Recognizability of morphisms

MARIE-PIERRE BÉAL ⓘ†, DOMINIQUE PERRIN† and ANTONIO RESTIVO‡

† *Université Gustave Eiffel, CNRS, LIGM, F-77454 Marne-la-Vallée, France*
(e-mail: marie-pierre.beal@univ-eiffel.fr, dominique.perrin@esiee.fr)
‡ *Dipartimento di Matematica e Informatica, Università di Palermo, Italy*
(e-mail: antonio.restivo@unipa.it)

Abstract. We investigate several questions related to the notion of recognizable morphism. The main result is a new proof of Mossé's theorem and actually of a generalization to a more general class of morphisms due to Berthé *et al* [Recognizability for sequences of morphisms. *Ergod. Th. & Dynam. Sys.* **39**(11) (2019), 2896–2931]. We actually prove the result of Berthé *et al* for the most general class of morphisms, including ones with erasable letters. Our result is derived from a result concerning elementary morphisms for which we also provide a new proof. We also prove some new results which allow us to formulate the property of recognizability in terms of finite automata. We use this characterization to show that for an injective morphism, the property of being recognizable on the full shift for aperiodic points is decidable.

1. *Introduction*

In this paper, we study problems related to the recognizability of morphisms (also called substitutions). This notion concerns the unambiguity in the representation of an infinite sequence y as the image $\sigma(x)$ by a morphism σ of another sequence x, up to some normalized shift, called a centered σ-representation. It belongs to a general notion of unambiguity in symbolic dynamics (see [3]).

By Mossé's theorem [18, 19], every aperiodic primitive morphism σ is recognizable on the shift $X(\sigma)$ (see the precise definitions in §3). This surprising result was initially formulated (in an incorrect way) by [17] (see [13] on the genesis of the theorem and its possible variants). It was further generalized by Bezuglyi, Kwiatkowski, and Medynets [7], who proved that every aperiodic non-erasing morphism σ is recognizable on $X(\sigma)$. Next, it was proved by Berthé *et al* [6] that every non-erasing morphism σ is recognizable on $X(\sigma)$ for aperiodic points.

The main result of this paper is a generalization of Mossé's theorem.

THEOREM 1. *Every morphism σ is recognizable on $X(\sigma)$ for aperiodic points.*

This means that every aperiodic point in $X(\sigma)$ has a unique centered σ-representation as a shift of the image by σ of some $x \in X(\sigma)$.

We actually prove the result of [6] concerning the recognizability for aperiodic points for the most general class of morphisms, including ones containing erasable letters. Our proof does not use the fact that the shift $X(\sigma)$ defined for an aperiodic non-erasing morphism has a finite number of minimal subshifts (proved and used in [7]), or the stronger fact that the set of languages of points in a shift $X(\sigma)$ defined by a non-erasing morphism is finite (proved and used in [6]). Our proof relies on the notion of elementary morphism, due to Ehrenfeucht and Rozenberg [10]. By a result, proved independently by Karhumäki, Maňuch, and Plandowski [11] and by Berthé *et al* [6], every elementary morphism is recognizable for aperiodic points. We use this result to prove Mossé's theorem (and its generalizations). This represents actually also a substantial simplification of the proof, since the available proofs of Mossé's theorem are all more difficult, including the proof in [12] which is essentially reproduced in [9], using improvements from [13].

We also give a characterization of injective morphisms recognizable on the full shift in terms of groups in finite monoids (Theorem 6.7). This translation of the property of recognizability in terms of finite monoids is a new approach which puts in evidence for the strong link between recognizability and automata theory.

Finally, we give a quadratic-time algorithm to check whether an injective morphism is recognizable on the full shift for aperiodic points (Corollary 7.3).

Note that the notion of recognizability can also be defined for substitutions in dimension 2 or higher. This was first considered in [20] where the recognizability property is used to prove that a two-dimensional (2D) substitution shift is sofic. The property was also used in [1] to simulate an effective subshift by a sofic and also in [2]. A generalization of Mossé's theorem to the 2D case was proved in [28]. Let us also mention that the recognizability of morphisms has been extended to sequences of morphisms in [6] (see also [8]).

The paper is organized as follows. After an introductory section on the basic notions of symbolic dynamics, we formulate the precise definition of a morphism recognizable on a shift space and prove some elementary properties of recognizable morphisms. In §4, we introduce elementary morphisms and prove that every elementary morphism is recognizable for aperiodic points (Theorem 4.5). In §5, we give the new proof of Mossé's theorem and its extensions. In §6, we formulate a condition characterizing recognizable injective morphisms in terms of groups in finite monoids (Theorem 6.7). In §7, we show that all notions handled in this paper are decidable and, notably, by algorithms of low polynomial complexity.

2. *Symbolic dynamics*

We briefly recall the definitions of symbolic dynamics. For a more complete presentation, see [14] or the recent [9].

2.1. *Words.*   Let A be a finite alphabet. We denote by A^* the free monoid on A and by A^+ the set of non-empty words on A. The empty word is denoted by ε. We denote by $|u|$ the *length* of the word u.

For a word $w \in A^*$ and $a \in A$, we denote by $|w|_a$ the number of occurrences of a in w.

A word $s \in A^*$ is a *factor* of $w \in A^*$ if $w = rst$. The word r is called a *prefix* of w. It is *proper* if $r \neq w$ (that is, if st is not empty).

For $U \subset A^*$, we denote by U^* the submonoid of A^* generated by U. For $U = \{u\}$, we write u^* instead of $\{u\}^*$.

A set $U \subset A^*$ is a *code* if every $w \in U^*$ has a unique decomposition in words of U. A *prefix code* is a set $U \subset A^*$ such that no element of U is a prefix of another one.

Two words u, v are *conjugate* if $u = rs$ and $v = sr$ for some words r, s.

A word is *primitive* if it is not a power of a shorter word.

An integer $p \geq 1$ is a *period* of a word $w = a_0 a_1 \ldots a_{n-1}$ with $a_i \in A$ if $a_i = a_{i+p}$ for $0 \leq i \leq n - p - 1$.

2.2. *Shift spaces.* We consider the set $A^{\mathbb{Z}}$ of two-sided infinite sequences on A. For $x = (x_n)_{n \in \mathbb{Z}}$, and $i \leq j$, we denote by $x_{[i,j]}$ the word $x_i x_{i+1} \ldots x_j$ and $x_{[i,j)}$ the word $x_i x_{i+1} \ldots x_{j-1}$.

The set $A^{\mathbb{Z}}$ is a compact metric space for the distance defined for $x \neq y$ by $d(x, y) = 2^{-r(x,y)}$ with

$$r(x, y) = \min\{|n| \mid n \in \mathbb{Z}, x_n \neq y_n\}.$$

The *shift transformation* $S : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is defined by $y = S(x)$ if $y_n = x_{n+1}$ for every $n \in \mathbb{Z}$. We sometimes denote Sx instead of $S(x)$.

A *shift space* X on a finite alphabet A is a closed and shift invariant subset of $A^{\mathbb{Z}}$.

A *topological dynamical system* is a pair (X, S) of a compact metric space and a continuous map from X to itself. For every shift space X, since S is continuous and X is compact, the pair (X, S) is a topological dynamical system.

The *orbit* of a sequence $x \in A^{\mathbb{Z}}$ is the set $\{S^n(x) \mid n \in \mathbb{Z}\}$.

A point $x \in A^{\mathbb{Z}}$ is *periodic* if there is an $n \geq 1$ such that $S^n(x) = x$. Otherwise, it is *aperiodic*. A periodic point has the form $w^{\infty} = \ldots ww \cdot ww \ldots$ (the letter of index 0 of w^{∞} is the first letter of w). For $x \in A^{\mathbb{Z}}$, we denote $x^+ = x_0 x_1 \ldots$, which is an element of $A^{\mathbb{N}}$, and $x^- = \ldots x_{-2} x_{-1}$, which is the element y of $A^{-\mathbb{N}}$ defined by $y_{-n} = x_{-n-1}$ for $n \in \mathbb{N}$. For $x \in A^{-\mathbb{N}}$ and $y \in A^{\mathbb{N}}$, we denote by $z = x \cdot y$ the two-sided infinite sequence z such that $z^- = x$ and $z^+ = y$.

A word w is a factor of $x \in A^{\mathbb{Z}}$ if $w = x_i x_{i+1} \ldots x_{j-1}$ for some $i, j \in \mathbb{Z}$ with $i \leq j$.

The *language* of a shift space X, denoted $\mathcal{L}(X)$, is the set of factors of the elements of X. For $x \in A^{\mathbb{Z}}$, we also denote by $\mathcal{L}(x)$ the set of factors of x. Thus, $\mathcal{L}(X) = \bigcup_{x \in X} \mathcal{L}(x)$.

2.3. *Morphisms.* A morphism $\sigma : A^* \to B^*$ is a monoid morphism from A^* to B^*. It is *non-erasing* if $\sigma(a)$ is non-empty for every $a \in A$.

The *incidence matrix* of a morphism $\sigma : A^* \to B^*$ is the $(A \times B)$-matrix $M(\sigma)$ whose row of index a is the vector $(|\sigma(a)|_b)_{b \in B}$.

For example, if $\sigma : a \mapsto ab, b \mapsto ac, c \mapsto a$, we have

$$M(\sigma) = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

A morphism σ defines a map from $A^{\mathbb{N}}$ to $B^* \cup B^{\mathbb{N}}$ defined by $\sigma(x_0 x_1 \ldots) = \sigma(x_0)\sigma(x_1)\ldots$, from $A^{-\mathbb{N}}$ to $B^* \cup B^{-\mathbb{N}}$ defined by $\sigma(\ldots x_{-1} x_0) = \ldots \sigma(x_{-1})\sigma(x_0)$, and also a map from $A^{\mathbb{Z}}$ to $B^* \cup B^{\mathbb{N}} \cup B^{-\mathbb{N}} \cup B^{\mathbb{Z}}$ defined by $\sigma(x) = \sigma(x^-) \cdot \sigma(x^+)$.

Let $\sigma : A^* \to B^*$ be a morphism whose restriction to A is injective. The set $U = \sigma(A)$ is a code if and only if σ is injective on A^*. Note that σ can be injective on A^* without being injective on $A^{\mathbb{Z}}$ (the converse being obviously true). It is injective on $A^{\mathbb{Z}}$ if and only if it is injective on $A^{\mathbb{N}}$ and on $A^{-\mathbb{N}}$.

Example 2.1. The Fibonacci morphism $a \mapsto ab, b \mapsto a$ is injective on $A^{\mathbb{N}}$, as one may easily verify. The morphism $\sigma : a \mapsto a, b \mapsto ab, c \mapsto bb$ is not injective on $A^{\mathbb{N}}$ since $\sigma(ac^{\omega}) = \sigma(bc^{\omega})$.

Let $\sigma : A^* \to A^*$ be a morphism from A^* to itself. The *language* of σ, denoted $\mathcal{L}(\sigma)$, is the set of factors of the words $\sigma^n(a)$ for some $n \geq 0$ and $a \in A$. The *shift* defined by σ, denoted by $X(\sigma)$, is the set of sequences with all their factors in $\mathcal{L}(\sigma)$.

One has $\mathcal{L}(X(\sigma)) \subset \mathcal{L}(\sigma)$ but it is not true in general that $\mathcal{L}(X(\sigma)) = \mathcal{L}(\sigma)$. Indeed, the words of $\mathcal{L}(X(\sigma))$ can always be extended (we have $awb \in \mathcal{L}(X(\sigma))$ for some $a, b \in A$) while this needs not be true of the words of $\mathcal{L}(\sigma)$. Note that if $w \in \mathcal{L}(X(\sigma))$, then w is a factor of some $\sigma^n(a)$ for all large enough n.

An *erasable* letter of a morphism $\sigma : A^* \to A^*$ is a letter a in A such that $\sigma^n(a) = \varepsilon$ for some integer n. A word is *erasable* if it is formed of erasable letters.

If w is an erasable word, then $\sigma^{\mathrm{Card}(A)}(w) = \varepsilon$. Indeed, set $A_i = \{a \in A \mid \sigma^i(a) = \varepsilon\}$. Then $A_1 \subset A_2 \subset \cdots \subset A$ and thus there is $k \leq \mathrm{Card}(A)$ such that $A_k = A_{k+1}$, which implies $A_{k+j} = A_k$ for all $j \geq 0$.

PROPOSITION 2.2. *Let $\sigma : A^* \to A^*$ be a morphism. The set of erasable words in $\mathcal{L}(\sigma)$ is finite.*

We first prove the following well-known lemma (see, for example, [25, Lemma 5.5]).

LEMMA 2.3. *For every word $u \in \mathcal{L}(\sigma)$, there is some $m \geq 0$ and words $v_i, w_i \in \mathcal{L}(X)$ for $0 \leq i \leq m$, such that*

$$u = v_0 \sigma(v_1) \ldots \sigma^{m-1}(v_{m-1})\sigma^m(v_m)\sigma^{m-1}(w_{m-1}) \ldots \sigma(w_1)w_0, \qquad (2.1)$$

with $|v_i|, |w_i| \leq |\sigma|$.

Proof. We may assume that $|\sigma| \geq 1$ (otherwise $\mathcal{L}(\sigma) = A$ and the result is true). We use induction on the integer

$$n(u) = \min\{n \geq 0 \mid u \text{ is a factor of } \sigma^n(a) \text{ for some } a \in A\}.$$

The result is true if $n(u) \leq 1$, choosing $m = 0$ and $v_0 = u$. Otherwise, by definition of $\mathcal{L}(\sigma)$, there exists a word $u' \in \mathcal{L}(\sigma)$ such that $u = v_0 \sigma(u')w_0$. Choosing $u' \in \mathcal{L}(\sigma)$ of maximal length, we have moreover $|v_0|, |w_0| \leq |\sigma|$. By induction hypothesis, we have a decomposition of equation (2.1) for u', that is,

$$u' = v_0' \sigma(v_1') \ldots \sigma^{m-1}(v_{m-1}')\sigma^m(v_m')\sigma^{m-1}(w_{m-1}') \ldots \sigma(w_1')w_0'.$$

In this way, we obtain

$$u = v_0\sigma(u')w_0 = v_0\sigma(v'_0)\ldots\sigma^m(v'_{m-1})\sigma^{m+1}(v'_m)\sigma^m(w'_{m-1})\ldots\sigma(w'_0)w_0,$$

which is of the form of equation (2.1). □

Proof of Proposition 2.2. Let $u \in \mathcal{L}(\sigma)$ be erasable. Let $m \geq 0$, v_i, w_i with $|v_i|, |w_i| \leq |\sigma|$ be such that equation (2.1) holds. Since u is erasable, all v_i, w_i are erasable. Since $\sigma^{\mathrm{Card}(A)}(w) = \varepsilon$ for every erasable word w, we can assume that $m \leq \mathrm{Card}(A) - 1$. This implies that the length of u is bounded. □

Note that the maximal length of erasable words in $\mathcal{L}(\sigma)$ is, according to the proof above, bounded by $2|\sigma| \sum_{i=0}^{k-1} |\sigma|^i = 2|\sigma|(|\sigma|^k - 1)/(|\sigma| - 1)$, where $k = \mathrm{Card}(A)$.

COROLLARY 2.4. *Let* $\sigma : A^* \to A^*$ *be a morphism. For every x in $X(\sigma)$, the sequence $\sigma(x)$ is in $X(\sigma)$. The map $x \mapsto \sigma(x)$ is continuous on $X(\sigma)$.*

Proof. We have to prove that $\sigma(x)$ is two-sided infinite. By Proposition 2.2, x has an infinite number of non-erasable letters on the left and on the right, and thus $\sigma(x)$ is two-sided infinite. Since σ is continuous at every point x such that $\sigma(x)$ is infinite, it is continuous on $X(\sigma)$. □

Note that since $X = X(\sigma)$ is compact, and since σ is continuous on X by Corollary 2.4, the pair (X, σ) is a topological dynamical system. Thus, it is both a dynamical system (X, S) with respect to the shift transformation and a dynamical system (X, σ).

As another corollary of Proposition 2.2, we have the following characterization of the morphisms such that $\mathcal{L}(X(\sigma)) = \mathcal{L}(\sigma)$.

PROPOSITION 2.5. *Let* $\sigma : A^* \to A^*$ *be a morphism. One has $\mathcal{L}(\sigma) = \mathcal{L}(X(\sigma))$ if and only if every letter $a \in A$ is in $\mathcal{L}(X(\sigma))$.*

Proof. Assume that the condition is satisfied. Every $w \in \mathcal{L}(\sigma)$ is a factor of some $\sigma^n(a)$ for $a \in A$ and $n \geq 0$. Let $x \in X(\sigma)$ be such that $a \in \mathcal{L}(x)$. By Corollary 2.4, we have $\sigma^n(x) \in X(\sigma)$. Since $w \in \mathcal{L}(\sigma^n(x))$, we obtain $w \in \mathcal{L}(X(\sigma))$. The converse is obvious. □

Example 2.6. The morphism $\sigma : a \mapsto ab, b \mapsto abab$ is periodic. The closure of $\sigma(A^{\mathbb{Z}})$ is $(ab)^\infty \cup (ba)^\infty$.

A word $w \in A^*$ is *growing* for σ if the sequence $(|\sigma^n(w)|)_n$ is unbounded. A word is growing if some of its letters are growing. The morphism σ itself is said to be *growing* if all letters are growing.

Actually, we have the following property of growing letters.

PROPOSITION 2.7. *If $a \in A$ is growing for σ, then $\sigma^{r\,\mathrm{Card}(A)}(a)$ contains, for every $r \geq 0$, at least $r + 1$ non-erasable letters. In particular, $\lim_{n\to\infty} |\sigma^n(a)| = \infty$.*

Proof. Set $k = \mathrm{Card}(A)$. Assume first that $\sigma^k(a)$ contains only one non-erasable letter. Then, this letter has to be growing. Next, by the pigeonhole principle, there are i, p with

$i + p \leq k$ and $p \geq 1$ such that $\sigma^i(a) = ubv$ and $\sigma^p(b) = rbs$ with u, v, r, s erasable and b a growing letter. However, then, since $\sigma^{\mathrm{Card}(A)}(r) = \sigma^{\mathrm{Card}(A)}(s) = \varepsilon$, the word

$$w = \sigma^{p\,\mathrm{Card}(A))}(b) = \sigma^{p(\mathrm{Card}(A)-1)}(r) \ldots \sigma^p(r) rbs \sigma^p(s) \ldots \sigma^{p(\mathrm{Card}(A)-1)}(s)$$

is a finite fixed point of σ^p, that is, such that $\sigma^p(w) = w$, a contradiction with the fact that b is growing. This proves the statement for $r = 1$.

Next, assume that $\sigma^{rk}(a)$ contains $s \geq r + 1$ non-erasable letters $a_1, \ldots, a_s$. One of them, say a_i, has to be growing. Then each of the $\sigma(a_1), \ldots, \sigma(a_s)$ contains a non-erasing letter and $\sigma^k(a_i)$ contains at least two by the property for $r = 1$. Thus, $\sigma^{(r+1)k}(a)$ contains at least $r + 2$ non-erasing letters. □

3. Recognizable morphisms

Let $\sigma : A^* \to B^*$ be a morphism. A σ-*representation* of $y \in B^{\mathbb{Z}}$ is a pair (x, k) of a sequence $x \in A^{\mathbb{Z}}$ and an integer k such that

$$y = S^k(\sigma(x)), \tag{3.1}$$

where S denotes the shift transformation. The σ-representation (x, k) is *centered* if $0 \leq k < |\sigma(x_0)|$.

Note that, in particular, a centered σ-representation (x, k) is such that $\sigma(x_0) \neq \varepsilon$.

Note that if y has a σ-representation (x, k), it has a centered σ-representation (x', k') with x' a shift of x. Indeed, assume $k \geq 0$ (the case $k < 0$ is symmetric). Let $i \geq 0$ be such that $|\sigma(x_0 \ldots x_{i-1})| \leq k < |\sigma(x_0 \ldots x_i)|$. Set $k' = k - |\sigma(x_0 \ldots x_{i-1})|$ and $x' = S^i x$. Then, $S^{k'}\sigma(x') = S^{k'+|\sigma(x_0 \ldots x_{i-1})|}\sigma(x) = S^k \sigma(x) = y$ and $0 \leq k' < |\sigma(x'_0)|$. Thus, (x', k') is a centered σ-representation of y.

For a shift space X on A, the set of points in $B^{\mathbb{Z}}$ having a σ-representation (x, k) with $x \in X$ is a shift space on B which is the closure under the shift of $\sigma(X)$. Indeed, if (x, k) is the σ-representation of y, then $S(y)$ has the σ-representation (x', k') with

$$(x', k') = \begin{cases} (x, k+1) & \text{if } k + 1 < |\sigma(x_0)|, \\ (S(x), 0) & \text{otherwise.} \end{cases}$$

Definition 3.1. Let X be a shift space on A. A morphism $\sigma : A^* \to B^*$ is *recognizable on* X (respectively recognizable on X for aperiodic points) if for every point $y \in B^{\mathbb{Z}}$ (respectively every aperiodic point $y \in B^{\mathbb{Z}}$), there is at most one centered σ-representation (x, k) of y with $x \in X$.

For $X = A^{\mathbb{Z}}$, we simply say recognizable instead of recognizable on X. Note that, as an equivalent definition of recognizability on X (respectively recognizability for aperiodic points), for every $y, y' \in A^{\mathbb{Z}}$ and $0 \leq k < ||\sigma(y'_0)| - |\sigma(y_0)||$ such that $\sigma(y) = S^k(\sigma(y'))$ is in X (respectively is an aperiodic point in X), one has $k = k'$ and $y = y'$.

A morphism $\sigma : A^* \to B^*$ is *circular* if it is injective and if for every $u, v \in B^*$,

$$uv, vu \in \sigma(A^*) \Rightarrow u, v \in \sigma(A^*).$$

Note that a circular morphism is non-erasing, since otherwise it would not be injective.

The following property, originally from [26], is well known. We will not use it but we state it for the sake of clarity.
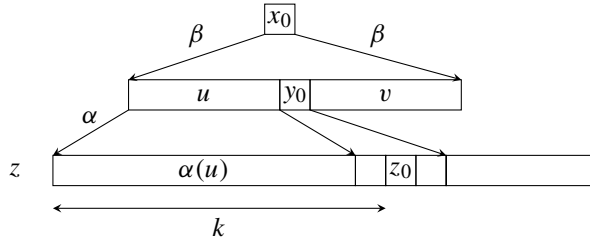
FIGURE 1. The composition $\sigma = \alpha \circ \beta$.

PROPOSITION 3.2. *A morphism is recognizable if and only if it is circular.*

Example 3.3. The Fibonacci morphism $\sigma : a \mapsto ab, b \mapsto a$ is circular and thus recognizable.

Example 3.4. The Thue–Morse morphism $\sigma : a \mapsto ab, b \mapsto ba$ is not circular. It is not recognizable since $(ab)^\infty$ can be obtained as $\sigma(a^\infty)$ and as $S(\sigma(b^\infty))$. However, it is recognizable for aperiodic points since any sequence containing aa or bb has at most one factorization in $\{ab, ba\}$.

Example 3.5. The morphism $\sigma : a \to aa, b \mapsto ab, c \mapsto ba$ is not recognizable for aperiodic points. Indeed, every sequence without occurrence of bb has two factorizations in words of $\{aa, ab, ba\}$.

PROPOSITION 3.6. *The family of morphisms recognizable for aperiodic points is closed under composition.*

Proof. Let $\sigma = \alpha \circ \beta$ with $\beta : A^* \to B^*$ and $\alpha : B^* \to C^*$. Assume that α, β are recognizable for aperiodic points. Let $z \in C^{\mathbb{Z}}$ be an aperiodic point. Let (x, k) be a centered σ-representation of z. Since $0 \le k < |\sigma(x_0)|$, there is a decomposition $\beta(x_0) = ubv$ with $u, v \in B^*$ and $b \in B$ such that $|\alpha(u)| \le k < |\alpha(ub)|$. Set $\ell = |u|$, $m = |\alpha(u)|$, and $y = S^\ell(\beta(x))$. Then, $y_0 = b$ and $z = S^{k-m}(\alpha(y))$ (see Figure 1). Thus, $(y, k - m)$ is a centered α-representation of z and (x, ℓ) is a β-representation of y. Conversely, if (y, n) is an α-representation of z and (x, ℓ) is a centered β-representation of y, then (x, k) with $k = |\beta(y_{-\ell} \ldots y_{-1})| + n$ is a centered σ-representation of z. This shows the uniqueness of (x, k). □

4. *Elementary morphisms*

Definition 4.1. A morphism $\sigma : A^* \to C^*$ is *elementary* (or *indecomposable*) if for every alphabet B and every pair of morphisms $\alpha : B^* \to C^*$ and $\beta : A^* \to B^*$ such that $\sigma = \alpha \circ \beta$, one has $\mathrm{Card}(B) \ge \mathrm{Card}(A)$.

If $\sigma : A^* \to C^*$ is elementary, one has in particular $\mathrm{Card}(C) \ge \mathrm{Card}(A)$ and moreover σ is non-erasing.

Example 4.2. The Thue–Morse morphism $\sigma : a \mapsto ab, b \mapsto ba$ is elementary. Indeed, if $\sigma = \alpha \circ \beta$ with $\beta : \{a, b\}^* \to c^*$, then $ab = \alpha(c^i)$ and $ba = \alpha(c^j)$, which is impossible.

The notion of elementary morphism appears for the first time in [**10**]. A sufficient condition for a morphism to be elementary can be formulated in terms of its incidence matrix.

PROPOSITION 4.3. *If the rank of $M(\sigma)$ is equal to* Card(A)*, then σ is elementary.*

Proof. Indeed, if $\sigma = \alpha \circ \beta$ with $\beta : A^* \to B^*$ and $\alpha : B^* \to C^*$, then

$$M(\sigma) = M(\beta)M(\alpha).$$

If rank$(M(\sigma)) =$ Card(A), then Card$(A) =$ rank$(M(\sigma)) \leq$ rank$(M(\alpha)) \leq$ Card(B). Thus, σ is elementary. $\qquad\square$

This condition is not necessary. For example, the Thue–Morse morphism $\sigma : a \mapsto ab, b \mapsto ba$ is elementary but its incidence matrix

$$M(\sigma) = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

has rank one.

If $\sigma : A^* \to C^*$ is a morphism, we define $\ell(\sigma) = \sum_{a \in A}(|\sigma(a)| - 1)$. We say that a decomposition $\sigma = \alpha \circ \beta$ with $\alpha : B^* \to C^*$ and $\beta : A^* \to B^*$ is *trim* if:

(i) α is non-erasing;

(ii)   for each $b \in B$, there is an $a \in A$ such that $\beta(a)$ contains b.

PROPOSITION 4.4. *Let $\sigma = \alpha \circ \beta$ with $\alpha : B^* \to C^*$ and $\beta : A^* \to B^*$ be a trim decomposition of σ. Then,*

$$\ell(\alpha \circ \beta) \geq \ell(\alpha) + \ell(\beta). \tag{4.1}$$

Proof. Set $\sigma = \alpha \circ \beta$. We have

$$\ell(\sigma) - \ell(\beta) = \sum_{a \in A}(|\sigma(a)| - |\beta(a)|) = \sum_{a \in A}\sum_{b \in B}(|\alpha(b)||\beta(a)|_b - |\beta(a)|_b)$$

$$= \sum_{a \in A}\sum_{b \in B}(|\alpha(b)| - 1)|\beta(a)|_b = \sum_{b \in B}\left((|\alpha(b)| - 1)\sum_{a \in A}|\beta(a)|_b\right).$$

Since α is non-erasing, every factor $|\alpha(b)| - 1$ is non-negative. Since every b appears in some $\beta(a)$, every factor $\sum_{a \in A}|\beta(a)|_b$ is positive, whence the conclusion. $\qquad\square$

The following result is from [**11**]. It also appears in [**6**] with the stronger hypothesis that $\sigma : A^* \to B^*$ is such that $M(\sigma)$ has rank Card(A).

THEOREM 4.5. *An elementary morphism is recognizable for aperiodic points.*

We first prove Theorem 4.5 in a particular case. A morphism $\sigma : A^* \to B^*$ with no erasable letter is *left marked* if every word $\sigma(a)$ for $a \in A$ begins with a distinct letter. Symmetrically, it is *right marked* if every word $\sigma(a)$ for $a \in A$ ends with a distinct letter. In particular, if σ is left marked, σ is injective on A and $\sigma(A)$ is a prefix code. It is clear that a marked morphism is elementary.

The following statement, which is a particular case of Theorem 4.5, appears in [**6**, Lemma 3.3]. We give an independent proof.
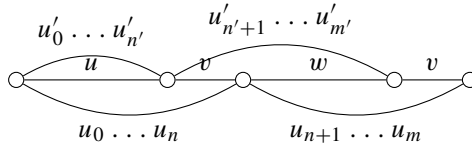
FIGURE 2. The words u, v, w.

PROPOSITION 4.6. *If $\sigma : A^* \to B^*$ is left marked, then it is recognizable for aperiodic points.*

We fist show the following elementary lemma.

LEMMA 4.7. *Let $\sigma : A^* \to B^*$ be an injective morphism and let $U = \sigma(A)$. If σ is not injective on $A^{\mathbb{N}}$, there exist words u, v, w such that*

$$u, uv, vw, wv \in U^* \quad and \quad v \notin U^*. \tag{4.2}$$

Proof. By the hypothesis, there exist $u_0, u_1, \ldots$ and $u'_0, u'_1, \ldots$ with $u_i, u'_i \in U$ such that $u_0 u_1 \ldots = u'_0 u'_1 \ldots$. We may assume that $u_0 \neq u'_0$. For every $n \geq 0$, there is v_n and $n' \geq 0$ such that $u_0 \ldots u_n = u'_0 \ldots u'_{n'} v_n$. Since σ is injective, we have $v_n \notin U^*$. We may moreover assume that v_n is a prefix of $u'_{n'+1}$. Let $n < m$ be such that $v_n = v_m$. Set $u'_{n'+1} \ldots u'_{m'} = v_n w$ (see Figure 2). Then $u = u'_0 \ldots u'_{n'}$, $v = v_n = v_m$, and w satisfy equation (4.2). $\square$

Proof of Proposition 4.6. Set $U = \sigma(A)$. Since U is a prefix code, σ is injective on $A^{\mathbb{N}}$. If it is not injective on $A^{-\mathbb{N}}$, by the symmetric version of Lemma 4.7, there are words u, v, w such that $u, vu, vw, wv \in U^*$ but $v \notin U^*$. We may assume that u, v, w are chosen of minimal length. Since σ is left marked, either u is a prefix of w or w is a prefix of u. In the first case, set $w = uw'$. Then, since U is prefix, $u, wv = uw'v \in U^*$ imply $w'v \in U^*$. However, then $(vu)(w'v)(u) = (vuw')(vu)$, which is a contradiction. Finally, if $u = wu'$, then $vw, vu = vwu' \in U^*$ imply $u' \in U^*$, and we may replace u, v, w by u', w, v, which is a contradiction again. Thus, σ is injective on $A^{-\mathbb{N}}$.

Assume now that $y \in B^{\mathbb{Z}}$ has two distinct centered σ-representations (x, k) and (x', k'). We may assume $k = 0$. Since σ is injective on $A^{-\mathbb{N}}$, we have $k' \neq 0$. We will prove that y is periodic.

Let P be the set of proper prefixes of U. For $p \in P$ and $a \in A$, there is at most one $q \in P$ such that $p\sigma(a) \in U^* q$. We denote $q = p \cdot a$. Let $p_0 = y_{-k'} \ldots y_{-1}$. Since $y = \sigma(x) = S^{k'}(\sigma(x'))$, we have

$$\sigma(\ldots x'_{-2} x'_{-1}) p_0 = \sigma(\ldots x_{-1}),$$
$$p_0 \sigma(x_0 x_1 \ldots) = \sigma(x'_0 x'_1 \ldots).$$

As a consequence, there exists for each $n \in \mathbb{Z}$ a word $p_n \in P$ such that $p_n \cdot x_n = p_{n+1}$. Since σ is left marked, there is for every non-empty $p \in P$ at most one $a \in A$ such that $p \cdot a$ is in P. However, all p_n are non-empty. This is clear if $n < 0$ since otherwise p_0 is also empty. For $n > 0$, we have
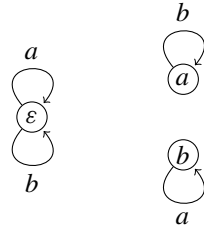
FIGURE 3. The graph associated with the Thue–Morse morphism.

$$\sigma(\ldots x'_{i_n}) p_n = \sigma(\ldots x_n),$$
$$p_n \sigma(x_{n+1} \ldots) = \sigma(x'_{i_n+1} \ldots),$$

and thus, since σ is injective on $A^{\mathbb{Z}}$, $p_n = \varepsilon$ implies that $x = x'$. Thus, x is periodic and y is also periodic.

Consider the labeled graph with P as a set of vertices and edges (p, a, q) if $p \cdot a = q$. By what we have seen, the path $\ldots p_n \xrightarrow{x_n} p_{n+1} \ldots$ is a cycle and thus y is periodic. $\square$

The graph used in the last part of the proof will appear again in §7.

Example 4.8. The Thue–Morse morphism $\sigma : a \to ab, b \to ba$ is left marked. Thus, it is recognizable for aperiodic points (as we have already seen). The graph used in the proof of Proposition 4.6 is represented in Figure 3.

The proof of Theorem 4.5 also uses the following statement, originally due to [15] (see also [4] and [16, Ch. 6]).

PROPOSITION 4.9. *If a morphism $\sigma : A^* \to C^*$ is not injective on $A^{\mathbb{N}}$, there is a trim decomposition $\sigma = \alpha \circ \beta$ with $\alpha : B^* \to C^*$ and $\beta : A^* \to B^*$ such that α is injective on $B^{\mathbb{N}}$, $\mathrm{Card}(B) < \mathrm{Card}(A)$, and every $b \in B$ appears as the first letter of $\beta(a)$ for some $a \in A$.*

Proof. Assume first that σ is non-erasing. We use an induction on $\ell(\sigma)$. If $\ell(\sigma) = 0$, set $B = \sigma(A)$. Let α be the identity on B and let $\beta = \sigma$. All conditions are clearly satisfied.

Assume now the statement is true for $\ell < \ell(\sigma)$. Since σ is not injective on $A^{\mathbb{N}}$, we have $\sigma(a_0 a_1 \ldots) = \sigma(a'_0 a'_1 \ldots)$ for some $a_i, a'_i \in A$ with $a_0 \neq a'_0$. We can assume that $\sigma(a_0)$ is a prefix of $\sigma(a'_0)$. Set $\sigma(a'_0) = \sigma(a_0) v$. If v is empty, set $B = A \setminus \{a_0\}$. Let α be the restriction of σ to B and let β be defined by $\beta(a'_0) = a_0$ and $\beta(a) = a$ for $a \neq a'_0$. Clearly, $\sigma = \alpha \circ \beta$ and all conditions are satisfied.

Next, assume the v is non-empty. Define $\alpha_1 : A^* \to C^*$ by $\alpha_1(a'_0) = v$ and $\alpha_1(a) = \sigma(a)$ for $a \neq a'_0$. Next, define $\beta_1 : A^* \to A^*$ by $\beta_1(a'_0) = a_0 a'_0$ and $\beta_1(a) = a$ for $a \neq a'_0$. Then, $\sigma = \alpha_1 \circ \beta_1$ since

$$\alpha_1 \circ \beta_1(a'_0) = \alpha_1(a_0 a'_0) = \sigma(a_0) v = \sigma(a'_0)$$

and $\alpha_1 \circ \beta_1(a) = \alpha_1(a) = \sigma(a)$ if $a \neq a_0'$. The morphism β_1 is injective on $A^{\mathbb{N}}$ because no word in $\beta_1(A)$ begins with a_0'. Thus, α_1 is not injective on $A^{\mathbb{N}}$. By equation (4.1), we have $\ell(\alpha_1) < \ell(\sigma)$. By induction hypothesis, we have a decomposition $\alpha_1 = \alpha_2 \circ \beta_2$ for $\beta_2 : A^* \to B^*$ and $\alpha_2 : B^* \to C^*$ with $\text{Card}(B) < \text{Card}(A)$, the morphism α_2 being injective on $B^{\mathbb{N}}$, and every letter $b \in B$ appearing as the initial letter in the word $\beta_2(a)$ for some $a \in A$. Note that since α_1 is non-erasing, β_2 is non-erasing.

Set $\beta = \beta_2 \circ \beta_1$. Since β_1, β_2 are non-erasing, β is non-erasing. Then, $\sigma = \alpha_1 \circ \beta_1 = \alpha_2 \circ \beta_2 \circ \beta_1 = \alpha_2 \circ \beta$. The decomposition $\sigma = \alpha_2 \circ \beta$ satisfies all the required conditions. Indeed, let $b \in B$. Then there is $a \in A$ such that b is the first letter of $\beta_2(a)$. If $a \neq a_0$, we have $\beta_1(a) = a$ and thus b is the first letter of $\beta(a)$. Suppose next that $a = a_0'$. Since $\sigma(a_0 a_1 \ldots) = \sigma(a_0' a_1' \ldots)$ and since α_2 is injective on $B^{\mathbb{N}}$, we have $\beta(a_0 a_1 \ldots) = \beta(a_0' a_1' \ldots)$. Since $\beta_1(a_0) = a_0$ and $\beta_1(a_0') = a_0 a_0'$, we obtain $\beta_2(a_0)\beta(a_1 \ldots) = \beta_2(a_0 a_0')\beta(a_1' \ldots)$ and thus

$$\beta(a_1 \ldots) = \beta_2(a_0')\beta(a_1' \ldots),$$

showing, since β is non-erasing, that b is the initial letter of $\beta(a_1)$.

Consider now a morphism σ such that the set $B = \{a \in A \mid \sigma(a) \neq \varepsilon\}$ is strictly contained in A. Let $\beta : A^* \to B^*$ be defined by $\beta(a) = a$ if $a \in B$ and $\beta(a) = \varepsilon$ otherwise. Let α be the restriction of σ to B^*. Then, $\sigma = \alpha \circ \beta$ and α is non-erasing. If α is injective on $B^{\mathbb{N}}$, we are done. Otherwise, by the first part of the proof, we have $\alpha = \alpha_1 \circ \beta_1$ with $\alpha_1 : B_1^* \to C^*$ and $\beta_1 : B^* \to B_1^*$ with α_1 injective on $B_1^{\mathbb{N}}$, $\text{Card}(B_1) < \text{Card}(B)$, and every $b_1 \in B_1$ appears as the first letter of some $\beta_1(b)$. Then, the decomposition $\sigma = \alpha_1 \circ (\beta_1 \circ \beta)$ satisfies all the conditions. $\square$

Example 4.10. Set $A = C = \{a, b, c\}$. The morphism $\sigma : a \mapsto ab, b \mapsto abc, c \mapsto cc$ is not injective on $A^{\mathbb{N}}$ because $\sigma(ac^\omega) = \sigma(bc^\omega) = abc^\omega$. The decomposition $\sigma = \alpha \circ \beta$ with $\alpha : u \mapsto ab, v \mapsto c$ and $\beta : a \mapsto u, b \mapsto uv, c \mapsto vv$ satisfies the conditions of Proposition 4.9.

By a symmetric version of Proposition 4.9, an elementary morphism $\sigma : A^* \to A^*$ is injective on $A^{-\mathbb{N}}$. Since a morphism which is injective on $A^{\mathbb{N}}$ and on $A^{-\mathbb{N}}$ is injective on $A^{\mathbb{Z}}$, we obtain the following corollary of Proposition 4.9.

COROLLARY 4.11. *An elementary morphism $\sigma : A^* \to C^*$ is injective on $A^{\mathbb{Z}}$.*

Proof of Theorem 4.5. Let $\sigma : A^* \to B^*$ be an elementary morphism. We use an induction on $\ell(\sigma)$. Since σ is elementary, it has no erasable letter and the minimal possible value of $\ell(\sigma)$ is 0. In this case, σ is a bijection from A to B and thus it is recognizable.

Assume now that σ is not recognizable on aperiodic points. Thus, there exist $x, x' \in A^{\mathbb{N}}$ and w with $0 < |w| < |\sigma(x_0)|$ such that $\sigma(x) = w\sigma(x')$ for some proper suffix w of $\sigma(a')$. Set $\sigma(a') = vw$. We can then write $\sigma = \sigma_1 \circ \tau_1$ with $\tau_1 : A^* \to A_1^*$ and $\sigma_1 : A_1^* \to B^*$ and $A_1 = A \cup \{a''\}$, where a'' is a new letter. We have $\tau_1(a') = a'a''$ and $\tau_1(a) = a$ otherwise. Next, $\sigma_1(a') = v, \sigma_1(a'') = w$, and $\sigma_1(a) = \sigma(a)$ otherwise. Since $\ell(\tau_1) > 0$, we have $\ell(\sigma_1) < \ell(\sigma)$ by equation (4.1).

Since τ_1 is injective on $A^{\mathbb{N}}$, σ_1 is not injective on $A_1^{\mathbb{N}}$. By Proposition 4.9, we can write $\sigma_1 = \sigma_2 \circ \tau_2$ with $\sigma_2 : A_2^* \to B^*$ and $\tau_2 : A_1^* \to A_2^*$ for some alphabet A_2 such that $\mathrm{Card}(A_2) < \mathrm{Card}(A_1)$ and that every letter $c \in A_2$ appears as the first letter of some $\tau_2(a)$ for $a \in A_1$. Then, by equation (4.1), we have

$$\ell(\sigma_1) \geq \ell(\sigma_2) + \ell(\tau_2). \tag{4.3}$$

If $\mathrm{Card}(A_2) < \mathrm{Card}(A)$, then σ is not elementary and we are done. Otherwise, we have $\mathrm{Card}(A_2) = \mathrm{Card}(A)$. We may also assume that σ_2 and $\tau_2 \circ \tau_1$ are elementary since otherwise σ is not elementary.

Since σ_2 is elementary and since $\ell(\sigma_2) \leq \ell(\sigma_1) < \ell(\sigma)$, by the induction hypothesis, σ_2 is recognizable for aperiodic points.

Since $\sigma = \sigma_2 \circ \tau_2 \circ \tau_1$, we have also

$$\ell(\sigma) \geq \ell(\sigma_2) + \ell(\tau_2 \circ \tau_1). \tag{4.4}$$

Thus, if $\ell(\sigma_2) > 0$, the inequality $\ell(\tau_2 \circ \tau_1) < \ell(\sigma)$ holds. Since $\tau_2 \circ \tau_1$ is elementary, we obtain that $\tau_2 \circ \tau_1$ is recognizable for aperiodic points by induction hypothesis. Thus, by Proposition 3.6, σ is recognizable for aperiodic points.

Let us finally assume that $\ell(\sigma_2) = 0$. Then, σ is left marked because σ_2 is a bijection from A_2 onto B and every letter of A_2 appears as an initial of $\tau_2(a)$ for $a \in A_1$. We obtain the conclusion by Proposition 4.6. □

5. *Recognizability and iterated morphisms*

In this section, we address the problem of the recognizability of morphisms $\sigma : A^* \to A^*$ on the shift $X(\sigma)$.

The following is proved in [7, Proposition 5.10] for non-erasing morphisms. We give a proof which holds for morphisms with erasable letters.

THEOREM 5.1. *Let* $\sigma : A^* \to A^*$ *be a morphism. Every point* y *in* $X(\sigma)$ *has a* σ-*representation* $y = S^k(\sigma(x))$ *with* $x \in X(\sigma)$.

Proof. Let $k = |\sigma|$. Let y be in $X(\sigma)$. For every $n > 2k$, there is an integer $m \geq 1$ such that $y_{[-n,n]}$ is a factor of $\sigma^m(a)$ for some letter $a \in A$.

Hence, $y_{[-n,n]} = s\sigma(a_1 \ldots a_\ell)p$, where $a_i \in A$, $a_1 \ldots a_\ell$ is a factor of $\sigma^{m-1}(a)$, s is a suffix of a word in $\sigma(A)$ and p is a prefix of a word in $\sigma(A)$. Since $n > 2k$, at least one letter a_i is such that $\sigma(a_i) \neq \varepsilon$. We write $a_1 \ldots a_\ell = u_1 \ldots u_r$, where $r \geq 1$, $u_j = v_j b_j$ with $b_j \in A$, $v_j \in A^*$ (the word v_j being possibly the empty word), $\sigma(v_j) = \varepsilon$, and $\sigma(b_j) \neq \varepsilon$.

Then, there are integers $n \leq k_1 < k_2 < \cdots < k_{r+1} \leq n+1$ such that $y_{[-n,n]} = s\sigma(u_1) \ldots \sigma(u_r)p$, with $s = y_{[-n,k_1)}, \sigma(u_j) = y_{[k_j,k_{j+1})}, p = y_{[k_{r+1},n]}$. Note that $\sigma(u_j) = \sigma(a_j)$ is non-empty and belongs to $\sigma(A)$.

For every i with $-n + k \leq i \leq n - k$, we denote by $f_n(i)$ the unique triple $(k_j, k_{j+1} - 1, u_j)$ defined above such that $k_j \leq i < k_{j+1}$.

Since $\sigma(A)$ is finite and since there is a finite number of erasable words in $\mathcal{L}(\sigma)$ by Proposition 2.2, there is a finite number of triples $f_n(0)$. Thus, there is a strictly increasing

sequence $(i_n)_{n \in \mathbb{N}}$ of natural integers such that $f_{i_n}(0)$ is constant. We denote this constant value by $f(0)$.

Taking a subsequence of $(i_n)_{n \in \mathbb{N}}$, we may also assume that all $f_{i_n}(-1)$ and $f_{i_n}(1)$ are equal to some triple $f(-1)$ and $f(1)$, respectively. By iterating his process, we define for each $i \in \mathbb{Z}$ a triple $f(i) = (j_i, \ell_i, u_i)$. By construction, $f(i) = f(i')$ for all $i, i' \in [j_i, \ell_i)$.

We now concatenate the words u_i to build a point x as follows. We define a strictly increasing sequence $(j_n)_{n \in \mathbb{Z}}$ of integers by $j_0 = 0$, for $n > 0$, j_n is the least integer larger than j_{n-1} such that $f(j_n) \neq f(j_{n-1})$, and for $n < 0$, j_n is the largest integer less than j_{n+1} such that $f(j_n) \neq f(j_{n+1})$. Let $x = \ldots u_{j_{-2}} u_{j_{-1}}.u_{j_0} u_{j_1} u_{j_2} \ldots$. By construction, $x \in X(\sigma)$ and there is some integer r such that $y = S^r(\sigma(x))$. $\qquad \square$

We will also need the following more technical statements. The first one concerns growing letters. Let $\sigma : A^* \to A^*$ be a morphism. Recall that a letter a is growing if $|\sigma^n(a)|$ is unbounded and that, in this case, by Proposition 2.7, one has actually $\lim_{n \to +\infty} |\sigma(a)| = +\infty$.

PROPOSITION 5.2. *Let $\sigma : A^* \to A^*$ be a morphism and let S be the set of right-infinite sequences x such that every $x_{[0,n]}$ is a prefix of some $\sigma^m(a)$ for a fixed letter a.*

If $x \in S$ contains a growing letter, there are integers r and $0 \leq k < r$ such that $x = \lim_{n \to +\infty} \sigma^{rn+k}(a)$.

The set of points $x \in S$ with no growing letters is a finite set of eventually periodic right-infinite sequences.

Proof. We first assume that x contains a growing letter. Let $x_i = b$ be the first growing letter of x. Thus, $x = x_{[0,i)} b x'$, where $x_{[0,i)}$ is non-growing. There are integers $m < m'$ such that $x_{[0,i)} b$ is a prefix of $\sigma^m(a)$ and of $\sigma^{m'}(a)$. Let $r = m' - m$.

Since $x_{[0,i)} b$ is a prefix of $\sigma^m(a)$, $\sigma^r(x_{[0,i)} b)$ is a prefix of $\sigma^{m'}(a)$ and thus $\sigma^r(x_{[0,i)} b)$ is prefix comparable with $x_{[0,i)} b$. Since $x_{[0,i)}$ is non-growing, $\sigma^r(x_{[0,i)})$ is a prefix $x_{[0,j)}$ of $x_{[0,i)}$ and $\sigma^r(b) = x_{[j,i)} b u$, where u is a non-erasable word (otherwise, b would not be growing).

Then, for all integers n, $\sigma^{nr}(x_{[0,i)} b) = x_{[0,i)} b u \sigma^r(u) \ldots \sigma^{(n-1)r}(u)$. Thus, $\lim_{n \to +\infty} \sigma^{m+rn}(a)$ exists. It follows that $\lim_{n \to +\infty} \sigma^{m+k+rn}(a)$ exists for every $0 \leq k < r$. It also follows that x is one of the points $x^{(k,r)} = \lim_{n \to +\infty} \sigma^{k+rn}(a)$ for some $0 \leq k < r$.

Let us show that there is a finite number of such points. If y is another point of S with a growing letter, $y = \lim_{n \to +\infty} \sigma^{k'+r'n}(a)$ with $r' > r$, $0 \leq k' < r'$, then we have $y = x^{(k'',r)}$ for some $0 \leq k'' < r$.

We now assume that all letters of x are non-growing. There are non-negative integers $r, p \leq \mathrm{Card}(A)$ such that $\sigma^r(a) = ubv$ and $\sigma^p(b) = wbz$ with u, w non-growing, $b \in A$ growing. We get that for any $k \geq 0$,

$$\sigma^{r+kp}(a) = \sigma^{kp}(u) \sigma^{(k-1)p}(w) \ldots \sigma^p(w) w b z^{(k)}.$$

Since u and w are non-growing, there are non-negative integers i, i' such that $\sigma^{i'p}(u) = \sigma^{i'p+ip}(u)$ and $\sigma^{i'p}(w) = \sigma^{i'p+ip}(w)$. It follows that

$$\sigma^{r+i'p+kip}(a) = \sigma^{i'p}(u) \sigma^{((i'+ki)-1)p}(w) \ldots \sigma^p(w) w b z^{(i'+ki)}.$$

Note that w is non-erasable since otherwise x would have a growing letter. Thus, for large enough k, we get

$$\sigma^{r+i'p+kip}(a) = tz^{k-1}\sigma^{(i'-1)p}(w)\ldots\sigma^p(w)wbz^{(i'+ki)},$$

where $t = \sigma^{i'p}(u)\sigma^{(i'+i-1)p}(w)\ldots\sigma^{i'p}(w)$, and $z = \sigma^{(i'+i-1)p}(w)\ldots\sigma^{i'p}(w)$.

Every $x_{[0,n]}$ is a prefix of some $\sigma^{N_n}(a)$. There is an infinite number of n such that N_n is equal to $r + i'p + k_nip + h$ for some fixed $0 \le h < ip$ for some non-negative integer k_n. It follows that for an infinite number n, $x_{[0,n]}$ is a prefix of $\sigma^h(tz^{k_n-1}t')$, where $t' = \sigma^{(i'-1)p}(w)\ldots\sigma^p(w)w$. It follows that there is a finite number of words u, v depending only on σ such that $x = uv^\omega$. Hence the conclusion. $\square$

The second one gives a sufficient condition to have $X(\sigma) = X(\sigma^n)$. This is not always true, as shown by the example of $\sigma : a \mapsto bc, b \mapsto cc, c \mapsto bb$. We have $^\omega c \cdot b^\omega$ is in $X(\sigma)$ but not in $X(\sigma^2)$.

LEMMA 5.3. *Let $\sigma : A^* \to A^*$ be a morphism. If every letter $a \in A$ appears in $\sigma(A)$, then $X(\sigma^n) = X(\sigma)$ for every $n \ge 1$.*

Proof. It is enough to show that $\mathcal{L}(\sigma^n) = \mathcal{L}(\sigma)$. We first clearly have $\mathcal{L}(\sigma^n) \subset \mathcal{L}(\sigma)$. Conversely, let $u \in \mathcal{L}(\sigma)$. Then u is a factor of some $\sigma^m(a)$. Let k be such that $kn \le m < (k+1)n$. Since every letter appears in $\sigma(A)$, the letter a appears in $\sigma^{(k+1)n-m}(b)$ for some letter b and thus u is a factor of $\sigma^{n(k+1)}(b)$. Hence, $u \in \mathcal{L}(\sigma^n)$. $\square$

A morphism $\sigma : A^* \to A^*$ is *primitive* if there is an integer $n \ge 1$ such that every $b \in A$ appears in every $\sigma^n(a)$ for $a \in A$.

A morphism $\sigma : A^* \to A^*$ is *aperiodic* if $X(\sigma)$ does not contain periodic points.

The following result is proved in [6] in the case of non-erasing morphisms. It is a generalization of Mossé's theorem asserting that every aperiodic primitive morphism σ is recognizable on $X(\sigma)$. Our new proof holds for the general case of morphisms with erasable letters and relies on Theorem 4.5. It also gives a proof of the original version of Mossé's theorem which is easier than the previous ones (see the comment after the proof).

THEOREM 5.4. *Every morphism $\sigma : A^* \to A^*$ is recognizable on $X(\sigma)$ for aperiodic points.*

Proof. Let $\sigma : A^* \to A^*$ be a morphism.

Case 1. We first assume that every letter of A is a letter of some word of $\sigma(A)$. By Lemma 5.3, we have $X(\sigma) = X(\sigma^n)$ for every positive integer n.

It is enough to prove the statement for a power σ^n of σ. Indeed, assume that σ^n is recognizable on $X(\sigma^n) = X(\sigma)$ for aperiodic points. Let x be an aperiodic point $x \in X(\sigma)$ and let (z, K) be its unique centered σ^n-representation. Let $\sigma^{n-1}(z_0) = uav$ with $a \in A$ be the unique factorization of $\sigma^{n-1}(z_0)$ such that $|\sigma(u)| \le K < |\sigma(ua)|$. Set $y = S^{|u|}\sigma^{n-1}(z)$ and $\sigma(a) = sx_0t$. Then, $(y, |s|)$ is the unique centered σ-representation of x.
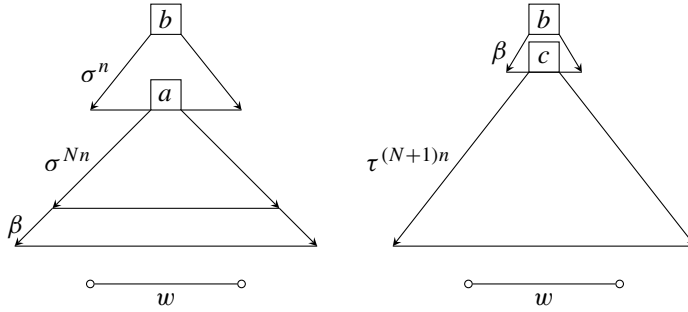
FIGURE 4. Proving that w is a factor of $\tau^m(c)$.

Indeed, it is a centered σ-representation of x. If (y', k') is another centered σ-representation of x, let (z', r') be a centered σ^{n-1}-representation of y. Set $\sigma^{n-1}(z'_0) = u'a'v'$ with $|u'| = r'$ and $\sigma(a') = s'x_0t'$ with $|s'| = k'$. Then, $u'a'$ is a prefix of $\sigma^{n-1}(z'_0)$ such that $|\sigma(u')| \le |\sigma(u')| + k' < |\sigma(u'a')|$. Since $(z', |\sigma(u')| + k')$ is a centered σ^n-representation of x, we have $z = z'$, $K = |\sigma(u')| + k'$ and thus $ua = u'a'$, which implies $y = y'$ and $k' = |s|$.

Choose n such that σ^n has a decomposition $\sigma^n = \alpha \circ \beta$ with $\beta : A^* \to B^*$ and $\alpha : B^* \to A^*$, and $\mathrm{Card}(B)$ minimal. Then, $\tau = \beta \circ \alpha$ is elementary. Indeed, if $\tau = \gamma \circ \delta$ with $\delta : B^* \to C^*$ and $\gamma : C^* \to B^*$ is a decomposition of τ such that $\mathrm{Card}(C) < \mathrm{Card}(B)$, then $\sigma^{2n} = (\alpha \circ \gamma) \circ (\delta \circ \beta)$ is a decomposition of σ^{2n} with $\delta \circ \beta : A^* \to C^*$ and $\alpha \circ \gamma : C^* \to A^*$ such that $\mathrm{Card}(C) < \mathrm{Card}(B)$, which is a contradiction.

It is easy to check that α is also elementary. Moreover, we have

$$\beta(X(\sigma)) \subset X(\tau). \tag{5.1}$$

Indeed, consider $x \in X(\sigma)$ and let w be a factor of $\beta(x)$. We have to prove that w is a factor of some $\tau^m(c)$ for $c \in B$. Now, since $x \in X(\sigma^n)$, there in an $N \ge 1$ such that w is a factor of some $\beta \circ \sigma^{Nn}(a)$ for $a \in A$ and $N \ge 1$, and also a factor of $\beta \circ \sigma^{(N+1)n}(b)$ with a a factor of $\sigma^n(b)$ (see Figure 4). Since $\sigma^n = \alpha \circ \beta$, there is a letter c such that $a \in \alpha(c)$ and $c \in \beta(b)$. Since $\beta \circ \sigma^n = \tau^n \circ \beta$, we obtain that w is a factor of $\tau^{(N+1)n}(c)$.

Let $x \in X(\sigma)$ be an aperiodic point. Consider two centered σ^n-representations (y, k) and (y', k') of x with $y, y' \in X(\sigma)$. Let (z, ℓ) and (z', ℓ') be centered σ^n-representations of y and y', respectively, with $z, z' \in X(\sigma)$ (we use here Theorem 5.1). Then, $(\beta(z), m)$ and $(\beta(z'), m')$ are, for some unique m, m', some centered τ-representations of $\beta(y)$ and $\beta(y')$, respectively (see Figure 5). The fact that m, m' are unique results from the fact that τ is elementary and thus recognizable for aperiodic points by Theorem 4.5.

Since α is elementary, it is recognizable for aperiodic points. Since $\alpha(\beta(y)) = \sigma^n(y)$ and $\alpha(\beta(y')) = \sigma^n(y')$, this implies that $\beta(y), \beta(y')$ belong to the same orbit. Since τ is recognizable for aperiodic points, we obtain that $\beta(z)$ and $\beta(z')$ belong to the same orbit. Applying α again, we conclude that y, y' belong to the same orbit. Since x is aperiodic, this implies that $y = y'$ and $k = k'$. Thus, σ^n is recognizable for aperiodic points.
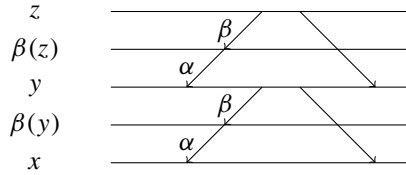
FIGURE 5. The points x, y, z.

Case 2. We now prove the general case. We prove the result by induction on the number of letters which do not appear in some word of $\sigma(A)$. The case where there is no such letter is Case 1 and thus the property holds. Let a be a letter of A which does not appear in a word in $\sigma(A)$ and set $B = A \setminus \{a\}$. We denote by σ_B the morphism σ restricted to B^*. By induction hypothesis, σ_B is recognizable on $X(\sigma_B)$ for aperiodic points. We denote by K the maximal length of all $\sigma^n(b)$ for non-growing letters b in B.

Let y be an aperiodic point having two centered σ-representations (x, k) and (x', k') with $x, x' \in X(\sigma)$. We cannot have $x, x' \in X(\sigma_B)$ and we may assume that x belongs to $X(\sigma) \setminus X(\sigma_B)$. Thus, there is an integer m such that $x_{[-m,m]}$ is not a factor of any $\sigma^n(b)$ for $b \in B$. For each integer $n \geq m$, there is an integer $N(n)$ such that $x_{[-n,n]}$ is a factor of $\sigma^{N(n)}(a)$.

We have $\sigma(a) = b_1 \ldots b_\ell$ with $b_i \in B$. Since $x_{[-m,m]}$ is not a factor of any $\sigma^n(b_i)$, there are integers $1 \leq i_n \leq \ell$, $-m \leq k_n < m$ such that $x_{[-n,k_n)}$ is a suffix of $\sigma^{N(n)-1}(b_1 \ldots b_{i_n})$ and $x_{[k_n,n]}$ is a prefix of $\sigma^{N(n)-1}(b_{i_n+1} \ldots b_\ell)$. Let b_{j_n} be the last growing letter of $b_1 \ldots b_{i_n}$ and b_{r_n} be the first growing letter of $b_{i_n+1} \ldots b_\ell$. Note that such growing letters exist for large enough n.

There is an infinite number of integers n such that $i_n = i$, $j_n = j$, $r_n = r$, $k_n = M$, where $1 \leq j \leq i < r \leq \ell$ and $-m \leq M < m$.

Since $b_{j+1} \ldots b_i$ and $b_{i+1} \ldots b_{r-1}$ are non-growing, the lengths of all words $\sigma^{N(n)-1}(b_{j+1} \ldots b_i)$ and $\sigma^{N(n)-1}(b_{i+1} \ldots b_{r-1})$ are bounded by $K\ell$. Thus, there is an infinite number of integers n such that moreover $|\sigma^{N(n)-1}(b_{j+1} \ldots b_i)| = p$, $|\sigma^{N(n)-1}(b_{i+1} \ldots b_{r-1})| = p'$ for some fixed integers $0 \leq p, p' \leq K\ell$.

Let $b = b_j$ and $c = b_r$. Since b, c are growing, for each n, there are integers m, m' such that $x_{[-n,M-p)}$ is a suffix of $\sigma^m(b)$ and $x_{[M+p',n]}$ is a prefix of $\sigma^{m'}(c)$.

By Proposition 5.2, there are finite sets L, R of respectively left- and right-infinite sequences, and a finite set U of words of length at most $2K\ell$ such that x is a shift of tut' with $t \in L$, $u \in U$, and $t' \in R$. Thus, there is a finite number of such orbits.

We define a sequence $(x^{(i)})_{i \geq 0}$ of two-sided infinite sequences $x^{(i)}$ by $x^{(0)} = x$ and $x^{(i)} \in X(\sigma) \setminus X(\sigma_B)$ such that $x^{(i-1)} = S^k \sigma(x^{(i)})$ for some k. There is an infinite number of i such that $x^{(i)}$ are shifts of the same sequence. Thus, there are integers i, j with $j \geq 1$ such that $\sigma^j(x^{(i)})$ is a shift of $x^{(i)}$. As a consequence, $y \in X(\sigma) \setminus X(\sigma_B)$. Thus, $x, x' \in X(\sigma) \setminus X(\sigma_B)$.

As above, we define sequences $(x^{(i)})$ and $(x'^{(i)})$ for x and x'. Thus, there are integers i, j with $j \geq 1$ such that $\sigma^j(x^{(i)})$ is a shift of $x^{(i)}$ and $\sigma^j(x'^{(i)})$ is a shift of $x'^{(i)}$. We get that there is an integer i such that $x^{(i)}$ and $x'^{(i)}$ are in the same orbit and thus x and x' also.

Now if $x \neq x'$ of $k \neq k'$ with $0 \leq k < |\sigma(x_0)|$ and $0 \leq k' < |\sigma(x_0')|$, we get that y is periodic, which is excluded. Thus, y has a unique centered σ-representation in $X(\sigma)$. $\square$

Note that to prove Mossé's theorem itself, one only needs the first case in the above proof. Indeed, if σ is primitive, every letter appears in $\sigma(A)$. Note also that in this case, Proposition 5.2 is not used. The previous proofs of Mossé's theorem work on a fixed point of the morphism and handle indices of this sequence, resulting in fairly complicated arguments (see for example [12]). The proof given in [9] avoids these indices but remains essentially the same as that of [12]. The use of the notion of elementary morphism, through Theorem 4.5, seems to us a major simplification.

We give below an example of a morphism σ such that $X(\sigma)$ contains both periodic and non-periodic points.

Example 5.5. Let σ be the morphism $\sigma : a \mapsto bac, b \mapsto bb, c \mapsto cd, d \mapsto c$. The set $X(\sigma)$ contains the aperiodic point ${}^\omega b \cdot a\sigma^\omega(c)$, where $\sigma^\omega(c) = cdccd \ldots$ is the one-sided Fibonacci sequence. It also contains the periodic point $y = b^\infty$. Every point, except y, has a unique centered σ-representation.

6. *Automata and syntactic groups*

We now introduce notions from automata theory which will allow us to formulate a characterization of morphisms $\sigma : A^* \to B^*$ which are recognizable for aperiodic points (Theorem 6.5).

Let $\mathcal{A} = (Q, I, T)$ be a finite automaton on the alphabet A with Q as a set of states, I as a set of initial states, and T as a set of terminal states. Such an automaton is just a graph with Q as a set of vertices and edges labeled by A. The language *recognized* by $\mathcal{A}$ is the set of labels of paths from I to T. The automaton is *deterministic* if for every $q \in Q$ and a in A, there is at most one edge starting at q labeled a (the term deterministic corresponds to the term *right-resolving* used, in particular, in [14]).

An automaton is *unambiguous* if for every $p, q \in Q$ and $w \in A^*$, there is at most one path from p to q labeled by w. An automaton is *unambiguous for aperiodic points* if for every aperiodic two-sided infinite word x, there is at most one path of the automaton labeled by x.

PROPOSITION 6.1. *Let $\sigma : A^* \to B^*$ be a morphism. If σ is recognizable for aperiodic points, either σ is periodic or σ is injective.*

Proof. Assume that σ is not periodic. If σ is not injective, there are some distinct $u, v \in A^*$ such that $\sigma(u) = \sigma(v) = d$. Since σ is not periodic, there is some w such that $c = \sigma(w)$ and $\sigma(u)$ are not powers of the same primitive word. Then, ${}^\omega c \cdot dc^\omega$ is aperiodic and has more than one centered σ-representation. Thus, σ is not recognizable for aperiodic points. $\square$

For every finite set $U \subset B^+$, there is a particular automaton which recognizes U^*, called the *flower automaton* of U. Its set of states is the set Q defined as

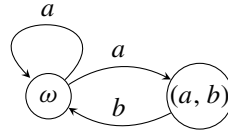$$Q = \{(u, v) \in B^+ \times B^+ \mid uv \in U\} \cup \{\omega\},$$

FIGURE 6. The flower automaton of $\sigma(A) = \{ab, a\}$.

where ω is a new element. There are four type of edges labeled by $a \in B$:

$$(u, av) \xrightarrow{a} (ua, v) \quad \text{for } uav \in U, u, v \neq 1;$$
$$\omega \xrightarrow{a} (a, v) \quad \text{for } av \in U, v \neq 1;$$
$$(u, a) \xrightarrow{a} \omega \quad \text{for } ua \in U, u \neq 1;$$
$$\omega \xrightarrow{a} \omega \quad \text{for } a \in U.$$

The state ω is both initial and terminal. It is easy to verify that the flower automaton recognizes U^*. Moreover, the set U is a code if and only if its flower automaton is unambiguous (see [5]).

Note that a morphism $\sigma : A^* \to B^*$ is left marked if and only if the flower automaton of $\sigma(A)$ is deterministic.

Example 6.2. Let $\sigma : a \mapsto ab, b \mapsto a$ be the Fibonacci morphism. The flower automaton $\mathcal{A}$ of $\sigma(A) = \{ab, a\}$ is represented in Figure 6.

Let $\mathcal{A}$ be a finite automaton. For $w \in A^*$, we denote by $\varphi_{\mathcal{A}}(w)$ the $Q \times Q$-relation defined by

$$\varphi_{\mathcal{A}}(w)_{p,q} = \begin{cases} 1 & \text{if } p \xrightarrow{w} q, \\ 0 & \text{otherwise.} \end{cases}$$

The monoid $M(\mathcal{A}) = \varphi_{\mathcal{A}}(A^*)$ is the *monoid of transitions* of the automaton $\mathcal{A}$. For $m \in M(\mathcal{A})$, we denote indifferently $m_{p,q} = 1$, $(p, q) \in m$ or $p \xrightarrow{m} q$ the fact that (p, q) are in relation by m.

When $\mathcal{A}$ is deterministic, each relation $\varphi_{\mathcal{A}}$ is a partial map from Q to itself and thus $M(\mathcal{A})$ is a submonoid of the monoid of partial maps from Q to Q.

When $\mathcal{A}$ is unambiguous, the monoid $M = M(\mathcal{A})$ is called an *unambiguous monoid of relations*. This means that for every $m, n \in M$ and $p, q \in Q$ such that $p \xrightarrow{mn} q$, there is a unique $r \in Q$ such that $p \xrightarrow{m} r \xrightarrow{n} q$. This also means that we can consider the elements of M as $\{0, 1\}$-matrices with $0, 1$ considered as integers.

As in any monoid, the Green relations $\mathcal{R}$ and $\mathcal{L}$ are defined by $m\mathcal{R}n$ if $mM = nM$ and, symmetrically, $m\mathcal{L}n$ if $Mm = Mn$. It is classical that $\mathcal{R}$ and $\mathcal{L}$ commute and thus that the composition $\mathcal{R}\mathcal{L} = \mathcal{L}\mathcal{R}$ is an equivalence, traditionally denoted by $\mathcal{D}$.

For an element m of a monoid M, we denote by $H(m)$ the $\mathcal{H}$-class of m, where $\mathcal{H}$ is the Green relation $\mathcal{H} = \mathcal{R} \cap \mathcal{L}$. It is a group if and only if it contains an idempotent e (see [5]). In this case, every $m \in H(e)$ has a unique inverse m^{-1} in the group $H(e)$.
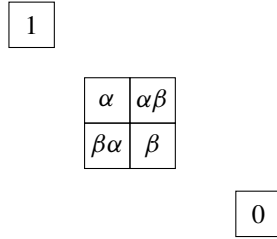
$$\boxed{1}$$

α	$\alpha\beta$
$\beta\alpha$	β

$$\boxed{0}$$

FIGURE 7. The monoid of transitions of $\mathcal{A}$.

Let M be a unambiguous monoid of relations on Q. A *fixed point* of a relation $m \in M$ is an element $q \in Q$ such that $q \xrightarrow{m} q$. A group in a monoid M is a subsemigroup of M which is a group. Let G be a group in M with neutral element e. Let S be the set of fixed points of e. The restriction of the elements of G to $S \times S$ is a faithful representation of G by permutations on S. The number of elements of S is called the *degree* of G.

The above representation of groups also exists in a monoid of relations which is ambiguous but is more complicated (see [24] or [23]).

A group in the monoid $M(\mathcal{A})$ is *strongly cyclic* (or *special*) if $\varphi_{\mathcal{A}}^{-1}(G)$ is a cyclic submonoid of A^*. This notion was introduced by Schützenberger in [27] (see also [22]). It implies that G itself is a cyclic group. It also implies that $\varphi^{-1}(D)$, where D is the $\mathcal{D}$-class containing G, is also included in the set of factors of the same cyclic submonoid. In particular, if e, f are idempotents in D, then $\varphi_{\mathcal{A}}^{-1}(e) = u^+$ and $\varphi_{\mathcal{A}}^{-1}(f) = v^+$, where u, v are conjugate. Moreover, if $m \in D$ is such that $m = em = mf$, then

$$\varphi_{\mathcal{A}}^{-1}(e) = (rs)^+, \quad \varphi_{\mathcal{A}}^{-1}(m) = (rs)^+r, \quad \varphi_{\mathcal{A}}^{-1}(f) = (sr)^+. \tag{6.1}$$

A pair (m, e) of elements in a monoid M is a *linked pair* if $m = me$ and $e = e^2$. The following result is [21, Theorem 2.2].

PROPOSITION 6.3. *Let $\varphi : A^* \to M$ be a morphism from A^* into a finite monoid M. For every $x \in A^{\mathbb{N}}$, there exists a linked pair (m, e) in M such that $x \in \varphi^{-1}(m)\varphi^{-1}(e)^{\omega}$.*

A dual statement holds for a left-infinite sequence. Consequently, for every $x \in A^{\mathbb{Z}}$, there is a triple (e, m, f) with e, f idempotents and $m = em = mf$ such that $x \in {}^{\omega}\varphi^{-1}(e)\varphi^{-1}(m)\varphi^{-1}(f)^{\omega}$.

Example 6.4. Let σ be the Fibonacci morphism and let $\mathcal{A}$ be the flower automaton of $\sigma(A) = \{ab, a\}$ (see Figure 6).

Set $\alpha = \varphi_{\mathcal{A}}(a)$ and $\beta = \varphi_{\mathcal{A}}(b)$. One has $a^2 \equiv a$, $aba \equiv a$, and $b^2 \equiv b^3$, which is a zero of the monoid. The monoid of transitions of $\mathcal{A}$ is formed of 6 elements pictured in Figure 7 (we adopt the usual egg-box representation of monoids corresponding to the Green relations, see [5]). Besides 1 and 0, there are three groups in $M(\mathcal{A})$ reduced to one element (α, $\alpha\beta$ and $\beta\alpha$), which have degree 1.

THEOREM 6.5. *Let $\sigma : A^* \to B^*$ be an injective morphism and let $\mathcal{A}$ be the flower automaton of $\sigma(A)$. The morphism σ is recognizable for aperiodic points if and only if $\mathcal{A}$ is unambiguous for aperiodic points.*

Proof. The morphism σ is recognizable for aperiodic points if and only if every aperiodic point x of $B^{\mathbb{Z}}$ has at most one decomposition in words of $\sigma(A)$, that is, if there is at most one two-sided infinite path of $\mathcal{A}$ labeled by x going through the state ω for an infinite number of positive and negative indices. As $\sigma(A)$ is finite, every two-sided infinite path of $\mathcal{A}$ goes through the state ω for an infinite number of positive and negative indices. Thus, σ is recognizable for aperiodic points if and only if $\mathcal{A}$ is unambiguous for aperiodic points. $\qquad\square$

An automaton $\mathcal{A}$ is *weakly deterministic* if there is an integer n such that for every state p and every word w of length n, there is at most one right-infinite path starting at p with label starting by w. Symmetrically, $\mathcal{A}$ is *weakly codeterministic* if there is an integer n such that for every state p and every word w of length n, there is at most one left-infinite path ending at p with label ending by w.

The notion of weakly deterministic automaton corresponds to that of a *right-closing* map in symbolic dynamics. More precisely, the map assigning its label to a right-infinite path in the automaton is right closing if and only if the automaton is weakly deterministic.

The following statement gives a necessary condition for an automaton to be unambiguous for aperiodic points. An automaton is *periodic* if the labels of all infinite paths are periodic. Otherwise, it is said to be *non-periodic*. Note that in a periodic automaton which is strongly connected, the labels of all finite paths are factors of u^* for a single word u.

PROPOSITION 6.6. *If a strongly connected non-periodic finite automaton is unambiguous for aperiodic points, it is weakly deterministic and co-deterministic.*

Proof. Assume that $\mathcal{A}$ is not weakly deterministic. Then there is a state p and a right-infinite sequence x such that there are two paths starting at p labeled x. Since $\mathcal{A}$ is strongly connected, there is a left-infinite path ending at p. Let y be the label of this path. Since $\mathcal{A}$ is non-periodic, we may choose y aperiodic. Then, $y \cdot x$ is an aperiodic point which is the label of more than one path in $\mathcal{A}$. The case where $\mathcal{A}$ is not weakly co-deterministic is symmetrical. $\qquad\square$

We now characterize as follows the unambiguous automata which are unambiguous for aperiodic points. Combined with Proposition 6.1 and Theorem 6.5, this will give us a characterization of morphisms which are recognizable for aperiodic points. Indeed, if σ is recognizable for aperiodic points, by Proposition 6.1, either it is periodic or it is injective. In the first case, it is trivially recognizable for aperiodic points. In the second case, by Theorem 6.5, it is recognizable for aperiodic points if and only if the flower automaton of $\sigma(A)$ is unambiguous for aperiodic points.

THEOREM 6.7. *A strongly connected unambiguous finite automaton $\mathcal{A}$ is unambiguous for aperiodic points if and only if the following conditions are satisfied.*
  (i) *$\mathcal{A}$ is weakly deterministic and co-deterministic.*
  (ii) *For every idempotent $e \in \varphi_{\mathcal{A}}(A^+)$ of rank at least 2, the group $H(e)$ is strongly cyclic.*
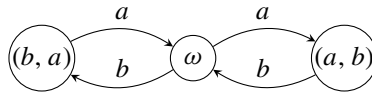
FIGURE 8. The flower automaton of $\sigma(A) = \{ab, ba\}$.

(iii)   *For every pair (e, f) of idempotents in $\varphi_{\mathcal{A}}(A^+)$ of rank at least 2, and every pair of distinct fixed points p, p' and q, q' of e and f, respectively, if some $m \in \varphi_{\mathcal{A}}(A^*)$ is such that $p \xrightarrow{m} q$ and $p' \xrightarrow{m} q'$, then e, f and m belong to the same $\mathcal{D}$-class.*

Proof. Assume that $\mathcal{A}$ is unambiguous for aperiodic points. By Proposition 6.6, condition (i) is satisfied. Let e be an idempotent in $M(\mathcal{A})$ of degree $d \geq 2$. If the group $G = H(e)$ is not strongly cyclic, there are words of arbitrary large minimal period in $L = \varphi_{\mathcal{A}}^{-1}(G)$ and thus there is an aperiodic sequence $x \in A^{\mathbb{Z}}$ such that all its factors are factors of words in L. Indeed, if G is not strongly cyclic, there are words u, v which are not powers of the same primitive word such that $e \in \varphi_{\mathcal{A}}(u) \cap \varphi_{\mathcal{A}}(v)$. Then, $\{u, v\}^*$ contains words of arbitrary large minimal period and thus an infinite sequence x with all its factors which are factors of words in $\{u, v\}^*$. Then, x is the label of d paths in $\mathcal{A}$ and consequently, $\mathcal{A}$ is not recognizable for aperiodic points. This proves that condition (ii) holds. Assume finally that m is such that $p \xrightarrow{m} q$ and $p' \xrightarrow{m} q'$ for some fixed points p, p' and q, q' of two idempotents $e, f \in \varphi(A^+)$. If e, f do not belong to the same $\mathcal{D}$-class, we have $e \in \varphi_{\mathcal{A}}(u^+)$ and $f \in \varphi_{\mathcal{A}}(v^+)$ for non-conjugate primitive words u, v (two idempotents are in the same $\mathcal{D}$-class if and only if they are conjugate). Let w be such that $\varphi(w) = m$. Then ${}^{\omega}uwv^{\omega}$ is an aperiodic sequence which is the label of two distinct paths.

Assume conversely that the conditions are satisfied. Consider a point $x \in A^{\mathbb{Z}}$ which is the label of more than one path. Since $M = M(\mathcal{A})$ is a finite monoid, there is, by Proposition 6.3, some $m \in M$ and idempotents $e, f \in M$ with $em = mf = m$ such that $x \in {}^{\omega}EwF^{\omega}$ with $E = \varphi_{\mathcal{A}}^{-1}(e)$, $\varphi_{\mathcal{A}}(w) = m$, and $F = \varphi_{\mathcal{A}}^{-1}(f)$. The two paths have the form $p \xrightarrow{e} p \xrightarrow{m} q \xrightarrow{f} q$ and $p' \xrightarrow{e} p' \xrightarrow{m} q' \xrightarrow{f} q'$. If $p = p'$, then $\mathcal{A}$ is not weakly deterministic. Similarly, if $q = q'$, it is not weakly co-deterministic. Thus, by condition (iii), e, m, f belong to the same $\mathcal{D}$-class. By condition (ii), using equation (6.1), this implies that x is periodic. $\square$

Example 6.8. Let $\sigma : a \mapsto ab, b \mapsto ba$ be the Thue–Morse morphism and let $\sigma(A) = \{ab, ba\}$. The flower automaton of $\sigma(A)$ is represented in Figure 8. The monoid of transitions of $\mathcal{A}$ is represented in Figure 9 with $\alpha = \sigma(a)$ and $\beta = \sigma(b)$. There are two groups of degree 2, each reduced to one element, namely ab and ba. They are strongly cyclic since $\varphi_{\mathcal{A}}^{-1}(\alpha\beta) = (ab)^*$.

7. *Efficient algorithms*

The conditions of Theorem 6.7 give an effective characterization of morphisms recognizable for aperiodic points. We now consider the problem of finding a more efficient procedure to check whether this property holds.
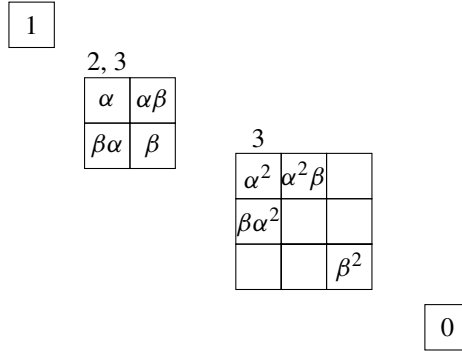
FIGURE 9. The monoid of transitions of $\mathcal{A}$.

If $\mathcal{A} = (Q, I, T)$ is a finite automaton on A, the *square* $\mathcal{A} \times \mathcal{A}$ of the automaton $\mathcal{A}$ is the following automaton. Its set of states is $Q \times Q$ and its edges are the $((p, q), a, (r, s))$ such that (p, a, r) and (q, a, s) are edges of $\mathcal{A}$.

The *diagonal* of $\mathcal{A} \times \mathcal{A}$ is the set of states of the form (p, p) with $p \in Q$. A strongly connected component of an automaton is *non-trivial* if it contains at least one cycle.

A *simple path* in $\mathcal{A}$ is a path with all states distinct except the extremities. A *simple cycle* around a state p of $\mathcal{A}$ is a simple path from p to p.

It is easy to verify that $\mathcal{A}$ is unambiguous if and only if there is no path in $\mathcal{A} \times \mathcal{A}$ going from a diagonal state to a diagonal state and going through a non-diagonal one. This gives a polynomial algorithm to check whether an automaton is unambiguous.

It is also easy to verify that if $\mathcal{A}$ is unambiguous, its square is also unambiguous. Indeed, assume that there are two paths in $\mathcal{A} \times \mathcal{A}$:

$$(p, q) \xrightarrow{w} (u, v) \xrightarrow{w'} (r, s);$$
$$(p, q) \xrightarrow{w} (u', v') \xrightarrow{w'} (r, s),$$

then there are paths $p \xrightarrow{w} u \xrightarrow{w'} r$, $p \xrightarrow{w} u' \xrightarrow{w'} r$ and $q \xrightarrow{w} v \xrightarrow{w'} s$, $q \xrightarrow{w} v' \xrightarrow{w'} s$ in $\mathcal{A}$ implying $u = u'$ and $v = v'$.

We have already seen in Proposition 6.1 that if σ is a morphism which is recognizable for aperiodic points, then it is injective or periodic.

The size of an automaton is the sum of the number of states and the number of edges of the automaton.

PROPOSITION 7.1. *Let $\mathcal{A}$ be an unambiguous strongly connected automaton. Then $\mathcal{A}$ is unambiguous for aperiodic points if and only if the following conditions are satisfied.*
  (i)   *Every non-trivial strongly connected component of $\mathcal{A} \times \mathcal{A}$ out of the diagonal is reduced to a cycle.*
  (ii) *There is no path between two non-trivial strongly connected components of $\mathcal{A} \times \mathcal{A}$.*
All these conditions can be checked in a quadratic time in the size of $\mathcal{A}$.

Proof. Since $\mathcal{A}$ is unambiguous, $\mathcal{A} \times \mathcal{A}$ is unambiguous. Note that the set of diagonal states is a non-trivial strongly connected component of $\mathcal{A} \times \mathcal{A}$. It cannot contain non-diagonal states since $\mathcal{A}$ is unambiguous.

We first show that the conditions are necessary. Let C be a non-trivial strongly connected component of $\mathcal{A} \times \mathcal{A}$ which is non-diagonal. Let π be a simple cycle labeled by u around (p, q) with $p \neq q$ in C and another cycle π' which is not a power of π around (p, q) labeled by v. Since $\mathcal{A} \times \mathcal{A}$ is unambiguous, u and v are not a power of the same word. Thus, there is a two-sided infinite sequence x which is a concatenation of words u and v which is not periodic. This sequence is the label of a two-sided infinite path of $\mathcal{A} \times \mathcal{A}$ going through (p, q) after reading u or v. Since $p \neq q$, this leads to two distinct paths labeled by x in $\mathcal{A}$ and thus $\mathcal{A}$ is not unambiguous for aperiodic points.

Let C and C' be two non-trivial non-diagonal strongly connected components of $\mathcal{A} \times \mathcal{A}$. Then C and C' are reduced to a cycle. Let $(p, q) \in C$ with $p \neq q$ and $(r, s) \in C'$ with $r \neq s$, let π be a simple cycle labeled by u around (p, q), and π' be a simple cycle labeled by v around (r, s). Let us assume that there is a path from (p, q) to (r, s) labeled by w in $\mathcal{A} \times \mathcal{A}$. Assume that u and v are not powers of two conjugate words, then the two-sided infinite word $x = {}^{\omega}uwv^{\omega}$ is aperiodic and $\mathcal{A}$ is not unambiguous for aperiodic points. Assume now that $u = (rs)^k$ and $v = (sr)^{k'}$ with rs primitive. The word $x = {}^{\omega}uwv^{\omega}$ is periodic if and only if $w \in (rs)^* r$. However, in this case, if $w = (rs)^m r$, the word $(rs)^{kk'}(rs)^m r = (rs)^m r(sr)^{kk'}$ is the label of two distinct paths from (p, q) to (r, s) which is impossible since $\mathcal{A} \times \mathcal{A}$ is unambiguous.

Let us now assume that the strongly connected component of diagonal points is connected to a non-trivial non-diagonal strongly connected component. For instance, if there is a path labeled by w from a state (p, p) to a state (q, r) with $q \neq r$ belonging to an non-trivial strongly connected component.

Assume that the graph of $\mathcal{A}$ is not reduced to one cycle. Then there are a simple cycle π around (p, p) labeled u and another cycle π' around (p, p) labeled v which is not a power of π. The words u and v are not a power of a same word. Hence, there is a left-infinite word y being a concatenation of words u and v labeling a path ending in (p, p) and which is not ultimately periodic. Let z be the label of a cycle around (q, r). Then ywz^{ω} is an aperiodic point labeling two distinct paths of $\mathcal{A}$.

If $\mathcal{A}$ is reduced to one cycle, there is no path from a diagonal state to a non-diagonal one in $\mathcal{A} \times \mathcal{A}$. Thus, if condition (ii) is not satisfied, $\mathcal{A}$ is not unambiguous for aperiodic points.

We now show that the conditions are sufficient. We show that if all conditions hold, $\mathcal{A}$ is unambiguous for aperiodic points. Let x be an aperiodic point which is the label of two distinct paths of $\mathcal{A}$. Then there is a two-sided infinite path $(p_i, q_i)_{i \in \mathbb{Z}}$ in $\mathcal{A} \times \mathcal{A}$ labeled by x such that $(p_i)_{i \in \mathbb{Z}} \neq (q_i)_{i \in \mathbb{Z}}$. Without loss of generality, we may assume that $p_0 \neq q_0$. There is an infinite number of $i < 0$ such that $(p_i, q_i) = (p, q)$ for some states p, q. There is also an infinite number of $j > 0$ such that $(p_j, q_j) = (r, s)$ for some states r, s. We cannot have $p = q$ and $r = s$ since $\mathcal{A}$ is unambiguous.

Assume that $p = q$. Then, $r \neq s$ and there is a path from (p, p) to the non-trivial strongly connected component of (r, s) which is forbidden. Similarly, it is impossible to have $r = s$ and $p \neq q$.
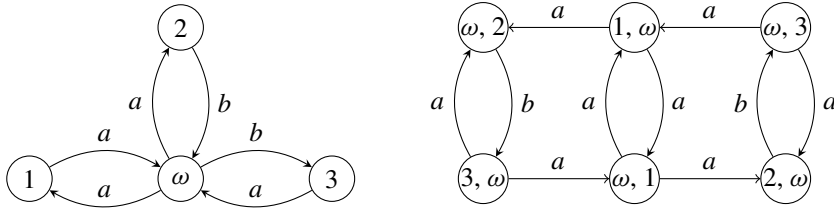
FIGURE 10. The automata $\mathcal{A}$ and $\mathcal{A} \times \mathcal{A}$.

Assume now that $p \neq q$ and $r \neq s$. If the strongly connected components of (p, q) and (r, s) are distinct, then there is a path between these two non-trivial components which is forbidden. If the components of (p, q) and (r, s) are the same, then x is periodic, which is a contradiction.

The conditions can be checked in time $O(n^2)$, where n is the size of $\mathcal{A}$. □

Example 7.2. Let us consider again the morphism $\sigma : a \mapsto aa, b \mapsto ab, c \mapsto ba$ of Example 3.5. The flower automaton $\mathcal{A}$ of $\sigma(A)$ is represented in Figure 10 on the left. The non-diagonal part of the automaton $\mathcal{A} \times \mathcal{A}$ has a strongly connected component, which is represented on the right. This component is not reduced to a cycle and thus condition (i) is not satisfied, which is consistent with the fact that σ is not recognizable for aperiodic points, as we have seen in Example 3.5.

Note that Proposition 7.1 gives an easy proof of Proposition 4.6. Indeed, if $\sigma : A^* \to B^*$ is left marked, let $\mathcal{A}$ be the flower automaton of $\sigma(A)$. Since σ is left marked, $\mathcal{A}$ is deterministic and thus $\mathcal{A} \times \mathcal{A}$ is also. Note that if $p \neq \omega$, there is at most one edge going out of p in $\mathcal{A}$.

Thus, if (p, q) is a state of $\mathcal{A} \times \mathcal{A}$ with p or q distinct from ω, there is at most one edge going out of (p, q) in $\mathcal{A} \times \mathcal{A}$. Further, since $\mathcal{A}$ is deterministic, there is no edge from a diagonal state to a non-diagonal one in $\mathcal{A} \times \mathcal{A}$.

As a consequence, each non-trivial strongly connected component of $\mathcal{A} \times \mathcal{A}$ out of the diagonal is reduced to a cycle and there is no path between two non-trivial strongly connected components of $\mathcal{A} \times \mathcal{A}$. Hence, σ is recognizable for aperiodic points.

We define the size of a finite set of words as the sum of the lengths of words of the set.

COROLLARY 7.3. *It can be checked in quadratic time in the size of $\sigma(A)$ whether an injective morphism $\sigma : A^* \to B^*$ is recognizable for aperiodic points.*

Proof. The flower automaton of $\sigma(A)$ is unambiguous and strongly connected. The result follows directly from Proposition 7.1. The algorithm runs in time $O(n^2)$, where n is the size of $\sigma(A)$ that is the sum of the lengths of the words of $\sigma(A)$. □

References

[1] N. Aubrun and M. Sablik. Simulation of effective subshifts by two-dimensional subshifts of finite type. *Acta Appl. Math.* **126** (2013), 35–63.

[2] N. Aubrun and M. Sablik. Multidimensional effective *S*-adic systems are sofic. *Unif. Distrib. Theory* **9**(2) (2014), 7–29.

[3] M.-P. Béal, D. Perrin and A. Restivo. Unambiguously coded systems. *European J. Combin.*, to appear, *Preprint*, 2021, arXiv:2103.01012.

[4] J. Berstel, D. Perrin, J.-F. Perrot and A. Restivo. Sur le théorème du défaut. *J. Algebra* **60**(1) (1979), 169–180.

[5] J. Berstel, D. Perrin and C. Reutenauer. *Codes and Automata*. Cambridge University Press, Cambridge, 2009.

[6] V. Berthé, W. Steiner, J. M. Thuswaldner and R. Yassawi. Recognizability for sequences of morphisms. *Ergod. Th. & Dynam. Sys.* **39**(11) (2019), 2896–2931.

[7] S. Bezuglyi, J. Kwiatkowski and K. Medynets. Aperiodic substitution systems and their Bratteli diagrams. *Ergod. Th. & Dynam. Sys.* **29**(1) (2009), 37–72.

[8] S. Donoso, F. Durand, A. Maass and S. Petite. Interplay between finite topological rank minimal Cantor systems, *S*-adic subshifts and their complexity. *Trans. Amer. Math. Soc.* **374** (2021), 3453–3489.

[9] F. Durand and D. Perrin. *Dimension Groups and Dynamical Systems*. Cambridge University Press, Cambridge, 2022.

[10] A. Ehrenfeucht and G. Rozenberg. Elementary homomorphisms and a solution of the DOL sequence equivalence problem. *Theoret. Comput. Sci.* **7**(2) (1978), 169–183.

[11] J. Karhumäki, J. Maňuch and W. Plandowski. A defect theorem for bi-infinite words. *Theoret. Comput. Sci.* **292**(1) (2003), 237–243. Selected Papers in honor of J. Berstel.

[12] P. Kurka. *Topological and Symbolic Dynamics (Cours Spécialisés [Specialized Courses], 11)*. Société Mathématique de France, Paris, 2003.

[13] R. Kyriakoglou. Recognizable substitutions. *PhD Thesis*, Université Paris Est, 2019.

[14] D. Lind and B. Marcus. *An Introduction to Symbolic Dynamics and Coding (Cambridge Mathematical Library)*, 2nd edn. Cambridge University Press, 2021.

[15] M. Linna. The decidability of the DOL prefix problem. *Int. J. Comput. Math.* **6**(2) (1977), 127–142.

[16] M. Lothaire. *Algebraic Combinatorics on Words (Encyclopedia of Mathematics and its Applications, 90)*. Cambridge University Press, Cambridge, 2002.

[17] J. C. Martin. Minimal flows arising from substitutions of non-constant length. *Math. Syst. Theory* **7** (1973), 72–82.

[18] B. Mossé. Puissances de mots et reconnaissabilité des points fixes d'une substitution. *Theoret. Comput. Sci.* **99**(2) (1992), 327–334.

[19] B. Mossé. Reconnaissabilité des substitutions et complexité des suites automatiques. *Bull. Soc. Math. France* **124**(2) (1996), 329–346.

[20] S. Mozes. Tilings, substitution systems and dynamical systems generated by them. *J. Anal. Math.* **53**(1) (1989), 139–186.

[21] D. Perrin and J.-E. Pin. *Infinite Words: Automata, Semigroups, Logic and Games*. Elsevier, Amsterdam, 2004.

[22] D. Perrin and G. Rindone. On syntactic groups. *Bull. Belg. Math. Soc. Simon Stevin* **10**(suppl.) (2003), 749–759.

[23] D. Perrin and A. Ryzhikov. The degree of a finite set of words. *Proc. 40th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2020, December 14–18, 2020, BITS Pilani, K K Birla Goa Campus, Goa, India (Virtual Conference) (LIPIcs, 182)*. Eds. N. Saxena and S. Simon. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2020, pp. 54:1–54:16.

[24] D. Perrin and A. Ryzhikov. The degree of a finite set of words. *Preprint*, 2022, arXiv:2106.14471.

[25] M. Queffélec. *Substitution Dynamical Systems—Spectral Analysis (Lecture Notes in Mathematics, 1294)*, 2nd edn. Springer-Verlag, Berlin, 2010.

[26] A. Restivo. On a question of McNaughton and Pappert. *Inform. Control* **25** (1974), 1.

[27] M.-P. Schützenberger. A property of finitely generated submonoids of free monoids. *Algebraic Theory of Semigroups*. Ed. G. Pollak. North-Holland, Amsterdam, 1979, pp. 545–576.

[28] B. Solomyak. Nonperiodicity implies unique composition for self-similar translationally finite tilings. *Discrete Comput. Geom.* **20**(2) (1998), 265–279.