main idea is the following: to every $\{\subseteq, \approx\}-$formula φ with n free variables one associates a $\{+, =\}-$formula φ^* with $2^n - 1$ variables such that for all finite sets $X_1, \ldots, X_n \subseteq \mathbb{N}$,

$$\langle S^+(\mathbb{N}); \subseteq, \approx \rangle \models \varphi(X_1, \ldots, X_n) \Longleftrightarrow \langle \mathbb{N}; +, = \rangle \models \varphi^*(x_1, \ldots, x_{2^n})$$

where each x_i corresponds to an integer of the form

$$\sharp\Big(\bigcap_{j \in J} X_j \cap \bigcap_{k \in K} \overline{X_k} \Big)$$

for a partition (J, K) of $\{1, 2, \ldots, n\}$, with $J \neq \emptyset$.

■

The second example of decidable extension of Skolem arithmetic obtained with the Feferman-Vaught technique was given by Maurin [Mau97], who proved the decidability of the theory of $\langle \mathbb{N} \setminus \{0\}; =, \times, <_P \rangle$, where $<_P$ denotes the usual order relation restricted to prime numbers. We will see in paragraph 3.4 that on the other hand $\mathrm{Th}(\mathbb{N}; \times, =, <)$ is undecidable.

Lemma 42. *The structure* $\langle \mathbb{N} \setminus \{0\}; \times_g, <_P \rangle$ *is isomorphic to a weak generalized power of* $\langle \mathbb{N}; +_g, 0 \rangle$ *relative to* $\langle S^*(\mathbb{N}); \subseteq, \mathrm{FIN}, \ll \rangle$*, where* $X \ll Y$ *iff* $X = \{x\}$*,* $Y = \{y\}$*, with* $x < y$*.*

Proof. Consider again the function $\psi : \mathbb{N} \setminus \{0\} \to \mathbb{N}_0^{(\mathbb{N})}$ defined in the proof of Theorem 36, which induces an isomorphism between $\langle \mathbb{N} \setminus \{0\}; \times_g, <_P \rangle$ and $\langle \mathbb{N}_0^{(\mathbb{N})}; M, L \rangle$, where

- $M(f, g, h)$ holds iff $f(n) + g(n) = h(n)$ for every $n \in \mathbb{N}$
- $L(f, g)$ holds iff there exist $n_1, n_2 \in \mathbb{N}$ such that
  - $n_1 < n_2$
  - $f(n_1) = g(n_2) = 1$
  - $f(n) = 0$ whenever $n \neq n_1$
  - $g(n) = 0$ whenever $n \neq n_2$.

We have to show that M and L are accessible in $(\langle \mathbb{N}; +_g, 0 \rangle, \langle S^*(\mathbb{N}); \subseteq, \mathrm{FIN}, \ll \rangle)$. The case of M is treated in Example 2.

For L, one checks that $L(f, g)$ holds iff

$$\langle S^*(\mathbb{N}); \subseteq, \mathrm{FIN}, \ll \rangle \models \exists X(T_1 \ll X) \wedge \exists Y(T_2 \ll Y) \wedge T_3 \ll T_4$$

where

$$T_1 = \{x \in \mathbb{N} : \langle \mathbb{N}; +_g, 0 \rangle \models \neg(+_g(f(x), 0, 0))\},$$
$$T_2 = \{x \in \mathbb{N} : \langle \mathbb{N}; +_g, 0 \rangle \models \neg(+_g(g(x), 0, 0))\},$$
$$T_3 = \{x \in \mathbb{N} : \langle \mathbb{N}; +_g, 0 \rangle \models +_g(f(x), 0, 1)),$$

and

$$T_4 = \{x \in \mathbb{N} : \langle \mathbb{N}; +_g, 0 \rangle \models +_g(g(x), 0, 1))$$

(we abusively use the constant 1 to simplify formulas, this constant is definable in $\langle \mathbb{N}; +_g, 0 \rangle$).

The first part of the above formula , "$\exists X(T_1 \ll X) \wedge \exists Y(T_2 \ll Y)$" simply expresses that T_1 and T_2 are singletons. ∎

Theorem 43. *The elementary theory of* $\langle \mathbb{N} \setminus \{0\}; =, \times, <_P \rangle$ *is decidable.*

Proof. The theory of $\langle \mathbb{N} \setminus \{0\}; \times, =, <_P \rangle$ clearly reduces to the one of $\langle \mathbb{N} \setminus \{0\}; \times_g, <_P \rangle$. Thus by Proposition 40 and Theorem 39 we only have to show that $\langle \mathbb{N}; +_g, 0 \rangle$ and $\langle S^+(\mathbb{N}); \subseteq, \ll \rangle$ have decidable theories.

For $\langle \mathbb{N}; +_g, 0 \rangle$, one uses reduction to Presburger arithmetic.

Let us show that $\mathrm{Th}(S^+(\mathbb{N}); \subseteq, \ll)$ reduces to $\mathrm{Th}(\mathbb{N}; =, +, V_2)$, which together with Theorem 21 yields the result. Consider the function $h : S^+(\mathbb{N}) \to \mathbb{N}$ which maps every finite set $X \subseteq \mathbb{N}$ to $h(X) = \sum_{i \in X} 2^i$; h is one-one, thus there are binary relations $\subseteq^*$ and $\ll^*$ such that

$$\langle S^+(\mathbb{N}); \subseteq, \ll \rangle \cong \langle \mathbb{N}; \subseteq^*, \ll^* \rangle$$

Now $\subseteq^*$ and $\ll^*$ are 2−recognizable; indeed we have

$$[\subseteq^*]_2 = A^* \setminus \left(\binom{0}{0} A^* \cup A^* \binom{1}{0} A^* \right)$$

where $A = \left\{ \binom{0}{0}, \binom{0}{1}, \binom{1}{0}, \binom{1}{1} \right\}$ and

$$[\ll^*]_2 = \binom{0}{1} \binom{0}{0}^* \binom{1}{0} \binom{0}{0}^*.$$

Thus by Theorem 20 these relations are definable in $\langle \mathbb{N}; =, +, V_2 \rangle$. This shows that $\mathrm{Th}(\mathbb{N}; \subseteq^*, \ll^*)$ reduces to $\mathrm{Th}(\mathbb{N}; =, +, V_2)$. ∎

In the next paragraph we propose an alternative proof of the previous theorem which emphasizes the "automata flavour" of the above proof.

Let us mention that Maurin specified the previous decidability result by showing that a lower complexity bound for deciding the truth of a sentence of length n is a tower of exponentials of height cn, for some constant c [Mau97], i.e. it is not elementary – recall that the lower bound for $\langle \mathbb{N}; \times, = \rangle$ "only" involves a triple exponential.

One can ask whether Maurin's result still holds if we replace $<_P$ by some "more expressive" fragment of order relation. In particular Maurin asked whether the same holds for the order $<_\Pi$ restricted to primary numbers; it is quite easy to check that

$$\mathrm{Def}(\mathbb{N} \setminus \{0\}; =, \times, <_P) \subseteq \mathrm{Def}(\mathbb{N} \setminus \{0\}; =, \times, <_\Pi).$$

We will show in paragraph 3.4 that replacing $<_P$ by $<_\Pi$ yields undecidability.

3.3 Revisiting Skolem arithmetic via automata theory

The "automata techniques" of the previous section allow to give an alternative proof of Theorem 43. Let us explain the main ideas. As we did for $\langle \mathbb{N}; =, +, V_k \rangle$ we first need to encode integers, and n−tuples of integers, as words over finite alphabets.

we define $c : \mathbb{N} \setminus \{0\} \to \{0, 1, \square\}^*$ as follows:

- $c(1) = \lambda$;
- if $n \neq 1$ then n can be written as $n = \prod_{i=0}^{k} \pi(i)^{f_n(i)}$ with $f_n(k) \neq 0$. Then we set $c(n) = [f_0(n)]_2 \square [f_1(n)]_2 \square \ldots \square [f_k(n)]_2$ (recall that $[\alpha]_2$ is the word over the alphabet $\{0, 1\}$ naturally associated with the binary expansion of α – see paragraph 2.5)

For example we have $c(2^5 3^3) = 101\square 11$, and $c(2^2 7^6) = 10\square\square\square 110$.

We can extend our definition of c to allow encoding of tuples: given a $k-$tuple $(n_1, \ldots, n_k)$ of integers, set

$$c((n_1, \ldots, n_k)) = w_0 \begin{pmatrix} \square \\ \vdots \\ \square \end{pmatrix} w_1 \begin{pmatrix} \square \\ \vdots \\ \square \end{pmatrix} \ldots \begin{pmatrix} \square \\ \vdots \\ \square \end{pmatrix} w_t$$

where $\begin{pmatrix} \square \\ \vdots \\ \square \end{pmatrix}$ is obtained by stacking k letters $\square$,

$$w_i = [(f_{n_1}(i), \ldots, f_{n_k}(i))]_2, \quad i = 0, 1, \ldots, t$$

and $(f_{n_1}(t), \ldots, f_{n_k}(t)) \neq (0, \ldots, 0)$. Moreover set $c((0, \ldots, 0))$ as the empty word. As an example, we have

$$c((2^5 3^3, 2^2 7^6)) = \binom{1}{0}\binom{0}{1}\binom{1}{0}\binom{\square}{\square}\binom{1}{0}\binom{1}{0}\binom{\square}{\square}\binom{\square}{\square}\binom{0}{1}\binom{0}{1}\binom{0}{0}$$

Lemma 44. *For every $n \geq 1$, if $M \subseteq (\mathbb{N} \setminus \{0\})^n$ is definable in $\langle \mathbb{N} \setminus \{0\}; \times, <_P \rangle$ then c(M) is regular.*

Proof (sketch). By induction on the number of quantifiers of a prenex formula which defines M. The main difficulty is to initialize induction, which can be done by showing that the images of $\mathbb{N} \setminus \{0\}$, $\times_g$ and $<_P$ by c are regular languages (observe that $\mathrm{Def}(\mathbb{N} \setminus \{0\}; =, \times, <_P)$ $=\mathrm{Def}(\mathbb{N} \setminus \{0\}; \times_g, <_P)$).

- $c(\mathbb{N} \setminus \{0\})$ is regular since

  $$c(\mathbb{N} \setminus \{0\}) = B^* \setminus (0B^* \cup B^*\square \cup B^*\square 0B^*)$$

  with $B = \{0, 1, \square\}$.

- $c(\{(x, y, z) : \times_g(x, y, z)\})$ is also regular: the required finite automaton essentially checks correctness of binary addition between each block of $\begin{pmatrix} \square \\ \square \\ \square \end{pmatrix}$.

- the set $c(\{(x, y) : x <_P y\})$ is regular, since

  $$c(\{(x, y) : x <_P y\}) = \binom{\square}{\square}^* \binom{1}{0}\binom{\square}{\square}\binom{\square}{\square}^* \binom{0}{1}.$$

■

The above lemma expresses that the structure $\langle \mathbb{N} \setminus \{0\}; \times, <_P \rangle$ is *automatic* in the sense of Hodgson. Decidability of the theory then follows (like Büchi Arithmetic) from the fact that the decision problem for sentences reduces to the emptiness problem for finite automata, which is decidable by Kleene.

Note that the above ideas are very close to the ones used by Hodgson in [Hod82] where he proves that automaticity of structures is preserved under weak direct product.

3.4 Undecidable extensions of $\langle \mathbb{N}; =, \times \rangle$

Starting from the (undecidable) theory of $\langle \mathbb{N}; =, \times, + \rangle$ one can replace $+$ by "weaker" relations or functions. Two natural candidates are the order relation $<$ and the successor function S; note that we have

$$\mathrm{Def}(\mathbb{N}; S, =) \subseteq \mathrm{Def}(\mathbb{N}; <, =) \subseteq \mathrm{Def}(\mathbb{N}; +, =)$$

(indeed an automorphism argument shows that strict inclusions hold).

The following result is due to J.Robinson [Rob49].

Proposition 45. $\mathrm{Def}(\mathbb{N}; =, \times, S) = \mathrm{Def}(\mathbb{N}; =, \times, <) = \mathrm{Def}(\mathbb{N}; =, \times, +)$.

Proof. Since successor function is definable in $\langle \mathbb{N}; < \rangle$, and $<$ is in turn definable in $\langle \mathbb{N}; =, + \rangle$, it is sufficient to show that $+$ is definable in $\langle \mathbb{N}; =, \times, S \rangle$. This comes from the so-called *Tarski's identity*: for all $x, y, z \in \mathbb{N}$,

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

The right term of this equivalence can easily be expressed in terms of $\times$ and S. ∎

The previous proposition has been sharpened by Korec [Kor96] (recall that $\mathrm{Neib}(x, y)$ means $|x - y| = 1$).

Proposition 46. $\mathrm{Def}(\mathbb{N}; =, \mathrm{Neib}, \times) = \mathrm{Def}(\mathbb{N}; =, +, \times)$.

This result was needed in the proof of Theorem 7.

Proof. Note first that every integer is definable in the structure. We shall therefore freely use constants in the defining formulas.

The main idea is to use Tarski's identity to define a relation close to $+_g$, and then define $+$.

Consider the formula $\psi(x, y, z)$:

$$[z \neq 0 \wedge \exists u, v, w(\mathrm{Neib}(4xz, u) \wedge \mathrm{Neib}(4yz, v) \wedge \mathrm{Neib}(4xy, w) \wedge \mathrm{Neib}(uv, 4z^2 w)]$$

$$\vee [z = 0 \wedge x = y]$$

We shall show that ψ defines the relation $R = \{(x, y, z) : \ x + y = z \ \text{ or } \ |x - y| = z\}$.

Indeed assume that $\psi(x, y, z)$ holds. The case $z = 0$ is obvious. Now if $z \neq 0$, then we have

$$u = 4xz \pm 1, \quad v = 4yz \pm 1, \quad w = 4xy \pm 1, \quad uv = 4z^2 w \pm 1$$

that is,

$$16xyz^2 \pm 4xz \pm 4yz \pm 1 = 16xyz^2 \pm 4z^2 \pm 1.$$

The last signs in both sides must coincide due to the congruence modulo 4. Thus after simplification we get $|x \pm y| = z$, that is $(x, y, z) \in R$.

Conversely if $(x, y, z) \in R$ then for $z \neq 0$ (the case $z = 0$ is obvious) we have

- if $z = x + y$ then $\psi(x, y, z)$ holds for the values $u = 4xz + 1, v = 4yz + 1, w = 4xy + 1$;

- if $z = x - y$, with $x \geq y$ w.l.o.g., then convenient values are $u = xz - 1, v = 4yz + 1, w = xy + 1$.

Let us now define the congruence classes modulo 4. We use the notation $x \equiv_4 i$ (for $0 \leq i < 4$). We can already define $x \equiv_4 0$ and $x \equiv_4 2$ by the formulas $\exists y(x = 4y)$ and $\exists y, z(\text{Neib}(2y, z) \wedge x = 2z)$, respectively.

For the two other congruence classes we need to define some intermediate predicates, namely the set OS of odd squares, and the two congruence classes modulo 8, $x \equiv_8 4$ and $x \equiv_8 3$ (with similar notations as above).

A defining formula for $OS(x)$ is $\exists y, z(\text{Neib}(2y, z) \wedge x = z^2)$. The relation $x \equiv_8 4$ is defined by $\exists y, z(\text{Neib}(2y, z) \wedge x = 4z)$.

We shall show that $x \equiv_8 3$ can be defined by the formula

$$\exists u, v, w, y, z\ (OS(u)\ \wedge\ OS(v)\ \wedge\ OS(w)\ \wedge\ \psi(u, v, y) \wedge$$

$$y \equiv_4 2\ \wedge\ \psi(y, w, x)\ \wedge\ \psi(x, 1, z)\ \wedge\ z \equiv_8 4)$$

On one hand if $x \equiv_8 3$ then by [Nar86], x is a sum of three squares u, v, w, all of them being odd (since every square is congruent to 0 or 1 modulo 4). Thus the previous formula holds for these values of u, v, w, with $y = u + v$ and $w = x - y$.

Conversely if there exist u, v, w, y, z such that the formula holds, then we have $y = |u \pm v|$. The case $y = |u - v|$ is excluded since $y \equiv_4 2$ and u, v are congruent to 1 modulo 4. Thus $y = u + v$, which yields $y \equiv_8 2$. We also have $x = |y \pm w|$, and the case $x = |y - w|$ must be excluded since the two last subformulas using z show that x must be congruent to 3 or 5 modulo 8. Thus we have $x = y + w = u + v + w$, which implies $x \equiv_8 3$ (since u, v, w are all congruent to 1 modulo 8).

We are now able to define the two congruence classes $x \equiv_4 1$ and $x \equiv_4 3$ by the formulas $\exists y\ (y \equiv_8 3\ \wedge\ \psi(y, 2, x))$ and $\exists y\ (y \equiv_4 1\ \wedge \psi(y, 2, x))$.

Finally we can define $z = x + y$ by the formula

$$\exists u, v\ (\text{Neib}(4x, u)\ \wedge\ u \equiv_4 3\ \wedge\ \text{Neib}(4y, v)\ \wedge v \equiv_4 1\ \wedge \psi(u, v, 4z)) \vee$$

$$\vee(x = 0\ \wedge\ y = z).$$

■

A class of undecidable extensions of Skolem Arithmetic was exhibited by Cegielski, Matiyasevich and Richard [CMR96], who proved the following result.

Theorem 47. *Let $p : \mathbb{N} \to P$ be injective. Then $Th(\mathbb{N}; =, \times, p)$ is undecidable.*

In particular Theorem 47 holds if p denotes the prime enumerating function π.

Proof. For every integer $x \geq 1$ let $\nu(x)$ denote the number of distinct prime divisors of x. Consider the equivalence relation $\sim$ on positive integers defined by $x \sim y$ iff $\nu(x) = \nu(y)$. Moreover let $x \lhd y$ mean $\nu(x) \leq \nu(y)$, and $\otimes(x, y, z)$ mean that $\nu(z) = \nu(x)\nu(y)$. The relations $\lhd$ and $\otimes$ are clearly compatible with $\sim$. Moreover

$$\langle(\mathbb{N} \setminus \{0\})_{/\sim}; \lhd_{/\sim}, \otimes_{/\sim}\rangle \cong \langle \mathbb{N}; <, \times_g \rangle.$$

Now $\mathrm{Th}(\mathbb{N}; <, \times_g)$ is undecidable by Proposition 45, thus in order to prove undecidability of $\mathrm{Th}(\mathbb{N}; =, \times, \pi)$ it suffices to "define" $\langle (\mathbb{N}\setminus\{0\})_{/\sim}; \lhd_{/\sim}, \otimes_{/\sim}\rangle$ in $\langle \mathbb{N}; =, \times, \pi\rangle$. More precisely we have to show that the set $\mathbb{N}\setminus\{0\}$, and the relations $\sim, \lhd, \otimes$ are definable in $\langle =, \times, \pi\rangle$ (see e.g. [Rab65, Ric85a] where this undecidability method is detailed).

The case of $\mathbb{N}\setminus\{0\}$ is straightforward. The idea for defining $x \lhd y$ is to translate the existence of an injective map from $\mathrm{Supp}(x) \setminus \mathrm{Supp}(y)$ to $\mathrm{Supp}(y) \setminus \mathrm{Supp}(x)$. More precisely a defining formula for $x \lhd y$ expresses the fact that there exists an integer c such that

$\mathrm{Supp}(c) = \{p(r_0 s_0), \ldots, p(r_u s_u)\}$ for some distinct primes $r_0, \ldots, r_u, s_0, \ldots, s_u$ such that $\{(r_i, s_i) | i \leq u\}$ is the graph of an injective map from $\mathrm{Supp}(x) \setminus \mathrm{Supp}(y)$ to $\mathrm{Supp}(y) \setminus \mathrm{Supp}(x)$.

It is quite clear, on one hand, that the existence of such a c is equivalent to $x \lhd y$, and on the other hand that the above properties for c are definable.

¿From $\lhd$ we easily define $x \sim y$. Finally for $\otimes$ one uses almost the same idea as for $\lhd$: this time a defining formula for $\otimes(x, y, z)$ asserts the existence of integers c', x', y', z' such that:

- $x \sim x'$, $y \sim y'$, $z \sim z'$
- x', y', z' are pairwise coprime
- $\mathrm{Supp}(c') = \{p(r_0 s_0 t_0), \ldots, p(r_k s_k t_k)\}$ where $r_0, \ldots, r_k, s_0, \ldots, s_k, t_0, \ldots, t_k$ are distinct primes such that $\{(r_i, s_i, t_i) | i \leq k\}$ is the graph of a one-to-one map between $\mathrm{Supp}(x') \times \mathrm{Supp}(y')$ and $\mathrm{Supp}(z')$.

■

Note that the previous proof does not need the full strength of $\langle \mathbb{N}; \times, p\rangle$, indeed the same result holds for $\mathrm{Th}\langle \mathbb{N}; |, p\rangle$.

Let us mention a related open question: is $+$ definable in $\langle \mathbb{N}; =, \times, \pi\rangle$ (recall that π enumerates primes) ? Note that [CMR96] provides an example of an injective map $p : \mathbb{N} \to P$ for which $+$ is not definable in $\langle \mathbb{N}; =, \times, p\rangle$.

We close the section by answering Maurin's question (see paragraph 3.2): does Theorem 43 about decidability of $\mathrm{Th}(\mathbb{N}\setminus\{0\}; =, \times, <_P)$ still hold if we replace $<_P$ by $<_\Pi$, the order relation restricted to the set Π of primary numbers ?

This question was answered negatively by Richard and the author [BR98].

Theorem 48. *$Th(\mathbb{N}; =, \times, <_\Pi)$ is undecidable.*

Proof. We use the same idea as in the proof of Theorem 47, namely we define $\lhd$ and $\otimes$ in $\langle \mathbb{N}; =, \times, <_\Pi\rangle$. This time the idea for defining $x \lhd y$ goes as follows: the formula asserts the existence of an integer c and a prime p such that c can be written as

$$c = q_1^{a_1} q_2^{a_2} \ldots q_n^{a_n}$$

where

- $q_0, \ldots, q_n$ are distinct primes
- $\mathrm{Supp}(x) \setminus \mathrm{Supp}(y) \subseteq \{q_1, \ldots q_n\} \subseteq (\mathrm{Supp}(x) \cup \mathrm{Supp}(y)) \setminus (\mathrm{Supp}(x) \cap \mathrm{Supp}(y))$
- $q_1^{a_1} < q_2^{a_2} < \cdots < q_n^{a_n}$
- for every $i < n$, $q_i \in \mathrm{Supp}(x) \setminus \mathrm{Supp}(y)$ iff $q_{i+1} \in \mathrm{Supp}(y) \setminus \mathrm{Supp}(x)$
- $q_0 \in \mathrm{Supp}(x) \setminus \mathrm{Supp}(y)$ and $q_n \in \mathrm{Supp}(y) \setminus \mathrm{Supp}(x)$

The above properties express that $\{(q_{2i}, q_{2i+1}) : \ i \leq n/2\}$ is the graph of an injection from $\mathrm{Supp}(x) \setminus \mathrm{Supp}(y)$ to $\mathrm{Supp}(y) \setminus \mathrm{Supp}(x)$.

An analog idea can be used to define $\otimes(x, y, z)$: one introduces pairwise coprime integers x', y', z' such that $x \sim x'$, $y \sim y'$, $z \sim z'$, and express the existence of an integer c' of the form

$$c' = {q'}_1^{b_1} {q'}_2^{b_2} \ldots {q'}_{3m}^{b_{3m}}$$

where the ${q'}_i$'s are distinct primes, ${q'}_1^{b_1} < {q'}_2^{b_2} < \ldots {q'}_{3m}^{b_{3m}}$, and $\{({q'}_{3i}, {q'}_{3i+1}, {q'}_{3i+2}) : 1 \leq i \leq m\}$ is the graph of a bijection between $\mathrm{Supp}(x') \times \mathrm{Supp}(y')$ and $\mathrm{Supp}(z')$. ∎

In fact [BR98] proves a stronger result, namely that + is definable in the structure.

3.5 Notes

Cegielski proved that the theory of $\langle \mathbb{N}; =, \times \rangle$ is not finitely axiomatizable [Ceg81]. Models of the theory were explored by Chatzidakis [Cha81].

Korec proves [Kor97] undecidability of the theory of $\langle \mathbb{N}; \times, =, S^k \rangle$, where $S^k(x) = x + k$ (with $k \geq 1$), as well as the theory of $\langle \mathbb{N}; \times, =, L_{p,q} \rangle$, where $L_{p,q}(x) = px + q$ (with $p, q \geq 1$). He also asks whether + is definable in $\langle \mathbb{N}; \times, =, x \mapsto x^2 + 1 \rangle$, and in $\langle \mathbb{N}; \times, =, X \rangle$ where X denotes the range of a polynomial function.

4 A question of Julia Robinson

In the present section we discuss definability issues for structures where + and × are *simultaneously* replaced by weaker relations. We have the following situation:

$$\begin{array}{ccccc}
\mathrm{Def}(\mathbb{N}; =, \perp, +) & \subseteq & \mathrm{Def}(\mathbb{N}; =, |, +) & \subseteq & \mathrm{Def}(\mathbb{N}; =, \times, +) \\
\bigcup | & & \bigcup | & & \bigcup | \\
\mathrm{Def}(\mathbb{N}; \perp, <) & \subseteq & \mathrm{Def}(\mathbb{N}; |, <) & \subseteq & \mathrm{Def}(\mathbb{N}; =, \times, <) \\
\bigcup | & & \bigcup | & & \bigcup | \\
\mathrm{Def}(\mathbb{N}; \perp, S) & \subseteq & \mathrm{Def}(\mathbb{N}; |, S) & \subseteq & \mathrm{Def}(\mathbb{N}; =, \times, S)
\end{array}$$

We shall focus on the structures $\langle \mathbb{N}; S, | \rangle$ and $\langle \mathbb{N}; S, \perp \rangle$, which were first considered by Julia Robinson [Rob49]. In this paper she proved that + and × are definable in $\langle \mathbb{N}; S, | \rangle$ (see Theorem 49 below) and asked whether the same holds for $\langle \mathbb{N}; S, \perp \rangle$. Up to now the question is still open. Woods (and independently Richard) proved undecidability of the theory, and showed that J.Robinson's question is strongly connected with a difficult number-theoretic conjecture, today known as *Erdös-Woods*

Conjecture, which roughly states that any integer is completely determined by the set of its prime divisors and the set of prime divisors of some of its neighbours. These results are discussed in the second paragraph. In the final paragraph we state some partial answer to Robinson's question due to Richard, who proved that all arithmetical relations restricted to the set Π of prime powers are definable in $\langle \mathbb{N}; S, \perp \rangle$.

4.1 The theory of $\langle \mathbb{N}; S, | \rangle$

Let us first recall Robinson's result [Rob49] about $\langle \mathbb{N}; S, | \rangle$.

Theorem 49. $\mathrm{Def}(\mathbb{N}; |, S) = \mathrm{Def}(\mathbb{N}; =, \times, +)$. *Thus* $Th(\mathbb{N}; S, |)$ *is undecidable.*

Proof. Thanks to Proposition 45 it suffices to define $\times$ in $\langle \mathbb{N}; |, S \rangle$. Let us show that for all positive integers x, y, z, one has $z = xy$ iff the following property, which we denote $(*)$, holds :

For every $m \in \mathbb{N}$ prime to xy there exist coprime integers x', y' , both prime to xyz, such that

$$\begin{cases} xx' \equiv -1 \pmod{m} \\ yy' \equiv -1 \pmod{m} \\ zx'y' \equiv 1 \pmod{m} \end{cases}$$

Let us show that if $z = xy$ then (x, y, z) satisfies $(*)$. Let m be prime to x and y. There exist x'' and y'' such that $xx'' \equiv -1 \pmod{m}$ and $yy'' \equiv -1 \pmod{m}$. The integers x'' and y'' being prime to m, it follows from Dirichlet's Theorem that there exist two primes x' and y', greater than x, y and z and such that $x' \equiv x'' \pmod{m}$ and $y' \equiv y'' \pmod{m}$. One checks easily that x' and y' satisfy conditions of $(*)$.

Conversely if (x, y, z) satisfies $(*)$ then for every m prime to x and y, there exist x' and y' such that

$$zx'y' \equiv 1 \equiv (-1) \cdot (-1) \equiv (xx') \cdot (yy') \pmod{m}$$

which implies

$$zx'y' \equiv (xy) \cdot (x'y') \pmod{m}$$

Now, from the congruences of $(*)$ and the fact that $x'y'$ is prime to m, one deduces that

$$z \equiv xy \pmod{m}.$$

This is true for infinitely many values of m, thus $z = xy$.

It remains to express property $(*)$ in the language $\{S, |\}$, which is done easily, and yields a definition for $\times$. ∎

As an immediate corollary we get

$$\mathrm{Def}(\mathbb{N}; |, <) = \mathrm{Def}(\mathbb{N}; =, |, +) = \mathrm{Def}(\mathbb{N}; =, \times, +).$$

Cegielski [Ceg90] specified Theorem 49 by giving an axiomatization of Peano Arithmetic in the language $\{S, |\}$. Moreover Korec [Kor96] proved that Theorem 49 still holds if we replace the successor function by the relation $\mathrm{Neib}(x, y)$ (which holds iff $|x - y| = 1$).

4.2 $\langle \mathbb{N}; S, \perp \rangle$ and Erdös-Woods' conjecture

We now turn to Robinson's (open) question of whether $+$ and $\times$ are definable in the structure $\langle \mathbb{N}; S, \perp \rangle$. Up to now, the main contributions on the subject are due to A.Woods and D.Richard.

We shall concentrate in this paragraph on Woods' proofs (as far as we know, the only source was Wood's PhD Thesis [Woo81]).

Woods' first important result is the following (see next paragraph for an alternative proof).

Theorem 50. *$Th(\mathbb{N}; S, \perp)$ is undecidable.*

Proof. We use the same technique as the one for Theorem 47, i.e. we show that $\lhd$ and $\otimes$ are definable in $\langle \mathbb{N}; S, \perp \rangle$.

For $x \geq 1$, let $\overline{x}$ be the class of x with respect to the equivalence relation $\mathrm{Supp}(x) = \mathrm{Supp}(y)$. Moreover let $\delta(x)$ be the set of classes $\overline{q} \in \overline{P}$ such that $gcd(x, q) \neq 1$.

Note that the set of primary numbers Π, in other words the set of integers x such that $\overline{x} \in \overline{P}$, is definable in $\langle \mathbb{N}; S, \perp \rangle$ (and even in $\langle \mathbb{N}; \perp \rangle$).

We shall define the relation "$\nu(x) \leq \nu(y)$, $x \perp y$, and both x, y are odd", from which a defining formula for $x \lhd y$ can be derived easily. Given x, y odd and relatively prime, the idea for defining $\nu(x) \leq \nu(y)$ is to translate the existence of an injection $f : \delta(x) \to \delta(y)$ through the existence of an integer c such that $\delta(c) = \{\overline{q_1}, \overline{q_2}, \ldots, \overline{q_t}\}$ where each $\overline{q_i}$ encodes a unique pair $(\overline{r}, f(\overline{r}))$. For this we need that each $\overline{q_i}$ "distinguishes" two elements in $\delta(x) \cup \delta(y)$, one in each subset.

To this aim let us introduce an encoding technique that allows a class $\overline{q} \in \overline{P}$ to distinguish, in a finite set C of elements of $\overline{P} \setminus \{2\}$, some subset D.

Given $q \in P$, we define $\mathrm{Cod}(\overline{q}, C)$ as the subset $D \subseteq C$ of classes $\overline{r} \in P$ such that there exists r', with $\overline{r'} = \overline{r}$, for which $q' \equiv 1 \pmod{r'}$ for every q' which satisfies $\overline{q'} = \overline{q}$.

It follows from Dirichlet's Theorem that given any finite set $C \subseteq \overline{P} \setminus \{2\}$ and any $D \subseteq C$ there is some $\overline{q}$ that satisfies $\mathrm{Cod}(\overline{q}, C) = D$: indeed if $C = \{\overline{s_1}, \ldots, \overline{s_t}\}$ with $s_i \in P$ $(i = 1, \ldots, t)$, then we can choose a prime solution of the system:

$$q \equiv \begin{cases} 1 \pmod{s_i} & \text{for all } s_i \text{ such that } \overline{s_i} \in D \\ -1 \pmod{s_i} & \text{for all } s_i \text{ such that } \overline{s_i} \in C \setminus D \end{cases}$$

We can "define" $\mathrm{Cod}(q, c)$ in $\langle \mathbb{N}; S, \perp \rangle$ in the following sense: the ternary relation $\mathrm{Cod}'(u, v, w)$ which holds iff $(\overline{u} \in \overline{P}$, $\delta(v) \subseteq \delta(w) \subseteq \overline{P} \setminus \{\overline{2}\}$, and $\mathrm{Cod}(\overline{u}, \delta(w)) = \delta(v))$ is definable.

This leads to a defining formula for "$\nu(x) \leq \nu(y)$, $x \perp y$ and x, y odd": it expresses the existence of an odd integer c such that $\delta(c) = \{\overline{q}_1, \overline{q}_2, \ldots, \overline{q}_t\}$ where:

- for each i there is a couple $(\overline{r}_i, \overline{r}'_i) \in \delta(x) \times \delta(y)$ such that $\mathrm{Cod}(\overline{q}_i, \delta(x) \cup \delta(y)) = \{\overline{r}_i, \overline{r}'_i\}$;
- the set $\{(\overline{r}_i, \overline{r}'_i) : \ 1 \leq i \leq t\}$ is the graph of an injective map $f : \delta(x) \to \delta(y)$.

For $\otimes$ one uses the same encoding idea: indeed given integers x, y, z, which we assume to be odd and pairwise coprime w.l.o.g. , we have $\nu(x) \times \nu(y) = \nu(z)$ iff there exists an odd integer d such that $\delta(d) = \{\overline{q}_1, \overline{q}_2, \ldots, \overline{q}_t\}$ where:

- for each i there is a triple $(\overline{r}_i, \overline{r}'_i, \overline{r}''_i) \in \delta(x)\times\delta(y)\times\delta(z)$ such that $\mathrm{Cod}(\overline{q}_i, \delta(x)\cup\delta(y)\cup\delta(z)) = \{\overline{r}_i, \overline{r}'_i, \overline{r}''_i\}$;
- the set $\{(\overline{r}_i, \overline{r}'_i, \overline{r}''_i)) : \ 1 \leq i \leq t\}$ is the graph of a bijective map $f : \delta(x) \times \delta(y) \to \delta(z)$.

■

The difficulty to define $\lhd$ and $\otimes$ in the previous proof partly has to do with the fact that the set of primes (and the relation *"x is a prime divisor of y"*) does not seem to be definable in the structure $\langle \mathbb{N}; S, \perp\rangle$ (whereas it is clearly definable in the structures considered in Theorems 47 and 48). Richard [Ric85a] actually proved that the set of primes is definable in $\langle \mathbb{N}; S, \perp\rangle$ –see next paragraph.

The next theorem provides a re-formulation of Robinson's question.

Theorem 51 (Woods). *The following claims are equivalent :*
(1) $+$ *and* $\times$ *are definable in* $\langle \mathbb{N}; S, \perp, =\rangle$*;*
(2) *Equality relation* $=$ *is definable in* $\langle \mathbb{N}; S, \perp\rangle$*;*
(3) *There exists* $k \in \mathbb{N}$ *such that for all* $x, y \in \mathbb{N}$,
$\Big[\mathrm{Supp}(x+i) = \mathrm{Supp}(y+i) \quad \textit{for} \ \ i = 0, 1, \ldots, k\Big]$ *implies* $x = y$.

Proof. (3)→(2) is obvious.

(2)→(3) : assume $\varphi(x, y)$ defines $x = y$. Consider the greatest k that appears in a term $S^k(x)$ in the formula $\varphi(x, y)$ (and set $k = 0$ if there is no such term). Then one checks that for all x_1, x_2, if $\mathrm{Supp}(x_1 + i) = \mathrm{Supp}(x_2 + i)$ for $i = 0, \ldots, k$, then for every y the formula $\varphi(x_1, y)$ holds iff $\varphi(x_2, y)$ does. Therefore (3) must hold for this value of k (otherwise we find x_1, x_2, $x_1 \neq x_2$, such that $\varphi(x_1, x_2)$ holds). The proof for (1)→(3) is similar.

(3)→(1) Assume (3) holds for some integer k. We shall prove that the function ν^{-1} is definable in $\langle \mathbb{N}; S, \perp\rangle$. Indeed we showed in the proof of Theorem 50 that $\lhd$ and $\otimes$ are definable in $\langle \mathbb{N}; S, \perp\rangle$, thus if we could define ν^{-1} then we would get a definition for $<$ and $\times$, from which a definition for $+$ will follow (using Tarski's identity, see previous section).

We shall introduce a (definable) relation $A(n, z)$ which holds only if $\nu(z) = n+k$, and such that for any n there exists z such that $A(n, z)$ holds. From A and $\sim$ one then easily defines the function ν^{-1}.

Roughly speaking, z will be defined such that $\delta(z) = \{\overline{q}_1, \ldots, \overline{q}_{n+k}\}$ where each q_i encodes $\mathrm{Supp}(i)$.

We define the relation $A(n, z)$ to hold iff either $n = 0$ and z has exactly k prime divisors (this case is definable), or z has at least k distinct prime divisors and there exist two disjoint finite sets C, D of elements of $\overline{P}$, a class $\overline{r} \in P$, $\overline{r} \notin C \cup D$, such that:

- The set $\{\mathrm{Cod}(\overline{q}, D) : \overline{q} \in \delta(z)\}$ is totally ordered for the inclusion relation.

Let $\delta(z) = \{\overline{q_1}, \overline{q_2}, \ldots, \overline{q_t}\}$, with $\mathrm{Cod}(\overline{q}_i, C) \subseteq \mathrm{Cod}(\overline{q}_{i+1}, C)$ $(1 \leq i < t)$.

$$\text{We set } \mathrm{Dec}(\overline{q}_i) = \begin{cases} \mathrm{Cod}(\overline{q}_i, C) \cup \{2\} & \text{if } \mathrm{Cod}(\overline{q}_i, \{\overline{r}\}) = \{\overline{r}\} \\ \mathrm{Cod}(\overline{q}_i, C) & \text{otherwise} \end{cases}$$

- $(\mathrm{Dec}(\overline{q}_1), \ldots, \mathrm{Dec}(\overline{q}_{k+1})) = (\delta(1), \ldots, \delta(k+1))$;
- if
$$(\mathrm{Dec}(\overline{q}_i), \mathrm{Dec}(\overline{q}_{i+1}), \ldots, \mathrm{Dec}(\overline{q}_{i+k})) = (\delta(j), \ldots, \delta(j+k))$$
for some integer j, then
$$(\mathrm{Dec}(\overline{q}_{i+1}), \mathrm{Dec}(\overline{q}_{i+2}), \ldots, \mathrm{Dec}(\overline{q}_{i+k+1})) = (\delta(j+1), \ldots, \delta(j+k+1))$$
$(i \leq t-k)$
- $(\mathrm{Dec}(\overline{q}_{t-k}), \mathrm{Dec}(\overline{q}_{t-k+1}), \ldots, \mathrm{Dec}(\overline{q}_t)) = (\delta(n), \ldots, \delta(n+k))$.

We leave to the patient reader the easy-but-tedious task to show that $A(n,z)$ is definable in $\langle \mathbb{N}; S, \perp \rangle$. Note that in the defining formula one translates the existence of C by the existence of an integer y such that $\delta(y) = C$; a similar idea is used for D.

On one hand if $A(n,z)$ holds then the three last conditions, combined with our assumption that (3) holds for the value k, ensure that $\nu(z) = n+k$.

Conversely given $n \in \mathbb{N}$, one can find z such that $A(n,z)$ holds. For this we first choose $n+k$ prime numbers $r_1, \ldots, r_{n+k}$ all greater than $n+k$, and set $D = \{\overline{r}_1, \ldots, \overline{r}_{n+k}\}$. We also choose some prime number r greater than all r_i's. Then we set C as the set of classes of prime numbers $\leq n+k$; we have $C \cap D = \emptyset$. Then we choose z as an integer with support $\{q_1, \ldots, q_{n+k}\}$, where each q_i satisfies :

- $\mathrm{Cod}(\overline{q}_i, D) = \{\overline{r}_1, \ldots, \overline{r}_i\}$
- $\mathrm{Cod}(\overline{q}_i, \{\overline{r}\}) = \{\overline{r}\}$ iff i is even;
- $\mathrm{Cod}(\overline{q}_i, C) = \{\overline{p}_1, \ldots, \overline{p}_{m_i}\}$ where $\{p_1, \ldots, p_{m_i}\} = \mathrm{Supp}(i) \setminus \{2\}$.

Then it is clear that z satisfies the conditions required in the definition of $A(n,z)$. ∎

Condition (3) in the statement of the previous theorem is known as *Erdös-Woods Conjecture*. Let us state it again:

Erdös-Woods Conjecture (EW): *There exists $k \in \mathbb{N}$ such that for all $x, y \in \mathbb{N}$,*

$$\Big[\mathrm{Supp}(x+i) = \mathrm{Supp}(y+i) \quad \text{for } \; i = 0, 1, \ldots, k\Big] \; \text{implies } \; x = y.$$

(EW) is closely related to another conjecture formulated by Erdös in [Erd80]; in this paper he considered the problem to find integers k, l, m, n, with $k \geq l \geq 3$ and $(m,k) \neq (n,l)$, such that $(m+1)(m+2)\ldots(m+k)$ and $(n+1)(n+2)\ldots(n+l)$,

with $k \geq l \geq 3$ and $(m,k) \neq (n,l)$ have the same prime factors. For example $2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10$ and $14 \cdot 15 \cdot 16$ (or $48 \cdot 49 \cdot 50$) have the same prime factors. He conjectured that for $k = l \geq 3$ there are only finitely many solutions.

It is known that the constant k in (EW) must be greater than 1. Indeed Erdös noticed (see problem B19 in [Guy94]) that for any $n \in \mathbb{N}$, the integers $x = 2^n - 2$ and $y = 2^n(2^n - 2)$ have the same support, as well as $x + 1$ and $y + 1$.

Langevin ([Lan92, Lan93], see also [Lan96]) studied connections between (EW) and other classical conjectures in arithmetic.

Let us mention that Vsemirnov recently proved an analogue of (EW) for polynomial rings [Vse00].

4.3 Definability within $\langle \mathbb{N}; S, \perp \rangle$

Richard proposed in [Ric85a] another proof for undecidability of $\mathrm{Th}(\mathbb{N}; S, \perp)$, and specified the expressive power of $\langle \mathbb{N}; S, \perp \rangle$ by proving that all arithmetical relations restricted to the set Π of prime powers are definable in this structure. Recall that $X \subseteq \mathbb{N}^k$ is *arithmetical* if it is definable in $\langle \mathbb{N}; =, \times, + \rangle$.

This shows for instance that the relations *"x and y are consecutive primes"* or *"x and y are two primary numbers such that $x < y$"* are definable in $\langle \mathbb{N}; S, \perp \rangle$.

Richard's proof uses number-theoretical results which state that an analogue of (EW) holds if we assume x, y to be prime powers. The starting point is the following result due to Bang [Bang].

Theorem 52. *Let $x \geq 2$. For every $n \geq 1$, the integer $x^n - 1$ has a* primitive divisor*, i.e. a prime divisor which does not divide any integer $x^m - 1$ for $0 < m < n$, except in the following cases.*

(i) $n = 1$, $x = 2$;

(ii) $n = 2$, $x = 2^\alpha - 1$ for some $\alpha \geq 1$;

(iii) $n = 6$, $x = 2$.

Similarly $x^n + 1$ has a primitive divisor, except in the case ($x = 2$ and $n = 3$).

Bang's result has been extended later by Zsigimondy, [Zsi], and also Birkhoff and Vandiver [BV04] (see [Sha82]), for integers of the form $x^n - y^n$, and by Carmichael [Car14] for integers of the form $x^n + y^n$.

Theorem 52 admits the following corollary.

Corollary 53. *For every integer $x \geq 2$ and all $\alpha, \beta \in \mathbb{N}$ the following holds:*

(i) The equality $\mathrm{Supp}(x^\alpha + 1) = \mathrm{Supp}(x^\beta + 1)$ *is equivalent to*
"$\alpha = \beta$ or ($x = 2$ and $\alpha, \beta \in \{1, 3\}$)".

(ii) The equality $\mathrm{Supp}(x^\alpha - 1) = \mathrm{Supp}(x^\beta - 1)$ *is equivalent to*
"$\alpha = \beta$ or ($x = 2^u - 1$ for some $u \geq 2$, and $\alpha, \beta \in \{1, 2\}$)".

Assuming x to be prime in the previous corollary leads to the following weakening of (EW) for prime powers.

Proposition 54. *Let $y, z \in \Pi$. If* $\mathrm{Supp}(y+j) = \mathrm{Supp}(z+j)$ *for every $j \in \{-1, 0, 1\}$ then $y = z$.*

The following theorem is due to Carmichael and Lucas [Car14].

Theorem 55. *If $x, y \geq 1$ are relatively prime then for all $m, n \geq 1$ we have*

$$\gcd\left[\frac{x^m - y^m}{x - y}, \frac{x^n - y^n}{x - y}\right] = \frac{x^{\gcd(m,n)} - y^{\gcd(m,n)}}{x - y}.$$

In the sequel we shall use the following consequence of Carmichael-Lucas theorem.

Corollary 56. *For every integer $x \geq 2$ and all $\alpha, \beta \in \mathbb{N}$, the inclusion*

$$\mathrm{Supp}(x^\alpha - 1) \subseteq \mathrm{Supp}(x^\beta - 1)$$

is equivalent to "$\alpha \mid \beta$ or ($x = 2^u - 1$ for some $u \geq 2$, and $\alpha \in \{1, 2\}$)".

Proof. The equivalence is clear if $\alpha = 0$ or $\beta = 0$. Assume now that $\alpha\beta \neq 0$. On one hand if $\alpha|\beta$ then $x^\alpha - 1|x^\beta - 1$ which ensures $\mathrm{Supp}(x^\alpha - 1) \subseteq \mathrm{Supp}(x^\beta - 1)$. Moreover if $x = 2^u - 1$ for some $u \geq 2$ then obviously $\mathrm{Supp}(x + 1) \subseteq \mathrm{Supp}(x - 1)$, so that $\mathrm{Supp}(x - 1) = \mathrm{Supp}(x^2 - 1)$. Now $\mathrm{Supp}(x - 1) \subseteq \mathrm{Supp}(x^\beta - 1)$ for every β, thus $\mathrm{Supp}(x^2 - 1) \subseteq \mathrm{Supp}(x^\beta - 1)$ for every β, which gives the required result.

Conversely assume that $\mathrm{Supp}(x^\alpha - 1) \subseteq \mathrm{Supp}(x^\beta - 1)$; then by Theorem 55 we have

$$\mathrm{Supp}\Big(\frac{x^\alpha - 1}{x - 1}\Big) \cap \mathrm{Supp}\Big(\frac{x^\beta - 1}{x - 1}\Big) = \mathrm{Supp}\Big(\frac{x^{\gcd(\alpha,\beta)} - 1}{x - 1}\Big)$$

which yields by our hypothesis

$$\mathrm{Supp}\Big(\frac{x^\alpha - 1}{x - 1}\Big) = \mathrm{Supp}\Big(\frac{x^{\gcd(\alpha,\beta)} - 1}{x - 1}\Big)$$

that is,

$$\mathrm{Supp}(x^\alpha - 1) = \mathrm{Supp}(x^{\gcd(\alpha,\beta)} - 1)$$

which by Corollary 53 yields either $\alpha = \gcd(\alpha, \beta)$ i.e. $\alpha|\beta$, or ($x = 2^u - 1$ for some $u \geq 2$, and $\gcd(\alpha, \beta), \alpha \in \{1, 2\}$) from which the result follows. ∎

Let us state a first definability result (that was promised in the previous paragraph).

Proposition 57. *The set P of primes is definable in $\langle \mathbb{N}; S, \perp \rangle$*

Proof. The relations $x = 0$, $x = 1$, and the set Π of primary numbers, are easily definable in our structure (even in $\langle \mathbb{N}; \perp \rangle$). Then $x = 2$ is definable by the formula

$$\Pi(x) \ \wedge \ \Pi(S^{(2)}(x)) \ \wedge \ \neg(x \perp S^{(2)}(0)).$$

Then Corollary 53 allows to define the relation $x =_\Pi y$ interpreted as equality relation restricted to Π, since $x =_\Pi y$ holds iff the following conditions hold:

- x, y are in Π,
- $\mathrm{Supp}(x) = \mathrm{Supp}(y)$ and $\mathrm{Supp}(x + 1) = \mathrm{Supp}(y + 1)$
- if $\mathrm{Supp}(x) = 2$, then $x = 2$ iff $y = 2$.

From $=_\Pi$ it is easy to define any constant n: Take a prime $p > n$, then $x = n$ iff $S^{(p)}(0) =_\Pi S^{(n-p)}(x)$.

Then we can define the function $Pred_\Pi : \mathbb{N} \to \mathbb{N}$ which maps every integer x to $x - 1$ in case $x \in \Pi$, and to 0 otherwise.

In order to define the set of primes, consider the sets

$$A = \{p^\alpha : \ p \ \text{ prime, } \ \alpha \geq 1 \ \text{ and } \ \mathrm{Supp}(p^\alpha - 1) \subseteq \mathrm{Supp}(p^\beta - 1) \ \text{ for every } \ \beta \geq 1\}$$

and

$$B = \{p^\alpha : \ p^\alpha \in A \ \text{ and } \ \mathrm{Supp}(p^\alpha + 1) \subseteq \mathrm{Supp}(p^\gamma + 1) \ \text{ for every } \ p^\gamma \in A\};$$

Both A and B are definable in $\langle \mathbb{N}; S, \perp \rangle$ (one uses $Pred_\Pi$). Let us show that $B = P$. First of all Corollary 56 yields

$$A = P \cup \{p^2 : \ p \ \text{ is a prime of the form } \ 2^u - 1 \ \text{ with } \ u \geq 2\}.$$

Moreover if p is a prime of the form $2^u - 1$ for some $u \geq 2$ (i.e. if p is a Mersenne prime) then

$$p^2 + 1 = 2(2^u(2^{u-1} - 1) + 1).$$

Now $u \geq 2$ thus $(2^u(2^{u-1} - 1) + 1)$ is odd and > 1, therefore $\mathrm{Supp}(p^2 + 1)$ is not contained in $\mathrm{Supp}(p+1)$ (which equals $\{2\}$). It follows that $p^2 \notin B$. The conclusion is $B = P$.

■

Proposition 58. *The set P_5 of powers of 5, and both relations $\{(5^n, 5^{n+1}) : \ n \in \mathbb{N}\}$ and $\{(5^m, 5^n) : \ m|n\}$ are definable in $\langle \mathbb{N}; S, \perp \rangle$.*

The choice of 5 in the above proposition allows to avoid the case $x = 2^u - 1$ in corollaries 53 (ii) and 56.

Proof. The set P_5 is easily definable, since the constant 5 and the binary relation *"x is prime and y is a power of x"* are.

In order to define $\{(5^n, 5^{n+1}) : \ n \in \mathbb{N}\}$, one uses the fact that given $n \in \mathbb{N}$, the integer 5^{n+1} is the only non-trivial power of 5, say 5^t, which satisfies

$$\mathrm{Supp}(5^t - 5) = \{5\} \cup \mathrm{Supp}(5^n - 1).$$

Indeed in this case we have

$$\mathrm{Supp}(5^t - 5) = \mathrm{Supp}(5(5^{t-1} - 1)) = \{5\} \cup \mathrm{Supp}(5^{t-1} - 1).$$

It follows that $\mathrm{Supp}(5^{t-1} - 1) = \mathrm{Supp}(5^n - 1)$, which yields $t = n + 1$ by Corollary 53 (ii).

Finally $\{(5^m, 5^n) : \ m|n\}$ is definable thanks to Corollary 56, which ensures that $\mathrm{Supp}(5^m - 1) \subseteq \mathrm{Supp}(5^n - 1)$ iff $m|n$. ■

As a corollary we get an alternative proof of undecidability of $\mathrm{Th}(\mathbb{N}; S, \perp)$ (Theorem 50). Indeed from the previous Proposition and Theorem 49 one can deduce that both relations $Add_5 = \{(5^x, 5^y, 5^z) : \ x + y = z\}$ and $Times_5 = \{(5^x, 5^y, 5^z) : xy = z\}$ are definable in $\langle \mathbb{N}; S, \perp \rangle$, and undecidability follows from the fact that $\langle P_5; Add_5, Times_5 \rangle$ and $\langle \mathbb{N}; +_g, \times_g \rangle$ are isomorphic.

The previous fact also implies the following.

Corollary 59. *If $R \subseteq \mathbb{N}^n$ is arithmetical then the relation $\{(5^{x_1}, \ldots, 5^{x_n}) : \ (x_1, \ldots, x_n) \in R\}$ is definable in $\langle \mathbb{N}; S, \perp \rangle$.*

Now we can state Richard's main definability result [Ric85a].

Theorem 60. *Let $k \geq 1$, and let $X \subseteq \mathbb{N}^k$ be an arithmetical relation. The set $X \cap \Pi^k$ is definable in $\langle \mathbb{N}; \perp, S \rangle$.*

One may think that the above definability property is strong enough to ensure that $+$ and $\times$ are definable in $\langle \mathbb{N}; S, \perp \rangle$. This is not true in general, as one can prove that the structure $\langle \mathbb{N}; \perp, <_\Pi \rangle$, where $<_\Pi$ denotes order relation restricted to Π, also enjoys this property, but neither $+$ nor $\times$ are definable in the structure (see [BR98]).

In order to prove Theorem 60, we first need some auxiliary definable relations.

Lemma 61. *The two following relations are definable in $\langle \mathbb{N}; S, \perp \rangle$:*

$A(x, y)$: "$x = q^n - 1$ for some prime q and some $n \geq 2$, and y is a primitive divisor of x"

$B(x, y)$: "x, y are distinct primes and $Ord(y, x) = x - 1$"

Proof (sketch). The main idea for defining A is to use the following consequence of Corollary 56: for q prime and $n \geq 3$, y is a primitive divisor of $q^n - 1$ iff $q \in \mathrm{Supp}(p^n - 1)$ and moreover if $\mathrm{Supp}(p^m - 1) \subseteq \mathrm{Supp}(p^n - 1)$ implies $q \notin \mathrm{Supp}(p^m - 1)$ for every $m \neq n$. For $n \leq 2$, note further that all prime divisors of $p-1$ are primitive, and that the primitive divisors of $p^2 - 1$ are the prime divisors of $p^2 - 1$ which do not divide $p - 1$.

The predicate A allows then to develop the following encoding device: one can encode any finite set of powers of a prime p, say $\{p^{n_1}, p^{n_2}, \ldots, p^{n_t}\}$ with $n_1 < n_2 < \ldots, < n_t$, by some integer c whose support consists in the primes $q_{n_1}, q_{n_2}, \ldots, q_{n_t}$ where each q_i is a primitive divisor of $p^{n_i} - 1$. Bang's Theorem allows to ensure that such an encoding is coherent.

Using this idea, we can associate with any couple of distinct primes x, y some integer $c_{x,y}$ which encodes (in the previous sense) the set $\{y^\alpha : \alpha | Ord(y, x)\}$ (note that by Corollary 56 we have –apart from some exceptional cases– $\alpha | Ord(y, x)$ iff $\mathrm{Supp}(y^\alpha - 1) \subseteq \mathrm{Supp}(y^\beta - 1)$ where x is a primitive divisor of $y^\beta - 1$). Thus $\nu(c_{x,y})$ equals the number of divisors of $Ord(y, x)$.

Now one can define B using the fact that $Ord(y, x) = x - 1$ iff $\nu(c_{x,z}) \leq \nu(c_{x,y})$ for every prime $z \neq x$. Indeed for every prime $z \neq x$ we have $Ord(z, x) | x - 1$, thus $\nu(c_{x,z})$ is always less than or equal to the number of divisors of $x - 1$. ∎

Lemma 62. *The restriction of $x \mapsto 5^x$ to the set P is definable in $\langle \mathbb{N}; S, \perp \rangle$.*

Proof. By Corollary 59 it suffices to define the restriction to P of the function $x \mapsto 5^{x-1}$.

We have to recover (by means of definable properties) 5^{p-1} from a prime p. We shall distinguish two cases.

First case : p *is the only primitive divisor of* $5^{Ord(5,p)} - 1$
In this case we first recover $5^{Ord(5,p)}$ from p, using the definable relation

$$\{(x, y) : \ x \ \text{ is a primitive divisor of } \ 5^{Ord(5,y)} - 1\}.$$

Then we can recover 5^{p-1} from $5^{Ord(5,p)}$, using this time the relation

$$\{(5^m, 5^n) : \ n \ \text{ is the only primitive divisor of } \ 5^{5^m-1}\}$$

which is definable by Corollary 59.

Second case : $5^{Ord(5,p)} - 1$ *has at least two primitive divisors*
In this case one uses the fact that 5^{p-1} is the only power of 5, say 5^a, which has the following property (which we denote by (P)):

There exist two primes t, q such that
(1) $t \geq 7$;
(2) $q \neq p$;
(3) $t \equiv 5 \pmod{q}$;
(4) $Ord(t, p) = p - 1$;
(5) q *is a primitive divisor of both and* $5^a - 1$ *and* $t^{p-1} - 1$.

This property is expressible using Lemma 61.

Let us first prove that 5^{p-1} enjoys (P). Note that the integer $5^{p-1} - 1$ has at least a primitive divisor $q \neq p$:
– if $Ord(5, p-1) = p - 1$ then this is a consequence of our very hypothesis
– if $Ord(5, p-1) \neq p - 1$, then $5^{p-1} - 1$ has at least a primitive divisor by Theorem 52, but it cannot be p which is already a primitive divisor of $5^{Ord(5,p-1)} - 1$.

Consider thus this primitive divisor q. Using the fact that $(\mathbb{Z}_{/p\mathbb{Z}})^*$ is cyclic and Dirichlet's Theorem, allows to claim that there exists a prime number t satisfying (1), (3) and (4). Now (3) implies that $Ord(5, q) = Ord(t, q)$, which together with (4) implies (5).

Conversely if 5^a satisfies (P) then again (3) implies that $Ord(t, q) = Ord(5, q)$, and by (5) it follows that q is a primitive divisor of both $t^a - 1$ and $t^{p-1} - 1$, which implies $a = p - 1$ by Corollary 53(ii). ∎

Proof of Theorem 60 . By Corollary 59 it is sufficient to show that the restriction to Π of the function $f : x \mapsto 5^x$ is definable in $\langle \mathbb{N}; S, \perp \rangle$. We use Proposition 54 which ensures that a prime power q is entirely determined by the sequence $(\mathrm{Supp}(q-1), \mathrm{Supp}(q), \mathrm{Supp}(q+1))$.

Let us describe how to "catch" (by means of definable relations) the integer $f_\Pi(q) = 5^{p^n}$ from the prime power $q = p^n$ (p prime). First, from p^n we get the prime

p and then $f_P(p) = 5^p$, from which we isolate the set of integers of the form 5^{p^t} (for some $t \in \mathbb{N}$) (i.e. we define $U(x, y, z)$: "x is a power of some prime p, $y = 5^p$ and $z = 5^{p^t}$ for some $t \in \mathbb{N}$"). We can define from each integer $y = 5^{p^t}$ the sets $Z_-(y) = \{5^r : r \in \mathrm{Supp}(p^t - 1)\}$ and $Z_+(y) = \{5^r : r \in \mathrm{Supp}(p^t + 1)\}$ (i.e. we define $V(x, y)$:"$x = 5^n$ and $y = 5^p$ for some prime p and some $n \in \mathbb{N}$, with $p|n$"). Now by Proposition 54, the integer 5^{p^n} (that is $f_\Pi(p^n)$) is the only integer of the form 5^{p^t} such that $Z_-(5^{p^t}) = f_P(\mathrm{Supp}(p^n - 1))$ and $Z_+(5^{p^t}) = f_P(\mathrm{Supp}(p^n + 1))$.

■

4.4 Notes

• Richard proved (see [GR89]) that both + and × are definable in $\langle \mathbb{N}; S, \perp, R\rangle$ when R denotes any of the following relations:

- *"x is a power of y "*
- *"x is a quadratic residue modulo the prime y "*
- *"x is prime and $x + y = z$ "*
- *"x is prime and $xy = z$".*

See also [Nez97] for related definability results.

Acknowledgments

I wish to express my gratitude to my PhD advisor, Professor Denis Richard, for his exciting introduction to the subject, and for having encouraged me to write extended presentations for the text of my PhD Thesis. They provide the basis for the present paper, together with talks given at Université Paris 7, Université Libre de Bruxelles, and Université de Mons-Hainaut.

Most of the paper was completed while the author was holding a post-doctoral Marie Curie training grant (TMR program) at Université de Mons-Hainaut, Institut de Mathématique et d'Informatique. I thank Christian Michaux and all people there for their hospitality.

Finally I thank the referee (and Christian Michaux again) for many helpful suggestions.

References

[Bang] A.S.Bang, *Taltheoretiske Undersogelser*, Tidskrift f. Math., Ser. 5, 4, 70–80 and 130–137 (1886)

[BJW93] P.T.Bateman, C.G.Jockusch, A.R.Woods, Decidability and undecidability with a predicate for the primes, *J. Symbolic Logic* 58 (1993) 672–687.

[BPW00] O.Belegradek, Y.Peterzil, F.O.Wagner, *Quasi-o-minimal structures*, Journal of Symbolic Logic, to appear.

[Bel76] A.P.Beltyukov, Decidability of the universal theory of natural numbers with addition and divisibility (in Russian), Zap. Nauchn. Semin. Leningr. Otd. Mat. Inst. Steklova 60, 15-28 (1976).

[Bes97a] A.Bès, *On Pascal triangles modulo a prime power*, Annals of Pure and Applied Logic 89 (1997), 17–35.

[Bes97b] A.Bès, *Undecidable extensions of Büchi Arithmetic and Cobham-Semënov Theorem*, JSL 62(4) (1997), 1280–1296.

[BR98] A.Bès, D.Richard, *Undecidable extensions of Skolem Arithmetic*, Journal of Symbolic Logic 63(2), 379–401 (1998).

[Bes00] A.Bès, *An extension of the Cobham-Semënov Theorem*, J.Symb.Log. 65 (1), 201–211 (2000).

[BV04] G.D.Birkhoff, H.S.Vandiver, *On the integral divisors of* $a^n - b^n$, Ann. Math. 5, 173–180 (1904).

[BG00] A.Blumensath, E.Grädel, *Automatic structures*, Proc. 15th IEEE Symp. on Logic in Computer Science, 2000, 51–62.

[Bof98] M.Boffa, *More on an undecidability result of Bateman, Jockusch and Woods*, J.Symb.Log 63 (1), p.50 (1998).

[Bru85] V. Bruyère, Entiers et automates finis, *Mémoire de fin d'études*, Université de Mons (1985).

[Bru95] V. Bruyère, *Automata and numeration systems*, Semin. Lothar. Comb. 35, 19 pages, 1995

(available on Internet: http://www.emis.de/journals/SLC/).

[BH97] V.Bruyère, G.Hansel, *Bertrand numeration systems and recognizability*, Theoretical Computer Science 181 (1997), 17–43.

[BHMV94] V.Bruyère, G.Hansel, C.Michaux, R.Villemaire, *Logic and p−recognizable sets of integers*, Bull. Belg. Math. Soc. 1, 1994, 191–238.

[Buc60] J. R. Büchi, Weak second-order arithmetic and finite automata, *Z. Math. Logik Grundlag. Math.* **6** (1960) 66–92.

[Buc65] J.R.Büchi, *Transfinite automata recursions and weak second order theory of ordinals*, Logic Methodology Philos. Sci., Proc. 1964 Int. Congr. 3-23 (1965).

[Buc90] J.R.Büchi, The collected works of J.Richard Büchi, Edited by Saunders Mac Lane and Dirk Siefkes, Springer-Verlag (1990).

[Car14] L.C.Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. Math. 15 (2), 30–69, (1913-14).

[Ceg81] P.Cegielski, *Théorie élementaire de la multiplication des entiers naturels*, Model Theory and Arithmetic, Proc., Paris 1979/80, Lect. Notes Math. 890, 44–89 (1981).

[Ceg90] P.Cegielski, *Quelques contributions à l'étude des arithmétiques faibles*, Thèse de doctorat d'état, Université Paris 7, 1990.

[Ceg96] P.Cegielski, *Definability, decidability, complexity*, Ann. Math. Artif. Intell. 16, No.1-4, 311-341 (1996).

[CMR96] P.Cegielski, Y.Matiyasevich, D.Richard, *Definability and decidability issues in extensions of the integers with the divisibility predicate*, JSL 61(2), 515–540 (1996).

[CRV00] P.Cegielski, D.Richard, M.Vsemirnov, *On the additive theory of prime numbers*, Journal of Symbolic Logic (to appear).

[Cha81] Z.Chatzidakis, *La représentation en termes de faisceaux des modèles de la théorie élémentaire de la multiplication des entiers naturels*, Model theory and arithmetic, Proc., Paris 1979/80, Lect. Notes Math. 890, 90-110 (1981).

[CP86] G. Cherlin, F. Point, On extensions of Presburger arithmetic, Proc. 4th Easter Model Theory conference, Gross Köris 1986 Seminarberichte 86, Humboldt Universität zu Berlin (1986) 17–34.

[Cob69] A. Cobham, On the base-dependence of sets of numbers recognizable by finite automata, *Math. Systems Theory* **3** (1969) 186–192.

[Del97] F.Delon, Q muni de l'arithmétique faible de Penzin est décidable. (Q equipped with Penzin's weak arithmetic is decidable), Proc. Am. Math. Soc. 125, No.9, 2711-2717 (1997).

[Dic04] L.E.Dickson, *A new extension of Dirichlet's theorem on prime numbers*, Messenger of Math., 33, 155–161 (1904).

[Dur98] F.Durand, *A generalization of Cobham's theorem* , Theory Comput. Syst. 31 (2), 169–185 (1998).

[Eil74] S. Eilenberg, *Automata, Languages and Machines*, Vol. A, Academic Press, New-York (1974).

[ER66] C. C. Elgot, M. O. Rabin, Decidability and undecidability of second (first) order theory of (generalized) successor, *J. Symbolic Logic* **31** (1966) 169–184.

[End72] H. E. Enderton, *An introduction to mathematical logic*, Academic Press (1972).

[Erd80] P.Erdös, *How many pairs of products of consecutive integers have the same prime factors ?*, Am. Math. Monthly 87 (5), 391–392 (1980).

[Esp99] R.Espel-Lima, *Counting and $k-$recognizability*, Fund.Info. (to appear).

[Fab94] S.Fabre, *Une généralisation du thèorême de Cobham*, Acta Arithmetica 67 (1994), 197-208.

[Fag75] R.Fagin, Monadic generalized spectra, Z. Math. Logik Grundlagen Math. 21, 89-96 (1975).

[Fagn97] I.Fagnot, *Sur les facteurs des mots automatiques*, Theor. Comput. Sci. 172, No.1-2, 67-89 (1997).

[Fagn00] I.Fagnot, *Cobham's Theorem and automaticity in non-standard bases*, preprint

[FV59] S.Feferman and R.L.Vaught, *The first order properties of products of algebraic systems*, Fundamenta Math. 47, 1959, 57-103.

[FeRa79] J.Ferrante, C.W.Rackoff, The computational complexity of logical theories, Lecture Notes in Mathematics. 718 (1979).

[FiRa74] M.J.Fischer, M.O.Rabin, *Super-exponential complexity of Presburger arithmetic*, Complexity of Comput., Proc. Symp. appl. Math., New York City 1973, 27-41 (1974).

[Fra85] A.S.Fraenkel, *Systems of numeration*, Am.Math.Monthly 92 (1985), 105–114.

[FS94] C.Frougny, B.Solomyak, *On representation of integers in linear numeration systems*, in Pollicott, Mark (ed.) et al., Ergodic theory of $\mathbb{Z}^d$ actions. Proceedings of the Warwick symposium, Warwick, UK, 1993-94. New York: Cambridge University Press. Lond. Math. Soc. Lect. Note Ser. 228 (1996), 345–368.

[Fro00] C.Frougny, *Numeration systems*, Algebraic Combinatorics on words, Chapter 7. Cambridge University Press, to appear.

[GS66] S. Ginsburg, E. H. Spanier, Semigroups, Presburger formulas and languages, *Pacific J. Math.* 16 (1966) 285–296.

[Gri91] S.Grigorieff, *Décidabilité et complexité des théories logiques*, in: *Logique et Informatique: une introduction* (Ed. B.Courcelle et M.Nivat), INRIA, 1991, 7–97.

[GR89] S.Grigorieff, D.Richard, *Contribution à l'étude d'une conjecture de théorie des nombres par le codage ZBV*, L'enseignement mathématique, 2eme Serie, Tome 35, Fascicule 1-2, 125–189 (1989).

[Guy94] R.K.Guy, *Unsolved problems in number theory*, 2nd ed. Springer-Verlag (1994).

[Han82] G. Hansel, A propos d'un théorème de Cobham, in : *Actes de la fête des mots*, D. Perrin, Ed., Greco de Programmation, CNRS, Rouen (1982).

[Han98] G.Hansel, *Systèmes de numération indépendants et syndéticité*, Theor. Comp. Science 204, No.1-2, 119–130 (1998).

[Hod82] B.R.Hodgson, *On direct products of automaton decidable theories*, TCS 19 (1982), 331–335.

[Hod83] B.R.Hodgson, Décidabilité par automate fini, *Ann. Sci. Math. Québec* 7 (1983) 39–57.

[Hon86] J. Honkala, A decision method for the recognizability of sets defined by number systems, *RAIRO Inform. Théor. Appl.* **20** (1986) 395–403.

[Kor93] I.Korec, *Definability of arithmetic operations in Pascal triangle modulo an integer divisible by two primes*, Grazer Matematische Berichte 318, 1993, 53- 62.

[Kor95] I.Korec, *Elementary theories of structures containing generalized Pascal triangles modulo a prime* , Proc. of the 5th Conference on Discrete Mathematics and Applications, Blagoevgrad/Predel, ed. S.Shtrakov and Iv.Mirchev, Blagoevgrad, 1995, 91-102.

[Kor96] I.Korec, *Definability of addition from multiplication and neighbourhood relation and some related results*, Nowak, W. G. (ed.) et al., Proceedings of the conference on analytic and elementary number theory: a satellite conference of the European Congress on Mathematics '96, Vienna, July 18–20, 1996. Dedicated to the honour of the 80th birthday of E. Hlawka, Universitaet Wien, Institut fuer Mathematik, Institut fuer Mathematik und Statistik, 137-148 (1996).

[Kor97] I.Korec, *A list of arithmetical structures strongest with respect to the first-order definability*, preprint.

[Kor00] I.Korec, *Definability of arithmetical operations from binary quadratic forms*, preprint.

[Lan92] M.Langevin, *Partie sans facteur carré d'un produit d'entiers voisins*, Approximations diophantiennes et nombres transcendants, C.-R. Colloq., Luminy/ Fr. 1990, 203–214 (1992).

[Lan93] M.Langevin, *Cas d'égalité pour le théorème de Mason et applications de la conjecture (abc) (Extremal cases for Mason's theorem and applications of the (abc) conjecture)*, C.R. Acad. Sci., Paris, Serie I 317, No.5, 441–444 (1993).

[Lan96] M.Langevin, *Sur quelques conséquences de la conjecture (abc) en arithmétique et en logique (On certain consequences of the (abc) conjecture in arithmetic and in logic)*, Rocky Mt. J. Math. 26, No.3, 1031–1042 (1996).

[LM00] T.Lavendhomme, A.Maes, *Note on the undecidability of* $< N; +, P_{m,r} >$, *Cahiers du Centre de Logique* 11, UCL (2000).

[Lip78] L.Lipshitz, The Diophantine problem for addition and divisibility, Trans. Am. Math. Soc. 235, 271-283 (1978).

[Mae98] A.Maes, *Morphisms and almost-periodicity*, Discrete Applied Mathematics 86 (1998), 233–248.

[Mae00a] A.Maes, *More on morphisms and almost-periodicity*, TCS 231 (2000), 205–215.

[Mae00b] A.Maes, *Revisiting Semënov's result about decidability of extensions of Presburger Arithmetic*, *Cahiers du Centre de Logique* 11, UCL (2000).

[Mat70] Y.Matiyasevich, Enumerable sets are diophantine, Sov. Math., Dokl. 11, 354-358 (1970); translation from Dokl. Akad. Nauk SSSR 191, 279-282 (1970).

[Mau97] F.Maurin, *The theory of integer multiplication with order restricted to primes is decidable*, J. Symb. Log. 62, No.1, 123-130 (1997).

[Maz94] B.Mazur, Questions of decidability and undecidability in number theory, J. Symb. Log. 59, No.2, 353-371 (1994).

[MP86] C. Michaux, F. Point, Les ensembles k-reconnaissables sont définissables dans $\langle \mathbb{N}; +, V_k \rangle$, *C. R. Acad. Sci. Paris* **303** (1986) 939–942.

[MV93] C. Michaux, R. Villemaire, Cobham's theorem seen through Büchi theorem, Proc. Icalp'93, *Lecture Notes in Comput. Sci.* **700** (1993) 325–334.

[MV96a] C.Michaux, R.Villemaire, *Presburger arithmetic and recognizability of sets of natural numbers by automata: new proofs of Cobham's and Semenov's theorems*, Annals of Pure and Applied Logic 77 (1996), 251–277. .

[MV96b] C.Michaux, R.Villemaire, *Open questions around Büchi and Presburger arithmetics*, *in*: Logic: From foundations to applications, Proc. European Logic Colloquium'93, Oxford University Press (1996), 353–383.

[Mos52] A.Mostowski, *On direct products of theories*, J. Symbolic Logic 17, 1-31 (1952).

[Muc91] A. Muchnik, Definable criterion for definability in Presburger Arithmetic and its application, *preprint in Russian*, Institute of New Technologies (1991).

[Nar86] W.Narkiewicz, Classical problems in number theory, PWN, Warsaw, 1986.

[Nez97] F.Nézondet, *$p-$destinée et applications à la théorie du successeur et de la coprimarité sur les entiers*, Ph.D. Thesis, Université d'Auvergne, 1997.

[Per90] D. Perrin, Finite automata, in: *Handbook of Theoretical Computer Science*, vol. B, J. Van Leeuwen, Ed., Elsevier (1990) 2–57.

[Phe94] T.Pheidas, Extensions of Hilbert's tenth problem, J. Symb. Log. 59, No.2, 372-397 (1994).

[Pin96] J.E.Pin, Logic, semigroups and automata on words, Ann. Math. Artif. Intell. 16, No.1-4, 343-384 (1996).

[Poi00a] F.Point, *On extensions of Presburger Arithmetic*, Cahiers du Centre de Logique 11, UCL (2000).

[Poi00b] F.Point, *On decidable extensions of Presburger Arithmetic: from A.Bertrand numeration systems to Pisot numbers*, J. Symb. Logic (to appear).

[PB97] F.Point, V.Bruyère, *On the Cobham-Semenov theorem*, Theory of Computing Systems 30 (1997), 197–220.

[PW00] F.Point, F.O.Wagner, *Essentially periodic ordered groups*, Annals of Pure and Applied Logic, to appear.

[Pre29] M.Presburger, On the completeness of a certain system of arithmetic of whole numbers in which addition occurs as the only operation, Hist. Philos. Logic 12, No.2, 225-233 (1991), reprint of M. Presburger, Über die Volständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt, *C. R. 1er congrès des Mathématiciens des pays slaves*, Varsovie (1929) 92–101.

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

[Rab65] M.O.Rabin, *A simple method for undecidability proofs and some applications*, Logic Methodology Philos. Sci., Proc. 1964 internat. Congr. 58-68 (1965).

[Rab69] M.O.Rabin, *Decidability of second order theories and automata on infinite trees*, Trans. Amer. Math. Soc. 141, 1-35, 1969

[Rab77] M. O. Rabin, Decidable theories, in : *Handbook of Mathematical Logic*, J. Barwise, Ed., North Holland, Amsterdam (1977) 595–629.

[Ram95] O.Ramare, *On Snirel'man constant*, Ann. Sc. Norm. Super. Pisa, Cl.Sci, IV Ser.22, No 4, 645–706, 1995.

[RV83] H.Reisel, R.C.Vaughan, *On sums of primes*, Ark. für Math. 21, number 1, 45-74 (1983).

[Res00] J.P.Ressayre, *Weak Arithmetics*, preprint.

[Rib96] P.Ribenboim, The new book of prime number records, 3rd ed, Springer-Verlag (1996).

[Ric84] D.Richard, *The arithmetics as theories of two orders*, Annals of Discrete Mathematics 23, 287–312 (1984).

[Ric85a] 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, 221–247 (1985).

[Ric85b] D.Richard, *Définissabilité en arithmétique et méthode de codage ZBV appliquée à des langages avec successeur et coprimarité*, Thèse d'Etat, Université de Lyon, 1985.

[Ric89] D.Richard, *Equivalence of some questions in mathematical logic with some conjectures in number theory*, Number Theory and Applications, Richard MOLLIN ed., NATO ASI Series, Series C: Mathematical and Physical Sciences, Vol. 265, 529-545 (1989).

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

[Rob58] R.M.Robinson, *Restricted set-theoretical definitions in arithmetic*, Proc. Am. Math. Soc. 9, 238-242 (1958).

[RS97] C.C.Rodriganez, R.Schoof, *The support problem and its elliptic analogue*, J.Number Theory 64 (2), 276–290 (1997).

[Sem77] A.L. Semenov, Presburgerness of predicates regular in two number systems (in Russian), *Sibirsk. Mat. Zh.* 18 (1977) 403–418, English translation, *Siberian Math. J.* 18 (1977) 289–299.

[Sem79] A.L. Semenov, On certain extensions of the arithmetic of addition of natural numbers, *Izv. Akad. Nauk. SSSR ser. Mat.* 43 (1979) 1175–1195, English translation, *Math. USSR-Izv.* 15 (1980) 401–418.

[Sem83] A.L. Semenov, Logical theories of one-place functions on the set of natural numbers (in Russian), *Izv. Akad. Nauk. SSSR ser. Mat.* 47 (1983) 623–658, English translation, *Math. USSR-Izv.* 22 (1984) 587–618.

[Sha82] H.Shapiro, Introduction to the theory of numbers, Wiley, NY, 1982.

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

[Smo91] C.Smorynski, Logical Number Theory I, Springer-Verlag (1991).

[Tho76] W.Thomas, *A note on undecidable extensions of monadic second order successor arithmetic*, Arch. Math. Logik. 17, 1975, 43–44.

[Tho79] , W.Thomas, *Star-free regular sets of $\omega-$sequences*, Inf. Control 42, 1979, 148–156.

[Tho97] W.Thomas, Languages, Automata, and Logic, in: Handbook of Formal Language Theory (G. Rozenberg, A. Salomaa, Eds.),Vol. III, Springer-Verlag , New York, 389-455 (1997).

[vdD85] L. van den Dries, The field of reals with a predicate for the powers of two, *Manuscripta Math.* 54 (1985) 187–195.

[Vil92a] R. Villemaire, Joining k- and l-recognizable sets of natural numbers, Proc. Stacs'92, *Lecture Notes in Comput. Sci.* 577 (1992) 83–94.

[Vil92b] R. Villemaire, The theory of $\langle \mathbb{N}; +, V_k, V_l \rangle$ is undecidable, *Theoret. Comput. Sci.* 106 (1992) 337–349.

[Vse00] M.Vsemirnov, *The Woods-Erdös conjecture for polynomial rings*, Annals of Pure and Applied Logic (to appear).

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

[Zsi] K.Zsigmondy, *Zur Theorie der Potenzreste*, Monatshefte Math. Phys. 3, 265–284 (1892).

Table of main notations

S	the successor function
$\mathrm{Neib}(x, y)$	holds whenever $\lvert x - y\rvert = 1$
$+$	addition function
$+_g$	graph of addition
$\times$	multiplication function
$\times_g$	graph of multiplication
$\mid$	divisibility relation
$\perp$	relative primeness relation ($x \perp y$ iff $\gcd(x, y) = 1$)
P	the set of primes
$\pi(n)$	the $n-$th prime ($(\pi(0) = 2, \pi(1) = 3, \dots)$
Π	the set of primary numbers (powers of primes)
$\mathrm{Supp}(x)$	the set of prime divisors of x (its *support*)
$x \sim y$	holds whenever $\mathrm{Supp}(x)$ and $\mathrm{Supp}(y)$ have the same cardinality
C	the set of squares
P_k	the set of powers of k
$V_k(x)$	the greatest power of k which divides x (with $V_k(0) = 1$)
$[x]_k$	the $k-$ary expansion of x (e.g. $[12]_2 = 1100$)
$<_X$	the restriction of the usual order relation to $X \subseteq \mathbb{N}$
$S^+(\mathbb{N})$	the set of finite subsets of $\mathbb{N}$
$S^*(\mathbb{N})$	the set of finite or co-finite subsets of $\mathbb{N}$
$A^e(\mathbb{N})$	the set of functions $f : \mathbb{N} \to A$ such that $f(n) = e$ for almost all n
$\mathrm{FIN}(X)$	holds whenever $X \subseteq \mathbb{N}$ is finite

Service de Science des Systèmes d'Information
Université de Mons-Hainaut
E-mail: bes@logique.jussieu.fr