ELSEVIER

Theoretical Computer Science 293 (2003) 55–82

Theoretical Computer Science

www.elsevier.com/locate/tcs

The finite power property in free groups ☆

Flavio d'Alessandro[a,*], Jacques Sakarovitch[b]

[a] *Dipartimento di matematica, Università degli Studi di Napoli - Federico II, Italy*
[b] *Laboratoire Traitement et Communication de l'Information, E.N.S.T./C.N.R.S., Paris, France*

Abstract

We show that the finite power property is decidable for rational sets in the free group. The complexity of the construction involved in the decision procedure may be lowered to $O(n^3)$—where n is the cardinality of the state set of the automaton that defines the rational set.

Résumé

La propriété de puissance finie est décidable pour les parties rationnelles du groupe libre. La complexité de la construction utilisée par la procédure de décision peut être ramenée à $O(n^3)$—où n est le nombre d'états de l'automate qui définit la partie rationnelle.

Keywords: Formal languages; Distance automata; Free group

1. Introduction

A subset L of a free monoid A^* is said to have *the finite power property*, or, in an older terminology, to be *limited*, if there exists an integer n such that

$$L^* = L^{\leqslant n}$$

(where $L^{\leqslant n}$ denotes the set ${}^1A^* \cup L \cup L^2 \cup \cdots \cup L^n$); in other words, if L is such that the *infinite* sum L^* reduces to a *finite* one.

☆ Journal version of a communication published under the same title in *Idempotency*, Cambridge University Press, 1998 (cf. [7]).

* Corresponding author. Dip. di Matematica 'Guido Castelnuovo' Piazzale Aldo Moro 2, I-00185 Roma, Italy.

E-mail address: dalessan@mat.uniroma1.it (F. d'Alessandro).

0304-3975/03/$ - see front matter
PII: S0304-3975(02)00232-3

In 1966, Brzozowski raised the question whether such a property is decidable for rational languages, positively settled in 1978 by Hashiguchi [10] and Simon [17], independently. Soon afterwards, it was established that the same property is undecidable for context-free languages, the next class in the Chomsky hierarchy of languages [13].

Clearly, the decidability of the finite power property may be investigated for any family of (effectively defined) subsets in any monoid—under the natural restriction that multiplication and rational sets can be effectively computed. We shall prove here the following.

Theorem 1. *It is decidable whether a rational set of a free group has the finite power property.*

Note that the family of rational subsets of the free group defines a family of deterministic context-free languages for which the finite power property is thus decidable.

In order to elaborate on Theorem 1 let us first come back to the finite power property for rational languages. The basic notion involved in the problem is the one of *distance automaton*. A distance automaton $\mathscr{A}$ is a (finite nondeterministic) automaton the transitions of which are not only labelled by a letter in an alphabet A but also given *a coefficient*, taken in the "min-plus" semiring $\mathscr{M}$; the automaton $\mathscr{A}$ then associates a coefficient, denoted by $f\|\mathscr{A}\|$, to every word f of A^*: $f\|\mathscr{A}\|$ is an integer if f is accepted by $\mathscr{A}$, is the infinite otherwise.

The *transition monoid* of a distance automaton is thus a monoid of matrices with entries in $\mathscr{M}$. Simon's solution of Brzozowski's problem amounts to proving the decidability of the finiteness of a (finitely generated) monoid of such matrices, for the distance automaton involved in the problem has a particular form.

A distance automaton $\mathscr{A}$ is said to be *bounded* if the finite coefficients $f\|\mathscr{A}\|$ are bounded when f ranges over A^*. Later, Hashiguchi established that it is decidable whether a distance automaton is bounded [11,12]. This gives an alternative to Simon's solution, but it is more complicated (cf. [18] for a complete analysis of the relationships between the various problems and solutions in the domain).

The first idea which our proof of Theorem 1 is based on is the transfer of the problem into a problem for languages in the free monoid. Let X be a rational set in the free group $F(A)$; it is known (Benois's theorem) that the corresponding set of reduced words $R = X\imath$ is a rational language. It is not true that X has the finite power property if and only if R has it. But we show that there exists an effectively computable distance automaton, noted $\mathscr{U}_X$, such that X has the finite power property if and only if $\mathscr{U}_X$ is bounded. The solution follows then from Hashiguchi's result (for distance automata).

The situation is even closer to the one in the free monoid for we show that X has the finite power property if and only if the transition monoid of $\mathscr{U}_X$ is finite (Proposition 14). Finally we also show that the automaton $\mathscr{U}_X$ may be replaced in these decision procedures by another one, the computation of which is very efficient (Proposition 19).

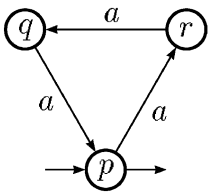


Fig. 1. The automaton $\mathscr{A}_1$.

2. Distance automata and the finite power property

We basically follow the definitions and notations of [8,5] for rational and recognizable sets as well as for automata. Let us recall though few elements of the vocabulary.

In the sequel A denotes a finite set or alphabet and A^* the free monoid generated by A. The elements of A are called *letters* and those of A^* *words*. The identity element of A^* is denoted by 1_{A^*}. A subset of A^* is also called a *language* (*over* A).

A finite *automaton over a finite alphabet* A, $\mathscr{A} = \langle Q, A, E, I, T\rangle$ is a directed graph labelled by elements of A; Q is the finite set of *states*, $I \subseteq Q$ is the set of *initial* states, $T \subseteq Q$ is the set of *terminal* states and $E \subseteq Q \times A \times Q$ is the set of labelled *edges*. We shall consider only finite automata and thus call them simply *automata* in the sequel.

We also note $p \xrightarrow{a} q$ for $(p,a,q) \in E$, or even $p \xrightarrow[\mathscr{A}]{a} q$ if there is a possible ambiguity on the automaton. A *computation* c in $\mathscr{A}$ is a finite sequence of labelled edges that form a path in the graph:

$$c = q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} \cdots \to q_{n-1} \xrightarrow{a_n} q_n.$$

The state q_0 is the *origin*, and the state q_n is the *end* of the computation c; the *label* of c, denoted by $|c|$, is the element $a_1 a_2 \cdots a_n$ of A^*. The computation c is *successful* if $q_0 \in I$ and $q_n \in T$. The *language recognized* (or *accepted*) by $\mathscr{A}$ is the subset of A^*, denoted by $|\mathscr{A}|$, consisting of the labels of successful computations of $\mathscr{A}$. As labelled graphs, automata have a natural graphic representation.

Example 1. Let $\mathscr{A}_1 = \langle \{p,q,r\}, a, E_1, p, p\rangle$ be the automaton over the one letter alphabet $A_1 = \{a\}$, the edges of which are: $E_1 = \{(q,a,p),(p,a,r),(r,a,q)\}$. Then $\mathscr{A}_1$ is represented as in Fig. 1a and $|\mathscr{A}_1| = \{a^n \mid n \equiv 0 \mod 3\}$.

A subset of A^* is said to be *recognizable* if, and only if, it is recognized by a finite automaton over A. The family of recognizable languages, $\mathrm{Rec}\, A^*$, is closed under union, intersection and complementation.

In A^*—as in any monoid M—the family of *rational subsets*, denoted by $\mathrm{Rat}\, A^*$—or $\mathrm{Rat}\, M$—is the smallest family of subsets of A^* (of M) containing the finite subsets and closed under union, product and star. Kleene's theorem states that $\mathrm{Rat}\, A^* = \mathrm{Rec}\, A^*$ (if A is finite).

2.1. Matrix representations of automata

An automaton $\mathscr{A} = \langle Q, A, E, I, T \rangle$ can also be described by a *matrix representation* (λ, μ, v), where

$$\mu : A^* \to \mathbb{B}^{Q \times Q}$$

is a morphism from A^* into the monoid of square Boolean matrices of dimension Q, λ and v are, respectively, a Boolean row vector and column vector of dimension Q. It then holds that

$$|\mathscr{A}| = \{ f \in A^* \mid (\lambda \cdot f\mu \cdot v) = 1 \}$$

or equivalently

$$\forall f \in A^*, \quad f \in |\mathscr{A}| \quad \Leftrightarrow \quad (\lambda \cdot f\mu \cdot v) = 1.$$

Example 1 (continued). The automaton $\mathscr{A}_1$ has the following matrix representation:

$$\lambda_1 = (1 \quad 0 \quad 0), \quad a\mu_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

The matrix representation is particularly suited for the generalization of automata to automata with *multiplicity*, i.e. automata which do not only "accept" (or "reject") a word but associate to every word f a coefficient, the *multiplicity* of f, taken in a suitable semiring. We consider in this paper *distance automata* which are precisely automata of that kind, with multiplicities taken in the "min-plus" semiring.

2.2. The "min-plus" semiring

We denote by $\mathscr{M}$ the idempotent "min-plus" semiring $(\mathbb{N} \cup \{+\infty\}; \min, +)$, which we also call "*tropical semiring*" according to an established use in the field of automata theory (cf. [15]).

The "addition" of $\mathscr{M}$ is the min operation on the set $\mathbb{N} \cup \{+\infty\}$, for which the identity element, the "zero" of $\mathscr{M}$, denoted by $0_{\mathscr{M}}$, is the element $+\infty$; indeed $\min\{x, +\infty\} = x$ for every x in $\mathbb{N} \cup \{+\infty\}$. The "multiplication" of $\mathscr{M}$ is the usual $+$ operation with the natural convention that $x + (+\infty) = (+\infty) + x = +\infty$ for every x in $\mathbb{N} \cup \{+\infty\}$; 0, the identity element for $+$, is thus the "one" of $\mathscr{M}$ which we denote by $1_{\mathscr{M}}$.

Notation. There is a true difficulty in coining notation for the operations of the semiring $\mathscr{M}$. They should refer clearly to addition and multiplication symbols in order to keep their outlook to algebraic formulae. They can hardly be simply $+$ and $\times$ for $\times$ (in $\mathscr{M}$) is $+$ (in $\mathbb{N}$)…. Many authors use $\oplus$ and $\otimes$ and we would do so if we were not using the tensor product as well, naturally noted $\otimes$. We shall use the symbols $\underset{\mathscr{M}}{+}$ and $\underset{\mathscr{M}}{\bullet}$, but we stick to the classical $\sum$, without any diacritic, for summation.

The semiring $\mathscr{M}$ is *idempotent*: $x \underset{\mathscr{M}}{+} x = \min(x,x) = x$ for any x in $\mathscr{M}$ and thus *positive*: the mapping $\mathrm{supp}: \mathscr{M} \to \mathbb{B}$ defined by $\mathrm{supp}(x) = 1_{\mathbb{B}}$ for any $x \neq +\infty$ and $\mathrm{supp}(\infty) = 0_{\mathbb{B}}$ is a morphism. The subset $\{0_{\mathscr{M}}, 1_{\mathscr{M}}\} = \{+\infty, 0\}$ is a semiring of $\mathscr{M}$, isomorphic to $\mathbb{B}$.

Moreover, $\mathscr{M}$ is *complete*: the operation $\sum_{i\in\mathscr{J}} x_i$ is defined in $\mathscr{M}$ for any family $\{x_i\}_{i\in\mathscr{J}}$ of elements of $\mathscr{M}$, where $\mathscr{J}$ is any set of indices, *finite* or *infinite*.

2.3. Distance automata

Let $\mathscr{A} = \langle Q, A, E, I, T\rangle$ be an automaton as above; we turn $\mathscr{A}$ into a *distance automaton* by adjoining to $\mathscr{A}$ a mapping

$$\sigma : E \to \mathscr{M},$$

which associates *a distance*[1] to every edge.

We find it convenient to adopt in the sequel the notations introduced in [18]: for a computation c in $\mathscr{A}$, its *label*, denoted by $|c|$, is the product of letters of its edges and the *multiplicity* of c, denoted by $\|c\|$, is the product of multiplicities of its edges that is, since we are in $\mathscr{M}$, the sum of integers which are the coefficients of the edges.

As for classical automata we denote by $|\mathscr{A}|$ the set of labels of successful computations. The *behaviour* of $\mathscr{A}$ is a mapping from A^* into $\mathscr{M}$ (we later call such a mapping *a series*) denoted by $\|\mathscr{A}\|$: for every word f of A^*, $f\|\mathscr{A}\|$, called *the multiplicity of* f is the sum, that is—since we are in $\mathscr{M}$—the *minimum* of the multiplicities $\|c\|$ for all successful computations c, the label $|c|$ of which is equal to f. Note that $|\mathscr{A}| = \{f \in A^* \mid f\|\mathscr{A}\| < +\infty\}$.

A distance automaton $\mathscr{A}$ can be equivalently described by a *representation* (η, κ, ζ) where $\kappa : A^* \to \mathscr{M}^{Q\times Q}$ is a morphism from A^* into $\mathscr{M}^{Q\times Q}$ and where η and ζ are two row and column vectors of dimension Q with entries in $\mathscr{M}$. For every f in A^* it then holds $f\|\mathscr{A}\| = \eta \underset{\mathscr{M}}{\bullet} f\kappa \underset{\mathscr{M}}{\bullet} \zeta$.

Note that any "classical" automaton $\mathscr{A}$ is easily, and canonically, turned into a distance automaton, denoted again by $\mathscr{A}$, where the multiplicity of every existing edge is 0. If (λ, μ, ν) is the representation of $\mathscr{A}$ as a classical automaton then the representation (η, κ, ζ) of $\mathscr{A}$ as a distance automaton is obtained by replacing $0_{\mathbb{B}}$ with $0_{\mathscr{M}} = +\infty$ and $1_{\mathbb{B}}$ with $1_{\mathscr{M}} = 0$ in the matrices and vectors. It then holds that, for every f in $|\mathscr{A}|$, $f\|\mathscr{A}\| = 0$ (and for every f not in $|\mathscr{A}|$, $f\|\mathscr{A}\| = +\infty$).

A distance automaton $\mathscr{A}$ is said to be *bounded* if there exists an integer M such that, for every $f \in |\mathscr{A}|$, $f\|\mathscr{A}\| < M$.

Theorem 2 (Hashiguchi [11]). *It is decidable whether a distance automaton is bounded.*

[1] This is the established terminology in automata theory, after the work of Hashiguchi; the term *cost* or *weight* would have been better fitted.

Several proofs of this fundamental result have been given subsequently (cf. [18] for complete references). In the two cases we shall be interested in (rational sets in a free monoid and in a free group), the decidability of the finite power property directly follows from Hashiguchi's theorem after the construction of a distance automaton; however we shall see that in both cases they may also be derived, with a little more work, from another theorem, the proof of which is easier.

2.4. The finite power property

Let L be a language of A^* and let f be a word in L^*. We call *the order of f with respect to L*, denoted by $o_L(f)$, the least integer n such that f is in L^n:

$$o_L(f) = \min\{n \in \mathbb{N} \mid f \in L^n\}.$$

With that definition, L has the finite power property, if and only if there exists a bound for the order of all words of L^*.

Let us recall a construction due to Simon (cf. [17]) which, given an automaton $\mathscr{A} = \langle Q, A, E, I, T\rangle$ yields a distance automaton $\mathscr{S}_{\mathscr{A}}$ which computes the order of every word with respect to $L = |\mathscr{A}|$.

Let first $\mathscr{S}_{\mathscr{A}} = \langle Q \cup s, A, E', s, s\rangle$ be the automaton which recognizes L^*, obtained by the classical construction: s is a new state which does not belong to Q and E' is formally defined by the formula

$$\begin{aligned} E' = E &\cup \{(s,a,s) \mid (i,a,t) \in E,\ i \in I,\ t \in T\} \\ &\cup \{(s,a,p) \mid (i,a,p) \in E,\ i \in I\} \\ &\cup \{(p,a,s) \mid (p,a,t) \in E,\ t \in T\}. \end{aligned}$$

We then turn $\mathscr{S}_{\mathscr{A}}$ into a distance automaton with the distance map $\sigma : E' \to \mathscr{M}$ defined by

$$(p,a,q)\sigma = \begin{cases} 1 & \text{if } q = s, \\ 0 & \text{otherwise.} \end{cases}$$

Example 1 (continued). The only transition with distance explicitly written on its label in Fig. 2 is the one with distance 1, indicated with a double arrow as well. The other transitions with a single letter as label have distance 0.

Proposition 1 (Simon [17]). *Let $\mathscr{A}$ be an automaton over A which recognizes a language L. Then $\mathscr{S}_{\mathscr{A}}$ is a distance automaton which computes the order of any word of A^* with respect to L:*

$$|\mathscr{S}_{\mathscr{A}}| = L^* \quad \text{and} \quad \forall f \in A^*,\ f\|\mathscr{S}_{\mathscr{A}}\| = o_L(f).$$

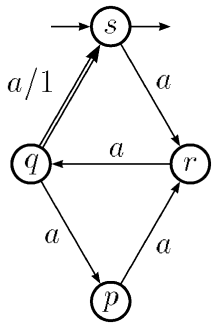


Fig. 2. $\mathscr{S}_{\mathscr{A}_1}$, the Simon automaton of $\mathscr{A}_1$.

Proof. To every successful computation $c = i \xrightarrow{f} t$ of $\mathscr{A}$ corresponds a (unique) successful computation $d = s \xrightarrow{f} s$ of $\mathscr{S}_{\mathscr{A}}$ which passes by exactly the same states as c except for the extremities, that is the origin i and the end t of the computation. Hence $\|d\| = 1$. Let now be f in L^*; for every factorization $f = f_1 f_2 \cdots f_k$ with $f_i \in L$ there exists a computation d of $\mathscr{S}_{\mathscr{A}}$

$$d = s \xrightarrow{f_1} s \xrightarrow{f_2} s \to \cdots \to s \xrightarrow{f_{k-1}} s \xrightarrow{f_k} s$$

with $\|d\| = k$. Thus for every f in L^* $f\|\mathscr{S}_{\mathscr{A}}\| = \min\{k \mid f \in L^k\} = o_L(f)$. □

By a slight abuse, we also call *the Simon automaton of a rational subset L of* A^*, and denote it by $\mathscr{S}_L$, any automaton $\mathscr{S}_{\mathscr{A}}$, where $\mathscr{A}$ is any automaton which recognizes L. The following is then a direct consequence of Theorem 2 and of Proposition 1.

Theorem 3 (Hashiguchi [10], Simon [17]). *It is decidable whether a given rational subset of a free monoid has the finite power property.*

Note that none of the references we quoted for Theorem 3 makes use of Theorem 2. The proof in [10] is direct and combinatorial (and rather a prefiguration of Theorem 2 than a consequence of it). The proof in [17] takes advantage of a property of the distance automaton $\mathscr{S}_L$ which is stated in the following.

Proposition 2 (Simon [17]). *Let $\mathscr{S}_L = (\eta, \kappa, \zeta)$ be the Simon automaton of a rational language L of A^*. Then $\mathscr{S}_L$ is a bounded distance automaton if and only if the matrix monoid $A^*\kappa = (A\kappa)^*$ is finite.*

Theorem 3 is then a direct consequence of the following.

Theorem 4 (Simon [17]). *Given a finite subset X of $\mathscr{M}^{n\times n}$, it is decidable whether the matrix submonoid X^* of $\mathscr{M}^{n\times n}$ is finite.*

3. The relative finite power property

Before turning to the finite power property in the free group, we slightly generalize the notion of the finite power property in the free monoid, for the techniques involved will be used in the sequel.

Given two subsets L and K of A^*, we say that L satisfies the *finite power property relative to* K if there exists an integer n such that

$$L^* \cap K = L^{\leqslant n} \cap K.$$

The usual definition of the finite power property is obtained by setting $K = A^*$.

Example 2. Let $\tilde{A}_1 = \{a, \bar{a}\}$ and $R_1 = \{a^3\}^* \cup \{\bar{a}^2\}^*$. R_1 is not limited in $\tilde{A}_1^*$ since, for every integer m, $(a^3\bar{a}^2)^m$ belongs to R_1^n if and only if $n = 2m$. Let now $K_1 = a^* \cup \bar{a}^*$. It is clear that $R_1^* \cap K_1 = R_1 \cap K_1\,(= R_1)$ and thus R_1 is limited relative to K_1.[2]

Theorem 3 generalizes in the following:

Proposition 3. *Given L and K, two rational subsets of A^*, it is decidable whether L has the finite power property relative to K.*

The proof of Proposition 3 requires some definitions and the quotation of few classical results.

Hadamard product of series: let us adopt the terminology of formal power series in order to deal with distance automata.

Any mapping s from A^* into $\mathscr{M}$ is also called *a* (*formal power*) *series over A^* with coefficients in $\mathscr{M}$* and is written accordingly

$$s = \sum_{f \in A^*} \langle s, f \rangle f,$$

where $\langle s, f \rangle$, the *coefficient of f in s*, is indeed the value of s on f, i.e. $\langle s, f \rangle = (f)s$. The set of all series over A^* with coefficients in $\mathscr{M}$ is denoted by $\mathscr{M}\langle\langle A^* \rangle\rangle$.

The set of subsets of A^*, $\mathfrak{P}(A^*)$, is isomorphic to $\mathbb{B}\langle\langle A^* \rangle\rangle$, the semiring of series over A^* with coefficients in the Boolean semiring $\mathbb{B}$. The interest of this framework is that it allows us to deal with languages of A^* (i.e. subsets of A^*) or with mappings from A^* into $\mathscr{M}$ with coherent terminology and identical formulae. For instance, if $\mathscr{A}$ is an automaton with representation (λ, μ, ν) then

$$|\mathscr{A}| = \sum_{f \in A^*} (\lambda \cdot f\mu \cdot \nu) f$$

and if $\mathscr{A}$ is a distance automaton with representation (η, κ, ζ) then

$$\|\mathscr{A}\| = \sum_{f \in A^*} (\eta \underset{\mathscr{M}}{\bullet} f\kappa \underset{\mathscr{M}}{\bullet} \zeta) f.$$

[2] The notations in this example fit the conventions that will be taken later in Sections 4 and 5.

A series in $\mathscr{M}\langle\langle A^*\rangle\rangle$ is said to be *rational* if it is the behaviour of a (finite) distance automaton over A.

As the definition of the relative finite power property suggests, the next thing we have to do in that setting is to generalize the intersection of languages to series.

Definition 1 & Notation. The Hadamard product of two series s and t of $\mathscr{M}\langle\langle A^*\rangle\rangle$, denoted by $s \odot t$, is defined by the following:

$$\forall f \in A^*, \quad \langle s \odot t, f\rangle = \langle s, f\rangle \underset{\mathscr{M}}{\bullet} \langle t, f\rangle = \langle s, f\rangle + \langle t, f\rangle.$$

It should be clear that the same formula, applied to series in $\mathbb{B}\langle\langle A^*\rangle\rangle$, defines exactly the intersection. The following result holds.

Theorem 5 (Schützenberger [16]). *The Hadamard product of two rational series of $\mathscr{M}\langle\langle A^*\rangle\rangle$ is a rational series.*

We have to be more specific on the construction on which this result relies. It is indeed the mere generalization of the direct product of automata for the intersection of languages.

Let (η, κ, ζ) be the representation—of dimension Q—of the distance automaton $\mathscr{A}$ and (η', κ', ζ') be the representation—of dimension Q'—of the distance automaton $\mathscr{A}'$. Let us define the *tensor product* of the two representations by

$$(\eta, \kappa, \zeta) \otimes (\eta', \kappa', \zeta') = (\eta \otimes \eta', \kappa \otimes \kappa', \zeta \otimes \zeta').$$

It is the representation of dimension $Q \times Q'$, defined by the following formulae:

$$\begin{aligned}
&\forall a \in A,\ a(\kappa \otimes \kappa')_{(p,p'),(q,q')} = (a\kappa)_{(p,q)} \underset{\mathscr{M}}{\bullet} (a\kappa')_{(p',q')} = (a\kappa)_{(p,q)} + (a\kappa')_{(p',q')},\\
&(\eta \otimes \eta')_{(q,q')} = \eta_q \underset{\mathscr{M}}{\bullet} \eta'_{q'} = \eta_q + \eta'_{q'}\\
&(\zeta \otimes \zeta')_{(p,p')} = \zeta_p \underset{\mathscr{M}}{\bullet} \zeta'_{p'} = \zeta_p + \zeta'_{p'}.
\end{aligned}$$

The automaton $\mathscr{A} \otimes \mathscr{A}'$ is defined as the one whose representation is $(\eta, \kappa, \zeta) \otimes (\eta', \kappa', \zeta')$. With these notations, it then holds:

Proposition 4 (Schützenberger [16]).

$$\|\mathscr{A}\| \odot \|\mathscr{A}'\| = \|\mathscr{A} \otimes \mathscr{A}'\|,$$

which not only proves Theorem 5 but also shows that it is "effective". These formulae will probably be better understood when applied to our current example.

Example 2 (continued). Fig. 3 displays the distance automaton $\mathscr{S}_{R_1}$ for $R_1 = (a^3)^* \cup (\bar{a}^2)^*$, the characteristic distance automaton $\mathscr{K}_1$ of the language $K_1 = (a)^* \cup (\bar{a})^*$, and the tensor product $\mathscr{S}_{R_1} \otimes \mathscr{K}_1$. Since a 18×18 matrix is something unreadable, we have represented the transition graphs of the corresponding automata.

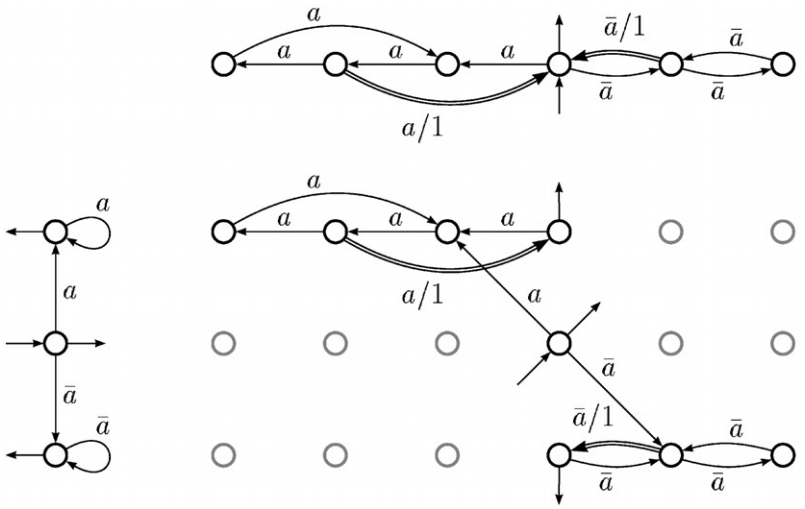


Fig. 3. The automata $\mathscr{S}_{R_1}$, $\mathscr{K}_1$ et $\mathscr{S}_{R_1} \otimes \mathscr{K}_1$.

Proof of Proposition 3. Let $\mathscr{K}$ be the characteristic distance automaton of K and let $\mathscr{S}_L$ be the Simon's automaton of L. Then for every f in A^*

$$f(\|\mathscr{S}_L\| \odot \|\mathscr{K}\|) = f\|\mathscr{S}_L \otimes \mathscr{K}\| = \begin{cases} o_L(f) & \text{if } f \in K, \\ +\infty & \text{otherwise.} \end{cases}$$

Hence L has the finite power property relative to K if and only if $\mathscr{S}_L \otimes \mathscr{K}$, which is effectively computable by Proposition 4, is bounded in distance, and this is decidable by Theorem 3. □

4. The free group: its elements and rational sets

Let A be a finite alphabet, $\bar{A}$ a disjoint copy of A and $\tilde{A} = A \cup \bar{A}$.

The free group generated by A, $F(A)$, is the quotient of $\tilde{A}^*$ by the congruence generated by the relations $\{z\bar{z} = 1_{\tilde{A}^*} \mid z \in \tilde{A}\}$—with the natural convention that $\overline{(\bar{z})} = z$. That congruence induces a canonical morphism:

$$\alpha : \tilde{A}^* \to F(A).$$

4.1. Dyck reduction

A word of $\tilde{A}^*$ is called *reduced* if it does not contain any factor of the form $z\bar{z}$, with z in $\tilde{A}$. Every element w of $\tilde{A}^*$ is congruent *modulo* α to a unique reduced word,

denoted by $w\rho$, and this defines a mapping

$$\rho : \tilde{A}^* \to \tilde{A}^*$$

called *Dyck reduction* (cf. [14]). Since $u\rho = v\rho$ implies $u\alpha = v\alpha$, there is a (unique) injective function

$$\iota : F(A) \to \tilde{A}^* \quad \text{such that} \quad \alpha \circ \iota = \rho.$$

We denote by K the set $(\tilde{A}^*)\rho$ of *reduced words* of $\tilde{A}^*$. The subset $(1_{F(A)})\alpha^{-1}$ is known as the *Dyck language* (over A, or A^*) and is denoted by D_A^*; its elements are the *Dyck words*. Let δ be the reflexive, regular and transitive closure of the relation

$$\{z\bar{z} = 1_{\tilde{A}^*} \mid z \in \tilde{A}\}.$$

Then g is in $f\delta$ if there exists a sequence of words $u_0 = f$, u_1, …, u_{n-1} and $u_n = g$ such that for every i there exist z in $\tilde{A}$, u_i' and u_i'', such that $u_i = u_i' z\bar{z} u_i''$ and $u_{i+1} = u_i' u_i''$. The relation δ is characterized by the following:

Lemma 5 (cf. Berstel [4, Lemma II.3.6] for instance). *Let f and g in $\tilde{A}^*$ with $g = a_1 a_2 \dots a_n$ in $f\delta$. Then there exist words $w_0, w_1, \dots, w_n$ in D_A^* such that $f = w_0 a_1 w_1 a_2 w_2 \cdots w_{n-1} a_n w_n$.*

By definition, δ is thinner than $\alpha\alpha^{-1}$ and thus $g \in f\delta$ implies $g\alpha = f\alpha$; finally

$$\forall f \in \tilde{A}^*, \quad f\rho = f\delta \cap K.$$

4.2. Factorizations of Dyck words

The subset D_A^* is a submonoid (for it is the inverse image of a submonoid); let D_A be the minimal generating set of D_A^*:

$$D_A = (D_A^* \setminus 1_{\tilde{A}^*}) \setminus (D_A^* \setminus 1_{\tilde{A}^*})^2.$$

Then D_A^* is *freely* generated by D_A, that is every w in $D_A^* \setminus 1_{\tilde{A}^*}$ has a *unique factorization*

$$w = w_1 w_2 \cdots w_n$$

with every w_i in D_A. Every word w in D_A may in turn be factorized as

$$w = z w' \bar{z}$$

with $z \in \tilde{A}$ and $w' \in D_A^*$ (cf. [4, Section II.3]).

Definition 2 & Notation. For every Dyck word w, we recursively define two integers: $h(w)$, called the *height* of w, and $p(w)$, the *width* of w, by the following

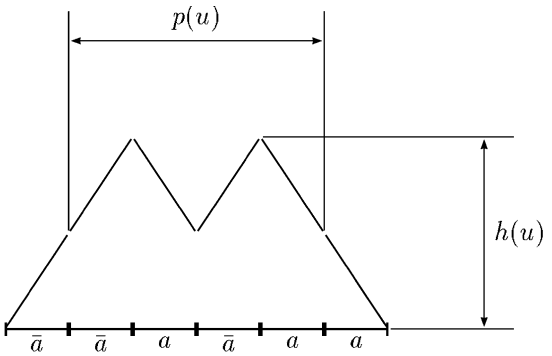


Fig. 4. The moves of the stack of $\mathscr{P}$ while reading u_1.

formulae:

$$h(1_{\tilde{A}^*}) = 0,$$

$$h(w) = \begin{cases} 1 + h(w') & \text{if } w \in D_A \quad \text{and} \quad w = zw'\bar{z} \ (z \in \tilde{A}, w' \in D_A^*), \\ \max\limits_{1 \leqslant i \leqslant n} \{h(w_i)\} & \text{if } w \notin D_A \quad \text{and} \quad w = w_1 \cdots w_n \ (w_i \in D_A), \end{cases}$$

$$p(1_{\tilde{A}^*}) = 0,$$

$$p(w) = \begin{cases} 1 & \text{if } w = z\bar{z} \ (z \in \tilde{A}), \\ p(w') & \text{if } w \in D_A \quad \text{and} \quad w = zw'\bar{z} \ (z \in \tilde{A}, w' \in D_A^+), \\ \max\limits_{1 \leqslant i \leqslant n} (\{p(w_i)\}, n) & \text{if } w \notin D_A \quad \text{and} \quad w = w_1 \cdots w_n \ (w_i \in D_A). \end{cases}$$

Although their definitions are nonoriented, these two integers $h(w)$ and $p(w)$ refer indeed to the *left most reduction* of the Dyck words. Such a reduction is performed for instance by the (stateless) pushdown automaton $\mathscr{P}$ which works as follows: it reads words of $\tilde{A}^*$ and writes the letters in the stack unless the currently read letter x is equal to the inverse letter of the topmost symbol of the stack; in this case, it erases this symbol from the stack. Then, for every w in D_A^*, $h(w)$ is the maximal level of the stack during the computation of $\mathscr{P}$ when reading w whereas $p(w)$ is the maximal number of consecutive passages of the stack at the same level *without going below that level*.

Example 3. If $u_1 = \bar{a}\,\bar{a}\,a\,\bar{a}\,a\,a$, then $h(u_1) = p(u_1) = 2$ and Fig. 4 shows the moves of the stack of $\mathscr{P}$ while reading u_1.

These integers $h(w)$ and $p(w)$ also describe two possible factorizations of w which are expressed in the following Lemma:

Lemma 6. *Let w be in D_A^* and let $h(w)=h$ and $p(w)=p$. The following hold*:
(i) *There exist words $v_1,\dots,v_p\in D_A$ and $f,g\in\tilde{A}^*$ such that*

$$w = f v_1 \cdots v_p g.$$

(ii) *There exist words $u_0,\dots,u_h\in D_A^*$ such that $w=u_h$ and*

$$u_{i+1} = f_i u_i g_i \quad \text{with} \quad f_i, g_i \in \tilde{A}^+, \ f_i g_i \in D_A^+ \quad \text{and} \quad h(u_i) = i.$$

Proof. (i) By induction on the length $|w|$ of w in D_A^*. If $|w|=2$ then $w=z\bar{z}$, $z\in\tilde{A}$, and $p(w)=1$ by definition.

Let w be in D_A^*, with $|w|>2$.

If $w\in D_A$, then $w=z\,w'\bar{z}$, $z\in\tilde{A}$, and $w'\in D_A^*$. Since $p=p(w)=p(w')$, by definition the induction hypothesis implies $w'=f'v_1\cdots v_pg'$, with $v_i\in D_A$ and $f',g'\in\tilde{A}^*$. Thus $w=fv_1\cdots v_pg$, with $f=zf'$ and $g=g'\bar{z}$.

If $w\notin D_A$, then $w=w_1\cdots w_n$, with $n\geqslant 2$, and $w_i\in D_A$. If $p(w)>n$ there exists an $i\leqslant n$ such that $p(w)=p(w_i)$. Then $|w_i|<|w|$ and from a factorization of w_i (induction hypothesis) one builds a factorization of w as above. Finally the claim is obvious for $p=n$.

(ii) By induction on $h(w)$, $w\in D_A^+$. If $h(w)=1$, then $w=w_1\cdots w_n$, with $w_i\in D_A$ and $h(w_i)=1$ for every i. Thus $w_1=z\bar{z}$ and a possible factorization is $w=u_1=f_0\,u_0\,g_0=(z)(1_{\tilde{A}^*})(\bar{z}\,w_2\cdots w_n)$.

Suppose $h(w)>1$. If $w\in D_A$, then $w=z\,w'\bar{z}$, $z\in\tilde{A}$ and $h(w')=h-1$. The factorization $w=(z)(w')(\bar{z})$ makes up the factorization found for w' by the induction hypothesis. If $w\notin D_A$ then $w=w_1\cdots w_n$, with $w_i\in D_A$. By definition, there exists an i such that $h(w_i)=h(w)$ and from the factorization $w_i=(z)(w_i')(\bar{z})$ one gets the factorization $w=u_h=(w_1\cdots w_{i-1}\,z)(w_i')(\bar{z}\,w_{i+1}\cdots w_n)$.

Example 3 (continued). $u_1=1_{\tilde{A}^*}\cdot\bar{a}\cdot\bar{a}\cdot 1_{\tilde{A}^*}\cdot a\cdot\bar{a}\,a\,a\cdot 1_{\tilde{A}^*}=\bar{a}\cdot\bar{a}\,a\cdot\bar{a}\,a\cdot a$.

4.3. A combinatorial property

There are only a finite number of Dyck words of given height and width. This statement is made precise by the following:

Lemma 7 (Autebert and Beauquier [1]). *Let h and p be two positive integers and let $N(h,p)=2p(p^h-1)/(p-1)$. For any $w\in D_A^*$ the length of which is greater than $N(h,p)$, either $p(w)>p$ or $h(w)>h$ holds.*

This lemma has been stated in [1] for the so-called *restricted* (or *one-sided*, or *semi-*) Dyck language $D_A'^*$ i.e. the set of words of $\tilde{A}^*$ which are equivalent to $1_{\tilde{A}^*}$ *modulo* the congruence generated by the relation $\{a\,\bar{a}=1_{\tilde{A}^*}\mid a\in A\}$ (and called the *one-sided Dyck* congruence). For the sake of completeness, we give the proof of the lemma in the case of the Dyck language, following almost *verbatim* the proof of [1]. What requires indeed more care in this case is, or was, the definitions of height and width of words, for the process of reduction *modulo* the Dyck congruence is ambiguous whereas the

process of reduction *modulo* the one-sided Dyck congruence is not. For instance the word u of the previous example could be reduced as

$$\bar{a}\,\bar{a}\,\underline{a\,\bar{a}}\,a\,a \;\to\; \bar{a}\,\underline{\bar{a}\,a}\,a \;\to\; \underline{\bar{a}\,a} \;\to\; 1_{\tilde{A}^*},$$

which corresponds to a width of 1 and height of 3. This is the reason why it was necessary to make explicit that we consider the *leftmost* reduction and this makes the process unambiguous then.

Proof of Lemma 7. We prove, by induction on h, that any word of width (atmost) p has a length smaller than or equal to $N(h,p)$.

Let $w=w_1w_2\cdots w_n\in D_A^*$ with $w_i\in D_A$. If $h(w)=1$ then $h(w_i)=1$ for every i and thus $w_i=z_i\bar{z}_i$, with $z_i\in\tilde{A}$. Then $p(w)\leqslant p$ implies $|w|\leqslant 2p=N(1,p)$ and the induction basis holds.

Suppose now that $h(w)=h+1$. Then $w=w_1w_2\cdots w_n$ with $w_i=z_i\,w_i'\,\bar{z}_i\in D_A$ and $z_i\in\tilde{A}$. Thus, for every i, $h(w_i')=h_i\leqslant h$. Let $p_i=p(w_i)=p(w_i')$. By the induction hypothesis, it follows that

$$|w_i'| \leqslant 2p_i\frac{p_i^{h_i}-1}{p_i-1} \leqslant 2p_i\frac{p_i^{h}-1}{p_i-1},$$

so that, since $|w_i|=|w_i'|+2$,

$$|w| \leqslant 2n+\sum_{i=1}^{n} 2p_i\frac{p_i^{h}-1}{p_i-1}.$$

Since $p=\max(n,\max\{p_i\mid 1\leqslant i\leqslant n\})$, it comes

$$|w| \leqslant 2p+p\left(2p\,\frac{p^h-1}{p-1}\right)=2p\left(1+p\left(\frac{p^h-1}{p-1}\right)\right)=N(h+1,p). \qquad \square$$

Remarks 1. (i) The expression $(p^h-1)/(p-1)$ stands indeed for $1+p+\cdots+p^{h-1}$ and its value is defined even if $p=1$ (in which case $N(h,1)=2h$).

(ii) The proof of the lemma itself shows that the bound is sharp, even in the case of a one-letter alphabet $A_1=\{a\}$. Following the steps of the proof we define inductively, for all integers p and h, the words $v_{h,p}$ as

$$v_{1,1}=a\,\bar{a},\quad \forall p\in\mathbb{N}\quad v_{1,p}=(v_{1,1})^p \quad\text{and}\quad \forall h\in\mathbb{N}\quad v_{h+1,p}=(a\,v_{h,p}\bar{a})^p.$$

It is clear that

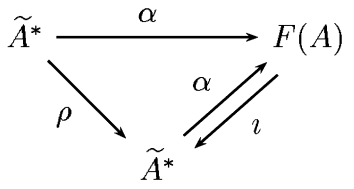
$$|v_{h,p}|=N(h,p),\quad h(v_{h,p})=h \quad\text{and}\quad p(v_{h,p})=p.$$

(iii) Let us finally note that the notion of height of a (one-sided) Dyck word appears also in the completely different context of the *dot-depth hierarchy*.

Let $L_n'=\{w\in D_A'^*\mid h(w)\leqslant n\}$ and $L_n=\{w\in D_A^*\mid h(w)\leqslant n\}$. The dot-depth of L_n' is exactly $n+1$, the dot-depth of L_n is exactly $2n+1$; this is the example used to prove that the dot-depth hierarchy is infinite [6,19].

4.4. Rational sets in $F(A)$

The definitions in Section 4.1 give the commutative diagram:



Rational sets in the free group are characterized by the following:

Theorem 6 (Benois [2]). *A subset X of $F(A)$ is in* $\mathrm{Rat}\, F(A)$ *if, and only if, $X\imath$ is in* $\mathrm{Rat}\, \tilde{A}^*$,

which directly derives from

Proposition 8 (Benois [2]). *If R is in* $\mathrm{Rat}\, \tilde{A}^*$ *then $R\rho$ is in* $\mathrm{Rat}\, \tilde{A}^*$.

The proof of Proposition 8 due to Fliess [9] is well-suited to generalization to series.

Definition 3 & Notation. Let $\mathscr{A} = (\lambda, \mu, \nu)$ be an automaton over $\tilde{A}^*$. We denote by $H_{\mathscr{A}}$ the image of the Dyck language over A by μ, i.e.

$$H_{\mathscr{A}} = \sum_{f \in D_A^*} f\mu$$

and by $\mathscr{A}\delta$ the automaton the representation (λ, π, ζ) of which is defined by

$$\forall a \in \tilde{A}, \qquad a\pi = H_{\mathscr{A}} a\mu \quad \text{and} \quad \zeta = H_{\mathscr{A}} \nu.$$

It then holds

Proposition 9 (Fliess [9]). $|\mathscr{A}|\delta = |\mathscr{A}\delta|$.

Proposition 9 will be established in the next section for the (more general) case of series. Since $R\rho = R\delta \cap K$ (and $\mathrm{Rat}\, \tilde{A}^*$ is closed under intersection) Proposition 8 follows.

The matrix $H_{\mathscr{A}}$ is well-defined for the Boolean semiring is complete. Its computation is effective, as stated in the following:

Proposition 10 (Benois and Sakarovitch [3]). *Let $\mathscr{A}$ be an automaton over $\tilde{A}$. Then $H_{\mathscr{A}}$, and thus $\mathscr{A}\delta$, are computable in* $\mathrm{O}(n^3)$, *where n is the cardinality of the state set of $\mathscr{A}$.*

5. Finite power property in $F(A)$

We are now ready to prove the result of this paper.

Theorem 1. *It is decidable whether a rational set of a free group has the finite power property.*

We first prove that the finite power property in $F(A)$ may be transferred to a problem of the same nature in the free monoid $\tilde{A}^*$.

Proposition 11. *Let X be any subset of $F(A)$ and $R = X\imath$ its canonical image in $\tilde{A}^*$. Then, for any integer $m \geqslant 0$, $X^* = X^{\leqslant m}$ if and only if $R^*\rho = (R^{\leqslant m})\rho$.*

Proof. Since α is a morphism and $\alpha = \rho \circ \alpha$, it holds, for every positive integer n

$$X^n = (R\alpha)^n = (R^n)\alpha = ((R^n)\rho)\alpha. \tag{1}$$

Therefore $(R^*)\rho = (R^{\leqslant m})\rho$ implies $X^* = X^{\leqslant m}$. Conversely, since $\alpha \circ \imath$ is the identity on K, we have $(X^n)\imath = (R^n)\rho$ by taking the image of (1) by $\imath$. Thus $X^* = X^{\leqslant m}$ implies $(R^*)\rho = (R^{\leqslant m})\rho$. □

Note that $X^* = X^{\leqslant m}$ obviously derives from $R^* = R^{\leqslant m}$ (since $X = R\alpha$) but the converse is not true as shown in the following example:

Example 4. Let $F_1 = F(\{a\})$ be the one generator free group (i.e. F_1 is isomorphic to $\mathbb{Z}$—but its operation is written multiplicatively), and let

$$X_1 = \{a^3\}^* \cup \{\bar{a}^2\}^*.$$

Every element of F_1, and thus of X_1^*, is written as the product of at most two elements of X_1 (since $a^m = (a^3)^m(\bar{a}^2)^m$ and $\bar{a}^n = (a^3)^n(\bar{a}^2)^{2n}$).

On the other hand, $(a^3\bar{a}^2)^m$ does not belong to any $R_1^n = (X_1\imath)^n$, for $n < 2m$.

We shall prove that Proposition 9—which deals with (classical) automata, i.e. with rational series with coefficients in the Boolean semiring—may be generalized to automata with multiplicity in $\mathscr{M}$, i.e. to rational series with coefficients in $\mathscr{M}$. We first recall how a relation from $\tilde{A}^*$ into itself—δ in this instance—is generalized to a mapping of $\mathscr{M}\langle\langle\tilde{A}^*\rangle\rangle$ into itself.[3]

5.1. Image of a series by a relation

For any $f \in \tilde{A}^*$, $f\delta$ is a subset of $\tilde{A}^*$. The relation δ is additively extended to $\mathfrak{P}(A^*)$: for any subset L of $\tilde{A}^*$, $L\delta$ is defined as

$$L\delta = \bigcup_{f \in L} f\delta.$$

[3] This generalization depends of course neither on δ nor on $\mathscr{M}$.

Let us rewrite these definitions with the notations and conventions of series. The subset $f\delta$ may be written as

$$f\delta = \sum_{g\in\tilde{A}^*} \langle f\delta, g\rangle g,$$

where $\langle f\delta, g\rangle$ denotes the *coefficient* of g in $f\delta$, i.e.

$$\langle f\delta, g\rangle = \begin{cases} 1 & \text{if } g \in f\delta, \\ 0 & \text{otherwise.} \end{cases}$$

Note then that

$$\forall f, g \in \tilde{A}^*, \quad \langle f\delta, g\rangle = \langle g\delta^{-1}, f\rangle.$$

Along the same line, a subset L of $\tilde{A}^*$ is written as

$$L = \sum_{f\in\tilde{A}^*} \langle L, f\rangle f.$$

It then follows that:

$$L\delta = \sum_{f\in\tilde{A}^*} [\langle L, f\rangle f\delta] = \sum_{f\in\tilde{A}^*} \left[\sum_{g\in\tilde{A}^*} (\langle L, f\rangle\langle f\delta, g\rangle) g \right].$$

The infinite summations do not bring in any problem for $\mathbb{B}$ is *complete*. Distributivity and associativity yield

$$L\delta = \sum_{g\in\tilde{A}^*} \left[\sum_{f\in\tilde{A}^*} (\langle L, f\rangle\langle f\delta, g\rangle) g \right],$$

i.e.

$$\langle L\delta, g\rangle = \sum_{f\in\tilde{A}^*} (\langle L, f\rangle\langle f\delta, g\rangle) = \sum_{f\in g\delta^{-1}} \langle L, f\rangle.$$

Such equality holds indeed for any series over a complete semiring of coefficients. Let us for instance consider series in $\mathscr{M}\langle\langle\tilde{A}^*\rangle\rangle$. The subset $f\delta$ is replaced by its *characteristic series* noted $f\underline{\delta}$

$$\langle f\underline{\delta}, g\rangle = \begin{cases} 1_{\mathscr{M}} = 0 & \text{if } g \in f\delta, \\ 0_{\mathscr{M}} = +\infty & \text{otherwise.} \end{cases}$$

Let s be a series in $\mathscr{M}\langle\langle \tilde{A}^* \rangle\rangle$; its image by $\underline{\delta}$ is thus defined by

$$\langle s\underline{\delta}, g\rangle = \sum_{f\in\tilde{A}^*} (\langle s, f\rangle \underset{\mathscr{M}}{\bullet} \langle f\underline{\delta}, g\rangle) = \sum_{f\in g\delta^{-1}} \langle s, f\rangle = \min_{f\in g\delta^{-1}} \langle s, f\rangle. \tag{2}$$

5.2. Image of a rational series by the relation δ

Definitions, and notations, taken for the image of an automaton under the relation δ generalize to distance automata.

Definition 4 & Notation. Let $\mathscr{A} = (\eta, \kappa, \zeta)$ be a distance automaton over $\tilde{A}^*$. We denote by $C_{\mathscr{A}}$ the image of the Dyck language over A by κ, i.e.

$$C_{\mathscr{A}} = \sum_{f\in D_A^*} f\kappa$$

and by $\mathscr{A}\delta$ the distance automaton, the $\mathscr{M}$-representation (η, σ, χ) of which is defined by

$$\forall a \in \tilde{A}, \qquad a\sigma = C_{\mathscr{A}} \underset{\mathscr{M}}{\bullet} a\kappa \quad \text{and} \quad \chi = C_{\mathscr{A}} \underset{\mathscr{M}}{\bullet} v.$$

It then holds

Proposition 12. $\|\mathscr{A}\|\underline{\delta} = \|\mathscr{A}\delta\|$.

Proof. From (2) follows:

$$\forall g \in \tilde{A}^*, \quad \langle \|\mathscr{A}\|\underline{\delta}, g\rangle = \sum_{f\in g\delta^{-1}} f\|\mathscr{A}\| = \sum_{f\in g\delta^{-1}} \langle \|\mathscr{A}\|, f\rangle$$

$$= \sum_{f\in g\delta^{-1}} \eta \underset{\mathscr{M}}{\bullet} f\kappa \underset{\mathscr{M}}{\bullet} \zeta.$$

Let $g = a_1 a_2 \cdots a_n$. By Lemma 5, the words of $g\delta^{-1}$ are exactly those of the form $w_0 a_1 w_1 a_2 \cdots w_{n-1} a_n w_n$, where $w_0, w_1, \ldots, w_n$ are in D_A^*. We then have, for every g in $\tilde{A}^*$:

$$\langle \|\mathscr{A}\|\underline{\delta}, g\rangle = \sum_{w_0,\ldots,w_n\in D_A^*} \eta \underset{\mathscr{M}}{\bullet} (w_0 a_1 \cdots w_{n-1} a_n w_n)\kappa \underset{\mathscr{M}}{\bullet} \zeta$$

$$= \eta \underset{\mathscr{M}}{\bullet} \left(\sum_{w_0,\ldots,w_n\in D_A^*} w_0\kappa \underset{\mathscr{M}}{\bullet} a_1\kappa \underset{\mathscr{M}}{\bullet} \cdots \underset{\mathscr{M}}{\bullet} w_{n-1}\kappa \underset{\mathscr{M}}{\bullet} a_n\kappa \underset{\mathscr{M}}{\bullet} w_n\kappa \right) \underset{\mathscr{M}}{\bullet} \zeta$$

$$= \eta \underset{\mathscr{M}}{\bullet} \left(\sum_{w_0\in D_A^*} w_0\kappa \right) \underset{\mathscr{M}}{\bullet} a_1\kappa \underset{\mathscr{M}}{\bullet} \cdots$$

$$\cdots \underset{\mathscr{M}}{\bullet} \left(\sum_{w_{n-1}\in D_A^*} w_{n-1}\kappa \right) \underset{\mathscr{M}}{\bullet} a_n\kappa \underset{\mathscr{M}}{\bullet} \left(\sum_{w_n\in D_A^*} w_n\kappa \right) \underset{\mathscr{M}}{\bullet} \zeta$$

$$= \eta \underset{\mathscr{M}}{\bullet} (C_{\mathscr{A}} \underset{\mathscr{M}}{\bullet} a_1\kappa \underset{\mathscr{M}}{\bullet} \cdots \underset{\mathscr{M}}{\bullet} C_{\mathscr{A}} \underset{\mathscr{M}}{\bullet} a_n\kappa) \underset{\mathscr{M}}{\bullet} C_{\mathscr{A}} \underset{\mathscr{M}}{\bullet} \zeta$$

$$= \eta \underset{\mathscr{M}}{\bullet} (a_1\sigma \underset{\mathscr{M}}{\bullet} \cdots \underset{\mathscr{M}}{\bullet} a_n\sigma) \underset{\mathscr{M}}{\bullet} \chi = \eta \underset{\mathscr{M}}{\bullet} g\sigma \underset{\mathscr{M}}{\bullet} \chi. \qquad \square$$

An immediate consequence of Proposition 12 is that $(|\mathscr{A}|)\delta = |\mathscr{A}\delta|$.

The following proposition shows that the matrix $C_{\mathscr{A}}$ is effectively computable:

Proposition 13. *There exists a finite effectively computable subset $T \subseteq D_A^*$ such that $C_{\mathscr{A}} = \sum_{w\in T} w\kappa$.*

Proof. Let r be the cardinality of the state set Q of $\mathscr{A}$, i.e. the dimension of the representation κ, and let $N = N(r^2, r)$ be the integer defined in Lemma 7. We prove that $T = D_A^* \cap \tilde{A}^{\leqslant N}$.

Note $C = C_{\mathscr{A}}$. For every pair (q, q') of states of $\mathscr{A}$ such that $C_{q,q'} < \infty$, let w be a word of D_A^* of *minimal length* for which $C_{q,q'} = w\kappa_{q,q'}$.

Assume that $|w| > N$. Then by Lemma 7, we have either $p(w) \geqslant r$ or $h(w) \geqslant r^2$. In the first case, by Lemma 6, we have $w = f\, v_1 \cdots v_r\, g$, for some f, $g \in \tilde{A}^*$, with $v_i \in D_A$. Let c be a computation from q to q' with label w and $\|c\| = C_{q,q'}$:

$$c = q \xrightarrow{f} q_1 \xrightarrow{v_1} q_2 \xrightarrow{v_2} \cdots \xrightarrow{v_r} q_{r+1} \xrightarrow{g} q'.$$

By definition of r, there exist distinct integers n and m such that $1 \leqslant n < m \leqslant r+1$ and $q_m = q_n$, so that the computation

$$e = q_n \xrightarrow{v_n} q_{n+1} \xrightarrow{v_{n+1}} \cdots \xrightarrow{v_{m-1}} q_m$$

is a cycle. Therefore, $w' = f\, v_1\, v_2 \cdots v_{n-1}\, v_m \cdots v_r\, g$ is in D_A^* and is the label of the computation c' from q to q'

$$c' = q_i \xrightarrow{f} q_1 \xrightarrow{v_1} \cdots \to q_{n-1} \xrightarrow{v_{n-1}} q_n \xrightarrow{v_m} q_{m+1} \xrightarrow{v_{m+1}} \cdots \xrightarrow{v_r} q_{r+1} \xrightarrow{g} q'.$$

It holds $\|c'\| \leqslant \|c\|$ and then $(w'\kappa)_{q,q'} = (w\kappa)_{q,q'}$. Since $|w'| < |w|$, contradiction with the choice of w.

In the second case, we have $h(w) \geqslant r^2$ and, by Lemma 6, there exists a sequence[4] of words of D_A^*: $w = u_0, u_1, \ldots, u_h$ such that $u_{i-1} = f_i\, u_i\, g_i$, with $|f_i\, g_i| > 0$. Then $w = f_0\, f_1 \cdots f_{h-1}\, f_h\, u_h\, g_h\, g_{h-1} \cdots g_1\, g_0$; let

$$c = q \xrightarrow{f_0} p_0 \to \cdots p_{h-1} \xrightarrow{f_h} p_h \xrightarrow{u_h} q_h \xrightarrow{g_h} q_{h-1} \to \cdots q_1 \xrightarrow{g_1} q_0 \xrightarrow{g_0} q'$$

be a computation from q to q' with label w. Since $h \geqslant r^2$ there exist two distinct integers n and m, $0 \leqslant n < m \leqslant h$ such that $p_m = p_n$ and $q_n = q_m$. We have $u_n = (f_{n+1} \cdots f_m)\, u_m\, (g_m \cdots g_{n+1})$ and the computations

$$e = p_n \xrightarrow{f_{n+1}} p_{n+1} \to \cdots \to p_{m-1} \xrightarrow{f_m} p_m$$

[4] Note that the numbering adopted for the u_i here is the reverse of the one used in the statement and the proof of Lemma 6 for it is much more readable.

and

$$f = q_m \xrightarrow{g_m} q_{m-1} \to \cdots \to q_{n+1} \xrightarrow{g_{n+1}} q_n$$

are two cycles. Therefore, $w' = (f_0\, f_1 \cdots f_n)\, u_m\, (g_n \cdots g_1\, g_0)$ is the label of a computation c' from q to q'. As above, it holds $\|c'\| \leqslant \|c\|$, $(w'\kappa)_{q,q'} = (w\kappa)_{q,q'}$ and $|w'| < |w|$, a contradiction.

Thus, if $w \in D_A^*$ is of minimal length for which $C_{q,q'} = (w\kappa)_{q,q'} < \infty$, then $|w| \leqslant N$ so that $w \in T$. Therefore $C_{\mathscr{A}} = \sum_{w \in T} w\kappa$. □

5.3. Proof of Theorem 1

The proof is now a walk—every step of which is effective—through all results we have gathered so far.

Let X be a rational subset of $F(A)$ and let $R = X\imath$ be its canonical image in $\tilde{A}^*$. By Proposition 11, it suffices to decide whether there exists a positive integer m such that $(R^*)\rho = (R^{\leqslant m})\rho$.

By Theorem 6, $R \in \mathrm{Rat}\, \tilde{A}^*$. Let $\mathscr{S}_R$ be the Simon automaton of R, which we denote also $\mathscr{S}_X$. ($\forall f \in \tilde{A}^*\, f\|\mathscr{S}_X\| = o_R(f)$, the smallest integer n such that $f \in R^n$.)

Let $\mathscr{T}_X = \mathscr{S}_X \delta$. By Proposition 12, $f\|\mathscr{T}_X\|$ is the smallest integer m such that f belongs to $(R^m)\delta$. By Proposition 13, $\mathscr{T}_X$ is effectively computable.

Let $K = (\tilde{A}^*)\rho$ be the set of reduced words of $\tilde{A}^*$ and $\mathscr{K}$ its characteristic distance automaton.

For every f in $\tilde{A}^*$, $f(\|\mathscr{T}_X\| \odot \|\mathscr{K}\|)$ is the smallest integer m for which $f \in (R^m)\rho$.

Let us call

$$\mathscr{U}_X = \mathscr{T}_X \otimes \mathscr{K}$$

the *B-automaton*[5] of X. By Proposition 4

$$\|\mathscr{U}_X\| = \|\mathscr{T}_X\| \odot \|\mathscr{K}\|.$$

Hence the set X has the finite power property if and only if $\mathscr{U}_X$ is bounded—which is decidable by Theorem 2.

5.4. Another proof for Theorem 1

In Section 2, we recalled that the finite power property of a rational language L may be decided by considering only the finiteness of the transition monoid of $\mathscr{S}_L$. The same scheme applies indeed to Theorem 1.

[5] As a sign of friendship to Brzozowski.

Proposition 14. *Let X be a rational subset of $F(A)$ and let $\mathscr{U}_X$ be its B-automaton. Then $\mathscr{U}_X$ is bounded if, and only if, its transition monoid is finite.*

Proof. Let (η,κ,ζ), (η,σ,ξ) and (χ,π,ψ) be the $\mathscr{M}$-representations of $\mathscr{S}_X$, $\mathscr{T}_X$ and $\mathscr{U}_X$ respectively. The representations κ and σ have the same dimension Q (the state set of $\mathscr{S}_X$) and π has dimension $Q\times P$ (where P is the state set of $\mathscr{K}$). By definition of $\mathscr{U}_X$, for any $((p,r),(q,s))$ in $(Q\times P)\times(Q\times P)$ and for any f in $\tilde{A}^*$,

$$f\pi_{(p,r),(q,s)} < \infty \Rightarrow f\pi_{(p,r),(q,s)} = f\sigma_{p,q}. \tag{3}$$

The proof of Proposition 14 and its preparation follow then [17], almost *verbatim*.

Let $\Delta:\mathfrak{P}(\mathscr{M})\to\mathbb{N}$ be the map that associates to any subset of $\mathscr{M}$ its maximum finite element:

$$X\Delta = \max\{0\cup\{x<+\infty \mid x\in X\}\}.$$

The map Δ is extended to subsets of matrices with entries in $\mathscr{M}$ by considering that every matrix is the (unstructured) set of its entries.

Thus, for any subset X of matrices (of fixed dimensions), $X\Delta=0$ if no matrix has finite coefficients, or $X\Delta=+\infty$ if the finite coefficients of matrices of X are not bounded, or $X\Delta=m<+\infty$ if the maximum finite coefficients of matrices in X is m. Then X is finite if and only if $X\Delta<+\infty$.

Lemma 15 (Simon [17]). $(\tilde{A}^*\pi)\Delta\leqslant(\tilde{A}^*\|\mathscr{U}_X\|)\Delta+1$.

Proof. Let $M=(\tilde{A}^*\|\mathscr{U}_X\|)\Delta$ (i.e. for every w in $|\mathscr{U}_X|$, $w\|\mathscr{U}_X\|\leqslant M$). Assume that there exist some $((p,r),(q,s))$ in $(Q\times P)\times(Q\times P)$ and some f in $\tilde{A}^*$ such that $f\pi_{(p,r),(q,s)}=k>M+1$. By (3), $f\sigma_{p,q}=k$.

By definition of σ (i.e. of $\mathscr{T}_X$), there exists a computation

$$c = p \xrightarrow[\mathscr{S}_X]{g} q$$

such that $g\rho=f$ and such that its weight $\|c\|=k$ *is minimum for that property*. By construction of $\mathscr{S}_X$, c factorizes into

$$c = p \xrightarrow{g_0} s \xrightarrow{g_1} s \xrightarrow{g_1} s \to \cdots \to s \xrightarrow{g_{k-1}} s \xrightarrow{g_k} q.$$

Let $y=g_1g_2\cdots g_{k-1}$; since s is the (unique) initial and final state of $\mathscr{S}_X$, $y\in(X\iota)^*$ and thus $y\rho\in|\mathscr{U}_X|$. By hypothesis on $\mathscr{U}_X$, $(y\rho)\|\mathscr{U}_X\|=h\leqslant M$ which implies that there exists an x in $(X\iota)^h$ such that $x\rho=y\rho$. Let us consider the computation

$$c' = p \xrightarrow[\mathscr{S}_X]{g_0} s \xrightarrow[\mathscr{S}_X]{x} s \xrightarrow[\mathscr{S}_X]{g_k} q$$

(the central part exists since $x \in (X\iota)^*$ and s is the (unique) initial and final state of $\mathcal{S}_X$). It then comes

$$(|c'|)\rho = (g_0\, x\, g_k)\rho = (g_0\, x\rho\, g_k)\rho = (g_0\, y\rho\, g_k)\rho = (g_0\, y\, g_k)\rho = (|c|)\rho$$

and

$$\|c'\| = h + 1 < k = \|c\|.$$

Contradiction with the assumption c is of minimal weight.

Since the inequation

$$(\tilde{A}^* \| \mathcal{U}_X \|)\Delta \leqslant (\tilde{A}^* \pi)\Delta + \psi\Delta$$

obviously holds, $\mathcal{U}_X$ is bounded if and only if $\tilde{A}^*\pi$ is finite. The proof of Proposition 14 is thus complete. □

5.5. On the complexity of the solution

The above proof consists in the effective construction of the distance automaton $\mathcal{U}_X$; the conclusion follows from the fact it is decidable whether it is bounded.

If n is the size of an automaton that defines X the complexity of that decision procedure is $O(3^{n^2})$, whether one uses Theorem 2 or Simon's solution (i.e. Proposition 2). [It would be interesting indeed to have actual implementations of both methods in order to make more precise comparisons].

We focus here on the complexity of the construction of $\mathcal{U}_X$ itself. As it is conducted in Section 5.2, it goes by the computation of a matrix C. This matrix is the sum of all matrices $f\kappa$ for f in D_A^* of length smaller than or equal to $2n(2^{n^2}+1)/(n-1)$. Even if there are "only" $O(n)$ words of length $2n$ in D_A^*, this rough evaluation gives a complexity larger than $O(2^{n^2})$ for the computation of C. A more serious estimation of that complexity would be obtained by the study of the algorithm that we give in Appendix A.3. But the solution is even simpler, as far as *the complexity of the decision procedure* is concerned, for we show that there exists *another* distance automaton $\mathcal{U}'_X$, that *is bounded exactly when* $\mathcal{U}_X$ *is*, and that can be build in $O(n^3)$ operations.

The idea underlying the construction of $\mathcal{U}'_X$ is the utilization of the algorithm that is behind Proposition 10—i.e. the one that computes the so-called matrix H—to compute a matrix, which we note C', with entries in $\mathcal{M}$. The distance automaton $\mathcal{U}'_X$ is then derived from C' as $\mathcal{U}_X$ is derived from C. The core of the proof is the fact that $\mathcal{U}'_X$ is bounded exactly when $\mathcal{U}_X$ is. The following definition proves to be useful before going to these two points:

Let $\psi : \mathcal{M} \to \mathcal{M}$ be the mapping defined by

$$0\psi = 0, \quad x\psi = 1, \quad 0 < x < +\infty \quad \text{and} \quad (+\infty)\psi = +\infty.$$

If $\mathcal{A} = (\eta, \kappa, \zeta)$ is a distance automaton, we define the automaton $\mathcal{A}\psi$ to be the one with representation $(\eta\psi, \kappa\psi, \zeta\psi)$. Since ψ *is not a morphism* (of the semiring $\mathcal{M}$),

$f\|\mathscr{A}\psi\| = (f\|\mathscr{A}\|)\psi$ *does not hold.* However, if $M = (\eta \cup \tilde{A}\kappa \cup \zeta)\Delta$, it is easily seen that

$$f\|\mathscr{A}\psi\| \leqslant f\|\mathscr{A}\| \leqslant M(f\|\mathscr{A}\psi\| + 2),$$

which directly implies

Proposition 16. *Let $\mathscr{A}$ and $\mathscr{B}$ be two distance automata such that $\mathscr{A}\psi = \mathscr{B}\psi$. Then $\mathscr{A}$ is bounded if and only if $\mathscr{B}$ is bounded.*

Let $H = H_{\mathscr{S}_X}$ and $C = C_{\mathscr{S}_X}$ be the matrices computed from $\mathscr{S}_X$ as in Definitions 3 and 4. Let C' be the matrix (with entries in $\mathscr{M}$) defined by

$$\begin{aligned} &\forall p,q \in Q,\ p \neq q \quad H_{p,q} = 1_{\mathbb{B}} \Rightarrow C'_{p,q} = 1, \\ &\qquad\qquad\qquad\quad H_{p,q} = 0 \Rightarrow C'_{p,q} = +\infty, \\ &\forall p \in Q, \quad C'_{p,p} = 0. \end{aligned}$$

Note that the two 1's in the first equation are different (and that $H_{p,p} = 1_{\mathbb{B}}$ for every p in Q). It follows from the definition that:

$$\forall p,q \in Q, \qquad C'_{p,q} \neq +\infty \ \Leftrightarrow\ \exists f \in D_A^*, \quad f\kappa_{p,q} \neq +\infty.$$

An algorithm computing H has been proved to be of complexity $O(n^3)$ in [3] and the same holds thus for C' (cf. Sections A.1 and A.2 of Appendix A).

Proposition 17. $C\psi = C'\psi$.

We first prove a property of the automaton $\mathscr{S}_X$.

Lemma 18. *Let X be a rational set of $F(A)$; let c be a computation of $\mathscr{S}_X$, the Simon's automaton of $R = X\iota$. Then*

$$|c| \in D_A^+ \ \Rightarrow\ \|c\| \geqslant 1.$$

Proof. Let

$$c = q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \to \cdots \to q_{n-1} \xrightarrow{a_n} q_n$$

be a computation in $\mathscr{S}_X$. From the definition of $\mathscr{S}_X$, $\|c\| = 0$ implies that none of the q_i is equal to s, the initial and final state of $\mathscr{S}_X$, i.e. c does not pass through s, and thus $|c|$ is a factor of an element of R. Then $|c|$ cannot be in D_A^+ for R is a set of *reduced words* of $\tilde{A}^*$.

Proof of Proposition 17. Let p and q be two states of $\mathscr{S}_X$ and let

$$c = p \xrightarrow[\mathscr{S}_X]{f} q$$

be a computation with f in D_A^* and such that $\|c\| = C_{p,q}$.

If $p=q$ then $H_{p,q}=1$ and $C'_{p,q}=0$ by definition, and $C_{p,q}=0$ since $f=1_{\tilde{A}^*}$.
If $p\neq q$ then $H_{p,q}=1$ and $C'_{p,q}=1$ by definition, and $C_{p,q}\geqslant 1$ by Lemma 18.
If such a computation does not exists, then $H_{p,q}=0$, $C'_{p,q}=+\infty$ and $C_{p,q}=+\infty$.
Thus in any case $C\psi=C'\psi$. □

Let (η,κ,ζ) be the representation of $\mathscr{S}_X$ and let $\mathscr{T}'_X=(\eta,\sigma',\chi')$ be the automaton defined by

$$\forall a\in\tilde{A},\qquad a\sigma'=C'\underset{\mathscr{M}}{\bullet}a\kappa \quad\text{and}\quad \chi'=C'\underset{\mathscr{M}}{\bullet}\zeta.$$

Let $\mathscr{U}'_X$ be the distance automaton defined by

$$\mathscr{U}'_X=\mathscr{T}'_X\otimes\mathscr{K}.$$

We then have

Proposition 19. $\mathscr{U}_X\psi=\mathscr{U}'_X\psi$.

Proof. From the definition of ψ it follows that for any x and y in $\mathscr{M}$ one has

$$(x\underset{\mathscr{M}}{+}y)\psi=(x\psi\underset{\mathscr{M}}{+}y\psi)\quad\text{and}\quad(x\underset{\mathscr{M}}{\bullet}y)\psi=(x\psi\underset{\mathscr{M}}{\bullet}y\psi)\psi$$

from which it holds

$$\forall a\in\tilde{A},\qquad(C\underset{\mathscr{M}}{\bullet}a\kappa)\psi=(C'\underset{\mathscr{M}}{\bullet}a\kappa)\psi\quad\text{and}\quad(C\underset{\mathscr{M}}{\bullet}\zeta)\psi=(C'\underset{\mathscr{M}}{\bullet}\zeta)\psi$$

and the conclusion follows. □

Appendix A

For sake of completeness, we recall here the algorithm presented in [3] for the computation of the matrix $H_{\mathscr{A}}$. We then reproduce it with the small two modifications necessary to compute $C'_{\mathscr{A}}$. Finally we derive from it an algorithm that computes $C_{\mathscr{A}}$ which is less brute force than the one underlying Proposition 13. The proof of its correctness is left to the reader; the evaluation of a good bound to its complexity is an open problem.

A.1. Computation of $H_{\mathscr{A}}$

A queue of labelled edges (i.e. triples in $(Q\times\tilde{A}\times Q)$), called *EDGE*, is initialized with the labelled edges of $\mathscr{A}$. The matrix $H_{\mathscr{A}}$ is initialized with all entries equal to 0 except the diagonal ones, which are set to 1. For every a in $\tilde{A}$, the matrix $a\pi$ is initialized to $a\mu$.

Because of lines (a) and (a′) that behave as a guard, block (b) and block (b′) (boxed) are entered at most n^2 times; their complexity is $O(n)$ because of line (c) (resp. (c′)).

```
while NonEmpty(EDGE)
 do (i, a, j) := Front(EDGE); Pop(EDGE);
    forall q ∈ Q
     do if ā π_{j,q} ≠ 0 then
          do if H_{i,q} = 0 then                                   (a)
               do H_{i,q} := 1;                                    (b)
                  forall z ∈ Ã
                   do forall p ∈ Q                                 (c)
                        do if z π_{q,p} ≠ 0 then
                             do if z π_{i,p} = 0 then
                                  do z π_{i,p} := 1;
                                     Enter((i, z, p), EDGE)
                                  od
                             od
                        od
                   od
               od
          od
          if ā π_{q,i} ≠ 0 then
          do if H_{q,j} = 0 then                                   (a′)
               do H_{q,j} := 1;                                    (b′)
                  forall z ∈ Ã
                   do forall p ∈ Q                                 (c′)
                        do if z π_{j,p} ≠ 0 then
                             do if z π_{q,p} = 0 then
                                  do z π_{q,p} := 1;
                                     Enter((q, z, p), EDGE)
                                  od
                             od
                        od
                   od
               od
          od
     od
od
```

Computation of $H_{\mathcal{A}}$

A.2. Computation of $C'_{\mathcal{G}_X}$

We keep the notations of the proof of Proposition 17. The matrix C' is initialized with all entries equal to $+\infty$ except the diagonal ones, which are set to 0. For every

a in $\tilde{A}$, the matrix $a\sigma'$ is initialized to $a\kappa$.

```
while NonEmpty(EDGE)
 do (i,a,j) := Front(EDGE); Pop(EDGE);
    forall q ∈ Q
     do if ā σ'_{j,q} ≠ +∞ then
          do if C'_{i,q} = +∞ then                                   (a)
             ┌──────────────────────────────────────────────────────┐
             │ do C'_{i,q} := 1;                                    (b)
             │    forall z ∈ Ã
             │     do forall p ∈ Q                                  (c)
             │          do if zσ'_{q,p} ≠ +∞ then
             │               do if zσ'_{i,p} = +∞ then
             │                    do zσ'_{i,p} := 1;
             │                       Enter((i,z,p), EDGE)
             │                    od
             │               od
             │          od
             │     od
             │ od
             └──────────────────────────────────────────────────────┘
          od
          if ā σ'_{q,i} ≠ +∞ then
          do if C'_{q,j} = +∞ then                                   (a')
             ┌──────────────────────────────────────────────────────┐
             │ do C'_{q,j} := 1;                                    (b')
             │    forall z ∈ Ã
             │     do forall p ∈ Q                                  (c')
             │          do if zσ'_{j,p} ≠ +∞ then
             │               do if zσ'_{q,p} = +∞ then
             │                    do zσ'_{q,p} := 1;
             │                       Enter((q,z,p), EDGE)
             │                    od
             │               od
             │          od
             │     od
             │ od
             └──────────────────────────────────────────────────────┘
          od
     od
od
```

The algorithm transformed for the computation of $C'_{\mathcal{S}_X}$

A.3. Computation of $C_{\mathcal{S}_X}$

The matrix C is initialized as was C': every entry is set to $+\infty$ except the diagonal ones, which are set to 0. For every a in $\tilde{A}$, the matrix $a\sigma$ is initialized to $a\kappa$.

The lines (a) and (a′) are not a guard anymore, and blocks (b) and (b′) (boxed) may be entered more than n^2 times.

```
while NonEmpty(EDGE)
 do  (i,a,j) := Front(EDGE); Pop(EDGE);
     forall q ∈ Q
      do  if ā σ_{j,q} ≠ +∞ then
          do  if C_{i,q} > a σ_{i,j} + ā σ_{j,q} then                    (a)
              ┌──────────────────────────────────────────────────────┐
              │ do  C_{i,q} := a σ_{i,j} + ā σ_{j,q};                (b)
              │     forall z ∈ Ã
              │      do  forall p ∈ Q
              │           do  if z σ_{q,p} ≠ +∞ then
              │                do  if z σ_{i,p} > C_{i,q} + z σ_{q,p} then
              │                     do  z σ_{i,p} := C_{i,q} + z σ_{q,p};
              │                         Enter((i,z,p), EDGE)
              │                     od
              │                od
              │           od
              │      od
              │ od
              └──────────────────────────────────────────────────────┘
          od
          if ā σ_{q,i} ≠ +∞ then
          do  if C_{q,j} > ā σ_{q,i} + a σ_{i,j} then                    (a′)
              ┌──────────────────────────────────────────────────────┐
              │ do  C_{q,j} := ā σ_{q,i} + a σ_{i,j};                (b′)
              │     forall z ∈ Ã
              │      do  forall p ∈ Q
              │           do  if z σ_{j,p} ≠ +∞ then
              │                do  if z σ_{q,p} > C_{q,j} + z σ_{j,p} then
              │                     do  z σ_{q,p} := C_{q,j} + z σ_{j,p};
              │                         Enter((q,z,p), EDGE)
              │                     od
              │                od
              │           od
              │      od
              │ od
              └──────────────────────────────────────────────────────┘
          od
     od
od
```

The algorithm transformed for the computation of $C_{\mathcal{S}_X}$

References

[1] J.M. Autebert, J. Beauquier, Une caractérisation des générateurs standard, RAIRO I.T. (1974) 63–83.
[2] M. Benois, Parties rationnelles du groupe libre, C.R. Acad. Sci. Paris, Sér. A 269 (1969) 1188–1190.

[3] M. Benois, J. Sakarovitch, On the complexity of some extended word problems defined by cancellation rules, Inform. Proc. Lett. 23 (1986) 281–287.
[4] J. Berstel, Transductions and Context-Free Languages, Teubner, Stuttgart, 1979.
[5] J. Berstel, Ch. Reutenauer, Rational Series and their Languages, Springer, Berlin, 1988.
[6] J. Brzozowski, R. Knast, The dot-depth hierarchy of star-free events is infinite, J. Comput. System Sci. 16 (1978) 37–55.
[7] F. d'Alessandro, J. Sakarovitch, The finite power property for rational sets of the free group, in: J. Gunawardena (Ed.), Idempotency, Cambridge University Press, Cambridge, 1998, pp. 80–87.
[8] S. Eilenberg, Automata, Languages, and Machines, Vol. A, Academic Press, New York, 1974.
[9] M. Fliess, Deux applications de la représentation matricielle d'une série non commutative, J. Algebra 19 (1971) 344–353.
[10] K. Hashiguchi, A decision procedure for the order of regular events, Theoret. Comput. Sci. 72 (1979) 27–38.
[11] K. Hashiguchi, Limitedness theorem on finite automata with distance functions, J. Comput. System Sci. 24 (1982) 233–244.
[12] K. Hashiguchi, Improved limitedness theorems on finite automata with distance functions, Theoret. Comput. Sci. 72 (1990) 27–38.
[13] C.E. Hughes, S.M. Selkow, The finite power property for context-free languages, Theoret. Comput. Sci. 15 (1981) 111–114.
[14] R.C. Lyndon, P.E. Schupp, Combinatorial Group Theory, Springer, Berlin, 1977.
[15] J.-E. Pin, Tropical semirings, in: J. Gunawardena (Ed.), Idempotency, Cambridge University Press, Cambridge, 1998, pp. 50–69.
[16] M.P. Schützenberger, On a theorem of R. Jungen, Proc. Amer. Math. Soc. 13 (1962) 885–889.
[17] I. Simon, Limited subsets of a free monoid, Proc. 19th Ann. Symp. on Foundation of Computer Science, 1978, pp. 143–150.
[18] I. Simon, Recognizable sets with multiplicities in the tropical semiring, Lecture Notes in Computer Science, Vol. 324, Springer, Berlin, 1988, pp. 107–120.
[19] P. Weil, Some results on the dot-depth hierarchy, Semigroup Forum 46 (1993) 352–370.