ELSEVIER

Theoretical Computer Science 169 (1996) 185–200

Theoretical Computer Science

Polynomial closure of group languages and open sets of the Hall topology

Jean-Eric Pin*

LITP/IBP, Université Paris VII et CNRS, Tour 55-56, 2 place Jussieu, 75251 Paris Cedex 05, France

1. Introduction

The aim of this paper is to show that the two classes of recognizable (or regular) languages of the title are actually the same. But a title has to be short and ours does not mention two other important characterizations given in this paper: an algebraic characterization, on which our proofs rely, and a more algorithmic one in terms of finite automata. This gives four possible points of view to look at our class and so, the reader may choose between combinatorics, topology, algebra or automata according to her or his preferences. We present the language perspective, the topological aspects, the algebraic characterization and the connections with automata in this order.

The *polynomial closure* of a class of languages $\mathscr{L}$ of A^* is the set of languages that are finite unions of languages of the form $L_0a_1L_1\cdots a_nL_n$, where the a_i's are letters and the L_i's are elements of $\mathscr{L}$. The fact that letters are inserted between the L_i's is a technical facility that makes life easier. The terminology *polynomial closure*, first introduced by Schützenberger [23], comes from the algebraic notation for the rational expressions, in which union is denoted by $+$. This closure operation leads to natural hierarchies among recognizable languages. Define a boolean algebra as a set of languages of A^* closed under finite union and complement. Now, start with a given boolean algebra of recognizable languages, and call it the level 0. Then define recursively the higher levels as follows: the level $n+1/2$ is the polynomial closure of the level n and the level $n+1$ is the boolean closure of the level $n+1/2$. Note that a set of level m is also a set of level n for every $n \geqslant m$. The main problems concerning these hierarchies is to know whether they are infinite and whether each level is decidable.

At least three different hierarchies of this type were proposed in the literature and the three of them were proved to be infinite. If one starts with finite or cofinite languages,[1] one gets the famous "dot-depth hierarchy". This hierarchy was presented for instance in the invited lecture of I. Simon at the ICALP 1993 [24]. If one starts with

* e-mail: pin@litp.ibp.fr.

[1] In this particular case, languages must be considered as subsets of A^+. This is a subtle, but important detail.

PII S0304-3975(96)00120-X

the trivial boolean algebra (A^* and $\emptyset$) one gets the Straubing–Thérien concatenation hierarchy. These hierarchies have some nice connections with quantifiers hierarchies in formal logic [25, 17]. The third hierarchy, called the *group languages hierarchy* [10], is obtained by taking the group languages as level 0. A *group language* is simply a recognizable language accepted by a *permutation automaton*, that is, a complete deterministic finite automaton in which each letter induces a permutation on the set of states. Thus our class, the polynomial closure of group languages, is exactly the level 1/2 of this hierarchy. It may seem a little disappointing to stay below level 1 of a hierarchy, but the reader should be aware that the decidability problem is an open problem (for the three hierarchies) for all levels >1. The decidability of level 1 is now proved for the three hierarchies, but it is an extremely difficult result for the group languages hierarchy [8, 7]. One of the nontrivial consequences of the results of this paper is that level 1/2 is also decidable.

The *Hall topology* (also called *profinite group topology*) was first introduced for the free group by Hall [6] and extended to the case of free monoids by Reutenauer [19]. The group languages form a basis for this topology, that is, the open sets are finite or infinite unions of group languages. There are several other equivalent definitions for this topology, that are detailed in Section 3. Of course, an open set is not in general recognizable and there are also recognizable languages which are not open. Our main result states that a recognizable set is open if it belongs to the polynomial closure of group languages. This result looks like a conjuring trick since it amounts to replace infinite union by finite union and product.

A simple characterization can also be given in terms of syntactic monoids. Recall that a *monoid* is a set equipped with an associative multiplication and an identity (denoted by 1) for this multiplication. An *ordered monoid* $(M, \leqslant)$ is a monoid M equipped with a (partial) *stable* order relation $\leqslant$: for every $u, v, x \in M$, $u \leqslant v$ implies $ux \leqslant vx$ and $xu \leqslant xv$. An *order ideal* of $(M, \leqslant)$ is a subset I of M such that, if $x \leqslant y$ and $y \in I$, then $x \in I$.

Let $(M, \leqslant)$ be an ordered monoid and let η be a surjective semigroup morphism from A^* onto M, which can be considered as a morphism of ordered monoid from $(A^*, =)$ onto $(M, \leqslant)$. In this paper, the postfix notation $x\eta$ (resp. $x\eta^{-1}$) will be used in place of the more standard notation $\eta(x)$ (resp. $\eta^{-1}(x)$). A language of A^* is said to be *recognized* by η if $L = P\eta^{-1}$ for some order ideal P of M. By extension, L is said to be *recognized* by $(M, \leqslant)$ if there exists a surjective morphism from A^* onto M that recognizes L. If M is a finite group, then the only stable order relation is the equality relation (see Lemma 6.4) and thus every subset of M is an order ideal. It follows that a language L is a group language if there exists a monoid morphism η from A^* onto a finite group G and a subset P of G such that $L = P\eta^{-1}$.

Let L be a language of A^*. One defines a stable quasiorder $\preccurlyeq_L$ and a congruence relation $\sim_L$ on A^* by setting

$u \preccurlyeq_L v$ if and only if, for every $x, y \in A^*$, $xvy \in L$ implies $xuy \in L$,

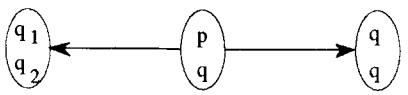
$u \sim_L v$ if and only if $u \preccurlyeq_L v$ and $v \preccurlyeq_L u$.

The congruence $\sim_L$ is called the *syntactic congruence* of L and the quasiorder $\preccurlyeq_L$ induces a stable order $\leqslant_L$ on $M(L) = A^*/\sim_L$. The ordered monoid $(M(L), \leqslant_L)$ is called the *syntactic ordered semigroup* of L, the relation $\leqslant_L$ is called the *syntactic order* of L and the canonical morphism η_L from A^* onto $M(L)$ is called the *syntactic morphism* of L. Finally, the subset $P = L\eta_L$ of $M(L)$ is called the *syntactic image* of L. It is a well-known fact that a language is recognizable if its syntactic monoid is a finite monoid. Similarly, a language is a group language if its syntactic monoid is a finite group. Now, the author conjectured in [11] that a recognizable language L is open if its syntactic image P satisfies the following property: for every $s, t \in M(L)$ and for every idempotent $e \in M(L)$, $st \in P$ implies $set \in P$. This is equivalent to saying that the ordered syntactic monoid of L satisfies the simple identity

$$e \leqslant 1 \text{ for every idempotent } e \in M. \tag{1.1}$$

This conjecture was proved by Ribes and Zalesskii [21] using sophisticated algebraic tools (profinite trees acting on groups). Now by our main result, Condition 1.1 also characterizes the polynomial closure of group languages. We also prove two topological properties: two disjoint recognizable open sets can be separated by a clopen set and the closure of a recognizable open set of A^* is a recognizable clopen set. Again, the proof makes use of algebraic and combinatorial arguments.

Finally, we show that a recognizable language belongs to the polynomial closure of the group languages if the graph which is the direct product of two copies of the reflexive and transitive closure of its minimal automaton contains no configuration of the form



where q_1 is a final state and q_2 is a nonfinal state. This result leads to a polynomial-time algorithm for testing, given an n-state deterministic automaton $\mathscr{A}$, whether the language accepted by $\mathscr{A}$ belongs to the polynomial closure of the group languages, or, equivalently, is open in the Hall topology.

We tried to keep the paper self-contained. The techniques of semigroup theory required in the proofs are introduced in Section 2. The Hall topology is defined in Section 3, the main result is presented in Section 4 and the algorithms are discussed in Section 5. The separation property is presented in Section 6. Some open problems are discussed in Section 7.

2. Useful facts about monoids

In this section, we state without proof three results of semigroup theory that are needed in this paper.

If M and N are monoids, a *monoid morphism* $\alpha : M \to N$ is a map from M into N such that $(u\alpha)(v\alpha) = (uv)\alpha$ for every $u, v \in M$. An *idempotent* of M is an element e such that $e^2 = e$. The set of idempotents of a monoid M is denoted by $E(M)$.

Proposition 2.1. *In a finite monoid, every element has a unique idempotent power.*

The unique idempotent power of an element x is usually denoted x^ω. Our second result can be considered as a weak form of Ramsey's theorem in combinatorics [12].

Proposition 2.2. *Let γ be a monoid morphism from A^* onto a finite monoid M and let k be a positive integer. Then there exists an integer N and an idempotent e of M such that every word of A^* of length greater that N factorizes as $u = u_0u_1 \cdots u_{k+1}$ with $u_1, u_2, \ldots, u_k \in A^+$ and $u_1\gamma = u_2\gamma = \cdots = u_k\gamma = e$.*

The last result may appear somewhat artificial to the reader. It is in fact connected to one of the deepest results in semigroup theory, but it would take us too far afield to present this topic. The interested reader is referred to the survey article [7]. Let M be a finite monoid and let $D(M)$ be the smallest submonoid of M closed under weak conjugation, that is, such that the conditions $a\bar{a}a = a$ and $n \in D(M)$ imply $an\bar{a} \in D(M)$ and $\bar{a}na \in D(M)$. One can see $D(M)$ as the subset of M generated by the following context-free grammar

$$\begin{cases} S \to SS + 1 \\ S \to aS\bar{a} + \bar{a}Sa \quad \text{for each pair } (a, \bar{a}) \text{ such that } a\bar{a}a = a. \end{cases}$$

Notice that since M is finite, $D(M)$ can be effectively calculated. It is easy to see that $D(M)$ always contains $E(M)$. Indeed, if e is an idempotent, then one can take $a = \bar{a} = e$ and $n = 1$. Then since $1 \in D(M)$ (because $D(M)$ is a monoid), one has $an\bar{a} = ee = e \in D(M)$.

The deep result of Ash [1, 2], first conjectured by Rhodes, states that this submonoid $D(M)$ is related to finite groups as follows.

Theorem 2.3. *Let $\alpha : A^* \to M$ be a surjective monoid morphism. Then there exists a finite group G and a monoid morphism $\beta : A^* \to G$ such that $D(M) = \{u\alpha \mid u \in A^* \text{ and } u\beta = 1\}$.*

Notice that nothing is said about the size of the group G, which can actually be rather large.

3. The Hall topology

We define in this section the Hall topology. It follows from a well known result of algebra (*the free group is residually finite* [6]) that two distinct words u and v of A^* can always be separated by a finite group in the following sense: there exists

a finite group G and a monoid morphism $\varphi : A^* \to G$ such that $u\varphi \neq v\varphi$. We give here a self-contained proof of this fact. Consider the minimal deterministic (but non complete) automaton recognizing the language $\{u, v\}$ but separating u and v. For instance, if $u = abbab$ and $v = ababb$, this automaton is drawn in Fig. 1.

In this automaton, each letter induces an injective map from the set of states into itself. Complete these injective maps into permutation of the set of states in an arbitrary way and remove the final state corresponding to the letter v. One such completion is shown in Fig. 2.

The resulting automaton is a permutation automaton, which recognizes a group language L. By construction, $u \in L$ but $v \notin L$. Therefore, the syntactic monoid of L, which is a finite group, separates u and v.

Set, for every $u, v \in A^*$,

$$r(u, v) = \min \{Card(G) \mid G \text{ is a finite group that separates } u \text{ and } v\}$$

and

$$d(u, v) = e^{-r(u,v)}$$

with the usual conventions $\min \emptyset = \infty$ and $e^{-\infty} = 0$. Then d is a distance (in fact an ultrametric distance) which defines a topology on A^*, called the *profinite group*

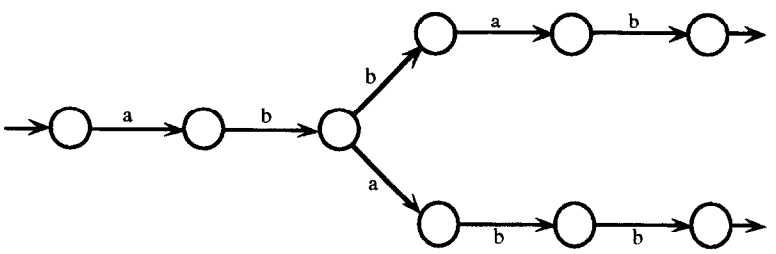


Fig. 1. The minimal automaton of $\{abbab, ababb\}$.

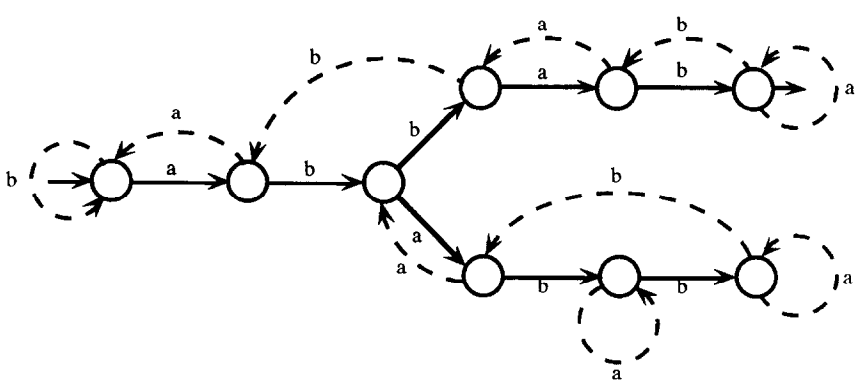


Fig. 2. A possible completion.

topology of the free monoid. This topology, introduced by Reutenauer [19], is an analog for the free monoid to the topology of the free group introduced by Hall [6]. It is the coarsest topology such that every monoid morphism from A^* into a discrete finite group is continuous. The group languages form a basis for this topology and the concatenation product is a continuous operation. The interested reader is referred to [11, 19] for a more detailed study of the Hall topology. An example of a converging sequence is given by the following proposition, due to [19].

Proposition 3.1. *For every word* $u \in A^*$, $\lim_{n\to\infty} u^{n!} = 1$.

As the multiplication is continuous and a closed set contains the limit of any converging sequence, it follows that if L is a closed set, and if $xu^{n!}y \in L$ for all $n \geqslant 0$, then $xy \in L$. This gives the following corollary [11, 16]. Recall that $u^+ = \{u^n \mid n > 0\}$.

Corollary 3.2. *Let* L *be a closed set and* u *be a word of* A^*. *If* $xu^+y \subseteq L$, *then* $xy \in L$.

In fact, the converse of Corollary 3.2 is also true. This was first conjectured by the author and recently proved by Ribes and Zalesskii [21] (see also [1, 2] and the survey [7] for related problems).

Theorem 3.3. *A recognizable set of* A^* *is closed if for every* $u \in A^*$, $xu^+y \subseteq L$ *implies* $xy \in L$.

Since an open set is the complement of a closed set, one can also state:

Theorem 3.4. *A recognizable set of* A^* *is open if for every* $u \in A^*$, $xy \in L$ *implies* $xu^+y \cap L \neq \emptyset$.

These conditions can be easily converted in terms of ordered syntactic monoids.

Theorem 3.5. *Let* L *be a recognizable language of* A^* *and let* $(M, \leqslant)$ *be its ordered syntactic monoid.*

(1) L *is closed if for every* $e \in E(M)$, $1 \leqslant e$.

(2) L *is open if for every* $e \in E(M)$, $e \leqslant 1$.

Proof. We give the proof for the open sets. The case of closed sets is dual. By Theorem 3.4, it suffices to verify that condition (1.1) is equivalent with condition (3.1)

$$\text{for every } u \in A^*, xy \in L \text{ implies } xu^+y \cap L \neq \emptyset. \tag{3.1}$$

Let $\eta : A^* \to M$ be the syntactic morphism of L and let $P = L\eta$. Let $e \in E(M)$. By definition of the order on M, $e \leqslant 1$ if, for every $s, t \in M$, $st \in P$ implies $set \in P$.

Assume that condition (1.1) is satisfied and let $u \in A^*$. By Proposition 2.1, there exists an integer $\omega > 0$ such that $(u\eta)^\omega$ is idempotent. Therefore, for every $x, y \in A^*$, $xy \in L$ implies $xu^\omega y \in L$ and $xu^+y \cap L \neq \emptyset$. Thus condition (3.1) is verified.

Conversely, assume that condition (3.1) is satisfied. Let $e \in E(M)$ and $s, t \in M$ be such that $st \in P$. Let $x \in s\eta^{-1}$, $y \in t\eta^{-1}$ and $u \in e\eta^{-1}$. Then $xy \subset L$ and by Proposition 3.1, there exists $n > 0$ such that $xu^n y \in L$. Since u and u^2 are syntactically equivalent, this implies $xuy \in L$ and thus condition (1.1) is verified. □

Corollary 3.6. *A recognizable language is clopen if it is a group language.*

Proof. By Theorem 3.5, a recognizable language is clopen if the identity is the unique idempotent of its syntactic monoid. Now a finite monoid with a unique idempotent is a group. □

We also need a slightly stronger condition on the syntactic image.

Corollary 3.7. *Let P be the syntactic image of a recognizable open set of A^*. Then $s_1 s_2 \cdots s_n \in P$ implies $D(M)s_1D(M)\cdots D(M)s_nD(M) \subseteq P$.*

Proof. It suffices to prove that

$$\text{for every } s,t \in M,\ st \in P \text{ implies } sD(M)t \subseteq P. \tag{3.2}$$

Indeed, (3.2) applied with $t = 1$ (resp. $s = 1$) shows that $s \in P$ implies $sD(M) \subseteq P$ and $D(M)s \subseteq P$. Therefore, $s \in P$ implies $D(M)sD(M) \subseteq P$. Next, assume by induction that $s_1 s_2 \cdots s_{n-1} \in P$ implies $D(M)s_1D(M)\cdots D(M)s_{n-1}D(M) \subseteq P$ and suppose that $s_1 s_2 \cdots s_n \in P$. Then, for each $d_0, d_1, \ldots, d_n \in D$, $d_0 s_1 d_1 \cdots d_{n-2} s_{n-1} s_n d_n \in P$ by the induction hypothesis. Set $s = d_0 s_1 d_1 \cdots d_{n-2} s_{n-1}$ and $t = s_n d_n$. Property 3.2 gives $d_0 s_1 d_1 \cdots d_{n-2} s_{n-1} d_{n-1} s_n d_n \in P$ and thus $D(M)s_1D(M)\cdots D(M)s_nD(M) \subseteq P$.

We now prove (3.2). Let N be the set of all $n \in M$ such that $st \in P$ implies $snt \in P$. Then N is a submonoid of M which contains $E(M)$ by Theorem 3.5. Now if $a\bar{a}a = a$ and $n \in N$, then $st \in P$ implies $sa\bar{a}t \in P$ and $s\bar{a}at \in P$ since $a\bar{a}$ and $\bar{a}a$ are idempotents (because $(a\bar{a})(a\bar{a}) = (a\bar{a}a)\bar{a} = a\bar{a}$ and $(\bar{a}a)(\bar{a}a) = \bar{a}(a\bar{a}a) = \bar{a}a$). Now the condition $(sa)(\bar{a}t) \in P$ implies $(sa)n(\bar{a}t) \in P$ and thus $an\bar{a} \in N$. Similarly, $(s\bar{a})(at) \in P$ implies $(s\bar{a})n(at) \in P$ whence $\bar{a}na \in N$. Therefore N is closed under weak conjugation and thus contains $D(M)$. □

Theorem 3.5 also has some strong consequences on the algebraic structure of M. Recall that an element $\bar{x}$ of a monoid M is an *inverse* of an element x if $x\bar{x}x = x$ and $\bar{x}x\bar{x} = \bar{x}$. A *block group* is a monoid such that every element has at most one inverse.

Theorem 3.8. *Let L be a recognizable language of A^*. If L is open or closed, then its syntactic monoid is a block group.*

Proof. Let $(M, \leqslant)$ be the ordered syntactic monoid of L. Suppose that an element x has two inverses x_1 and x_2. Then $(x_1x)(x_1x) = (x_1xx_1)x = x_1x$ and similarly, xx_1, x_2x and xx_2 are idempotent. Thus if L is closed, Theorem 3.5 shows that $x_1 \leqslant (x_2x)x_1(xx_2) =$

$x_2(xx_1x)x_2 = x_2xx_2 = x_2$ and similarly $x_2 \leqslant x_1$. Thus $x_1 = x_2$ and M is a block group. The proof is similar for L open. □

A subset I of a monoid M is an *ideal* if, for every $x \in I$ and $y \in M$, $xy, yx \in I$. Ideals are naturally ordered by inclusion. It is not difficult to see that in a finite monoid, there is a smallest nonempty ideal, called the *minimal ideal* of M. Standard results of semigroup theory show that the minimal ideal of a block group is a group. Therefore Theorem 3.8 gives the following corollary.

Corollary 3.9. *Let L be a recognizable language of A^*. If L is open or closed, then the minimal ideal of its syntactic monoid is a group.*

4. Main result

Denote by $A^*\mathscr{G}$ the set of all group languages on A^* and by $\mathrm{Pol}(A^*\mathscr{G})$ the polynomial closure of $A^*\mathscr{G}$. Thus a language is in $\mathrm{Pol}(A^*\mathscr{G})$ if it is a finite union of languages of the form $L_0a_1L_1 \cdots a_kL_k$ where the L_i's are group languages. The following result was proved in [11, 16].

Theorem 4.1. *Every recognizable set of* $\mathrm{Pol}(A^*\mathscr{G})$ *is open in the Hall topology.*

Our main result states that the converse is also true.

Theorem 4.2. *Every recognizable open set belongs to* $\mathrm{Pol}(A^*\mathscr{G})$.

Proof. Let X be a recognizable open set of A^* and let $\alpha : A^* \to M$ be the syntactic monoid of X. Let $P = X\alpha$ be the image of X in M. By Theorem 2.3, there exist a finite group G and a monoid morphism $\beta : A^* \to G$ such that $D(M) = \{u\alpha \mid u \in A^* \text{ and } u\beta = 1\}$. Let $R = 1\beta^{-1}$. By construction, R is recognized by G and thus is a group language. Furthermore, for every $u \in R$, $u\beta = 1$ and thus $R\alpha = D(M)$. Let $\gamma : A^* \to M \times G$ be the monoid morphism defined by $m\gamma = (m\alpha, m\beta)$ and let $N = N(\gamma)$ be the integer occurring in Proposition 2.2 for $k = 2$. Thus every word of A^* of length $> N$ factorizes as $u = u_0u_1u_2u_3$ with $u_1, u_2 \in A^+$ and $u_1\gamma = u_2\gamma = f$ where f is an idempotent of $M \times G$. Note that, since 1 is the unique idempotent of G, $f = (e, 1)$ for some $e \in E(M)$. Therefore, the condition on u_1 and u_2 can be rewritten as $u_1\alpha = u_2\alpha = e$ and $u_1\beta = u_2\beta = 1$. In particular, it follows that $u_1, u_2 \in R$. We claim that

$$X = \bigcup_{\substack{a_1 \cdots a_n \in X \\ n \leqslant N}} Ra_1Ra_2 \cdots Ra_nR. \tag{4.1}$$

Let Y be the right hand side of the formula (4.1). To verify the inclusion $Y \subseteq X$, it suffices to prove that $Y\alpha$ is contained in P. Let $a_1 \cdots a_n \in X$, with $n \leqslant N$.

Then $(a_1 \cdots a_n)\alpha \in X\alpha = P$. Now

$$(Ra_1Ra_2 \cdots Ra_nR)\alpha = (R\alpha)(a_1\alpha)(R\alpha) \cdots (a_n\alpha)(R\alpha)$$
$$\subseteq D(M)(a_1\alpha)D(M) \cdots D(M)(a_n\alpha)D(M).$$

It follows, by Corollary 3.7, that $(Ra_1Ra_2 \cdots Ra_nR)\alpha$ is contained in P and thus $Y\alpha$ is contained in P.

We now prove the inclusion $X \subseteq Y$. Let $u \in X$. We show by induction on the length of u that $u \in Y$. If $|u| \leqslant N$, then $u = a_1 \cdots a_n$ with $n \leqslant N$. Since the empty word belongs to R, one also has $u \in Ra_1R \cdots a_nR$ and thus $u \in Y$. Assume that $|u| > N$. Then u factorizes as $u_0u_1u_2u_3$ as indicated above. It follows that $u\alpha = (u_0\alpha)(u_1\alpha)(u_2\alpha)(u_3\alpha) = (u_0\alpha)ee(u_3\alpha) = (u_0\alpha)e(u_3\alpha) = (u_0\alpha)(u_1\alpha)(u_3\alpha) = (u_0u_1u_3)\alpha$. Thus $u\alpha = u'\alpha$ where $u' = u_0u_1u_3$. Now, since u' is shorter that u, one has $u' \in Y$ by the induction hypothesis. Therefore, there exists a word $a_1 \cdots a_n \in X$ (with $n \leqslant N$) and words $r_0, r_1, \ldots, r_n \in R$ such that $u' = r_0a_1r_1 \cdots a_nr_n$. Thus u_0, u_1 and u_3 can be factorized as follows:

$$u_0 = r_0a_1r_1 \cdots a_ir_i',$$
$$u_1 = r_i''a_{i+1} \cdots a_jr_j',$$
$$u_3 = r_j''a_{j+1} \cdots a_nr_n$$

with $r_i'r_i'' = r_i$ and $r_j'r_j'' = r_j$ for some i, j such that $0 \leqslant i \leqslant j \leqslant n$. Now $r_j'u_2r_j'' \in R$ since $(r_j'u_2r_j'')\beta = (r_j'\beta)(u_2\beta)(r_j''\beta) = (r_j'\beta)1(r_j''\beta) = (r_j'r_j'')\beta = r_j\beta = 1$. It follows that $u = u_0u_1u_2u_3 = r_0a_1r_1 \cdots a_j(r_j'u_2r_j'')a_{j+1} \cdots a_nr_n$ whence $u \in Ra_1R \cdots a_nR$ and $u \in Y$. □

It is interesting to note that the integer N occurring in the proof of Theorem 4.2 depends on the cardinality of the group G. Although we did not give any explicit bound on the size of G, it suffices to know that G is finite to prove the existence of the bound N.

Another surprising consequence of the proof is the polynomial expression of X given by the formula (4.1). Recall that a language is in $\mathrm{Pol}(A^*\mathscr{G})$ if it is a finite union of languages of the form $L_0a_1L_1 \cdots a_kL_k$ where the L_i's are group languages. But formula (4.1) shows that the L_i's occurring in the expression for X are all equal to R. In other words, every polynomial of group languages for X is equivalent to a polynomial in R. This surprising result can be explained in two steps.

Lemma 4.3. *Let H be a finite group, P a subset of H and $\gamma : A^* \to H$ be a surjective morphism. Then $P\gamma^{-1}$ is equal to a polynomial in $1\gamma^{-1}$.*

Proof. First, $P\gamma^{-1} = \bigcup_{g \in P} g\gamma^{-1}$. Thus, it suffices the result for $P = \{g\}$. We claim that

$$g\gamma^{-1} = \bigcup_{a_1 \cdots a_k \in E} (1\gamma^{-1})a_1(1\gamma^{-1}) \cdots (1\gamma^{-1})a_k(1\gamma^{-1}) \tag{4.2}$$

where E is the set of words $a_1 \cdots a_k$ such that $(a_1 \cdots a_k)\gamma = g$ and the $k+1$ elements 1γ, $a_1\gamma$, $(a_1 \cdots a_k)\gamma$ are all distincts. Let L be the right hand side of (4.2). The inclusion $L \subseteq g\gamma^{-1}$ is clear. Conversely, if $u\gamma = g$, there exists a unique factorization $u = u_0a_1u_1 \cdots a_ku_k$ such that

(1) $u_0, \ldots, u_k \in A^*$, $a_1, \ldots, a_k \in A$,

(2) for $1 \leqslant i \leqslant k$, $u_0a_1 \ldots u_{i-1}a_iu_i$ is the longest prefix of u such that $(u_0a_1 \ldots u_{i-1}a_i)\gamma = (u_0a_1 \ldots u_{i-1}a_iu_i)\gamma$ and u_0 is the longest prefix such that $u_0\gamma = 1$.

By construction, $u_i\gamma = 1$ and $a_1 \cdots a_k \in E$. Therefore $u \in L$, which proves the claim and the lemma. □

It follows that polynomial expressions of group languages are equivalent with polynomial expressions of group languages of the form $1\gamma^{-1}$ (inverse image of the identity). However this does not explain yet why only one group language occurs in formula (4.1). The trick is that if $L_0, \ldots, L_n$ are group languages recognized by groups $G_0, \ldots, G_n$, respectively, then the group $G = G_0 \times \cdots \times G_n$ recognizes $L_0, \ldots, L_n$. Indeed, suppose that $L_i = P_i\gamma_i^{-1}$ for some $P_i \subseteq G_i$ and some monoid morphism $\gamma_i : A^* \to G_i$ and let $\alpha_i : G_i \to G$ be the group morphism defined by $g\alpha_i = (1, \ldots, 1, g, 1, \ldots, 1)$, where g is in the ith position. Finally, set $\varphi_i = \gamma_i\alpha_i$ and $Q_i = P_i\alpha_i$. Then $P_i = P_i\alpha_i\alpha_i^{-1} = Q_i\alpha_i^{-1}$ and thus $L_i = Q_i\alpha_i^{-1}\gamma_i^{-1} = Q_i\varphi_i^{-1}$.

5. Algorithms

In this section, we give a polynomial time algorithm for testing, given an n-state deterministic automaton $\mathscr{A}$, whether the language L accepted by $\mathscr{A}$ belongs to $\mathrm{Pol}(A^*\mathscr{G})$, or, equivalently, whether L is open in the Hall topology. First we may assume that $\mathscr{A}$ is a complete, minimal, deterministic automaton, since completion and minimalization can be achieved in polynomial time and do not increase the number of states by more than one. Before giving the details of our algorithms, let us fix some convenient notations. Given a finite (complete) deterministic automaton $\mathscr{A} = (Q, A, \cdot)$, we denote by $\mathscr{A}^2 = (Q^2, A, \cdot)$ the direct product of two copies of $\mathscr{A}$, where the action of A on Q^2 is given by

$$(q_1, q_2) \cdot a = (q_1 \cdot a, q_2 \cdot a).$$

We also denote by $G(\mathscr{A})$ (resp. $G_2(\mathscr{A})$) the reflexive and transitive closure of the transition graph of $\mathscr{A}$ (resp. $\mathscr{A}^2$). For instance, if $\mathscr{A}$ is the automaton represented in Fig. 3 then $\mathscr{A}^2$ is the automaton given in Fig. 4 and $G_2(\mathscr{A})$ is the graph given in Fig. 5. A labelled graph G is a *configuration* of $\mathscr{A}$ if G is isomorphic to a subgraph of $G_2(\mathscr{A})$. We can now characterize the open recognizable subsets of A^* as follows.

Theorem 5.1. *Let $\mathscr{A} = (Q, A, E, \{i\}, F)$ be the minimal automaton of a language L. Then L is open if there exist no configuration of $\mathscr{A}$ of the form given in Fig. 6 with $q_1 \in F$ and $q_2 \notin F$.*

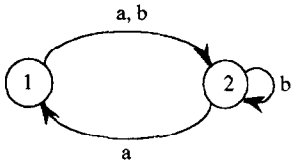


Fig. 3.

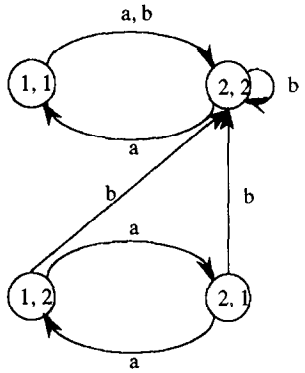


Fig. 4.

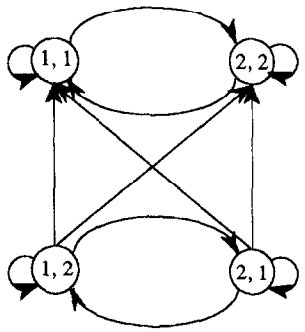


Fig. 5.

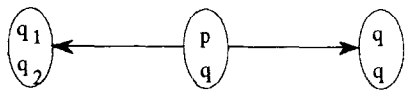


Fig. 6.

Proof. Suppose that L is open, and consider a configuration in $\mathscr{A}$ of the form above. Then there exist two words u and y such that, in $\mathscr{A}$, $p \cdot u = q \cdot u = q$, $p \cdot y = q_1$ and $q \cdot y = q_2$. Since $\mathscr{A}$ is minimal, every state of $\mathscr{A}$ is accessible and in particular, there exists a word $x \in A^*$ such that $i \cdot x = p$. On the one hand, $i \cdot xy = p \cdot y = q_1 \in F$ and

thus $xy \in L$. On the other hand, for every $n > 0$, $i \cdot xu^n y = p \cdot u^n y = q \cdot y = q_2 \notin F$. Therefore $xu^+ y \cap L = \emptyset$, in contradiction with Theorem 3.4.

Conversely, suppose that $\mathscr{A}$ has no configuration of the form above. We show that L is open by using Theorem 3.4. Let x, y and u be words such that $xy \in L$. By Proposition 2.1, there exists an integer n such that $q \cdot u^n = q \cdot u^{2n}$ for all $q \in Q$. Set $v = u^n$, $p = i \cdot x$, $q = p \cdot v$, $q_1 = p \cdot y$ and $q_2 = q \cdot y$. Then $q \cdot v = p \cdot v^2 = p \cdot v = q$ and $q_1 = i \cdot xy \in F$ since $xy \in L$. Therefore $q_2 \in F$, otherwise $\mathscr{A}$ would contain a forbidden configuration. It follows $i \cdot xvy = q_2 \in F$ and thus $xvy \in L$. Therefore $xu^+ y \cap L \neq \emptyset$ and L is open. □

The previous result yields to a polynomial-time algorithm to check whether the language accepted by of a n-state deterministic automaton is open.

Corollary 5.2. *There is a polynomial time algorithm for testing whether the language accepted by an n-state minimal automaton is open.*

Proof. One can check whether $\mathscr{A}$ contains a configuration of the form (5.4) by computing G_2 and by verifying there are no quadruples $\{p, q, q_1, q_2\}$ of states such that

(a) $((p,q),(q,q))$ is an edge in $G_2(\mathscr{A})$, and

(b) $((p,q),(q_1,q_2))$ is an edge in $G_2(\mathscr{A})$,

(c) $q_1 \in F$ and $q_2 \notin F$.

Since G_2 has n^2 vertices, this gives a polynomial algorithm. □

6. A separation result

A language K *separates* two (disjoint) languages L_1 and L_2 if either $L_1 \subseteq K \subseteq A^* \setminus L_2$ or $L_2 \subseteq K \subseteq A^* \setminus L_1$. The aim of this section is to prove the following theorem:

Theorem 6.1. *Any two disjoint languages of* $\mathrm{Pol}(A^*\mathscr{G})$ *can be separated by a group language.*

Theorem 6.1 follows from a series of lemmæ of independent interest. Let L_1 and L_2 be two disjoint languages of $\mathrm{Pol}(A^*\mathscr{G})$.

Lemma 6.2. *There exists a morphism* η *from* A^* *onto an ordered monoid satisfying* (1.1) *which recognizes simultaneously* L_1 *and* L_2.

Proof. Let, for $i = 1, 2$, $\eta_i : A^* \to M_i$ be the syntactic morphism of L_i. Let $\eta : A^* \to M_1 \times M_2$ be the morphism defined by $a\eta = (a\eta_1, a\eta_2)$ for every $a \in A$ and let $M = A^*\eta$. By Theorem 3.8, M_1 and M_2 are ordered monoid satisfying (1.1) and thus M is also an ordered monoid satisfying (1.1). For $i = 1, 2$, let $I_i = \{(x_1, x_2) \in M \mid x_i \in L_i\eta_i\}$. Then I_i is an order ideal of M: if $(x_1, x_2) \in I_i$ and $(y_1, y_2) \leqslant (x_1, x_2)$ for some $(y_1, y_2) \in M$, then $y_i \leqslant x_i$ and since $L_i\eta_i$ is an order ideal of M_i, $y_i \in L_i\eta_i$ and $(y_1, y_2) \in$

I_i. Finally $I_i\eta^{-1} = L_i$ since $L_i\eta_i\eta_i^{-1} = L_i$. Thus η simultaneously recognizes L_1 and L_2. □

Let M be an ordered monoid satisfying (1.1) recognizing simultaneously L_1 and L_2. Given a subset I of M, denote by $\bar{I}$ the smallest subset E of M containing I and such that, if $x \in E$ and y is comparable to x, then $y \in E$.

Lemma 6.3. *If I is an order ideal of M, then $\bar{I}$ recognizes a group language.*

Proof. It suffices to show that the syntactic monoid of $\bar{I}$ in M is a group. Let $e \in E(M)$. Then $e \leqslant 1$ by definition of the order on M. We claim that $e \sim_{\bar{I}} 1$. Indeed, for every $x, y \in M$, $xey \leqslant xy$ and thus the conditions $xey \in \bar{I}$ and $xy \in \bar{I}$ are equivalent by definition of $\bar{I}$. Thus the identity is the unique idempotent of $M/\sim_{\bar{I}}$. It follows by Propostion 2.1 that, for each element x of $M/\sim_{\bar{I}}$, $x^{\omega-1}$ is an inverse of x and thus $M/\sim_{\bar{I}}$ is a group. □

We now establish some properties of ordered monoids satisfying (1.1). We first consider the case of ordered groups.

Lemma 6.4. *The only stable order relation on a finite group is the equality relation.*

Proof. Suppose that $x \leqslant y$. Then $x^{\omega-1} \leqslant y^{\omega-1}$ and thus $x \leqslant y = x^\omega y = xx^{\omega-1}y \leqslant xy^{\omega-1}y = xy^\omega = x$, that is, $x = y$. □

Lemma 6.5. *If two elements of M have a common upper bound, they also have a common lower bound.*

Proof. By Corollary 3.9, the minimal ideal of M is a group G. Let e be its identity. If $x \leqslant z$ and $y \leqslant z$, then $ex \leqslant ez$ and $ey \leqslant ez$. Since G is an ideal, $e \in G$ implies $ex, ey, ez \in G$. Now by Lemma 6.4, the restriction of the order to G is the equality relation. Thus $ex = ez = ey$ and since $e \leqslant 1$, $ex \leqslant x$ and $ey \leqslant y$. Thus ex is a common lower bound of x and y. □

Lemma 6.6. *Let I be an order ideal of M. Then $x \in \bar{I}$ if there exists $y \in I$ such that $y \leqslant x$.*

Proof. Let $J = \{x \in M \mid \exists y \in I \text{ such that } y \leqslant x\}$. Then J contains I and is a subset of $\bar{I}$ by definition. Let $x, y \in M$ be such that $x \leqslant y$. If $x \in J$, there exists $z \in I$ such that $z \leqslant x$. It follows $z \leqslant y$ by transitivity and thus $y \in J$. Conversely, if $y \in J$, there exists $z \in I$ such that $z \leqslant y$. Since y is a common upper bound of x and z, there exists by Lemma 6.5 an element t such that $t \leqslant x$ and $t \leqslant z$. Now $t \in I$ since $z \in I$. Thus $x \in J$. It follows that $x \in J$ if $y \in J$ and therefore $\bar{I} = J$. □

Lemma 6.7. *If I_1 and I_2 are two disjoint order ideals of an ordered monoid satisfying* (1.1), *then $\bar{I}_1$ and $\bar{I}_2$ are also disjoint.*

Proof. Assume that $\bar{I}_1$ and $\bar{I}_2$ are not disjoint and let $z \in \bar{I}_1 \cap \bar{I}_2$. By Lemma 6.6, there exist $x_1, x_2 \in I$ such that $x_1 \leqslant z$ and $x_2 \leqslant z$. Now, by Lemma 6.5, there exists t such that $t \leqslant x_1$ and $t \leqslant x_2$. It follows that $t \in I_1 \cap I_2$, a contradiction. □

We can now conclude the proof of Theorem 6.1. Let $K = \bar{I}_1 \eta^{-1}$. Since $\bar{I}_1$ contains I_1, K contains L_1. Furthermore, K is a group language by Lemma 6.3 and since $\bar{I}_1$ and $\bar{I}_2$ are disjoint by Lemma 6.7, K is disjoint from L_2. □

Theorem 6.1 has some interesting topological consequences.

Corollary 6.8. *Any two disjoint recognizable open sets can be separated by a recognizable clopen set.*

I am indebted to Daniel Lascar, from the Department of Logic, University of Paris VII, for pointing out the next corollary. Let us first mention another consequence of the conjecture on open sets mentionned in the introduction and recently proved by Ribes and Zalesskii [21]. It was shown in [16], this former conjecture implies that the closure of a recognizable language is recognizable. Corollary 6.9 shows that the closure of a recognizable open language is a group language.

Corollary 6.9. *The closure of a recognizable open set is a recognizable clopen set.*

Proof. Let L be a recognizable open set and let $\bar{L}$ be its closure. Since $\bar{L}$ is recognizable, its complement is a recognizable open set, disjoined from L. By Corollary 6.8, there exists a clopen set C such that $L \subseteq C \subseteq \bar{L}$. It follows that $C = \bar{L}$, since $\bar{L}$ is by definition the smallest closed set containing L. □

7. Conclusion and open problems

To sum up, we have proved the following theorem

Theorem 7.1. *Let L be a recognizable set of A^*, let M be its syntactic monoid and let P be its syntactic image. Then the following conditions are equivalent.*

(a) *L belongs to the polynomial closure of group languages,*
(b) *L is open in the group topology,*
(c) *for every $u \in A^*$, $xy \in L$ implies $xu^+y \cap L \neq \emptyset$.*
(d) *for every $s, t \in M$ and $e \in E(M)$, $st \in P$ implies $set \in P$,*
(e) *the minimal automaton of L does not contain the configuration given in Fig. 6, with $q_1 \in F$ and $q_2 \notin F$.*

and we have derived some topological consequences of this result. The Hall topology, as defined in this article, is actually a special case of the topologies defined by Hall in his seminal paper [6]. Indeed, one can attach a topology to each class of finite groups closed under taking subgroups, quotients and finite direct products. For instance, one may consider the p-groups (for some prime p), the solvable groups or the nilpotent groups. To have the definition of the corresponding topology, just replace in the definition every occurrence of "group" by "p-group" (resp. solvable group, nilpotent group). One can show, in these three examples, that the topology can be defined by a distance. The question is now to characterize the recognizable open sets with respect to these topologies and the polynomial closure of the corresponding group languages. There is some hope to solve both questions in the case of p-groups since Ribes and Zalesskii have recently proved an analogous of their result for p-groups [22], but the problem seems to be more difficult for the two other classes.

References

[1] C.J. Ash, Inevitable sequences and a proof of the type II conjecture, in: *Proc. Monash Conf. on Semigroup Theory* (World Scientific, Singapore, 1991) 31–42.

[2] C.J. Ash, Inevitable Graphs: A proof of the type II conjecture and some related decision procedures, *Internat. J. Algebra Comp.* **1** (1991) 127–146.

[3] J. Berstel, *Transductions and Context Free Languages* (Teubner, Leipzig, 1979).

[4] S. Eilenberg, *Automata, Languages and Machines, Vol. A* (Academic Press, New York, 1974).

[5] S. Eilenberg, *Automata, Languages and Machines, Vol. B* (Academic Press, New York, 1976).

[6] M. Hall Jr., A topology for free groups and related groups, *Ann. of Maths* **52** (1950) 127–139.

[7] K. Henckell, S.W. Margolis, J.-E. Pin and J. Rhodes, Ash's Type II Theorem, Profinite Topology and Malcev Products, *Internat. J. Algebra Comput.* **1** (1991) 411–436.

[8] K. Henckell and J. Rhodes, The theorem of Knast, the $PG = BG$ and Type II Conjectures, in: J. Rhodes, ed., *Monoids and Semigroups with Applications* (Word Scientific, 1991) 453–463

[9] S.W. Margolis and J.-E. Pin, Varieties of finite monoids and topology for the free monoid, in: K. Byleen, P. Jones and F. Pastijn, eds., *Proc. 1984 Marquette Conf. on Semigroups*, (Dept. Mathematics, Statistics and Computer Science, Marquette University, 1984) 113–130.

[10] S.W. Margolis and J.E. Pin, Product of group languages, *Proc. FCT Conf.*, Lecture Notes in Computer Science, Vol. 199 (Springer, Berlin, 1985) 285–299.

[11] J.-E. Pin, Finite group topology and p-adic topology for free monoids, in: *Proc. 12th ICALP*, Lecture Notes in Computer Science, Vol. 194, (Springer, Berlin, 1985) 445–455.

[12] J.-E. Pin, *Variétés de langages formels* (Masson, Paris, 1984). *Varieties of formal languages* (North Oxford Academic, London, 1986 and Plenum, New York, 1986).

[13] J.-E. Pin, *On the languages recognized by finite reversible automata*, in: *Proc.14th ICALP*, Lecture Notes in Computer Science, Vol. 267 (Springer, Berlin, 1987) 237–249.

[14] J.-E. Pin, A topological approach to a conjecture of Rhodes, *Bull. Austral. Math. Soc.* **38** (1988) 421–431.

[15] J.-E. Pin, Relational morphisms, transductions and operations on languages, in: J.E. Pin, ed., *Formal Properties of Finite Automata and Applications*, Lecture Notes in Computer Science, Vol. 386 (Springer, Berlin 1989) 120–137.

[16] J.-E. Pin, Topologies for the free monoid, *J. Algebra* **137** (1991) 297–337.

[17] J.-E. Pin, Logic, semigroups and automata on words, *Annals of Mathematics and Artificial Intelligence* **16** (1996) 343–384.

[18] J.-E. Pin and C. Reutenauer, A conjecture on the Hall topology for the free group, *Notices London Math. Soc.* **23** (1991) 356–362.

[19] Ch. Reutenauer, Une topologie du monoïde libre, *Semigroup Forum* **18** (1979) 33–49.

[20] Ch. Reutenauer, Sur mon article "Une topologie du monoïde libre", *Semigroup Forum* **22** (1981) 93–95.

[21] L. Ribes and P.A. Zalesskii, On the profinite topology on a free group, *Bull. London Math. Soc.* **25** (1993) 37–43.
[22] L. Ribes and P.A. Zalesskii, The pro-p topology of a free group and algorithmic problems in semigroups, *Internat. J. Algebra Comp.* **4** (1994) 359–374.
[23] M.P. Schützenberger, Sur le produit de concaténation non ambigu, *Semigroup Forum* **13** (1976) 47–75.
[24] I. Simon, The product of rational languages, in: *Proc. ICALP 1993*, Lecture Notes in Computer Science, Vol. 700 (Springer, Berlin, 1993), 430–444.
[25] W. Thomas, Classifying regular events in symbolic logic, *J. Comput. System Sci* **25** (1982) 360–375.