

The Monadic Theory of Morphic Infinite Words and Generalizations

Olivier Carton¹

*Institut Gaspard Monge, Université de Marne-la-Vallée, 5 boulevard Descartes, Champs-sur-Marne,
F-77454 Marne-la-Vallée Cedex 2, France
E-mail: Olivier.Carton@univ-mlv.fr*

and

Wolfgang Thomas²

*Lehrstuhl für Informatik VII, RWTH Aachen, Ahornstr. 55, D-52056 Aachen, Germany
E-mail: thomas@informatik.rwth-aachen.de*

We present new examples of infinite words which have a decidable monadic theory. Formally, we consider structures $\langle \mathbb{N}, <, P \rangle$ which expand the ordering $\langle \mathbb{N}, < \rangle$ of the natural numbers by a unary predicate P ; the corresponding infinite word is the characteristic 0-1-sequence x_P of P . We show that for a morphic predicate P the associated monadic second-order theory $\text{MTh}(\mathbb{N}, <, P)$ is decidable, thus extending results of Elgot and Rabin (1966) and Maes (1999). The solution is obtained in the framework of semigroup theory, which is then connected to the known automata theoretic approach of Elgot and Rabin. Finally, a large class of predicates P is exhibited such that the monadic theory $\text{MTh}(\mathbb{N}, <, P)$ is decidable, which unifies and extends the previously known examples. © 2002 Elsevier Science (USA)

Key Words: second-order; morphic predicates.

1. INTRODUCTION

In this paper we study the following decision problem about a fixed ω -word x :

(Acc_x) Given a Büchi automaton \mathcal{A} , does \mathcal{A} accept x ?

If the problem (Acc_x) is decidable, this means intuitively that one can use x as external oracle information in nonterminating finite-state systems and still keep decidability results on their behaviour. We solve this problem for a large class of ω -words, the so-called *morphic words* and some generalizations, complementing and extending results of Elgot and Rabin [11] and Maes [15].

The problem (Acc_x) is motivated by a logical decision problem regarding monadic theories, starting from the fundamental work of Büchi [8] on the equivalence between the monadic second-order theory $\text{MTh}(\mathbb{N}, <)$ of the linear order $\langle \mathbb{N}, < \rangle$ and ω -automata (more precisely: Büchi automata). Büchi used this reduction of formulas to automata to show that $\text{MTh}(\mathbb{N}, <)$ is decidable. The decidability proof is based on the fact that a sentence ϕ of the monadic second-order language of $\langle \mathbb{N}, < \rangle$ can be converted into an input-free Büchi automaton \mathcal{A} such that ϕ holds in $\langle \mathbb{N}, < \rangle$ iff \mathcal{A} admits some successful run; the latter is easily checked.

It was soon observed that Büchi's Theorem is applicable also in a more general situation, regarding expansions of $\langle \mathbb{N}, <, P \rangle$ of the structure $\langle \mathbb{N}, < \rangle$ by a fixed predicate $P \subseteq \mathbb{N}$. Here one starts with a formula $\phi(X)$ with one free set variable and considers an equivalent Büchi automaton \mathcal{A} over the input alphabet $\mathbb{B} = \{0, 1\}$: The formula $\phi(X)$ is true in $\langle \mathbb{N}, < \rangle$ with P as interpretation of X iff \mathcal{A} accepts the characteristic word x_P over \mathbb{B} associated with P (the i th letter of x_P is 1 iff $i \in P$). In other words: The theory $\text{MTh}(\mathbb{N}, <, P)$ is decidable if one can determine, for any given Büchi automaton \mathcal{A} , whether \mathcal{A} accepts x_P . Elgot and Rabin [11] followed this approach via the decision problem (Acc_{x_P}) and found several interesting predicates P such that $\text{MTh}(\mathbb{N}, <, P)$ is decidable, among them the set of factorial numbers $n!$, the set of k -th powers n^k for any fixed k , and the set of k -powers k^n for any fixed k .

¹ URL: <http://www-igm.univ-mlv.fr/~carton/>.

² URL: <http://www-i7.informatik.rwth-aachen.de/~thomas/>.

Elgot and Rabin (and later also Siefkes [18]) used an automata theoretic analysis, which we call the *contraction method*, for the solution of the decision problem (Acc_{x_P}) . The idea is to reduce the decision problem to the case of ultimately periodic ω -words (which is easily solvable). Given P as one of the predicates mentioned above, Elgot and Rabin showed that for any Büchi automaton \mathcal{A} , the 0-sections in x_P can be contracted in such a way that an *ultimately periodic* ω -word β is obtained which is accepted by \mathcal{A} iff x_P is accepted by \mathcal{A} . For the ultimately periodic word β , one can easily decide whether it is accepted by \mathcal{A} .

More recently, A. Maes [15] studied “morphic predicates,” which are obtained by iterative application of a morphism on words (see Section 2 for definitions). The morphic predicates include examples (for instance, the predicate of the Fibonacci numbers) which do not seem to be accessible by the Elgot–Rabin method. Maes proved that for any morphic predicate P , the *first-order* theory $\text{FTh}(\mathbb{N}, <, P)$ is decidable, and he also introduced appropriate (although special) versions of morphic predicates of higher arity. It remained open whether for each morphic predicate P , the monadic theory $\text{MTh}(\mathbb{N}, <, P)$ is decidable.

In the present paper we answer this question positively, based on a new (and quite simple) semigroup approach to the decision problem (Acc_{x_P}) : In Section 2 we show that for morphic predicates P the problem (Acc_{x_P}) is decidable. As a consequence, we find new examples of predicates P with decidable monadic theory $\text{MTh}(\mathbb{N}, <, P)$. Prominent ones are the Fibonacci predicate (consisting of all Fibonacci numbers) and the Thue–Morse word predicate (consisting of those numbers whose binary expansion has an even number of 1’s).

In the second part of the paper, we embed this approach into the framework of the contraction method. This method is shown to be applicable to predicates which we call “residually ultimately periodic.” We prove two results: Each morphic predicate is residually ultimately periodic, and a certain class of residually ultimately periodic predicates shares strong closure properties, among them under sum, product, and exponentiation. This allows to obtain many example predicates P for which the monadic theory $\text{MTh}(\mathbb{N}, <, P)$ is decidable.

It should be noted that for certain concrete applications (such as for the Fibonacci predicate) the semigroup approach is much more convenient than an explicit application of the contraction method, and only an analysis in retrospect reveals the latter possibility. Also morphic predicates like the Thue–Morse word predicate are not approachable directly by the contraction method, because there are no long sections of 0’s or 1’s.

Let us finally comment on example predicates P where the corresponding Büchi acceptance problem (Acc_{x_P}) and hence $\text{MTh}(\mathbb{N}, <, P)$ is undecidable, and give some comments on unsettled cases and on related work.

First we recall a simple recursive predicate P such that $\text{MTh}(\mathbb{N}, <, P)$ is undecidable. For this, consider a non-recursive, recursively enumerable set Q of positive numbers, say with recursive enumeration m_0, m_1, m_2, \dots . Define $P = \{n_0, n_1, n_2, \dots\}$ by $n_0 = 0$ and $n_{i+1} = n_i + m_i$. Then P is recursive but even the first-order theory $\text{FTh}(\mathbb{N}, <, P)$ is undecidable: We have $k \in Q$ iff for some element x of P , the element $x + k$ is the next element after x in P , a condition which is expressible by a first-order sentence ϕ_k over $(\mathbb{N}, <, P)$. Büchi and Landweber [9] and Thomas [19] determined the recursion theoretic complexity of theories $\text{MTh}(\mathbb{N}, <, P)$ for recursive P ; it turns out, for example, that for recursive P the theory $\text{MTh}(\mathbb{N}, <, P)$ is truth-table-reducible to a complete Σ_2 -set, and that this bound cannot be improved. The situation changes when recursive predicates over countable ordinals are considered (see [22]). In [20] it was shown that for each predicate P , the full monadic theory $\text{MTh}(\mathbb{N}, <, P)$ is decidable iff the weak monadic theory $\text{WMTh}(\mathbb{N}, <, P)$ is (where all set quantifiers are assumed to range only over finite sets). However, there are examples P such that the first-order theory $\text{FTh}(\mathbb{N}, <, P)$ is decidable but $\text{WMTh}(\mathbb{N}, <, P)$ is undecidable [19].

In the present paper we restrict ourselves to expansions of $(\mathbb{N}, <)$ by unary predicates. For expansions $(\mathbb{N}, <, f)$ by unary functions f , the undecidability of $\text{MTh}(\mathbb{N}, <, f)$ arises already in very simple cases, like for the doubling function $n \mapsto 2n$. For a survey on these theories see [16].

On the other hand, it seems hard to provide mathematically natural recursive predicates P for which $\text{MTh}(\mathbb{N}, <, P)$ is undecidable. A prominent example of a natural predicate P where the decidability of $\text{MTh}(\mathbb{N}, <, P)$ is unsettled is the prime number predicate. As remarked already by Büchi and Landweber in [9], a decidability proof should be difficult because it would in principle answer unsolved number theoretic problems like the twin prime hypothesis (which states that infinitely many pairs $(p, p + 2)$

of primes exist). The only known result is that $\text{MTh}(\mathbb{N}, <, P)$ is decidable under the linear case of Schinzel's hypothesis [4].

Part of the results of the present paper has been presented at the conference MFCS'2000 [10].

2. BÜCHI AUTOMATA OVER MORPHIC PREDICATES

A *morphism* τ from A^* to itself is an application such that the image of any word $u = a_1 \dots a_n$ is the concatenation $\tau(a_1) \dots \tau(a_n)$ of the images of its letters. A morphism is then completely defined by the images of the letters. In the sequel, we describe morphisms by just specifying the respective images of the letters as in the following example

$$\tau : a \mapsto ab \quad b \mapsto ccb \quad c \mapsto c.$$

If τ is a morphism from A^* into B^* and if $x = a_0 a_1 a_2 \dots$ is an infinite word, the word $\tau(a_0)\tau(a_1)\tau(a_2) \dots$ is also denoted by $\tau(x)$. Let A be a finite alphabet and let τ be a morphism from A^* to itself. For any integer n , we denote τ^n the composition of n copies of τ . Let $(x_n)_{n \geq 0}$ be the sequence of finite words defined by $x_n = \tau^n(a)$ for any integer n . If the first letter of $\tau(a)$ is a , then each word x_n is a prefix of x_{n+1} . If furthermore the sequence of length $|x_n|$ is not bounded, the sequence $(x_n)_{n \geq 0}$ converges to an infinite word x which is denoted by $\tau^\omega(a)$. The word x is a *fixed point* of the morphism since it satisfies $x = \tau(x)$.

EXAMPLE 2.1. Let consider the morphism τ given by

$$\tau : a \mapsto ab \quad b \mapsto ccb \quad c \mapsto c.$$

The words $x_n = \tau^n(a)$ for $n = 1, 2, 3, 4$ are respectively equal to

$$\begin{aligned} \tau(a) &= ab & \tau^3(a) &= abccbccccb \\ \tau^2(a) &= abccb & \tau^4(a) &= abccbccccbcccccb \end{aligned}$$

It can be easily proved by induction on n that $\tau^{n+1}(a) = abc^2bc^4b \dots c^{2n}b$. Therefore, the fixed point $\tau^\omega(a)$ is equal to the infinite word $abc^2bc^4bc^6bc^8 \dots$.

An infinite word x over B is said to be *morphic* if there is a morphism τ from A^* to itself and a morphism σ from A^* to B^* such that $x = \sigma(\tau^\omega(a))$. In the sequel, the alphabet B is often the alphabet $\mathbb{B} = \{0, 1\}$ and the morphism σ is letter to letter.

The *characteristic word* of a predicate P over the set \mathbb{N} of non-negative integers is the infinite word $x_P = (b_n)_{n \geq 0}$ over the alphabet \mathbb{B} defined by $b_n = 1$ iff $n \in P$ and $b_n = 0$ otherwise. A predicate is said to be *morphic* iff its characteristic word is morphic.

These definitions are illustrated by the following two examples.

EXAMPLE 2.2. Consider the morphism τ introduced in the preceding example and the morphism σ given by

$$\sigma : a \mapsto 1 \quad b \mapsto 1 \quad c \mapsto 0$$

The morphic word $\sigma(\tau^\omega(a)) = 1100100001 \dots$ is actually the characteristic word of the predicate $P = \{n^2 \mid n \in \mathbb{N}\}$. This can be easily proved using the equality $(n+1)^2 = \sum_{k=0}^n 2k+1$. The square predicate is therefore morphic.

It will be proved in the sequel that the class of morphic predicates contains all predicates of the form $\{n^k \mid n \in \mathbb{N}\}$ and $\{k^n \mid n \in \mathbb{N}\}$ for any fixed integer k .

EXAMPLE 2.3. Consider the morphism τ from \mathbb{B}^* to \mathbb{B}^* defined by

$$\tau : 0 \mapsto 01 \quad 1 \mapsto 10$$

The fixed point $\tau^\omega(1) = 100101100110 \dots$ is the characteristic word of the predicate P with $n \in P$ iff the binary expansion of n contains an even number of 1. The fixed point $\tau^\omega(1)$ is the well-known Thue–Morse word. We refer the reader to [5] for an interesting survey on that sequence and related works of A. Thue.

Recall that a *Büchi automaton* is an automaton $\mathcal{A} = (Q, E, I, F)$ where Q is a finite set of states, $E \subseteq Q \times A \times Q$ is the set of transitions and I and F are the sets of initial and final states. A path is successful if it starts in an initial state and goes infinitely often through a final state. An infinite word is accepted if it is the label of a successful path. We refer the reader to [21] for a complete introduction. Now we can state the main result and in the corollary, its formulation in the context of monadic theories:

THEOREM 2.1. *Let $x = \sigma(\tau^\omega(a))$ be a fixed morphic word where $\tau : A^* \rightarrow A^*$ and $\sigma : A^* \rightarrow B^*$ are morphisms. For any Büchi automaton \mathcal{A} , it can be decided whether x is accepted by \mathcal{A} .*

As explained in the introduction, the theorem can be transferred to a logical decidability result, invoking Büchi's Theorem [8] on the equivalence between monadic formulas over $\langle \mathbb{N}, < \rangle$ and Büchi automata:

COROLLARY 2.1. *For any unary morphic predicate P , the monadic second-order theory of $\langle \mathbb{N}, <, P \rangle$ is decidable.*

Proof (of Theorem 2.1). Let $\mathcal{A} = (Q, E, I, F)$ be a Büchi automaton. Define the equivalence relation \equiv over A^+ by

$$u \equiv u' \stackrel{\text{def}}{\iff} \forall p, q \in Q \quad \begin{cases} p \xrightarrow{u} q \Leftrightarrow p \xrightarrow{u'} q \\ p \xrightarrow{u}_F q \Leftrightarrow p \xrightarrow{u'}_F q \end{cases}$$

where $p \xrightarrow{u} q$ means that there is a path from p to q labeled by u and $p \xrightarrow{u}_F q$ means that there is a path from p to q labeled by u which hits some final state. This equivalence relation captures that two finite words have the same behavior in the automaton with respect to the Büchi acceptance condition. It was already introduced by Büchi in [8].

Denote by π the projection from A^+ to A^+/\equiv which maps each word to its equivalence class.

The equivalence relation \equiv is a congruence of finite index. Indeed, for any words u, v, u' , and v' , the following implication holds: If

$$\left. \begin{array}{l} u \equiv u' \\ v \equiv v' \end{array} \right\} \Rightarrow uv \equiv u'v'.$$

This property allows us to define a product on the classes which endows the set A^+/\equiv with a structure of finite semigroup. The projection π is then a morphism from A^+ onto A^+/\equiv .

Furthermore, for any fixed states p and q , there are at most three possibilities for any word u : Either there is a path from p to q through a final state, or there is a path from p to q but not through a final state or there is no path from p to q labeled by u . This proves that the number of classes is bounded by 3^{n^2} where n is the number of states of the automaton.

The following observation gives the main property of the congruence \equiv . Suppose that the two infinite words x and x' can be factored $x = u_0u_1u_2 \dots$ and $x' = u'_0u'_1u'_2 \dots$ such that $u_k \equiv u'_k$ for any $k \geq 0$. Then x is accepted by \mathcal{A} iff x' is accepted by \mathcal{A} . Indeed, suppose that x is the label of a successful path. This path can be factored

$$q_0 \xrightarrow{u_0} q_1 \xrightarrow{u_1} q_2 \xrightarrow{u_2} \dots$$

where q_0 is initial and where the finite path $q_k \xrightarrow{u_k} q_{k+1}$ meets a final state for infinitely many k . Since $u_k \equiv u'_k$ for any $k \geq 0$, there is another path

$$q_0 \xrightarrow{u'_0} q_1 \xrightarrow{u'_1} q_2 \xrightarrow{u'_2} \dots$$

where the finite path $q_k \xrightarrow{u'_k} q_{k+1}$ meets a final state whenever $q_k \xrightarrow{u_k} q_{k+1}$ does. This proves that x' is also the label of a successful path and that it is accepted by \mathcal{A} . In particular, if an infinite word x can be factored $x = u_0 u_1 u_2 \dots$ such that $u_1 \equiv u_2 \equiv \dots$, then x is accepted by \mathcal{A} iff $u_0 u_1^\omega$ is also accepted by \mathcal{A} .

Since a is the first letter $\tau(a)$, the word $\tau(a)$ is equal to au for some nonempty finite word u . It may be easily verified by induction on n that for any integer n , one has

$$\tau^{n+1}(a) = au\tau(u)\tau^2(u) \dots \tau^n(u).$$

The word $x = \sigma(\tau^\omega(a))$ can be factored $x = u_0 u_1 u_2 \dots$, where $u_0 = \sigma(au)$ and $u_n = \sigma(\tau^n(u))$ for $n \geq 1$.

We claim that there are two positive integers n and p such that for any $k \geq n$, the relation $u_k \equiv u_{k+p}$ holds. This relation is equivalent to $\pi(u_k) = \pi(u_{k+p})$. A morphism from A^+ into a semigroup is completely determined by the images of the letters. Therefore, there are finitely many morphism from A^+ into the finite semigroup A^+/\equiv . This implies that there are two positive integers n and p such that $\pi \circ \sigma \circ \tau^n = \pi \circ \sigma \circ \tau^{n+p}$. This implies that $\pi \circ \sigma \circ \tau^k = \pi \circ \sigma \circ \tau^{k+p}$ for any k greater than n , and thus $u_k \equiv u_{k+p}$. Note that these two integers n and p can be effectively computed. It suffices to check that $\sigma(\tau^n(b)) \equiv \sigma(\tau^{n+p}(b))$ for any letter b of the alphabet A .

Define the sequence $(v_k)_{k \geq 0}$ of finite words by $v_0 = u_0 \dots u_{n-1}$ and $v_k = u_{n+(k-1)p} \dots u_{n+kp-1}$ for $k \geq 1$. The word x can be factored $x = v_0 v_1 v_2 \dots$ and the relations $v_1 \equiv v_2 \equiv v_3 \dots$ hold. This proves that the word x is accepted by the automaton \mathcal{A} iff the word $v_0 v_1^\omega$ is accepted by \mathcal{A} . This can obviously be decided. ■

3. A LARGE CLASS OF MORPHIC PREDICATES

The purpose of this section is to give a uniform representation of a large class of morphic predicates: We will show that each predicate $P = \{Q(n)k^n \mid n \in \mathbb{N}\}$ for $k \geq 0$ and a polynomial $Q(n)$ with non-negative integer values is morphic. This supplies a large class of predicates P where the decision problem $(\text{Acc}_{x,p})$ and hence the monadic theory of $(\mathbb{N}, <, P)$ are decidable. In particular, the classical examples $\{k^n \mid n \in \mathbb{N}\}$ or $\{n^k \mid n \in \mathbb{N}\}$ for some fixed k in \mathbb{N} of [11] are covered by this.

As a preparation, we shall develop a sufficient condition on sequences $(u_n)_{n \geq 0}$ to define a morphic predicate. It will involve the notion of a \mathbb{N} -rational sequence. These considerations will also show that the Fibonacci predicate $\{F_n \mid n \in \mathbb{N}\}$ (where $F_0 = F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$) is morphic.

We refer the reader to [17] for a complete introduction and to [3] for a survey although we recall here the definitions.

DEFINITION 3.1. A sequence $(u_n)_{n \geq 0}$ of integers is \mathbb{N} -rational if there is a graph G allowing multiple edges and sets I and F of vertices such that u_n is the number of paths of length n from a vertex of I to a vertex of F . The graph G is said to *recognize* the sequence $(u_n)_{n \geq 0}$.

An equivalent definition is obtained by considering non-negative matrices. A sequence $(u_n)_{n \geq 0}$ is \mathbb{N} -rational iff there is a matrix M in $\mathbb{N}^{k \times k}$ and two vectors L in $\mathbb{B}^{1 \times k}$ and C in $\mathbb{B}^{k \times 1}$ such that $u_n = L M^n C$. It suffices indeed to consider the adjacency matrix M of the graph and the two characteristic vectors of the sets I and F of vertices. It is also possible to assume that the two vectors L and C respectively belong $\mathbb{N}^{1 \times k}$ and $\mathbb{N}^{k \times 1}$ instead of $\mathbb{B}^{1 \times k}$ and $\mathbb{B}^{k \times 1}$ since the class of \mathbb{N} -rational sequences is obviously closed under addition. A triplet (L, M, C) such that $u_n = L M^n C$ is called a *matrix representation* of the sequence $(u_n)_{n \geq 0}$ and the integer k is called the *dimension* of the representation. The following example illustrates these notions.

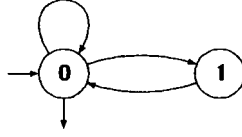


FIG. 1. A graph for the Fibonacci sequence.

EXAMPLE 3.1. The number of successful paths of length n in the graph pictured in Fig. 1 is the Fibonacci number F_n , where $F_0 = F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$. This shows that the sequence $(F_n)_{n \geq 0}$ is \mathbb{N} -rational. This sequence has the matrix representation of dimension 2

$$L = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \quad M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad C = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

which can be deduced from the graph of Fig. 1.

We now state the main result of this section.

THEOREM 3.1. *Let u_n be a sequence of non-negative integers and let $d_n = u_{n+1} - u_n$ be the sequence of differences. If there is some integer ℓ such that $d_n \geq 1$ for any $n \geq \ell$ and such that the sequence $(d_n)_{n \geq \ell}$ is \mathbb{N} -rational, then the predicate $P = \{u_n \mid n \in \mathbb{N}\}$ is morphic.*

As a first illustration of the theorem, reconsider the predicate of the Fibonacci numbers F_n : Each difference $d_n = F_{n+1} - F_n$ is equal to F_{n-1} , it obviously satisfies $d_n \geq 1$ for $n \geq 1$, and the sequence $(F_n)_{n \geq 0}$ is \mathbb{N} -rational as shown in Example 3.1. So the Fibonacci predicate is morphic.

With the following corollary we obtain a large collection of morphic predicates, including the predicates of the form $\{n^k \mid n \in \mathbb{N}\}$ and $\{k^n \mid n \in \mathbb{N}\}$ considered in [11].

COROLLARY 3.1. *Let Q be a polynomial such that $Q(n)$ is integer for any integer n and let k be a positive integer. The predicate $P = \{Q(n)k^n \mid n \in \mathbb{N} \text{ and } Q(n) \geq 0\}$ is morphic.*

The proof of the corollary is entirely based on the following lemma.

LEMMA 3.1. *Let Q be a polynomial with a positive leading coefficient such that $Q(n)$ is integer for any integer n . Let k be a positive integer and let u_n be defined by $u_n = Q(n)k^n$. There is a non-negative integer ℓ such that the sequence $(u_{n+\ell})_{n \geq 0}$ is \mathbb{N} -rational.*

Note that such a polynomial may have non-integer coefficients as the polynomial $Q(x) = x(x+1)/2$.

Proof. Let d be the degree of Q . We claim that there are then a non-negative integer ℓ and positive integers a_0, \dots, a_d such that for any n ,

$$Q(n + \ell) = \sum_{i=0}^d a_i \binom{n}{i}.$$

For any integer m , define the polynomial $Q_m(n)$ by $Q_m(n) = Q(n + m)$. Since $Q_m(n)$ is integer for any integer n , the polynomial $Q_m(n)$ is equal to a linear combination of the binomials with integer coefficients (see [12, p. 189]). There is a unique sequence $b_{m,0}, \dots, b_{m,d}$ of $d + 1$ integers such that for any integer n

$$Q_m(n) = \sum_{i=0}^d b_{m,i} \binom{n}{i}.$$

Since the binomials satisfy the well-known relation $\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$, it follows that the coefficients $b_{m,i}$ satisfy the following relation. For any integer m , one has $b_{m+1,d} = b_{m,d}$ and $b_{m+1,i} = b_{m,i} + b_{m,i+1}$ for $i < d$. Since the leading coefficient of Q_m is positive, the coefficient $b_{m,d}$ is also positive for any m . Using the relation on the coefficients on the $b_{m,i}$, it can be proved by induction on the difference $d - i$

that for any $i \leq d$, there is an integer ℓ_i such that $b_{m,i}$ is positive for any $m \geq \ell_i$. Let ℓ be the integer defined by $\ell = \max\{\ell_i \mid i \leq d\}$ and let a_i be equal to $b_{\ell,i}$ for $i \leq d$. They obviously satisfy the claimed property.

We now define the matrix M and the vectors L and C as follows. The vector L is the vector of dimension $d + 1$ defined by $L_0 = k^\ell$ and $L_i = 0$ for $1 \leq i \leq d$. The matrix M is the square matrix of dimension $d + 1$ defined by $M_{i,j} = k$ if $i = j - 1$ or $i = j$ and $M_{i,j} = 0$ otherwise for $0 \leq i, j \leq d$. The vector C is the vector of dimension $d + 1$ defined by $C_i = a_i$ for $0 \leq i \leq d$. It is pure routine to prove by induction on n that LM^n is the vector L_n given by $L_{n,i} = k^{n+\ell} \binom{n}{i}$ for $0 \leq i \leq d$. Therefore $u_{n+\ell}$ is equal to $LM^n C$ for any $n \geq 0$ and the sequence $(u_{n+\ell})_{n \geq 0}$ is \mathbb{N} -rational. ■

The proof of Theorem 3.1 needs some preliminary result that we now state. This lemma makes easier the proof that certain predicates are morphic. It essentially states that the property of being morphic is preserved by shifting and by changing a finite number of values. In particular, if two predicates P and P' coincide for almost every n , then P is morphic iff P' is morphic.

LEMMA 3.2. *Let P be a predicate and let R be a finite set of integers. Let k be a non-negative integer and let P' be the predicate $R \cup \{n + k \mid n \in P\}$. Then P is morphic iff P' is morphic.*

Proof. Let P be a morphic predicate. Assume that the characteristic word x_P of P is equal to $\sigma(\tau^\omega(a))$ where τ and σ are respectively morphisms from A^* into itself and from A^* into \mathbb{B}^* . Let x be the fixed point $\tau^\omega(a)$ and let u be the finite word such that $\tau(a) = au$. The infinite word x can be then factorized

$$x = au\tau(u)\tau^2(u) \dots$$

We first prove that both predicates $P' = \{n + 1 \mid n \in P\}$ and $P'' = \{0\} \cup P'$ are also morphic. Let A' be the alphabet $A \cup \{a_0, a_1\}$ where a_0 and a_1 are two new symbols. Define the morphism τ' from A'^* into itself by $\tau'(a_0) = a_0a_1$, $\tau'(a_1) = u$, and $\tau'(b) = \tau(b)$ for any b in A . It is clear that the fixed point $x' = \tau'^\omega(a_0)$ is equal to

$$x' = a_0a_1u\tau(u)\tau^2(u) \dots$$

Define the morphism σ' from A'^* into \mathbb{B}^* by $\sigma'(a_1) = \sigma(a)$ and $\sigma'(b) = \sigma(b)$ for any b in A . If $\sigma'(a_0)$ is set to 0, then the word $\sigma'(\tau'^\omega(a_0))$ is the characteristic word of P' and if $\sigma'(a_0)$ is set to 1, then the word $\sigma'(\tau'^\omega(a_0))$ is the characteristic word of P'' .

We now prove that there is a positive integer k such that the predicate $P' = \{n - k \mid n \geq k \text{ and } n \in P\}$ is morphic. Let A' be the alphabet $A \cup \{a_0\}$ where a_0 is a new symbol. Define the morphism τ' from A'^* into itself by $\tau'(a_0) = a_0\tau(u)$ and $\tau'(b) = \tau(b)$ for any b in A . It is clear that the fixed point $x' = \tau'^\omega(a_0)$ is equal to

$$x' = a_0\tau(u)\tau^2(u)\tau^3(u) \dots$$

Let k be the length of u . Define the morphism σ' from A'^* into \mathbb{B}^* by $\sigma(a_0) = P(k)$ and $\sigma'(b) = \sigma(b)$ for any b in A . The word $\sigma'(\tau'^\omega(a_0))$ is the characteristic word of P' .

The claimed result follows then easily from the two previous results. ■

The following two results will be used in the proof of Theorem 3.1. The first result is due to Schützenberger. We refer the reader to [17, Theorem II.8.6] and [6, Theorem V.2.1] for complete proofs.

THEOREM 3.2 (Schützenberger 1970). *Let $(u_n)_{n \geq 0}$ be a \mathbb{N} -rational sequence such that $u_n \geq 1$ for any n . The sequence $(u_n - 1)_{n \geq 0}$ is also \mathbb{N} -rational.*

For the next result, we need the notion of a D0L-sequence. A \mathbb{N} -rational sequence $(u_n)_{n \geq 0}$ of integers is said to be a D0L-sequence if it can be recognized by a graph all of whose states are final. Equivalently, a \mathbb{N} -rational sequence $(u_n)_{n \geq 0}$ is a D0L-sequence if it has a matrix representation (L, M, C) such that all components of L are either 0 or 1 and such that all components of C are equal to 1. We have then the following result [17, Lemma III.7.4].

LEMMA 3.3. *Every \mathbb{N} -rational sequence $(u_n)_{n \geq 0}$ can be decomposed into D0L-sequences. This means that there are two integers K and p such that each sequence $(u_{k+np})_{n \geq 0}$ for $k \geq K$ is a D0L-sequence.*

We finally come to the proof of Theorem 3.1.

Proof. We suppose that $d_n = u_{n+1} - u_n$ satisfies $d_n \geq 1$ for $n \geq \ell$ and that the sequence $(d_n)_{n \geq \ell}$ is \mathbb{N} -rational. By Lemma 3.2, it may be assumed without loss of generality that $\ell = 0$. By Theorem 3.2, the sequence $(v_n)_{n \geq 0}$ defined by $v_n = d_n - 1$ is \mathbb{N} -rational. By Lemma 3.3, that sequence can be decomposed into D0L-sequences. There are two integers K and p such that each sequence $(v_{k+np})_{n \geq 0}$ for $k \geq K$ is a D0L-sequence. By Lemma 3.2, it may be assumed again without loss of generality that $K = 0$ and that $u_0 = 0$. For $k < p$, define the sequence $v_k = (v_{k,n})_{n \geq 0}$ by $v_{k,n} = v_{k+np}$. Each sequence v_k has a matrix representation (L_k, M_k, C_k) such that each component of L_k are either 0 or 1 and such that all components of C_k are equal to 1. Let h_k be the dimension of that representation. Define the alphabet A by

$$A = \{a\} \cup \{b_k \mid 0 \leq k < p\} \cup \{c_{k,i} \mid 0 \leq k < p \text{ and } 1 \leq i \leq h_k\}.$$

Define the morphism from A^* into itself by

$$\begin{aligned} a &\mapsto ac_{0,1}^{L_{0,1}} \dots c_{0,h_0}^{L_{0,h_0}} b_0 c_{1,1}^{L_{1,1}} \dots c_{1,h_1}^{L_{1,h_1}} b_1 c_{2,1}^{L_{2,1}} \dots b_{p-1} \\ b_k &\mapsto b_k \\ c_{k,i} &\mapsto c_{k,1}^{M_{k,i,1}} \dots c_{k,h_k}^{M_{k,i,h_k}}. \end{aligned}$$

It can be easily proved by induction on n that

$$\tau^{n+1}(a) = a \prod_{i=0}^n w_{0,i} b_0 w_{1,i} b_1 \dots w_{p-1,i} b_{p-1}$$

where each $w_{k,i}$ is a word on the alphabet $\{c_{k,j} \mid 1 \leq j \leq h_k\}$ of length $v_{k,i}$. Actually the number of occurrences of the letter $c_{k,j}$ in the word $w_{k,i}$ is the j th component of the vector $L_k M_k^i$. Define then the morphism σ from A^* into \mathbb{B}^* by $\sigma(a) = 1$, $\sigma(b_k) = 1$ for $0 \leq k < p$ and $\sigma(c_{k,j}) = 0$ for $0 \leq k < p$ and $1 \leq j \leq h_k$. ■

As a complement to Corollary 3.1 (that predicates $\{Q(n)k^n \mid n \in \mathbb{N}\}$ are morphic), we formulate a necessary condition for a predicate P to be morphic. It turns out that the factorial predicate $\{n! \mid n \in \mathbb{N}\}$ does not fall under this condition, which shows that it is not morphic. In the subsequent section, we shall develop a framework where such predicates can be handled together with the morphic ones, thus unifying the contraction method of Elgot and Rabin with the results above.

PROPOSITION 3.1. *Let $(u_n)_{n \geq 0}$ be a strictly increasing sequence of integers. If the predicate $\{u_n \mid n \in \mathbb{N}\}$ is morphic, then $u_{n+1} - u_n = O(k^n)$ for some integer k .*

Proof. Suppose that the characteristic word of the predicate $\{u_n \mid n \in \mathbb{N}\}$ is equal to $\sigma(\tau^\omega(a))$ where τ and σ are respectively morphisms from A^* into itself and from A^* into \mathbb{B}^* . Let x be the fixed point $\tau^\omega(a)$ and let u be the finite word such that $\tau(a) = au$. The infinite word x can be then factorized

$$x = au\tau(u)\tau^2(u) \dots$$

Let k be the integer defined by $k = \max_{b \in A} |\tau(b)|$. It can be easily shown by induction on n that $|\tau^n(b)| \leq k^n$ for any letter b . Let B the set of letters b such that $\sigma(b)$ contains at least one 1, that is $B = \{b \mid \sigma(b) \notin 0^*\}$. We claim that if for a fixed letter b , there is an integer n such that $\tau^n(b)$ contains a letter of B , the smallest integer satisfying this property is smaller than the cardinality of A . This follows from the fact that a letter c appears in $\tau^n(b)$ iff there is a sequence b_0, \dots, b_n of letters such that $b_0 = b$, $b_n = c$ and b_{i+1} appears in $\tau(b_i)$ for $0 \leq i < n$. For any integer n , the word $\tau^n(a) \dots \tau^{n+p}(a)$ where $p = |A|$ contains therefore a letter of B and the result follows easily. ■

4. PROFINITELY ULTIMATELY PERIODIC PREDICATES

In this section, we develop a framework which merges the contraction method of Elgot and Rabin with the semigroup approach used for morphic predicates. The common generalization of the two approaches is captured by the notion of profinite ultimate periodicity infinite words. We introduce these words and we show that morphic words belong to this class. The application to the contraction method is developed in the subsequent section.

DEFINITION 4.1. A sequence $(u_n)_{n \geq 0}$ of words over an alphabet A is said to be *profinutely ultimately periodic* if for any morphism μ from A^+ into a finite semigroup S , the sequence $\mu(u_n)$ is ultimately periodic.

This property is said to be effective iff for any morphism μ from A^+ into a finite semigroup, two integers n and p such that for any $k \geq n$, $\mu(u_k) = \mu(u_{k+p})$ can be effectively computed. An infinite word x is called profinitely ultimately periodic if it can be factorized $x = u_0 u_1 u_2 \dots$, where the sequence $(u_n)_{n \geq 0}$ is effectively profinitely ultimately periodic. The following proposition shows how this property can be used for deciding the problem (Acc_x) . The notion of profinite ultimate periodicity comes from the proof of Theorem 2.1. The core of the following proof is therefore the same as the proof of Theorem 2.1 but we repeat it for the reader's convenience.

PROPOSITION 4.1. *If the infinite word x is profinitely ultimately periodic, the problem (Acc_x) is decidable.*

Proof. Let $\mathcal{A} = (Q, E, I, F)$ be a Büchi automaton. Define the equivalence relation \equiv over A^+ by

$$u \equiv u' \stackrel{\text{def}}{\iff} \forall p, q \in Q \quad \begin{cases} p \xrightarrow{u} q \Leftrightarrow p \xrightarrow{u'} q \\ p \xrightarrow{u}_F q \Leftrightarrow p \xrightarrow{u'}_F q. \end{cases}$$

The relation \equiv is a congruence of finite index. The application which maps any finite word to its class is therefore a morphism from A^+ into the finite semigroup A^+/\equiv .

This congruence has the following main property. Suppose that the two infinite words x and x' can be factored as $x = u_0 u_1 u_2 \dots$ and $x' = u'_0 u'_1 u'_2 \dots$ such that $u_k \equiv u'_k$ for any $k \geq 0$. Then x is accepted by \mathcal{A} iff x' is accepted by \mathcal{A} .

Since the sequence $(u_n)_{n \geq 0}$ is profinitely ultimately periodic, there are two integers n and p such that for any k greater than n , $u_k \equiv u_{k+p}$. Therefore, x is accepted by \mathcal{A} iff the word $v_0 v_1^\omega$ is accepted by \mathcal{A} , where $v_0 = u_0 \dots u_{n-1}$ and $v_1 = u_n \dots u_{n+p-1}$. ■

We illustrate this notion by the following example.

EXAMPLE 4.1. The sequence of words $(a^{n!})_{n \geq 0}$ is profinitely ultimately periodic. This sequence is actually profinitely ultimately constant. It is indeed well known that for any element s of a finite semigroup S and any integer n greater than the cardinality of S , $s^{n!}$ is equal to a fixed element, usually denoted s^ω in the literature [2, p. 72].

The sequences of words which are profinitely ultimately constant have been considerably studied. They are called implicit operations in the literature [2]. A slight variant of the previous example shows that the sequence $(u_n)_{n \geq 0}$ defined by $u_n = 0^{n!-1} 1$ is also profinitely ultimately constant. Since $(n+1)! - n! - 1$ is equal to $nn! - 1$, the word $u_0 u_1 u_2 \dots$ is the characteristic word of the factorial predicate $P = \{n! \mid n \in \mathbb{N}\}$. The monadic theory of $(\mathbb{N}, <, P)$, where P is the factorial predicate, is therefore decidable by the previous proposition.

In the following propositions we connect the profinitely ultimately periodic sequences to the infinite words obtained by iterating morphisms.

PROPOSITION 4.2. *Let τ be a morphism from A^* into itself and let u be a word over A . The sequence $u_n = \tau^n(u)$ is profinitely ultimately periodic, and this property is effective.*

Proof. Let μ be a morphism from A^+ into a finite semigroup S . Since S is finite, there are finitely many morphisms from A^+ into S . Therefore, there are two integers n and p such that $\mu \circ \tau^n = \mu \circ \tau^{n+p}$.

This implies that for any k greater than n , one has $\mu \circ \tau^k = \mu \circ \tau^{k+p}$, and thus $u_k = u_{k+p}$. Note that the two integers n and p can be effectively computed. It suffices to find n and p such that $\mu(\tau^n(a)) = \mu(\tau^{n+p}(a))$ for any letter a in A . ■

It follows from the proposition that a morphic word has a factorization whose factors form a profinitely ultimately periodic sequence. Let x be a morphic word $\sigma(\tau^\omega(a))$ where τ and σ are morphisms and let u be the finite word such that $\tau(a) = au$. The word x can be factored $x = u_0 u_1 u_2 \dots$ where $u_0 = \sigma(au)$ and $u_n = \sigma(\tau^n(u))$ for $n \geq 1$. By the proposition, the sequence $(\tau^n(u))_{n \geq 0}$ is profinitely ultimately periodic. The sequence $(u_n)_{n \geq 0}$ is therefore also profinitely ultimately periodic.

5. THE PREDICATE CLASS \mathcal{K}

The decidability of the decision problem (Acc_x) for an infinite word x involves a “good” factorization of the word x . In the case of morphic words, this factorization is naturally provided by the generation of x via a morphism. Another approach is to consider the canonical factorization of the word x induced by the blocks 0^*1 which form the word x (representing the distances between the successive elements of the predicate). The contraction method as developed by Elgot and Rabin [11] and Siefkes [18] reduces the sequence of these finite words from 0^*1 to an ultimately periodic sequence. In this section we embed this method into the framework developed above.

If $(k_n)_{n \geq 0}$ is a strictly increasing sequence of integers, the characteristic word x_P of the predicate $P = \{k_n \mid n \in \mathbb{N}\}$ can be canonically factorized $x = u_0 u_1 u_2 \dots$ where u_n is the word $0^{k_{n+1}-k_n-1}1$ over the alphabet \mathbb{B} . If this sequence $(u_n)_{n \geq 0}$ of words is profinitely ultimately periodic and if furthermore this property is effective, it is decidable whether the word x_P is accepted by a Büchi automaton and the monadic theory of $(\mathbb{N}, <, P)$ is therefore decidable. We will prove that the class of sequences $(k_n)_{n \geq 0}$ such that this property holds contains interesting sequences like $(n^k)_{n \geq 0}$, $(k^n)_{n \geq 0}$ and $(n!)_{n \geq 0}$ and that it is also closed under several natural operations like sum, product and exponentiation.

The following lemma essentially states that it suffices to consider the sequence $u_n = a^{k_{n+1}-k_n}$ over a one-letter alphabet.

LEMMA 5.1. *Let $(u_n)_{n \geq 0}$ be a sequence of words over A and let a be a letter. The sequence $(u_n)_{n \geq 0}$ is profinitely ultimately periodic iff the sequence $(u_n a)_{n \geq 0}$ is profinitely ultimately periodic. Moreover this property is effective for $(u_n)_{n \geq 0}$ iff it is effective for $(u_n a)_{n \geq 0}$.*

Proof. It is clear that if the sequence $(u_n)_{n \geq 0}$ is profinitely ultimately periodic, then the sequence $(u_n a)_{n \geq 0}$ is also profinitely ultimately periodic. Indeed, for any morphism μ from A^+ into a finite semigroup, the relation $\mu(u_n a) = \mu(u_n)\mu(a)$ implies that if the sequence $\mu(u_n)_{n \geq 0}$ is ultimately periodic, then the sequence $\mu(u_n a)$ is also ultimately periodic.

Conversely let μ be a morphism from A^+ into a finite semigroup S . Let \hat{S} be the semigroup $S^1 \times S$ with the product defined by $(s, t)(s', t') = (sts', t')$ and let $\hat{\mu}$ be the morphism from A^+ into \hat{S} defined by $\hat{\mu}(a) = (1, \mu(a))$. It may be verified easily by induction on the length on the word w that $\hat{\mu}(wa) = (\mu(w), \mu(a))$. Therefore, if the sequence $(u_n a)_{n \geq 0}$ is profinitely ultimately periodic, the sequences $\hat{\mu}(u_n a)$ and $\mu(u_n)$ are ultimately periodic. The sequence $(u_n)_{n \geq 0}$ is then profinitely ultimately periodic. ■

If A is the one-letter alphabet $\{a\}$, the semigroup A^* is isomorphic to the set \mathbb{N} of integers by identifying any word a^n with the integer n . Therefore, a sequence $(k_n)_{n \geq 0}$ of integers is said to be profinitely ultimately periodic iff the sequence a^{k_n} is profinitely ultimately periodic.

DEFINITION 5.1. Let \mathcal{K} be the class of increasing sequences $(k_n)_{n \geq 0}$ of integers such that the sequence $(k_{n+1} - k_n)_{n \geq 0}$ is profinitely ultimately periodic.

By Lemma 5.1 and by Proposition 4.1, we conclude:

THEOREM 5.1. *Let $(k_n)_{n \geq 0}$ be in \mathcal{K} and let x_P be the characteristic word of the predicate $P = \{k_n \mid n \in \mathbb{N}\}$. Then the decision problem (Acc_{x_P}) is decidable and the monadic theory $\text{MTh}(\mathbb{N}, <, P)$ is also decidable.*

We give two comments, the first one on the relation between the class \mathcal{K} and profinitely ultimately periodic sequences, the second one on a similar class of predicates introduced by Siefkes [18].

As stated in Corollary 5.1 below, each sequence in \mathcal{K} is profinitely ultimately periodic. The converse is not true as the following example shows. Let $x = b_0b_1b_2 \dots$ be an infinite word over the alphabet \mathbb{B} , that is $b_i \in \mathbb{B}$. Consider the sequence $(k_n)_{n \geq 0}$ defined by $k_n = (\sum_{i=0}^n b_i)!$. If the word x has infinitely many occurrences of 1, the sequence $(k_n)_{n \geq 0}$ is then profinitely ultimately periodic (cf. Example 4.1). However, if the word x is not ultimately periodic, the sequence $(k_{n+1} - k_n)_{n \geq 0}$ is not profinitely ultimately periodic.

In [18], Siefkes studies predicates generated by sequences $(k_n)_{n \geq 0}$ satisfying two conditions: to be “effectively ultimately reducible” (which corresponds to being effectively profinitely ultimately periodic), and to have an essentially increasing sequence of differences $k_{n+1} - k_n$, i.e., for each $d \geq 0$, we have $k_{n+1} - k_n > d$ for $n > n_d$ (with n_d effectively computable from d). The second assumption ensures that the sequence $(k_{n+1} - k_n)_{n \geq 0}$ is profinitely ultimately periodic in our sense. Although most natural predicates of the class \mathcal{K} can also be treated by Siefkes’ approach, there are some exceptions. For instance, let $(k_n)_{n \geq 0}$ be defined by $k_n = (n/2)!$ if n is even and by $k_n = ((n-1)/2)! + 2$ if n is odd. This sequence $(k_n)_{n \geq 0}$ is in the class \mathcal{K} but Siefkes’ second assumption does not apply.

The following theorem shows that the class \mathcal{K} contains interesting sequences and that it is closed under several natural operations.

THEOREM 5.2. *Any sequence $(k_n)_{n \geq 0}$ such that the sequence $(k_{n+1} - k_n)_{n \geq 0}$ is \mathbb{N} -rational belongs to \mathcal{K} . If the sequences $(k_n)_{n \geq 0}$ and $(\ell_n)_{n \geq 0}$ belong to \mathcal{K} , the following sequences also belong to \mathcal{K} :*

- (sum and product) $k_n + \ell_n$ and $k_n \ell_n$.
- (difference) $k_n - \ell_n$ provided $\lim_{n \rightarrow \infty} ((k_{n+1} - k_n) - (\ell_{n+1} - \ell_n)) = \infty$.
- (exponentiation) k^{ℓ_n} for a fixed integer k and $k_n^{\ell_n}$.
- (generalized sum and product) $\sum_{i=0}^{\ell_n} k_i$ and $\prod_{i=0}^{\ell_n} k_i$.

By Lemma 3.1, the class \mathcal{K} contains any sequence of the form $k^n Q(n)$ where k is a positive integer and Q is a polynomial such that $Q(n)$ is integer for any integer n . By applying the generalized product to the sequences $k_n = \ell_n = n$, the sequence $(n!)_{n \geq 0}$ belongs to \mathcal{K} .

The closure by differences shows that \mathcal{K} contains any rational sequence $(k_n)_{n \geq 0}$ of integers such that $\lim_{n \rightarrow \infty} (k_{n+1} - k_n) = \infty$. Indeed, any rational sequence of integers is the difference of two \mathbb{N} -rational sequences [17, Corollary II.8.2].

The class \mathcal{K} is also closed by other operations. For instance, it can be proved that if both sequences $(k_n)_{n \geq 0}$ and $(\ell_n)_{n \geq 0}$ belong to \mathcal{K} , then the sequence $(K_n)_{n \geq 0}$ defined by $K_n = \sum_{i+j=n} k_i \ell_j$ also belongs to \mathcal{K} .

The class \mathcal{K} is closed under sum, difference, product, and exponentiation but the following example shows that it is not closed under quotient.

EXAMPLE 5.1. Consider the sequence $k_n = \binom{2n}{n} = \frac{2n!}{n!n!}$. This sequence is not profinitely ultimately periodic since the sequence $(k_n \bmod 4)$ is not ultimately periodic. It turns out that $(k_n \bmod p)$ is not ultimately periodic unless $p = 2$ [1]. It can be easily seen that the greatest integer m such that 2^m divides k_n is the number of 1 in the binary expansion n . Therefore, $(k_n \bmod 4)$ is equal to 2 if n is a power of 2 and to 0 otherwise.

For two integers t and p , define the equivalence relation $\equiv_{t,p}$ on \mathbb{N} as follows. For any integers k and k' , one has

$$k \equiv_{t,p} k' \stackrel{\text{def}}{\iff} \begin{cases} k = k' & \text{if } k < t \text{ or } k' < t \\ k = k' \bmod p & \text{otherwise.} \end{cases}$$

The integers t and p are respectively called the *threshold* and the *period* of the relation $\equiv_{t,p}$. Note that the relation $k \equiv_{t,p} k'$ always implies that $k = k' \bmod p$. The equivalence relation $\equiv_{t,p}$ is of finite index and it is compatible with sums and products. Indeed if $k \equiv_{t,p} k'$ and $\ell \equiv_{t,p} \ell'$ hold then both relations $k + \ell \equiv_{t,p} k' + \ell'$ and $k\ell \equiv_{t,p} k'\ell'$ also hold. All relations $\equiv_{t,p}$ for t and p capture the property of being profinitely ultimately periodic for sequences of integers.

LEMMA 5.2. *A sequence $(k_n)_{n \geq 0}$ of integers is profinitely ultimately periodic iff for any integers t and p there are two integers t' and p' such that for any n greater than t' , one has $k_n \equiv_{t,p} k_{n+p'}$.*

Proof. Indeed, this condition is sufficient since for any element s of a finite semigroup, there are two integers t and p such that $s^t = s^{t+p}$. Conversely, this condition is also necessary. The set $\mathbb{N}/\equiv_{t,p}$ equipped with addition is a finite semigroup and the canonical projection from \mathbb{N} to $\mathbb{N}/\equiv_{t,p}$ is a morphism. ■

The following result is almost trivial but it will often be used.

LEMMA 5.3. *Let \equiv_{t_i, p_i} for $1 \leq i \leq \ell$ be ℓ relations associated with fixed integers t_i and p_i and let $(k_{j,n})_{n \geq 0}$ for $1 \leq j \leq m$ be m profinitely ultimately periodic sequences of integers. There are two integers r and q such that $k_{j,n} \equiv_{t_i, p_i} k_{j,n+q}$ for any $1 \leq i \leq \ell$, any $1 \leq j \leq m$ and any n greater than r .*

Proof. Since each sequence $(k_{i,n})_{n \geq 0}$ is profinitely ultimately periodic, there are two integer $r_{i,j}$ and $q_{i,j}$ such that $k_{j,n} \equiv_{t_i, p_i} k_{j,n+q_{i,j}}$ for any n greater than $t_{i,j}$. The two integers r and q defined by $r = \max_{i,j} \{r_{i,j}\}$ and $q = \prod_{i,j} q_{i,j}$ satisfy the required property. ■

The following lemma states that the class of profinitely ultimately periodic sequences of integers is closed under sum and product. These results follow from a more general result (not needed here) which states the class of profinitely ultimately periodic sequences of words are closed under substitution. More precisely, if the sequence $(\tau_n)_{n \geq 0}$ of morphisms from A^* into B^* is such that each sequence $(\tau_n(a))_{n \geq 0}$ is profinitely ultimately periodic and if the sequence $(u_n)_{n \geq 0}$ of words over A is also profinitely ultimately periodic, then the sequence $(\tau_n(u_n))_{n \geq 0}$ is then profinitely ultimately periodic. If each word u_n is for instance equal to the fixed word $u = ab$ and if the morphism τ_n maps a to v_n and b to w_n , the word $\tau_n(u)$ is equal to $v_n w_n$. The class of profinitely ultimately periodic sequences of words are closed under concatenation. If u_n is equal to a^{k_n} and if $\tau_n(a)$ is equal to a^{ℓ_n} , then $\tau_n(u_n)$ is equal to $a^{k_n \ell_n}$. We give here a direct proof of these results which relies on the compatibility of any relation $\equiv_{t,p}$ with sums and products.

LEMMA 5.4. *Let $(k_n)_{n \geq 0}$ and $(\ell_n)_{n \geq 0}$ be two profinitely ultimately periodic sequences of integers. Both sequences $(k_n + \ell_n)_{n \geq 0}$ and $(k_n \ell_n)_{n \geq 0}$ are also profinitely ultimately periodic. If $\lim_{n \rightarrow \infty} (k_n - \ell_n) = \infty$, then the sequence $(k_n - \ell_n)_{n \geq 0}$ is also profinitely ultimately periodic.*

The following example shows that the assumption on the limit of the sequence $k_n - \ell_n$ is really necessary. Let $x = b_0 b_1 b_2 \dots$ be an infinite word over the alphabet \mathbb{B} . Consider the sequences $(k_n)_{n \geq 0}$ and $(\ell_n)_{n \geq 0}$ defined by $k_n = 1 + (1 + b_n)n!$ and $\ell_n = n!$. These two sequences are obviously profinitely ultimately periodic (cf. Example 4.1). However, the difference $k_n - \ell_n$ is equal to $1 + b_n n!$. If the word x is not ultimately periodic, the sequence $(k_n - \ell_n)_{n \geq 0}$ is not profinitely ultimately periodic.

Proof. By Lemma 5.3, there are then r and q such that $k_n \equiv_{t,p} k_{n+q}$ and $\ell_n \equiv_{t,p} \ell_{n+q}$ for any n greater than r . This yields $k_n + \ell_n \equiv_{t,p} k_{n+q} + \ell_{n+q}$ and $k_n \ell_n \equiv_{t,p} k_{n+q} \ell_{n+q}$ for n greater than r . The sequences $(k_n + \ell_n)_{n \geq 0}$ and $(k_n \ell_n)_{n \geq 0}$ are profinitely ultimately periodic.

The relations $k_n \equiv_{t,p} k_{n+q}$ and $\ell_n \equiv_{t,p} \ell_{n+q}$ imply that $k_n = k_{n+q} \pmod p$ and $\ell_n = \ell_{n+q} \pmod p$. This yields $k_n - \ell_n = k_{n+q} - \ell_{n+q} \pmod p$. Since $\lim_{n \rightarrow \infty} (k_n - \ell_n) = \infty$, the difference $k_n - \ell_n$ is greater than t for all n greater than some r' . Then for any n greater than r and r' , one has $k_n - \ell_n \equiv_{t,p} k_{n+q} - \ell_{n+q}$ for n greater than r' and the sequence $(k_n - \ell_n)_{n \geq 0}$ is profinitely ultimately periodic. ■

The following lemma states that the class of profinitely ultimately periodic sequences of integers is closed under generalized sum and product when $\ell_n = n$. It will be used to prove the general case.

LEMMA 5.5. *Let $(k_n)_{n \geq 0}$ be a profinitely ultimately periodic sequence of integers. The sequences $(K_n)_{n \geq 0}$ and $(L_n)_{n \geq 0}$ defined by $K_n = \sum_{i=0}^n k_i$ and $L_n = \prod_{i=0}^n k_i$ are also profinitely ultimately periodic.*

Proof. Let $\equiv_{t,p}$ be the relation associated with two fixed integers t and p . There are then two integers r and q such that $k_n \equiv_{t,p} k_{n+q}$ for any n greater than r . Let k be the sum $\sum_{i=r+1}^{r+q} k_i$. Note that $\sum_{i=r+1}^{r+\ell q} k_i \equiv_{t,p} \ell k$ for any integer ℓ . There are then two integers r' and q' such that $r'k \equiv_{t,p} (r' + q')k$.

We claim that, $K_n \equiv_{t,p} K_{n+qq'}$ holds for any n greater than $r + r'p$. Indeed, one has

$$\begin{aligned}
 K_n &= \sum_{i=0}^r k_i + \sum_{i=r+1}^{r+r'q} k_i + \sum_{i=r+r'q+1}^n k_i \\
 &\equiv_{t,p} \sum_{i=0}^r k_i + r'k + \sum_{i=r+r'q+1}^n k_i \\
 &\equiv_{t,p} \sum_{i=0}^r k_i + (r' + q')k + \sum_{i=r+r'q+1}^n k_{i+qq'} \\
 &\equiv_{t,p} \sum_{i=0}^r k_i + \sum_{i=r+1}^{r+r'q+qq'} k_i + \sum_{i=r+r'q+qq'+1}^{n+qq'} k_i \\
 &\equiv_{t,p} K_{n+qq'}.
 \end{aligned}$$

The proof for L_n is very similar. It suffices to replace each sum with a product. For instance, the constant k is defined by $k = \prod_{i=r+1}^{r+q} k_i$ and the two integers r' and q' are chosen such that $k^{r'} \equiv_{t,p} k^{r'+q'}$. ■

The previous lemma has the following corollary.

COROLLARY 5.1. *Any sequence $(k_n)_{n \geq 0}$ in \mathcal{K} is profinitely ultimately periodic.*

The following lemma is needed to prove that the class \mathcal{K} is closed under generalized sum and product.

LEMMA 5.6. *Let $(k_n)_{n \geq 0}$, $(\ell_n)_{n \geq 0}$ and $(d_n)_{n \geq 0}$ be three profinitely ultimately periodic sequences of integers. Both sequences $(K_n)_{n \geq 0}$ and $(L_n)_{n \geq 0}$ defined by $K_n = \sum_{i=\ell_n}^{\ell_n+d_n} k_i$ and $L_n = \prod_{i=\ell_n}^{\ell_n+d_n} k_i$ are then profinitely ultimately periodic.*

Proof. Let $\equiv_{t,p}$ be the relation associated with two fixed integers t and p . There are then two integers r and q such that $k_n \equiv_{t,p} k_{n+q}$ for any n greater than r . Let k be the sum $\sum_{i=r+1}^{r+q} k_i$. Note that $\sum_{i=n+1}^{n+q} k_i \equiv_{t,p} k$ for any integer n greater than r . There are then two integers r' and q' such that $r'k \equiv_{t,p} (r' + q')k$. By Lemma 5.3, there are also two integers r'' and q'' such that $\ell_n \equiv_{r,q} \ell_{n+q''}$ and $d_n \equiv_{r+r'q,qq'} d_{n+q''}$ for any n greater than r'' . We claim that $K_n \equiv_{t,p} K_{n+q''}$ for any n greater than r'' .

We first claim that $K_{n+q''} \equiv_{t,p} \sum_{i=\ell_n}^{\ell_n+d_{n+q''}} k_i$. If $\ell_n = \ell_{n+q''}$ the result obviously holds. Otherwise, one has $\ell_n \geq r$ and $\ell_{n+q''} \geq r$. Since $\ell_n = \ell_{n+q''} \bmod q$, one has $k_i \equiv_{t,p} k_{i+\ell}$, where $\ell = \ell_{n+q''} - \ell_n$ for any $\ell_n \leq i$. This proves the claim.

We now prove that $\sum_{i=\ell_n}^{\ell_n+d_{n+q''}} k_i \equiv_{t,p} K_n$. If $d_n = d_{n+q''}$, the result holds obviously. Otherwise, one has $d_n \geq r + r'q$ and $d_{n+q''} \geq r + r'q$. By symmetry, we may assume that $d_{n+q''} > d_n$. Since $d_{n+q''} = d_n \bmod qq'$, we may also suppose that $d_{n+q''} = d_n + \ell qq'$ for some integer ℓ . One has then

$$\begin{aligned}
 K_{n+q''} &\equiv_{t,p} \sum_{i=\ell_n}^{\ell_n+d_n+\ell qq'} k_i \equiv_{t,p} \sum_{i=\ell_n}^{\ell_n+d_n-r'q} k_i + (r' + \ell q')k \\
 &\equiv_{t,p} \sum_{i=\ell_n}^{\ell_n+d_n-r'q} k_i + r'k \equiv_{t,p} \sum_{i=\ell_n}^{\ell_n+d_n} k_i.
 \end{aligned}$$

The proof for L_n is similar. It suffices to replace each sum by a product. ■

We finally come to the proof of Theorem 5.2.

Proof. We prove that any sequence $(k_n)_{n \geq 0}$ such that the sequence $(k_{n+1} - k_n)_{n \geq 0}$ is \mathbb{N} -rational belongs to \mathcal{K} . This follows from Theorem 3.1 and from Proposition 4.2 but we also provide a direct proof. If the sequence $(d_n)_{n \geq 0}$ is defined by $d_n = k_{n+1} - k_n$ is \mathbb{N} -rational, there is a matrix representation (L, M, C) such that $d_n = LM^nC$ for any $n \geq 0$. Extend the relation $\equiv_{t,p}$ to matrices by setting

$M \equiv_{t,p} M'$ iff the relation $M_{k,\ell} \equiv_{t,p} M'_{k,\ell}$ holds for any (k, ℓ) -entry of the matrices. There are then two integers r and q such that $M^r \equiv_{t,p} M'^{r+q}$ and this implies $M^n \equiv_{t,p} M'^{n+q}$ for n greater than r . Thus, one has $d_n \equiv_{t,p} d_{n+q}$ for n greater than r .

If both sequences $(k_n)_{n \geq 0}$ and $(\ell_n)_{n \geq 0}$ belong to \mathcal{K} , Lemma 5.4 applied to the sequences $(k_{n+1} - k_n)_{n \geq 0}$ and $(\ell_{n+1} - \ell_n)_{n \geq 0}$ shows that the sequence $(k_n + \ell_n)_{n \geq 0}$ belongs then to \mathcal{K} . If furthermore, the assumption on the limit is fulfilled, it also shows that the sequence $(k_n - \ell_n)_{n \geq 0}$ belongs then to \mathcal{K} .

The difference $k_{n+1}\ell_{n+1} - k_n\ell_n$ is equal to $k_{n+1}(\ell_{n+1} - \ell_n) + (k_{n+1} - k_n)\ell_n$. By Lemma 5.5, the sequences $(k_n)_{n \geq 0}$ and $(\ell_n)_{n \geq 0}$ are profinitely ultimately periodic. By Lemma 5.4, the sequence of differences is then profinitely ultimately periodic and the sequence $(k_n\ell_n)_{n \geq 0}$ belongs then to \mathcal{K} .

The difference $k^{\ell_{n+1}} - k^{\ell_n}$ is equal to $k^{\ell_n}(k^{\ell_{n+1}-\ell_n} - 1)$. By Lemma 5.5, both sequences k^{ℓ_n} and $k^{\ell_{n+1}-\ell_n}$ are profinitely ultimately periodic. By Lemma 5.4, the sequence of differences is then profinitely ultimately periodic and the sequence $(k^{\ell_n})_{n \geq 0}$ belongs then to \mathcal{K} .

Let K_n be the sum $\sum_{i=0}^{\ell_n} k_i$. The difference $K_{n+1} - K_n$ is equal to the sum $\sum_{i=\ell_n+1}^{\ell_{n+1}} k_i$. By Lemma 5.5, the sequence $(\ell_n)_{n \geq 0}$ is profinitely ultimately periodic and by Lemma 5.6, the sequence of differences is then profinitely ultimately periodic.

Let K_n be the product $\prod_{i=0}^{\ell_n} k_i$. The difference $K_{n+1} - K_n$ is equal to

$$\left(\prod_{i=0}^{\ell_n} k_i \right) \left(\prod_{i=\ell_n+1}^{\ell_{n+1}} k_i - 1 \right).$$

By Lemma 5.6, the sequence $(L_n)_{n \geq 0}$ defined by $L_n = \prod_{i=\ell_n+1}^{\ell_{n+1}} k_i$ is profinitely ultimately periodic. By Lemma 5.5 applied to the sequence $(L_n)_{n \geq 0}$, the sequence $(L'_n)_{n \geq 0}$ defined by $L'_n = \prod_{i=0}^{\ell_n} k_i$ is also profinitely ultimately periodic. By Lemma 5.4, the sequence of differences is then profinitely ultimately periodic and the sequence $(K_n)_{n \geq 0}$ belongs then to \mathcal{K} .

Let d_n be the difference $k_{n+1} - k_n$; let d'_n be the difference $k^{\ell_{n+1}} - k^{\ell_n}$. We assume that the sequence $(k_n)_{n \geq 0}$ is strictly increasing and we also assume that $\ell_n \geq 2$ for n greater than some constant which can be effectively computed. We prove that the sequence $(d'_n)_{n \geq 0}$ is profinitely ultimately periodic. Let $\equiv_{t,p}$ be the relation associated with two fixed integers t and p . We first claim that $d'_n \geq t$ for any n greater than t . One has indeed the following inequalities:

$$d'_n \geq k_{n+1}^{\ell_n} - k_n^{\ell_n} \geq k_{n+1}^2 - k_n^2 = (k_{n+1} + k_n)d_n.$$

Since the sequence $(k_n)_{n \geq 0}$ is assumed to be strictly increasing, d_n is non-zero and k_n is greater than t for any n greater than t .

By Lemma 5.3, there are two integers s and m such that $k^n \equiv_{t,p} k^{n+m}$ for any integer k and any integer n greater than s . Note that if $n \geq s$ and if $k \equiv_{t,p} \ell$, then $k^n \equiv_{t,p} \ell^n \equiv_{t,p} \ell^{n+m}$. By Lemma 5.3, there are two integers r and q such that $k_n \equiv_{t,p} k_{n+q}$, $d_n \equiv_{t,p} d_{n+q}$, $\ell_n \equiv_{s,m} \ell_{n+q}$ for any integer n greater than r . We claim that $d'_n \equiv_{t,p} d'_{n+q}$ for any integer n greater than r . Since $d'_n \geq t$ and $d'_{n+q} \geq t$, it suffice to prove that $d'_n = d'_{n+q} \bmod p$. The relations $k_n \equiv_{t,p} k_{n+q}$ and $\ell_n \equiv_{s,m} \ell_{n+q}$ imply $k_n^{\ell_n} \equiv_{t,p} k_{n+q}^{\ell_{n+q}}$. The relation $k_{n+1} \equiv_{t,p} k_{n+q+1}$ and $\ell_{n+1} \equiv_{r,q} \ell_{n+q+1}$ imply $k_{n+1}^{\ell_{n+1}} \equiv_{t,p} k_{n+q+1}^{\ell_{n+q+1}}$. These two relations then imply $d'_n = d'_{n+q} \bmod p$. ■

6. CONCLUSION

We have introduced a large class of unary predicates P over \mathbb{N} such that the corresponding Büchi acceptance problem Acc_{x_P} (and hence the monadic theory $\text{MTh}(\mathbb{N}, <, P)$) is decidable. The class contains all morphic predicates (which solves a problem of Maes [14, 15]). The connection to the work of Elgot and Rabin [11] and Siefkes [18] was established by extending the class of morphic predicates to the class of the profinitely ultimately periodic predicates. Finally, strong closure properties (under sum, product, and exponentiation) were shown for certain profinitely ultimately periodic predicates (where the sequence of differences of successive elements is profinitely ultimately periodic). Altogether we obtain a large collection of concrete examples P such that $\text{MTh}(\mathbb{N}, <, P)$ is decidable, containing for each k the k th powers and the k -powers, the value sets of polynomials over the integers, the factorial

predicate, and the Fibonacci predicate, as well as the predicates derived from morphic words such as the Thue–Morse word and the Fibonacci word.

Let us mention some open problems.

Our results do not cover expansions of $\langle \mathbb{N}, < \rangle$ by tuples (P_1, \dots, P_n) of predicates rather than by single predicates. In his dissertation, Hosch [13] has solved the problem for the special case of the predicates $P_i = \{n^{2^i} \mid n \in \mathbb{N}\}$. We do not know whether $\text{MTh}(\mathbb{N}, <, P_1, \dots, P_n)$ is decidable if the P_i are just known to be profinitely ultimately periodic.

There should be more predicates P for which the Büchi acceptance problem Acc_{x_P} and hence the theory $\text{MTh}(\mathbb{N}, <, P)$ is decidable. A possible next step is to consider Sturmian words, a natural generalization of morphic words (see [7]).

Finally, we should recall the intriguing question already raised by Büchi and Landweber in [9] (“Problem 1”) about existence of “interesting” recursive predicates P such that $\text{MTh}(\mathbb{N}, <, P)$ is undecidable. A particular case is the prime number predicate; its status in this problem is only partially settled [4].

ACKNOWLEDGMENT

The authors would like to thank Jorge Almeida, Jean-Paul Allouche, Jean Berstel, Jacques Désarménien and the anonymous referee for very interesting suggestions and comments.

REFERENCES

- Allouche, J.-P., von Haeseler, F., Peitgen, H.-O., and Skordev, G. (1996), Linear cellular automata, finite automata and Pascal’s triangle, *Discrete Appl. Math.* **66**, 1–22.
- Almeida, J. (1994), “Finite Semigroups and Universal Algebra,” World Scientific, Singapore.
- Bassino, F., Béal, M.-P., and Perrin, D. (2000), “Length Distributions and Regular Sequences,” Technical Report, IGM.
- Bateman, P. T., Jockusch, C. G., and Woods, A. R. (1993), Decidability and undecidability of theories with a predicate for the primes, *J. Symbolic Logic* **58**, 672–687.
- Berstel, J. (1990), Axel Thue’s work on repetitions in words, in “Séries Formelles et Combinatoire Algébrique” (P. Leroux and C. Reutenauer, Eds.), Publications du LaCIM, pp. 65–80, Université du Québec à Montréal.
- Berstel, J., and Reutenauer, C. (1988), “Rational Series and Their Languages,” Springer-Verlag, Berlin.
- Berstel, J., and Séébold, P. (2000), “Algebraic Combinatorics on Words,” Chap. 2, pp. 40–96, Cambridge Univ. Press, Cambridge, UK.
- Büchi, J. R. (1962), On a decision method in the restricted second-order arithmetic, in “Proc. Int. Congress Logic, Methodology and Philosophy of science, Berkeley 1960,” pp. 1–14, Stanford Univ. Press, Stanford, CA.
- Büchi, J. R., and Landweber, L. H. (1966), Definability in the monadic second-order theory of successor, *J. Symbolic Logic* **31**, 169–181.
- Carton, O., and Thomas, W. (2000), The monadic theory of morphic infinite words and generalizations, in “MFCS’2000” (M. Nielsen and B. Rovan, Eds.), Lecture Notes in Computer Science, Vol. 1893, pp. 275–284, Springer-Verlag, Berlin/New York.
- Elgot, C. C., and Rabin, M. O. (1996), Decidability and undecidability of extensions of second (first) order theory of (generalized) successor, *J. Symbolic Logic* **31**(2), 169–181.
- Graham, R. L., Knuth, D. E., and Patashnik, O. (1994), “Concrete Mathematics,” Addison–Wesley, Reading, MA.
- Hosch, F. A. (1971), “Decision Problems in Büchi’s Sequential Calculus,” Dissertation, University of New Orleans, LA.
- Maes, A. (1998), Decidability of the First-Order Theory of $\langle \mathbb{N}, <, P \rangle$ for Morphic Predicates P , Technical Report 9806, University of Kiel.
- Maes, A. (1999), An automata theoretic decidability proof for the first-order theory of $\langle \mathbb{N}, <, P \rangle$ with morphic predicate P , *J. Autom. Lang. Comb.* **4**, 229–245.
- Michaux, C., and Villemaire, R. (1996), Open questions around Büchi and Presburger arithmetics, in “Logic: From Foundations to Applications, European Logic Colloquium, Oxford, 1996” (W. Hodges *et al.*, Eds.), pp. 353–383, Clarendon, Oxford.
- Salomaa, A., and Soittola, M. (1978), “Automata-Theoretic Aspects of Formal Power Series,” Springer-Verlag, New York.
- Siefkes, D. (1970), Decidable extensions of monadic second order successor arithmetic, in “Automatentheorie und Formale Sprachen, Mannheim, 1970” (J. Doerr and G. Hotz, Eds.), pp. 441–472, B.I. Hochschultaschenbücher, Mannheim.
- Thomas, W. (1978), The theory of successor with an extra predicate, *Math. Ann.* **237**, 121–132.
- Thomas, W. (1980), On the bounded monadic theory of well-ordered structures, *J. Symbolic Logic* **45**, 334–338.
- Thomas, W. (1990), Automata on infinite objects, in “Handbook of Theoretical Computer Science” (J. van Leeuwen, Ed.), Vol. B, Chap. 4, pp. 133–191, Elsevier.
- Thomas, W. (1997), Ehrenfeucht games, the composition method, and the monadic theory of ordinal words, in “Structures in Logic and Computer Science, A Selection of Essays in Honor of A. Ehrenfeucht” (J. Mycielski *et al.*, Eds.), Lecture Notes in Computer Science, pp. 118–143, Springer-Verlag, Berlin.