Theoretical Computer Science 106 (1992) 337–349
Elsevier



# Note

# The theory of $\langle \mathbb{N}, +, V_k, V_l \rangle$ is undecidable

Roger Villemaire

*Département de mathématiques et d'informatique, Université du Québec à Montréal, C.P. 8888, succ. A, Montréal (Québec), Canada H3C 3P8*

Communicated by D. Perrin
Received September 1991
Revised January 1992

*Abstract*

Villemaire, R., The theory of $\langle \mathbb{N}, +, V_k, V_l \rangle$ is undecidable, Theoretical Computer Science 106 (1992) 337–349.

We first give a simple encoding for $k$-automata in $\langle \mathbb{N}, +, V_k \rangle$, where $V_k$ is the function from $\mathbb{N}\setminus\{0\}$ to $\mathbb{N}$ mapping $x$ to the largest power of $k$ which divides $x$. This, with a result of Hodgson, gives a proof of Büchi's theorem, which states that a subset of $\mathbb{N}^n$ is $k$-recognizable by automata if and only if it is definable in $\langle \mathbb{N}, +, V_k \rangle$. Our proof also shows that every formula of $\langle \mathbb{N}, +, V_k \rangle$ is equivalent to a $\exists\forall\exists$-formula. Furthermore, solving a problem of A. Joyal, we show that the first-order theory of $\langle \mathbb{N}, +, V_k, V_l \rangle$ is undecidable for $k, l$ multiplicatively independent.

## 1. Introduction

Büchi's theorem states that a set of natural numbers is $k$-recognizable by automata if and only if it is definable in the first-order structure $\langle \mathbb{N}, +, V_k \rangle$, where $V_k$ is the function from $\mathbb{N}\setminus\{0\}$ to $\mathbb{N}$ mapping $x$ to $V_k(x)$, the largest power of $k$ which divides $x$. Büchi stated this result in [2, Theorem 9] with $P_k$ in place of $V_k$, where $P_k(x)$ is a unary predicate satisfied by $x$ if and only if $x$ is a power of $k$. McNaughton in his review [8] noted that the proof of Büchi did not work for $\langle \mathbb{N}, +, P_k \rangle$ and conjectured that the statement was false. This last claim was proved by Semenov in [11, Corollary 4].

Correspondence to: R. Villemaire, Département de mathématiques et d'informatique, Université du Québec à Montréal, C.P. 8888, succ. A, Montréal (Québec), Canada H3C 3P8

Bruyère in [1] showed that Büchi's proof can be modified slightly to yield that being $k$-recognizable is equivalent to being definable in $\langle \mathbb{N}, +, V_k \rangle$ (see also [9] for a different proof). The proof of Büchi introduces, in an intermediary step, a monadic second-order structure. Michaux and Point showed in [9], using a result of Hodgson, that one can prove the result in a direct way, avoiding any new structure. Their proof is by induction on regular operations. I show in this paper that their induction can be replaced by a simple encoding of automata in $\langle \mathbb{N}, +, V_k \rangle$. My proof also shows that every formula of $\langle \mathbb{N}, +, V_k \rangle$ is equivalent to a $\exists\forall\exists$-formula.

Natural numbers $k, l$ are said to be *multiplicatively dependent* if there exist $n, m$ in $\mathbb{N}$ such that $k^n = l^m$. It is well known that if $k$ and $l$ are multiplicatively dependent then any set which is $k$-recognizable is also $l$-recognizable (see [4, Corollary 3.7]). Furthermore, Cobham proved in [3] (see also [6, 10]) that, for $k, l$ multiplicatively independent, a set which is $k$- and $l$-recognizable is 1-recognizable; hence, a union of a finite set with finitely many arithmetic progressions. Since any 1-recognizable set is $k$-recognizable for any $k$ (see [4, Proposition 3.4]), this means that this intersection is the smallest possible.

By Büchi's theorem we know that the class of $k$-recognizable sets is closed under intersection, complementation and projection. A. Joyal asked if, for $k$ and $l$ multiplicatively independent, there is some sort of machine which recognizes exactly the sets which are in the smallest class containing all $k$-recognizable, all $l$-recognizable and closed under intersection, complementation, and projection. This is equivalent to asking for a type of machine which recognizes exactly the sets definable in $\langle \mathbb{N}, +, V_k, V_l \rangle$. I show in this paper that this is not possible. Actually, multiplication is definable in $\langle \mathbb{N}, +, V_k, V_l \rangle$; hence, any set of the arithmetical hierarchy is definable in $\langle \mathbb{N}, +, V_k, V_l \rangle$.

This shows in particular that $\langle \mathbb{N}, +, V_2, V_3 \rangle$ is undecidable, answering a question of Bruyère ([1, p. IV 18]) (see also [14]).

## 2. Finite automata

Let us first recall some definitions and facts about automata.

Let $\Sigma$ be an *alphabet*, i.e. a finite set. $\Sigma^*$ will denote the set of *words* of finite length on $\Sigma$ containing the *empty* word $\lambda$ formed of no symbol. Any subset $L$ of $\Sigma^*$ will be called a *language* on the alphabet $\Sigma$.

**Definition.** Let $\Sigma$ be an alphabet. A $\Sigma$-automaton $\mathscr{A}$ is a quadruplet $(Q, q_0, \Gamma, T)$, where $Q$ is a finite set, called the set of *states* of $\mathscr{A}$, $q_0$ is an element of $Q$, called the *initial state* of $\mathscr{A}$, $\Gamma$ is a subset of $Q$, called the set of *final states*, and, finally, $T$ is a function from $Q \times \Sigma$ to $Q$, called the *transition function*.

The intended behaviour of an automaton is defined in the following way. First we can extend the transition function $T$ of a $\Sigma$-automaton to a function $T^*$ from $Q \times \Sigma^*$

to $Q$ in the following way:

$$T^*(q, \sigma) = T(q, \sigma) \quad \text{for } \sigma \in \Sigma,$$

$$T^*(q, \alpha\sigma) = T(T^*(q, \alpha), \sigma) \quad \text{for } \alpha \in \Sigma^* \text{ and } \sigma \in \Sigma.$$

Furthermore, we have the following definitions.

**Definition.** A word $\alpha \in \Sigma^*$ is said to be *accepted* by the $\Sigma$-automaton $(Q, q_0, \Gamma, T)$ if $T^*(q_0, \alpha) \in \Gamma$.

**Definition.** A language $L$ on $\Sigma$ is said to be *$\Sigma$-recognizable* if there exists a $\Sigma$-automaton such that the set of words accepted by this automaton is exactly $L$.

Let $\Sigma$ be an alphabet containing the symbol 0. Let $\alpha = \sigma_1 \ldots \sigma_m$ and $\beta = \rho_1 \ldots \rho_n$ be words on $\Sigma$, where $\sigma_1, \ldots, \sigma_m, \rho_1, \ldots, \rho_n$ are in $\Sigma$. The *convolution* $\alpha * \beta$ is the word $(\sigma_1, \rho_1) \ldots (\sigma_n, \rho_n)$ on $\Sigma^2$. If $n \neq m$, we cannot make the convolution of $\alpha$ and $\beta$ in this first sense but it is possible to generalize the definition in the following way. Add 0 to the right of the shortest (in number of letters) of $\alpha$, $\beta$, often enough to make the two words of the same length. Then take the convolution of these two words and denote it by $\alpha * \beta$.

In general, let $\Sigma$ be an alphabet and let $n$ be a natural number. We associate with an $n$-tuple $(\alpha_1, \ldots, \alpha_n)$ of words on $\Sigma$ its *convolution* in the following way. Take $m$ to be the maximal length of the words $\alpha_1, \ldots, \alpha_n$. Add to the right of each $\alpha_i$ the necessary number of symbols 0 to get words of length $m$ and call these new words $\alpha_i^0$, $i = 1, \ldots, n$. Finally, take the word on $\Sigma^n$ having as $i$th letter the tuple formed by the $i$th letters of $\alpha^0, \ldots, \alpha_n^0$. This is the convolution $\alpha_1 * \cdots * \alpha_n$.

**Remark.** This is the approach adopted in [9]. For the case of a general first-order language see [7], where 0 is replaced by some symbol $\sharp$ not in $\Sigma$.

**Definition.** Let $\Sigma$ be an alphabet containing the symbol 0. We say that a subset $X$ of the cartesian product $(\Sigma^*)^n$ is *$\Sigma$-recognizable* if the set $\{\alpha_1 * \cdots * \alpha_n; (\alpha_1, \ldots, \alpha_n) \in X\}$ is $\Sigma^n$-recognizable.

Let us now introduce some operation on languages which preserve the property of being recognizable.

Let $L_1$ and $L_2$ be two languages. We denote by $L_1 \cap L_2$ the set-theoretic intersection of $L_1$, $L_2$ and by $L_1^c$ the set-theoretic complement of $L_1$. For $X$, a subset of the cartesian product $\Sigma^n$, we denote by $\wp_i X$ $(i = 1, \ldots, n)$ the $i$th projection, i.e. the set

$$\{(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n); \text{ there exists an } \alpha \text{ in } \Sigma^* \text{ such that}$$

$$(x_1, \ldots, x_{i-1}, \alpha, x_{i+1}, \ldots, x_n) \text{ is in } X\}.$$

We can now state a very important classical result.

**Theorem 2.1.** *Let $\Sigma$ be an alphabet and $L_1, L_2$ $\Sigma$-recognizable languages. Then $L_1 \cap L_2$ and $L_1^c$ are $\Sigma$-recognizable. Furthermore, if $L \subseteq (\Sigma^*)^n$ is $\Sigma$-recognizable then $\wp_i L$ is $\Sigma$-recognizable for all $i = 1, \ldots, n$.*

**Proof.** See [4, Proposition 2.2] to show that $L_1 \cap L_2$ and $L_1^c$ are $\Sigma$-recognizable.

For the last case see [7, step (iii) in the proof of Théorème 3.5] or [4, Proposition 3.3]. □

The elements of $\mathbb{N}$ can be represented as words on $\{0, 1, \ldots, k-1\}$ for $k > 1$ a natural number, as their inverse representation in basis $k$. An element of $\mathbb{N}^n$ is represented in base $k$ by the convolution of its components, which is a word on $\{0, 1, \ldots, k-1\}^n$.

**Definition.** We say that a subset $X$ of $\mathbb{N}^n$ is *$k$-recognizable* if the set of its representations in base $k$ is $\{0, 1, \ldots, k-1\}$-recognizable.

**Notation.** Let $k$ be an integer. We denote by $V_k(x)$ the function from $\mathbb{N} \setminus \{0\}$ to $\mathbb{N}$, which maps $x$ to the largest power of $k$ which divides $x$.

**Theorem 2.2.** (Büchi's theorem). *A subset of $\mathbb{N}^n$ is $k$-recognizable if and only if it is definable in $\langle \mathbb{N}, +, V_k \rangle$.*

**Proof.** That any subset of $\mathbb{N}^n$ definable in $\langle \mathbb{N}, +, V_k \rangle$ is $k$-recognizable follows from the proof of Théorème 3.5 of [7], since it is easy to show that $\{(x, y, z) \in \mathbb{N}^3;\ x + y = z\}$ and $\{(x, y) \in \mathbb{N}^2;\ V_k(x) = y\}$ are $k$-recognizable.

To show the converse, we need some lemmas in order to encode any automaton in $\langle \mathbb{N}, +, V_k \rangle$.

**Lemma 2.3.** *The following relation and functions are definable in $\langle \mathbb{N}, +, V_k \rangle$:*

(i) *For $j = 0, 1, \ldots, k-1$, "$x$ is a power of $k$ and the coefficient of this power of $k$ in the representation of $y$ in basis $k$ is $j$". We denote this relation by $X_{k,j}(x, y)$.*

(ii) *"The smallest power of $k$ strictly larger than $x$". We denote this function by $G(x)$.*

(iii) *"The power of $k$ which precedes $G(x)$". We denote this function by $G^-(x)$ ($G^-(0)$ being undefined).*

**Proof.** $X_{k,j}(x, y)$ is defined by the formula

$$V_k(x) = x \wedge (\exists z, t[z < x \wedge V_k(t) > x \wedge y = z + jx + t] \vee \exists z[z < x \wedge y = z + jx]).$$

Here $x > y$ stands for $\exists z[z \neq 0 \wedge y + z = x]$ and $jy$ represents $y + \cdots + y$ ($j$ times), which is a term in the language.

Furthermore, $G(x) = y$ is defined by the formula

$$V_k(y) = y \wedge y > x \wedge \forall z[V_k(z) = z \wedge z > x \Rightarrow y \leqslant z].$$

Finally, $G^-(x) = y$ can be defined as $ky = G(x)$. □

**Remark.** If $x = x_0 + x_1 k + \cdots + x_n k^n$, where $x_i \in \{0, 1, \ldots, k-1\}$ and $x_n \neq 0$ then $G(x) = k^{n+1}$ and $G^-(x) = k^n$.

**Proof of Theorem 2.2** (*conclusion*). Let $X \subseteq \mathbb{N}^n$ be $k$-recognizable by the automaton $\mathscr{A} = (Q, q_0, \Gamma, T)$. Let $Q = \{q_0, q_1, \ldots, q_t\}$ and take $k^s$ to be the smallest power of $k$ larger than $t$. Without loss of generality, we can replace $\{q_0, q_1, \ldots, q_t\}$ by $\{\sigma_0, \sigma_1, \ldots, \sigma_t\}$, a subset of $\{0, 1, \ldots, k-1\}^s$. We write $\sigma_j(i)$ for the $i$th component of $\sigma_j$, i.e. $\sigma_j = (\sigma_j(0), \ldots, \sigma_j(s))$. For $y \in \mathbb{N}$, let $y(i)$ be the $i$th digit of $y$ starting from the left, in the inverse representation of $y$ in base $k$, i.e. $y = y(0) + y(1)k + \cdots + y(r)k^r$, where $G^-(y) = k^r$.

Now $\bar{x} \in X$ if and only if there exist $y_1, \ldots, y_s$ coding the states by which $\mathscr{A}$ goes (starting by $\sigma_0$ and finishing by some states of $\Gamma$) when reading $\bar{x}$.

Hence, $\bar{x} = (x_1, \ldots, x_n) \in X$ if and only if there exist $y_1, \ldots, y_s$ in $\mathbb{N}$ such that $(y_1(0), \ldots, y_s(0)) = \sigma_0$; furthermore, if $(y_1(i), \ldots, y_s(i)) = \sigma_j$ and $T(\sigma_j, (x_1(i), \ldots, x_n(i))) = \sigma_{j'}$ then $(y_1(i+1), \ldots, y_s(i+1)) = \sigma_{j'}$.

Hence, $\bar{x} \in X$ if and only if the following formula is satisfied in $\langle \mathbb{N}, +, V_k \rangle$:

$$\exists u, y_1, \ldots, y_s \, V_k(u) = u \wedge \bigwedge_{r=1}^{s} X_{k, \sigma_0(r)}(1, y_r) \wedge \bigvee_{f \in \Gamma} \left( \bigwedge_{r=0}^{s} X_{k, f(r)}(u, y_r) \right)$$

$$\wedge \bigwedge_{(\sigma, (\rho_1, \ldots, \rho_n), \sigma') \in S} \forall z \left[ V_k(z) = z \wedge z < u \wedge \bigwedge_{r=0}^{s} X_{k, \sigma(r)}(z, y_r) \right.$$

$$\left. \wedge \bigwedge_{i=1}^{n} X_{k, \rho_i}(z, x_i) \rightarrow \bigwedge_{r=0}^{s} X_{k, \sigma'(r)}(kz, y_r) \right],$$

where $S = \{(\sigma, (\rho_1, \ldots, \rho_n), \sigma'); \, T(\sigma, (\rho_1, \ldots, \rho_n)) = \sigma'\}$. □

**Corollary 2.4.** *Every formula of* $\langle \mathbb{N}, +, V_k \rangle$ *is equivalent to a* $\exists\forall\exists$*-formula.*

**Proof.** In the proof of Lemma 2.3 we showed that $X_{k,j}$ are definable by $\exists\forall$-formulas and $\forall\exists$-formulas. Hence, the formula in the proof of Theorem 2.2 is $\exists\forall\exists$. Therefore, since any formula of $\langle \mathbb{N}, +, V_k \rangle$ defines a $k$-recognizable set, it is equivalent to a formula of this form, i.e. a $\exists\forall\exists$-formula.

## 3. Definability in $\langle \mathbb{N}, +, V_k, V_l \rangle$

**Notation.** Let $k \in \mathbb{N}$, we write $k^{\mathbb{N}}$ for the set of powers of $k$. It is easy to show that this set is definable in $\langle \mathbb{N}, +, V_k \rangle$.

Let $K_1 \cup \cdots \cup K_n$ be a disjoint partition of $k^{\mathbb{N}}$ and let $h : k^{\mathbb{N}} \rightarrow k^{\mathbb{N}}$ be a strictly increasing function having the following property:

(*) For all $i=1,\ldots,n$ and all $x, y$ in $K_i$, if $x<y$, then there exists $z\in(\mathrm{Im}\,h)^c$ (the complement of $\mathrm{Im}\,h$ in $k^{\mathbb{N}}$) such that $h(x)<z<h(y)$.

**Remark.** Note that (*) implies that the restriction of $h$ to $K_i$ is a "skipping" function, i.e. it skips at least one element of $k^{\mathbb{N}}$ between any consecutive arguments.

In order to show that $\langle \mathbb{N}, +, V_k, V_l\rangle$ is undecidable, we first define multiplication in $\langle \mathbb{N}, +, V_k, h, K_i;\ i=1,\ldots,n\rangle$ and then show that there exist such $h$ and $K_i$ $(i=1,\ldots,n)$ definable in $\langle \mathbb{N}, +, V_k, V_l\rangle$ for $k, l$ multiplicatively independent.

Niwiński pointed out to me that the method of proof I use is essentially the same as the one Elgot and Rabin used in [5]. Actually, it is possible to generalize slightly a result of Thomas [12, Theorem 2] in order to show that multiplication is definable in $\langle \mathbb{N}, +, V_k, h, K_i; i=1,\ldots,n\rangle$ (see [15]).

**Notation.** For $y\in k^{\mathbb{N}}$ we write $S(y)$ for the smallest power of $k$ which is larger than $y$ and is in $(\mathrm{Im}\,h)^c$; this is clearly definable in $\langle \mathbb{N}, +, V_k, h, K_i; i=1,\ldots,n\rangle$.

**Lemma 3.1.** There exist functions $H_i: k^{\mathbb{N}}\times K_i\to k^{\mathbb{N}}$, $i=1,\ldots,n$, definable in $\langle \mathbb{N}, +, V_k, h, K_i; i=1,\ldots,n\rangle$ such that for a fixed $x\in k^{\mathbb{N}}$, $H_i(x, y)$ is injective as a function of $y$ and $H_i(x, y)\geqslant x$ for all $y\in K_i$.

**Proof.** Let $H_i(x, y)=h^{(t)}(S\circ h(y))$, where $h^{(t)}$ is the composition of $h$, $t$ times with itself, and $t$ is the smallest natural number such that $h^{(t)}(S\circ h(y))\geqslant x$. Since $h$ is strictly increasing, there exists such a $t$. Note that all the $H_i$ are defined in the same way; only the domains differ. This is to ensure that they are injective as functions of $y$.

Let us show that $H_i(x, y)$ is injective as a function of $y$. Suppose that $H_i(x, y)=H_i(x, y')$. By definition $H_i(x, y)=h^{(t)}(S\circ h(y))$ and $H_i(x, y')=h^{(t')}(S\circ h(y'))$ for $t, t'$ natural numbers. Suppose, without loss of generality, that $t\geqslant t'$. From $h^{(t)}(S\circ h(y))=h^{(t')}(S\circ h(y'))$, it follows by injectivity of $h$ that $h^{(t-t')}(S\circ h(y))=S\circ h(y')$. Since $S\circ h(y')\notin \mathrm{Im}\,h$, we must have that $t'=t$ and, hence, $S\circ h(y)=S\circ h(y')$. From property (*), it follows that $y=y'$.

The second condition is trivially true.

$H_i(x, y)=z$ is definable in $\langle \mathbb{N}, +, V_k, h, K_i;\ i=1,\ldots,n\rangle$ by the formula saying "there exists $u\in\mathbb{N}$ which is the smallest satisfying $X_{k,1}(S\circ h(y), u)\wedge\forall t[t< x\wedge X_{k,1}(t, u)\to X_{k,1}(h(t), u)]$ and $z$ is the largest power of $k$ for which $X_{k,1}(z, u)$". Since $S(x)$ is definable in $\langle \mathbb{N}, +, V_k, h, K_i; i=1,\ldots,n\rangle$ this is also the case for $H_i(x, y)$. □

**Notation.** We write $\mathrm{Max}\,H_i(x, y)$ for the maximum of the set $\{H_i(x, y');\ y'\leqslant y\}$. This function is obviously definable in $\langle \mathbb{N}, +, V_k, h, K_i;\ i=1,\ldots,n\rangle$.

Let $L(x, y_1, \ldots, y_n, z, t)$ be the relation on $\mathbb{N}^{n+1} \times (k^{\mathbb{N}})^2$ defined by the following formula in the theory of $\langle \mathbb{N}, +, V_k, h, K_i; i = 1, \ldots, n \rangle$:

$$\forall u \bigwedge_{i=1}^{n} \{(V_k(u) = u) \wedge u \in K_i \Rightarrow \bigwedge_{j=0}^{k-1} [X_{k,j}(u, x) \leftrightarrow X_{k,j}(H_i(z, u), y_i)]\}$$

$$\wedge V_k(z) = z \wedge V_k(t) = t \wedge \bigwedge_{i=1}^{n} (\operatorname{Max} H_i(z, G^{-}(x)) < t).$$

**Remark.** Let the representations of $y_1, \ldots, y_n$ in basis $k$ be $y_{11} \ldots y_{1m_1}, \ldots, y_{n1} \ldots y_{nm_n}$, respectively; then the following figure illustrates the definition:

$$\begin{array}{ccc} y_1 = y_{11} \cdots & \boxed{\begin{array}{c}\text{the digits of} \\ y_1, \ldots, y_n \\ \text{appearing in} \\ \text{this box} \\ \text{encode } x\end{array}} & \cdots\ y_{1m_1} \\ \vdots \quad \vdots & & \vdots \\ y_n = y_{n1} \cdots & & \cdots\ y_{nm_n} \\ \uparrow & & \uparrow \\ z & & t \end{array}$$

**Lemma 3.2.** *For every* $x, x', y_1, \ldots, y_n \in \mathbb{N}$ *and every* $z, t \in k^{\mathbb{N}}$, $L(x, y_1, \ldots, y_n, z, t)$ *and* $L(x', y_1, \ldots, y_n, z, t)$ *imply* $x = x'$.

**Proof.** Obvious from the fact that the $H_i$'s are injective (see Lemma 3.1). □

**Lemma 3.3.** *Multiplication is definable in* $\langle \mathbb{N}, +, V_k, h, K_i; i = 1, \ldots, n \rangle$.

**Proof.** We want to define $x \cdot y = z$.

Let $y = y_0 + y_1 k + \cdots + y_n k^n$; then $z = xy_0 + xy_1 k + \cdots + xy_n k^n$.

The idea is to encode multiplication in the following way: $\|0|y_0 \ldots y_n\| xy_n| y_0 \ldots y_{n-1} \| \cdots \| xy_i + xy_{i+1} k + \cdots + xy_n k^{n-i} | y_0 \ldots y_{i-1} \| xy_{i-1} + xy_i k + xy_{i+1} k^2 + \cdots + xy_n k^{n-i+1} | y_0 \ldots y_{i-2} \| \cdots \| xy_0 + \cdots + xy_n k^n | 0 \|$, where $|$ and $\|$ are markers.

The set of markers will be the appearance of the digit 1 in two natural numbers. More precisely, for $z, z' \in \mathbb{N}$ we say that $(z, z')$ forms a *marker set*, denoted by $M(z, z')$ if all $k$-digits of $z$ and $z'$ are either 0 or 1. Furthermore, we say that a power $t$ of $k$ is a *double marker* for $(z, z')$, which we denote by $DM(t, z, z')$, if $X_{k,1}(t, z) \wedge X_{k,1}(t, z')$ and if there exists a $t'$ such that $kt' = t$; then $X_{k,0}(t', z) \wedge X_{k,0}(t', z')$. Also, we say that a power $t$ of $k$ is a *single marker* for $(z, z')$, denoted by $SM(t, z, z')$, if $X_{k,1}(t, z) \wedge X_{k,0}(t, z')$ and if there exists a $t'$ such that $kt' = t$; then $X_{k,0}(t', z) \wedge X_{k,0}(t', z')$. A *marker block* is any single or double marker. Finally, for $(z, z')$, a marker set, and $t$, a marker block of $z$, we denote by $NM_1(t, z, z')$, $NM_2(t, z, z')$, $NM_3(t, z, z')$, $NM_4(t, z, z')$ the successive marker blocks following $t$. Finally, let $LDM(z, z')$ be the last double marker of $(z, z')$ and $LSM(z, z')$ the last single marker. It is easy to see that

$M$, $DM$, $SM$, $NM_1$, $NM_2$, $NM_3$, $NM_4$, $LDM$ and $LSM$ are all definable in $\langle \mathbb{N}, +, V_k, h, K_i; i=1,\ldots,n\rangle$.

We can define our encoding in the following way:

$$\begin{aligned}
&\exists z_1,\ldots,z_n, w, w' M(w,w') \wedge DM(1,w,w') \wedge L(0,z_1,\ldots,z_n,1,NM(1,w,w'))\\
&\quad \wedge L(y,z_1,\ldots,z_n,NM_1(1,w,w'),NM_2(1,w,w'))\\
&\quad \wedge \forall u,v,v' \bigwedge_{j=1}^{k-1} \{DM(u,w,w') \wedge L(v,z_1,\ldots,z_n,u,NM_1(u,w,w'))\\
&\qquad\qquad \wedge L(v',z_1,\ldots,z_n,NM_1(u,w,w'),NM_2(u,w,w'))\\
&\qquad\qquad \wedge X_{k,j}(G^-(v'),v')\\
&\qquad\qquad \rightarrow L(kv+jx,z_1,\ldots,z_n,NM_2(u,w,w'),NM_3(u,w,w'))\\
&\qquad\qquad \wedge L(v'-jG^-(v'),z_1,\ldots,z_n,NM_3(u,w,w'),NM_4(u,w,w'))\}\\
&\qquad\qquad \wedge L(z,z_1,\ldots,z_n,LDM(w,w'),LSM(w,w')),
\end{aligned}$$

where, as before, $jx$ and $kv$ are terms in the language. This completes the proof. □

**Remark.** The proof of Lemma 3.3. actually shows that any recursive function is definable in $\langle \mathbb{N}, +, V_k, h, K_i; i=1,\ldots,n\rangle$.

It follows from Lemma 3.3 that if we can define such a function $h$ and sets $K_i$ for $i=1,\ldots,n$, we will have that $\langle \mathbb{N}, +, V_k, V_l\rangle$ is undecidable and that any set of the arithmetical hierarchy is definable in it.

We now show that it is possible to define such a function $h$ and sets $K_i$, $i=1,\ldots,n$ in $\langle \mathbb{N}, +, V_k, V_l\rangle$. We often use the following fact: For $k$, $n$ in $\mathbb{N}$, $k$ and $k^n$ are multiplicatively dependent; hence, any set which is $k$-recognizable is $k^n$-recognizable, and vice versa (see [4, Corollary 3.7]). This means that $V_k$ is definable in $\langle \mathbb{N}, +, V_{k^n}\rangle$ and $V_{k^n}$ is definable in $\langle \mathbb{N}, +, V_k\rangle$; therefore, we can consider $\langle \mathbb{N}, +, V_k\rangle$ and $\langle \mathbb{N}, +, V_{k^n}\rangle$ to be the same.

For the remaining part of this section let $k$ and $l$ be fixed multiplicatively independent natural numbers and $\mathrm{Supp}(x)$ be the set of prime divisors of $x$. Furthermore, let $k=p_1^{\alpha_1}\cdots p_m^{\alpha_m}$ and $l=p_1^{\beta_1}\cdots p_n^{\beta_n}$, where the $p_i$ are prime numbers.

We consider three cases.

*Case 1*: Suppose $\mathrm{Supp}(k)\not\subseteq\mathrm{Supp}(l)$ and $\mathrm{Supp}(l)\not\subseteq\mathrm{Supp}(k)$. We can suppose, without loss of generality, that $k>l$ since we can replace $k$ by one of its multiple. In this case we can easily define multiplication of a power of $k$ by a power of $l$.

**Lemma 3.4.** *Let $g: k^{\mathbb{N}}\times l^{\mathbb{N}}\rightarrow\mathbb{N}$ be multiplication, i.e. $g(x,y)=x\cdot y$. The function $g$ is definable in $\langle \mathbb{N}, +, V_k, V_l\rangle$.*

**Proof.** The function $g(x, y)=z$ is defined by the formula saying "$z$ is the smallest natural number such that $V_k(z)=x$ and $V_l(z)=y$". □

**Lemma 3.5.** *Let* $f: k^{\mathbb{N}} \to l^{\mathbb{N}}$ *be such that* $f(x)$ *is the smallest power of* $l$ *larger than* $x$. *The function* $f$ *is strictly increasing and definable in* $\langle \mathbb{N}, +, V_k, V_l \rangle$.

**Proof.** We show that for any two powers of $k$ there is a power of $l$ in between. Take $k^r$ and let $l^s$ be the largest power of $l$ smaller than $k^r$. Then $l^{s+1} > k^r$; furthermore, $l^{s+1} < k^r l < k^{r+1}$ since $l<k$ by hypothesis. Hence, $k^r < l^{s+1} < k^{r+1}$. Since $f$ is obviously definable in $\langle \mathbb{N}, +, V_k, V_l \rangle$, this completes the proof. □

**Lemma 3.6.** *Let* $u: \mathbb{N} \to k^{\mathbb{N}}$ *be such that* $u(x)$ *is the largest power of* $k$ *smaller than* $x$. *The function* $u$ *is definable in* $\langle \mathbb{N}, +, V_k \rangle$.

**Proof.** Obvious. □

**Lemma 3.7.** *Let* $h: k^{\mathbb{N}} \to k^{\mathbb{N}}$ *be such that* $h(x)=u \circ g(x, f(x))$. *Then* $h(x)=x^2$ *and* $h$ *is strictly increasing. Furthermore, if* $x<y$ *then there exists* $z \in (\operatorname{Im} h)^c$ *such that* $h(x)<z<h(y)$. *Finally,* $h$ *is definable in* $\langle \mathbb{N}, +, V_k, V_l \rangle$.

**Proof.** By definition, $u \circ g(x, f(x))=u(x \cdot f(x))=x \cdot u \circ f(x)$, for $x \in k^{\mathbb{N}}$. By definition of $f$, we have $u \circ f(x)=x$; hence, $u \circ g(x, g(x))=x \cdot x$. Therefore, $h$ is strictly increasing. Let us show that the second claim holds. This follows easily from the fact that $h(x)=x^2$. More precisely, $f(k^s)=k^{2s}<k^{2s+1}<k^{2s+2}=f(k^{s+1})$, for all $s \in \mathbb{N}$. Therefore, take $z=k^{2s+1}$; then $z \in (\operatorname{Im} h)^c$, since $h$ is increasing. Since $h$ is obviously definable in $\langle \mathbb{N}, +, V_k, V_l \rangle$, this completes the proof. □

**Conclusion.** In this case take $n=1$, $K_1=k^{\mathbb{N}}$.

*Case 2*: Suppose $\operatorname{Supp}(l) \subseteq \operatorname{Supp}(k)$ and for any $p_i, p_j \in \operatorname{Supp}(l)$, $\alpha_i/\beta_i=\alpha_j/\beta_j=\alpha/\beta$, where $\alpha, \beta \in \mathbb{N}$. Hence, $k^\beta=l^\alpha u$, $u \neq 1$, $\alpha \neq 0$, $(l, u)=1$ (since $k$ and $l$ are multiplicatively independent). Since $k$, $k^\beta$ and $l$, $l^\alpha$ are multiplicatively dependent, we can replace $k^\beta$ by $k$ and $l^\alpha$ by $l$ and assume that $k=lu$.

**Lemma 3.8.** *Let* $f: k^{\mathbb{N}} \to l^{\mathbb{N}}$ *be as in case* 1. *The function* $f$ *is strictly increasing. Furthermore, there exists* $d \in \mathbb{N} \setminus \{0\}$ *such that* $f(xk^d) \geqslant f(x) l^{(d+1)}$. *As before, this function is definable in* $\langle \mathbb{N}, +, V_k, V_l \rangle$.

**Proof.** It follows as in the proof of Lemma 3.5 that $f$ is strictly increasing.

For the second claim take $d$ to be the smallest natural number such that $u^d > l$. Therefore, for $x \in k^{\mathbb{N}}$, $f(x)/l < x$. Hence, $f(x)k^d/l < xk^d$; so, $f(x)l^d=f(x)l^d l/l \leqslant f(x)l^d u^d/l < xk^d$. Hence, $f(xk^d) > f(x)l^d$. □

**Lemma 3.9.** *Let $g': l^{\mathbb{N}} \to k^{\mathbb{N}}$ be the function which maps $l^m$ to $k^m$. The function $g'$ is strictly increasing. Furthermore, $g'$ is definable in $\langle \mathbb{N}, +, V_k, V_l \rangle$.*

**Proof.** Since $(l, u)=1$, it follows that $V_l(k^n)=V_l(l^n u^n)=V_l(l^n)=l^n$. Hence, we can define $g'(x)=y$ by the formula $V_l(y)=x$. The remaining part of the proof is obvious. □

**Remark.** The function $g'$ is multiplicative, i.e. $g'(x \cdot y)=g'(x) \cdot g'(y)$.

**Lemma 3.10.** *Let $h=g' \circ f: k^{\mathbb{N}} \to k^{\mathbb{N}}$. The function $h$ is strictly increasing. Furthermore, for all $x$ in $k^{\mathbb{N}}$, there exists a $z \notin \operatorname{Im} h$, with $h(x)<z<h(k^d x)$. (The $d$ is the one in Lemma 3.8.) Finally, $h$ is definable in $\langle \mathbb{N}, +, V_k, V_l \rangle$.*

**Proof.** Since $f$ is strictly increasing (by Lemma 3.8), it follows that $h$ is strictly increasing.

To prove the second claim it is sufficient to show that for all $x \in k^{\mathbb{N}}$, $h(xk^d)>h(x)k^d$. This is the same as showing that, for all $x \in k^{\mathbb{N}}$, $g'(f(xk^d))>g'(f(x))k^d$. Since, by Lemma 3.8, we have that, for any $x$ in $k^{\mathbb{N}}$, $f(xk^d) \geqslant f(x)l^{(d+1)}$, it follows (applying Lemma 3.9) that $g'(f(xk^d)) \geqslant g'(f(x)l^{(d+1)})$. Furthermore, by the remark above $g'(f(xk^d)) \geqslant g'(f(x))g'(l^{(d+1)})$; hence, $g'(f(xk^d))>g'(f(x))k^d$ since $g'$ is increasing by Lemma 3.9. Therefore, $h(xk^d)>h(x)k^d$.

Finally, it follows from Lemmas 3.8 and 3.9 that $h$ is definable in $\langle \mathbb{N}, +, V_k, V_l \rangle$.

**Definition.** An $x \in k^{\mathbb{N}}$ is an *i-argument* of $h$ if $h(x) \in \operatorname{Im} h$, $kh(x) \in \operatorname{Im} h, \ldots, k^{i-1}h(x) \in \operatorname{Im} h$ and $k^i h(x) \notin \operatorname{Im} h$.

**Corollary 3.11.** *Every $x \in k^{\mathbb{N}}$ is an $i$-argument for $h$, for some $i=1, \ldots, d$.*

**Proof.** Obvious from Lemma 3.10. □

Let $K_i$ be the set of all $i$-arguments of $h$. By Corollary 3.11, $k^{\mathbb{N}}$ is equal to the union of all $K_i$ and, by definition, the union is disjoint.

**Lemma 3.12.** *Property (*) holds for $h$ and $K_i$, $i=1, \ldots, d$.*

**Proof.** Let $x, y$ be in $K_i$ for some $i=1, \ldots, n$ and $x<y$. By definition $h(x) \in \operatorname{Im} h$, $kh(x) \in \operatorname{Im} h, \ldots, k^{i-1}h(x) \in \operatorname{Im} h$ and $k^i h(x) \notin \operatorname{Im} h$. Since $x, y$ are both $i$-arguments for the same $i$, it follows that $k^i h(x)<h(y)$; hence, $h(x)<k^i h(x)<h(y)$ and $k^i x \notin \operatorname{Im} h$, which proves that (*) holds. □

**Conclusion.** In this case take $k^{\mathbb{N}}=K_1 \cup \cdots \cup K_d$.

*Case 3.* Let $\operatorname{Supp}(l) \subseteq \operatorname{Supp}(k)$ and for some $p_i, p_j$, $\alpha_i/\beta_i<\alpha_j/\beta_j$. Hence, $m \leqslant n$ with, as before, $k=p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ and $l=p_1^{\beta_1} \cdots p_m^{\beta_m}$. We can suppose, without loss of generality,

that $\alpha_1/\beta_1 = \min\{\alpha_i/\beta_i;\ i=1,\ldots,m\}$ and $\alpha_m/\beta_m = \max\{\alpha_i/\beta_i;\ i=1,\ldots,m\}$. Furthermore, since $k^{\beta_1}$, $k$ and $l^{\alpha_1}$, $l$ are multiplicatively dependent we can suppose, without loss of generality, that $\alpha_1/\beta_1 = 1$; hence, $\alpha_m/\beta_m > 1$.

**Lemma 3.13.** *Let* $f' : k^{\mathbb{N}} \to l^{\mathbb{N}}$ *be the function which maps* $k^r$ *to* $l^s$, *where* $s = \lceil r\alpha_m/\beta_m \rceil$ *(the smallest natural number larger or equal to* $r\alpha_m/\beta_m$*). The function* $f'$ *is definable in* $\langle \mathbb{N}, +, V_k, V_l \rangle$ *and strictly increasing.*

**Proof.** We show that $f'(x) = y$ can be defined by the formula "$y$ is the smallest power of $l$ such that $\forall u[V_l(u) \geqslant y \Rightarrow V_k(u) \geqslant x]$".

Let $x = k^r$ and $y = l^s$. Take $u = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$ to be some natural number, where some $\gamma_i$ can be zero. There is no loss of generality in assuming that $u$ in the above formula is of this form since any prime factor different from $p_1, \ldots, p_n$ would not change the value of $V_l(u)$ and $V_k(u)$.

Now $V_k(u) = V_k(p_1^{\gamma_1} \cdots p_n^{\gamma_n}) = k^{\min\{[\gamma_i/\alpha_i];\ i=1,\ldots,n\}}$ and in the same way $V_l(u) = l^{\min\{[\gamma_i/\beta_i];\ i=1,\ldots,m\}}$. Hence, $V_l(u) \geqslant y \Rightarrow V_k(u) \geqslant x$ is equivalent to "$\min\{[\gamma_i/\beta_i];\ i=1,\ldots,m\} \geqslant s$ implies that $\min\{[\gamma_i/\alpha_i];\ i=1,\ldots,n\} \geqslant r$". Furthermore, this holds exactly if "for all $i$, $\gamma_i \geqslant s\beta_i$" implies "for all $i$, $\gamma_i \geqslant r\alpha_i$". Therefore, $\forall u[V_l(u) \geqslant y \Rightarrow V_k(u) \geqslant x]$ holds if and only if $r\alpha_i \leqslant s\beta_i$ for all $i$. Hence, "$y$ is the smallest power of $l$ such that $\forall u[V_l(u) \geqslant y \Rightarrow V_k(u) \geqslant x]$" if and only if $s = \lceil r(\alpha_m/\beta_m) \rceil$. The function $f'$ is strictly increasing since $\alpha_m/\beta_m > 1$. This completes the proof. □

**Lemma 3.14.** *Let* $g'' : l^{\mathbb{N}} \to k^{\mathbb{N}}$ *be the function which maps* $l^r$ *to* $k^r$. *The function* $g''$ *is definable in* $\langle \mathbb{N}, +, V_k, V_l \rangle$ *and strictly increasing.*

**Proof.** Since $\beta_1/\alpha_1 = 1$, we can argue as in the proof of Lemma 3.13 to show that $g''(x) = y$ can be defined by the formula "$y$ is the smallest natural number such that $\forall u[V_k(u) \geqslant y \Rightarrow V_l(u) \geqslant x]$". The function is strictly increasing by definition. □

**Lemma 3.15.** *Let* $h = g'' \circ f'$. *The function* $h$ *is strictly increasing and for all* $x$ *in* $k^{\mathbb{N}}$ *there is a* $z \notin \operatorname{Im} h$, *with* $h(x) < z < h(xk^{\beta_m})$.

**Proof.** By definition $h(k^r) = k^s$, where $s = \lceil r\alpha_m/\beta_m \rceil$. It is sufficient to show that $h(k^{r+\beta_m}) = h(k^r)k^{\alpha_m}$ since $\beta_m < \alpha_m$.

It is obvious that $\lceil (r+\beta_m)\alpha_m/\beta_m \rceil = \lceil r\alpha_m/\beta_m \rceil + \alpha_m$. This completes the proof. □

**Conclusion.** As in case 2 we can define a family $K_i$, $i=1,\ldots,\beta_m$, such that $h$ and $K_i$ satisfy (∗).

## 4. $\langle \mathbb{N}, +, V_k, V_l \rangle$ is undecidable

From Lemma 3.3 and the conclusion of the three cases, we now have the following results.

**Theorem 4.1.** *The theory of* $\langle \mathbb{N}, +, V_k, V_l \rangle$ *is undecidable for* $k, l$ *multiplicatively independent. Furthermore, we can define in it any set of the arithmetical hierarchy.*

**Corollary 4.2.** *For* $k, l$ *multiplicatively independent, the structures* $\langle \mathbb{N}, +, V_k, V_l \rangle$ *and* $\langle \mathbb{N}, +, \cdot \rangle$ *are inter-definable.*

**Proof.** Here we mean that multiplication is definable in $\langle \mathbb{N}, +, V_k, V_l \rangle$ and $V_k$, $V_l$ are definable in $\langle \mathbb{N}, +, \cdot \rangle$. The first fact follows from Lemma 3.3 and the conclusions of the three cases. The second follows from the fact that $V_k$ and $V_l$ are recognizable by automata; hence, as recursive functions they are definable in $\langle \mathbb{N}, +, \cdot \rangle$. This completes the proof. □

We conclude by giving an answer to a question of Bruyère (see [1, p. IV 18]).

**Corollary 4.3.** *Let* $k, l$ *be multiplicatively independent. Then for any* $m \in \mathbb{N}$ *the function* $V_m$ *is definable in* $\langle \mathbb{N}, +, V_k, V_l \rangle$.

**Proof.** As in the last proof, we can argue that $V_m$ is recursive and, hence, definable in $\langle \mathbb{N}, +, V_k, V_l \rangle$. □

## Acknowledgment

I thank Professor André Joyal for financial support and many fruitful discussions and also Professor Pierre Leroux for financial support. Many thanks to Christian Michaux for many discussions and for sending me material on automata and logic. Many thanks also go to Damian Niwiński, who pointed out to me that my method of proof was similar to the one in [5] and [12]. Finally, I thank the Laboratoire de combinatoire et d'informatique-mathématique de l'Université du Québec à Montréal for its hospitality. This work has been completed with the financial support of La Fondation de l'UQAM, the author holding the J.A. de Sève post-doctoral scholarship.

## References

[1] V. Bruyère, Entiers et automates finis, U.E. Mons (mémoire de licence en mathématiques) 1984–85.
[2] J.R. Büchi, Weak second-order arithmetic and finite automata, *Z. Math. Logik Grundlag. Math.* **6** (1960) 66–92.
[3] A. Cobham, On the base-dependence of sets of numbers recognizable by finite-automata, *Math. Systems Theory* **3** (1969) 186–192.
[4] S. Eilenberg, *Automata, Languages and Machines, Vol. A* (Academic Press, New York, 1974).
[5] C.C. Elgot and M.O. Rabin, Decidability and undecidability of extensions of second (first) order theory of (generalized) successor, *J. Symbolic Logic* **31** (2) (1966) 169–181.
[6] G. Hansel, A propos d'un théorème de Cobham, in: D. Perrin, ed., *Actes de la Fête des Mots, Greco de Programmation* (CNRS, Rouen, 1982).

[7] B. Hodgson, Décidabilité par automate fini, *Ann. Sci. Math. Québec* **7** (1) (1985) 39–57.
[8] R. McNaughton, Review of [2], *J. Symbolic Logic* **28** (1963) 100–102.
[9] C. Michaux and F. Point, Les ensembles $k$-reconnaissables sont définissables dans $\langle \mathbb{N}, +, V_k \rangle$, *C.R. Acad. Sci. Paris Sér. I Math.* **303** (19) (1986) 939–942.
[10] D. Perrin, Finite automata, in: J. van Leeuwen, ed., *Handbook of Theoretical Computer Science, Vol. B* (Elsevier, Amsterdam, 1990) 1–57.
[11] A.L. Semenov, On certain extensions of the arithmetic of addition of natural numbers, *Math. USSR-Izv.* **15** (2) (1980) 401–418.
[12] W. Thomas, A note on undecidable extensions of monadic second order successor arithmetic, *Arch. Math. Logic* **17** (1975) 43–44.
[13] W. Thomas, Automata on infinite objects, in: J. van Leeuwen, ed., *Handbook of Theoretical Computer Science, Vol. B* (Elsevier, Amsterdam, 1990) 133–191.
[14] R. Villemaire, $\langle \mathbb{N}, +, V_2, V_3 \rangle$ est indécidable, in: *C.R. Acad. Sci. Paris Sér. I Math.* **314** (1992) 775–777.
[15] R. Villemaire, Joining $k$- and $l$-recognizable sets of natural numbers, in: *Proc. STACS '92*, Lecture Notes in Computer Science, Vol. 577 (Springer, Berlin, 1992) 83–94.