On the equivalence of $\mathbb{Z}$-automata

Marie-Pierre Béal[1], Sylvain Lombardy[2], and Jacques Sakarovitch[3]

[1] Institut Gaspard-Monge, Université Marne-la-Vallée.
[2] LIAFA, Université Paris 7.
[3] LTCI, CNRS / Ecole Nationale Supérieure des Télécommunications. (UMR 5141)
beal@univ-mlv.fr lombardy@liafa.jussieu.fr sakarovitch@enst.fr

Abstract. We prove that two automata with multiplicity in $\mathbb{Z}$ are equivalent, *i.e.* define the same rational series, if and only if there is a sequence of $\mathbb{Z}$-coverings, co-$\mathbb{Z}$-coverings, and circulations of -1, which transforms one automaton into the other. Moreover, the construction of these transformations is effective.
This is obtained by combining two results: the first one relates coverings to conjugacy of automata, and is modeled after a theorem from symbolic dynamics; the second one is an adaptation of Schützenberger's reduction algorithm of representations in a field to representations in an Euclidean domain (and thus in $\mathbb{Z}$).

1 Introduction

Equivalence of $\mathbb{Z}$-automata is decidable with polynomial (cubic) complexity. This is not a new result: it is more than forty years old. We investigate it again in order to give more *structural information* on two equivalent $\mathbb{Z}$-automata. A first and simple example should make clear what we mean by that before we state the precise results we are aiming at.

An example Let us consider the two $\mathbb{Z}$-automata $\mathcal{A}_1$ and $\mathcal{B}_1$ of Figure 1. They are equivalent.[1] This can be proved by checking that series $|\mathcal{A}_1|$ and $|\mathcal{B}_1|$ have the same coefficients on every word of $\{a, b\}^*$ up to length 8 — which would be the algorithm derived from the *Equality Theorem* — or by verifying that the *reduced representation* of the series $|\mathcal{A}_1| - |\mathcal{B}_1|$ has dimension 0.

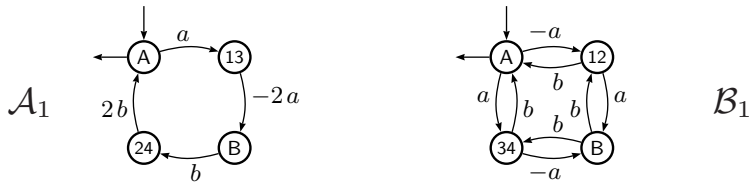


Fig. 1. Two equivalent $\mathbb{Z}$-automata.

We aim here at the construction of the two $\mathbb{Z}$-automata $\mathcal{C}_1$ and $\mathcal{D}_1$ of Figure 2. They are equivalent as one is obtained from the other by multiplying by -1 the

[1] This equivalence expresses a "shuffle identity": $(a\,b)^* \between (-a\,b)^* = (-4\,a^2b^2)^*$ that was mentioned to us by M. Waldschmidt (personnal communication).

coefficients of both the incoming and outgoing transitions around the state 1. The automata $\mathcal{C}_1$ and $\mathcal{A}_1$ are equivalent as $\mathcal{A}_1$ is obtained from $\mathcal{C}_1$ by merging the states 1 and 3 on one hand, the states 2 and 4 on the other hand, as these merged states have *the same incoming transitions* and as the outgoing transitions are added. The automata $\mathcal{D}_1$ and $\mathcal{B}_1$ are equivalent as $\mathcal{B}_1$ is obtained from $\mathcal{D}_1$ by merging the states 1 and 2 on one hand, the states 3 and 4 on the other hand, as these merged states have *the same outgoing transitions* and as the incoming transitions are added.

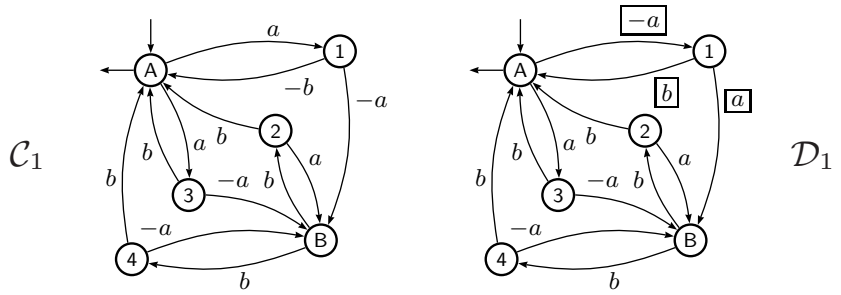


Fig. 2. Two other equivalent $\mathbb{Z}$-automata.

Equivalence of $\mathcal{A}_1$ and $\mathcal{B}_1$ boils down to the obvious three equivalences: $\mathcal{A}_1$ and $\mathcal{C}_1$, $\mathcal{C}_1$ and $\mathcal{D}_1$, and $\mathcal{D}_1$ and $\mathcal{B}_1$. The general case will not be that simple, but will nevertheless follow the same scheme.

The general framework and our results Finite automata with multiplicity in $\mathbb{Z}$ — with multiplicity in $\mathbb{Q}$ or in a commutative field $\mathbb{F}$ as well — were introduced as soon as 1961 by M.P. Schützenberger in a paper entitled: *On the definition of a family of automata* [17]. At that time, the emphasis was put on the investigation of new models of computation that allow the definition of *new families of languages* inside or outside Chomsky's hierarchy. The $\mathbb{Z}$-automata define one of the latter by way of the support of the series they realize. But Schützenberger's seminal paper also generalizes the theory of *rational formal power series* from one variable to several non commuting variables. Among other things, the existence of reduced $\mathbb{F}$-automata that realize a given $\mathbb{F}$-rational series, and the similarity between two equivalent reduced $\mathbb{F}$-automata is shown there. An algorithm is given — more or less explicitely — that computes a reduced $\mathbb{F}$-automaton. The decidability of the equivalence of $\mathbb{Z}$-automata is a direct consequence of the latter.

In [6] Eilenberg stated the *Equality Theorem* but disregarded the notion of reduced representation although the complexity of the corresponding equivalence algorithms blows up from polynomial to exponential without the latter. In other books on automata with multiplicity ([15, 10]) the equivalence of $\mathbb{Z}$-automata is reduced to the one of rational series over one variable. Schützenberger's reduction algorithm was made explicit in [5][2] and above all in [3]. The generalization to skew fields of coefficients is straightforward (as was noted for instance in [8]). The

[2] If a paper written in French is not considered to be cryptic.

importance of the decidablity of the equivalence of automata with multiplicity in a (sub-semiring of a) skew field appears clearly with its role in the proof of the decidability of the equivalence of deterministic k-tape transducers [9].

Our contribution to this now well-established chapter of automata theory is based on two notions: *covering* and *conjugacy* of automata and develops in two directions: the generalization and reinterpretation of the *Finite Equivalence Theorem* of symbolic dynamics for $\mathbb{Z}$-automata on one hand and of the reduction algorithm for automata with multiplicity in an Euclidean domain on the other hand. The two results are combined in our last theorem (Theorem 4) that expresses the equivalence of two $\mathbb{Z}$-automata as a sequence of six coverings and a conjugacy of a special kind, all effectively computable.

Coverings, conjugacy and the conjugacy theorems A *finite* automaton $\mathcal{A}$ over an alphabet A with multiplicity in a semiring $\mathbb{K}$, or $\mathbb{K}$-automaton for short, can be written in a compact way as $\mathcal{A} = \langle I, E, T\rangle$ where E is a square matrix of finite dimension Q whose entries are linear combinations of letters (with coefficients in $\mathbb{K}$) and where I and T are two vectors — respectively row vector and column vector — with entries in $\mathbb{K}$ as well. We can view each entry $E_{p,q}$ as the label of a unique arc which goes from state p to state q in the graph whose set of vertices is Q (if $E_{p,q} = 0_{\mathbb{K}}$, we consider that there is *no* arc from p and q).

The *behaviour* of $\mathcal{A}$, denoted $|\mathcal{A}|$, is the series such that the coefficient of a word w is the coefficient of w in $I \cdot E^{|w|} \cdot T$. It is part of Kleene-Schützenberger Theorem that every $\mathbb{K}$-rational series is the behaviour of a $\mathbb{K}$-automaton of the form we have just defined. For missing definitions, we refer to [6, 3, 14].

$\mathbb{K}$-coverings and co-$\mathbb{K}$-coverings are generalizations of morphisms of classical (Boolean) automata to $\mathbb{K}$-automata; the precise definition will be given and discussed in Section 2 but typically a $\mathbb{K}$-*covering* is the map that sends the above automaton $\mathcal{D}_1$ onto $\mathcal{B}_1$ and a *co*-$\mathbb{K}$-*covering* is the map that sends $\mathcal{C}_1$ onto $\mathcal{A}_1$. The second notion, the conjugacy of ($\mathbb{K}$-)automata, comes from symbolic dynamics (we follow [12]) and can be described as follow.

Definition 1. *An automaton* $\mathcal{A} = \langle I, E, T\rangle$ is conjugate to *an automaton* $\mathcal{B} = \langle J, F, U\rangle$ *if there exists a matrix* X *with entries in* $\mathbb{K}$ *such that*

$$I\,X = J, \qquad E\,X = X\,F, \quad \textit{and} \quad T = X\,U.$$

The matrix X *is the* transfer matrix *of the conjugacy and we write* $\mathcal{A} \overset{X}{\Longrightarrow} \mathcal{B}$.

Obviously two conjugate automata are equivalent (*i.e.* have the same behaviour). Remark that in spite of the idea conveyed by the terminology, the conjugacy relation[3] *is not an equivalence* but a *preorder* relation. Suppose that $\mathcal{A} \overset{X}{\Longrightarrow} \mathcal{B}$ holds; if $\mathcal{B} \overset{Y}{\Longrightarrow} \mathcal{C}$ then $\mathcal{A} \overset{XY}{\Longrightarrow} \mathcal{C}$, but if $\mathcal{C} \overset{Y}{\Longrightarrow} \mathcal{B}$ then $\mathcal{A}$ is not necessarily conjugate to $\mathcal{C}$, we write $\mathcal{A} \overset{X}{\Longrightarrow} \mathcal{B} \overset{Y}{\Longleftarrow} \mathcal{C}$ and we refer to this situation as "a chain of two (convergent) conjugacies".

[3] A conjugacy of automata was called *a backward elementary equivalence* in [2]. The transfer matrix X is called a *simulation* from $\mathcal{A}$ to $\mathcal{B}$ in [4].

We shall see that $\mathbb{K}$-coverings are realized by conjugacy with special transfer matrices. The following theorems express a kind of converse. (A matrix is *non degenerate* if it contains no zero row nor zero column.)

Theorem 1. *Let $\mathcal{A}$ and $\mathcal{B}$ be two $\mathbb{Z}$-automata. We have $\mathcal{A} \overset{X}{\Longrightarrow} \mathcal{B}$ with a non-negative and nondegenerate transfer matrix X if and only if there exists a $\mathbb{Z}$-automaton $\mathcal{C}$ that is a co-$\mathbb{Z}$-covering of $\mathcal{A}$ and a $\mathbb{Z}$-covering of $\mathcal{B}$.*

One of the reasons that make Theorem 1 interesting in our opinion is the relationship it bears with the Finite Equivalence Theorem of symbolic dynamics and we develop this point at Section 2.3. In order to state the results under the most general form in the sequel, let us write $\mathbb{H}$ for a ring that is either $\mathbb{Z}$ or a division ring[4]. By the following, we free ourselves from the two hypotheses on the transfer matrix (we call *circulation matrix* a diagonal invertible matrix).

Theorem 2. *Let $\mathcal{A}$ and $\mathcal{B}$ be two $\mathbb{H}$-automata. We have $\mathcal{A} \overset{X}{\Longrightarrow} \mathcal{B}$ if and only if there exists two $\mathbb{H}$-automata $\mathcal{C}$ and $\mathcal{D}$ and a circulation matrix D such that $\mathcal{C}$ is a co-$\mathbb{H}$-covering of $\mathcal{A}$, $\mathcal{D}$ and a $\mathbb{H}$-covering of $\mathcal{B}$ and $\mathcal{C} \overset{D}{\Longrightarrow} \mathcal{D}$.*

This theorem describes precisely the situation in our first example: $\mathcal{A}_1$ is conjugate to $\mathcal{B}_1$ with the transfer matrix X_1 shown opposite.

$$X_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Equivalence, conjugacy and the reduction theorems Our second contribution consists in establishing a kind of converse to the equivalence of conjugate $\mathbb{K}$-automata in two important cases: skew fields and Euclidean domains[5].

Theorem 3. *Let $\mathbb{L}$ be a skew field, or an Euclidean domain. If $\mathcal{A}$ and $\mathcal{B}$ are two equivalent $\mathbb{L}$-automata, then there exist two $\mathbb{L}$-automata $\mathcal{C}$ and $\mathcal{D}$ and three $\mathbb{L}$-matrices X, Y and Z such that:*

$$\mathcal{A} \overset{X}{\Longrightarrow} \mathcal{C} \overset{Y}{\Longleftarrow} \mathcal{D} \overset{Z}{\Longrightarrow} \mathcal{B}. \tag{1}$$

The alternative hypotheses correspond indeed to two different results, and two distinct proofs.

If $\mathbb{L}$ is a skew field, the proof is based on Schützenberger's algorithm that computes a reduced representation (*i.e.* an automaton with a minimal number of states) for a given $\mathbb{L}$-rational series. This algorithm may be interpreted as the effective computation of the transfer matrices of a chain of two (divergent or convergent) conjugacies. As the same algorithm implies that two minimal $\mathbb{L}$-automata are similar[6], Equation 1 holds, with the supplementary condition that the $\mathbb{L}$-automata $\mathcal{C}$ and $\mathcal{D}$ are minimal.

[4] *i.e.* a skew field. In Section 2.2, we take even more general hypotheses.

[5] An Euclidean domain is a principal *commutative* ring with no divisors of zero and where the gcd of any two elements is effectively computable.

[6] *i.e.* conjugate with a transfer matrix which is invertible.

In the case where $\mathbb{L}$ is an Euclidean domain ($\mathbb{Z}$ for instance), we prove that the above reduction algorithm can be transformed in such a way that it still computes a reduced $\mathbb{L}$-representation. As far as we know, this is the first reduction algorithm for automata with multiplicity in such rings. Another step of proof is then necessary to establish Theorem 3 in this case, for minimal automata are not necessarily conjugate anymore.

Combining Theorem 2 and Theorem 3 together with some further properties of coverings yields the final result of this paper, illustrated in Figure 3 [as we shall see below, coverings and co-coverings are special cases of conjugacy, which we represent with simple arrows, solid for coverings, dashed for co-coverings; a dotted simple arrow represents conjugacy with a circulation matrix].

Theorem 4. *Two $\mathbb{H}$-automata $\mathcal{A}$ and $\mathcal{B}$ are equivalent if and only if there exist two $\mathbb{H}$-automata $\mathcal{C}$ and $\mathcal{D}$ such that there is a sequence of three $\mathbb{H}$-coverings and co-$\mathbb{H}$-coverings from $\mathcal{C}$ onto $\mathcal{A}$ on one hand and from $\mathcal{D}$ onto $\mathcal{B}$ on the other hand, and a conjugacy by a circulation matrix between $\mathcal{C}$ and $\mathcal{D}$.*

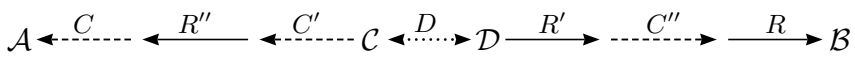


Fig. 3. The decomposition of the equivalence between $\mathbb{H}$-automata.

2 The conjugacy theorems

The two main ingredients in Theorem 2 are the notion of coverings and the property of *equisubtractivity* in a semiring, which albeit simple will be crucial for the proof.

2.1 $\mathbb{K}$-coverings and co-$\mathbb{K}$-coverings

The standard notion of morphisms of automata is not well-suited to automata with multiplicity in that it does not capture some similarities between these automata that we would like to be able to describe. Hence the definitions we take now. For the rest of the section, $\mathcal{A} = \langle I, E, T\rangle$ is a $\mathbb{K}$-automaton of dimension Q.

An equivalence φ on Q or, which is the same, a surjective map $\varphi\colon Q \to R$ is *Out-licit* (understood, *with respect to* $\mathcal{A}$) if for any two equivalent states p and p' modulo φ the *sum* of the labels of the transitions that go from p to *all the states of a whole class* modulo φ is equal to the *sum* of the labels of the transitions that go from p' to the same states *and* if any two entries of T indexed by equivalent states modulo φ are equal.[7] We denote by $[q]_\varphi$ the class of q modulo φ.

Definition 2 ([14]). *A surjective map $\varphi\colon Q \to R$ is Out-licit with respect to $\mathcal{A}$ if the following holds:*

$$\forall p, p', q \in Q \qquad p \equiv p' \mod \varphi \implies \begin{cases} \text{(i)} & \displaystyle\sum_{r\in[q]_\varphi} E_{p,r} = \sum_{s\in[q]_\varphi} E_{p',s} \\ \text{(ii)} & T_p = T_{p'} \end{cases} \tag{2}$$

[7] This definition bears some resemblance with the one of block-stochastic matrix, as given in [10, Ex. 4.5]

If $\varphi\colon Q \to R$ *is Out-licit,* the $\mathbb{K}$-quotient of $\mathcal{A}$ by φ *is the automaton* $\mathcal{B} = \langle J, F, U\rangle$ *of dimension* R*, defined by the following:*

$$\forall (r,s) \in R^2, \quad \forall p \in \varphi^{-1}(r),$$
$$J_s = \sum_{q\in\varphi^{-1}(s)} I_q, \qquad F_{r,s} = \sum_{q\in\varphi^{-1}(s)} E_{p,q}, \qquad U_r = T_p. \tag{3}$$

The automaton $\mathcal{B}$ *is called* a $\mathbb{K}$-quotient *of* $\mathcal{A}$ *and, conversely,* $\mathcal{A}$ *is called* a $\mathbb{K}$-covering *of* $\mathcal{B}$*. We write also* $\varphi\colon \mathcal{A} \to \mathcal{B}$ *and call it, by way of metonymy,* a $\mathbb{K}$-covering from $\mathcal{A}$ onto $\mathcal{B}$.[8]

If $\varphi\colon Q \to R$ is a map, the above condition and construction may be elegantly described by means of the $Q \times R$-matrix H_φ naturally associated with φ: its (q, r) entry is 1 if $\varphi(q) = r$, 0 otherwise. Since φ is a map, each row of H_φ contains exactly one 1 and since φ is surjective, each column of H_φ contains at least one 1. We call H_φ *the amalgamation matrix*[9] associated with φ. The following expresses that a quotient is a conjugate.

Proposition 1. *There is a* $\mathbb{K}$*-covering* φ *from* $\mathcal{A}$ *onto* $\mathcal{B}$ *if and only if there exists an amalgamation matrix* X *such that* $\mathcal{A} \overset{X}{\Longrightarrow} \mathcal{B}$ *(and in this case* $X = H_\varphi$*).*

The notion of $\mathbb{K}$-quotient is *lateralized* in that it refers not to the transitions of the automaton but to the *outgoing* transitions from the states of the automaton. Somehow, it is the price we pay for extending the notion of morphism of automata. Therefore the *dual* notions of *In-licit* map, *co-*$\mathbb{K}$*-quotient* and *co-*$\mathbb{K}$*-covering* are defined in a natural way and we have:

Proposition 2. *There is a co-*$\mathbb{K}$*-covering* ψ *from* $\mathcal{A}$ *onto* $\mathcal{B}$ *if and only if there exists an amalgamation matrix* X *such that* $\mathcal{A} \overset{{}^tX}{\Longrightarrow} \mathcal{B}$ *(and in this case* $X = H_\psi$*).*

It follows that every $\mathbb{K}$-automaton is equivalent to any of its $\mathbb{K}$-quotients or co-$\mathbb{K}$-quotients. Clearly, if $\varphi : Q \to R$ and $\psi : R \to S$ are surjective maps, then $H_{\varphi\psi} = H_\varphi H_\psi$. Hence $\mathbb{K}$-coverings (resp. co-$\mathbb{K}$-coverings) are closed under composition.

2.2 Decomposition of conjugacy

The proof of Theorem 2 involves indeed two properties.

We call *equisubtractive* a semiring is in which for all p, q, r and s such that $p+q = r+s$ there exist x, y, z and t such that $p = x+y$, $q = z+t$, $r = x+z$ and $s = y+t$. The semiring $\mathbb{N}$ and all rings are equisubtractive, and if $\mathbb{K}$ is equisubtractive, then so are $\mathbb{K}\langle A^*\rangle$ and $\mathbb{K}\langle\langle A^*\rangle\rangle$.

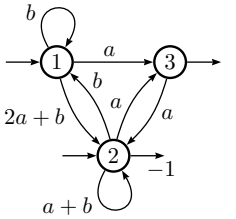
[8] Definition 2 has probably been stated independently a number of times. We relied on [14] where both the definition and its matrix expression are given. It was used in full generality in [13]. If $\mathbb{K} = \mathbb{B}$, the Boolean semiring, a $\mathbb{B}$-quotient is a simulation in the sense of [1].

[9] This is the terminology proposed in [12, Def. 8.2.4].

We say that a semiring has property (P) if *every element is a sum of units*. The ring $\mathbb{Z}$ and all fields have property (P). In any semiring with (P), every matrix X can be written as $X = C\,D\,R$ where C is an amalgamation, R a co-amalgamation and D a circulation matrix. In $\mathbb{Z}$, the dimension of D will be the sum of the absolute value of the entries of X.

Theorem 2 indeed holds for equisubtractive semiring $\mathbb{K}$ with (P). Its proof will be sketched with the following example.

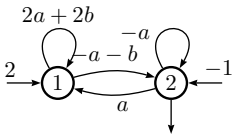
Example 2. Let $\mathcal{A}_2 = \langle I_2, E_2, T_2\rangle$ and $\mathcal{B}_2 = \langle J_2, F_2, U_2\rangle$ be the two $\mathbb{Z}$-automata defined by:



$$I_2 = \begin{pmatrix}1&1&0\end{pmatrix}, \quad E_2 = \begin{pmatrix}b & 2a+b & a\\ b & a+b & a\\ 0 & a & 0\end{pmatrix}, \quad T_2 = \begin{pmatrix}0\\-1\\1\end{pmatrix},$$

and

$$J_2 = \begin{pmatrix}2&-1\end{pmatrix}, \quad F_2 = \begin{pmatrix}2a+2b & -a-b\\ a & -a\end{pmatrix}, \quad U_2 = \begin{pmatrix}0\\1\end{pmatrix}.$$



One can check that $\mathcal{A}_2 \overset{X_2}{\Longrightarrow} \mathcal{B}_2$, with $X_2 = \begin{pmatrix}1&0\\1&-1\\0&1\end{pmatrix}$.

It then comes, $X_2 = C_2\,D_2\,R_2$ with

$$C_2 = \begin{pmatrix}1&0&0&0\\0&1&1&0\\0&0&0&1\end{pmatrix}, \quad D_2 = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&1\end{pmatrix}, \quad \text{and} \quad R_2 = \begin{pmatrix}1&0\\1&0\\0&1\\0&1\end{pmatrix}.$$

The proof of Theorem 2 amounts then to computing $\mathcal{C}_2 = \langle K_2, G_2, V_2\rangle$ and $\mathcal{D}_2 = \langle L_2, H_2, W_2\rangle$ such that:

$$\mathcal{A}_2 \overset{C_2}{\Longrightarrow} \mathcal{C}_2 \overset{D_2}{\Longrightarrow} \mathcal{D}_2 \overset{R_2}{\Longrightarrow} \mathcal{B}_2\,.$$

We set $K_2 = I_2\,C_2$, $L_2 = K_2\,D_2$, $W_2 = R_2\,U_2$, $V_2 = D_2\,W_2$ and we are left with the computation of $G_2\,D_2 = D_2\,H_2$, a 4×4 matrix. This matrix is composed of sub-matrices and the sum of the entries on every column and every row of each of these sub-matrices is given by the products $E_2\,C_2\,D_2$ and $D_2\,R_2\,F_2$. The sub-matrix decomposition and the "constraints" of our example are shown at Figure 4. The fact that $\mathcal{B}_2$ is conjugate to $\mathcal{A}_2$ ensures that these constraints are consistent and the equisubtractivity of $\mathbb{Z}$ allows to compute a solution:

$$G_2 = \begin{pmatrix}b & 2a+b & 2a+b & a\\ b & 2a+b & a+b & 0\\ 0 & -a & 0 & a\\ 0 & a & a & 0\end{pmatrix}, \quad H_2 = \begin{pmatrix}b & 2a+b & -2a-b & a\\ b & 2a+b & -a-b & 0\\ 0 & a & 0 & -a\\ 0 & a & -a & 0\end{pmatrix}.$$

This completes Example 2, and with it the proof of Theorem 2.

Finally, we note that if X is a non negative and non degenerate matrix, D is the identity matrix and Theorem 1 follows.

The dots figure the coefficients of the matrix, the cartouches figure their sums.

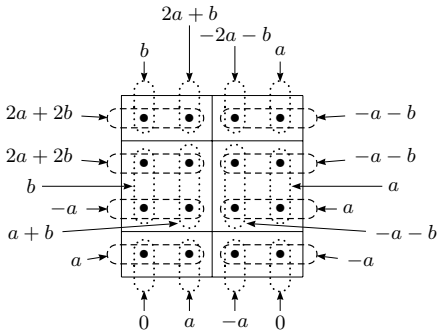


Fig. 4. Computation of $G_2\,D_2 = D_2\,H_2$ in Theorem 2.

2.3 The link with symbolic dynamics

We claim that Theorem 1 is a generalization of (a part of) the Finite Equivalence Theorem, a standard result in symbolic dynamics (*cf.* [12, Theorem 8.3.7]).

Theorem 5 (FET). *Two irreducible sofic shifts are finitely equivalent if and only if they have the same entropy.*

This requires some definitions to be understood. Symbolic dynamics deals with sets of *bi-infinite words*, *i.e.* subsets of $A^{\mathbb{Z}}$, closed under the *shift operation* and called *shifts*. A *sofic shift* X is the set of labels of bi-infinite paths in a finite labelled graph G and is *irreducible* if such G can be chosen to be a strongly connected graph. The set of finite factors of words in a shift X is denoted $F(\mathsf{X})$, the *entropy* of X is defined by: $h(\mathsf{X}) = \lim_{n\to\infty} \frac{1}{n} \log_2 \mathrm{Card}\,(F(\mathsf{X}) \cap A^n)$ and is an effectively computable "dynamic invariant" of a sofic shift. A shift X is *of finite type* if it is defined by the condition that $F(\mathsf{X})$ does not contain a finite set of words (*i.e.* $A^* \setminus F(\mathsf{X})$ is a finitely generated ideal).

Let $\mathsf{X} \subseteq A^{\mathbb{Z}}$ and $\mathsf{W} \subseteq C^{\mathbb{Z}}$ be two sofic shifts. A map $\Phi\colon \mathsf{W} \to \mathsf{X}$ is called a *k-block map* if there exist a map $\overline{\Phi}\colon C^k \to A$ and two nonnegative integers m (for memory) and a (for anticipation) with $k = m + 1 + a$ such that $\Phi((c_n)_{n\in\mathbb{Z}}) = (a_n)_{n\in\mathbb{Z}}$ iff $\overline{\Phi}(c_{n-m} \dots c_n \dots c_{n+a}) = a_n$ for every $n \in \mathbb{Z}$. A *block map* is a k-block map for some positive integer k. A block map[10] is *finite-to-one* if the cardinal of $\Phi^{-1}(\mathbf{x})$ is bounded (independently of $\mathbf{x}$).

Two sofic shifts X and Y are *finitely equivalent* if is there is a shift of finite type W together with finite-to-one and onto block maps such that $\Phi\colon \mathsf{W} \to \mathsf{X}$ and $\Psi\colon \mathsf{W} \to \mathsf{Y}$. All terms used in the FET are now defined. The connection with Theorem 1 requires one more definition, and a double encoding.

An *edge shift* X is a sofic shift with an underlying graph G whose edges all have distinct labels. It is thus completely described by the adjacency matrix X of G, a matrix with entries in $\mathbb{N}$.

[10] Note that for $\Phi\colon \mathsf{W} \to \mathsf{X}$ being a (k-)block map does not depend on W and X whereas the property of being finite-to-one does, and this is the reason why we consider that the definition of Φ depend on W and X.

Standard techniques in symbolic dynamics reduce the FET to the case of edge shifts X and Y whose adjacency matrices are denoted by X and Y respectively. The proof of sufficiency of the entropy condition relies then on two steps. The first step, known as Furstenberg's lemma, shows that, when X and Y have equal entropy, there is a nonnegative and nonnull matrix F such that $XF = FY$. The second step constructs the adjacency matrix W of an edge shift W, together with finite-to-one and onto block maps $\Phi\colon \mathsf{W} \to \mathsf{X}$ and $\Psi\colon \mathsf{W} \to \mathsf{Y}$.

Now, the edge shifts X and Y may be seen as $\mathbb{N}$-automata over a one letter alphabet. Theorem 1 then applies to these two automata and yields an automaton that corresponds to the edge shift W, the covering and co-covering corresponding to block maps Φ and Ψ. The computation of the matrix G in the proof of Theorem 2 corresponds to the original construction for the second step of the proof of the FET, known as "filling in the tableau" (see [12, Example 8.3.11]).

3 The reduction theorems

A $\mathbb{K}$-automaton $\mathcal{A} = \langle I, E, T\rangle$ can be seen as a triple (I, μ, T), where μ is the morphism from A^* into $\mathbb{K}^{n\times n}$ such that $E = \sum_{a\in A} \mu(a)a$. A $\mathbb{K}$-representation, or a $\mathbb{K}$-automaton, is *minimal* if it has a minimal dimension, or a minimal number of states, among all $\mathbb{K}$-representations, or all $\mathbb{K}$-automata, that realize the same series.

3.1 Reduction in a skew field

The computation of a minimal representation by Schützenberger's reduction algorithm [17, 3] has two symmetrical steps: a *left reduction* and a *right reduction*; it may be described within the framework of conjugacy of automata.

The left reduction of $\mathcal{A} = (I, \mu, T)$ consists in computing a matrix X whose rows form a basis of the vector space[11] $\langle I\,\mu(A^*)\rangle$. The matrix X uniquely defines the automaton $\mathcal{B}$ such that $\mathcal{B} \overset{X}{\Longrightarrow} \mathcal{A}$; the dimension of $\mathcal{B}$ is equal to the one of $\langle I\,\mu(A^*)\rangle$. Likewise, the right reduction of $\mathcal{A}$ consists in computing a matrix Y whose columns form a basis of the (right) vector space $\langle \mu(A^*)\,T\rangle$ and Y uniquely defines the automaton $\mathcal{C}$ such that $\mathcal{A} \overset{Y}{\Longrightarrow} \mathcal{C}$; the dimension of $\mathcal{C}$ is equal to the one of $\langle \mu(A^*)T\rangle$. The following property is the basis of the reduction algorithm:

Proposition 3. *Let $\mathbb{F}$ be a skew field. A left reduction followed by a right reduction applied to a $\mathbb{F}$-automaton $\mathcal{A}$ yields an equivalent minimal automaton.*

The computation of a left or right reduction (*i.e* the computation of bases of the appropriate subspaces) is made effective, *via* the *completion basis theorem* by the following lemma.

Lemma 1. *Let (I, μ, T) be a $\mathbb{F}$-representation and P a finite subset of A^* which contains the empty word 1_{A^*}. If, for every a in A and every w in P, $I\,\mu(wa)$ belongs to $\langle I\,\mu(P)\rangle$ then $\langle I\,\mu(P)\rangle = \langle I\,\mu(A^*)\rangle$ (and the symmetric for $\langle \mu(P)\,T\rangle$).*

[11] Modules over a skew field are called vector spaces (*cf.* [11]). As $\mathbb{F}$ is non commutative, one should distinguish between *left* and *right* vector spaces. $I\,\mu(S)$ is the set of vectors $I\,\mu(w)$ for $w \in S$; $\langle U\rangle$ is the vector space generated by the set U of vectors.

The algorithm of left reduction consists in finding such a finite set P by considering words of A^* in the lexicographic order; P is prefix-closed and the set $I\,\mu(P)$ is a basis of $\langle I\,\mu(A^*)\rangle$. Likewise, the algorithm of right reduction yields a suffix-closed set of words. The reduction algorithm applied to two equivalent $\mathbb{F}$-automata (using the same order) yields the *same* minimal automaton and conversely we have the following.

Lemma 2 ([7]). *If $\mathbb{F}$ is a skew field, two minimal equivalent $\mathbb{F}$-automata are similar, i.e. conjugate with an invertible transfer matrix.*

If $\mathcal{A}$ and $\mathcal{B}$ are two equivalent $\mathbb{F}$-automata, then there exist two reduced automata $\mathcal{R}$ and $\mathcal{R}'$ such that $\mathcal{A} \overset{X}{\Longleftarrow}\overset{Y}{\Longrightarrow} \mathcal{R}$, and symmetrically $\mathcal{B} \overset{X'}{\Longrightarrow}\overset{Y'}{\Longleftarrow} \mathcal{R}'$. By Lemma 2, $\mathcal{R} \overset{Z}{\Longrightarrow} \mathcal{R}'$. Hence, $\mathcal{A} \overset{X}{\Longleftarrow}\overset{YZY'}{\Longrightarrow}\overset{X'}{\Longleftarrow} \mathcal{B}$, which proves Theorem 3.

3.2 Reduction in an Euclidean domain

We now deal with automata with multiplicity in an Euclidean domain $\mathbb{K}$ instead of in a skew field $\mathbb{F}$. (In particular, $\mathbb{Z}$ is an Euclidean domain.) There is a *dimension theory* for the free modules[12] over $\mathbb{K}$ just as the one for the vector spaces over $\mathbb{F}$ — that is any two bases of a $\mathbb{K}$-module have the same cardinal. On the other hand the completion basis theorem does not hold anymore in $\mathbb{K}$-modules. We present here a reduction algorithm that overcomes this difficulty.

In fact the proof of Proposition 3 and Lemma 1 readily extends for Euclidean domain but does not yields an effective procedure anymore. The problem arises from the fact that two $\mathbb{K}$-modules can be strictly contained one in the other and still have the same dimension. Nevertheless, the following result implies the existence of an effective procedure for the reduction algorithm.

Proposition 4. *Let (I, μ, T) be a $\mathbb{K}$-representation. There exists a finite subset P of A^* such that $\langle I\,\mu(P)\rangle = \langle I\,\mu(A^*)\rangle$.*

In contrast with the case where the multiplicity is taken in a field, we have no a priori bound (given the dimension of (I, μ, T)) on the number of elements in the set P and the basis of $\langle I\mu(P)\rangle$ is not found in the set of vectors $\{I\mu(w) \mid w \in P\}$ but in the set of the linear combinations of them.

Example 3. Let $\mathcal{A}_3 = \langle I_3, \mu_3, T_3\rangle$ be the $\mathbb{Z}$-automaton defined by:

$$I_3 = \begin{pmatrix}3 & 4\end{pmatrix},\ \mu_3(a) = \begin{pmatrix}-1 & 4\\ 1 & -3\end{pmatrix},\ \mu_3(b) = \begin{pmatrix}-4 & 3\\ 3 & -2\end{pmatrix},\ T_3 = \begin{pmatrix}1\\ 1\end{pmatrix}.$$

Here $\langle I\mu(A^*)\rangle$ is $\mathbb{Z}^2$ and a finite set P such that $\langle I\mu(P)\rangle = \mathbb{Z}^2$ is for instance $\{\varepsilon, a, ab\}$. Neither $\{\varepsilon, a\}$ nor $\{\varepsilon, b\}$ — that are the only prefix-closed sets of cardinal 2 — corresponds to a basis.

The reduction algorithm yields then directly a chain of four conjugacies between two equivalent $\mathbb{K}$-automata. Lemma 2 does not hold anymore and reducing the length of the chain from four to three requires a new result from which Theorem 3 then follows easily.

[12] All the modules we consider here are free and we just call them modules.

Proposition 5. *Let $\mathbb{K}$ be an Euclidean domain. If $\mathcal{A}$ and $\mathcal{B}$ are equivalent $\mathbb{K}$-automata, with $\mathcal{B}$* right reduced*, then there are a $\mathbb{K}$-automaton $\mathcal{C}$ and matrices X and Y such that: $\mathcal{A} \overset{X}{\Longleftarrow} \mathcal{C} \overset{Y}{\Longrightarrow} \mathcal{B}$.*

4 Final result

We first establish a number of properties for coverings that can be seen as "backward Church-Rosser properties", that is properties that allow to complete a commutative diagram when the *lower part* of it is known.

Proposition 6. *Let $\mathbb{K}$ be an* equisubtractive *semiring and let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ be three $\mathbb{K}$-automata.*

(a) If $\mathcal{A}$ and $\mathcal{B}$ are $\mathbb{K}$-coverings of $\mathcal{C}$ (resp. co-$\mathbb{K}$-coverings of $\mathcal{C}$), there exists a $\mathbb{K}$-automaton $\mathcal{D}$ which is a $\mathbb{K}$-covering (resp. a co-$\mathbb{K}$-covering) of both $\mathcal{A}$ and $\mathcal{B}$.

(b) If $\mathcal{A}$ is a $\mathbb{K}$-covering of $\mathcal{C}$ and $\mathcal{B}$ is a co-$\mathbb{K}$-covering of $\mathcal{C}$, there exists a $\mathbb{K}$-automaton $\mathcal{D}$ which is both a co-$\mathbb{K}$-covering of $\mathcal{A}$ and a $\mathbb{K}$-covering of $\mathcal{B}$.

Lemma 3. *Let D be a circulation, C a co-amalgamation and R an amalgamation matrix such that DC and RD are defined. Then there exist circulation matrices D' and D'' such that $DC = CD'$ and $RD = D''R$.*

The proof of Theorem 4 now boils down to the diagram of Figure 5. Given equivalent $\mathbb{H}$-automata $\mathcal{A}$ and $\mathcal{B}$, Theorem 3 yields the bottom line of the diagram whereas Theorem 2 allows to build the diagrams 1, 2 and 3; Proposition 5 (a) gives 4 and 5, Lemma 3 6, 7 and 8; Proposition 5 (b) gives 9 and Lemma 3 again completes the full diagram with 10 and 11.

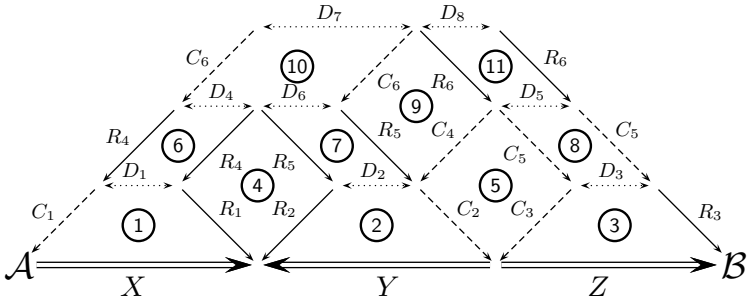


Fig. 5. Proof of Theorem 4.

5 The way for further developments

The gap that still remains between the above results and those formely known raise a number of questions. Let $\mathcal{A}$ and $\mathcal{B}$ be two equivalent $\mathbb{Z}$-automata. We know that they are not always conjugate one to the other and it is decidable (*cf.* [16]) in polynomial time (resp. in exponential time) if $\mathcal{A}$ is conjugate to $\mathcal{B}$ with a transfer matrix in $\mathbb{Z}$ (resp. with a transfer matrix in $\mathbb{N}$). Theorem 2 states the existence of a chain of three conjugacies between $\mathcal{A}$ and $\mathcal{B}$.

One then may ask whether *three* conjugacies are necessary (in general), and, if yes, whether it is decidable when *two* conjugacies suffice.

If moreover $\mathcal{A}$ and $\mathcal{B}$ are (equivalent) $\mathbb{N}$-automata, one may ask also whether the chain of conjugacies could be always realized with transfer matrices in $\mathbb{N}$ and, if not, whether it is decidable when this property holds.

By means of techniques different from the ones presented here, it can be shown that in both cases the stronger property holds: the answer to the first question is no and two conjugacies always suffice, the answer to the second question is yes and two equivalent $\mathbb{N}$-automata are joined by a chain of *four* conjugacies with transfer matrices in $\mathbb{N}$. This is the object of on-going work of the authors and will be presented in a forthcoming publication.[13]

Acknowledgements The authors are grateful to a careful referee whose remarks helped them to make the definitions more precise and the presentation hopefully clearer and to Prof. W. Kuich who pointed to several references.

References

1. Arnold, A. *Finite Transitions Systems*. Prentice-Hall, 1994.
2. Béal, M.-P., and Perrin, D. On the generating sequences of regular languages on k symbols. *J. ACM 50* (2003), 955–980.
3. Berstel, J., and Reutenauer, Ch. *Rational Series and their Languages*. Springer, 1988.
4. Bloom, S., and Esik, Z. *Iteration Theories*. Springer, 1993.
5. Cardon, A., and Crochemore, M. Détermination de la représentation standard d'une série reconnaissable. *RAIRO Inform. Théor. 14* (1980), 371–379.
6. Eilenberg, S. *Automata, Languages, and Machines. Vol. A*. Academic Press, 1974.
7. Fliess, M. Matrices de Hankel. *J. Math. Pures Appl. (9) 53* (1974), 197–222.
8. Flouret, M., and Laugerotte, E. Noncommutative minimization algorithms. *Inform. Process. Lett. 64* (1997), 123–126.
9. Harju, T., and Karhumäki, J. The equivalence problem of multitape finite automata. *Theoret. Comput. Sci. 78* (1991), 347–355.
10. Kuich, W., and Salomaa, A. *Semirings, Automata, Languages*. Springer, 1986.
11. Lang, S. *Algebra*. Addison Wesley, 1965.
12. Lind, D., and Marcus, B. *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press, 1995.
13. Lombardy, S. and Sakarovitch, J. Derivatives of rational expressions with multiplicity. *Theoret. Comput. Sci. 332* (2005), 141–177.
14. Sakarovitch, J., *Eléments de théorie des automates*, Vuibert, 2003. English translation, Cambridge Universit Press, to appear.
15. Salomaa, A., and Soittola, M. *Automata-theoretic Aspects of Formal Power Series*. Springer, 1978.
16. Schrijver, A. *Theory of Linear and Integer Programming*. Wiley, 1986.
17. Schützenberger, M. P. On the definition of a family of automata. *Information and Control 4* (1961), 245–270.

[13] The above questions were quoted as open problems in the paper that was submitted to ICALP and reviewed by the PC. But since then, we have made progress and are able to answer them. They are thus not open problems anymore, and on the other hand we could not include the answers as results since they have not been refereed.