MPRI, Fondations mathématiques de la théorie des automates

Olivier Carton, Jean-Éric Pin

Examen du 3 mars 2014. Durée: 2h 30, notes de cours autorisées

⋆ ⋆ ⋆

> **Avertissement :** On attachera une grande importance à la clarté, à la précision et à la concision de la rédaction.

Tous les langages intervenant dans ce problème sont reconnaissables. On se propose d'étudier les langages satisfaisant les équations profinies suivantes:
(E$_1$) $(xy)^\omega = (yx)^\omega$ pour tout $x, y \in A^*$,
(E$_2$) $x^\omega y x^\omega = x^\omega y x^\omega y x^\omega$ pour tout $x, y \in A^+$,
(E$_3$) $x^\omega y^\omega = y^\omega x^\omega$ pour tout $x, y \in A^*$,
On notera que dans (E2), on impose que x soit un mot non vide.

Dans les deux premières parties, on examine quelques exemples de langages. Les parties (3) et (4) sont indépendantes.

1. Généralités

Soit L un langage reconnaissable de A^* et soit M son monoïde syntactique.

Question 1. Montrer que L vérifie (E3) si et seulement si les idempotents de M commutent.

Question 2. Montrer que si L vérifie (E2), alors M est apériodique. Montrer par un exemple que la réciproque n'est pas vraie.

Question 3. Montrer que si L vérifie (E1) et (E2), alors L est testable par morceaux.

2. Un exemple

On considère sur l'alphabet $A = \{a, b\}$ le langage $L = (a^2)^* b (a^2)^* b$.

Question 4. Calculer l'automate minimal de L.

Question 5. Calculer le monoïde syntactique M de L (on trouvera 12 éléments et 6 $\mathcal{J}$-classes).

Question 6. Quels sont les idempotents de M?

Question 7. Déterminer la structure en $\mathcal{D}$-classes de M.

Question 8. Est-ce que L vérifie (E1)? (E2)? (E3)? (Justifier vos réponses).

3. S-langages

On appelle *S-langage* un langage de la forme

$$B_0^* a_1 B_1^* a_2 \cdots B_{n-1}^* a_n B_n^*$$

avec $B_0, ..., B_n \subseteq A$, $B_i \cap B_j = \emptyset$ pour $i \neq j$ et $a_i \in A - (B_{i-1} \cup B_i)$ pour $1 \leqslant i \leqslant n$. On notera que les B_i peuvent être vides. On note $\mathcal{B}$ l'algèbre de Boole engendrée par les S-langages.

Question 9. Dessiner sommairement l'automate minimal $\mathcal{A} = (Q, A, \cdot, q_0, F)$ d'un S-langage. Montrez qu'un S-langage est testable par morceaux.

Question 10. On note 0 l'état puits de $\mathcal{A}$. Montrer que pour tout $p, q \in Q$ et tout $a \in A$, $p\cdot a = q\cdot a \neq 0$ entraîne $p = q$.

Question 11. Montrer qu'un S-langage vérifie (E3).

Question 12. Montrer que tout langage de $\mathcal{B}$ vérifie (E1), (E2) et (E3).

Question 13. [Vraiment difficile] Montrer que tout langage vérifiant (E1), (E2) et (E3) appartient à $\mathcal{B}$.

4. Un peu d'algèbre...

Soit S un semigroupe fini et soit $E(S)$ l'ensemble de ses idempotents. On dit que deux éléments s et t sont *conjugués* s'il existe $u, v \in S^1$ tels que $uv = s$ et $vu = t$.

Question 14. Montrer que deux idempotents sont conjugués si et seulement si ils sont $\mathcal{J}$-équivalents.

Question 15. Soient $x, y \in S$. Montrer que $(xy)^\omega$ et $(yx)^\omega$ sont conjugués.

Question 16. Montrer l'équivalence des conditions suivantes:
(1) pour tout $x, y \in S$, $(xy)^\omega = (yx)^\omega$,
(2) si xy et yx sont idempotents, alors $xy = yx$,
(3) chaque $\mathcal{J}$-classe régulière de S est un groupe,
(4) si $e \in E(S)$ et $e \mathrel{\mathcal{J}} x$, alors $ex = xe$.

On suppose que S vérifie les conditions équivalentes de la question précédente.

Question 17. Montrer que pout tout $x, y \in S$, $(xy)^\omega x = x(xy)^\omega$

Question 18. Montrer que pout tout $x, y \in S$, $(x^\omega y^\omega)^\omega x = x(x^\omega y^\omega)^\omega$.

Question 19. Montrer que pout tout $x, y \in S$, $(xy)^\omega = (x^\omega y^\omega)^\omega$.

Question 20. Montrer que l'ensemble $E(S)$, muni de l'opération $*$ définie par $e * f = (ef)^\omega$, est un semigroupe idempotent et commutatif.

Question 21. Montrer que l'application π defined by $\pi(x) = x^\omega$ définit un morphisme surjectif de semigroupe de S sur $(E(S), *)$.

MPRI, Mathematical foundations of automata theory

Olivier Carton, Jean-Éric Pin

March 3, 2014. Duration: 2h 30.

⋆ ⋆ ⋆

Warning : Clearness, accuracy and concision of the writing will be rewarded.

In this problem, all the languages are supposed to be recognizable. The aim of this problem is to study the languages satisfying the following profinite equations:
(E$_1$) $(xy)^\omega = (yx)^\omega$ pour tout $x, y \in A^*$,
(E$_2$) $x^\omega y x^\omega = x^\omega y x^\omega y x^\omega$ pour tout $x, y \in A^+$,
(E$_3$) $x^\omega y^\omega = y^\omega x^\omega$ pour tout $x, y \in A^*$,
Observe that in (E2), it is required that x be a nonempty word.

In the first two parts, we consider a few examples of languages. Parts (3) and (4) are independent.

1. General results

Let L be a recognizable language of A^* and let M be its syntactic monoid.

Question 1. Prove that L satisfies (E3) if and only if the idempotents of M commute.

Question 2. Prove that if L satisfies (E2), then M is aperiodic. Give a counterexample to the converse statement.

Question 3. Prove that if L satisfies (E1) and (E2), then L is piecewise testable.

2. An example

Let $A = \{a, b\}$ and $L = (a^2)^* b (a^2)^* b$.

Question 4. Give the minimal automaton of L.

Question 5. Compute the syntactic monoid M of L (you should find 12 elements and 6 $\mathcal{J}$-classes).

Question 6. Give the idempotents of M?

Question 7. Give the $\mathcal{J}$-class structure of M.

Question 8. Does L satisfy (E1)? (E2)? (E3)? (Justify your answers).

3. S-languages

An *S-language* is a language of the form

$$B_0^* a_1 B_1^* a_2 \cdots B_{n-1}^* a_n B_n^*$$

where $B_0, ..., B_n \subseteq A$, $B_i \cap B_j = \emptyset$ for $i \neq j$ and $a_i \in A - (B_{i-1} \cup B_i)$ for $1 \leqslant i \leqslant n$. Note that the sets B_i might be empty. Let $\mathcal{B}$ be the Boolean algebra generated by the S-languages.

Question 9. Roughly draw the minimal automaton $\mathcal{A} = (Q, A, \cdot, q_0, F)$ of a S-language. Prove that a S-language is piecewise testable.

Question 10. Let us denote by 0 the sink state of $\mathcal{A}$. Show that for all $p, q \in Q$ and all $a \in A$, $p\cdot a = q\cdot a \neq 0$ implies $p = q$.

Question 11. Show that a S-language satisfies (E3).

Question 12. Prove that every language of $\mathcal{B}$ satisfies (E1), (E2) and (E3).

Question 13. [Very difficult] Show that a language satisfying (E1), (E2) and (E3) belongs to $\mathcal{B}$.

4. A little bit of algebra...

Let S be a finite semigroup and let $E(S)$ be its set of idempotents. Two elements s and t are said to be *conjugate* if there exist $u, v \in S^1$ such that $uv = s$ and $vu = t$.

Question 14. Show that two idempotents are conjugate if and only if they are $\mathcal{J}$-equivalent.

Question 15. Let $x, y \in S$. Show that $(xy)^\omega$ and $(yx)^\omega$ are conjugate.

Question 16. Show that the following conditions are equivalent:

(1) for all $x, y \in S$, $(xy)^\omega = (yx)^\omega$,

(2) if xy and yx are idempotent, then $xy = yx$,

(3) each regular $\mathcal{J}$-class of S is a group,

(4) if $e \in E(S)$ and $e \mathrel{\mathcal{J}} x$, then $ex = xe$.

Suppose now that S satisfies the equivalent conditions of the previous question.

Question 17. Show that for all $x, y \in S$, $(xy)^\omega x = x(xy)^\omega$

Question 18. Show that for all $x, y \in S$, $(x^\omega y^\omega)^\omega x = x(x^\omega y^\omega)^\omega$.

Question 19. Show that for all $x, y \in S$, $(xy)^\omega = (x^\omega y^\omega)^\omega$.

Question 20. Show that the set $E(S)$, equipped with the operation $*$ defined by $e * f = (ef)^\omega$, is an idempotent and commutative semigroup.

Question 21. Show that the map π defined by $\pi(x) = x^\omega$ induces a surjective semigroup morphism from S onto $(E(S), *)$.

Solution

1. General results

Let $\eta : A^* \to M$ be the syntactic morphism of L and let $\widehat{\eta} : \widehat{A^*} \to M$ be its continuous extension.

Question 1. Follows from the fact that for every $e \in E(M)$, there is an $x \in A^*$ such that $\widehat{\eta}(x^\omega) = e$. Thus $x^\omega y^\omega = y^\omega x^\omega$ just means that the idempotents commute in M.

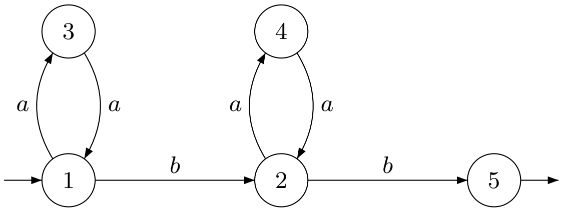
Question 2. Taking $y = x$ in (E2) yields $x^\omega x x^\omega x x^\omega = x^\omega x x^\omega$, that is $x^{\omega+2} = x^{\omega+1}$. Multiplying by $x^{\omega-1}$ yields $x^{\omega+1} = x^\omega$. It follows that M is aperiodic.

Question 3. The equations (E1) and $x^{\omega+1} = x^\omega$ define the variety of $\mathcal{J}$-trivial monoids. Thus M is $\mathcal{J}$-trivial and L is piecewise testable by Simon's theorem.

2. An example

Let $A = \{a, b\}$ and $L = (a^2)^*b(a^2)^*b$.

Question 4. The minimal automaton of L is



Question 5. Here is the syntactic monoid of L

	1	2	3	4	5
$*\ 1$	1	2	3	4	5
a	3	4	1	2	0
b	2	5	0	0	0
$*\ a^2$	1	2	3	4	0
ab	0	0	2	5	0
ba	4	0	0	0	0
b^2	5	0	0	0	0
aba	0	0	4	0	0
ab^2	0	0	5	0	0
ba^2	2	0	0	0	0
$*\ bab$	0	0	0	0	0
aba^2	0	0	2	0	0

Relations:

$$a^3 = a \qquad a^2b = b \qquad b^2a = 0 \qquad b^3 = 0 \qquad bab = 0$$

Question 6. Idempotents:

$$E(S) = \{1, a^2, bab\}$$

Question 7. $\mathcal{J}$-class structure:

^{*1}

$^*a^2 \quad a$

b
ab

b^2
ab^2

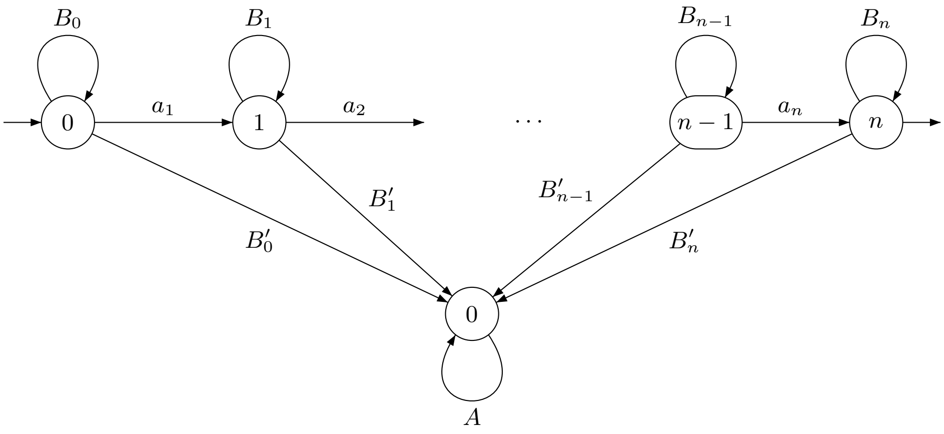
ba^2	ba
aba^2	aba

$^*bab$

Question 8. L satisfies (E3) since the idempotent commute. It does not satisfy (E2) since M is not aperiodic. It also satisfies (E2). Indeed, $(xy)^\omega$ and $(yx)^\omega$ are two conjugated idempotents and thus belong to the same $\mathcal{J}$-class. But each $\mathcal{J}$-class contains a unique idempotent.

3. S-languages

Question 9. Setting $B'_i = A - B_i$, the minimal automaton of a S-language L looks like this:



Now since $a_i \notin B_{i-1}$ for $1 \leqslant i \leqslant n$, it follows from Proposition IX.1.13 that the syntactic monoid of a S-language is $\mathcal{R}$-trivial. Now since $a_i \notin B_i$ for $1 \leqslant i \leqslant n$, the same argument can be applied to the reverse of the language. It follows that the syntactic monoid of a S-language is $\mathcal{L}$-trivial and hence $\mathcal{J}$-trivial. Now by Simon's theorem, a S-language is piecewise testable.

Question 10. Suppose that $p \cdot a = q \cdot a \neq 0$. Thus we get $q \cdot a = q$, whence $a \in B_q$, a contradiction.

Question 11. It follows from the previous question that the nonzero transitions of $\mathcal{A}$ are injective. It follows that the idempotents are partial identities and they commute. Therefore every S-language satisfies (E3).

Question 12. It suffices to prove that every S-language satisfies (E1), (E2) and (E3). It was just done before for (E3). Furthermore (E1) is satisfied by every piecewise testable language. Thus it just remains to show that every S-language satisfies (E2). Using the condition that the B_i's are pairwise disjoint, we observe that if x is nonempty, then $ux^\omega yx^\omega v \in L$, then all the letters of x and y are contained in some B_i. It follows that $ux^\omega yx^\omega yx^\omega v \in L$. A similar argument shows that $ux^\omega yx^\omega yx^\omega v \in L$ implies $ux^\omega yx^\omega v \in L$ and thus L satisfies the equation (E2).

Question 13. *Show that a language satisfying (E1), (E2) and (E3) belongs to $\mathcal{B}$.* See

C. Selmi, Strongly locally testable semigroups with commuting idempotents and related languages, *Theor. Inform. Appl.* **33**,1 (1999), 47–57.

4. A little bit of algebra...

This part was based on the following article:

D. M. Davenport, On power commutative semigroups, *Semigroup Forum* **44**,1 (1992), 9–20.

Let S be a finite semigroup and let $E(S)$ be its set of idempotents. Let us recall the definition of the naturel order on idempotents: if $e, f \in E(S)$, we set $e \leqslant f$ if $ef = fe = e$.

Question 14. See Proposition 2.22.

Question 15. Let $u = x$ and $v = y(xy)^{\omega-1}$. Then $(xy)^\omega = uv$ and $(yx)^\omega = vu$.

Question 16.

(1) ⇒ (2). If xy and yx are idempotent, then $(xy)^\omega = xy = yx = (yx)^\omega$.

(2) ⇒ (1) follows from question 15.

(1) ⇒ (3). Let J be a regular $\mathcal{J}$-class of S and let $e, f \in J$. Then e and f are conjugate by question 14, say $e = uv$ and $f = vu$. It follows by (1) that $e = uv = (uv)^\omega = (vu)^\omega = vu = f$. But a regular $\mathcal{J}$-class containing a unique idempotent is a group.

(3) ⇒ (1). Observe that $(xy)^\omega$ and $(yx)^\omega$ are $\mathcal{J}$-equivalent (since $(xy)^\omega = (xy)^{2\omega} = x(yx)^{\omega-1}y$ and similarly $(yx)^\omega = y(xy)^{\omega-1}x$. Since by (3) each $\mathcal{J}$-class of S is a group, these two idempotents are equal.

(3) ⇒ (4). Let J be the $\mathcal{J}$-class of e and x. By (3), it is in fact a group with identity e. Thus $ex = x = xe$.

(4) ⇒ (3). If $x \mathrel{\mathcal{R}} e$, then $ex = x$ and thus by (4), $xe = x$. It follows that $x \leqslant_{\mathcal{L}} e$ and since $x \mathrel{\mathcal{J}} e$, $e \mathrel{\mathcal{L}} x$ and finally $e \mathrel{\mathcal{H}} x$. In the same way, $x \mathrel{\mathcal{L}} e$ implies $e \mathrel{\mathcal{H}} x$. It follows that the $\mathcal{J}$-class of e reduces to an $\mathcal{H}$-class and hence is a group.

Question 17. Let J be the $\mathcal{J}$-class of $(xy)^\omega$. Observe that $(xy)^\omega x \mathrel{\mathcal{R}} (xy)^\omega$. Therefore $(xy)^\omega x$ beongs to J and commutes with $(xy)^\omega$ since J is a group. Furthermore $(xy)^\omega = (yx)^\omega$, and thus

$$(xy)^\omega x = (xy)^\omega (xy)^\omega x = (xy)^\omega x (xy)^\omega = x(yx)^\omega (xy)^\omega = x(xy)^\omega (xy)^\omega = x(xy)^\omega.$$

Question 18. In the same way, $(x^\omega y^\omega)^\omega x \mathrel{\mathcal{R}} (x^\omega y^\omega)^\omega$ and thus $(x^\omega y^\omega)^\omega x$ is in J and commutes with $(x^\omega y^\omega)^\omega$. Therefore

$$(x^\omega y^\omega)^\omega x = (x^\omega y^\omega)^\omega \big((x^\omega y^\omega)^\omega x\big) = \big((x^\omega y^\omega)^\omega x\big)(x^\omega y^\omega)^\omega = (x^\omega y^\omega)^\omega x(y^\omega x^\omega)^\omega \tag{1}$$

Since $x(y^\omega x^\omega)^\omega \mathrel{\mathcal{L}} (y^\omega x^\omega)^\omega$, we also have $x(y^\omega x^\omega)^\omega \in J$ and hence

$$(x^\omega y^\omega)^\omega x(y^\omega x^\omega)^\omega = x(y^\omega x^\omega)^\omega(x^\omega y^\omega)^\omega = x(x^\omega y^\omega)^\omega(x^\omega y^\omega)^\omega = x(x^\omega y^\omega)^\omega \tag{2}$$

Putting (1) and (2) together, we get $(x^\omega y^\omega)^\omega x = x(x^\omega y^\omega)^\omega$.

Question 19. Let $e = (xy)^\omega$ and let $u \in \{x, y\}^*$. We show by induction on $|u|$ that $eu = ue \mathrel{\mathcal{H}} e$. This is clear if $|u| = 0$. Suppose that the result holds for u. Then $eux = uex = uxe$. Furthermore since $e \mathrel{\mathcal{L}} eu$, we get $e \mathrel{\mathcal{L}} ex \mathrel{\mathcal{R}} eux$. Thus $e \mathrel{\mathcal{H}} eux$. A similar argument would show that $euy = uye \mathrel{\mathcal{H}} e$, which concludes the induction.

Setting $f = (x^\omega y^\omega)^\omega$, we get in particular $ef = fe \mathrel{\mathcal{H}} e$. Now a similar argument can be used to show that for all $u \in \{x, y\}^*$, $fu = uf \mathrel{\mathcal{H}} f$. This will give $ef = fe \mathrel{\mathcal{H}} f$, and thus $e = f$.

Question 20. Let $e, f, g \in E(S)$. One has $e * e = (ee)^\omega = e$ and $e * f = (ef)^\omega = (fe)^\omega = f * e$. Furthermore, $(e*f)*g = ((ef)^\omega g)^\omega = ((ef)^\omega g^\omega)^\omega = (efg)^\omega$ by Question 19. It follows that the set $E(S)$, equipped with the operation $*$ defined by $e * f = (ef)^\omega$, is an idempotent and commutative semigroup.

Question 21. One has $\pi(e) = e$ and thus π is surjective. Furthermore, we have by Question 19 $\pi(xy) = (xy)^\omega = (x^\omega y^\omega)^\omega = \pi(x) * \pi(y)$. Thus π is a surjective semigroup morphism from S onto $(E(S), *)$.