RAIRO

INFORMATIQUE THÉORIQUE

GIUSEPPINA RINDONE

Sur les groupes syntaxiques d'un langage

RAIRO – Informatique théorique, tome 19, n° 1 (1985), p. 57-70.

http://www.numdam.org/item?id=ITA_1985__19_1_57_0

© AFCET, 1985, tous droits réservés.

L'accès aux archives de la revue « RAIRO – Informatique théorique » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

SUR LES GROUPES SYNTAXIQUES D'UN LANGAGE (*)

par Giuseppina RINDONE ⁽¹⁾

Communiqué par J.-E. PIN

Résumé. — Nous donnons une condition nécessaire pour qu'un groupe de permutations transitif fini G soit un groupe maximal du monoïde syntaxique de X^* , où X est une partie finie d'un code à groupe associé au groupe G . Nous montrons en outre que, sous ces hypothèses, si G n'est pas cyclique, on a l'inégalité :

$$\text{Card}(X) \geq d + 1,$$

où d est le degré de G .

Abstract. — We give a necessary condition for a finite transitive group G of permutations to be a maximal group of the syntactic monoid of X^* , where X is a finite part of a group-code associated to G . Moreover, we show that, under such hypothesis, if G is not cyclic, we have:

$$\text{Card}(X) \geq d + 1,$$

where d is the degree of G .

INTRODUCTION

Soit L une partie du monoïde libre A^* . On dit qu'un groupe G est un groupe syntaxique de L si G est, à un isomorphisme près, un groupe maximal du monoïde syntaxique $M(L)$ de L . D'après le théorème de M. P. Schützenberger [9], les parties de A^* dont tous les groupes syntaxiques sont triviaux sont des langages sans étoile.

L'étude des groupes dans $M(L)$, lorsque L est de la forme X^* avec X un code fini a fait l'objet de travaux très poussés (Perrin, Perrot, Schützenberger). Dans cette étude, le groupe de structure de l'idéal minimal de $M(X^*)$, appelé le groupe de Suschkewitsch du code, joue un rôle prépondérant car beaucoup

(*) Reçu septembre 1983, révisé juillet 1984.

(1) Faculté des Sciences, Université de Rouen, B.P. n° 67, 76130 Mont-Saint-Aignan, France et Laboratoire d'Informatique Théorique et de Programmation, 2, place Jussieu, 75005 Paris, France.

de propriétés du code se lisent directement sur le groupe de Suschkewitsch du code; mais J. F. Perrot a démontré que certains groupes de permutations transitifs ne peuvent apparaître comme groupe de Suschkewitsch d'un code préfixe X lorsque X est supposé fini [6]. C'est pourquoi on est amené à généraliser le problème et à se demander s'il peut apparaître comme groupe de structure d'une autre $\mathcal{D}$ -classe régulière de $M(X^*)$, qui ne soit pas nécessairement la $\mathcal{D}$ -classe de rang minimal, mais en conservant la propriété de finitude pour X .

D. Perrin donne dans [7] une condition suffisante pour que ceci se réalise et il en déduit que tout groupe de permutations transitif fini est le groupe de structure d'une $\mathcal{D}$ -classe régulière de $M(X^*)$. Cette dernière référence étant peu accessible, nous avons préféré, pour la commodité du lecteur, redonner entièrement les preuves.

Nous montrons ici que la condition évoquée dans [7] est aussi nécessaire et nous montrons que, pour la construction utilisée, le groupe en question est toujours le groupe de structure de la $\mathcal{D}$ -classe régulière de rang maximal.

Suivant un théorème de M. P. Schützenberger [10], si X est une partie finie de A^* et si d est le degré d'un groupe syntaxique G de X^* , avec G non cyclique, alors on a : $\text{Card}(X) \geq d$. Nous montrons que, lorsque X est une partie d'un code à groupe, cette borne peut être améliorée d'une unité.

RAPPELS ET NOTATIONS

Soit A un alphabet fini et A^* le monoïde libre sur A . On note 1 l'élément neutre de A^* (le mot vide), et $A^+ = A^* \setminus \{1\}$.

Soient $u, v \in A^*$ deux mots. On dit que u est *facteur* (respectivement *facteur gauche*, *facteur droit*) de v si $v \in A^* u A^*$ (resp. $v \in u A^*$, $v \in A^* u$); u est *facteur interne* (resp. *facteur gauche propre*, *facteur droit propre*) si $v \in A^+ u A^+$ (resp. $v \in u A^+$, $v \in A^+ u$). Pour toute partie L de A^* , on note $F(L)$ [resp. $FI(L)$] l'ensemble des facteurs (resp. facteurs internes) des mots de L et on pose $\overline{F}(L) = A^* \setminus F(L)$ et $\overline{FI}(L) = A^* \setminus FI(L)$.

Une partie X de A^* est un *code* ssi le sous-monoïde X^* de A^* , engendré par X , est libre de base X . On vérifie que si X est un code rationnel alors $F(X) \neq A^*$ et si X est un code maximal alors $F(X^*) = A^*$.

Une partie X de A^* telle que $XA^* \cap X = \emptyset$ est dite *préfixe*. On vérifie que X est préfixe ssi X^* est unitaire à gauche : pour tout $u, v \in A^*$, u et $uv \in X^*$ entraîne $v \in X^*$. On en déduit que toute partie préfixe est un code. La condition de maximalité pour les codes préfixes se traduit par la propriété de complétude à droite : pour tout $u \in A^*$, $u A^* \cap X^* \neq \emptyset$.

On définit de façon symétrique les codes *suffixes* et on dit que X est un code *bipréfixe* s'il est à la fois préfixe et suffixe.

Étant donné une partie L de A^* , le *monoïde syntaxique* de L , noté $M(L)$, est, par définition, le quotient de A^* par la congruence la plus grossière telle que L soit union de classes. Cette congruence, appelée *congruence syntaxique* de L , a pour expression : $u \equiv v \pmod{L}$ si et seulement si, quel que soit $(f, g) \in A^* \times A^*$ on a : $fug \in L$ si et seulement si $fv g \in L$.

Le morphisme canonique ϕ de A^* dans $M(L)$ est appelé le *morphisme syntaxique* de L . On sait que le monoïde syntaxique de L est isomorphe au monoïde des transitions de l'automate minimal de L , noté $\mathcal{A}(L)$. Dans la suite, par abus de langage, nous les identifions. D'après le théorème de Kleene, $M(L)$ est fini ssi L est une partie rationnelle de A^* .

Rappelons que si L est de la forme $L = X^*$ avec X un code préfixe, l'automate minimal de L a un seul état terminal confondu avec l'état initial; nous noterons 1 cet état. Nous avons alors : $L = \{w \in A^* : 1 \phi(w) = 1\}$.

Nous utiliserons la terminologie suivante pour les automates de la forme $\mathcal{A} = (Q, 1, 1)$:

pour tout $p, q \in Q$, on dit que le chemin $p \xrightarrow{w} q$ est simple ($w \in A^+$) si, pour tout $r \in Q$ tel que $p \xrightarrow{u} r \xrightarrow{v} q$ avec $u, v \in A^+$ et $w = uv$, on a $r \neq 1$.

Un chemin qui n'est pas simple est produit de chemins simples.

Nous renvoyons le lecteur à [1 ou 4] pour toutes les notions non définies ici et en particulier, pour ce qui concerne les relations de Green $\mathcal{R}$, $\mathcal{L}$, $\mathcal{H}$, $\mathcal{D}$, que nous aurons à utiliser, définies dans un monoïde.

CODES A GROUPE

Soient G un groupe de permutations transitif, H le sous-groupe de G fixant un point donné de l'ensemble sur lequel opère G et $\psi : A^* \rightarrow G$ un morphisme surjectif. Le sous-monoïde $\psi^{-1}(H)$ est unitaire à droite et à gauche car il en est ainsi de H dans G . Il est donc engendré par un code bipréfixe que nous nommons *code à groupe* et que nous notons $Z(G, H)_\psi$, ou tout simplement Z . On dit que Z est de *degré* d si G est de degré d . On vérifie facilement qu'un code à groupe est maximal en tant que code, il est donc maximal en tant que code bipréfixe.

Exemple : Soit G le groupe engendré par la permutation $\alpha = (0, 1, 2, \dots, n-1)$ et soit ψ le morphisme de A^* dans G défini par $\psi(a) = \alpha$, pour

tout $a \in A$. La base Z du noyau de ψ , qui est le code uniforme de longueur n : $Z = A^n$, est un code à groupe de degré n .

THÉORÈME 1 : Soit $Z = Z(G, H)_\psi$ un code à groupe. Le monoïde syntaxique de Z^* est isomorphe à G . En particulier Z est rationnel si et seulement si G est fini.

Preuve : Notons Q l'ensemble des classes latérales à droite de H dans G et soit $\mathcal{A} = (Q, 1, 1)$ l'automate sur l'alphabet A , où $1 = H$, avec les transitions $Hx_i \xrightarrow{a} Hx_j$ ($a \in A$) si et seulement si $x_i \psi(a) \in Hx_j$. On démontre facilement que l'automate ainsi défini est isomorphe à l'automate minimal de Z^* . $\square$

Le résultat suivant est bien connu [8] :

THÉORÈME 2 : Soit Z un code à groupe, $Z = Z(G, H)_\psi$. Z est fini si et seulement si $Z = A^n$. Et dans ce cas G est cyclique d'ordre n .

Donnons quelques définitions :

On nomme *point d'un mot* $w \in A^*$ tout couple de mots $(w_1, w_2) \in A^* \times A^*$ tel que $w = w_1 w_2$. Un mot w contient donc $|w| + 1$ points, où $|w|$ dénote la longueur de w .

Soit $X \subset A^*$. On appelle *interprétation* de w dans X^* , ou X -interprétation de w , tout triplet $(d, x, g) \in D \times X^* \times G$ tel que $w = dxg$, où D (resp. G) est l'ensemble des facteurs droits (resp. gauches) propres des mots de X .

On note $I_X(w)$ l'ensemble des X -interprétations de w .

On dit qu'une X -interprétation (d, x, g) de $w \in A^*$ *passé par le point* (w_1, w_2) de w s'il existe $x_1, x_2 \in X^*$ tels que $x = x_1 x_2$, $w_1 = dx_1$ et $w_2 = x_2 g$.

Une X -interprétation de w passant par le point (w_1, w_2) .

Un mot $w \in A^*$ est *X -plein* si, pour tout point de w , il existe une X -interprétation de w passant par ce point.

On vérifie sans difficulté :

PROPOSITION 1 : Soit X un code bipréfixe et soit $w \in A^*$. Pour tout point de w il existe au plus une X -interprétation de w passant par ce point.

PROPOSITION 2 : Soit X un code bipréfixe rationnel. X est maximal ssi tout mot de A^* est X -plein.

Soit L une partie de A^* et soit Q l'ensemble des états de l'automate minimal de L . Pour tout $w \in A^*$, nous noterons $\text{Im } \varphi(w)$ l'ensemble des images non nulles de $\varphi(w)$; c'est-à-dire :

$$\text{Im } \varphi(w) = \{q \in Q, q \neq 0 \text{ tels qu'il existe } p \in Q : p \varphi(w) = q\}.$$

On pose $\text{rang } \varphi(w) = \text{Card}(\text{Im } \varphi(w))$.

Dans le cas d'un code bipréfixe, la notion d'interprétation d'un mot $w \in A^*$ et la notion de rang de l'image syntaxique de w sont reliées par la proposition suivante :

PROPOSITION 3 : Soit X un code bipréfixe et soit φ le morphisme syntaxique de X^* . Pour tout $w \in A^*$ on a $\text{Card}(I_X(w)) \leq \text{rang } \varphi(w)$. Si $w \notin F(X)$ alors $\text{Card}(I_X(w)) = \text{rang } \varphi(w)$.

Preuve : Notons S l'ensemble des facteurs droits de w qui sont facteurs gauches d'un mot de X . D'après la proposition 1, l'application qui associe à toute X -interprétation (d, x, g) de w le mot g est une injection.

Soit $\mathcal{A}(X^*) = (Q, 1, 1)$ l'automate minimal de X^* . On définit $\alpha : I_X(w) \rightarrow \text{Im } \varphi(w)$ en posant $\alpha(d, x, g) = 1 \varphi(g)$. On a $1 \varphi(g) \in \text{Im } \varphi(w)$ puisque $g \in S$ et $(d, x, g) \in I_X(w)$.

La suffixité de X implique que α est injective.

Il reste à prouver que si $w \notin F(X)$ alors α est aussi surjective. En effet, pour tout $q \in \text{Im } \varphi(w)$, il existe $p \in Q$ ($p \neq 0$) tel que $p \varphi(w) = q$. De façon équivalente, il existe un chemin dans $\mathcal{A}(X^*)$ allant de p à q d'étiquette w . Ce chemin n'est pas simple puisque $w \notin F(X)$. Donc il existe $f, g \in A^*$ et $x_1, x_2, \dots, x_n \in X^*$ ($n \geq 0$) tel que $w = f x_1 x_2 \dots x_n g$ et les chemins :

$$p \xrightarrow{f} 1 \xrightarrow{x_1} 1 \dots \xrightarrow{x_n} 1 \xrightarrow{g} q$$

sont simples. Par conséquent $(f, x_1 x_2 \dots x_n, g)$ est une X -interprétation de w dont l'image par α est q . $\square$

COROLLAIRE 1 : Soit X un code bipréfixe rationnel et soient w et $w' \in A^* \setminus F(X)$.

1° Si $\varphi(w) \not\supseteq \varphi(w')$ alors $\text{Card}(I_X(w)) = \text{Card}(I_X(w'))$.

2° Si G est un groupe dans $M(X^*)$ de degré d et $\varphi(w) \in G$ alors $\text{Card}(I_X(w)) = d$.

La preuve est conséquence immédiate de la proposition précédente car $\varphi(w) \not\supseteq \varphi(w')$ implique $\text{rang } \varphi(w) = \text{rang } \varphi(w')$ et si $\varphi(w) \in G$ et $d = \text{degré}(G)$ alors $\text{rang } \varphi(w) = d$.

Dans le cas où X n'est pas bipréfixe, on retrouve des résultats similaires en introduisant les notions d'interprétations disjointes et parallèles. Le lecteur intéressé pourra consulter [5].

LEMME 1 : Soit X un code bipréfixe rationnel maximal. Pour tout $u, f, g \in A^*$, on a :

$$\text{Card}(I_X(u)) \leq \text{Card}(I_X(fug)).$$

En particulier, $\text{Card}(I_X(u)) < \text{Card}(I_X(fug))$ si $f, g \in A^+$ et $fug \in X$.

Preuve : D'après la proposition 2, le mot fug est X -plein. Par conséquent, chaque X -interprétation de u peut se prolonger en une X -interprétation de fug , ce qui prouve la première inégalité.

La deuxième inégalité est évidente car si u, f, g vérifient les hypothèses alors $(1, fug, 1) \in I_X(fug)$ et cette X -interprétation ne détermine aucune X -interprétation de u puisqu'elle ne passe pas aucun point de u .

PROPOSITION 4 : Soit $Z = Z(G, H)_\psi$ un code à groupe de degré d . Pour tout $w \in A^*$, $\text{Card}(I_Z(w)) \leq d$.

De plus, $\text{Card}(I_Z(w)) = d$ ssi $w \notin FI(Z)$.

Preuve : Soit $f \in A^* \setminus F(Z)$. Pour tout $w \in A^*$, on a :

$$\text{Card}(I_Z(w)) \leq \text{Card}(I_Z(fwf)) = d,$$

d'après le lemme 1 et la proposition 3.

Supposons $\text{Card}(I_Z(w)) = d$. Si $w \in FI(Z)$, il existe $z \in Z$ et $f, g \in A^+$ tel que $z = fwg$. D'après le lemme 1 $\text{Card}(I_Z(w)) < \text{Card}(I_Z(z))$ et d'après ce qui précède $\text{Card}(I_Z(z)) \leq d$. Absurde.

La réciproque se déduit immédiatement de la condition 2 du corollaire 1 puisque si $w \notin F(Z)$ alors $w \notin FI(Z)$. $\square$

Il ne sera plus question dans la suite que de groupes de permutations transitifs finis, et pour abréger nous dirons simplement groupes.

GROUPES SYNTAXIQUES

Soit $L \subset A^*$. On dit qu'un groupe G est un *groupe syntaxique* de L si G est, à un isomorphisme près, un groupe maximal du monoïde syntaxique $M(L)$ de L .

De la définition de code à groupe et du théorème 1, il s'ensuit que, pour tout groupe G , il existe un alphabet fini A et un sous-monoïde Z^* de A^* tel

que G est un groupe syntaxique de Z^* mais, d'après le théorème 2, à moins que G ne soit cyclique, Z est toujours infini. D'où le problème suivant : *un groupe quelconque peut-il être un groupe syntaxique d'un sous-monoïde finiment engendré?* Et plus précisément, si Z est un code à groupe associé au groupe G , existe-t-il des parties finies X de Z telles que G est un groupe syntaxique de X^* ?

La proposition qui suit affirme que, si une telle partie X existe, le groupe G appartient alors à la $\mathcal{D}$ -classe régulière (évidemment non triviale) de $M(X^*)$ de rang maximal.

Nous noterons ϕ le morphisme syntaxique de X^* .

PROPOSITION 5 : *Soient $Z = Z(G, H)_\psi$ un code à groupe de degré d et X une partie finie de Z . Si G' est un groupe dans $M(X^*)$ de degré d' , alors $d' \leq d$.*

Preuve : Soit $w \in A^*$ un mot tel que $\phi(w) \in G'$. Comme X est fini, on peut toujours supposer, quitte à considérer une puissance convenable de w , que $w \notin F(X)$.

D'après le corollaire 1 et la proposition 4, et du fait que chaque X -interprétation de w est une Z -interprétation, on déduit :

$$d' = \text{Card}(I_X(w)) \leq \text{Card}(I_Z(w)) \leq d. \quad \square$$

LEMME 2 : *Soient $Z = Z(G, H)_\psi$ un code à groupe et $X \subset Z$ une partie rationnelle. Si w et w' sont deux mots X -pleins de $A^* \setminus F(Z)$ alors $\phi(w) = \phi(w')$ implique $\psi(w) = \psi(w')$. Et si, en outre, $\phi(w) \not\sim \phi(w')$ alors $\psi(w) \neq \psi(w')$ implique $\phi(w) = \phi(w')$.*

Preuve : Soit $(u, v) \in A^* \times A^*$ tel que $uwv \in Z^*$. Comme $w \notin F(Z)$, il existe une Z -interprétation (f, z, g) de w telle que $uf, z, gv \in Z^*$.

Posons $\mathcal{A}(Z^*) = (Q, 1, 1)$ et soient $p, q \in Q$ les états tels que :

$$\left. \begin{array}{l} 1\psi(u) = p; \quad p\psi(f) = 1; \\ 1\psi(z) = 1; \quad 1\psi(g) = q; \quad q\psi(v) = 1. \end{array} \right\} \quad (1)$$

L'hypothèse w X -plein implique $(f, z, g) \in I_X(w)$. Par conséquent, il existe $(u', v') \in A^* \times A^*$ tel que $u'f, z, gv' \in X^*$; $u'f$ et gv' sont aussi dans Z^* puisque $X^* \subset Z^*$.

On en déduit, en utilisant (1) :

$$1\psi(u') = p \quad \text{et} \quad q\psi(v') = 1. \quad (2)$$

Par hypothèse $\varphi(w) = \varphi(w')$ et $w' \notin F(Z)$ [a fortiori $w' \notin F(X)$]. Il existe alors $(f', x', g') \in I_X(w')$ tel que $u'f', x', g'v'$ sont dans X^* , ce qui implique, en même temps que les relations (2) :

$$p\psi(f') = 1 \quad \text{et} \quad 1\psi(g') = q. \quad (3)$$

Des relations (1) + (3) on déduit $uw'v \in Z^*$, ce qui prouve $\psi(w) = \psi(w')$.

Supposons maintenant que w et w' sont X -pleins, $\psi(w) = \psi(w')$ et $\varphi(w) \not\mathcal{R} \varphi(w')$.

Soit $(u, v) \in A^* \times A^*$ tel que $uvw \in X^*$ et soit $(f, x, g) \in I_X(w)$ tel que $uf, x, gv \in X^*$. Comme $\psi(w) = \psi(w')$ et $w' \in F(Z)$, il existe $(f', z', g') \in I_Z(w')$ tel que $uf', z', g'v \in Z^*$. Le mot z' est dans X^* puisque $I_X(w') = I_Z(w')$. Il reste à prouver que uf' et $g'v$ sont dans X^* . En effet, posons $\mathcal{A}(X^*) = (S, 1, 1)$ et soient $r, s \in S$ tels que :

$$1 \xrightarrow{u} r \xrightarrow{f} 1 \xrightarrow{x} 1 \xrightarrow{g} s \xrightarrow{v} 1. \quad (1)$$

Comme $\varphi(w) \not\mathcal{R} \varphi(w')$ et $s \neq 0$, il existe $s' \in S$ ($s' \neq 0$) tel que $r\varphi(w') = s'$. Le chemin $r \xrightarrow{w'} s'$ n'est pas simple puisque $w' \notin F(X)$; et comme $uf' \in Z^*$ et Z est préfixe, ce chemin se factorise nécessairement en :

$$r \xrightarrow{f'} 1 \xrightarrow{z'} 1 \xrightarrow{g'} s'.$$

On en déduit que $uf' \in X^*$.

De la relation $\varphi(w) \mathcal{L} \varphi(w')$ et de la suffixité de Z , on déduit $g'v \in X^*$. $\square$

LEMME 3 : Soient $Z = Z(G, H)_\psi$ un code à groupe et X une partie rationnelle de Z . Soit encore Y une partie de A^* vérifiant les conditions :

1° pour tout $y \in Y$, l'ensemble des mots :

$$\{z \in Z \text{ t. q. } z \in A^* y A^*\}$$

est fini.

2° $\psi(Y^*) = G$.

3° $F(Y^*) \cap Z \subseteq X$.

Alors $\varphi(Y^+ \cap \bar{F}(Z))$ est contenu dans une $\mathcal{D}$ -classe de $M(X^*)$.

Preuve : Nous allons démontrer d'abord que, pour tout $y \in Y^+ \cap \bar{F}(Z)$ et pour tout $w \in Y^*$, on a :

$$\psi(y) = \psi(ywy) \quad \text{implique} \quad \varphi(y) = \varphi(ywy).$$

En effet, soit $(u, v) \in A^* \times A^*$ tel que $uyv \in X^*$. Comme $y \notin F(X)$ la factorisation en mots de X du mot uyv doit couper le mot y . Soient $y_1, y_2 \in A^*$ tels que $y = y_1 y_2$ et $uy_1 \in X^*, y_2 v \in X^*$.

On a alors $uyv \in Z^*$ et par conséquent, $uywyv \in Z^*$. La bipréfixité de Z implique $y_2 wy_1 \in Z^*$. Et comme $y_2 wy_1 \in F(Y^*)$ on déduit $y_2 wy_1 \in X^*$. Ainsi

$uywyv \in X^*$. De la même façon, on démontre que $uywyv \in X^*$ implique $uyv \in X^*$.

Soient maintenant $f, g \in Y^+ \cap \bar{F}(Z)$. Comme $\psi(Y^*) = G$, il existe $\bar{f}, \bar{g} \in Y^*$ tels que $\psi(\bar{f}) = [\psi(f)]^{-1}$ et $\psi(\bar{g}) = [\psi(g)]^{-1}$. On a alors :

$$\psi(f) = \psi(fg\bar{g}\bar{f}) \quad \text{et} \quad \psi(g) = \psi(g\bar{f}\bar{g}g).$$

On en déduit, d'après ce qui a été démontré ci-dessus, que $\varphi(f) \mathcal{D} \varphi(g)$.

C.Q.F.D. $\square$

La partie réciproque du théorème suivant est due à D. Perrin [7].

THÉORÈME 3 : Soient $Z = Z(G, H)_\psi$ un code à groupe de degré d et X une partie finie de Z . Alors $M(X^*)$ contient un groupe maximal équivalent à G ssi il existe un ensemble fini $Y \subset A^*$ vérifiant les conditions :

- 1° $\forall y \in Y, \{z \in Z \text{ t. q. } z \in A^* y A^*\} \text{ est fini.}$
- 2° $\psi(Y^*) = G.$
- 3° $F(Y^*) \cap Z \subseteq X.$

Preuve : Supposons que $M(X^*)$ contienne un groupe maximal G' équivalent à G . Soit Δ un ensemble de générateurs de G' . Il existe alors, pour tout $\partial \in \Delta$, un mot $y \in A^*$ tel que $\varphi(y) = \partial$.

Nous pouvons supposer, quitte à considérer une puissance convenable de y , que $y \notin F(X)$. Notons Y l'ensemble des mots, en bijection avec Δ , ainsi obtenus. Alors $\varphi(Y^+) = G'$. Du corollaire 1 et de la proposition 4, on déduit, pour tout $y \in Y^+$, les inégalités :

$$d = \text{Card}(I_X(y)) \leq \text{Card}(I_Z(y)) \leq d.$$

D'où $\text{Card}(I_Z(y)) = d$. D'après la proposition 4, $y \notin FI(Z)$, par conséquent $y^3 \notin F(Z)$. Ceci prouve qu'on peut choisir les mots $y \in Y$ tels que $y \notin F(Z)$.

La condition 1 est donc trivialement vérifiée. D'après la proposition 2, tout mot de Y^+ est un mot Z -plein; il est aussi X -plein puisque $\text{Card}(I_Z(y)) = \text{Card}(I_X(y))$. Ainsi $F(Y^*) \cap Z \subseteq X$.

Réciproquement, supposons qu'il existe un ensemble fini $Y \subset A^*$, vérifiant les conditions du théorème. On choisit $y \in Y^+$ qui n'est facteur d'aucun mot de Z et on pose $S = \varphi(y Y^* y)$. S est évidemment un sous-semi-groupe de $M(X^*)$.

D'après le lemme 3, S est contenu dans la $\mathcal{D}$ -classe contenant l'élément $\varphi(y)$.

On en déduit que S est contenu dans la $\mathcal{H}$ -classe contenant $\varphi(y)$ puisque, pour tout $s \in S$, $s = \varphi(y) \varphi(y' y) = \varphi(y y') \varphi(y)$ pour un certain $y' \in Y^*$.

On définit $\mu : S \rightarrow G$ par $\mu(\varphi(yy'y)) = \psi(yy'y)$.

D'après la condition 2, μ est un morphisme surjectif. La condition 3 entraîne que tout mot de S est X -plein et le lemme 2 permet de conclure que μ est aussi injectif. Ainsi S est un groupe dans $M(X^*)$ isomorphe à G . Il est de degré d et l'image de $\varphi(X^*)$ par μ est H .

Il reste encore à prouver qu'il est un groupe maximal. En effet, soit n un entier tel que $\varphi(y^n)$ soit l'identité de S . Alors, pour tout $f \in A^*$, si $\varphi(f) \notin \varphi(y)$, on a $\varphi(f) = \varphi(y^n f y^n)$. D'après le corollaire 1, les mots $y^n f y^n$ et y ont le même nombre de X -interprétations. On en déduit alors que $y^n f y^n$ est un mot X -plein.

Soit g un mot de Y^* tel que $\psi(g) = \psi(f)$.

Du lemme 2, il s'ensuit que $\varphi(y^n g y^n) = \varphi(y^n f y^n)$. Par conséquent $\varphi(f) \in S$ et donc S est une $\mathcal{H}$ -classe entière.

C.Q.F.D. $\square$

Le résultat suivant est conséquence du théorème 3 :

PROPOSITION 6 : *Tout groupe de permutations transitif fini est un groupe syntaxique d'un sous-monoïde finiment engendré.*

Preuve : Soient G un groupe de permutations transitif fini et H le sous-groupe de G , fixant un point donné de l'ensemble sur lequel opère G . Soit encore A un alphabet en bijection avec une partie génératrice de G . On étend cette bijection à un morphisme ψ de A^* sur G et soit $Z = Z(G, H)_\psi$ le code à groupe associé.

On choisit, pour chaque lettre $a \in A$, un mot $y \in A^*$ tel que :

1° $\psi(y) = \psi(a)$.

2° l'ensemble $\{z \in Z / z \in A^* y A^*\}$ est fini.

On note Y l'ensemble des mots, en bijection avec A , ainsi obtenus.

On définit X' comme la partie de Z formée des mots qui sont facteurs d'au moins un mot de Y^* , c'est-à-dire :

$$X' = \{z \in Z / \exists y \in Y^* \text{ tel que } y \in A^* z A^*\} = F(Y^*) \cap Z.$$

Évidemment X' est non vide puisque tout mot de A^* est facteur d'un mot de Z^* . De plus, X' est fini; en effet :

$$X' = (A^* Y A^* \cap X') \cup (X' \setminus A^* Y A^*).$$

Or l'ensemble $(A^* Y A^* \cap X')$ est fini car Y est fini et chaque $y \in Y$ n'est facteur que d'un nombre fini (disons k le maximum) de mots de Z donc :

$$\text{Card}(A^* Y A^* \cap X') \leq k \cdot \text{Card}(Y),$$

et, d'autre part,

$$\text{Card}(X' \setminus A^* Y A^*) \leq \sum_{y \in Y} |y|.$$

Pour toute partie finie X de Z telle que $X' \subseteq X$, le monoïde syntaxique de X^* contient un groupe maximal équivalent à G puisque toutes les hypothèses du théorème précédent sont satisfaites. $\square$

Exemple : Considérons le groupe de permutations G sur l'ensemble $\{1, 2, 3, 4\}$ engendré par les éléments $\alpha = (12)(34)$ et $\beta = (13)(24)$ et soit $\psi : \{a, b\}^* \rightarrow G$ le morphisme défini par $\psi(a) = \alpha$ et $\psi(b) = \beta$. Soit encore $Z = Z(G, H)_\psi$ le code à groupe associé, où H est l'identité de G . L'automate de Z^* peut être ainsi représenté :

Posons $y_a = ababa$ et $y_b = abababa$.

On vérifie facilement que l'ensemble $Y = \{y_a, y_b\}$ satisfait les conditions de la preuve de la proposition précédente. Le calcul des Z -interprétations des mots de Y^* donne l'ensemble :

$$X = \{abab, aa, baba, abaaba, baab\}.$$

Un choix différent de Y , $Y = \{aabab, bbaba\}$, donne un ensemble X de cardinalité 12. Dans les deux cas, G est, à un isomorphisme près, le groupe de structure de la $\mathcal{D}$ -classe régulière de $M(X^*)$ de rang maximal. Nous verrons au paragraphe suivant que $\text{Card}(X)$ est borné en fonction du degré de G et, dans le cas présent, $\text{Card}(X) = 5$ est la borne optimale.

Lorsque le groupe G contient un cycle de longueur égale à son degré, la construction donnée dans la proposition 6 fournit un ensemble ayant « le bon nombre d'éléments » :

PROPOSITION 7 [7]. — Soit G un groupe de permutations transitif sur l'ensemble $\{0, 1, \dots, n-1\}$ engendré par la permutation $\alpha = (0, 1, \dots, n-1)$ et par une partie T de G .

Soit $A = (a_t)_{t \in T + \alpha}$ un alphabet indexé par $T + \alpha$ et

$$X = a_\alpha^n + \{a_\alpha^i a_t a_\alpha^{n-i-t} / i \in \{1, \dots, n\}, t \in T\},$$

où les entiers i et $n-i-t$ sont pris mod n .

Alors le monoïde syntaxique de X^* contient un groupe maximal équivalent à G .

Preuve : Soit $\psi : A^* \rightarrow G$ le morphisme défini par :

$$\psi(a_t) = t, \quad \forall t \in T + \alpha.$$

On choisit, comme dans la preuve de la proposition 6 :

$$y_{a_\alpha} = a_\alpha^{n+1}$$

et pour tout $t \in T$:

$$y_{a_t} = a_\alpha^n a_t a_\alpha^n.$$

Le résultat est alors établi puisque l'ensemble X de l'énoncé est l'ensemble $F(Y^*) \cap Z$ où $Z = Z(G, H)_\psi$ (H étant le sous-groupe de G fixant le point 0). $\square$

Exemple : Soit $G = \mathcal{S}_3$ le groupe symétrique sur $\{0, 1, 2\}$ engendré par $\alpha = (012)$ et $\beta = (0, 1)$. La construction précédente donne l'ensemble :

$$X = \{a^3, ba^2, ab, a^2ba\}.$$

RELATION ENTRE LE DEGRÉ D'UN GROUPE SYNTAXIQUE DE X^* et $\text{Card}(X)$

Un premier résultat à l'égard de la relation entre le degré des groupes syntaxiques de X^* (avec X une partie finie quelconque de A^*) et $\text{Card}(X)$ est dû à M. P. Schützenberger. Il démontre dans [10] que si G est un groupe syntaxique de X^* de degré d et si G n'est pas cyclique alors $d \leq 2 \text{Card}(X)$.

Il conjecture que, sous les mêmes hypothèses, on ait :

$$d \leq \text{Card}(X) - 1.$$

Un résultat combinatoire sur les mots a permis de ramener cette borne à : $d \leq \text{Card}(X)$ (cf. [2, 3]).

Nous allons démontrer que, si X est une partie d'un code à groupe, nous avons le résultat cherché.

Nous avons vu que, pour tout $w \in \varphi^{-1}(G) \cap \bar{F}(X)$, $\text{Card}(I_X(w)) = d$. Il suffit alors de montrer que si $d = \text{Card}(X)$, alors G est cyclique.

Soit $w = a_1 a_2 \dots a_n$ un mot de A^* , ($a_i \in A$). Le plus petit entier p tel que $a_i = a_{i+p}$ est appelé *la période de w* ; on le note $p(w)$.

Soit (w_1, w_2) un point de w . Le plus petit entier r tel qu'il existe un mot $u \in A^*$ de longueur r vérifiant les deux conditions ci-dessous est appelé *la répétition de w au point (w_1, w_2)* :

$$1^\circ A^*u \cap A^*w_1 \neq \emptyset \quad \text{et} \quad 2^\circ uA^* \cap w_2A^* \neq \emptyset.$$

Un point (w_1, w_2) de w est un *point critique* de w si la répétition de w au point (w_1, w_2) est égale à la période de w .

Soit X une partie quelconque de A^* . Deux X -interprétations (q, x, p) et (q', x', p') d'un mot $w \in A^* \setminus F(X)$ sont *adjacentes* si elles passent toutes les deux par un même point de w ; c'est-à-dire s'il existe $x_1, x_2, x'_1, x'_2 \in X^*$ tels que $qx_1 = q'x'_1$ et $x_2p = x'_2p'$ avec $x = x_1x_2$ et $x' = x'_1x'_2$.

Deux X -interprétations non adjacentes sont dites *disjointes*.

Nous remarquons que si X est un code bipréfixe, deux X -interprétations distinctes d'un mot w sont toujours disjointes.

PROPOSITION 8 [5] : *Soient X une partie quelconque de A^* ; $k = \text{Card}(X)$, $w \in A^* \setminus F(X)$ un mot suffisamment long. Si w admet k X -interprétations disjointes deux à deux et l'une d'entre elles passe par un point critique de w , alors il existe $x \in X$ tel que $p(w) \leq |x|$.*

Preuve : Soit (w_1, w_2) un point critique de w et (q, d_1d_2, p) l'interprétation qui passe par ce point. Supposons d'abord que $d_1 \neq 1$ et $d_2 \neq 1$. Soient $x_1, x_2 \in X$ tel que $d_1 \in X^*x_1$ et $d_2 \in x_2X^*$.

Si $x_1 = x_2$, la répétition de w au point (w_1, w_2) est inférieure ou égale à $|x_1|$. Si $x_1 \neq x_2$, puisque w admet k X -interprétations disjointes deux à deux, il existe $x \in X$ qui recouvre deux fois le point (w_1, w_2) . x est alors de la forme $x = h^n l$ ($h, l \in A^*$, $h \in lA^*$ et $n \geq 0$). Le point (w_1, w_2) de w détermine alors un point (h_1, h_2) de h et la répétition de w au point (w_1, w_2) résulte inférieure ou égale à $|h| \leq |x|$.

Supposons maintenant $d_1 = 1$ ($d_2 = 1$); et soient $p', q' \in A^*$ tels que $p'q \in X$ ($pq' \in X$). En posant $p'q = x_1$ ($pq' = x_2$), nous sommes ramenés au cas précédent. $\square$

Nous sommes en mesure de démontrer le résultat énoncé plus haut :

PROPOSITION 9 : Soient $Z = Z(G, H)_\psi$ un code à groupe de degré d et X une partie finie de Z telle que G est un groupe syntaxique de X^* . Si G n'est pas cyclique alors $\text{Card}(X) \geq d + 1$.

Preuve : Si G est un groupe syntaxique de X^* , il existe, d'après le théorème 3, un ensemble $Y \subset A^*$ tel que $F(Y^*) \cap Z \subseteq X$ ce qui implique que tout mot de Y^+ est X -plein. En outre, d'après la preuve de ce théorème, on peut choisir Y tel que, pour tout $y \in Y^+$, $y \notin F(X)$ et $\varphi(Y^+) = G$.

Supposons maintenant $d = \text{Card}(X)$. De la proposition précédente on déduit que l'ensemble des périodes des mots de Y^+ est borné; il existe alors un mot $h \in A^*$ tel que $Y^+ \subseteq h^*$. Soit i la plus petite puissance de h tel que $\varphi(h^i) \in G$. Alors $\varphi(h^i)$ engendre G et G est cyclique contre l'hypothèse. $\square$

BIBLIOGRAPHIE

1. J. BERSTEL et D. PERRIN, *The Theory of Codes*, Academic Press (à paraître), cf. rapport L.I.T.P. n° 82-33, 84-5.
2. Y. CÉSARI et M. VINCENT, *Une caractérisation des mots périodiques*, C.R. Acad. Sc., t. 286, série A, 1978, p. 1175-1177.
3. J. P. DUVAL, *Périodes et répétitions des mots du monoïde libre*, Theoret. Comput. Sc., vol. 9, 1979, p. 17-26.
4. G. LALLEMENT, *Semigroups and Combinatorial Applications*, 1979, Wiley, New York.
5. E. LE REST et M. LE REST, *Sur les relations entre un nombre fini de mots*, 1979, Thèse 3^e cycle, Rouen.
6. J. F. PERROT, *Groupes de permutations associés aux codes préfixes finis* in *Permutations*, Actes du Colloque, 1972, Gauthier-Villars, Paris.
7. D. PERRIN, *Sur les groupes dans les monoïdes finis*, Actes du Colloque « Non Commutatives Methods in Algebraic and Geometric Combinatorics », A. DE LUCA, éd., Quaderni de la Ricerca Scientifica, vol. 109, 1981, p. 27-36.
8. M. P. SCHÜTZENBERGER, *Une théorie algébrique du codage*, C.R. Acad. Sc., t. 242, 1956, p. 862-864.
9. M. P. SCHÜTZENBERGER, *On Finite Monoids Having Only Trivial Subgroups*, Inform. and Control, vol. 8, 1965, p. 190-194.
10. M. P. SCHÜTZENBERGER, *A Property of Finitely Generated Submonoids of Free Monoids*, in *Algebraic Theory of Semigroups*, G. POLLACK, éd., North-Holland, 1979, p. 545-576.