Codes and sofic constraints

Marie-Pierre Béal* Dominique Perrin*

January 14, 2005

Abstract

We study the notion of a code in a sofic subshift. We first give a generalization of the Kraft-McMillan inequality to this case. We then prove that the polynomial of the alphabet in an irreducible sofic shift divides the polynomial of any finite code which is complete for this sofic shift. This settles a conjecture from Reutenauer.

1 Introduction

There is a rich and fruitful interplay between two theories which arose at first independently. One is the theory of automata and formal languages, born in the context of theoretical computer science. The other one is symbolic dynamics which arose from the theory of dynamical systems in topology and probability theory. The theory of variable-length codes is one of the contact points between these domains, with a counterpart in symbolic dynamics in renewal systems and finite-to-one maps. Antonio Restivo has initiated in [6] a new direction by studying systematically the notion of a code in a subshift of finite type. In particular, he has studied the relationship between maximal and complete codes, with results that essentially extend those known in the case of the free monoid, or equivalently the full shift in symbolic dynamics.

In this paper, we continue this exploration. First of all, we adopt a definition which is not exactly the same one. To be more specific, we consider a sofic shift S and a subset X of the set F_S of factors of S. We consider such a set X which is a code. Observe that we do not require, as in [6] and [7] that $X^* \subset F_S$. This modifies the subsequent notions of an S-complete or S-maximal code. Actually, our notion has also connections with the definition of a code in a graph introduced by Christophe Reutenauer in [8], as we shall see below. The case of bifix codes was studied by Clelia De Felice in [3]. Codes in subshifts have also a connection with the study of permutation groups in syntactic semigroups (see [5]).

We first show that one may generalize to this situation the classical Kraft-McMillan inequality. In fact, we associate to each set X of words a series $p_X(z)$

*Institut Gaspard-Monge, Université de Marne-la-Vallée, 77454 Marne-la-Vallée Cedex 2, France. {beal,perrin}@univ-mlv.fr

which, in the case where S is the full shift, reduces to the generating series of the words of X by length, *i.e.* $p_X(z) = \sum_{n\geq 1} u_n z^n$ where u_n is the number of words of length n in X. Let $h(S)$ be the entropy of S and let ρ_S be such that $h(S) = -\log(\rho_S)$. The precise definition of the entropy is given in the next section. It uses a logarithm and the same basis has to be used in both definitions of ρ_S and $h(S)$. In particular, $\rho_S = 1/k$ when S is the full shift on k symbols. We prove that if X is a code, then $p_X(\rho_S) \leq 1$. Actually, we obtain this result as a corollary of a more general one, corresponding to an assignment of real values to the letters generalizing the notion of a Bernoulli distribution (Theorem 1). We say that X is S-complete if $X \subset F_S \subset F(X^*)$, where $F(X^*)$ denotes the set of factors of the words in X^*. We prove that when X is regular, then $p_X(\rho_S) = 1$ if and only if X is S-complete. This is again obtained as a corollary of a more general result (Theorem 2).

We prove in a second part of the paper a generalization of a result of [8] concerning a multivariate polynomial $p(X)$ associated with a code X, called the *determinant of the code*. It says that, for a finite S-complete code, where S is an irreducible sofic shift, this polynomial is divisible by the polynomial $p(A)$. The proof uses the results of the previous section, in contrast with the algebraic arguments of [8] using the notion of syntactic category, a generalization of the syntactic semigroup.

2 Codes and sofic shifts

Let A be a finite alphabet. We denote by A^* the set of finite words and by $A^{\mathbb{Z}}$ the set of bi-infinite words on A. A *subshift* is a closed subset S of $A^{\mathbb{Z}}$ which is invariant by the shift transformation σ (*i.e.* $\sigma(S) = S$) defined by $\sigma((a_i)_{i\in\mathbb{Z}}) = (a_{i+1})_{i\in\mathbb{Z}}$.

A finite *automaton* is a finite multigraph labeled by a finite alphabet A. It is denoted $\mathcal{A} = (Q, E)$, where Q is a finite set of states, and E a finite set of edges labeled by A. A *sofic shift* is the set of labels of all bi-infinite paths on a finite automaton. A sofic shift is *irreducible* if there is such a finite automaton with a strongly connected graph. If $\mathcal{A}$ is deterministic, for any state $p \in Q$ and any word u, there is at most one path labelled u and going out of p. We denote by $p \cdot u$ the target of this path when it exists. Irreducible sofic shifts have a unique (up to isomorphisms of automata) *minimal deterministic automaton*, that is a deterministic automaton having the fewest states among all deterministic automata representing the shift. This automaton is called the *right Fischer cover* of the shift. A *subshift of finite type* is defined as the bi-infinite words on a finite alphabet avoiding a finite set of finite words. It is a sofic shift. An *edge shift* is the set of the labels of all bi-infinite paths on a finite automaton where all edges have distinct labels. The *full shift* on the finite alphabet A is the set of all bi-infinites sequences on A, *i.e.* $A^{\mathbb{Z}}$.

Let S be a subshift on the alphabet A. We denote by F_S the set of finite factors, or blocks, of words in S. We denote by $h(S)$ the entropy of a S. It is equal to entropy $h(L)$ of the language $L = F_S$, where

$$h(L) = \limsup_{n\to\infty} \frac{1}{n} \log \operatorname{Card}(L \cap A^n).$$

We denote by ρ_S the unique positive real number such that $h(S) = \log(1/\rho_S)$. The positive real number ρ_S is the convergence radius of the generating series of L by length.

Example 1 If S be the full shift on A, then $\rho_S = 1/\operatorname{Card}(A)$.

Example 2 Let S be the irreducible subshift of finite type on $A = \{a, b\}$ defined by the finite set of forbidden sequences $I = \{bb\}$. It is the so-called *golden mean system*, and ρ_S is the inverse of the golden mean, solution of $\rho_S^2 = 1 - \rho_S$. The right Fischer cover of S is represented on Figure 1.

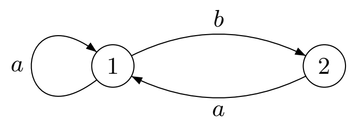

Figure 1: The golden mean system.

A set of finite words X on an alphabet A is a *code* if and only if whenever $x_1x_2\ldots x_n = y_1y_2\ldots y_m$, where $x_i, y_j \in X$ and n, m are positive integers, one has $n = m$ and $x_i = y_i$ for $1 \le i \le n$. If X is set of finite words on a finite alphabet, X^* denotes all finite concatenations of words of X.

Let S be a sofic shift. A set X on the alphabet A is said to be *complete* in S, or S-*complete*, if $X \subset F_S$, and any word in F_S is a factor of a word in X^*. Observe that we do not require that $X^* \subset F_S$.

A code X is S-*maximal* if $X \subset F_S$ and it is maximal for this property.

Let S be an irreducible sofic shift over the alphabet A. Let (Q, E) be its right Fischer cover. Let μ be the morphism from A^* into the monoid of $Q \times Q$ matrices over the monoid $A^* \cup \{0\}$ defined as follows. For each word u, the matrix $\mu(u)$ is defined by

$$\mu(u)_{pq} = \begin{cases} u & \text{if } p \cdot u = q \\ 0 & \text{otherwise.} \end{cases}$$

The elements of the matrix $\mu(u)$ can be considered as subsets of A^*, interpreting 0 as the empty set. The morphism μ can be extended to the semiring $\mathfrak{P}(A^*)$ of subsets of A^* by linearity. Thus, it becomes a morphism from $\mathfrak{P}(A^*)$ to the semiring of $Q \times Q$ matrices on $\mathfrak{P}(A^*)$.

For any subset X of A^*, we have

$$\mu(X^n) = \mu(X)^n,$$

and

$$\mu(X^*) = \sum_{n\geq 0} \mu(X^n).$$

We denote by π an assignment of positive real values to the elements of A. We extend it to a semigroup morphism from $A^* \cup \{0\}$ to $\mathbb{R}$.

We denote by $u \mapsto f_u(z)$ the morphism from A^* into the monoid of $Q \times Q$ matrices with coefficients in the polynomial ring $\mathbb{R}[z]$, defined for each word w by

$$f_u(z)_{pq} = \begin{cases} \pi(u)z^{|u|} & \text{if } p \cdot u = q \\ 0 & \text{otherwise.} \end{cases}$$

If U is a set of words, we denote by $f_U(z)$ the matrix whose coefficients are real power series defined by

$$f_U(z) = \sum_{u\in U} f_u(z).$$

Actually, $f_U(z)$ can also be considered as a series whose coefficients are real matrices. In this sense, we will talk about the radius of convergence of $f_U(z)$ and denote it by $\rho(f_U(z))$. It is the minimum of the radii of convergence of its elements when viewed as a matrix.

Note that, for a set of words U, the elements of the matrix $f_U(z)$ are obtained from the elements of $\mu(U)$ as the generating series of the values by π. More precisely

$$f_U(z)_{pq} = \sum \pi(u)z^{|u|},$$

where the sum runs over all $u \in \mu(U)_{pq}$.

If X is a code, then

$$f_{X^n}(z) = (f_X(z))^n,$$

and

$$f_{X^*}(z) = (I - f_X(z))^{-1}.$$

We consider the polynomial $d(z) = \det(I - f_A(z))$. We say that an assignment π is *admissible* if the following condition is satisfied: the value $z = 1$ is a root of $d(z)$ and $|\theta| \geq 1$ for any other root θ.

There is always at least one admissible assignment for each nonempty alphabet. For instance, one can show that the assignment defined by $\pi(a) = \rho_S$ for any $a \in A$ is admissible (see for example [4]).

An admissible assignment can be seen as a generalization of a Bernoulli distribution on the alphabet. Actually, when S is the full shift on A, both definitions coincide. Indeed, in this case, $f_A(1) = \sum_{a\in A} \pi(a)$ and thus π is admissible if and only if $\sum_{a\in A} \pi(a) = 1$.

Note that, when π is admissible, the radius of convergence of $f_{A^*}(z)$ is 1. Indeed, for every complex number z such that $|z| < 1$, $\det(I - f_A(z)) \neq 0$ and thus $f_{A^*}(z)$ converges.

The following example describes the admissible assignments in the case of the golden mean system.

Example 3 We consider again the golden mean system of Example 2. The morphism μ is defined by:

$$\mu(a) = \begin{bmatrix} a & 0 \\ a & 0 \end{bmatrix}, \qquad \mu(b) = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}.$$

Let $\pi(a) = p$, $\pi(b) = q$. We have

$$f_a(z) = \begin{bmatrix} pz & 0 \\ pz & 0 \end{bmatrix}, \qquad f_b(z) = \begin{bmatrix} 0 & qz \\ 0 & 0 \end{bmatrix}, \qquad f_A(z) = \begin{bmatrix} pz & qz \\ pz & 0 \end{bmatrix}.$$

Hence $d(z) = 1 - pz - pqz^2$. Thus π is admissible if and only if $p(1+q) = 1$. In particular, $\pi(a) = \pi(b) = \rho_S$ is admissible.

Our first result is the following statement.

Theorem 1 *Let S be an irreducible sofic shift and let π be an admissible assignment. If $X \subset A^+$ is a code, then the series $f_X(z)$ converges for $z = 1$ and* $\det(I - f_X(1)) \geq 0$.

Proof Let $\mathcal{A} = (Q, E)$ be the right Fischer cover of S. For any two states $p, q \in Q$, $\mu(X^*)_{pq} \subseteq \mu(A^*)_{pq}$. Thus $\rho(f_{X^*}(z)) \geq \rho(f_{A^*}(z))$. Since π is admissible, $\rho(f_{A^*}(z)) = 1$. It follows that $\rho(f_{X^*}(z)) \geq 1$. Since X is a code, $f_{X^*}(z) = (I - f_X(z))^{-1}$. Thus $\det(I - f_X(z)) \neq 0$ for $0 \leq z < 1$. Since $\det(I - f_X(0)) = 1$, we obtain $\det(I - f_X(z)) \geq 0$ for $0 \leq z < 1$ by continuity. Again by continuity we conclude that $\det(I - f_X(1)) \geq 0$. $\square$

Example 4 Let S be the golden mean system and let $X = \{aa, ab\}$. Let $\pi(a) = p$, $\pi(b) = q$ be an admissible assignment, *i.e.* such that $p(1+q) = 1$. We have

$$f_X(z) = \begin{bmatrix} p^2 z & pqz^2 \\ p^2 z & pqz^2 \end{bmatrix}.$$

Hence $\det(I - f_X(1)) = 1 - p^2 - pq$ which is at most equal to 1.

We will now prove a complement to Theorem 1 describing the equality case. The proof uses the following lemma stating a classical property on regular languages. If u is word and L a set of finite words, $u^{-1}L$ denotes the set $\{w \in A^* \mid uw \in L\}$.

Lemma 1 *If L is a regular language of finite words, then there is a finite subset P of A^* such that the set of factors $F(L)$ of L satisfies $F(L) \subseteq \bigcup_{v,w \in P} v^{-1}Lw^{-1}$.*

Proof Let $\mathcal{A} = (Q, I, T, E)$ be a finite automaton recognizing the language L with I the set of initial states, T the set of terminal states, and E the set of edges. We may assume that, for each state $q \in Q$, there exist $(i, t) \in I \times T$ and two words v_q, w_q such that $i \xrightarrow{v_q} q \xrightarrow{w_q} t$. For each word $u \in F(L)$, there exist $p, q \in Q$ such that $p \xrightarrow{u} q$. Thus $v_p u w_q \in L$. This shows that $F(L) \subseteq \bigcup_{p,q \in Q} v_p^{-1} L w_q^{-1}$. $\square$

Theorem 2 *Let S be an irreducible sofic shift and let π be an admissible assignment. If $X \subset F_S$ is a regular code, then X is S-complete if and only if* $\det(I - f_X(1)) = 0$.

Proof Let $\mathcal{A} = (Q, E)$ be the right Fischer cover of S. Let p be a state of $\mathcal{A}$. If X is S-complete, any word u in F_S with $p \cdot u = p$ is a factor of a word in X^*. If u is factor of word in X, then there are states $s, t \in Q$ such that u is factor of a word in $\mu(X)_{st}$, since $X \subset F_S$. If u is not factor of a word in X, by considering the words u^n, for $n \geq 1$, we get that u is factor of some word in $\mu(X^*)_{st}$, for some states $s, t \in Q$. It follows that, in any case, there are two states $s, t \in Q$ such that u is factor of a word in $\mu(X^*)_{st}$. Since X is regular, $\mu(X^*)_{st}$ is also regular. It follows from Lemma 1 that, for each $p \in Q$, there is a finite set of words U such that

$$\mu(A^*)_{pp} \subset \bigcup_{s,t \in Q} \bigcup_{v,w \in U} v^{-1}\mu(X^*)_{st}w^{-1}.$$

For any $s, t \in Q$, any $v, w \in A^*$,

$$\rho(f_{v^{-1}\mu(X^*)_{st}w^{-1}}(z)) \geq \rho(f_{\mu(X^*)_{st}}(z)) \geq \rho(f_{X^*}(z)).$$

Thus $\rho(f_{A^*}(z)) \geq \rho(f_{X^*}(z))$. Since π is admissible, $\rho(f_{A^*}(z)) = 1$. By Theorem 1, $\rho(f_{X^*}(z)) \geq 1$. Hence $\rho(f_{X^*}(z)) = 1$.

Since X is a regular code, for any two states $p, q \in Q$, $f_{X^*}(z)_{pq}$ is a rational series with nonnegative real coefficients. By Lemma [2, Lemma 2.3 pp.82], either $f_{X^*}(z)_{pq}$ is a polynomial, or the minimal modulus of the poles of $f_{X^*}(z)_{pq}$ is itself a pole. Since $f_{X^*}(z) = (I - f_X(z))^{-1}$, it follows that $\det(I - f_X(z))$ vanishes at 1.

Conversely, let us assume that X is not S-complete. There is a word $u \in F_S$ such that u is not factor of any word in X^*. Thus $X^* \subseteq A^* - A^*uA^*$.

Because S is irreducible and π assigns a positive real value to each letter, the matrix $f_A(1)$ is an irreducible nonnegative real matrix. Thus, it follows from Proposition [4, Theorem 4.4.7] that, for $p, q \in Q$, $\rho(f_{A^*-A^*uA^*}(z)_{pq}) > \rho(f_{A^*}(z)_{pq})$.

We get that, for any states $p, q \in Q$,

$$1 = \rho(f_{A^*}(z)) \leq \rho(f_{A^*}(z)_{pq}) < \rho(f_{A^*-A^*uA^*}(z)_{pq}) \leq \rho(f_{X^*}(z)_{pq}).$$

Hence $\rho(f_{X^*}(z)) > 1$. This implies that $\det(I - f_X(1)) > 0$. $\square$

We now derive from Theorem 1 and Theorem 2 two corollaries which constitute a generalization of the Kraft-McMillan inequality. Let π be the admissible assignment defined by $\pi(a) = \rho_S$ for any $a \in A$. For a subset X of A^*, we denote for convenience

$$p_X(z) = 1 - \det(I - f_X(z/\rho_S)).$$

Thus $p_X(\rho_S) = 1 - \det(I - f_X(1))$. When S is the full shift on k symbols $\rho_S = 1/k$ and $p_X(z) = \sum_{n \geq 1} u_n z^n$, where u_n is the number of words of length

n in X. Thus the inequality $p_X(\rho_S) \leq 1$ takes the form $\sum_{n\geq 1} u_n k^{-n} \leq 1$, which is the Kraft-McMillan inequality.

Corollary 3 *Let S be an irreducible sofic shift. If $X \subset A^+$ is a code, then $p_X(\rho_S) \leq 1$.*

Corollary 4 *Let S be an irreducible sofic shift and let $X \subset F_S$ be a regular code. The code X is S-complete if and only if $p_X(\rho_S) = 1$.*

The following examples illustrate the different possible cases. The first two ones give examples of S-complete codes.

Example 5 Let S be the golden mean system. The set $X = a + ab$ is both a code and an S-complete set. We have $p_X(z) = z + z^2$ and thus $p_X(\rho_S) = 1$.

Example 6 Let S be the golden mean system again. Let $X = aa + ab + ba$. The set X is an S-complete code since it is formed of all factors of length 2 of S. We have

$$p_X(z) = 3z^2 - z^4,$$

and

$$p_X(\rho_S) = 3\rho_S^2 - \rho_S^4 = 1.$$

The last example shows a case of a code which is not S-complete.

Example 7 Let S be the even system represented on Figure 2. The set $X =$

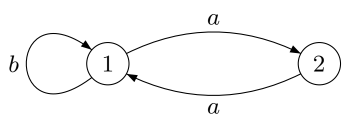

Figure 2: The even system.

$b(a^2)^*b$ is a code. It is not S-complete. The value of ρ_S is the same as for the golden mean system. We have

$$f_X(z/\rho_S) = \begin{bmatrix} z^2(z^2)^* & 0 \\ 0 & 0 \end{bmatrix},$$

and $p_X(z) = 1 - (1 - z^2(z^2)^*) = 1 - (1 - \frac{z^2}{1-z^2}) = \frac{z^2}{1-z^2}$. Hence $p_X(\rho_S) = \frac{2}{1+\sqrt{5}} < 1$.

We briefly investigate the relation between the extremal properties of being S-complete and S-maximal. It is shown in [7] (and it is also a consequence of a result of [1]) that, when S is a subshift of finite type, any S-maximal code is S-complete (with the definitions of an S-code given in [7]). The result still holds for shifts of finite type with our definitions of S-maximal and S-complete codes.

Conversely, there is an example in [8] of an S-complete code which is not S-maximal. Indeed, consider the shift S described in Figure 3. The code $X = \{ab\}$

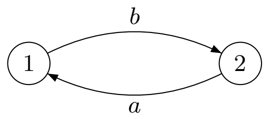

Figure 3: A shift of null entropy.

is S-complete and not S-maximal since it is included in $\{ab, ba\}$.

3 Factorization

In this section, we consider the case where X is a finite code, and S is an irreducible sofic shift with $\mathcal{A}$ as right Fischer cover. We prove that the polynomial of the alphabet for S divides the polynomial of any finite code X which is complete for S. Both polynomials are defined below. This settles a conjecture from Reutenauer given in [8, pp. 150]. In [8, pp. 150], Reutenauer proves the same result when S is an edge shift satisfying a constraint called the condition (0): each state of its right Fischer cover has a loop.

Let us denote by α the morphism obtained from μ by taking the commutative image of the elements. For any finite code X, the polynomial $p(X) = \det(I - \alpha(X))$ is in $\mathbb{Z}[A]$, the set of polynomials over $\mathbb{Z}$ in the commuting variables a in A. The polynomial $\det(I - f_X(z))$ and $p_X(z)$ are of course closely related to $p(X)$. Indeed, for any point $\mathbf{x} = (\pi(a)z)_{a \in A}$, where π is an assignment, $\det(I - f_X(z)) = p(X)(\mathbf{x})$, where $p(X)(\mathbf{x})$ denotes the value of $p(X)$ at the point $\mathbf{x}$.

Theorem 5 *Let S be an irreducible sofic shift. When X is a finite S-complete code, the polynomial $p(X)$ is a multiple of the polynomial $p(A)$.*

Proof We first assume that S is an irreducible edge shift.

It is known that $\det(I - \alpha(A))$ is equal to

$$1 + \sum_{k \geq 1} (-1)^k \sum_{c_1 \dots c_k} \alpha(c_1) \dots \alpha(c_k),$$

where the second sum is over all simple cycling paths $c_1, \dots, c_k$ of S which do not share any state, two by two. If c is such a simple cycling path, $\alpha(c)$ denotes its label seen as a monomial of $\mathbb{N}[A]$. Since S is an irreducible edge shift, the partial degree of $p(A)$ in each letter is at most 1 and all its monomials have coefficients 1 or -1. Moreover, it is proven in [8, Theorem 3] that $p(A)$ is an irreducible polynomial of $\mathbb{Z}[A]$.

Let a be a letter appearing in a simple cycling path c with $\alpha(c) = au$, and $B = A - \{a\}$. Thus u is a word of commutative letters in B. It follows from the above remarks that

$$p(A) = -au(1-q) + 1 + r,$$

where q and r are polynomials in $\mathbb{Z}[B]$ with no constant term. The polynomials $p(X)$ and $p(A)$ can be seen as polynomials in a with coefficients in $\mathbb{Z}[B]$.

We now divide $p(X)$ by $p(A)$ in $\mathbb{Z}[A, \frac{1}{u(1-q)}]$. Thus

$$p(X) = p(A)\, s + t,$$

where s and t are polynomials in $\mathbb{Z}[A, \frac{1}{u(1-q)}]$ which are respectively the quotient and the rest of this division. The degree of t in a is zero. It follows that there is a positive integer n such that

$$p(X)(u(1-q))^n = p(A)\, s' + t',$$

with $s' \in \mathbb{Z}[A]$, $t' \in \mathbb{Z}[B]$.

Let π be an admissible assignment. We denote by $\boldsymbol{\pi}$ the point $\boldsymbol{\pi} = (\pi(a) = \rho_S)_{a \in A}$. Let $\mathbf{w} = (\pi(b) = \rho_S)_{b \in B}$. We get

$$p(A)(\boldsymbol{\pi}) = \det(I - \alpha(A))(\boldsymbol{\pi}) = \det(I - f_A(1)) = 0.$$

Hence $(au(1-q))(\boldsymbol{\pi}) = (1+r)(\boldsymbol{\pi})$, or

$$\rho_S = \frac{(1+r)(\mathbf{w})}{(u(1-q))(\mathbf{w})}.$$

We denote by $B(\mathbf{w}, \varepsilon)$ the ball of dimension $\mathrm{Card}(B)$ and radius $\varepsilon > 0$ centered at $\mathbf{w}$. A positive ball is a ball containing only points with positive coefficients. There is a positive ball $B(\mathbf{w}, \varepsilon)$ such that, for any point denoted $\mathbf{x} = (x_1, \ldots, x_{|B|})$ in $B(\mathbf{w}, \varepsilon)$, $\frac{(1+r)(\mathbf{x})}{(u(1-q))(\mathbf{x})} > 0$, and the assignment $\pi_{\mathbf{x}}$ defined by

$$\begin{aligned} \pi_{\mathbf{x}}(b) &= x_b \text{ if } b \in B, \\ \pi_{\mathbf{x}}(a) &= \frac{(1+r)(\mathbf{x})}{(u(1-q))(\mathbf{x})}, \end{aligned}$$

is admissible.

Indeed, since S is irreducible, by the Perron-Frobenius theorem, $z = 1$ is a simple root of $\det(I - f_A(z))$ with the assignment π. Moreover, the roots of modulus 1 are $e^{2i\pi/k}$ for $0 \leq k \leq m-1$, where m is a positive integer. By definition of $\pi_{\mathbf{x}}$, $z = 1$ is still a root of $\det(I - f_A(z))$ with the assignment $\pi_{\mathbf{x}}$. When $\mathbf{x}$ is close enough to $\mathbf{w}$, it is the single positive real root of modulus less than or equal to 1. Thus, again by the Perron-Frobenius theorem, any root of $\det(I - f_A(z))$ with the assignment $\pi_{\mathbf{x}}$ has a modulus greater than or equal to 1. Hence $\pi_{\mathbf{x}}$ is admissible.

By Theorem 2, $p(X)(\boldsymbol{\pi}) = 0$ and $p(A)(\boldsymbol{\pi}) = 0$ for any $\boldsymbol{\pi} = (\pi(a))_{a \in A}$ where π is an admissible assignment. We get that t' vanishes at any point in $B(\mathbf{w}, \varepsilon)$.

Because $B(\mathbf{w}, \varepsilon)$ has dimension $\mathrm{Card}(B)$, we conclude that t' vanishes, and $p(A)$ divides $p(X)(u(1-q)^n$. Since $p(A)$ is irreducible and has a monomial containing the letter a, $p(A)$ divides $p(X)$ in $\mathbb{Z}[A]$.

We now extend the result for irreducible edges shifts to irreducible sofic shifts.

Let S be an irreducible sofic shift and let $\mathcal{A}$ be its right Fischer cover. We denote by $\mathcal{A}'$ the automaton obtained from $\mathcal{A}$ as follows. For any $a \in A$, if there are m edges labelled by a in $\mathcal{A}$, one labels these edges by $a_1, \ldots, a_m$ respectively in $\mathcal{A}'$. We denote by A' the finite alphabet formed of the letters with indices. Since all edges of $\mathcal{A}'$ have distinct labels, $\mathcal{A}'$ is the right Fischer cover of an irreducible edge shift S'. We denote by φ the map assigning a to each a_i, for any $a \in A$, and its extension as a morphism from A'^* to A^*. Note that, for each path $p \xrightarrow{u} q$ in $\mathcal{A}$, there is a unique path $p \xrightarrow{u'} q$ in $\mathcal{A}'$ with $\varphi(u') = u$, since $\mathcal{A}$ is deterministic.

Let X be a finite S-complete code. We define the finite set of words X' as the set of labels v of all paths in $\mathcal{A}'$ such that $\varphi(v) \in X$.

We claim that X' is a code. Indeed, whenever $u'_1 u'_2 \ldots u'_r = v'_1 v'_2 \ldots v'_s$, with r, s positive integers, and $u'_i, v'_j \in X'$, we have

$$\varphi(u'_1)\varphi(u'_2)\ldots\varphi(u'_r) = \varphi(v'_1)\varphi(v'_2)\ldots\varphi(v'_s).$$

Since X is a code, $r = s$ and $\varphi(u'_i) = \varphi(v'_i)$ for any $1 \leq i \leq r$. It follows that $|u'_i| = |v'_i|$ for any $1 \leq i \leq r$ and finally $u'_i = v'_i$.

We claim that X' is a finite S'-complete code. Since $\mathcal{A}$ is a minimal deterministic automaton recognizing the sofic shift S, it has a strongly connected graph and a synchronizing word (or reset sequence) u. A synchronizing word in a deterministic automaton is a word u such that the cardinality of the set $Q \cdot u = \{p \cdot u \mid p \in Q\}$ is one. Hence $Q \cdot u = \{q_0\}$. Moreover u is the label of a path from p to q_0 in $\mathcal{A}$, where p is some state in Q.

Let w' be a factor in $F_{S'}$. There is path $q \xrightarrow{w'} r$ in $\mathcal{A}'$ and a path $q \xrightarrow{w} r$ in $\mathcal{A}$ with $\varphi(w') = w$. Let x, y and z be words of A^* labels of paths from q_0 to p, from q_0 to q, and r to p, respectively. Hence we have in $\mathcal{A}$ the path

$$q_0 \xrightarrow{x} p \xrightarrow{u} q_0 \xrightarrow{y} q \xrightarrow{w} r \xrightarrow{y} p \xrightarrow{u} q_0.$$

Since X is S-complete, $xuywzu$ is a factor of a word in X^*. Moreover, there are two states $s, t \in Q$ such that $xuywzu$ is factor of a word in $\mu(X^*)_{st}$ (see the beginning of proof of Theorem 2). As a consequence, and since u is synchronizing, there are words $g, h \in A^*$ such that

$$s \xrightarrow{g} q_0 \xrightarrow{y} q \xrightarrow{w} r \xrightarrow{z} p \xrightarrow{u} q_0 \xrightarrow{h} t$$

is a path in $\mathcal{A}$ labelled by a word in X^*. Let

$$s \xrightarrow{g''} q_0 \xrightarrow{y''} q \xrightarrow{w''} r \xrightarrow{z''} p \xrightarrow{u''} q_0 \xrightarrow{h''} t$$

be the unique path in $\mathcal{A}'$ such that $\varphi(l'') = l$ for $l = g, y, w, z, u$, and h. We have $g''y''w''z''u''h'' \in X'^*$. Moreover since $q \xrightarrow{w''} r$ and $q \xrightarrow{w'} r$ are paths in $\mathcal{A}'$ and $\varphi(w') = \varphi(w'')$, $w' = w''$. It follows that w' is factor of a word in X'^*.

Finally, we apply the result obtained in the case of irreducible edge shifts to S' and X'. It follows that $p(A')$ divides $P(X')$ in $\mathbb{Z}[A']$. By removing the indices of the letters in A' (or, equivalently, by applying φ), we obtain that $p(A)$ divides $P(X)$ in $\mathbb{Z}[A]$. $\square$

The following example illustrates Theorem 5 in the case of an irreducible edge shift.

Example 8 If S is the irreducible edge shift described in Figure 4, then

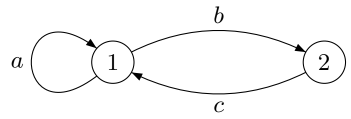

Figure 4: An edge shift.

$$\mu(a) = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}, \quad \mu(b) = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}, \quad \mu(c) = \begin{bmatrix} 0 & 0 \\ c & 0 \end{bmatrix}.$$

Let X be the finite S-complete code $\{aa, ab, ca, cb, bc\}$. We get

$$\mu(X) = \begin{bmatrix} a^2 + bc & ab \\ ca & cb \end{bmatrix}.$$

We have

$$\begin{aligned} p(X) &= 1 - a^2 - 2bc + b^2c^2 \\ &= (1 + a + bc)(1 - a - bc) \\ &= (1 + a + bc)\, p(A). \end{aligned}$$

The next example illustrates the proof of Theorem 5 in the case of an irreducible subshift of finite type which is not an edge shift.

Example 9 If S be the golden mean subshift, then

$$\mu(a) = \begin{bmatrix} a & 0 \\ a & 0 \end{bmatrix}, \quad \mu(b) = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}.$$

Let X be the finite S-complete code $X = \{aa, ab, aab\}$. The shift S' is recognized by the automaton of Figure 5. Note that S' is, up to a renaming of the alphabet, the edge shift of Example 8. We have $X' = \{a_1a_1, a_1b, a_1a_1b, a_2a_1, a_2b, a_2a_1b\}$,

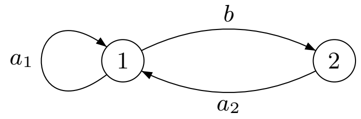

Figure 5: The edge shift S'.

and

$$\mu(X') = \begin{bmatrix} a_1a_1 & a_1b + a_1a_1b \\ a_2a_1 & a_2b + a_2a_1b \end{bmatrix}.$$

We get

$$\begin{aligned} p(X') &= (1 + a_1)(1 - a_1 - a_2b) \\ &= (1 + a_1)\, p(A'). \end{aligned}$$

As a consequence

$$\begin{aligned} p(X) &= (1 + a)\, p(A), \\ p(A) &= (1 - a - ab). \end{aligned}$$

We may observe that the factorization of $p(X)$ can be obtained from the following factorization of the matrix $(I - \mu(X))$:

$$I - \mu(X) = (I + \mu(a))(I - \mu(A))(I + \mu(b)).$$

This phenomenon is linked, in the case of the full shift, to Reutenauer's noncommutative factorization theorem [2]. We do not know whether this theorem holds for shifts of finite type.

The last example below shows an irreducible sofic shift S which is not a shift of finite type. We give an example of an S-complete code X for which there are two ways to find the factorization of $p(X)$.

Example 10 If S is the irreducible sofic shift described in Figure 6, then

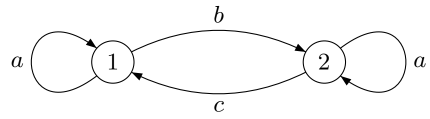

Figure 6: A sofic shift.

$$\mu(a) = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, \quad \mu(b) = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}, \quad \mu(c) = \begin{bmatrix} 0 & 0 \\ c & 0 \end{bmatrix}.$$

Let X be the finite S-complete code $\{aa, ab, ac, ba, bc, cb, ca\}$. We get

$$\mu(X) = \begin{bmatrix} a^2 + bc & ab + ba \\ ac + ca & a^2 + cb \end{bmatrix}.$$

We have

$$\begin{aligned} p(X) &= 1 - 2a^2 - 2bc + a^4 + b^2c^2 - 2a^2bc \\ &= (1 - 2a - bc + a^2)(1 + 2a + a^2 - bc) \\ &= p(A)(1 + 2a + a^2 - bc). \end{aligned}$$

From $1 - A^2 = (1 - A)(1 + A)$, we get

$$I - \mu(A^2) = (I - \mu(A))(I + \mu(A)).$$

It follows that

$$\det(I - \alpha(A^2)) = \det(I - \alpha(A))\det(I + \alpha(A)).$$

Since $\det(I - \alpha(A^2)) = p(X)$, $\det(I - \alpha(A)) = p(A)$, and $\mu(A) = \left(\begin{smallmatrix} a & b \\ c & a \end{smallmatrix}\right)$, we recover the factorization of $p(X)$:

$$\begin{aligned} p(X) &= \det(I - \alpha(A^2)) \\ &= \det(I - \alpha(A))\det(I + \alpha(A)) \\ &= p(A)(1 + 2a + a^2 - bc). \end{aligned}$$

Acknowledgment We thank an anonymous reviewer for constructive suggestions which helped us to improve the presentation of this article.

References

[1] J. Ashley, B. Marcus, D. Perrin, and S. Tuncel, *Surjective extensions of sliding-block codes*, SIAM J. Discrete Math., 6 (1993), pp. 582–611.

[2] J. Berstel and Ch. Reutenauer, *Rational Series and their Languages*, Springer-Verlag, 1988.

[3] C. De Felice, *Finite biprefix sets of paths in a graph*, Theoret. Comput. Sci., 58 (1988), pp. 103–128. Thirteenth International Colloquium on Automata, Languages and Programming (Rennes, 1986).

[4] D. A. Lind and B. H. Marcus, *An Introduction to Symbolic Dynamics and Coding*, Cambridge, 1995.

[5] D. Perrin and G. Rindone, *Syntactic groups*, Bulletin of the Belgium Mathematical Society, (2004). to appear.

[6] A. Restivo, *Codes and local constraints*, Theoret. Comput. Sci., 72 (1990), pp. 55–64.

[7] ———, *Codes with constraints*, in Mots, Lang. Raison. Calc., Hermès, Paris, 1990, pp. 358–366.

[8] Ch. Reutenauer, *Ensembles libres de chemins dans un graphe*, Bull. Soc. Math. France, 114 (1986), pp. 135–152.