A robust class of regular languages

Antonio Cano Gómez[1] and Jean-Éric Pin[2*]

[1] Departamento de Sistemas Informáticos y Computación, Universidad Politécnica de Valencia, Camino de Vera s/n, P.O. Box: 22012, E-46020 - Valencia.
[2] LIAFA, Université Paris-Diderot and CNRS, Case 7014, 75205 Paris Cedex 13, France.

Abstract. In this survey paper, we present known results and open questions on a proper subclass of the class of regular languages. This class, denoted by $\mathcal{W}$, is especially robust: it is closed under union, intersection, product, shuffle, left and right quotients, inverse of morphisms, length preserving morphisms and commutative closure. It can be defined as the largest positive variety of languages not containing the language $(ab)^*$. It admits a nontrivial algebraic characterization in terms of finite ordered monoids, which implies that $\mathcal{W}$ is decidable: given a regular language, one can effectively decide whether or not it belongs to $\mathcal{W}$. We propose as a challenge to find a constructive description and a logical characterization of $\mathcal{W}$.

Warning. In this paper, square brackets are used as a substitute to "respectively" to gather several definitions [properties] into a single one.

The search for robust classes of regular languages is an old problem of automata theory, which occurs in particular in the study of regular model checking [3]. In this survey paper, we present known results and open questions on a proper subclass of the class of regular languages, introduced a few years ago by the authors in connection with the study of the shuffle product [6, 7]. This class, denoted by $\mathcal{W}$, is especially robust: it is closed under union, intersection, product, shuffle, left and right quotients, inverse of morphisms, length preserving morphisms and commutative closure. Furthermore, this class is decidable: there is an algorithm to decide whether a given regular language belongs to $\mathcal{W}$ or not. As such, it might offer an appropriate framework for modeling certain problems arising in the verification of concurrent systems.

The class $\mathcal{W}$ is also interesting on its own and appears in the study of three operations on languages: length preserving morphisms, inverse of substitutions and shuffle product. More specifically, $\mathcal{W}$ is the largest proper positive variety of languages closed under one of these operations. It is also the largest positive variety of languages not containing the language $(ab)^*$.

* The authors acknowledge support from the AutoMathA programme of the European Science Foundation.

All these results rely on an algebraic characterization of $\mathcal{W}$ in terms of ordered monoids (Theorem 4.3). It gives us the opportunity to review this algebraic approach and to apply it to a concrete example.

Our paper is organised as follows. In Section 1, we briefly introduce the definitions needed for this paper, including the notion of ordered automaton, which might be new to most readers. Section 2 presents the algebraic background. Again, the less familiar notions are probably those of ordered monoid and of profinite monoids. Section 3 is devoted to general results derived from the algebraic approach, including specific results on length preserving morphisms and the shuffle operation. The class $\mathcal{W}$, its algebraic characterization and its main properties are presented in Section 4. Closure under partial commutation is discussed in Section 5. Finally, we propose a few open problems on $\mathcal{W}$ in the final section. One of them is to find a logical characterization for $\mathcal{W}$, a problem which is widely open.

1 Languages and automata

In this paper, an *alphabet* is a finite set whose elements are called *letters*. The free monoid A^* is the set of words on the alphabet A. The length of a word u is denoted by $|u|$. The *empty word*, denoted by 1, is the unique word of length 0.

1.1 Ordered automata

An *ordered automaton* is a deterministic automaton equipped with a partial order on its set of states. This order is required to be compatible with the action of each letter. Formally, we are given an automaton $\mathcal{A} = (Q, A, \cdot\,, i, F)$ and a partial order $\leqslant$ on Q such that, for all $p, q \in Q$ and $a \in A$, $p \leqslant q$ implies $p\cdot a \leqslant q\cdot a$.

If $\mathcal{A}$ is a minimal deterministic automaton, there is a canonical way to define a partial order on Q, called the *syntactic order* on Q. Define a relation $\leqslant$ on Q by $p \leqslant q$ if and only if for each $u \in A^*$,

$$q\cdot u \in F \Rightarrow p\cdot u \in F$$

It is clear that $\leqslant$ is reflexive and transitive. To see it is a partial order, suppose that $p \leqslant q$ and $q \leqslant p$. Then, for all $u \in A^*$, one gets $q\cdot u \in F$ if and only if $p\cdot u \in F$, which gives $p = q$ since $\mathcal{A}$ is minimal.

Thus every language admits a *minimal ordered automaton*. In the remainder of this paper, we consider only regular languages and finite automata.

Example 1.1. For the minimal automaton of the language $(ab)^*$ represented in Figure 1, the order on the set of states is $1 < 0$ and $2 < 0$.

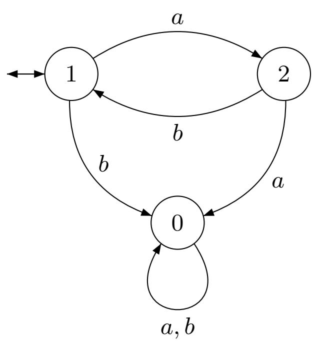


Figure 1. The minimal automaton of $(ab)^*$.

Example 1.2. For the minimal automaton of the language $(ab)^* \cup A^*aaA^*$ (with $A = \{a, b\}$) represented in Figure 2, the order on the set of states is $0 < 1 < 3$ and $0 < 2 < 4 < 3$.

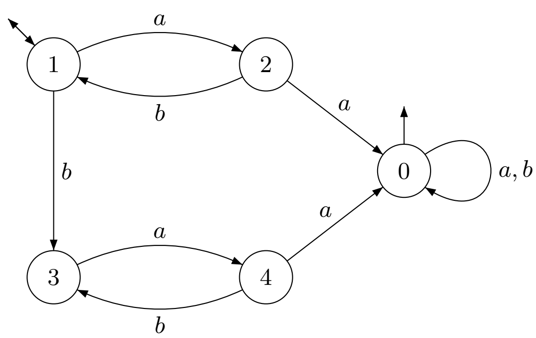


Figure 2. The minimal automaton of $(ab)^* \cup A^*aaA^*$.

1.2 Operations on languages

A number of operations preserve regular languages: Boolean operations, product, star, shuffle, quotients, morphisms, inverse of morphisms, etc.

Boolean operations comprise union, intersection and complement. Let L_1 and L_2 be two languages of A^*. The *(concatenation) product* of L_1 and L_2 is the language

$$L_1L_2 = \{x_1x_2 \mid x_1 \in L_1,\ x_2 \in L_2\}$$

Their *shuffle* is the language

$$L_1 \sqcup\!\sqcup L_2 = \{w \in A^* \mid w = u_1v_1 \cdots u_nv_n \text{ for some } n \geqslant 0 \text{ such that } u_1 \cdots u_n \in L_1, v_1 \cdots v_n \in L_2\}$$

Given a language L and a word u, the *left and right quotients* of L by u are the languages

$$u^{-1}L = \{x \in A^* \mid ux \in L\}$$
$$Lu^{-1} = \{x \in A^* \mid xu \in L\}$$

A *morphism* between two free monoids A^* and B^* is a map $\varphi : A^* \to B^*$ such that, for all $u, v \in A^*$, $\varphi(uv) = \varphi(u)\varphi(v)$. This condition implies in particular that $\varphi(1) = 1$. The morphism φ is *length preserving* if, for all $u \in A^*$, the condition $|\varphi(u)| = |u|$ is satisfied. This is equivalent to requiring that, for all $a \in A$, $\varphi(a) \in B$.

The languages of A^* form a monoid for the concatenation product, called the *monoid of languages* of A^*. A *substitution* from A^* into B^* is a monoid morphism σ from A^* into the monoid of languages on B^*. In particular, $\sigma(1) = \{1\}$, the language reduced to the empty word and if $u = a_1 \cdots a_n$, $\sigma(u) = \sigma(a_1) \cdots \sigma(a_n)$. Thus a substitution is completely determined by the languages $\sigma(a)$, for $a \in A$.

The *inverse substitution* σ^{-1} maps a language K of B^* onto the language $\sigma^{-1}(K)$ of A^*, defined by

$$\sigma^{-1}(K) = \{u \in A^* \mid \sigma(u) \cap K \neq \emptyset\}$$

1.3 Classes of languages and varieties of languages

A *class of languages* is a correspondence $\mathcal{C}$ which associates with each alphabet A a set $\mathcal{C}(A^*)$ of regular languages of A^*. It is *closed under inverse of morphisms [substitutions]* if, for any morphism [substitution] $\varphi : A^* \to B^*$ and for any language $L \in \mathcal{C}(B^*)$, the language $\varphi^{-1}(L)$ belongs to $\mathcal{C}(A^*)$. Similarly, it is *closed under length-preserving morphism* if, for any length-preserving morphism $\varphi : A^* \to B^*$ and for any language $L \in \mathcal{C}(A^*)$, the language $\varphi(L)$ belongs to $\mathcal{C}(B^*)$. Finally, it is closed under union [intersection, complement, residuals, product, shuffle, etc.] if, for each alphabet A, the set $\mathcal{C}(A^*)$ is closed under union [intersection, complement, residuals, product, shuffle, etc.]

A class of regular languages is said to be *proper* if it is not the class of all regular languages.

A *positive variety of languages* is a class of regular languages closed under union, intersection, residuals and inverses of morphisms. A *variety of languages* is a positive variety closed under complement.

2 A bit of algebra

In this section, we gather the algebraic notions used in this paper: semigroups, monoids, ordered monoids, power monoids, profinite monoids and varieties.

2.1 Semigroups and monoids

A *semigroup* is a set equipped with an associative operation, usually denoted multiplicatively. A *monoid* is a semigroup with an identity element, usually denoted by 1.

An element e of a monoid is *idempotent* if $e^2 = e$. Given an element s of a finite semigroup S, s^ω denotes the unique idempotent of the subsemigroup of S generated by s. Two elements s and t of a semigroup are *mutually inverse* if $sts = s$ and $tst = t$.

Let M be a finite monoid. The *exponent* of M is the least integer ω such that for all $x \in M$, x^ω is idempotent. Its *period* is the least integer p such that for all $x \in M$, $x^{\omega+p} = x^\omega$.

An *ideal* of a monoid M is a subset I of M such that $MIM \subseteq I$. An ideal I is called *minimal* if, for every J of M, the condition $J \subseteq I$ implies $J = \emptyset$ or $J = I$. Every finite monoid admits a unique minimal ideal. This minimal ideal I has a very constrained structure: in particular, if e is an idempotent of I and x is an element of M, then $(exe)^\omega = e$.

Let M and N be two monoids. A *morphism of monoids* from M into N is a function $\varphi : M \to N$ such that $\varphi(1) = 1$ and for all $x, y \in M$, $\varphi(xy) = \varphi(x)\varphi(y)$.

A *transformation* on a set Q is a map from Q to Q. We use the notation $q\cdot f$ to denote the image of an element $q \in Q$ by f, instead of the standard $f(q)$. The product of two transformations f and g is the transformation fg defined, for all $q \in Q$, by $q\cdot(fg) = (q\cdot f)\cdot g$. Note that, in traditional notation, the function fg would be denoted $g \circ f$. Equipped with this product, the set of transformations on Q form a monoid, denoted by $\mathcal{T}(Q)$.

Given a deterministic automaton $\mathcal{A} = (Q, A, \cdot, i, F)$, each word $u \in A^*$ defines a transformation on Q, which maps the state q onto the state $q\cdot u$. The set of all these transformations form a submonoid of $\mathcal{T}(Q)$, called the *transition monoid* of $\mathcal{A}$. One can also attach a finite monoid to a nondeterministic automaton. See [14, 16] for more details.

The monoid attached to the minimal automaton of a language is called its *syntactic monoid*. It can be defined directly as follows. The *syntactic congruence* of a language L of A^* is the congruence $\sim_L$ defined on A^* by setting $u \sim_L v$ if and only if, for every $x, y \in A^*$,

$$xvy \in L \Leftrightarrow xuy \in L$$

The *syntactic monoid* is the quotient of A^* by $\sim_L$ and the natural morphism from A^* onto M is called the *syntactic morphism* of L.

2.2 Ordered monoids

An *ordered monoid* is a monoid M equipped with a partial order $\leqslant$ compatible with the product on M: for all $x, y, z \in M$, if $x \leqslant y$ then $zx \leqslant zy$ and $xz \leqslant yz$.

Let $(M, \leqslant)$ be an ordered monoid. An *order ideal* of M is a subset I of M such that if $x \in I$ and $y \leqslant x$ then $y \in I$. A *filter* of M is a subset F of M such that if $x \in F$ and $x \leqslant y$ then $y \in F$. Note that a subset of M is a filter if and only if its complement is an order ideal.

Let M and N be two ordered monoids. A *morphism of ordered monoids* is an order-preserving monoid morphism from M into N. We say that N is a *quotient* of M if there exists a surjective morphism of ordered monoids from M onto N. An *ordered submonoid* of M is a submonoid of M, equipped with the restriction of the order on M.

The *product* of a family $(M_i)_{i \in I}$ of ordered monoids is the ordered monoid defined on the set $\prod_{i \in I} M_i$. The multiplication and the order relation are defined componentwise.

2.3 Monoids and automata

There are two ways to make use of monoids to describe languages.

The first solution bypasses the notion of automata by defining directly languages recognized by an [ordered] monoid. We just recall this definition in the ordered case [14, 16]. A language L of A^* is *recognized by an ordered monoid* $(M, \leqslant)$ if and only if there exist an order ideal I of M and a monoid morphism η from A^* into M such that $L = \eta^{-1}(I)$.

The second solution relies on the notion of transition monoid. If a deterministic automaton $\mathcal{A} = (Q, A, \cdot, i, F)$ is partially ordered, then its transition monoid M can be ordered in a natural way. It suffices to set $u \leqslant v$ if and only if, for every $x \in M$ and $q \in Q$,

$$q \cdot vx \in F \Rightarrow q \cdot ux \in F$$

If $\mathcal{A}$ is the ordered minimal automaton of a language L, we obtain the *syntactic ordered monoid* of L. The *syntactic order* $\leqslant$ on M can also be defined directly. Let $\eta : A^* \to M$ be the syntactic morphism of L. Then, given $u, v \in M$, one has $u \leqslant v$ if and only if, for all $x, y \in M$,

$$xvy \in \eta(L) \Rightarrow xuy \in \eta(L)$$

Example 2.1. The minimal automaton $\mathcal{A}$ of the language $(ab)^*$ is represented in Figure 1. The transition monoid of $\mathcal{A}$ contains six elements which correspond to the words 1, a, b, ab, ba and aa.

1	a	b	aa	ab	ba
1	2	0	0	1	0
2	0	1	0	0	2

Furthermore aa is a zero of this monoid and thus can be denoted 0. Finally, the syntactic ordered monoid of $(ab)^*$ is the ordered monoid

$$B_2^{1-} = \{1, a, b, ab, ba, 0\}$$

presented by the relations $aba = a$, $bab = b$ and $aa = bb = 0$. The syntactic order is given by $1 \leqslant ab$, $1 \leqslant ba$ and $x \leqslant 0$ for every $x \in M$. This ordered monoid will play an important role in this paper.

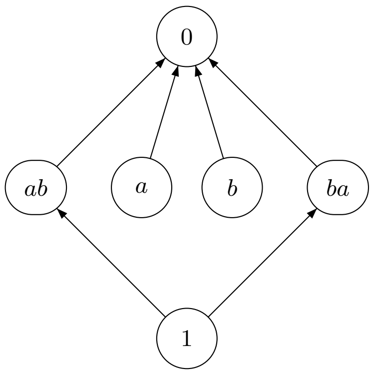


Figure 3. The order on B_2^{1-}.

2.4 Power monoids

Let M be a monoid and let $\mathcal{P}(M)$ be the set of subsets of M. Define the *product of two subsets* X and Y of M as the set

$$XY = \{xy \mid x \in X \text{ and } y \in Y\}$$

This operation makes $\mathcal{P}(M)$ a monoid, called the *power monoid* of M.

It is possible to extend this notion to ordered monoids [7, 19]. Let $(M, \leqslant)$ be an ordered monoid. Define the *product of two filters* F and G of M as the filter generated by the set FG:

$$\uparrow FG = \{z \in M \mid \text{there exist } x \in F \text{ and } y \in G \text{ such that } xy \leqslant z\}$$

This operation turns the set of filters on M into an ordered monoid, denoted by $\mathcal{P}^+(M, \leqslant)$, in which the order relation is the reverse inclusion $\supseteq$.

2.5 Profinite monoids

We briefly recall the definition of a free profinite monoid. More details can be found in [1, 2]. Let A be an alphabet. A monoid M *separates* two words u and v of the free monoid A^* if there exists a morphism φ from A^* onto M such that $\varphi(u) \neq \varphi(v)$. We set

$$r(u, v) = \min\bigl\{|M| \bigm| M \text{ is a monoid that separates } u \text{ and } v\bigr\}$$

and $d(u, v) = 2^{-r(u,v)}$, with the usual conventions $\min \emptyset = +\infty$ and $2^{-\infty} = 0$. Then d is an *ultrametric* on A^*, that is, satisfies the following properties, for all $u, v, w \in A^*$,

(1) $d(u, v) = 0$ if and only if $u = v$,
(2) $d(u, v) = d(v, u)$,

(3) $d(u, w) \leqslant \max\{d(u, v), d(v, w)\}$.

For the metric d, the closer are two words, the larger is the monoid needed to separate them.

As a metric space, A^* admits a completion, denoted by $\widehat{A^*}$. As A^* is dense in $\widehat{A^*}$ and since the product on A^* is uniformly continuous, it can be extended by continuity to $\widehat{A^*}$. The resulting monoid is called the *free profinite monoid* on A. This is a topological compact monoid which admits a unique minimal ideal. The elements of $\widehat{A^*}$ are called *profinite words*.

It can be shown that, for each profinite word x, the sequence $(x^{n!})_{n \geqslant 0}$ is a Cauchy sequence. It converges to an idempotent element of $\widehat{A^*}$, denoted by x^ω.

Every monoid morphism from A^* into a finite monoid M (considered as a discrete metric space), can be extended by continuity to a morphism from $\widehat{A^*}$ into M. In particular, the image of x^ω under any morphism $\varphi : A^* \to M$ into a finite monoid M is well defined: it is the unique idempotent of the subsemigroup of M generated by $\varphi(x)$. This fully justifies the natural formula $\varphi(x^\omega) = (\varphi(x))^\omega$, in which the ω on the right hand side denotes the exponent of M.

2.6 Varieties of finite monoids

A *variety of finite monoids* is a class of finite monoids closed under taking submonoids, quotients and finite direct products. *Varieties of finite ordered monoids* are defined analogously.

Given a variety of finite ordered monoids $\mathbf{V}$, the variety of finite ordered monoids $\mathbf{P}^+\mathbf{V}$ is generated by the monoids of the form $\mathcal{P}^+(M, \leqslant)$ where $(M, \leqslant) \in \mathbf{V}$.

In the same way as varieties in Birkhoff sense, varieties of finite monoids can be equationally defined, but this description involves *profinite equations*, which are formal equalities between two profinite words. More precisely, let u and v be two profinite words of $\widehat{A^*}$. A finite monoid M *satisfies the profinite equation* $u = v$ if and only if, for each morphism $\varphi : \widehat{A^*} \to M$, $\varphi(u) = \varphi(v)$. Similarly, a finite ordered monoid M *satisfies the profinite equation* $u \leqslant v$ if and only if, for each morphism $\varphi : \widehat{A^*} \to M$, $\varphi(u) \leqslant \varphi(v)$.

Given a set E of profinite equations, the class of finite [ordered] monoids satisfying all the equations of E form a variety of finite [ordered] monoids, denoted by $[\![E]\!]$. Reiterman's theorem [20] states that every variety of finite monoids can be defined by a set of profinite equations of the form $u = v$. As shown in [17], this result extends to varieties of finite ordered monoids, using equations of the form $u \leqslant v$.

For instance the variety **Com** of finite commutative monoids is defined by the single equation $xy = yx$. The variety of finite groups is defined by the single equation $x^\omega = 1$. The variety of finite ordered monoids $\mathbf{P}^+\mathbf{G}$ is defined by the single equation $x^\omega \leqslant 1$ [18].

3 The algebraic approach

The general idea of the algebraic approach is to classify regular languages through algebraic properties of their syntactic [ordered] monoid. We recall here two versions of the variety theorem. Extended versions were also obtained in [23, 9] and a unified version is proposed in [11].

3.1 The variety theorem

Denote by $\mathbf{V} \to \mathcal{V}$ the correspondence which associates to a variety of finite [ordered] monoids the class $\mathcal{V}$ of all languages of A^* whose syntactic [ordered] monoid belongs to $\mathbf{V}$. One can show that $\mathcal{V}$ is a [positive] variety of languages.

Similarly, we denote by $\mathbf{V} \to \mathcal{V}$ the correspondence which associates to a [positive] variety of languages $\mathcal{V}$ the smallest variety of finite [ordered] monoids $\mathbf{V}$ containing the syntactic [ordered] monoids of the languages of $\mathcal{V}$.

The original variety theorem is due to Eilenberg [8]. Its ordered version was proved by the second author in [15].

Theorem 3.1 (Variety theorem). *The correspondences $\mathbf{V} \to \mathcal{V}$ and $\mathcal{V} \to \mathbf{V}$ are mutually inverse one to one correspondences between the varieties of finite [ordered] monoids and the [positive] varieties of languages.*

For instance, the variety of languages corresponding to **Com** is the variety $\mathcal{C}om$ of all commutative languages. Recall that a language L is *commutative* if $a_1a_2 \cdots a_n \in L$ implies $a_{\sigma(1)}a_{\sigma(2)} \cdots a_{\sigma(n)} \in L$ for each permutation σ of $\{1, 2, \ldots, n\}$. Other descriptions of $\mathcal{C}om$ can be found in [8, 13].

The variety of languages corresponding to **G** is the variety of group languages. Recall that a *group language* is a regular language whose syntactic monoid is a group, or, equivalently, is recognized by a finite deterministic automaton in which each letter defines a permutation of the set of states.

The languages of the positive variety corresponding to $\mathbf{P}^+\mathbf{G}$ are the polynomials of group languages. Recall that, given a class $\mathcal{C}$ of regular languages, the *polynomial languages* of $\mathcal{L}$ are the finite unions of languages of the form $L_0a_1L_1 \cdots a_kL_k$ where $a_1, \ldots, a_k$ are letters and $L_0, \ldots, L_k$ are languages of $\mathcal{C}$.

3.2 Length preserving morphisms and inverse of substitutions

Power monoids are the appropriate tool to study length preserving morphisms [12, 21, 22]. We recall here the ordered version of these results [7, 19].

Given a positive variety of languages $\mathcal{V}$, the positive variety of languages $\Lambda^+\mathcal{V}$ is defined as follows. For each alphabet A, $\Lambda^+\mathcal{V}(A^*)$ is the lattice of languages generated by the languages of the form $\varphi(L)$, where $L \in \mathcal{V}(B^*)$ for some alphabet B and φ is a length preserving morphism from B^* into A^*.

Proposition 3.2. *Let $\mathcal{V}$ be a positive variety of languages and let $\mathbf{V}$ be the corresponding variety of finite ordered monoids. Then $\Lambda^+\mathcal{V}$ is a positive variety of languages and the corresponding variety of finite ordered monoids is $\mathbf{P}^+\mathbf{V}$.*

There is a similar result for inverse of substitutions. Given a positive variety of languages $\mathcal{V}$, the positive variety of languages $\Sigma^+\mathcal{V}$ is defined as follows. For every alphabet A, $\Sigma^+\mathcal{V}(A^*)$ is the lattice of languages generated by the languages of the form $\sigma^{-1}(L)$, where $L \in \mathcal{V}(B^*)$ for some alphabet B and σ is a substitution from A^* into B^*.

Proposition 3.3. *Let $\mathbf{V}$ be a variety of finite ordered monoids and $\mathcal{V}$ the corresponding positive variety of languages. Then $\Sigma^+\mathcal{V}$ is a positive variety of languages that corresponds to $\mathbf{P}^+\mathbf{V}$. In particular, $\Sigma^+\mathcal{V} = \Lambda^+\mathcal{V}$.*

3.3 The shuffle operation

Power monoids also make an important tool to study the shuffle product, due to the following result.

Proposition 3.4. *Let L_1 and L_2 be two languages of A^*, recognized respectively by the ordered monoids M_1 and M_2. Then $L_1 ш L_2$ is recognized by the ordered monoid $\mathcal{P}^+(M_1 \times M_2)$.*

A [positive] variety of languages $\mathcal{V}$ is *closed under shuffle* if the shuffle product of two languages of $\mathcal{V}$ is also in $\mathcal{V}$. It is closed under length preserving morphisms if $\Lambda^+\mathcal{V} = \mathcal{V}$ and it is closed under inverse of substitutions if $\Sigma^+\mathcal{V} = \mathcal{V}$. As a consequence of Propositions 3.2, 3.3 and 3.4, we get the following result.

Proposition 3.5.

(1) *If a positive variety of languages is closed under length preserving morphisms, then it is closed under inverse of substitutions and under shuffle.*
(2) *If a positive variety of languages is closed under inverse of substitutions, then it is closed under length preserving morphisms and under shuffle.*

One may wonder whether a positive variety of languages is closed under length preserving morphisms if and only if it is closed under shuffle. This result holds for varieties of languages but depends on the classification of varieties closed under shuffle. It is still an open problem for positive varieties of languages.

It is easy to see that the variety of all commutative languages is closed under shuffle. Actually, the commutative varieties of languages closed under shuffle were characterised by Perrot [12]: they correspond to the varieties of commutative monoids whose groups belong to a given variety of commutative groups. Perrot also conjectured that the only non commutative variety of languages closed under shuffle was the variety of all regular languages, a result that was finally proved in 1998 by Esik and Simon [10]. Therefore the variety of commutative languages is the largest proper variety of languages closed under shuffle. This completes the classification of the varieties of languages closed under shuffle.

Classifying the positive varieties closed under shuffle seems to be a really challenging problem on which only partial results are known [4, 7]. A first question is to know whether the result of Esik and Simon also holds for positive varieties: in other words, is there a largest proper positive variety closed under shuffle? This question was solved positively by the authors in [7].

Theorem 3.6. *There is a largest proper positive variety of languages closed under shuffle.*

This positive variety, denoted by $\mathcal{W}$ in the sequel, enjoys a number of interesting properties which are detailed in the next section.

4 A robust class of languages

We start with a characterization of $\mathcal{W}$ in terms of languages, also given in [7]. The difficult part is to prove the existence of a largest positive variety of languages satisfying the condition of the theorem.

Theorem 4.1. *The positive variety $\mathcal{W}$ is the largest positive variety of languages such that, for $A = \{a, b\}$, the language $(ab)^*$ does not belong to $\mathcal{W}(A^*)$.*

Let us denote by $\mathbf{W}$ the variety of finite ordered monoids corresponding to $\mathcal{W}$. Theorem 4.1 can be translated immediately as follows:

Theorem 4.2. *The variety of finite ordered monoids $\mathbf{W}$ is the largest variety of finite ordered monoids not containing the ordered monoid B_2^{1-}.*

These characterizations are useful to prove that a language is not in $\mathcal{W}$. For instance, let $A = \{a, b\}$. We claim that the language $L = (aab)^* \cup A^*b(aa)^*abA^*$ is not in $\mathcal{W}(A^*)$. Assume the contrary and let $\varphi : A^* \to A^*$ be the morphism defined by $\varphi(a) = aa$ and $\varphi(b) = b$. Then since a positive variety of languages is closed under inverse of morphisms, the language $\varphi^{-1}(L) = (ab)^*$ belongs to $\mathcal{W}(A^*)$, a contradiction with Theorem 4.1.

Theorems 4.1 and 4.2 are simple to state but they do not provide any algorithm to decide whether a given regular language belongs to $\mathcal{W}$ or, equivalently, whether a given finite ordered monoid belongs to $\mathbf{W}$. A solution to this problem was given in [7].

Theorem 4.3. *A finite ordered monoid M belongs to $\mathbf{W}$ if and only if, for any pair (s, t) of mutually inverse elements of M, and any element z of the minimal ideal of the submonoid of M generated by s and t, $(stzst)^\omega \leqslant st$.*

Other equational descriptions are given in [7]. We now give a new formulation of Theorem 4.3 that is closer to automata theory. Before stating this result precisely, let us introduce some terminology.

Consider a deterministic automaton $\mathcal{A} = (Q, A, \cdot, i, F)$, a state p of Q and two words u and v of A^*. Let us say that u and v are *mutually inverse in $\mathcal{A}$* if, for every state p, $p\cdot uvu = p\cdot u$ and $p\cdot vuv = p\cdot v$. This is clearly equivalent to saying that u and v define two mutually inverse transformations in the transformation monoid of $\mathcal{A}$.

We are interested in the graph $G(p, u, v)$ whose vertices are the states of the form $p\cdot z$, where $z \in \{u, v\}^*$ and the edges are of the form $q \to q\cdot u$ and $q \to q\cdot v$. As in any directed graph, the states of $G(p, u, v)$ are partially ordered by the reachability relation. To avoid any confusion with the syntactic order on Q, we will say that a state q_2 *is deeper that a state* q_1 if there is path from q_1 to q_2. Our new result can now be formulated as follows.

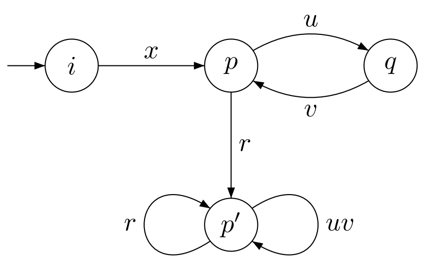
Theorem 4.4. *Let L be a regular language of A^*, let $\mathcal{A} = (Q, A, \cdot, i, F)$ be its minimal ordered automaton. Then L does not belong to $\mathcal{W}(A^*)$ if and only if there exist two states p and q of Q, two words u and v of A^*, mutually inverse in $\mathcal{A}$ such that $p \cdot u = q$, $q \cdot v = p$, a deepest state p' of the graph $G(p, u, v)$ and a word $r \in \{u, v\}^*$ such that $p \cdot r = p' \cdot r = p' \cdot uv = p'$ and $p' \not\leqslant p$ in the syntactic order on Q.*

Proof. Note that one may have $q = p$, but the condition $p' \not\leqslant p$ implies that p' is different from p. Let us denote by $(M, \leqslant)$ the syntactic ordered monoid of L and by $\eta : A^* \to M$ its syntactic morphism. Let ω be the exponent of M.

First assume that L does not belong to $\mathcal{W}(A^*)$. According to Theorem 4.3, there is a pair (s, t) of mutually inverse elements of M, generating a submonoid N of M and an element z of the minimal ideal of N such that $(stzst)^\omega \not\leqslant st$. Let us fix two words $u, v \in A^*$ such that $\eta(u) = s$ and $\eta(v) = t$. Then u and v are by construction mutually inverse in $\mathcal{A}$. Since z belongs to N, there is also a word $w \in \{u, v\}^*$ such that $\eta(w) = z$. The condition $(stzst)^\omega \not\leqslant st$ implies that there exist two words $x, y \in A^*$ such that

$$xuvy \in L \quad \text{and} \quad x(uvwuv)^\omega y \notin L \tag{1}$$

Let us set $r = (uvwuv)^\omega$, $q = i \cdot xu$, $p = q \cdot v$ and $p' = p \cdot r$. Since s and t are mutually inverse, the words u and uvu define the same transformation on Q and in particular, $p \cdot u = i \cdot xuvu = i \cdot xu = q$. Further $p' \cdot r = p \cdot rr = p \cdot r = p'$ and $p' \cdot uv = p \cdot (uvwuv)^\omega uv = p \cdot (uvwuv)^\omega = p'$ since r and uv define idempotent transformations on Q.



We claim that p' is a deepest state of the graph $G(p, u, v)$. Indeed, consider a state reachable from p', say $q' = p' \cdot f$ for some $f \in \{u, v\}^*$. Since $\eta(r)$ is an idempotent of the minimal ideal of N, one has $\eta((rfr)^\omega) = \eta(r)$. Since $p' \cdot r = p'$, it follows that $p' = p' \cdot r = p' \cdot (rfr)^\omega = q' \cdot r(rfr)^{\omega - 1}$ and thus p' is reachable from q', which proves the claim.

Finally, it follows from (1) that $i \cdot xuvy \in F$ and $i \cdot x(uvwuv)^\omega y \notin F$, whence $p \cdot y \in F$ and $p' \cdot y \notin F$. Therefore $p' \not\leqslant p$ and the condition on $\mathcal{A}$ is satisfied.

Suppose now that the condition on $\mathcal{A}$ is satisfied. Since $\mathcal{A}$ is minimal, each state of Q is accessible and there exists a word x such that $i \cdot x = p$. Set $s = \eta(u)$

and $t = \eta(v)$. Then s and t are two mutually inverse elements of M which generate a submonoid N of M. Let I be the minimal ideal of N and let f be a word of $\{u, v\}^*$ such that $\eta(f)$ belongs to I. Since p' is a deepest state of $G(u, v)$, the state p' can be reached from $p' \cdot f$ and hence there is a word $g \in \{u, v\}^*$ such that $p' \cdot fg = p'$. Setting $w = rfg$, we get $p' \cdot w = p' \cdot rfg = p' \cdot fg = p'$. Therefore $p' = p' \cdot r = p' \cdot fg = p' \cdot uv$ and thus we obtain

$$i \cdot xuv = p \quad \text{and} \quad i \cdot x(uvwuv)^\omega = i \cdot x(uvrfguv)^\omega = p' \tag{2}$$

Now, since $p' \not\leqslant p$, there exists a word y such that $p \cdot y \in F$ but $p' \cdot y \notin F$. Consequently, it follows from (2) that $i \cdot xuvy \in F$ but $i \cdot x(uvwuv)^\omega y \notin F$, that is, $xuvy \in L$ but $x(uvwuv)^\omega y \notin L$. Setting $z = \eta(w)$, we get $(uvzuv)^\omega \not\leqslant uv$. Further, since $\eta(f) \in I$ and $z = \eta(r)\eta(f)\eta(g)$, z also belongs to I. Thus by Theorem 4.3, L does not belong to $\mathcal{W}(A^*)$. $\square$

For instance, let us come back to Examples 1.1 and 1.2. If $\mathcal{A}$ is the minimal automaton of $(ab)^*$ represented in Figure 1, one can take $p = 1$, $q = 2$, $p' = 0$, $u = a$, $v = b$ and $r = a$ to verify that $\mathcal{A}$ satisfies the conditions of Theorem 4.4. Thus $(ab)^*$ is not in $\mathcal{W}(A^*)$.

On the other hand, one can verify that the minimal automaton of $(ab)^* \cup A^*aaA^*$ represented in Figure 2 does not satisfy the conditions of Theorem 4.4. Thus $(ab)^* \cup A^*aaA^*$ belongs to $\mathcal{W}(A^*)$.

Note that the condition that u and v are mutually inverse in $\mathcal{A}$ is mandatory. Consider for instance the minimal automaton of the language $(ab)^* \cup (ab)^*bA^* \cup (ab)^*aabA^*$ on the alphabet $\{a, b\}$, represented in Figure 4. The order on the set of states is $3 < 1 < 4 < 0$ and $3 < 2 < 0$.

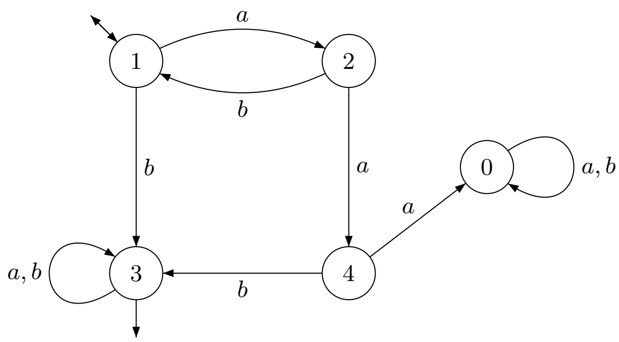


Figure 4. The minimal automaton of $(ab)^* \cup (ab)^*bA^* \cup (ab)^*aabA^*$.

Setting $p = 1$, $q = 2$, $p' = 0$ and $r = a^3$, one has $p \cdot a = q$, $q \cdot b = p$, $p \cdot r = p' \cdot r = p' \cdot uv = p'$ and $p' \not\leqslant p$. Further, $r \in \{a, b\}^*$ and p' is a deepest state in the graph $G(a, b)$. However, a and b are not mutually inverse and one can actually verify that $\mathcal{A}$ does not satisfy the conditions of Theorem 4.4. In particular, taking $u = aba$ and $v = b$ does not work, since there is no word $r \in \{u, v\}^*$ such that $p \cdot r' = p'$. Thus L belongs to $\mathcal{W}(A^*)$.

A key property of $\mathbf{W}$, also proved in [7], is stated in the next theorem

Theorem 4.5. *The equality* $\mathbf{W} = \mathbf{P}^+\mathbf{W}$ *holds.*

Propositions 3.2, 3.3 and 3.5 now give immediately:

Corollary 4.6. *The positive variety* $\mathcal{W}$ *is closed under length preserving morphisms, inverse of substitutions and shuffle.*

In fact, a stronger property holds [7].

Theorem 4.7.

(1) *The positive variety* $\mathcal{W}$ *is the largest proper positive variety of languages closed under length preserving morphisms.*
(2) *The positive variety* $\mathcal{W}$ *is the largest proper positive variety of languages closed under inverse of substitutions.*
(3) *The positive variety* $\mathcal{W}$ *is the largest proper positive variety of languages closed under shuffle.*

Let us mention another important closure property of $\mathcal{W}$.

Proposition 4.8. *The positive variety* $\mathcal{W}$ *is closed under product.*

Proof. It suffices to use a standard trick to simulate a concatenation product by a shuffle product. Let L_1 and L_2 be two languages of $\mathcal{W}(A^*)$. Let $\bar{A} = \{\bar{a} \mid a \in A\}$ be a copy of A and let π_A and $\pi_{\bar{A}}$ be the morphisms from $(A \cup \bar{A})^*$ onto A^* defined by $\pi_A(a) = \pi_{\bar{A}}(\bar{a}) = a$ and $\pi_A(\bar{a}) = \pi_{\bar{A}}(a) = 1$ for all $\bar{a} \in A$. Consider the two languages of $(A \cup \bar{A})^*$

$$K_1 = \pi_A^{-1}(L_1) \cap A^* \qquad K_2 = \pi_{\bar{A}}^{-1}(L_2) \cap \bar{A}^*$$

Thus K_1 is just the same language as L_1, but on a larger alphabet, and K_2 is a copy of L_2. Finally, let

$$K = (K_1 \text{ Ш } K_2) \cap A^*\bar{A}^*$$

Since $\mathcal{W}$ is closed under intersection, inverse of morphisms and shuffle and since A^*, $\bar{A}^*$ and $A^*\bar{A}^*$ are languages of $\mathcal{W}((A \cup \bar{A})^*)$, one gets $K \in \mathcal{W}((A \cup \bar{A})^*)$. Finally let $\pi : (A \cup \bar{A})^* \to A^*$ be the morphism defined by $\pi(\bar{a}) = \pi(a) = a$. Now $\pi(K) = L_1L_2$ and since $\mathcal{W}$ is closed under length preserving morphisms, $L_1L_2 \in \mathcal{W}(A^*)$. $\square$

Note, however, that $\mathcal{W}$ is not the largest proper positive variety of languages closed under product. Indeed the variety of star-free languages is closed under product, but contains $(ab)^*$.

5 Closure under commutation and partial commutation

The class $\mathcal{W}$ also occurs in the study of commutation relations.

Let A be an alphabet and let I be a symmetric and irreflexive relation on A (often called the *independence relation*). We denote by $\sim_I$ the congruence on A^* generated by the set $\{ab = ba \mid (a,b) \in I\}$. If L is a language on A^*, we also denote by $[L]_I$ the closure of L under $\sim_I$. When I is the relation $\{(a,b) \in A \times A \mid a \neq b\}$, we simplify the notation to $\sim$ and $[L]$, respectively. Thus $\sim$ is the commutation relation and $[L]$ is the *commutative closure* of L. A class $\mathcal{C}$ of languages is *closed under I-commutation* if $L \in \mathcal{C}$ implies $[L]_I \in \mathcal{C}$. It is *closed under commutation* if $L \in \mathcal{C}$ implies $[L] \in \mathcal{C}$.

Since the commutative closure of the language $(ab)^*$ is nonregular, a class of regular languages closed under commutation cannot contain $(ab)^*$. What happens for varieties and positive varieties of languages? One can show that there is a largest variety of languages $\mathcal{V}$ such that, for $A = \{a,b\}$, the language $(ab)^*$ does not belong to $\mathcal{V}(A^*)$. It is denoted by $\mathcal{DS}$ since the corresponding variety of finite monoids is the variety $\mathbf{DS}$. Recall that a finite monoid belongs to $\mathbf{DS}$ are if each of its regular $\mathcal{D}$-classes form a semigroup. In fact, one can show that $\mathcal{DS}$ is also the largest variety of languages closed under commutation. The corresponding result for positive varieties states that $\mathcal{W}$ is the largest positive variety of languages closed under commutation. Actually, a stronger result holds [5]. Define the *period* (respectively *exponent*) of a regular language as the period (respectively exponent) of its syntactic monoid.

Theorem 5.1. *Let L be a language of $\mathcal{W}(A^*)$. Then $[L]$ is regular and commutative (and hence belongs to $\mathcal{W}(A^*)$) and its period divides that of L.*

For partial commutations, a weaker result holds if I is transitive [5]. Recall that in this case, $A^*/{\sim_I}$ is a free product of free commutative monoids.

Theorem 5.2. *Let L be a language of $\mathcal{W}(A^*)$ and let I be a transitive independence relation. Then $[L]_I$ is a regular language.*

Although we know that $[L]_I$ is regular in this case, we don't know whether $[L]_I$ necessarily belongs to $\mathcal{W}(A^*)$.

6 Conclusion and open questions

We have seen that the class $\mathcal{W}$ is closed under the following operations: union, intersection, product, shuffle, left and right quotients, inverse of morphisms, length preserving morphisms and commutative closure. It is a decidable variety and the corresponding variety of finite ordered monoids $\mathbf{W}$ is precisely known. The positive variety $\mathcal{W}$ can be defined alternatively as the largest proper positive variety of languages satisfying (1) [(2), (3), (4)]:

(1) not containing the language $(ab)^*$;

(2) closed under shuffle;

(3) closed under length preserving morphisms;
(4) closed under inverse of substitutions.

Despite these numerous closure properties, we don't know of any constructive description of $\mathcal{W}$, similar to the definition of the star-free languages. For instance, the least positive variety of languages satisfying Conditions (1)-(4) is the variety of polynomials of group languages, which is strictly contained in $\mathcal{W}$. Is it possible to find more powerful operators to generate the languages of $\mathcal{W}$? We let this question as a research problem for the reader.

Another research problem is to find a logical description for $\mathcal{W}$. The fact that $\mathbf{W}$ contains all finite groups and even $\mathbf{DS}$ might be a problem, since no logical description is available for the corresponding subvarieties of $\mathcal{W}$.

Finally, it would be nice to have an evocative name for $\mathcal{W}$ and the authors would appreciate any motivated suggestion...

References

1. J. Almeida, *Finite semigroups and universal algebra. Series in Algebra*, vol. 3, World Scientific, Singapore, 1994.
2. J. Almeida and P. Weil, Relatively free profinite monoids: an introduction and examples, in *NATO Advanced Study Institute Semigroups, Formal Languages and Groups*, J. Fountain (éd.), pp. 73–117, Kluwer Academic Publishers, 1995.
3. A. Bouajjani, A. Muscholl and T. Touili, Permutation Rewriting and Algorithmic Verification, *Information and Computation* **205**,2 (2007), 199–224.
4. A. Cano Gómez, *Semigroupes ordonnés et opérations sur les langages rationnels*, PhD thesis, Université Paris 7 and Departamento de Sistemas Informáticos y Computación, Universidad Politécnica de Valencia, 2003.
5. A. Cano Gómez, G. Guaiana and J.-E. Pin, When does partial commutative closure preserve regularity?, in *35th ICALP*, Berlin, 2008, p. to appear, *Lect. Notes Comp. Sci.*, Springer.
6. A. Cano Gómez and J.-E. Pin, On a conjecture of Schnoebelen, in *DLT 2003*, Z. Ésik and Z. Fülöp (éd.), Berlin, 2003, pp. 35–54, *Lect. Notes Comp. Sci.* n° 2710, Springer.
7. A. Cano Gómez and J.-É. Pin, Shuffle on positive varieties of languages, *Theoret. Comput. Sci.* **312** (2004), 433–461.
8. S. Eilenberg, *Automata, Languages and Machines*, vol. B, Academic Press, New York, 1976.
9. Z. Ésik, Extended temporal logic on finite words and wreath products of monoids with distinguished generators, in *DLT 2002, Kyoto, Japan*, Ito, Masami et al. (éd.), Berlin, 2002, pp. 43–58, *Lect. Notes Comp. Sci.* n° 2450, Springer.
10. Z. Ésik and I. Simon, Modeling Literal Morphisms by Shuffle, *Semigroup Forum* **56** (1998), 225–227.
11. M. Gehrke, S. Grigorieff and J.-E. Pin, Duality and equational theory of regular languages, in *35th ICALP*, Berlin, 2008, p. to appear, *Lect. Notes Comp. Sci.*, Springer.
12. J.-F. Perrot, Variétés de langages et operations, *Theoret. Comput. Sci.* **7** (1978), 197–210.
13. J.-E. Pin, *Varieties of formal languages*, North Oxford, London and Plenum, New-York, 1986. (Translation of *Variétés de langages formels*, Masson, 1984).

14. J.-E. Pin, Finite semigroups and recognizable languages: an introduction, in *NATO Advanced Study Institute Semigroups, Formal Languages and Groups*, J. Fountain (éd.), pp. 1–32, Kluwer academic publishers, 1995.
15. J.-E. Pin, A variety theorem without complementation, *Russian Mathematics (Izvestija vuzov.Matematika)* **39** (1995), 80–90.
16. J.-E. Pin, Syntactic semigroups, in *Handbook of formal languages*, G. Rozenberg and A. Salomaa (éd.), vol. 1, ch. 10, pp. 679–746, Springer, 1997.
17. J.-E. Pin and P. Weil, A Reiterman theorem for pseudovarieties of of finite first-order structures, *Algebra Universalis* **35** (1996), 577–595.
18. J.-E. Pin and P. Weil, Semidirect products of ordered semigroups, *Communications in Algebra* **30** (2002), 149–169.
19. L. Polák, Operators on classes of regular languages, in *Semigroups, Algorithms, Automata and Languages (Coimbra, 2001)*, G. Gomes, J.-E. Pin and P. Silva (éd.), pp. 407–422, World Scientific Publ., River Edge, NJ, 2002.
20. J. Reiterman, The Birkhoff theorem for finite algebras, *Algebra Universalis* **14** (1982), 1–10.
21. C. Reutenauer, Sur les variétés de langages et de monoïdes, in *Theoretical computer science (Fourth GI Conf., Aachen)*, vol. 67, pp. 260–265, Springer-Verlag, Berlin, 1979.
22. H. Straubing, Recognizable Sets and Power Sets of Finite Semigroups, *Semigroup Forum* **18** (1979), 331–340.
23. H. Straubing, On logical descriptions of regular languages, in *LATIN 2002*, Berlin, 2002, pp. 528–538, *Lect. Notes Comp. Sci.* n° 2286, Springer.