	ANNÉE UNIVERSITAIRE 2009/2010 1ÈRE SESSION DE PRINTEMPS	
	Parcours : CSB6 **Code UE :** INF253 **Corrigé de l'Épreuve :** Informatique Théorique 2 **Date :** 11 Mai 2010	

Exercice 1 [20 points]

$$L := (a+b)^*(a+c)(a+b+c)^2$$

1- L est reconnu par l'automate fini non-déterministe schématisé sur la figure 1.
Dans ce qui suit, les positions des lettres dans un mot u de longueur ℓ, sont les entiers de 0

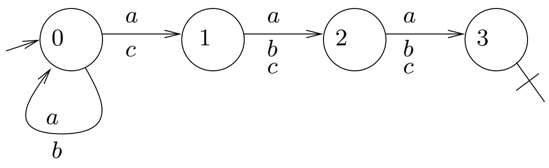

FIG. 1 – Un automate reconnaissant L

à $\ell - 1$.
2- Soient $u, u' \in \{a,b\}^3$ tels que $u \neq u'$.
Il existe $k \in [0,2]$ tel que

$$u[k] = a \Leftrightarrow u'[k] = b$$

Soit $\beta = a^k$. Alors

$$u \cdot \beta \in L \Leftrightarrow u' \cdot \beta \notin L$$

donc

$$\beta \in u^{-1}L \Leftrightarrow \beta \notin u'^{-1}L$$

ce qui montre que

$$u \not\equiv u'.$$

3- Soient $u, u' \in \{a,b,c\}^3, |u|_c = 0$ et $|u'|_c = 1$.
Soit $\beta = c^3$. Alors $u \cdot \beta \in L$ tandis que $u' \cdot \beta \notin L$ donc $\beta \in u^{-1}L$ tandis que $\beta \notin u'^{-1}L$ ce qui montre que

$$u \not\equiv u'.$$

4- Soient $u, u' \in \{a,b,c\}^3, |u|_c = 1, |u'|_c = 1$ et la position de la lettre c dans u et u' n'est pas la même.
Il existe $k, k' \in [0,2]$ tels que $u[k] = u'[k'] = c$ et $k \neq k'$.
Supposons, pour fixer les idées que $0 \leq k < k' \leq 2$. Soit $\beta = c^{k'}$.
Alors

$$u \cdot c^{k'} \quad \in \quad (a+b)^* c (a+b)^{2-k} c^{k'}$$

$$\begin{aligned} &\subseteq (a+b)^*c(a+b+c)^{2+(k'-k)} \\ &\subseteq (a+b)^*c(a+b+c)^3(a+b+c)^* \\ &\subseteq (a+b+c)^* \setminus L. \end{aligned}$$

$$\begin{aligned} u' \cdot c^{k'} &\in (a+b)^*c(a+b)^{2-k'}c^{k'} \\ &\subseteq (a+b)^*c(a+b+c)^2 \\ &\subseteq L \end{aligned}$$

Donc $\beta \notin u^{-1}L$ tandis que $\beta \in u'^{-1}L$, ce qui entraine que

$$u \not\equiv u'.$$

Si, au contraire, $k > k'$, par le même raisonnement, $u \cdot c^k \in L$ tandis que $u' \cdot c^k \notin L$, ce qui entraine aussi que

$$u \not\equiv u'.$$

5- Soient $u, u' \in \{a,b\}^k$ avec $0 \leq k \leq 2$ et $u \neq u'$.
Il existe $i \in [0,k]$ tel que

$$u[i] = a \Leftrightarrow u'[i] = b$$

Soit $\beta = a^i$. Alors

$$uca^{2-k} \cdot \beta \in L \Leftrightarrow u'ca^{2-k} \cdot \beta \notin L$$

donc

$$\beta \in (uca^{2-k})^{-1}L \Leftrightarrow \beta \notin (u'ca^{2-k})^{-1}L$$

ce qui montre que

$$uca^{2-k} \not\equiv u'ca^{2-k}.$$

6- $(cb^3)^{-1}L = \emptyset$.
7- Soient $u, u' \in R$ et $u \neq u'$. Il résulte des questions précédentes que, si $u, u' \in R$ et $u \neq u'$ alors $u \not\equiv u'$
8- L'affirmation

$$\forall u \in \{a,b,c\}^*, \exists u' \in R, u \equiv u'$$

est fausse : pour tout $u \in R$, $u^{-1}L \neq \emptyset$, donc le mot $u = cb^3$ n'a pas de représentant (modulo $\equiv$) dans R.
9- L'automate déterministe complet *minimal* de L a pour ensemble d'états $\mathbb{Q}(L)$. L'application $\varphi : X^* \to \mathbb{Q}(L)$ définie par

$$\varphi(u) = u^{-1}L$$

a pour image $\mathbb{Q}(L)$ et pour noyau l'équivalence $\equiv$. Elle induit une bijection $\bar{\varphi} : X^*/\equiv \to \mathbb{Q}(L)$.
Donc $\mathrm{Card}(\mathbb{Q}(L)) = \mathrm{Card}(X^*/\equiv)$.
Par ailleurs, de l'automate de la question 1, on déduit, par déterminisation, un automate déterministe complet reconnaissant L et possédant 2^4 états.
Donc $\mathrm{Card}(\mathbb{Q}(L)) \leq 2^4$ ce qui revient à $\mathrm{Card}(X^*/\equiv) \leq 2^4$.
10- Posons :

$$R' := R \cup \{cb^3\}.$$

Il vérifie bien :

$$\mathrm{Card}(R') = 2^4 \tag{1}$$

$$\forall u, u' \in R', u \neq u' \Rightarrow u \not\equiv u' \tag{2}$$

11- Par la propriété (2), l'application $u \mapsto [u]_\equiv$ est une injection de R' dans $X^*/\equiv$, donc

$$\mathrm{Card}(R') \leq \mathrm{Card}(X^*/\equiv).$$

ce qui, vu la majoration de la question 8 et la propriété (1) fournit :

$$2^4 = \mathrm{Card}(R') \leq \mathrm{Card}(X^*/\equiv) \leq 2^4.$$

Le nombre $\mathrm{Card}(X^*/\equiv)$, pris en sandwich entre 2^4 et 2^4, ne peut être que 2^4 en personne !
12-L'application $u \mapsto [u]_\equiv$ est une injection de R' dans $X^*/\equiv$ qui ont le même nombre (fini) d'éléments : cette application est donc une *bijection*, ce qui prouve que

$$\forall u \in \{a,b,c\}^*, \exists! u' \in R', u \equiv u'.$$

13- L'automate déterministe complet de L a comme ensemble d'états $\mathbb{Q}(L)$. Par la qu. 9, $\bar{\varphi} : \mathrm{Card}(X^*/\equiv) \to \mathbb{Q}(L)$ est une bijection. Donc l'automate déterministe complet de L a 2^4 états.
14- Le langage L_n est reconnu par l'automate fini non-déterministe à n états schématisé sur la figure 2.
15- Posons

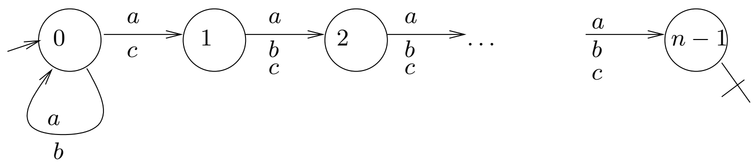

FIG. 2 – Un automate reconnaissant L_n

$$R'_n := \{a,b\}^{n-1} \cup \{uca^{n-2-k} \mid 0 \leq k \leq n-2, u \in \{a,b\}^k\} \cup \{cb^{n-1}\}$$

On démontre, par les arguments déjà utilisés dans les questions 2,3,4,5,6,7 que R'_n est un ensemble de mots sur lequel l'application $u \mapsto [u]_{\equiv_n}$ est injective. On calcule :

$$\mathrm{Card}(\{a,b\}^{n-1}) = 2^{n-1},\ \ \mathrm{Card}(\{uca^{n-2-k} \mid 0 \leq k \leq n-2, u \in \{a,b\}^k\}) = \sum_{k=0}^{n-2} 2^k = 2^{n-1} - 1,$$

et $\mathrm{Card}(\{cb^{n-1}) = 1$, d'où :

$$\mathrm{Card}(R'_n) = 2^{n-1} + (2^{n-1} - 1) + 1 = 2^n$$

Le nombre de classes de la relation d'équivalence $\equiv_n$ est supérieur ou égal à $\mathrm{Card}(R'_n) = 2^n$ (c.f. plus haut l'injection)
Par ailleurs, comme L_n est reconnu par un a.f. à n états (qu. 13), on sait que : le nombre de

classes de la relation d'équivalence $\equiv_n$ est inférieur ou égal à 2^n.
On conclut de ces deux inégalités que

$$\mathrm{Card}(X^*/\equiv_n) = 2^n.$$

16- L'automate déterministe complet minimal de L_n a donc 2^n états.
17- Soit $n \geq 0$. Tout automate fini à n états et ayant comme ensemble d'états finaux l'ensemble vide, reconnaît l'ensemble vide. Or le nombre de résiduels de l'ensemble vide vaut 1. Donc

$$\mathrm{dmin}(n) = 1.$$

On a vu en cours que tout automate fini à n états est équivalent à un automate déterministe complet qui possède 2^n états, donc $\mathrm{dmax}(n) \leq n$.
L'exemple L_n montre que, il existe un automate fini $\mathcal{A}$ à n états tel que $\mathrm{Card}(\mathbb{Q}(L_{\mathcal{A}})) = 2^n$.
Donc

$$\mathrm{dmax}(n) = 2^n.$$

Exercice 2 [12 points]
On admet que, si $(L_i)_{i\in I}$ est une famille de langages sur X et M un langage sur X, alors

$$(\bigcup_{i\in I} L_i)^{-1}M = \bigcup_{i\in I} L_i^{-1}M. \tag{3}$$

1- Supposons que le langage M possède n résiduels. Soit L un langage quelconque.
En utilisant l'égalité (3) :

$$\begin{aligned} L^{-1}M &= (\bigcup_{u\in L}\{u\})^{-1}M \\ &= \bigcup_{u\in L}(\{u\}^{-1}M) \\ &= \bigcup_{u\in L}(u^{-1}M) \end{aligned}$$

Posons $\mathbb{Q}_L(M) := \{u^{-1}M \mid u \in L\}$. Le langage $L^{-1}M$ est l'union des résiduels de M qui appartiennent à $\mathbb{Q}_L(M)$. Comme $\mathbb{Q}(M)$ a n éléments, $\mathbb{Q}_L(M)$ peut prendre au plus 2^n valeurs (en fonction de L). Le nombre de valeurs possibles pour $L^{-1}M$ est donc majoré par 2^n.
2- Chaque résiduel de M est rationnel. Comme les rationnels sont clos par union finie, $L^{-1}M = \bigcup_{R\in\mathbb{Q}_L(M)} R$ est rationnel.
3- Supposons que M est un langage algébrique sur Y et que L est un langage rationnel sur Y.
On introduit un alphabet auxiliaire $\bar{Y} := \{\bar{a}, \bar{b}, \bar{c}\}$ et les homomorphismes $\varphi, \psi : (Y \cup \bar{Y})^* \to Y^*$ définis par :

$$\forall y \in Y, \varphi(y) = y, \varphi(\bar{y}) = y, \psi(y) = \varepsilon, \psi(\bar{y}) = y.$$

3.1 Comme L est rationnel, $L \cdot \bar{Y}^*$ est rationnel.
Comme l'ensemble des langages algébriques est clos par homomorphisme inverse, $\varphi^{-1}(M)$ est algébrique.
Comme l'intersection d'un langage algébrique et d'un langage rationnel est algébrique, $\varphi^{-1}(M) \cap (L \cdot \bar{Y}^*)$ est algébrique.
3.2 $L^{-1}M = \psi(\varphi^{-1}(M) \cap (L \cdot \bar{Y}^*))$. Comme l'ensemble des langages algébriques est clos par

homomorphisme, on en déduit que $L^{-1}M$ est algébrique.
4- Le langage SYM est engendré par la grammaire $G := \langle\{a,b,c\},\{S\},P,S\rangle$, où P est constitué des règles :

$$S \to aSa + bSb + cSc + \#$$

Comme $M = (\text{SYM} \cap a^+b^+c^+)^+$, M_0 est algébrique (d'après les propriétés de clôture de l'ensemble des langages algébriques).
5- Le langage N est engendré par la grammaire $G := \langle\{a,b,c\},\{\sigma,S_0,S_1,S_2\},P,\sigma\rangle$, où P est constitué des règles :

$$\begin{array}{rcl} \sigma & \to & S_0\# \\ S_0 & \to & cS_0c + cS_1cc \\ S_1 & \to & bS_1b + bS_2bb \\ S_2 & \to & aS_2a + a\#aa \end{array}$$

Comme N est algébrique, les propriétés de clôture de l'ensemble des langages algébriques entraînent que L est aussi algébrique.
6- $((abc\#)^{-1}M) \cap c^+b^+a^+ = \{cba\}$
$((abc\#N)^{-1}M) \cap c^+b^+a^+ = \{ccbbaa\}$
7- Soit $n \geq 0$.
$((abc\#N^n)^{-1}M) \cap c^+b^+a^+ = \{c^{n+1}b^{n+1}a^{n+1}\}$ (ce langage est réduit à un seul mot).
8- $L = \bigcup_{n\in\mathbb{N}} abc\#N^n$ donc, par l'identité (3),

$$\begin{array}{rcl} L^{-1}M & = & (\bigcup\limits_{n\in\mathbb{N}} abc\#N^n)^{-1}M \\ & = & \bigcup\limits_{n\in\mathbb{N}} (abc\#N^n)^{-1}M \end{array}$$

La distributivité généralisée de l'intersection sur l'union entraîne alors que

$$\begin{array}{rcl} L^{-1}M \cap c^+b^+a^+ & = & (\bigcup\limits_{n\in\mathbb{N}} (abc\#N^n)^{-1}M) \cap c^+b^+a^+ \\ & = & \bigcup\limits_{n\in\mathbb{N}} ((abc\#N^n)^{-1}M)) \cap c^+b^+a^+ \\ & = & \bigcup\limits_{n\in\mathbb{N}} \{c^{n+1}b^{n+1}a^{n+1}\} \quad \text{en utilisant la qu. 7} \\ & = & \{c^{n+1}b^{n+1}a^{n+1} \mid n \geq 0\} \\ & = & \{c^nb^na^n \mid n \geq 1\}. \end{array}$$

9- On sait que le langage $\{c^nb^na^n \mid n \geq 1\}$ n'est pas algébrique. Comme l'ensemble des langages algébrique est clos par intersection avec les rationnels, on en déduit que $L^{-1}M$ n'est pas algébrique. Or, d'après les questions 4,5 L et M sont algébriques. Il n'est donc pas vrai que, pour tous langages algébriques L et M, le langage $L^{-1}M$ est algébrique.

10- Introduisons une lettre $z \notin \{a, b, c, \#\}$ et étudions le cas du langage $L_1 := L \cup (Mz)$. Remarquons que :

$$L_1^{-1}L_1 = L^{-1}L \cup L^{-1}(Mz) \cup (Mz)^{-1}L \cup (Mz)^{-1}(Mz)$$

Mais $(Mz)^{-1}L = \emptyset$ et $(Mz)^{-1}(Mz) = \{\varepsilon\}$. Remarquons enfin que les mots de $L^{-1}L$ ne comportent pas d'occurrence de z. Nous obtenons donc que :

$$\begin{aligned} L_1^{-1}L_1 \cap \{a, b, c, \#\}^* z &= L^{-1}(Mz) \\ &= (L^{-1}M)z \text{ (car } z \text{ n'a pas d'occurence dans } L). \end{aligned}$$

Comme $(L^{-1}M)$ est non-algébrique, et est l'image de $(L^{-1}M)z$ par effacement de la lettre z, ce qui est une opération d'homomorphisme, $(L^{-1}M)z$ est aussi non-algébrique. On en déduit que $L_1^{-1}L_1 \cap \{a, b, c, \#\}^* z$ est non-algébrique et finalement que $L_1^{-1}L_1$ est non-algébrique. Nous en concluons qu'il n'est pas vrai que, pour tout langage algébrique L, le langage $L^{-1}L$ est algébrique.

Exercice 3 [11 points]

1-

$$f(a, a) \in L_1, m(a) \notin L_1; \;\; m(m(a)) \in L_2, f(m(a), m(a)) \notin L_2; \;\; f(a, f(a, a)) \in L_3, f(a, a) \notin L_3$$

2-Pour chaque L_i ($1 \leq i \leq 3$), nous proposons un automate fini de termes $\mathcal{A}_i$ qui reconnaît exactement L_i.

$\mathcal{A}_1 = \langle F, \{0, 1\}, Q_{1,+}, \delta_1\rangle$ où $Q_{1,+} = \{0\}$ et δ_1 est formé des transitions :

$$a \to 1, \;\; m(0) \to 0, \;\; m(1) \to 1, \;\; \forall i, j \in \{0, 1\}, f(i, j) \to i + j \pmod 2.$$

L'idée directrice de $\mathcal{A}_1$ est qu'il atteint l'état i à la racine de t ssi la parité du nombre de feuilles de t vaut i.

$\mathcal{A}_2 = \langle F, Q_2, Q_{2,+}, \delta_2\rangle$ où

$$Q_2 = \{(0, i, 1, j) \mid 0 \leq i \leq 2, 0 \leq j \leq 2\}, \;\; Q_{2,+} = \{(0, i, 1, j) \mid 0 \leq i \leq 1, 0 \leq j \leq 2\}.$$

δ_2 est formé des transitions :

$$a \to (0, 1, 1, 0) \;\; \forall i, j \in [0, 2], m((0, i, 1, j)) \to (0, j, 1, i),$$
$$\forall i, j, k, \ell \in [0, 2], f((0, i, 1, j), (0, k, 1, \ell)) \to (0, \min(j + \ell, 2), 1, \min(i + k, 2))$$

L'idée directrice de $\mathcal{A}_1$ est qu'il atteint l'état $(0, i, 1, j)$ à la racine de t ssi le nombre de branches de longueur paire vaut i au seuil 2, et le nombre de branches de longueur impaire vaut j au seuil 2.

$\mathcal{A}_3 = \langle F, Q_3, Q_{3,+}, \delta_3\rangle$ où

$$Q_3 = \mathcal{P}(\{0, 1, 2\}), \;\; Q_{3,+} = \{P \in Q_3 \mid 1 \in P\}$$

et δ_3 est formé des transitions :

$$a \to \{1\} \;\; m(P) \to \emptyset, \;\; f(P, P') \to \{i \in \{1, 2\} \mid 3 - i \in P \cup P'\}$$

L'idée directrice de $\mathcal{A}_3$ est qu'il atteint l'état P à la racine de t ssi P est l'ensemble des états de l'automate fini de mots représenté sur la figure 4 obtenus en parcourant toutes les branches

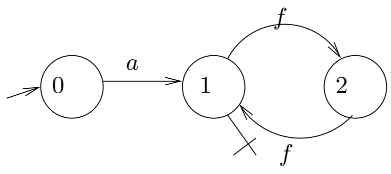

FIG. 3 – Un automate (de mots) reconnaissant $a(ff)^*$

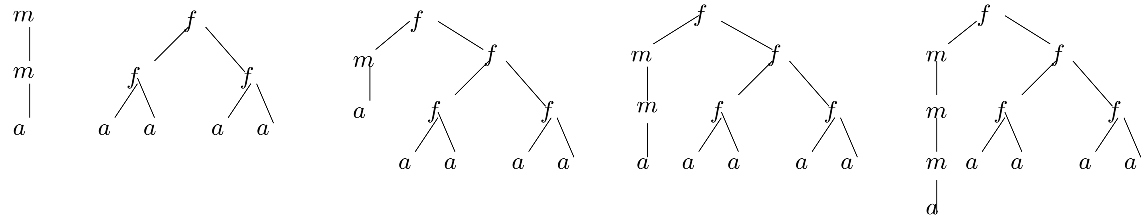

FIG. 4 – Les cinq termes de ex.3-qu.3

depuis leur feuille jusqu'à la racine de t.
3- Voir la figure 4.
4- Si $p \leq q$, alors l'une des plus courtes branches de $f(M_p, K_q)$ est la branche aboutissant à la feuille 0^p, qui est étiquetée par fm^pa alors qu'aucune des branches de K_q ne comporte d'étiquette m.
Si $p > q$, alors toutes les plus courtes branches de $f(M_p, K_q)$ aboutissent à une feuille de K_q : elles ne contiennent aucun noeid étiqueté par m.
On en conclut que :

$$f(M_p, K_q) \in L \Leftrightarrow 1 \leq p \leq q.$$

5- Par la question 4, $f(M_k, K_k) \in L$. Donc il existe une course ρ de l'automate $\mathcal{A}$ sur ce terme, telle que $\rho(\varepsilon) = r \in Q_+$. Notons $r_1 := \rho(0), r_2 := \rho(1)$. On a :

$$M_k \to_{\mathcal{A}}^* r_1, \;\; K_k \to_{\mathcal{A}}^* r_2 \;\; \wedge \;\; f(r_1, r_2) \to_{\mathcal{A}} r.$$

Les états r_1, r_2, r vérifient donc les conditions demandées.
6- Comme $\|M_k\| \geq k$, d'après le lemme d'itération des langages reconnaissables de termes, appliqué au langage $\{t \mid t \to_{\mathcal{A}}^* r_1\}$, il existe des contextes B, C et un terme d tels que

$$M_k = B[C[d]], \;\; \|C\| \geq 2 \;\; \wedge \;\; \forall n \in \mathbb{N}, B[C^n[d]] \to_{\mathcal{A}}^* r_1$$

Vu la forme du terme M_k, C doit être de la forme : $C := m^j(\bullet)$ avec $j \geq 1$. Donc, pour tout $n \geq 0, M_{k+(n-1)j} \to_{\mathcal{A}}^* r_1$. Posons $n := 2, p := k + j, q := k$. On a

$$p > q \geq 0 \;\; , \;\; M_p \to_{\mathcal{A}}^* r_1 \;\; \wedge \;\; K_q \to_{\mathcal{A}}^* r_2$$

Comme , par ailleurs, $f(r_1, r_2) \to_{\mathcal{A}} r$, on obtient que

$$p > q \geq 0 \;\; \wedge \;\; f(M_p, K_q) \in L$$

D'après la question 4, comme $p > q \geq 0$, $f(M_p, K_q) \notin L$.
Cette contradiction montre que l'hypothèse (**H**) est impossible : on a prouvé par l'absurde que L n'est pas rationnel.