Completing codes in a sofic shift

Marie-Pierre Béal, Dominique Perrin

Completing codes in a sofic shift

Marie-Pierre Béal[*,a], Dominique Perrin[*,a]

[a] *Université Paris-Est, LIGM CNRS, 77454 Marne-la-Vallée Cedex 2, France.*

Abstract

We define a code in a sofic shift as a set of blocks of symbols of the shift such that any block of the shift has at most one decomposition into code words. It is maximal if it is not strictly included in another one. Such a code is complete in the sofic shift if any block of the shift occurs within some concatenation of code words. We prove that a maximal code in an irreducible sofic shift is complete in this shift. We give an explicit construction of a regular completion of a regular code in a sofic shift. This extends the well known result of Ehrenfeucht and Rozenberg to the case of codes in sofic systems. We also give a combinatorial proof of a result concerning the polynomial of a code in a sofic shift.

Key words: automata and formal languages, codes, complete codes, sofic shifts, symbolic dynamics, variable length codes

1. Introduction

The classical notion of unique decipherability is defined on unconstrained words over a finite alphabet. It can be generalized to words satisfying some constraints. This generalization of the theory of (variable length) codes extends previous works of Reutenauer [1], Restivo [2] and Ashley *et al.* [3].

The main result of this paper is an extension of a classical result of Schützenberger [4] (see also [5]) relating the notions of completeness and maximality of codes. It is an extended version of the paper presented at the conference STACS'06 [6]. It is also the second part of a series of three contributions to the study of codes in sofic shifts [7], [6], and [8].

Let S be a sofic shift, *i.e.* the set of bi-infinite sequences of symbols labelling paths in a finite automaton. The set of factors of S, denoted by $\mathrm{Fact}(S)$, is the set of finite sequences of consecutive symbols (also called *blocks*) appearing in the elements of S. We call S-code a set of elements of $\mathrm{Fact}(S)$ such that any element of $\mathrm{Fact}(S)$ has at most one decomposition in code words. A set of words X is S-complete if any element of $\mathrm{Fact}(S)$ occurs within some concatenation of elements of X. An S-code is maximal if it is maximal for inclusion.

*Corresponding author

URL: `http://www.univ-mlv.fr/~beal` (Marie-Pierre Béal), `http://www.univ-mlv.fr/~perrin` (Dominique Perrin)

We prove that, for any irreducible sofic shift S, any maximal S-code is S-complete. Moreover, we give an effective embedding of a regular S-code into an S-complete one. This extends the well known theorem of Ehrenfeucht and Rozenberg [9] to codes in a sofic shift.

Our definition of S-codes generalizes the notion introduced by Restivo [2] and Ashley *et al.* [3]. In the first place, they consider subshifts of finite type instead of the more general notion of sofic shifts. Although shifts of finite type can also be described by a finite automaton, there is a real gap between the two classes, because representations of shifts of finite type have nice strong properties of synchronization that do not apply to sofic shifts in general. These properties are used to complete the codes. Secondly, they consider codes such that all concatenations of code words are in $\mathrm{Fact}(S)$, a condition that we do not impose. Our definition here is also slightly more general than the one used in our previous paper [7]. In fact, we only require the unique factorization for the words of $\mathrm{Fact}(S)$ and not for all products of code words. We think that this definition is more natural. The results of [7] all extend straightforwardly to this new class.

In the last section, we give a combinatorial proof of the main result of our previous paper [7] concerning the polynomial of a finite code. The proof is simpler and relates our result to the ones due to Williams [10] and Nasu [11].

The paper is organized as follows. We first recall some basic definitions from the area of symbolic dynamics and from the theory of codes. We introduce the notions of S-code, maximal S-code, and S-complete code when S denotes a sofic shift. In Section 3, we prove that any maximal S-code is S-complete. A combinatorial proof of the result of [7] is given in the last section.

2. Codes and Sofic Shifts

2.1. Sofic Shifts

Let A be a finite alphabet. We denote by A^* the set of finite words, by A^+ the set of nonempty 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 on 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. All states of such automata can be considered as both initial and final states.

A *sofic shift* is the set of labels of all bi-infinite paths in a finite automaton. We then say that the automaton *presents* or *accepts* the sofic shift. A sofic shift is *irreducible* if there is a finite automaton with a strongly connected graph. In this case the automaton also is said to be *irreducible*. An automaton $\mathcal{A} = (Q, E)$ is deterministic if, for any state $p \in Q$ and any word u, there is at most one path labeled by u and going out of p. When it exists, the target state of this path is denoted by $p \cdot u$. An automaton is *unambiguous* if there is at most one path labeled by u going from a state p to a state q for any given triple p, u, q.

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 presenting the shift. This automaton is called the *Fischer cover* of the shift (see [12, p. 98]). A *subshift of finite type* is defined as the set of bi-infinite words on a finite alphabet avoiding a finite set of finite words. It is a sofic shift. The *full shift* on the finite alphabet A is the set of all bi-infinite sequences on A, *i.e.* the set $A^{\mathbb{Z}}$.

The (topological) *entropy* of a sofic shift S is defined as

$$h(S) = \lim_{n\to\infty} \frac{1}{n} \log_2 s_n,$$

where s_n is the number of words of length n of $\mathrm{Fact}(S)$. The Fischer cover of a transitive sofic shift of null entropy is made of one cycle.

Example 1. Let S be the irreducible sofic subshift on $A = \{a, b\}$ defined by the automaton on the left of Figure 1. This automaton is the Fischer cover of S. This shift is the so-called *even system* since its bi-infinite sequences are those having an even number of b's between two a's. It is not a shift of finite type.

Let T be the irreducible shift on $A = \{a, b\}$ defined by the forbidden block bb. It is a shift of finite type. Its Fischer cover is given on the right of Figure 1. This shift is the so-called *golden mean system*.

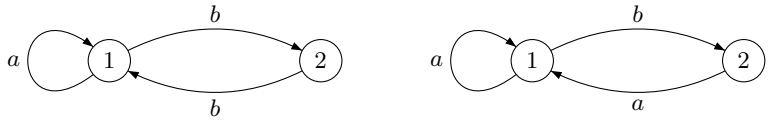

Figure 1: The Fischer covers of the even system S on the left, and of the golden mean system T on the right.

Let S be a subshift on the alphabet A. We denote by $\mathrm{Fact}(S)$ the set of finite factors (or blocks) of elements of S. Each element of $\mathrm{Fact}(S)$ is the label of a finite path in the Fischer cover of S.

Let $\mathcal{A}$ be a finite automaton. A word w is said to be a *synchronizing* word of $\mathcal{A}$ if w is the label of at least one path in $\mathcal{A}$ and any path labelled w ends in the same state depending only on w. If p denotes this state, one says that w *synchronizes* to p. For instance the words a, bab are synchronizing words of the Fischer cover of the even system. In the golden mean shift, which is a shift of finite type, each word of length 1, *i.e.* a or b, is a synchronizing word. For any Fischer cover of a shift of finite type S, there is a positive integer k such that any word of length k in $\mathrm{Fact}(S)$ is synchronizing.

Let L be a language of finite words. A word w is a *synchronizing* word of L if and only if whenever u, v are words such that uw and wv belong to L, one has uwv belongs to L. Note that if w is a synchronizing word of an automaton $\mathcal{A}$ recognizing a sofic shift S, it is a synchronizing word of the language $\mathrm{Fact}(S)$.

It is known that the Fischer cover of an irreducible sofic shift S has a synchronizing word (see for instance [12, Proposition 3.3.16]). If w is one of them, for any words u, v such that $uwv \in \mathrm{Fact}(S)$, uwv is also a synchronizing word.

2.2. Codes

Let S be a sofic shift. A set of finite words $X \subset \mathrm{Fact}(S)$ on an alphabet A is an *S-code* if and only if whenever $w = x_1x_2\dots x_n = y_1y_2\dots y_m$, where $x_i, y_j \in X$, n, m are positive integers, and $w \in \mathrm{Fact}(S)$, one has $n = m$ and $x_i = y_i$ for $1 \leq i \leq n$. Thus the classical definition of a code (also called a uniquely decipherable code) corresponds to the case where S is the full shift. Note that any code is an S-code but the converse is false as shown in the following example.

Example 2. The set $\{a, ab, ba\}$ is not a code since the block aba has two factorizations into codewords $a \cdot ba = ab \cdot a$. However it is not difficult to see that it is an S-code in the even system. Indeed, any word with two factorizations contains the block aba.

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 is an S-code and any word in $\mathrm{Fact}(S)$ is a factor of a word in X^*. For instance the code $X = \{a, bb\}$ is complete in the even system.

An S-code X is *maximal* if it is not strictly included in another S-code.

The following example of an S-complete code which is not maximal is given in [1]: Consider the shift of finite type S defined on the alphabet $A = \{a, b\}$ and avoiding the blocks aa and bb. The S-code $X = \{ab\}$ is S-complete but not maximal since X is strictly included in the S-code $Y = \{ab, ba\}$.

There is a connection between complete S-codes and a concept which has been studied in symbolic dynamics. This explains why the results proved in Section 4 are related with the results of Williams [10] and Nasu [11]. Let X be a complete S-code. Let $\mathcal{A} = (Q, E)$ be the Fischer cover of S. We build an automaton $\mathcal{B}$ computed from X and $\mathcal{A}$ as follows. The set of states of $\mathcal{B}$ is the union of the set of states Q of $\mathcal{A}$ and an additional set of dummy states. For each path in $\mathcal{A}$ labeled by a word in X going from a state p to a state q, we build a path in $\mathcal{B}$ from p to q with dummy states in-between. Let T be the subshift of finite type made of the bi-infinite paths of the graph of $\mathcal{B}$. The labelling of the paths in the automaton $\mathcal{B}$ defines a block map ϕ from T to S. The set X is an S-code if and only if ϕ is finite-to-one. It is S-complete if and only if ϕ is onto. Thus statements on complete S-codes can be reformulated as statements on finite-to-one factor maps between irreducible sofic shifts.

3. Completion of an S-Code

The following result generalizes the theorem of Ehrenfeucht and Rozenberg [9]. The proof uses the same type of construction as the original one, also used in the case of the extension to subshifts of finite type obtained in [3]. It requires however, as we shall see, a careful adaptation to extend to sofic shifts.

Theorem 1. *Let S be an irreducible sofic shift. If X is an S-code, there is an S-code Y such that $X \subseteq Y$ and Y is S-complete. If X is moreover regular, Y can be chosen regular.*

A nonempty word w of A^* is called *unbordered* if no proper nonempty left factor of w is a right factor of w. In other words, w is unbordered if and only if $w \in uA^+ \cap A^+u$ implies $u = \varepsilon$, where ε denotes the empty word.

Lemma 2 below provides the construction of an unbordered word in the set of factors of an irreducible sofic shift. It replaces the construction used in [5, Proposition 3.6] for the case of the full shift.

Lemma 2. *Let S be an irreducible sofic shift which has a positive entropy. Let z be a word in* $\mathrm{Fact}(S)$*. Then there is a word y in* $\mathrm{Fact}(S)$ *such that z is a factor of y and y is unbordered.*

Proof. Let $\mathcal{A}$ be a deterministic automaton presenting S.

Without loss of generality, one can assume that z is the label of a path from p to p in $\mathcal{A}$. Let C be the set of labels of first-return paths in $\mathcal{A}$ from p to p. Since the automaton $\mathcal{A}$ is deterministic, the set C is a code in the full shift. Set $z = c_1c_2\cdots c_r$ with $c_i \in C$. Since S has a positive entropy, there exists a word $c \neq c_1$ in C. The words c and z cannot be powers of the same word. Indeed, suppose that $c = t^n$ and $z = t^m$ with $t \in A^*$ and n, m positive integers. If $n \leq m$, then $t^{m-n} \in C^*$. Since C is a code, this forces $c = c_1$, a contradiction. Otherwise, $t^{n-m} \in C^*$ and thus $c = t^{n-m}t^m$ is not in C.

Let $w = u^mz^m$ with $m \geq 2$. Since $w \in C^*$, we have $w \in \mathrm{Fact}(S)$. By [13, Theorem 9.2.4 pp. 166], w is a primitive word. Let y be the Lyndon word conjugate to w. It belongs to $\mathrm{Fact}(S)$ since any conjugate of a word in C^* is in $\mathrm{Fact}(S)$. By a well known result (see [13, Proposition 5.1.2 p. 65]), a Lyndon word is unbordered. Thus y is an unbordered in $\mathrm{Fact}(S)$. It is trivial that z is a factor of y since $m \geq 2$.

We are now ready to prove Theorem 1.

Proof of Theorem 1. Let S be an irreducible sofic shift. We denote by $\mathcal{A}$ the Fischer cover of S. Let X be an S-code.

Let us suppose that X is not S-complete. Consequently there is a word z in $\mathrm{Fact}(S)$ which is not in $\mathrm{Fact}(X^*)$.

We first assume that S has a null entropy. This means that the Fischer cover $\mathcal{A}$ is made of a unique cycle. One can assume that there is a state p such that p has no outgoing path in $\mathcal{A}$ labeled in X. Otherwise X is already S-complete. Since $\mathcal{A}$ is irreducible, one can assume without loss of generality that z is the label of a path in $\mathcal{A}$ going from a state p to itself, and that z is moreover a synchronizing word of $\mathcal{A}$. We set $Y = X \cup \{z\}$. Let us show that Y is an S-code. Assume the contrary and consider a relation

$$x_1x_2\cdots x_n = y_1y_2\cdots y_m,$$

with $x_1x_2\cdots x_n \in \mathrm{Fact}(S)$, $x_i, y_j \in Y$, and $x_n \neq y_m$. The set X being an S-code, at least one of the words x_i, y_j must be z. Hence, for instance $x_1x_2\cdots x_n = x_1x_2\cdots x_rzx_{r+1}\ldots x_n$. The word $zx_{r+1}\cdots x_n$ is the label of a path in $\mathcal{A}$ going through the state p after reading the label z. Since p has no outgoing path in $\mathcal{A}$ labeled in X, it follows that $x_{r+1}\cdots x_n = z^{n-r}$. Hence there is a positive integer k such that $x_1x_2\cdots x_n = x_1x_2\cdots x_rz^k$ with $x_1, x_2, \ldots, x_r \neq z$. Since z is not a factor of X^*, there is also a positive integer l such that $y_1y_2\cdots y_m = y_1y_2\cdots y_tz^l$ with $y_1, y_2, \cdots, y_t \neq z$. The above relation becomes

$$x_1x_2\cdots x_rz^k = y_1y_2\cdots y_tz^l,$$

which contradicts the hypothesis that $x_n \neq y_m$ since $z \notin \mathrm{Fact}(X^*)$. It is trivial that Y is S-complete.

We may now assume that S has a positive entropy. Without loss of generality, by extending z on the right, one can moreover assume that z is a synchronizing word of $\mathcal{A}$. By Lemma 2, we construct a word $y \in \mathrm{Fact}(S)$ which is unbordered and has z as factor. This latter point implies that y is a synchronizing word of $\mathcal{A}$, and hence a synchronizing word of $\mathrm{Fact}(S)$.

If L is a language of finite words, we denote by $u^{-1}L$ (resp. Lu^{-1}) the set of words z such that $uz \in L$ (resp. $zu \in L$).

We define the sets U and Y by

$$U = y^{-1}\,\mathrm{Fact}(S)y^{-1} - X^* - A^*yA^*, \tag{1}$$

$$Y = X \cup y(Uy)^*. \tag{2}$$

The rest of the proof consists in verifying the following three properties.

- The set Y is a subset of $\mathrm{Fact}(S)$.
- The set Y is an S-code.
- The set Y is S-complete.

Let us show that Y is a subset of $\mathrm{Fact}(S)$. For any word $u \in U$, $yuy \in Fact(S)$. Since y is a synchronizing word of $\mathrm{Fact}(S)$, for any two words w, w' with $wy, yw' \in \mathrm{Fact}(S)$, $wyw' \in \mathrm{Fact}(S)$. It follows that for any two words $u, u' \in U$, $yuyu'y$ belongs to $\mathrm{Fact}(S)$. By recurrence, $y(Uy)^* \subseteq \mathrm{Fact}(S)$, and thus $Y \subseteq \mathrm{Fact}(S)$.

Now we show that Y is an S-code. Assume the contrary and consider a relation

$$y_1y_2\ldots y_n = y'_1y'_2\ldots y'_m,$$

with $y_1, \ldots, y'_m \in Y$, $y_1y_2\ldots y_n \in \mathrm{Fact}(S)$ and $y_1 \neq y'_1$. The set X being a code, one of these words must be in $Y - X$. Assume that one of $y_1, \ldots, y_n$ is in $Y - X$, and let k be the smallest index such that $y_k \in y(Uy)^*$. From $y \notin \mathrm{Fact}(X^*)$ it also follows that $y_k \notin \mathrm{Fact}(X^*)$. Consequently at least one of $y'_1, \ldots, y'_m$ is in $y(Uy)^*$. Let l be the smallest index such that $y'_l \in y(Uy)^*$. Then

$$y_1\ldots y_{k-1}y, \quad y'_1y'_2\ldots y'_{l-1}y \in X^*y.$$

Since $y \notin \mathrm{Fact}(X^*)$ and y is unbordered, X^*y is a prefix code. It follows that $y_1 \dots y_{k-1} = y'_1 y'_2 \dots y'_{l-1}$. The set X being a code and $y_1 \neq y'_1$, $k = l = 1$. Set

$$y_1 = yu_1y \dots yu_qy,$$
$$y'_1 = yu'_1y \dots yu'_ry,$$

with $u_1, \dots u_q, u'_1, \dots u'_r \in U$. Assume $|u_1| > |u'_1|$. The word u'_1y is a prefix of u_1y. Since y is unbordered and $u_1 \notin A^*yA^*$, we get $u'_1 = u_1$. Let us assume that $r \geq q$ (the opposite case is similar). By recurrence, we get that

$$u_1 = u'_1, \ \dots \ , u_q = u'_q.$$

Let $t = u'_{q+1}y \cdots u'_ry$. We have

$$y_2 \cdots y_n = ty'_2 \cdots y'_m.$$

The word y is a factor of t and thus occurs also in $y_2 \dots y_n$. This shows that at least one of $y_2, \dots, y_n$, say y_i is in $y(Uy)^*$. Suppose i is chosen minimal. Then $y_2 \cdots y_{i-1} \in X^*$. Since y is unbordered and $U \cap A^*yA^* = \emptyset$, $u'_{q+1} = y_2 \cdots y_{i-1}$. Thus $u'_{q+1} \in X^*$, in contradiction with the hypothesis $u'_{q+1} \in U$. This shows that Y is an S-code.

Finally, let us show that Y is S-complete. Let us assume that the word y is the label of a path from p to q in $\mathcal{A}$. Let $t \in \mathrm{Fact}(S)$. By extending t on the right and on the left, one may assume, without loss of generality, that t is a label of a path from q to p in $\mathcal{A}$. It follows that yty also is in $\mathrm{Fact}(S)$. Hence $t \in y^{-1}\,\mathrm{Fact}(S)y^{-1}$. Set

$$t = v_1yv_2y \cdots yv_{n-1}yv_n,$$

with $v_1, \dots, v_n \in A^* - A^*yA^*$. Each yv_iy is factor of t for $2 \leq i \leq n-1$. Hence $v_i \in y^{-1}\,\mathrm{Fact}(S)y^{-1}$ for $2 \leq i \leq n-1$. Since $yty \in \mathrm{Fact}(S)$, v_1 and v_n also belong to $y^{-1}\,\mathrm{Fact}(S)y^{-1}$. Set

$$V = y^{-1}\,\mathrm{Fact}(S)y^{-1} - A^*yA^*.$$

Thus $v_i \in V$ for $1 \leq i \leq n$ and $U = V - X^*$. Let $v_{i_1}, v_{i_2}, \dots, v_{i_k}$ be the v_i's which are in X^*. Then

$$yty = (yv_1y \cdots yv_{i_1-1}y)v_{i_1}(yv_{i_1+1}y \cdots yv_{i_2-1}y)v_{i_2} \times \cdots \times v_{i_k}(yv_{i_k+1}y \cdots yv_{i_v}y).$$

Each parenthesized word is in $y(Uy)^*$. Thus the whole word is in Y^*.

It is clear from Equations (1) and (2) that Y is regular when X is regular.

Remark 1. When X is a regular S-code, the S-complete code Y of Theorem 1 can be computed in an effective way from Equations (1) and (2). More precisely, we consider a sofic shift S defined by its Fisher cover. This gives a non-deterministic automaton recognizing $\mathrm{Fact}(S)$. The S-code X is given by a deterministic automaton. Equations (1) and (2) allow to build a finite automaton recognizing Y.

Remark 2. Note that our proof shows that, if S is an irreducible sofic shift with a positive entropy, and X is a code, then X can be completed into a code Y (*i.e* a code for the full shift) which is S-complete. We do not know whether this property also holds for irreducible shifts of entropy zero.

In [14, 2] (see also [3]), it is proved that if S is an irreducible shift of finite type and X a code with $X^* \subseteq \mathrm{Fact}(S)$ which is not S-complete, X can be embedded into an S-complete set which is moreover a code (*i.e.* a code for the full shift). The proof of our theorem allows us to recover this result. Indeed, when $X^* \subseteq \mathrm{Fact}(S)$, our construction builds an S-code Y which is a code. Moreover, the S-complete code Y that we have built satisfies also $Y^* \subseteq \mathrm{Fact}(S)$, when $X^* \subseteq \mathrm{Fact}(S)$. This is due to the strong synchronization properties of the Fischer cover of an irreducible shift of finite type.

Example 3. We consider the even system S of Example 1 on the alphabet $A = \{a, b\}$. Let $X = \{a, ba\}$. The set X is an S-code but it is not S-complete since for instance $z = bb$ does not belong to $\mathrm{Fact}(X^*)$. The regular completion of X is obtained following the proof of Theorem 1. We replace z by bba in order to get a synchronizing word. The proof of Lemma 2 says that the word $y = aaabbabb$ is an unbordered word of $\mathrm{Fact}(S)$. Note that a smaller y can be chosen. For instance $y = bba$ also is an allowable unbordered word of $\mathrm{Fact}(S)$. We then define U and Y as in Equations (1) and (2) and get

$$\begin{aligned} z &= bba \text{ (synchronizing)},\\ y &= bba \text{ (unbordered)},\\ U &= a^*(bb)^+,\\ Y &= a + ba + bba(a^*(bb)^+bba)^*. \end{aligned}$$

The set Y is a regular S-complete code.

We derive the following corollary which generalizes to codes in irreducible sofic shifts the fact that any maximal code is complete [5, Theorem 5.1].

Corollary 3. *Let S be an irreducible sofic shift. Any maximal S-code is S-complete.*

4. Polynomial of a Code

In the rest of this paper, S is an irreducible sofic shift recognized by its Fischer cover $\mathcal{A} = (Q, E)$. Let $\mu_{\mathcal{A}}$ (or μ) be the morphism from A^* into $\mathbb{N}^{Q\times Q}$ defined as follows. For each word u, the matrix $\mu(u)$ is defined by

$$\mu(u)_{pq} = \begin{cases} 1 & \text{if } p \cdot u = q \\ 0 & \text{otherwise.} \end{cases}$$

The matrix $\alpha_{\mathcal{A}}(u)$ (or $\alpha(u)$) is defined by $\alpha(u) = \mu(u)u$. Thus the matrix $\alpha(u)$ is obtained from $\mu(u)$ by replacing its coefficients 1 by the word u. The

coefficients of $\alpha(u)$ are either 0 or u. In this way α is a morphism from A^* into the monoid of matrices with elements in the set of subsets of A^*.

The morphism α is extended to subsets of A^* by linearity.

For a finite set X, we denote by p_X the polynomial in commuting variables:

$$p_X = \det(I - \alpha(X)).$$

The following result is proved in [7]. It is a generalization of a result of C. Reutenauer [1] who has proved it under more restrictive assumptions.

Theorem 4. *Let S be an irreducible sofic shift and let X be a finite complete S-code. The polynomial p_A divides p_X.*

Example 4. For the even shift and the set $X = \{aa, ab, ba, bb\}$, we have

$$\alpha(A) = \begin{bmatrix} a & b \\ b & 0 \end{bmatrix} \quad \text{and} \quad \alpha(X) = \begin{bmatrix} aa + bb & ab \\ ba & bb \end{bmatrix},$$

and $p_A = 1 - a - bb$, $p_X = 1 - aa - 2bb + b^4 = (1 + a - bb)(1 - a - bb)$.

We present here two combinatorial proofs of this result, which come as an alternative to the analytic proof presented in [7]. Both proofs rely on the reduction of automata with multiplicities.

The first proof goes along the same line as the proof of a result of S. Williams presented in Kitchen's book [15, p. 156], giving a necessary condition to the existence of a finite-to-one factor map between irreducible sofic shifts.

We first build as in Section 2 an automaton $\mathcal{B}$ computed from X and $\mathcal{A}$ as follows. The set of states of $\mathcal{B}$ contains the set of states Q of $\mathcal{A}$. For each path in $\mathcal{A}$ labeled by a word in X going from state p to state q, we build a path in $\mathcal{B}$ from p to q with dummy states in-between as shown in Example 5. The automaton $\mathcal{B}$ is finite when X is finite. It is unambiguous if and only if the set X is an S-code. It presents the sofic shift S if and only if the set X is S-complete.

Example 5. Consider the code $X = \{aa, ab, ba, bb\}$ in the even system S. The automaton $\mathcal{B}$ is represented in the right part of Figure 2.

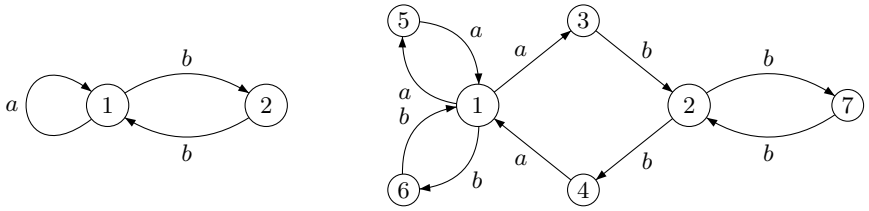

Figure 2: The automaton $\mathcal{A}$ (on the left), and the automaton $\mathcal{B}$ computed from $\mathcal{A}$ and $X = \{aa, ab, ba, bb\}$ (on the right).

Thus, since X is a complete S-code, $\mathcal{B}$ is unambiguous and presents S. Without loss of generality, one can assume that $\mathcal{B}$ is irreducible. Otherwise, it is possible to keep only a strongly connected component of $\mathcal{B}$ presenting S. By definition,

$$p_A = \det(I - \alpha_{\mathcal{A}}(A)) \quad \text{and} \quad p_X = \det(I - \alpha_{\mathcal{A}}(X)).$$

Furthermore,

$$\det(I - \alpha_{\mathcal{A}}(X)) = \det(I - \alpha_{\mathcal{B}}(A)).$$

Indeed,

$$\det(I - \alpha_{\mathcal{B}}(A)) = \sum (-1)^k P_{c_1} \cdots P_{c_k},$$

where the sum is on the sets of independent cycles $c_1, \ldots, c_k$ of the automaton $\mathcal{B}$. Consider the transformation of $\mathcal{B}$ contracting each path $p \xrightarrow{a_1} d_1 \xrightarrow{a_2} d_2 \cdots \xrightarrow{a_n} q$, where d_i are dummy states into $p \xrightarrow{a_1 \cdots a_n} q$. It gives an automaton whose edges are labelled by words of X and whose adjacency matrix is $\alpha_{\mathcal{A}}(X)$. Since it does not change the labels of cycles, we obtain the formula.

Hence, Theorem 4 is a consequence of the following result.

Proposition 5. *Let S be an irreducible sofic shift and let $\mathcal{A}$ be its Fischer cover. If $\mathcal{B}$ is an unambiguous and irreducible automaton presenting S,* $\det(I - \alpha_{\mathcal{A}}(A))$ *divides* $\det(I - \alpha_{\mathcal{B}}(A))$.

Proof. The *degree* of a word u in an automaton is defined as the number of paths labeled by u. The degree of an automaton is the minimal non-null value of the degrees of words. Any unambiguous irreducible automaton of degree k has the following property: for any word u of degree k and any word w such that uwu has a non-null degree, uwu has degree k.

We first assume that the Fischer cover $\mathcal{A}$ of S is *codeterministic* (or *left resolving*): for any state $p \in Q$ and any word u, there is at most one path labeled by u and ending at p. In this case the degree of $\mathcal{A}$ is $d = 1$. Indeed, since $\mathcal{A}$ is a Fischer cover, it has a synchronizing word. Since $\mathcal{A}$ is codeterministic, each synchronizing word has degree 1.

Let v (resp. w) be a word which has a non-null and minimal degree k (resp. $d = 1$) in $\mathcal{B}$ (resp. in $\mathcal{A}$). Since $\mathcal{B}$ is irreducible, there are words z, z' such that $vzwz'v$ has a non-null degree. Hence $vzwz'v$ has degree k in $\mathcal{B}$ and degree $d = 1$ in $\mathcal{A}$. We set $u = vzwz'v$.

An $\mathbb{N}$-automaton with a set of states Q is a triple $\langle I, \mu, T\rangle$, where I and T are two vectors — respectively initial row vector and final column vector — with entries in $\mathbb{N}$, and where μ is a morphism from A^* into $\mathbb{N}^{Q\times Q}$. It is equivalently defined by the triple $\langle I, \alpha(A), T\rangle$. Two $\mathbb{N}$-automata $\langle I, \mu, T\rangle$ and $\langle J, \mu', F\rangle$ are *equivalent* if and only if, for any word $w \in A^*$, $I\mu(w)T = J\mu'(w)F$.

Let $\mathbf{1}_{\mathcal{A}}$ be the row-vector with all coefficients equal to 1 of size the number of states of $\mathcal{A}$, and $\mathbf{1}_{\mathcal{A}}^t$ its transpose. It follows from the definition of the word u that the two $\mathbb{N}$-automata

$$\mathcal{C} = \langle k\mathbf{1}_{\mathcal{A}}\mu_{\mathcal{A}}(u), \quad \mu_{\mathcal{A}}, \quad \mu_{\mathcal{A}}(u)\mathbf{1}_{\mathcal{A}}^t\rangle,$$

and

$$\mathcal{D} = \langle d\mathbf{1}_{\mathcal{B}}\mu_{\mathcal{B}}(u), \quad \mu_{\mathcal{B}}, \quad \mu_{\mathcal{B}}(u)\mathbf{1}_{\mathcal{B}}^t \rangle,$$

are equivalent.

The standard Schützenberger reductions of the $\mathbb{N}$-automata $\mathcal{C}$ and $\mathcal{D}$ over the field $\mathbb{R}$ are similar. The reduction of each $\mathbb{N}$-automaton is obtained through a left reduction followed by a right reduction (see for instance [16] or [17]).

Since u has degree 1 in $\mathcal{A}$, the initial row (resp. final column) vector of $\mathcal{C}$ has a unique non-null coefficient. Consequently, since $\mathcal{A}$ is deterministic (resp. codeterministic) and irreducible, the automaton $\mathcal{C}$ is left (resp. right) reduced. Hence $\mathcal{C}$ is already reduced.

Finally, it is not difficult to see that the transition matrix of $\mathcal{D}$ is similar to a matrix having a principal subblock equal to the transition matrix of its left (or right) reduced form. It follows that $\det(I - \alpha_{\mathcal{A}}(A))$ divides $\det(I - \alpha_{\mathcal{B}}(A))$.

The extension of the proof to sofic shifts that may not have a codeterministic Fischer cover can be obtained with a specialization argument as follows. In the general case, we number the labels of edges of the automaton $\mathcal{A}$ so that all edges have distinct labels (see the left part of Figure 3). We get a codeterministic Fischer cover $\mathcal{A}'$ presenting a new shift S'. We denote by A' the new alphabet. We define X' as the set of words $u \in A'^*$ labels of paths in $\mathcal{A}'$, such that the word obtained from u by removing the numbers is in X. We build an automaton $\mathcal{B}'$ such that for each path in $\mathcal{A}'$ labeled by a word in X' going from state p to state q, we build a path in $\mathcal{B}'$ from p to q with dummy states in-between (see the right part of Figure 3). Since $\mathcal{A}'$ is codeterministic, we have $\det(I - \alpha_{\mathcal{A}'}(A'))$ divides $\det(I - \alpha_{\mathcal{B}'}(A'))$. As a consequence, $\det(I - \alpha_{\mathcal{A}}(A))$ divides $\det(I - \alpha_{\mathcal{B}}(A))$.

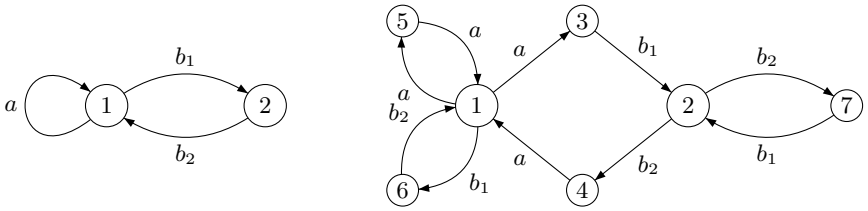

Figure 3: The automaton $\mathcal{A}'$ (on the left), and the automaton $\mathcal{B}'$ computed from $\mathcal{A}'$ and $X' = \{aa, ab_1, b_2a, b_1b_2, b_2, b_1\}$ (on the right).

Example 6. We continue with Example 5. The word $u = bab$ has degree 2 in $\mathcal{B}$ and 1 in $\mathcal{A}$. Hence the $\mathbb{N}$-automata

$$\mathcal{C} = \langle \begin{bmatrix} 0 & 2 \end{bmatrix}, \quad \mu_{\mathcal{A}}(A) = \begin{bmatrix} a & b \\ b & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rangle,$$

and

$$\mathcal{D} = \langle \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad \mu_{\mathcal{B}}(A), \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}^t \rangle,$$

are equivalent. We obtain a right-reduction of the automaton $\mathcal{D} = \langle I, E = \alpha_{\mathcal{B}}(A), T \rangle$ by computing a basis of the vector space generated by the vectors in

$\mu(A^*)T$. We can choose the basis $(T, \mu(b)T, \mu(ab)T)$ since $\mu(a)T = 0$, $\mu(bb)T = T$, $\mu(bab)T = T$ and $\mu(aab)T = \mu(ab)T$. This basis is extended to a basis of $\mathbb{R}^7$, for instance with the first 4 column vectors $e_1, \dots e_4$ of the canonical basis of $\mathbb{R}^7$.

Let F and H be the matrices

$$F = \begin{bmatrix} \begin{bmatrix} 0 & b & b \\ b & 0 & 0 \\ 0 & a & a \end{bmatrix} & \begin{bmatrix} b & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ a & 0 & 0 & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} & \begin{bmatrix} -a & -b & a & 0 \\ -b & 0 & 0 & b \\ a & 0 & 0 & 0 \\ -a & 0 & 0 & 0 \end{bmatrix} \end{bmatrix}, \qquad H = \begin{bmatrix} \begin{bmatrix} 0 & b \\ b & a \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \end{bmatrix} \\ \begin{bmatrix} 1 & 0 \end{bmatrix} & \begin{bmatrix} 0 \end{bmatrix} \end{bmatrix}.$$

We get that E is similar to F. Let us denote by G the upper left block matrix of size 3 of F. The right-reduced automaton

$$\langle \begin{bmatrix} 2 & 0 & 0 \end{bmatrix}, G = \begin{bmatrix} 0 & b & b \\ b & 0 & 0 \\ 0 & a & a \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \rangle$$

can be now reduced on the left side. We get that G is similar to H. The upper left block matrix of size 2 of G is similar to $\alpha_{\mathcal{A}}(A)$. As a consequence, $\det(I - \alpha_{\mathcal{A}}(A)) = 1 - a - bb$ divides $\det(I - H)$ which divides $\det(I - F) = \det(I - \alpha_{\mathcal{B}}(A)) = (1 - a - bb)(1 + a - bb)$.

A variant of the above combinatorial proof uses an argument due to Nasu [11].

We denote by M (resp. M') the matrix $M = \sum_{a \in A} \mu_{\mathcal{A}}(a)$ and (resp. $M' = \sum_{a \in A} \mu_{\mathcal{B}}(a)$). It is known from the Perron-Frobenius theory that M and M' have the same positive spectral radius λ, the logarithm of λ being the topological entropy of the sofic shift S [12]. Let U, V (resp. U', V') be two real positive left and right eigenvectors of M (resp. of M') for the eigenvalue λ. One can choose these vectors such that $UV = U'V' = 1$. With these settings, the two $\mathbb{R}$-automata $\mathcal{C} = \langle U, \mu_{\mathcal{A}}, V \rangle$ and $\mathcal{D} = \langle U', \mu_{\mathcal{B}}, V' \rangle$ are equivalent.

The proof of this equivalence relies on the following arguments. One first divides $\mu_{\mathcal{A}}$ and $\mu_{\mathcal{B}}$ by λ to reduce to the case $\lambda = 1$.

For any word $x \in A^*$ and any $\mathbb{R}$-automaton $\mathcal{S} = \langle I, \mu, T \rangle$, we denote by $\pi_{\mathcal{S}}(x)$ the real coefficient $I\mu(x)T$. We say that $\pi_{\mathcal{S}}$ is *recognized* by $\mathcal{S}$. The functions $\pi_{\mathcal{C}}$ and $\pi_{\mathcal{D}}$ define two rational probability measures on A^* [18]. By definition, this means that they are recognized by an $\mathbb{R}$-automaton and satisfy the coherence condition: for any $x \in A^*$, for any $k \geq 0$,

$$\sum_{w \in A^k} \pi_{\mathcal{S}}(xw) = \pi_{\mathcal{S}}(x).$$

Let us prove that $\pi_{\mathcal{C}}$ satisfies this condition (the proof for $\pi_{\mathcal{D}}$ is similar). For

any $x \in A^*$, for any $k \geq 0$, $\mu = \mu_{\mathcal{A}}$,

$$\begin{aligned}\sum_{w\in A^k} \pi_{\mathcal{C}}(xw) &= U \sum_{w\in A^k} \mu(x)\mu(w)V,\\ &= U\mu(x) \sum_{w\in A^k} \mu(w)V,\\ &= U\mu(x)M^kV = U\mu(x)V = \pi_{\mathcal{C}}(x).\end{aligned}$$

These measures $\pi_{\mathcal{S}}$ for $\mathcal{S}$ equal to $\mathcal{C}$ or $\mathcal{D}$ satisfy the following two additional properties.

- The left invariance property: for any $x \in A^*$, for any $k \geq 0$,

$$\sum_{w\in A^k} \pi_{\mathcal{S}}(wx) = \pi_{\mathcal{S}}(x).$$

- An ergodic property: for any $x, y \in A^*$,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \sum_{w\in A^i} \pi_{\mathcal{S}}(xwy) = \pi_{\mathcal{S}}(x)\pi_{\mathcal{S}}(y).$$

The left invariance is proved as the coherence condition. Let us now show the ergodic property. For any $x, y \in A^*$, $\mu = \mu_{\mathcal{A}}$,

$$\begin{aligned}\lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \sum_{w\in A^i} \pi_{\mathcal{C}}(xwy) &= \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} U\mu(x) \sum_{w\in A^i} \mu(w)\mu(y)V,\\ &= U\mu(x)(\lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} M^i)\mu(y)V,\\ &= U\mu(x)(VU)\mu(y)V,\\ &= \pi_{\mathcal{A}}(C)\pi_{\mathcal{C}}(y).\end{aligned}$$

The third equality above uses the fact that $(\lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} M^i) = VU$ since M is an irreducible stochastic matrix.

Moreover, since the automata $\mathcal{A}$ and $\mathcal{B}$ are unambiguous, one can show that there are positive real numbers ρ, ρ' such that for any $x \in A^*$,

$$\pi_{\mathcal{C}}(x) \leq \rho\, \pi_{\mathcal{D}}(x) \quad \text{and} \quad \pi_{\mathcal{D}}(x) \leq \rho'\, \pi_{\mathcal{C}}(x).$$

Indeed, for any word x, we have $\mu_{\mathcal{A}}(x) = 0$ if and only if $\mu_{\mathcal{B}}(x) = 0$. Hence $\pi_{\mathcal{C}}(x) = 0$ if and only if $\pi_{\mathcal{D}}(x) = 0$. Moreover, since $\mathcal{A}$ is unambiguous, for any word x such that $\mu_{\mathcal{A}}(x) \neq 0$, we have

$$\min_{i,j} U_i V_j \leq U\mu_{\mathcal{A}}(x)V \leq (\sum_i U_i) \max_i (V_i).$$

Hence, for any word x such that $\mu_{\mathcal{A}}(x) \neq 0$, there are positive real numbers k_1, k_2, k_1', k_2' with

$$k_1 \leq U\mu_{\mathcal{A}}(x)V \leq k_2,$$
$$k_1' \leq U'\mu_{\mathcal{B}}(x)V' \leq k_2'.$$

As a consequence, there are positive real numbers ρ, ρ' such that for any $x \in A^*$, $\pi_{\mathcal{C}}(x) \leq \rho\, \pi_{\mathcal{D}}(x)$ and $\pi_{\mathcal{D}}(x) \leq \rho'\, \pi_{\mathcal{C}}(x)$.

We deduce the equivalence of $\mathcal{C}$ and $\mathcal{D}$ from these inequalities as follows. Let x be a word such that $\mu_{\mathcal{A}}(x) \neq 0$. Let us assume that $\pi_{\mathcal{C}}(x) > \pi_{\mathcal{D}}(x)$. We have

$$\begin{aligned}\pi_{\mathcal{C}}(x)\pi_{\mathcal{C}}(x) &= \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \sum_{w\in A^i} \pi_{\mathcal{C}}(xwx),\\ &\leq \rho \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \sum_{w\in A^i} \pi_{\mathcal{D}}(xwx),\\ &= \rho\, \pi_{\mathcal{D}}(x)\pi_{\mathcal{D}}(x).\end{aligned}$$

By induction, we get

$$(\pi_{\mathcal{C}}(x))^n \leq \rho(\pi_{\mathcal{D}}(x))^n.$$

Or equivalently,

$$\left(\frac{\pi_{\mathcal{C}}(x)}{\pi_{\mathcal{D}}(x)}\right)^n \leq \rho,$$

which contradicts the hypothesis. Hence $\pi_{\mathcal{C}}(x) \leq \pi_{\mathcal{D}}(x)$. We obtain similarly $\pi_{\mathcal{D}}(x) \leq \pi_{\mathcal{C}}(x)$ and thus $\mathcal{C}$ and $\mathcal{D}$ are equivalent.

A reduction of these automata is used to finish this proof as in the previous proof.

Acknowledgments The authors would like to thank the anonymous reviewers for improving the presentation.

References

[1] Ch. Reutenauer, Ensembles libres de chemins dans un graphe, Bull. Soc. Math. France 114 (2) (1986) 135–152.

[2] A. Restivo, Codes and local constraints, Theoret. Comput. Sci. 72 (1) (1990) 55–64.

[3] J. Ashley, B. Marcus, D. Perrin, S. Tuncel, Surjective extensions of sliding-block codes, SIAM J. Discrete Math. 6 (4) (1993) 582–611.

[4] M. P. Schützenberger, Une théorie algébrique du codage, C. R. Acad. Sci. Paris 242 (1956) 862–864.

[5] J. Berstel, D. Perrin, Theory of codes, Vol. 117 of Pure and Applied Mathematics, Academic Press Inc., Orlando, FL, 1985, http://www-igm.univ-mlv.fr/~berstel/LivreCodes/Codes.html.
URL `http://www-igm.univ-mlv.fr/ berstel/LivreCodes/Codes.html`

[6] M.-P. Béal, D. Perrin, Complete codes in a sofic shift, in: STACS 2006, Vol. 3884 of Lecture Notes in Comput. Sci., Springer, Berlin, 2006, pp. 127–136.

[7] M.-P. Béal, D. Perrin, Codes and sofic constraints, Theoret. Comput. Sci. 340 (2) (2005) 381–393.

[8] M.-P. Béal, D. Perrin, Codes, unambiguous automata and sofic systems, Theoret. Comput. Sci. 356 (1-2) (2006) 6–13.

[9] A. Ehrenfeucht, G. Rozenberg, Each regular code is included in a maximal regular code, RAIRO Inform. Théor. Appl. 20 (1) (1986) 89–96.

[10] S. Williams, Lattice invariants for sofic shifts, Ergodic Theory and Dynamical Systems 11 (1991) 787–801.

[11] M. Nasu, An invariant for bounded-to-one factor maps between transitive sofic subshifts, Ergodic Theory Dynam. Systems 5 (1) (1985) 89–105.

[12] D. Lind, B. Marcus, An Introduction to Symbolic Dynamics and Coding, Cambridge University Press, Cambridge, 1995.

[13] M. Lothaire, Combinatorics on words, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1983.

[14] A. Restivo, Codes with constraints, in: Mots, Lang. Raison. Calc., Hermès, Paris, 1990, pp. 358–366.

[15] B. P. Kitchens, Symbolic dynamics, Universitext, Springer-Verlag, Berlin, 1998, one-sided, two-sided and countable state Markov shifts.

[16] J. Berstel, C. Reutenauer, Rational series and their languages, Vol. 12 of EATCS Monographs on Theoretical Computer Science, Springer-Verlag, Berlin, 1988.

[17] J. Sakarovitch, Éléments de théorie des automates, Vuibert, Paris, 2003, english translation to appear, Cambridge University Pres.

[18] G. Hansel, D. Perrin, Rational probability measures, Theoret. Comput. Sci. 65 (2) (1989) 171–188.