Undecidable Extensions of Büchi Arithmetic and Cobham-Semënov Theorem

Alexis Bès

Published in J.Symb.Logic 62(4), 1280–1296 (1997)

Abstract

Let k and l be two multiplicatively independent integers, and let $L \subseteq \mathbb{N}^n$ be a $l-$recognizable set which is not definable in $\langle \mathbb{N}; + \rangle$. We prove that the elementary theory of $\langle \mathbb{N}; +, V_k, L \rangle$, where $V_k(x)$ denotes the greatest power of k dividing x, is undecidable. This result leads to a new proof of the Cobham-Semënov theorem.

1. Introduction

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. Bruyère proved in [Bru85] that the (first-order) definable sets of $\langle \mathbb{N}; +, V_k \rangle$ coincide with the $k-$recognizable sets. This result implies (see e.g. [Hod83]) the decidability of the elementary theory of $\langle \mathbb{N}; +, V_k \rangle$. On the other hand, Villemaire proved ([Vil92a], see also [Vil92b]) that for k and l multiplicatively independent (i.e. $k^a \neq l^b$ for all nonzero integers a, b) the elementary theory of $\langle \mathbb{N}; +, V_k, V_l \rangle$ is undecidable. In this paper we improve the latter result by showing that for k and l multiplicatively independent, if $L \subseteq \mathbb{N}^n$ is $l-$recognizable and not definable in $\langle \mathbb{N}; + \rangle$ then the elementary theory of $\langle \mathbb{N}; +, V_k, L \rangle$ is undecidable. This answers a question of Michaux and Villemaire [MV93].

In order to obtain such a result, we first prove in Section 3 that for every $l-$recognizable set $L \subseteq \mathbb{N}^n$ which is not definable in $\langle \mathbb{N}; + \rangle$, the set P_l of powers of l is definable in the structure $\langle \mathbb{N}; +, L \rangle$; the proof rests on automata theory arguments and uses two theorems of Michaux and Villemaire related to proper extensions of Presburger Arithmetic. In Section 4, by use of simple arithmetical tools and following the structure of Villemaire's proof for $\langle \mathbb{N}; +, V_k, V_l \rangle$, it is proved that for k, l multiplicatively independent, multiplication is definable in the structure $\langle \mathbb{N}; +, V_k, P_l \rangle$.

Section 5 deals with the Cobham-Semënov Theorem, which states that for k, l multiplicatively independent, every subset of $\mathbb{N}^n$ which is $k-$ and $l-$recognizable is definable in $\langle \mathbb{N}; + \rangle$. We show that the previous results provide simple arguments to prove this theorem.

2. Preliminaries

This section provides the basic notations, definitions, results and tools that will be used in the paper.

2.1 Finite automata and $k-$recognizable sets

Let Σ be a finite alphabet. We denote by Σ^* the set of finite words over Σ, including the empty word denoted by λ. For every $u \in \Sigma^*$ we shall denote by $|u|$ the length of u. For all $u, v \in \Sigma^*$, we shall say that u is a *right factor* of v if there exists $w \in \Sigma^*$ such that $v = w \cdot u$. We shall speak of *strict* factor in the case where $w \neq \lambda$.

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*. As usual, δ is extended in a natural way to a function $\delta^* : Q \times \Sigma^*$ as follows:

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

A word $w \in \Sigma^*$ is *accepted* by the Σ-automaton $\mathcal{A} = (Q, q_0, \delta, Q')$ if $\delta^*(q_0, w) \in Q'$. We say that a state $q \in Q$ is *visited* during the computation of w by $\mathcal{A}$ if there exists a right factor v of w such that $\delta^*(q_0, v) = q$.

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

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

Conversely for every word $w \in \Sigma_l^*$, $w \neq \lambda$, if $w = \lambda_t \ \ldots \lambda_0$ (with $\lambda_i \in \Sigma_l$) we denote by $\overline{w}^l$ the integer $x = \sum_{i=0}^{t} \lambda_i l^i$. Moreover we set $\overline{\lambda}^l = 0$.

Definition 2.1. A set $M \subseteq \mathbb{N}$ is said to be $l-$*recognizable* if the set $[M]_l$ is Σ_l-recognizable.

The previous notion can be extended to subsets of $\mathbb{N}^n$. For every $n-$tuple $x = (x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ we define $[x]_l$ as the word (of $n-$tuples)

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

over Σ_l^n, where $m_i = |x_i|$ and $m = \max\{m_1, \ldots, m_n\}$. As previously for every $M \subseteq \mathbb{N}^n$ we shall denote by $[M]_l$ the set $\{[a]_l \mid a \in M\}$.

Definition 2.2. A set $M \subseteq \mathbb{N}^n$ is said to be $l-$*recognizable* if the set $[M]_l$ is Σ_l^n-recognizable.

2.2 Logic and $k-$recognizable sets

For every integer $k \geq 2$, let V_k denote the function which maps every nonzero integer x to the greatest power of k dividing x.

The following theorem, which was stated (in an incorrect form) by Büchi ([Buc60]) and proved by Bruyère ([Bru85]), settles the link between $k-$recognizable sets and Büchi Arithmetic of base k.

Theorem 2.3. (Büchi-Bruyère) *Let k be an integer greater than 1. A subset of $\mathbb{N}^n$ is $k-$recognizable if and only if it is definable in the structure $\langle \mathbb{N}; +, V_k \rangle$.*

This theorem admits the following corollary (see [Bru85], [Hod83]):

Corollary 2.4. *For every integer $k \geq 2$ the elementary theory of $\langle \mathbb{N}; +, V_k \rangle$ is decidable.*

Extensions of Büchi Arithmetic were first considered in [CP86], where the authors prove that the elementary theory of $\langle \mathbb{N}; +, V_k, x \mapsto k^x \rangle$ is undecidable. On the other hand, one can ask whether the situation changes if we add to the language $\{+, V_k\}$ the function V_l.

Definition 2.5 Two integers $k, l \geq 2$ are said to be *multiplicatively independent* if for all nonzero integers a, b we have $k^a \neq l^b$; otherwise we say that k, l are multiplicatively dependent.

It is easy to check that if k and l are multiplicatively dependent integers then V_l is definable in the structure $\langle \mathbb{N}; +, V_k \rangle$. However for k, l multiplicatively independent the situation, as testifies the following result which is due to Villemaire ([Vil92a], see also [Vil92b]), is quite different.

Theorem 2.6. **(Villemaire)** *If k and l are multiplicatively independent then multiplication is definable in the structure $\langle \mathbb{N}; +, V_k, V_l \rangle$. Therefore the elementary theory of this structure is undecidable.*

We prove in the sequel that the function V_l can be replaced in the previous theorem by any $l-$recognizable set $L \subseteq \mathbb{N}^n$ which is not definable in $\langle \mathbb{N}; + \rangle$.

2.3 Definability tools

Throughout the paper we shall work within extensions of Presburger arithmetic $\langle \mathbb{N}; + \rangle$. The following relations and functions are easily definable in this structure:
- the relations $x < y$ and $x \geq y$, denoted in the same way;
- for every constant c, the function, denoted by $\mathrm{MULT}_c(x)$, which maps every integer x to cx;
- for every constant c, the relation $x \equiv y \pmod{c}$, denoted by $\mathrm{CONGR}_c(x, y)$.

Let A be an infinite subset of $\mathbb{N}$. We denote by NEXT_A the function which maps every $x \in A$ to the least $y \in A$ greater than x. The function NEXT_A is definable in the structure $\langle \mathbb{N}; +, A \rangle$ by the formula

$$[y = \mathrm{NEXT}_A(x)] \Longleftrightarrow \{A(x) \wedge A(y) \wedge x < y \ \wedge \neg \exists z [x < z < y \wedge A(z)]\}.$$

Moreover, we shall use the following lemma. Recall that for any integer $n \geq 2$, we denote by P_n the set of powers of n.

Lemma 2.7. *If a and b are two multiplicatively dependent integers then P_b is definable in $\langle \mathbb{N}; +, P_a \rangle$.*

Proof. Let m and n be two positive integers such that $a^m = b^n$. The set of powers of a^m (that is, b^n) is the set of powers a^i of a such that

$$a^i \equiv 1 \pmod{a^m - 1}$$

Therefore P_{b^n} is definable in $\langle \mathbb{N}; +, P_a \rangle$ by the formula

$$P_{b^n}(x) \Longleftrightarrow [P_a(x) \wedge \mathrm{CONGR}_{a^m-1}(x, 1)]$$

From this we can deduce a definition of P_b in the structure $\langle \mathbb{N}; +, P_a \rangle$:

$$P_b(x) \Longleftrightarrow \big[\exists y \ \big(P_{b^n}(y) \ \wedge \ \bigvee_{i=0}^{n-1} \mathrm{MULT}_{b^i}(x) = y\big)\big].$$

□

3. Definability within $\langle \mathbb{N}; +, L \rangle$

For every $l \in \mathbb{N}$ let us denote by P_l the set of powers of l. The aim of this section is to prove the following result:

Theorem 3.1. *Let $l \geq 2$, $n \geq 1$ be two integers. If $L \subseteq \mathbb{N}^n$ is $l-$recognizable and not definable in $\langle \mathbb{N}; + \rangle$ then P_l is definable in $\langle \mathbb{N}; +, L \rangle$.*

Remark: it follows from theorem 2.3 that if L is $l-$recognizable then L is definable in $\langle \mathbb{N}; +, V_l \rangle$. Thus every relation definable in $\langle \mathbb{N}; +, L \rangle$ is definable in $\langle \mathbb{N}; +, V_l \rangle$ too, and therefore is $l-$recognizable (by virtue of the same theorem).

We shall make use of two theorems due to Michaux and Villemaire [MV96] (these results will be discussed in the last section of the paper).

Definition 3.2. Let $(a_n)_{n \in \mathbb{N}}$ be a strictly increasing sequence of integers, and let $A = \{a_n : n \in \mathbb{N}\}$. We say that A is *expanding* if the set $\{a_{n+1} - a_n : n \in \mathbb{N}\}$ is not bounded.

Theorem 3.3. (Michaux-Villemaire) *Let $A \subseteq \mathbb{N}$. If A is not definable in $\langle \mathbb{N}; + \rangle$ then there exists an expanding set $A' \subseteq \mathbb{N}$ which is definable in $\langle \mathbb{N}; +, A \rangle$.*

Theorem 3.4. (Michaux-Villemaire) *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 $\langle \mathbb{N}; + \rangle$.*

Proof of theorem 3.1. Let $L \subseteq \mathbb{N}^n$ be a $l-$recognizable set which is not definable in $\langle \mathbb{N}; + \rangle$. By theorem 3.4 there exists a set $L' \subseteq \mathbb{N}$ which is definable in $\langle \mathbb{N}; +, L \rangle$ and not definable in $\langle \mathbb{N}; + \rangle$. Then by theorem 3.3 we get an expanding set L'' which is definable in $\langle \mathbb{N}; +, L' \rangle$. Let $(l_n)_{n \in \mathbb{N}}$ be the sequence of elements of L'' arranged in increasing order. Now let M be the subset of L'' defined as follows:

$x \in M$ if and only if there exists $i \in \mathbb{N}$ such that:

(1) $x = l_i$;

(2) For every $j < i$ we have $l_{j+1} - l_j < l_{i+1} - l_i$.

The set L'' is expanding, thus M is infinite. Let $(m_n)_{n \in \mathbb{N}}$ be the sequence of elements of M arranged in increasing order. Let us prove that

$$\forall n \in \mathbb{N} \qquad m_{n+1} - m_n \geq n \tag{P}$$

Consider the function f which maps any $y \in L''$ to

$$f(y) = \mathrm{NEXT}_{L''}(y) - y.$$

Remark that

$$M = \{x \in L'' \;\mid\; \forall y \in L''(y < x \Longrightarrow f(y) < f(x))\};$$

from the definition of f and M it follows that

$$\forall n \in \mathbb{N} \qquad m_{n+1} - m_n \geq f(m_n) \geq n.$$

The set M is definable in $\langle \mathbb{N}; +, L'' \rangle$ by the formula

$$M(x) \Longleftrightarrow \big[L''(x) \wedge \; \forall y\{[y < x \wedge L''(y)] \Longrightarrow [\mathrm{NEXT}_{L''}(y) + x < \mathrm{NEXT}_{L''}(x) + y]\}\big].$$

M is *a fortiori* definable in $\langle \mathbb{N}; +, L \rangle$, and thus $l-$recognizable.

Now for the remainder of the proof of theorem 3.1 we fix

$$\mathcal{A} = (Q, q_0, \delta, Q')$$

as the Σ_l-automaton recognizing $[M]_l$.

The two following lemmas highlight some interesting consequences of property (P) for the set $[M]_l$.

Lemma 3.5. *Let $u, v, w_1, w_2 \in (\Sigma_l)^*$, $v \neq \lambda$. If $|w_1| = |w_2|$, and furthermore if for every $n \in \mathbb{N}$, $uv^n w_1$ and $uv^n w_2$ belong to $[M]_l$, then $w_1 = w_2$.*

Proof. Let c be the length of w_1 and w_2. Assume that $w_1 \neq w_2$. The hypothesis $| w_1 |=| w_2 |$ yields $\overline{w_1}^l \neq \overline{w_2}^l$. Assume, for example, $\overline{w_1}^l < \overline{w_2}^l$. Let $a = \overline{w_2}^l - \overline{w_1}^l$, and let N be an integer such that $\overline{uv^N w_1}^l \geq m_{a+1}$ (such an integer exists since $v \neq \lambda$). Then there exist $i_1, i_2 \geq a+1$ such that $\overline{uv^N w_1}^l = m_{i_1}$ and $\overline{uv^N w_2}^l = m_{i_2}$. Then

$$m_{i_2} - m_{i_1} = \overline{uv^N w_2}^l - \overline{uv^N w_1}^l = (\overline{uv^N}^l \cdot l^c + \overline{w_2}^l) - (\overline{uv^N}^l \cdot l^c + \overline{w_1}^l) = \overline{w_2}^l - \overline{w_1}^l = a$$

Now

$$m_{i_2} - m_{i_1} \geq m_{i_1+1} - m_{i_1}$$

and it follows from (P) that

$$m_{i_1+1} - m_{i_1} \geq i_1 \geq a+1$$

which cannot be. □

Let $S \subseteq (\Sigma_l)^*$ be the set of words w such that

(1) w is accepted by $\mathcal{A}$

(2) There do not exist two distinct right factors of w, say w_1 and w_2, such that

$$\delta^*(q_0, w_1) = \delta^*(q_0, w_2)$$

(that is, no state is visited several times during the computation of w by $\mathcal{A}$).

It is easily seen that S is not empty, and finite. Now let $B \subseteq (\Sigma_l)^*$ be the set of words w such that

(1) w is a right factor of some element in S

(2) there exists a word $u \neq \lambda$ such that $\delta^*(q_0, w) = \delta^*(q_0, uw)$

$[M]_l$ is infinite, thus B is not empty. Let b be an element of B of minimal length. The set $C = \{u : u \neq \lambda \ \textit{ and } \ \delta^*(q_0, b) = \delta^*(q_0, ub)\}$ is not empty; let v be an element of C of minimal length.

Let $M' \subseteq \mathbb{N}$ be the set $x \in M$ such that $[x]_l$ admits b for right factor.

Lemma 3.6. $[M']_l = \{av^n b | n \in \mathbb{N} \ \text{ and } \ ab \in S\}$

Proof. Let $a \in (\Sigma_l)^*$ and $n \in \mathbb{N}$. Suppose that $ab \in S$. From the definition of v we have $\delta^*(q_0, av^n b) = \delta^*(q_0, ab)$, thus $av^n b$ is accepted by $\mathcal{A}$, and $av^n b \in [M']_l$.

For the converse, let u be an element of $[M']_l$. There exists $a \in (\Sigma_l)^*$ and $n \in \mathbb{N}$, such that $u = av^n b$ and v is not a right factor of a. Let us show that ab belongs to S. The word $av^n b$ is accepted by $\mathcal{A}$, and $\delta^*(q_0, av^n b) = \delta^*(q_0, ab)$; therefore ab is accepted by $\mathcal{A}$. Thus there remains to show that no state is visited several times during the computation of ab by $\mathcal{A}$. Assume the contrary. Let b' be the smallest right factor of ab for which there exists w right factor of ab and distinct from b' such that $\delta^*(q_0, b') = \delta^*(q_0, w)$. Then there exist $a', z \in (\Sigma_l)^*$, $z \neq \lambda$ such that $ab = a'zb'$ and $\delta^*(q_0, b') = \delta^*(q_0, zb')$. The word b is a right factor of b', otherwise b' is a strict right factor of b, and the fact that $\delta^*(q_0, b') = \delta^*(q_0, zb')$ yields $b' \in B$, which contradicts the minimality of b. By setting $b' = a''b$ we then have $ab = a'za''b$ with $\delta^*(q_0, a''b) = \delta^*(q_0, za''b)$. Moreover $\delta^*(q_0, b) = \delta^*(q_0, vb)$. Thus for all $m_1, m_2 \in \mathbb{N}$, the word $a'z^{m_1}a''v^{m_2}b$ is accepted by $\mathcal{A}$. Let $r = |v|$ and $s = |z|$. For every $m \in \mathbb{N}$, the words $a'z^m z^r a''b$ and $a'z^m a''v^s b$ are accepted by $\mathcal{A}$. But

$$|z^r a''b| = s\ r + |a''| + |b| = |a''v^s b|$$

From lemma 3.5 we thus obtain $z^r a''b = a''v^s b$, that is

$$z^r a'' = a''v^s \tag{E}$$

If $|v| > |za''|$ then from (E) the word za'' is a strict right factor of v; but $\delta^*(q_0, a''b) = \delta^*(q_0, za''b)$, and this contradicts the minimality of v. It follows that $|v| \leq |za''|$ and by (E), v is a right factor of za'', *a fortiori* of $a = a'za''$, which contradicts the hypothesis on a. □

The set M' is definable in $\langle \mathbb{N}; +, M\rangle$ by the formula

$$M'(x) \Longleftrightarrow \left[M(x) \wedge \mathrm{CONGR}_{l^e}(x, \overline{b}^l)\right] \quad (\text{with} \quad e = |b|).$$

We will denote by $(m'_n)_{n\in\mathbb{N}}$ the sequence of elements of M' arranged in increasing order.

Let $U = \{u \mid u \cdot b \in S\}$. The set U is not empty and finite. From the previous lemma we get

$$[M']_l = \{uv^n b \mid n \in \mathbb{N} \text{ and } u \in U\} \tag{E'}$$

Lemma 3.7. *For every $w \in [M']_l$ there exists a single $u \in U$ and a single $n \in \mathbb{N}$ such that $w = uv^n b$.*

Proof. The identity (E') ensures us of the existence of u and n. For unicity, suppose that there exist $u, u' \in U$ and $n, n' \in \mathbb{N}$ such that $uv^n b = u'v^{n'} b$, with $n \leq n'$. We have $u = u'v^{n'-n}$. From the definition of U we have $u'v^{n'-n}b \in S$, and the fact that $\delta^*(q_0, b) = \delta^*(q_0, v^{n'-n}b)$ implies $n = n'$, and then $u = u'$. □

Let $p = \mathrm{Card}(U)$.

Lemma 3.8. *There exists $N \in \mathbb{N}$ such that for every integer $n > N$, for every $u \in U$ and every $r \in \mathbb{N}$, if $m'_n = \overline{uv^r b}^l$ then $m'_{n+p} = \overline{uv^{r+1} b}^l$.*

Proof. Let $\mu = \max\{\overline{uvb}^l \mid u \in U\}$ and let N be the integer such that $m'_N = \mu$. Let $n > N$; from the previous lemma there exists a single $u \in U$ and a single $r \in \mathbb{N}$ such that $m'_n = \overline{uv^r b}^l$.

Let us show that for every element u' of U different from u, there exists a single integer n' such that

$$\overline{uv^r b}^l < \overline{u'v^{n'} b}^l < \overline{uv^{r+1} b}^l$$

Let u' be an element of U, different from u, and let n' be the least integer such that $\overline{uv^r b}^l < \overline{u'v^{n'} b}^l$. We have $\overline{u'v^{n'} b}^l > m'_N$, thus $n' \geq 1$. Let us show that

$$\overline{u'v^{n'-1} b}^l < \overline{uv^r b}^l < \overline{u'v^{n'} b}^l < \overline{uv^{r+1} b}^l < \overline{u'v^{n'+1} b}^l \tag{E''}$$

The minimality of n' yields $\overline{u'v^{n'-1}b}^l \leq \overline{uv^rb}^l$, and by lemma 3.7 this inequality is a strict one. This yields $\overline{u'v^{n'}b}^l < \overline{uv^{r+1}b}^l$; finally $\overline{uv^rb}^l < \overline{u'v^{n'}b}^l$ implies $\overline{uv^{r+1}b}^l < \overline{u'v^{n'+1}b}^l$.

The sequence $(\overline{u'v^nb}^l)_{n\in\mathbb{N}}$ is strictly increasing, thus (E'') ensures us that n' is the only integer n such that

$$\overline{uv^rb}^l < \overline{u'v^nb}^l < \overline{uv^{r+1}b}^l$$

We thus have shown that for every $u' \in U$ different from u, there exists a single $n' \in \mathbb{N}$ such that $\overline{uv^rb}^l < \overline{u'v^{n'}b}^l < \overline{uv^{r+1}b}^l$. This implies that there exist at most $p-1$ elements of M' between $\overline{uv^rb}^l$ and $\overline{uv^{r+1}b}^l$. By lemma 3.7 these $p-1$ elements are distinct; therefore

$$\overline{uv^{r+1}b}^l = m'_{n+p}$$

$\square$

Let us now consider the sequence $(d_n)_{n\in\mathbb{N}}$ defined for every $n \in \mathbb{N}$ by

$$d_n = m'_{n+1} - m'_n.$$

Recall that N is the constant defined in the previous lemma.

Lemma 3.9. *Let $r = |v|$. For every $n > N$, $d_{n+p} = l^r \cdot d_n$.*

Proof. Let $n > N$. There exist $u_1, u_2 \in U$ and $s_1, s_2 \in \mathbb{N}$ such that

$$m'_n = \overline{u_1v^{s_1}b}^l \quad \text{and} \quad m'_{n+1} = \overline{u_2v^{s_2}b}^l.$$

By lemma 3.8 we have

$$m'_{n+p} = \overline{u_1v^{s_1+1}b}^l \quad \text{and} \quad m'_{n+p+1} = \overline{u_2v^{s_2+1}b}^l.$$

Therefore

$$\begin{array}{rcl}
d_{n+p} & = & m'_{n+p+1} - m'_{n+p} \\
& = & \overline{u_2v^{s_2+1}b}^l - \overline{u_1v^{s_1+1}b}^l \\
& = & (\overline{u_2v^{s_2}}^l \cdot l^{|vb|} + \overline{vb}^l) - (\overline{u_1v^{s_1}}^l \cdot l^{|vb|} + \overline{vb}^l) \\
& = & (\overline{u_2v^{s_2}}^l - \overline{u_1v^{s_1}}^l) \cdot l^{r+|b|} \\
& = & l^r \cdot (\overline{u_2v^{s_2}b}^l - \overline{u_1v^{s_1}b}^l) \\
& = & l^r \cdot (m'_{n+1} - m'_n) \\
& = & l^r \cdot d_n.
\end{array}$$

$\square$

Now consider the set $D = \{d_n \mid n > N\}$. The previous lemma yields the existence of p integers $c_0, c_1, \ldots, c_{p-1}$ such that

$$D = \bigcup_{i=0}^{p-1} \{c_i l^{rn} \mid n \in \mathbb{N}\}.$$

Moreover D is definable in $\langle \mathbb{N}; +, M' \rangle$ by the formula

$$D(x) \Longleftrightarrow \{\exists y[M'(y) \wedge y > m'_N \wedge x + y = \mathrm{NEXT}_{M'}(y)]\}.$$

For the remainder of the proof we set $m = l^r$. We shall denote by $x \bot y$ the relation "x is prime to y". For every integer x we denote by $\mathrm{Supp}(x)$ the *support* of x, that is the set of its prime divisors.

Let $c \in \mathbb{N}$ be such that $c \cdot c_0 = e \cdot m^n$, with $e \bot m$. Let $E = \{cx \mid x \in D\}$. If we set $c'_i = c\dot{c}_i$ for $i = 0, 1, \ldots, p-1$, we have

$$E = \bigcup_{i=0}^{p-1} \{c'_i m^n \mid n \in \mathbb{N}\}.$$

Moreover E is obviously definable in the structure $\langle \mathbb{N}; +, D\rangle$. We now intend to describe a congruence system whose set of solutions, restricted to E, is of the form $\{c'_0 m^{tn} \mid n \in \mathbb{N}\}$ for some integer $t \geq 1$.

For $i = 0, 1, \ldots, p-1$ we write c'_i as $c'_i = e_i \cdot g_i \cdot m^{n_i}$ with $e_i \bot m$, $\mathrm{Supp}(g_i) \subseteq \mathrm{Supp}(m)$ and n_i maximal. From the hypothesis on c we have $e_0 = e$ and $g_0 = 1$. Let $t \in \mathbb{N}$ be such that

$$m^t > \max(m^{n_0}, 1 + \max_{0 \leq i \leq p-1}(g_i)).$$

For any $r \in \mathbb{R}$, let us denote by $\lfloor r \rfloor$ the integer part of r. Further, for any prime q and any $x, \alpha \in \mathbb{N}$, we denote $q^\alpha || x$ for "$q^\alpha | x$ and $q^{\alpha+1} \not| x$". Let $F \subseteq \mathbb{N}$ be the set of integers x satisfying the three following conditions:

(1) for any prime q and any $\alpha \in \mathbb{N}$, if $q^\alpha || e_0$ then $q^\alpha || x$;

(2) for any prime q, if $q \not| e_0$ and $q | e_j$ for some $j \neq 0$, then $q \not| x$;

(3) $\left\lfloor \dfrac{x}{e_0} \right\rfloor \equiv l^{n_0} \pmod{m^t - 1}$.

Using the relation $\mathrm{CONGR}_c(x, y)$ one easily define F in $\langle \mathbb{N}; +, E\rangle$.

Lemma 3.10. *The following equality holds:*

$$E \cap F = \{c'_0 \cdot m^{tn} \mid t \in \mathbb{N}\}.$$

Proof. One checks that any integer of the form $c'_0 m^{tn}$, for some $n \in \mathbb{N}$, satisfies the three above conditions, and therefore belongs to $E \cap F$. For the converse inclusion, assume that $x \in E \cap F$. The integer x belongs to E, thus $x = c'_i m^n = e_i g_i m^{n_i + n}$ for some $i \in \{0, 1, \ldots, p-1\}$ and $n \in \mathbb{N}$. Now $x \in F$; therefore conditions (1) and (2) yield $e_i = e_0$. Then condition (3) imply that

$$g_i m^{n_i + n} \equiv m^{n_0} \pmod{m^t - 1}.$$

Since

$$m^t \equiv 1 \pmod{m^t - 1}$$

it follows that there exists $u \in \{0, 1, \ldots, t-1\}$ such that

$$g_i \equiv m^u \pmod{m^t - 1}.$$

The very definition of t and u then implies $g_i < m^t - 1$ and $m^u < m^t - 1$; this together with the previous congruence yields $g_i = m^u$. Now the definition of g_i (using the maximality of n_i) leads to $u = 0$, that is $g_i = 1$. Since $e_i = e_0$ and $g_i = 1$ we get

$$m^{n_i + n} \equiv m^{n_0} \pmod{m^t - 1}.$$

By our hypothesis on t, we have $m^{n_0} < m^t - 1$, therefore the previous congruence yields the existence of $k \in \mathbb{N}$ such that $n + n_i = n_0 + kt$. Finally

$$x = e_0 m^{n_i+n} = e_0 m^{n_0+kt} = c_0' m^{kt}$$

thus $x \in \{c_0' m^{tn} \mid n \in \mathbb{N}\}$, which implies $x \in E \cap F$. $\square$

We can complete now the proof of theorem 3.1. Indeed with the previous lemma one defines in $\langle \mathbb{N}; +, E\rangle$ the set P_{m^t} by the formula

$$P_{m^t}(x) \Longleftrightarrow \{\exists y[E(y) \wedge F(y) \wedge x = \mathrm{MULT}_{c_0'}(y)]\}.$$

Then by lemma 2.7, the set P_l is definable in $\langle \mathbb{N}; +, P_{m^t}\rangle$, and therefore definable in $\langle \mathbb{N}; +, L\rangle$. $\square$

4. Definability within $\langle \mathbb{N}; +, V_k, P_l\rangle$

In this section we show the following:

Theorem 4.1. *For all multiplicatively independent integers k and l, multiplication is definable in the structure $\langle \mathbb{N}; +, V_k, P_l\rangle$.*

The following result, which is due to Villemaire [Vil92b], is a first-order version of a Thomas' theorem [Tho75] related to extensions of the monadic second order theory of successor (this theorem being itself a generalization of results by Elgot and Rabin [ER66]).

Theorem 4.2. (Villemaire). *Let $k \in \mathbb{N}$, and let f be a function from P_k to P_k which satisfy the following properties:*

(1) *For every $n \in \mathbb{N}$, $f(k^{n+1}) \geq k \cdot f(k^n)$ (f is strictly increasing);*

(2) *There exists $d \in \mathbb{N}$ such that for every $n \in \mathbb{N}$ there exists an integer $n \leq m \leq n + d$ such that*

$$f(k^{m+1}) \geq k^2 \cdot f(k^m)$$

Then multiplication is definable in the structure $\langle \mathbb{N}; +, V_k, f\rangle$.

Remark. Without loss of generality the hypothesis of the previous theorem can be weakened by assuming that f satisfies properties (1) and (2) for every *n greater than some N*. Indeed in this case the function $f' : P_k \to P_k$ defined (for every $n \in \mathbb{N}$) by $f'(k^n) = f(k^{n+N})$ satisfies (1) and (2) for every $n \geq 0$; furthermore f' is definable in $\langle \mathbb{N}; +, V_k, f\rangle$ by the formula

$$[y = f'(x)] \iff y = f(\mathrm{MULT}_{k^N}(x)).$$

We shall follow the structure of Villemaire's proof of theorem 2.6 with some modifications. That is, we give here an uniform definition for the function f (see definition 4.6 below) required for the use in theorem 4.2, instead of giving a case-by-case definition as in Villemaire's paper.

For x and y coprime integers, we shall denote by $\mathcal{O}(x, y)$ the multiplicative order of x modulo y.

Lemma 4.3. *Let p be a prime number, x an integer prime to p, and α an integer greater than or equal to 2. If*

$$\mathcal{O}(x, p^{\alpha}) = \lambda \text{ and } \mathcal{O}(x, p^{\alpha+1}) \neq \lambda$$

then for every $i \in \mathbb{N}$,

$$\mathcal{O}(x, p^{\alpha+i}) = \lambda p^i \text{ and } \mathcal{O}(x, p^{\alpha+i+1}) \neq \lambda p^i.$$

Proof. By induction on i.

- The case $i = 0$ is immediate.
- Now if we assume that $\mathcal{O}(x, p^{\alpha+i}) = \lambda p^i$ and $\mathcal{O}(x, p^{\alpha+i+1}) \neq \lambda p^i$, then there exists $y \in \mathbb{N}$ such that

$$x^{\lambda p^i} = 1 + p^{\alpha+i} y \qquad \text{with} \quad \gcd(y, p) = 1$$

Thus

$$\begin{aligned} x^{\lambda p^{i+1}} &= (1 + p^{\alpha+i} y)^p \\ &= 1 + \sum_{\beta=1}^{p} \binom{p}{\beta} p^{(\alpha+i)\beta} y^{\beta} \\ &= 1 + p^{\alpha+i+1} y + \sum_{\beta=2}^{p} \binom{p}{\beta} p^{(\alpha+i)\beta} y^{\beta}. \end{aligned}$$

For every $\beta \geq 2$, one has $(\alpha + i)\beta > \alpha + i + 1$, thus $p^{\alpha+i+2}$ divides $\binom{p}{\beta} p^{(\alpha+i)\beta} y^{\beta}$, from which we deduce

$$x^{\lambda p^{i+1}} \equiv 1 \pmod{p^{\alpha+i+1}}$$

and

$$x^{\lambda p^{i+1}} \not\equiv 1 \pmod{p^{\alpha+i+2}}.$$

Therefore $\mathcal{O}(x, p^{\alpha+i+2}) \neq \lambda p^{i+1}$, and $\mathcal{O}(x, p^{\alpha+i+1}) \mid \lambda p^{i+1}$. By induction hypothesis we have $\lambda p^i \mid \mathcal{O}(x, p^{\alpha+i+1})$, and $\lambda p^i \neq \mathcal{O}(x, p^{\alpha+i+1})$. Since p is prime, it follows that

$$\mathcal{O}(x, p^{\alpha+i+1}) = \lambda p^{i+1}.$$

□

Proof of Theorem 4.1. Let k and l be two integers multiplicatively independent. We shall introduce a function f, definable in $\langle \mathbb{N}; +, V_k, P_l \rangle$, which satisfies properties (1) and (2) of Theorem 4.2 for every integer n greater than some N.

Assume

$$k = \prod_{i=1}^{r} p_i^{\alpha_i},$$

where the p_i's are distinct primes and $\alpha_i > 0$ $(i = 1, \ldots, r)$. We write l as

$$l = (\prod_{i=1}^{r} p_i^{\beta_i}) \cdot l',$$

where l' is prime to k (possibly $l' = 1$) and $\beta_i \geq 0$ $(i = 1, \ldots, r)$. In case $l' \neq 1$, let $\lambda_1, \ldots, \lambda_r$ and $\delta_1, \ldots, \delta_r$ be the integers such that for $i = 1, \ldots, r$ $\lambda_i = \mathcal{O}(l', p_i)$,

$$l'^{\lambda_i} \equiv 1 \pmod{p_i^{\delta_i}} \quad \text{and} \quad l'^{\lambda_i} \not\equiv 1 \pmod{p_i^{\delta_i+1}}.$$

We assume that k satisfies the two following hypothesis:

(i) For every $i \leq r$, if $\beta_i \neq 0$ then $\dfrac{\alpha_i}{\beta_i}$ is an integer.

(ii) For every $i \leq r$ we have $\alpha_i \geq \delta_i + 1$.

These hypothesis can be made without loss of generality: indeed it is easily seen that there exists a power of k, say k', which satisfies (i) and (ii), and one deduces easily from lemma 2.7 that the structures $\langle \mathbb{N}; +, V_k, P_l \rangle$ and $\langle \mathbb{N}; +, V_{k'}, P_l \rangle$ are inter-definable.

Lemma 4.4. *Assume $l' \neq 1$; let $\tau_1, \ldots, \tau_r$ be the integers defined by $\tau_i = \mathcal{O}(l', p_i^{\alpha_i})$ $(i = 1, \ldots, r)$. For every $j \in \mathbb{N}$ we have*

$$\mathcal{O}(l', p_i^{\alpha_i + j}) = p_i^j \cdot \tau_i.$$

Proof. Immediate from hypothesis (ii) and lemma 4.3. □

Definition 4.5. Let $(i_n)_{n \in \mathbb{N}}$ and $(j_n)_{n \in \mathbb{N}}$ be two sequences of integers defined in the following way: $i_0 = 0$, $j_0 = 0$, and for every $n \geq 1$:
- i_n is the least integer a such that there exists an integer $b \geq 1$ for which

$$l^a \equiv l^{a+b} \pmod{k^n}$$

- j_n is the least integer $b \geq 1$ such that

$$l^{i_n} \equiv l^{i_n + b} \pmod{k^n}.$$

Let us remark that (i_n, j_n) is the smallest (a, b) in lexicographical order such that

$$l^a \equiv l^{a+b} \pmod{k^n}.$$

Definition 4.6. Let $f : P_k \to P_k$ be the function defined for every $n \in \mathbb{N}$ by:

$$f(k^n) = \max\{k^m \mid m \in \mathbb{N} \text{ and } k^m \leq l^{i_n + j_n}\}.$$

Lemma 4.7. *The function f is definable in $\langle \mathbb{N}; +, V_k, P_l \rangle$.*

Proof. Let

$$A = \{(x, y, z) \mid x, y, z \in \mathbb{N} \text{ , } z \text{ is a power of } k \text{ and } x \equiv y \pmod{z}\}.$$

A is definable in $\langle \mathbb{N}; +, V_k, P_l \rangle$ by the formula

$$A(x, y, z) \iff \exists u' [V_k(z) = z \ \wedge \ V_k(u') \geq z \ \wedge \ (x + u' = y \ \vee \ y + u' = x)]$$

Now let $B = \{(x, y) \mid x, y \in \mathbb{N}$, and there exists $n \in \mathbb{N}$ such that $x = k^n$ and $y = l^{\,i_n + j_n}\}$. Using the remark after definition 4.5, and the fact that lexicographical order is well known to be definable in $\langle \mathbb{N};+\rangle$ one defines easily B in $\langle \mathbb{N};+,V_k,P_l\rangle$ Now we can define f in $\langle \mathbb{N};+,V_k,P_l\rangle$ by the formula

$$[y=f(x)] \Longleftrightarrow \{V_k(y)=y \wedge \exists z\ [B(x,z)\wedge y\leq z \wedge \mathrm{MULT}_k(y)>z]\}.$$

□

We now intend to prove that f satisfies properties (1) and (2) of theorem 4.2 for every n greater than some N'.

To illustrate our definition of f, let us first consider the simple case $k=4$, $l=5$. The hypothesis (i) and (ii) are clearly satisfied. Since 4 and 5 are coprime integers, for every $n\in\mathbb{N}$ there exists a positive integer b such that

$$5^b \equiv 1 \equiv 5^0 \pmod{4^n}.$$

From this we deduce that $i_n=0$. Now j_n is the least positive integer b such that

$$5^b\equiv 1 \pmod{4^n};$$

thus j_n is nothing but the multiplicative order of 5 modulo 4^n. We have $\mathcal{O}(5,4)=1$; from lemma 4.4 we deduce that for every positive integer n we have

$$j_n=\mathcal{O}(5,4^n)=4^{n-1}.$$

Therefore for every $n\geq 1$, $f(4^n)$ is the greatest power of 4 less than or equal to $5^{i_n+j_n}$, that is, to $5^{4^{n-1}}$. Now for every $n\geq 1$ we have

$$5^{4^n}\geq 5^{2+4^{n-1}}\geq 5^2\cdot 5^{4^{n-1}}\geq 4^2\cdot 5^{4^{n-1}}$$

which implies

$$f(4^{n+1})\geq 4^2\cdot f(4^n).$$

It follows that for every $n\geq 1$, f satisfies properties (1) and (2) of theorem 4.2, property (2) being satisfied for $d=0$.

Let us now turn to the general case.

Lemma 4.8. *There exists $N'\in\mathbb{N}$ such that f satisfies properties (1) and (2) of theorem 4.2 for every integer $n>N'$.*

Proof. We shall distinguish several cases depending on the supports of k and l (as in Villemaire's proof of theorem 2.6).

- *First case :* $\mathrm{Supp}(k)\cap\mathrm{Supp}(l)=\emptyset$ (*i.e.* $l=l'$).

In this case for every integer $n\geq 1$ there exists an integer $b\geq 1$ such that

$$l^b\equiv 1\equiv l^0 \pmod{k^n}$$

From this we deduce $i_n=0$.

Furthermore j_n is the least integer $b\geq 1$ such that

$$l^b\equiv 1 \pmod{k^n}$$

This congruence is equivalent to

$$l^b\equiv 1 \pmod{p_i^{\alpha_i n}} \qquad i=1,2,\ldots,r$$

Therefore by lemma 4.4 we have

$$j_n = \mathrm{lcm}(\mathcal{O}(l, p_1^{\alpha_1 n}), \ldots, \mathcal{O}(l, p_r^{\alpha_r n})) = \mathrm{lcm}(\tau_1 p_1^{\alpha_1(n-1)}, \ldots, \tau_r p_r^{\alpha_r(n-1)}).$$

For $i = 1, \ldots, r$ let

$$\tau_i = \prod_{j=1}^{r} p_j^{\gamma_j} \cdot \sigma_j \quad (\text{with } \gamma_j \in \mathbb{N}, \text{ and } \sigma_j \text{ prime to } p_1, p_2, \ldots, p_r)$$

and let

$$\kappa_i = \max\{\gamma_j \mid 1 \le j \le r \ \wedge \ j \ne i\}.$$

Moreover let $x' = \mathrm{lcm}(\sigma_1, \ldots, \sigma_r)$. We have

$$j_n = x' \cdot \Big(\prod_{i=1}^{r} p_i^{\max(\gamma_i + \alpha_i(n-1), \kappa_i)}\Big)$$

Let $N \in \mathbb{N}$ be such that $N \ge \max\{\frac{\kappa_i - \gamma_i}{\alpha_i} \mid i = 1, \ldots, r\} + 1$. For every $n \ge N$ we have

$$j_n = x' \cdot \Big(\prod_{i=1}^{r} p_i^{\alpha_i(n-1)+\gamma_i}\Big) = x' \cdot \prod_{i=1}^{r} p_i^{\gamma_i} \cdot k^{n-1},$$

that is

$$j_n = k \cdot j_{n-1}.$$

Let N' be an integer greater than N and such that $l^{(k-1)j_{N'}} \ge k^2$. Let us show that for every $n \ge N'$ we have $f(k^{n+1}) \ge k^2 \cdot f(k^n)$. If $n \ge N'$ then

$$l^{j_{n+1}} = l^{kj_n} = l^{(k-1)j_n} l^{j_n} \ge l^{(k-1)j_{N'}} l^{j_n} \ge k^2 l^{j_n}.$$

For every $m \in \mathbb{N}$ we have $i_m = 0$; this implies

$$\forall n \ge N' \quad l^{i_{n+1}+j_{n+1}} \ge k^2 \cdot l^{i_n + j_n}$$

From the very definition of f we get

$$\forall n \ge N' \quad f(k^{n+1}) \ge k^2 \cdot f(k^n)$$

Thus in this case f satisfies properties (1) and (2) of theorem 4.2 for every n greater than N' (property (2) being satisfied for $d = 0$).

- *Second case :* $\mathrm{Supp}(k) \subseteq \mathrm{Supp}(l)$.
  In this case we have

$$l = \Big(\prod_{i=1}^{r} p_i^{\beta_i}\Big) \cdot l' \ \text{ with } \ \beta_i > 0 \ \ (i = 1, \ldots, r)$$

For all $n, a, b \in \mathbb{N}$, $b \ge 1$, the congruence

$$l^a \equiv l^{a+b} \pmod{k^n}$$

is equivalent to

$$l^a \cdot (l^b - 1) \equiv 0 \pmod{k^n} \tag{1}$$

By our hypothesis for every $i \le r$, p_i divides l, thus $l^b - 1$ is prime to k, and (1) is equivalent to

$$l^a \equiv 0 \pmod{k^n} \tag{2}$$

This yields $j_n = 1$. On the other hand (2) is equivalent to

$$p_i^{a\beta_i} \equiv 0 \pmod{p_i^{n\alpha_i}} \qquad i = 1, \ldots, r$$

It follows that i_n is the least integer a such that

$$a \geq n \cdot \frac{\alpha_i}{\beta_i} \qquad i = 1, \ldots, r$$

Let $\mu = \max\{\frac{\alpha_i}{\beta_i} \mid i = 1, \ldots, r\}$. By initial hypothesis (i), μ is an integer. Therefore

$$\forall n \geq 0 \quad i_n = \mu n$$

From the definition for every $i \leq r$, $\mu\beta_i \geq \alpha_i$, thus

$$l^\mu = \prod_{i=1}^{r} p_i^{\mu\beta_i} \geq k$$

Furthermore k and l are multiplicatively independent, hence the equality $l^\mu = k$ is impossible. Thus $l^\mu > k$. Therefore for every $n \in \mathbb{N}$

$$l^{i_{n+1}+j_{n+1}} = l^{\mu(n+1)+1} = l^\mu \cdot l^{\mu n+1} \geq k \cdot l^{i_n+j_n}$$

From the definition of f, for every $n \in \mathbb{N}$

$$f(k^{n+1}) \geq k \cdot f(k^n)$$

which ensures us that f satisfies property (1) of Theorem 4.2. There remains to prove that property (2) is satisfied too. We have $l^\mu > k$, thus there exists a real $\epsilon > 0$ such that $l^\mu = k^{1+\epsilon}$. Let ν be the real such that $l = k^\nu$. For every $n \in \mathbb{N}$ we have

$$l^{i_n+j_n} = l^{\mu n+1} = k^{(1+\epsilon)n+\nu}.$$

From the previous inequality we deduce that for every $n \in \mathbb{N}$

$$f(k^n) = k^{\lfloor (1+\epsilon)n+\nu \rfloor}$$

Let d be an integer greater than $\frac{1}{\epsilon}$. For every $n \in \mathbb{N}$ we have

$$f(k^{n+d}) = k^{\lfloor (1+\epsilon)(n+d)+\nu \rfloor} = k^{\lfloor (1+\epsilon)n+d+d\epsilon+\nu \rfloor} \geq k^{\lfloor (1+\epsilon)n+\nu \rfloor+d+\lfloor d\epsilon \rfloor} \geq k^{d+1} \cdot f(k^n)$$

Thus for every $n \in \mathbb{N}$ there must exist an integer m between n and $n+d$, such that

$$f(k^{m+1}) \geq k^2 \cdot f(k^m)$$

f thus satisfies the two required properties of theorem 4.2.

- *Third case :* $\mathrm{Supp}(k) \cap \mathrm{Supp}(l) \neq \emptyset$ *and* $\mathrm{Supp}(k) \not\subseteq \mathrm{Supp}(l)$.
  Assume that $\mathrm{Supp}(k) \cap \mathrm{Supp}(l) = \{p_1, p_2, \ldots, p_s\}$ where $s < r$. We have

$$l = \Big(\prod_{i=1}^{s} p_i^{\beta_i}\Big) \cdot l' \quad \text{with} \quad \beta_i > 0 \quad (i = 1, \ldots, s)$$

Set $k^* = \prod_{j=s+1}^{r} p_i^{\alpha_i}$.

For all $n, a, b \in \mathbb{N}$, $b \geq 1$, the congruence

$$l^a \equiv l^{a+b} \pmod{k^n}$$

is equivalent to

$$\begin{cases} p_i^{a\beta_i} \equiv 0 \pmod{p_i^{n\alpha_i}} & i = 1, \dots, s \\ l^b \equiv 1 \pmod{p_j^{n\alpha_j}} & j = s+1, \dots, r \end{cases}$$

This case mixes the two preceding cases and a similar study yields, on one hand, the existence of an integer μ' such that for every $n \in \mathbb{N}$

$$i_n = \mu' n,$$

on the other hand the existence of two positive integers x'', N'' such that for every $n \geq N''$

$$j_n = {k^*}^{n-1} \cdot x''.$$

Let N be an integer greater than N'' and such that $l^{(k^*-1)j_N} \geq k^2$. For every $n \geq N$ one gets

$$l^{i_{n+1}+j_{n+1}} = l^{\mu'(n+1)} \cdot l^{j_{n+1}} \geq l^{i_n} \cdot l^{k^* j_n} \geq l^{i_n} \cdot l^{(k^*-1)j_n} l^{j_n} \geq k^2 \cdot l^{i_n+j_n}$$

This ensures us that for every $n \geq N$

$$f(k^{n+1}) \geq k^2 \cdot f(k^n)$$

Therefore f satisfies properties (1) and (2) of theorem 4.2 for every n greater than N ((2) being satisfied for $d = 0$). □

This completes the proof of theorem 4.1. □

Theorems 3.1 and 4.1 immediately lead to the main result:

Theorem 4.9. *Let n be a positive integer, and let k and l be multiplicatively independent integers. If $L \subseteq \mathbb{N}^n$ is $l-$recognizable and not definable in $\langle \mathbb{N}; + \rangle$ then multiplication is definable in $\langle \mathbb{N}; +, V_k, L \rangle$. Therefore the elementary theory of this structure is undecidable.*

5. The Cobham-Semënov Theorem

In this section we are concerned with the Cobham-Semënov theorem, which emphasizes the base-dependence of the notion of $k-$recognizable set.

Theorem 5.1. (Cobham, Semënov) *Let n be a positive integer, and let k and l be two multiplicatively independent integers. For every $A \subseteq \mathbb{N}^n$, if A is $k-$ and l- recognizable then A is definable in $\langle \mathbb{N}; + \rangle$.*

The case $n = 1$ was proved by Cobham in [Cob69]; Semënov extended the result to higher dimensions in [Sem77]. Eilenberg suggested in [Eil74] to find a simpler proof of Cobham's result. This was achieved by Hansel in [Han82]. Muchnik settled in [Muc91] a criterion for definability in $\langle \mathbb{N}; + \rangle$, which led him to an alternative (and simpler) proof of Semënov's theorem. A new proof (of Semënov's result) was recently given by Michaux and Villemaire [MV96]; it rests on the strength of theorems 3.3 and 3.4 which we used in Section 3, and on a theorem due to Hansel [Han82] (this result was already present in Cobham's proof [Cob69]).

Theorem 3.3. (Michaux-Villemaire) *Let $A \subseteq \mathbb{N}$. If A is not definable in $\langle \mathbb{N}; + \rangle$ then there exists an expanding set $A' \subseteq \mathbb{N}$ which is definable in $\langle \mathbb{N}; +, A \rangle$.*

Theorem 3.4. (Michaux-Villemaire) *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 $\langle \mathbb{N}; + \rangle$.*

Theorem 5.2. (Cobham,Hansel). *Let k and l be two multiplicatively independent integers. If $A \subseteq \mathbb{N}$ is $k-$ and $l-$recognizable then A is not expanding.*

Now the argument leading the authors to the proof of theorem 5.1 is the following: assume that there exists $L \subseteq \mathbb{N}^n$ which is $k-$ and $l-$ recognizable for k, l multiplicatively independent integers, and such that L is not definable in $\langle \mathbb{N}; + \rangle$. By theorem 3.4 there is a set $L' \subseteq \mathbb{N}$ definable in $\langle \mathbb{N}; +, L \rangle$ but not in $\langle \mathbb{N}; + \rangle$. The set L is $k-$ and $l-$recognizable; therefore L', being definable in $\langle \mathbb{N}; +, L \rangle$, is $k-$ and $l-$recognizable too. Now by theorem 3.3 there exists an expanding set $L'' \subseteq \mathbb{N}$ which is definable in $\langle \mathbb{N}; +, L' \rangle$. The set L'', like L', is $k-$ and $l-$recognizable, which contradicts theorem 5.2.

From the results of the previous sections we now propose two simple proofs of Cobham-Semënov theorem; the first one only involves theorem 3.1 and was suggested by C.Michaux, the second one uses theorem 4.9. One should note that our proofs rest in an essential way on theorems 3.3 and 3.4.

First proof of theorem 5.1. Assume that there exists $L \subseteq \mathbb{N}^n$ which is $k-$ and $l-$ recognizable for k, l multiplicatively independent, and not definable in $\langle \mathbb{N}; + \rangle$. By theorem 3.1 the set P_k is definable in $\langle \mathbb{N}; +, L \rangle$; now L is $l-$recognizable, thus every relation definable in $\langle \mathbb{N}; +, L \rangle$ is $l-$recognizable too; in this case P_k should be $l-$recognizable, which contradicts a result of Büchi [Buc60]. $\square$

Second proof of theorem 5.1. If there was some $L \subseteq \mathbb{N}^n$ not definable in $\langle \mathbb{N}; + \rangle$ and $k-$ and $l-$recognizable for k, l multiplicatively independent, then by theorem 4.9 the elementary theory of $\langle \mathbb{N}; +, V_k, L \rangle$ would be undecidable. But L is $k-$recognizable, thus definable in $\langle \mathbb{N}; +, V_k \rangle$; therefore the elementary theory of $\langle \mathbb{N}; +, V_k, L \rangle$ is just an extension by definition of the elementary theory of $\langle \mathbb{N}; +, V_k \rangle$, which is decidable; this cannot be. $\square$

Acknowledgements

I wish to thank Christian Michaux and Roger Villemaire for many helpful suggestions during the preparation of the paper.

References

[Bru85] V. Bruyère, *Entiers et automates finis*, U.E. Mons, mémoire de licence, 1984-85.

[Buc60] J.R.Büchi, *Weak second-order arithmetic and finite automata*, **Zeitschrift für Math. Logic Grundlagen Math. 6**, 1960, pp. 66-92.

[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, pp. 17-34.

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

[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 extensions of second (first) order theory of (generalized) successor*, **Journal of Symbolic Logic** vol.31 (2), 1966, pp. 169-181

[Han82] G.HANSEL, *A propos d'un théorème de Cobham*, in: D.Perrin, ed., Actes de la Fête des Mots, Greco de Programmation, CNRS, Rouen, France, 1992.

[Hod83] B. HODGSON, *Décidabilité par automate fini*, **Ann. Sci. Math. Québec 7**, 1983, pp. 39-57

[MV93] C.MICHAUX, R.VILLEMAIRE, *Open questions around Büchi and Presburger arithmetics*, to appear in Proceedings of Logic Colloquium'93, Oxford Univ. Press, 28pp.

[MV96] 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, pp. 251-277.

[Muc91] A.MUCHNIK, *Definable criterion for definability in Presburger Arithmetic and its application* (in russian), preprint, Institute of new technologies, 1991

[Sem77] A.L.SEMENOV, *The Presburger nature of predicates that are regular in two number systems*, **Siberian Math. J.** 18 (2), 1977, pp. 289-299.

[Tho75] W.THOMAS, *A note on undecidable extensions of monadic second order successor arithmetic*, **Arch. Math. Logik.** 17, 1975, pp. 43-44.

[Vil92a] R.VILLEMAIRE, $\langle I\!N; +, V_k, V_l\rangle$ *is undecidable*, **Theoretical Computer Science** 106, 1992, pp. 337-349.

[Vil92b] R.VILLEMAIRE, *Joining $k-$ and $l-$recognizable sets of natural numbers*, Proceedings of the 9th Symposium on Theoretical Aspects of Computer Science (STACS'92) Paris, France, **Springer Lecture Notes in Computer Science** , vol.577, 1992, pp. 83-94.

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