RAIRO
INFORMATIQUE THÉORIQUE

ROBERT CORI
DOMINIQUE PERRIN

Automates et commutations partielles

RAIRO – Informatique théorique, tome 19, nº 1 (1985), p. 21-32.
<http://www.numdam.org/item?id=ITA_1985__19_1_21_0>

R.A.I.R.O. Informatique théorique/Theoretical Informatics
(vol. 19, n° 1, 1985, p. 21 à 32)

AUTOMATES ET COMMUTATIONS PARTIELLES (*)

par Robert CORI (1) et Dominique PERRIN (2)

Communiqué par J. E. PIN

Résumé. — *On considère un alphabet A et une relation de commutation partielle entre les lettres de A. Le principal résultat de cet article donne une condition suffisante pour qu'un ensemble de mots clos par la relation de commutation soit reconnaissable par un automate fini. Plus précisément, si X est reconnaissable et si chaque fois que* $ab \sim ba$, *les lettres a et b n'apparaissent pas simultanément dans un même mot de X, alors la fermeture de* X^* *par la relation de commutation est reconnaissable.*

Abstract. — *We consider words over an alphabet equiped with a partial commutation rule. The main result of the paper gives a sufficient condition for a set of words closed under the commutation rule to be recognizable by a finite automaton. More precisely, if X is recognizable and if* $ab \sim ba$ *implies that the letters a and b do not appear in the same word of X, then the closure of* X^* *under the commutation rule is recognizable.*

INTRODUCTION

Les monoïdes partiellement commutatifs libres sont les objets obtenus en considérant des mots dans lesquels certaines des lettres sont autorisées à commuter. Ils ont, semble-t-il été utilisés pour la première fois par Cartier et Foata [1] dans le but d'étudier les problèmes de réarrangements sur les mots et, en particulier, de donner une forme plus générale au « Master Theorem » de McMahon. L'ouvrage de Cartier et Foata, qui date de 1969, contient entre autres la définition d'une forme normale pour les éléments d'un monoïde partiellement commutatif libre.

Plus récemment, les recherches menées sur les calculs en parallèle ont conduit à s'intéresser sous un autre angle à ces monoïdes. Dans ce cadre, les lettres sont considérées comme des actions pouvant être par exemple des

(*) Reçu et accepté juin 1984.
Ce travail a été réalisé dans le cadre du GRECO de Programmation, Contrat ADI n° 9683.
(1) Université de Bordeaux-I, Laboratoire de Mathématiques et Informatique, Laboratoire associé au C.N.R.S., 351, cours de la Libération, 33405 Talence Cedex, France.
(2) L.I.T.P., Université de Paris-VII, 2, place Jussieu, 75221 Paris Cedex 05, France.

instructions d'un ou de plusieurs programmes. Certaines de ces actions sont autorisées à commuter parce que l'ordre dans lequel elles sont effectuées ne modifie pas le résultat. Le cas contraire se produit par exemple pour deux actions du type

$$i \leftarrow i+1 \qquad \text{et} \qquad i \leftarrow 2^* i.$$

Le point de départ de notre travail est un article de Flé et Roucairol [3] où les auteurs démontrent un théorème surprenant. Ce résultat est, en termes de calculs parallèles, le suivant : si l'on désire effectuer séquentiellement des actions $a_{i,\,j}$ se regroupant par blocs nommés transactions :

$$x_1 = a_{1,\,1}\, a_{1,\,2} \ldots a_{1,\,n_1},$$

$$x_2 = a_{2,1}\, a_{2,2} \ldots a_{2,\,n_2},$$

$$\ldots,$$

$$x_k = a_{k,\,1}\, a_{k,\,2} \ldots a_{k,\,n_k},$$

de telle façon que, aux commutations autorisées près, le résultat soit équivalent à l'exécution de la suite de transactions :

$$y_1 . y_2 \ldots y_n \qquad \text{où} \quad y_i \in \{x_1, x_2, \ldots, x_k\},$$

un automate fini suffit pour contrôler la correction du déroulement des opérations.

En termes mathématiques, ce résultat s'énonce ainsi : si θ est une relation de commutation partielle sur A et si X est un ensemble fini de mots de A^* composé chacun de lettres qui ne commutent pas entre elles, alors la clôture selon θ du sous-monoïde X^* engendré par X est une partie reconnaissable de A^*.

Dans cet article, nous donnons une généralisation de ce résultat au cas où X est une partie reconnaissable de A^* au lieu d'une partie finie. Cette hypothèse a encore une interprétation en termes de mise en séquence de calculs. On peut en effet considérer, au lieu des blocs x_i ci-dessus des parties reconnaissables :

$$X_1, X_2, \ldots, X_k,$$

correspondant chacune aux exécutions possibles d'un programme p_i ($i=1, \ldots, k$). On n'autorise à commuter que des instructions appartenant à des programmes différents. On peut alors, comme dans le cas précédent, chercher à contrôler les exécutions qui forment des suites équivalentes par commutation à des exécutions d'une suite :

$$y_1 y_2 \ldots y_n,$$

où chacun des y_i est une exécution de l'un des programmes p_j. Notre résultat signifie que ce contrôle peut être effectué par un automate fini et donne un algorithme pour le construire. Cet algorithme donne pour le cas où X est fini une construction qui est plus directe que celle de [3] : elle permet en fait de ne pas construire l'automate tout entier à l'avance.

1. MONOIDES PARTIELLEMENT COMMUTATIFS LIBRES

Dans tout cet article, A désigne un alphabet fini. Nous suivons les notations de M. Lothaire pour les mots [4]. En particulier, la longueur du mot $w \in A^*$ est notée $|w|$ et pour une partie B de A, on note $|w|_B$ le nombre d'occurrences de lettres de B dans w. On note alph (w) l'ensemble des lettres qui apparaissent dans w :

$$\text{alph}(w) = \{ a \in A \mid |w|_a \geqq 1 \}.$$

Soit θ une relation réflexive et symétrique sur A. On note $\sim$ la congruence engendrée par les couples :

$$(ab, ba),$$

pour $(a, b) \in \theta$. On note $M(A, \theta)$ le quotient de A^* par cette congruence. On dit que c'est le *monoïde partiellement commutatif libre* sur A (relativement à θ).

Nous allons établir une suite de propriétés de $M(A, \theta)$ qui rendent le calcul dans $M(A, \theta)$ plus facile.

La proposition suivante donne un critère commode pour l'égalité des images de deux mots dans $M(A, \theta)$. Pour cela, on note pour $B \subset A$:

$$\pi_B : \quad A^* \to B^*,$$

le morphisme défini par $\pi_B(b) = b$ si $b \in B$ et $\pi_B(a) = 1$ si $a \in A - B$.

PROPOSITION 1.1. — *Soient u, $v \in A^*$. On a $u \sim v$ ssi :*

$$\pi_a(u) = \pi_a(v),$$

pour tout $a \in A$ et

$$\pi_{a,\, b}(u) = \pi_{a,\, b}(v),$$

pour tous a, $b \in A$ tels que $(a, b) \notin \theta$.

Démonstration : La condition est évidemment nécessaire. Pour montrer qu'elle est suffisante, raisonnons par récurrence sur la longueur commune de u et v. Pour $|u|=|v|=1$ l'énoncé est trivial. Supposons $|u|=|v|\geqq 2$ et posons $u=au'$ avec $a\in A$, $u'\in A^*$. Comme $\pi_a(u)=\pi_a(v)$ on a $\pi_a(v)\neq 1$. Posons $v=v'av''$ avec $\pi_a(v')=1$. Montrons d'abord que $av'\sim v'a$. Cela est vrai si $v'=1$. Sinon, soit $b\in\text{alph}(v')$. Alors $\pi_{a,b}(v)$ commence par b tandis que $\pi_{a,b}(u)$ commence par a. Cela implique $(a, b)\in\theta$. Ainsi toutes les lettres de v' commutent avec a et donc $av'\sim v'a$.

Ainsi, on a $v\sim av'v''$. Soient $c, d\in A$ tels que $(c, d)\notin\theta$. Si $a\notin\{c, d\}$, alors :

$$\pi_{c,d}(v'v'')=\pi_{c,d}(v)=\pi_{c,d}(u)=\pi_{c,d}(u').$$

Si par contre $a\in\{c, d\}$, supposons par exemple $c=a$. Alors $\pi_{a,d}(v')=1$ d'après ce qui précède et donc :

$$\pi_{a,d}(v'av'')=a\,\pi_{a,d}(v'')=a\,\pi_{a,d}(v'v'')=a\,\pi_{a,d}(u'),$$

d'où $\pi_{a,d}(v'v'')=\pi_{a,d}(u')$.

Comme par ailleurs $\pi_b(v'v'')=\pi_b(u')$ pour tout $b\in A$, on a donc $v'v''\sim u'$ par hypothèse de récurrence. Ainsi :

$u=au'\sim av'v''\sim v'av''=v$. ■

On déduit du résultat précédent un résultat qui implique que $M(A, \theta)$ est simplifiable, c'est-à-dire $uv\sim uw$ (resp. $vu\sim wu$) implique $v\sim w$.

COROLLAIRE 1.2 : *Soient $u, v\in A^*$ et $a\in A$ tels que :*

$$u=u'au'',\quad v=v'av'',$$

avec $\pi_a(u')=\pi_a(v')$. Alors $u\sim v$ implique :

$$u'u''\sim v'v''.$$

Démonstration : On a pour tout $b\in A$, $\pi_b(u'u'')=\pi_b(v'v'')$. Soient $b, c\in A$ tels que $(b, c)\notin\theta$. Si $a\notin\{b, c\}$, alors :

$$\pi_{b,c}(u'u'')=\pi_{b,c}(u)=\pi_{b,c}(v)=\pi_{b,c}(v'v'').$$

Sinon, supposons par exemple $b=a$. On a alors :

$$\pi_{a,c}(u')\,a\,\pi_{a,c}(u'')=\pi_{a,c}(u)=\pi_{a,c}(v)=\pi_{a,c}(v')\,a\,\pi_{a,c}(v'').$$

Comme $\pi_a(u')=\pi_a(v')$, on en déduit que $\pi_{a,c}(u'u'')=\pi_{a,c}(v'v'')=\pi_{a,c}(v'v'')$. D'après la proposition 1.3, on a donc $u'u''\sim v'v''$. ■

La proposition suivante donne les solutions de l'équation $xy=zt$ dans le monoïde $M(A, \theta)$. Pour cela, introduisons une définition. On dit que deux mots u, $v \in A^*$ *commutent absolument* si pour tous $a \in \mathrm{alph}(u)$, $b \in \mathrm{alph}(v)$, on a $(a, b) \in \theta$. On note $u \Gamma v$ le fait que u et v commutent absolument. Si $u \Gamma v$ on a certainement $uv \sim vu$ mais la réciproque n'est pas vraie, puisque par exemple $uu \sim uu$ bien que l'on n'aie pas nécessairement $u \Gamma u$.

PROPOSITION 1.3. — *Soient* $x, y, z, t \in A^*$. *On a :*

$$xy \sim zt$$

ssi $x \sim uv$, $y \sim rs$, $z \sim ur$, $t \sim vs$ *pour des mots* $u, v, r, s \in A^*$ *tels que* $v \Gamma r$.

Démonstration : La condition est suffisante puisque $v \Gamma r$ implique $vr \sim rv$ et donc $xy \sim uvrs \sim urvs \sim zt$. Pour montrer qu'elle est nécessaire on effectue une récurrence sur la longueur de x. Si $x=1$, on prend $u=v=1$ et $r=z$, $s=t$. Sinon, posons $x=ax'$ avec $a \in A$. Comme xy commence par a, toutes les lettres de zt qui se trouvent avant la première occurence de a commutent avec a. Distinguons deux cas :

Supposons d'abord que $\pi_a(z)=1$. On a alors d'après la remarque précédente $a \Gamma z$ et $t \sim at'$. De $ax'y \sim zat'$ on déduit $x'y \sim zt'$ d'après le corollaire 1.4. Par hypothèse de récurrence, on a :

$$x' \sim uv', \qquad y \sim rs, \qquad z \sim ur, \qquad t' \sim v's$$

et $v' \Gamma r$. Posons $v=av'$. Comme $a \Gamma z$ on a aussi $a \Gamma u$ et $a \Gamma r$. Comme $x=auv'$ et que $a \Gamma u$ on a donc $x \sim uav'=uv$. On obtient donc $x \sim uv$, $y \sim rs$, $z \sim ur$, $t \sim vs$ avec $v \Gamma r$.

Supposons ensuite que $\pi_a(z) \neq 1$. On a alors $z \sim az'$. Ainsi $x'y \sim z't$ d'où par hypothèse de récurrence $x' \sim u'v$, $y \sim rs$, $z \sim u'r$, $t \sim vs$ avec $r \Gamma v$. En posant $u=au'$ on obtient la conclusion. ■

COROLLAIRE 1.4 : *Soient* $u, v, x_1, x_2, \ldots, x_n \in A^*$. *On a :*

$$uv \sim x_1 x_2 \ldots x_n,$$

ssi $u \sim p_1 p_2 \ldots p_n$, $v \sim q_1 q_2 \ldots q_n$ *avec :*

$$p_i q_i = x_i \qquad (i \leq i \leq n),$$

$$q_i \Gamma (p_{i+1} \ldots p_n) \qquad (1 \leq i \leq n).$$

Démonstration : La condition est suffisante. En effet, on a :

$$\begin{aligned}uv &\sim p_1 p_2 \ldots p_n q_1 q_2 \ldots q_n,\\ &\sim (p_1 q_1) p_2 \ldots p_n q_2 \ldots q_n,\\ &\ldots,\\ &\sim (p_1 q_2)(p_2 q_2) \ldots (p_n q_n).\end{aligned}$$

Réciproquement, on raisonne par récurrence sur n. Si $n=0$ le problème est trivial. Pour $n \geqq 1$, posons $x=x_1$, $y=x_2 \ldots x_n$. Comme $uv \sim xy$, on a d'après la proposition 1.5 :

$$u \sim p_1 r, \qquad v \sim q_1 s, \qquad x \sim p_1 q_1, \qquad y \sim rs,$$

avec $r \Gamma q_1$. Par hypothèse de récurrence, on a :

$$r \sim p_2 \ldots p_n, \qquad s \sim q_2 \ldots q_k,$$

avec $p_i q_i = x_i$, $\Gamma q_i (p_{i+1} \ldots p_n)$ pour $2 \leqq i \leqq n$, d'où la conclusion. ■

2. RECONNAISSABILITÉ DANS $M(A, \theta)$

Dans un monoïde M quelconque, une partie X est reconnaissable si la famille des translatés $\{u^{-1} X\}$ (où $u^{-1} X$ dénote l'ensemble $\{v \mid uv \in X\}$) est une famille finie de parties de M.

Dans le cas où M est le monoïde libre A^*, on peut dire de manière équivalente que X est reconnu par un automate fini.

Dans M quelconque, on définit aussi les parties rationnelles comme celles obtenues à partir des parties finies par les opérations union, produit, passage au sous-monoïde engendré (ou étoile). Le théorème de Kleene affirme que dans A^*, il y a équivalence entre reconnaissabilité et rationnalité. Tel n'est pas le cas dans un monoïde quelconque, en particulier dans les monoïdes $M(A, \theta)$ comme le montre l'exemple suivant :

Exemple 2.1 : Soit $A=\{a, b\}$, $(a, b) \in \theta$. Le monoïde $M(A, \theta)$ est le monoïde commutatif libre à deux générateurs. Considérons le sous-monoïde X engendré par ab. C'est bien entendu, une partie rationnelle de $M(A, \theta)$. Par contre, cette partie n'est pas reconnaissable, car si on pose $u_i = a^i$, on a :

$$b^k \in u_i^{-1} X \quad \text{si et seulement si } k = i.$$

Ainsi les $u_i^{-1} X$ forment une famille infinie de parties. ■

Pour une partie X de A^* *on note* $[X]$ l'union des $\sim$ classes des éléments de X :

$$[X]=\{y \mid \exists x \in X;\ y \sim x\}.$$

On peut alors vérifier qu'une partie U de $M(A, \theta)$ est rationnelle si et seulement si $U=[X]$ où X est une partie rationnelle de A^*. D'autre part, une partie V de $M(A, \theta)$ est reconnaissable s'il existe X reconnaissable dans A^* tel que $X=[X]=V$.

Une partie reconnaissable de $M(A, \theta)$ est évidemment toujours rationnelle. Le problème se pose de savoir quelles sont les parties rationnelles de $M(A, \theta)$ qui sont reconnaissables. La réponse est connue dans les deux cas extrêmes : quand θ est vide, par le théorème de Kleene; quand θ est la relation universelle puisque dans ce cas les parties reconnaissables sont les combinaisons booléennes de parties de la forme :

$$X_{n,\,p}=\{w \in A^* \mid |w|_a=n+kp,\ k \geqq 0\},$$

pour $n, p \geqq 0$.

Pour étudier le cas général, on peut chercher à étudier le comportement des opérations rationnelles par rapport à la relation de commutation partielle. Pour l'union et le produit, le problème est sans difficulté.

PROPOSITION 2.1 : *Soient X, Y deux parties reconnaissables de A^*. Si $[X]=X$ et $[Y]=Y$ alors :*

$$[X \cup Y] \quad \text{et} \quad [XY],$$

sont des parties reconnaissables de A^*.

Démonstration : On a $[X \cup U]=[X] \cup [Y]=X \cup Y$ d'où le résultat puisque $X \cup Y$ est reconnaissable.

Posons $Z=[XY]$. On associe à chaque mot $u \in A^*$ l'ensemble :

$$\pi(u)=\{(p^{-1}X, p'^{-1}Y, \operatorname{alph}(p')) \mid u \sim pp'\}.$$

La famille des $\pi(u)$ pour $u \in A^*$ est finie puisque alph (p') est une partie de l'ensemble fini A et que les $p^{-1}X$ pour $p \in A^*$ forment une famille finie.

Pour prouver que Z est reconnaissable, il suffit donc de prouver que :

$$\pi(u)=\pi(t) \quad \Rightarrow \quad u^{-1}Z=t^{-1}Z.$$

Supposons pour cela que $uv \in Z$. On a $uv \sim xy$ pour $x \in X$, $y \in Y$. D'après la proposition 1.5, on obtient :

$$u \sim pp', \quad v \sim qq', \qquad x \sim pq, \qquad y \sim p'q',$$

avec $p' \Gamma q$.

Comme $[X]=X$ et $[Y]=Y$, on a $pq\in X$ et $p'q'\in Y$. Comme $\pi(u)=\pi(u')$, on a $t=rr'$ avec $p^{-1}X=r^{-1}X$, $p'^{-1}Y=r'^{-1}Y$, alph $(p')=$alph (r'). Ainsi $rq\in X$, $r'q'\in Y$ et $r'\Gamma q$. Cela entraîne que $tv\in Z$ d'où la conclusion. ■

Exemple 2.2 : Soit $A=B\cup C$ une partition de A. Supposons que θ ne mette en relation que des éléments de B avec des éléments de C. Si $X\subset B^*$, $Y\subset C^*$ on a trivialement $[X]=X$ et $[Y]=Y$. Dans le cas où toutes les lettres de B commutent avec toutes les lettres de C, l'ensemble $[XY]$ est le « shuffle » de X et Y, parfois noté $X \sqcup\!\sqcup Y$. ■

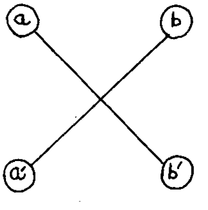
L'énoncé correspondant à la proposition 2.1 pour l'étoile est plus difficile. On ne peut l'énoncer de façon tout à fait similaire puisque dans l'exemple 2.1 on a $[X]=\{ab, ba\}$ qui est reconnaissable bien que $[X^*]=[[X]^*]$ ne le soit pas.

On dit qu'une partie X de A^* est *rigide* (relativement à θ) si pour tout $x\in X$ et tous a, $b\in$alph(x) avec $a\neq b$, on a $(a, b)\notin\theta$. Ainsi, si X est rigide, on a $[X]=X$ mais la réciproque est évidemment fausse. Le résultat suivant est une généralisation de celui de [3] qui correspond au cas où X est fini. C'est le plat de résistance.

THÉORÈME 2.2 : *Soit X une partie reconnaissable de A^*. Si X est rigide, alors $[X^*]$ est reconnaissable.*

Avant de donner la preuve, commençons par quelques exemples.

Exemple 2.3 : Soit $A=\{a, a', b, b'\}$ et considérons la relation θ dont le graphe est donné figure 1.



Soit $X=\{aa', bb'\}$. Un automate reconnaissant $[X^*]$ est donné sur la figure 1 ci-dessous :

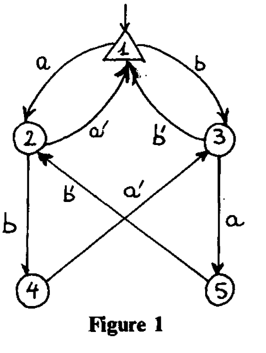


Figure 1

L'ensemble des états est $\{1, 2, 3, 4, 5\}$ et 1 est l'état initial ($\downarrow$) et aussi l'unique état final ($\triangle$). ■

Exemple 2.4 : Avec l'alphabet et relation de commutation de l'exemple précédent, considérons :

$$X = a^* a' \cup b^* b'$$

Un automate reconnaissant $[X^*]$ est cette fois :

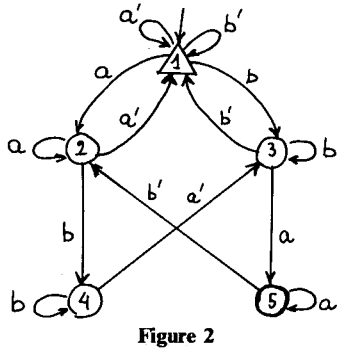


Figure 2

La démonstration du théorème 2.2 utilise le lemme suivant. Il s'agit d'une forme plus précise du corollaire 1.6.

LEMME 2.3 : *Soit X une partie rigide de A^*. Pour $u, v \in A^*$, on a :*

$$uv \in [X^*],$$

ssi il existe un entier $n \geq 0$, *des mots* y_i, $z_i \in X^*$ $(0 \leqq i \leqq n)$ *et des mots* u_i, $v_i \in A^+$ $(1 \leqq i \leqq n)$ *tels que :*

(i) $$u \sim y_0 u_1 y_1 u_2 \ldots u_n y_n;$$

(ii) $$v \sim z_0 v_1 z_1 v_2 \ldots v_n y_n;$$

(iii) $$u_i v_i \in X \qquad (1 \leqq i \leqq n);$$

(iv) $$z_i \Gamma (u_{i+1} y_{i+1} \ldots u_n y_n) \qquad (0 \leqq i \leqq n);$$

(v) $$v_i \Gamma (y_i u_{i+1} \ldots u_n y_n) \qquad (1 \leqq i \leqq n);$$

(vi) $$\mathrm{alph}(u_i) \cap \mathrm{alph}(u_j) = \varnothing \qquad (1 \leqq i < j \leqq n).$$

Démonstration : La condition est suffisante. En effet, on a alors :

$$uv \sim y_0 u_1 y_1 u_2 \ldots u_n y_n z_0 v_1 z_1 v_2 \ldots v_n y_n,$$

$$y_0 z_0 u_1 y_1 u_2 \ldots u_n y_n v_1 z_1 v_2 \ldots v_n z_n,$$

$$y_0 z_0 (u_1 v_1) y_1 u_2 \ldots u_n y_n z_1 v_2 \ldots v_n z_n,$$

$$\ldots,$$

$$y_0 z_0 (u_1 v_1) y_1 z_1 (u_2 v_2) \ldots (u_n v_n) y_n z_n.$$

Montrons ensuite qu'elle est nécessaire. La preuve est par récurrence sur le plus petit entier k tel que $uv \in X^k$. Pour $k=0$ tout va bien. Supposons $k \geqq 1$ et posons $uv \sim xy$ avec $x \in X$ et $y \in X^{k-1}$. D'après la proposition 1.5, on a :

$$u \sim pp', \qquad v \sim qq', \qquad x \sim pq, \qquad y \sim p' q',$$

avec $p' \Gamma q$. Par hypothèse de récurrence, on a :

(i) $$p' \sim y_1 u_2 y_2 u_3 \ldots u_n y_n;$$

(ii) $$q' \sim z_1 v_2 z_2 v_3 \ldots v_n z_n;$$

(iii) $$u_i v_i \in X \qquad (2 \leqq i \leqq n);$$

(iv) $$z_i \Gamma (u_{i+1} \ldots u_n y_n) \qquad (1 \leqq i \leqq n);$$

(v) $$v_i \Gamma (y_i u_{i+1} \ldots u_n y_n) \qquad (2 \leqq i \leqq n);$$

(vi) $$\operatorname{alph}(u_i) \cap \operatorname{alph}(u_j) = \varnothing \; (1 \leqslant i < j \leqslant n).$$

Distinguons maintenant trois cas.

1. si $p=1$, on pose $z'_1 = qz_1$. On a bien $z'_1 \Gamma (u_2 y_2 \ldots u_n y_n)$ puisque on a $q \Gamma (y_1 u_2 y_2 \ldots u_n y_n)$ et $z_1 \Gamma (u_2 y_2 \ldots u_n y_n)$. Les décompositions de u et v en :

$$u \sim y_1 u_2 y_2 u_3 \ldots u_n y_n, \qquad v \sim z'_1 v_2 z_2 \ldots v_n z_n,$$

satisfont les six conditions du lemme avec $y_0 = u_1 = z_0 = v_1 = 1$ et z'_1 au lieu de z_1.

2. si $q=1$, on pose $y'_1 = py_1$ et les décompositions :

$$u \sim y'_1 u_2 y_2 u_3 \ldots u_n y_n, \qquad v \sim z_1 v_2 z_2 \ldots v_n z_n,$$

satisfont les six conditions du lemme avec $y_0 = u_1 = z_0 = v_1 = 1$ et y'_1 au lieu de y_1.

3. si $p \neq 1$, $q \neq 1$, on distingue encore deux cas :

3 *a*. si alph $(p) \cap$ alph $(u_i) = \varnothing$ pour tout $i \in \{2, 3, \ldots, n\}$, on pose $u_1 = p$, $v_1 = q$. Les décompositions :

$$u \sim u_1 y_1 u_2 y_2 \ldots u_n y_n, \qquad v \sim v_1 z_1 v_2 \ldots v_n y_n,$$

satisfont toutes les conditions du lemme avec $y_0 = z_0 = 1$.

3 *b*. s'il existe un entier $i \in \{2, 3, \ldots, n\}$ tel que alph $(p) \cap$ alph $(u_i) \neq 0$, on peut supposer qu'il est unique sans quoi on peut itérer la construction qui va suivre. Soit $a \in$ alph $(p) \cap$ alph (u_i). Montrons d'abord que :

$$\operatorname{alph}(u_i) = \operatorname{alph}(q) = \{a\}.$$

Soit en effet $b \in \text{alph}\,(q)$. Comme $p' \Gamma q$, on a en particulier $u_i \Gamma q$. Supposons $a \neq b$. Comme a, $b \in \text{alph}\,(pq)$, que $pq \in X$ et que X est rigide, on a $(a, b) \notin \theta$ en contradiction avec $u_i \Gamma q$. Ainsi alph $(q) = \{a\}$.

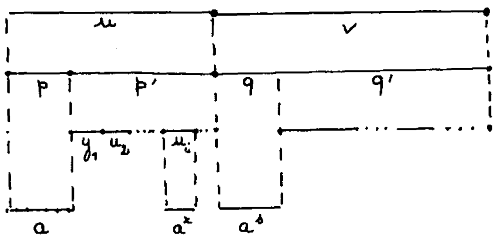


Figure 3

Comme $q \Gamma p'$, on a $a \Gamma (y_1 u_2 \ldots u_n y_n)$. Ensuite, comme on a $z_j \Gamma u_i$ pour $1 \leqslant j \leqslant i-1$, et $v_j \Gamma u_i$ pour $2 \leqslant j \leqslant i-1$ on a aussi $a \Gamma (z_1 v_2 \ldots v_{i-1} z_{i-1})$.

Posons $u_i = a^r$, $q = a^s$. Si $r < s$, on pose :

$$u_1 = pa^r, \qquad v_1 = a^{s-r}, \qquad y'_{i-1} = y_{i-1} y_i, \qquad z'_{i-1} = z_{i-1} a^r v_i z_i.$$

Les décompositions de u et v en :

$$v \sim v_1 z_1 v_2 \ldots z'_{i-1} v_{i+1} \ldots v_n z_n,$$

satisfont les conditions du lemme avec $y_0 = z_0 = u_i = 1$, y'_{i-1} et z'_{i-1} au lieu de y_{i-1} et z_{i-1} et avec un décalage d'indices pour $j \geqq i$. Si $r \geqq s$, on pose :

$$y_0 = pa^s, \qquad u'_i = a^{r-s}, \qquad v'_i = a^s v_i.$$

Les décompositions de u et v en :

$$u \sim y_0 y_1 u_2 \ldots y_{i-1} u'_i y_i \ldots u_n y_n, \qquad v \sim z_1 v_2 \ldots z_{i-1} v'_i z_i \ldots v_n z_n,$$

satisfont les conditions du lemme avec $u_1 = z_0 = v_1 = 1$ et u'_i, v'_i au lieu de u_i, v'_i.

Ceci achève la preuve du lemme. ■

Nous sommes maintenant en mesure de démontrer le théorème 2.2.

Démonstration du théorème : Pour chaque mot $u \in A^*$, on note $\sigma(u)$ l'ensemble constitué des $3n$-uplets :

$$(\text{alph}\,(u_1),\ u_1^{-1} X,\ \text{alph}\,(y_1),\ \text{alph}\,(u_2),$$
$$u_2^{-1} X,\ \text{alph}\,(y_2),\ \ldots,\ \text{alph}\,(u_n),\ u_n^{-1} X,\ \text{alph}\,(\text{alph}\,(\text{alph}\,(\text{alph}\,(y_n)),$$

pour tous les $(u_i, y_i)_{1 \leqslant i \leqslant n}$ tels que :

(i) $$u \sim y_0 u_1 y_1 u_2 \ldots u_n y_n;$$

(ii) $$y_i \in X^* \qquad (0 \leqslant i \leqslant n);$$

(iii) $$u_i \in A^+ \quad \text{et} \quad \text{alph}\,(u_i) \cap \text{alph}\,(u_j) = \varnothing \qquad (1 \leqq i \leqq n).$$

Il n'y a qu'un nombre fini de $\sigma(u)$ possibles. En effet, la condition (i) assure que $n \leqslant \mathrm{Card}(A)$. Ensuite, comme X est reconnaissable, il n'y a qu'un nombre fini de $u_i^{-1} X$ possibles. Et enfin, comme A est en douce supposé fini depuis le début, il n'y a qu'un nombre fini de alph (y_i) possibles.

Pour prouver que $Y=[X^*]$ est reconnaissable, il suffit donc de montrer que pour tous u, $t \in A^*$, on a :

$$\sigma(u)=\sigma(t) \quad \Rightarrow \quad u^{-1} Y = t^{-1} Y.$$

Supposons pour cela que $uv \in Y$. D'après le lemme 2.3, on a :

$$u \sim y_0 u_1 y_1 \ldots u_n y_n, \qquad v \sim z_0 v_1 y_1 \ldots v_n y_n,$$

pour des mots u_i, $v_i \in A^+$ et y_i, $z_i \in X^*$ satisfaisant les six conditions du lemme 2.3. Comme $\sigma(u)=\sigma(t)$, on a :

$$t \sim x_0 t_1 x_1 t_2 \ldots t_n x_n,$$

pour des mots x_i, t_i *tels que :*

$$x_i \in X^* \qquad (0 \leqq i \leqq n),$$
$$\mathrm{alph}\,(x_i) = \mathrm{alph}\,(y_i) \qquad (1 \leqslant i \leqslant n),$$
$$t_i^{-1} X = u_i^{-1} X \qquad (1 \leqq i \leqq n),$$
$$\mathrm{alph}\,(t_i) = \mathrm{alph}\,(u_i) \qquad (1 \leqq \leqslant i \leqslant N).$$

Comme $u_i v_i \in X$, on a $t_i v_i \in X$. Comme $z_i \Gamma (u_{i+1} y_{i+1} \ldots u_n y_n)$ et que :

$$\mathrm{alph}\,(u_{i+1} y_{i+1} \ldots u_n y_n) = \mathrm{alph}\,(t_{i+1} x_{i+1} \ldots t_n y_n)$$

on a $z_i \Gamma (t_{i+1} x_{i+1} \ldots t_n y_n)$. De même, on a $v_i \Gamma (x_i t_{i+1} \ldots t_n x_n)$. Ainsi $tv \in Z$, et ceci achève la démonstration du théorème. ■

BIBLIOGRAPHIE

1. P. Cartier et D. Foata, *Problèmes combinatoires de commutation et réarrangements*, Lecture Notes in Math., n° 85, 1969, Springer Verlag.
2. S. Eilenberg, *Automata, Languages and Machines*, vol. A, 1974, Academic Press.
3. M. P. Flé et G. Roucairol, *On Serializability of Iterated Transactions*, A.C.M. SIGACT-SIGOPS, 1982, p. 194-200.
4. M. Lothaire, *Combinatorics on Words*, 1983, Addison Wesley.