JOURNAL OF ALGEBRA 60, 169–180 (1979)

Sur le théorème du défaut

J. BERSTEL,* D. PERRIN,† J. F. PERROT,* ET A. RESTIVO‡

* *Université Paris 6*; † *Université de Rouen*; ‡ *Universita di Palermo*

Communicated by P. M. Cohn

Received June 5, 1978

1. INTRODUCTION

Le théorème du défaut (cf. [3, 4, 7]) peut être énoncé sous la forme suivante: soit X une partie finie du monoïde libre A^* sur l'ensemble A. Si le sous-monoïde de A^* engendré par X n'est pas libre, il existe une partie Y de A^* qui contient moins d'éléments que X et qui engendre un sous-monoïde Q contenant X: $X \subset Q \subset A^*$; $\text{Card}(Y) \leqslant \text{Card}(X) - 1$.

Le but de cette note est de préciser ce résultat en étudiant l'ensemble des sous-monoïdes libres contenant une partie donnée X de A^*. Du fait que l'intersection de sous-monoïdes libres est encore libre (cf. sect. 2), cet ensemble possède un plus petit élément qui est le plus petit sous-monoïde libre contenant X; cet objet a déjà été considéré par Spehner [11] qui a donné un algorithme permettant de le calculer à partir d'un ensemble fini X.

Nous établissons d'abord que si le sous-monoïde P engendré par X n'est pas libre, la base Y du plus petit sous-monoïde libre contenant X vérifie:

$$\text{Card}(Y) \leqslant \text{Card}(X) - 1$$

Ce résultat précise le théorème du défaut énoncé plus haut. Nous examinons les généralisations possibles de ce résultat à d'autres classes de sous-monoïdes étudiées par ailleurs (sect. 4).

Le problème du calcul de la base Y du plus petit sous-monoïde libre contenant X a été résolu par Spehner [11] dans le cas où X est fini. Nous présentons ici un algorithme différent qui s'applique à des classes plus générales de parties de A^*. Il repose sur une suite de transformations de l'ensemble X apparentées aux transformations de Nielsen et reprend des constructions classiques en théorie des codes (cf. [5], qui contient une bibliographie sur ce point).

Nous déduisons de cet algorithme un résultat suivant lequel Y est encore reconnaissable si X l'est, c'est à dire si X est union de classes d'une congruence de A^* d'index fini (théorème 6.1).

0021-8693/79/090169-12$02.00/0

2. Definitions et Notations

Soit A un ensemble quelconque nommé alphabet, et A^* le monoïde libre engendré par A; On note aussi X^* le sous-monoïde de A^* engendré par une partie quelconque $X \subset A^*$. Pour deux parties R, S de A^*, on pose:

$$R^{-1}S = \{m \in A^* / Rm \cap S \neq \varnothing\}, \qquad SR^{-1} = \{m \in A^* \mid mR \cap S \neq \varnothing\}$$

Le *libérateur* de R est, par définition l'ensemble:

$$\mathscr{L}(R) = R^{-1}R \cap RR^{-1}$$

Si P est un sous-monoïde, on a toujours l'inclusion $P \subseteq \mathscr{L}(P)$ et on rapelle le résultat suivant dû à Schützenberger [10] et démontré, par exemple, en [1]:

Proposition 2.1. *Un sous-monoide $P \subset A^*$ est libre ssi $P = \mathscr{L}(P)$.*

Du fait que $\mathscr{L}(P \cap Q) \subseteq \mathscr{L}(P) \cap \mathscr{L}(Q)$, on déduit qu'une intersection de sous-monoïdes libres est encore libre (résultat retrouvé ultérieurement par Tilson [12]); en particulier, il existe donc un plus petit sous-monoïde libre contenant une partie donnée.

3. Théorème du Défaut

Notre lemme principal s'énonce comme suit:

Lemme 3.1. *Soit X une partie donnée de A^* et soit Y la base du plus petit sous-monoide libre P contenant X, de sorte que:*

$$X \subseteq P \subseteq A^*, \qquad \textit{avec} \quad P = Y^*.$$

Tout élément de Y est initiale et terminale d'au moins un mot dans X; c'est à dire que l'on a:

$$Y \subseteq XP^{-1} \cap P^{-1}X$$

Démonstration. Supposons la conclusion fausse, et prenons un $y \in Y$ tel que, par exemple:

$$yY^* \cap X = \varnothing.$$

Nous montrons qu'alors $P = Y^*$ n'est pas minimal. Soit:

$$Z = \{zy^i \mid z \in Y - y, i \geqslant 0\} \cup (Y - y)y^*$$

Comme $X \subseteq 1 \cup (Y - y)Y^*$ Z^* et $y \notin Z^*$, on a $X \subseteq Z^* \subset Y^*$. Par ailleurs,

Z engendre librement Z^*. En effet, tout mot x dans Z possède une factorisation unique de la forme

$$x = x_1 x_2 \cdots x_n , \qquad x_1 ,..., x_n \in Y, \qquad x_1 \neq y,$$

et s'écrit donc de manière unique sous la forme:

$$x = z_1 y^{p_1} z_2 y^{p_2} \cdots z_r y^{p_r}, \quad z_1 ,..., z_r \in Y - y, p_i \geqslant 0. \quad \blacksquare$$

Nous utilisons le lemme de la facon suivante: soit α: $X - 1 \to Y$ l'application définie par:

$$\alpha(x) = y \qquad \text{si} \quad x \in yY^*$$

Elle est partout définie parce que $X \subseteq Y^*$ et elle est univoque car Y engendre librement Y^*. Le Lemme 1 dit alors que α est surjective; il en résulte que si X est fini, alors $\mathrm{Card}(X) \geqslant \mathrm{Card}(Y)$. Plus précisément:

THÉORÈME 3.2. *Soit X une partie donnée d'un monoïde libre A^* et soit Y la base du plus petit sous-monoïde libre contenant X. Si X n'engendre pas librement X^*, alors*

$$\mathrm{Card}(Y) \leqslant \mathrm{Card}(X) - 1.$$

Démonstration. Par hypothèse, il existe deux mots de X vérifiant

$$x_1 x_2 \cdots x_n = x_1' x_2' \cdots x_m' \qquad x_i , x_i' \in X, x_1 \neq x_1' .$$

On en tire $\alpha(x_1) = \alpha(x_1')$, donc α n'est pas injective, ce qui prouve l'inégalité annoncée. $\blacksquare$

Ce résultat entraine a fortiori que tout sous-monoïde engendré par un système générateur non libre X est contenu dans un sous-monoïde ayant strictement moins de générateurs que X (Théorème 1 de Ehrenfeucht et Rozenberg [3]).

Donnons comme cas particulier un résultat maintes fois retrouvé:

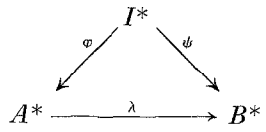
EXEMPLE. Si $X = \{x_1 , x_2\}$ et si X n'est pas libre, alors x_1 et x_2 sont puissance d'un même mot y:

$$x_1 = y^p, \qquad x_2 = y^q.$$

Dans un contexte voisin, le Théorème 1 est connu sous le nom de théorème du défaut: avec A. Lentin, appelons *équation* tout couple (f, f') de mots d'un monoïde libre I^* engendré par un ensemble I et *solution* de cette équation un morphisme:

$$\varphi: I^* \to A^*$$

tel que $\varphi(f) = \varphi(f')$. Si $\psi: I^* \to B^*$ est une autre solution de l'équation, alors ψ *procède* de φ s'il existe un morphisme λ faisant commuter le diagramme suivant:



Dans ce cas, les mots $\psi(i)$ $(i \in I)$ se décomposent en produits de mots $\lambda(a)$, avec $a \in A$, la forme de ces produits étant donnée par le solution "primitive" ψ. Le résultat suivant est établi en [4] (cf. aussi [7]):

THÉORÈME DU DÉFAUT. *Si $f \neq f'$, alors pour toute solution,*

$$\psi: I^* \to B^*$$

de l'équation (f, f'), il existe une solution $\varphi: I^* \to A^*$ telle que ψ procède de φ et que:

$$\mathrm{Card}(A) \leqslant \mathrm{Card}(I) - 1.$$

Démonstration. Soit $X = \psi(I) \subset B^*$ l'image de l'alphabet I par ψ et Y la base du plus petit sous-monoïde libre contenant X. On a:

$$\mathrm{Card}(Y) \leqslant \mathrm{Card}(X) \leqslant \mathrm{Card}(I)$$

et l'une au moins de ces inégalités est stricte: en effet, si la restriction de ψ à I n'est pas injective, on a: $\mathrm{Card}(X) \leqslant \mathrm{Card}(I) - 1$; si elle est injective, l'égalité $\psi(f) = \psi(f')$ avec $f \neq f'$ entraine que $X^* = \psi(I^*)$ n'est pas librement engendré par X et, d'après le Théorème 3.2, il vient $\mathrm{Card}(Y) \leqslant \mathrm{Card}(X) - 1$.

Soit alors λ une bijection d'un ensemble quelconque A sur Y, étendue à A^* et:

$$\varphi = \lambda^{-1} \circ \psi$$

On a bien $\mathrm{Card}(A) \leqslant \mathrm{Card}(I) - 1$ et ψ procède de φ. ∎

Remarque. Si, au lieu du Théorème 3.2, on applique au couple X, Y ci-dessus le Lemme 3.1, on en déduit que toute solution $\psi: I^* \to B^*$ procède d'une solution $\varphi: I^* \to A^*$ telle que toute lettre de A soit initiale et terminale d'au moins un mot de $\varphi(I)$. Cet énoncé est, lui aussi, établi en [4].

4. GÉNÉRALISATIONS

On peut chercher à étendre le Lemme 3.1 à d'autres familles de sous-monoïdes (fermées par intersection) que les sous-monoïdes libres. Par exemple, les sous-

monoïdes *unitaires à droite* définies par la condition: $P = P^{-1}P$ forment une famille fermée par intersection contenue dans celle des sous-monoïdes libres.

La même démonstration que celle du Lemme 3.1 montre que si Y est la base du plus petit sous-monoïde unitaire contenant un ensemble X, tout élément de Y est terminal d'un élément de X. Cela implique l'inégalité:

$$\mathrm{Card}(Y) \leqslant \mathrm{Card}(X)$$

On n'a cependant pas d'analogue du Théorème 3.2, comme le montre l'exemple de $X = \{a, ab\}$, $Y = \{a, b\}$.

La situation est la même "mutatis mutandis" pour les sous-monoïdes unitaires à gauche définis par la condition $PP^{-1} = P$.

En revanche, pour les sous-monoïdes unitaires (à gauche *et* à droite) on n'a plus d'analogue au Lemme 3.1; ainsi, par exemple, pour $X = \{a, c, abc\}$, on obtient $Y = \{a, b, c\}$.

On a cependant encore une inégalité large: $\mathrm{Card}(Y) \leqslant \mathrm{Card}(X)$. En effet, si X est fini, alors Y est fini (puisqu'il est constitué de facteurs de mots de X) et il peut être obtenu de la facon suivante: considérons la suite

$$X = Z_0 \subset Z_1^* \subset \cdots \subset Z_n^* = Y^*$$

où Z_{2i+1}^* (resp. Z_{2i}^*) est le plus petit sous-monoïde unitaire à gauche (resp. à droite) contenant Z_{2i}^* (resp. Z_{2i-1}^*). Cette suite est nécéssairement stationnaire à partir d'un certain rang puisque chaque Z_i est constitue de facteurs de mots de X; si $Z_n = Z_{n+1}$, alors Z_n^* est unitaire à gauche et à droite et on a bien $Z_n = Y$ puisque chacun des Z_i est inclus dans Y^*.

Une autre généralisation possible du Lemme 3.1 concerne les sous-monoïdes à *délai de déchiffrage fini*. Rappelons en la définition (cf. [8, 9]): soit P un sous-monoïde de A^*, et X son ensemble générateur minimal. On dit que P a un délai de déchiffrage fini s'il existe un entier d tel que l'on ait:

$$X^d A^* \cap X^{-1}P \subset P$$

Le plus petit des entiers d pour lesquels cette inclusion est vraie est le délai de déchiffrage de P. Un sous-monoïde unitaire à droite a un délai de déchiffrage nul. Cette famille de sous-monoïdes n'est pas fermée par intersection infinie comme le démontre l'exemple suivant:

$$Y_n = ab^{n+1}b^* \cup \{a^{i+1}b^i \mid 0 \leqslant i \leqslant n\}$$

Le sous-monoïde Y_n^* est unitaire à gauche mais a un délai de déchiffrage égal à $n + 1$, comme on le vérifie; l'intersection $\bigcap_{n \geqslant 0} Y_n^*$ est engendrée par:

$$Z = \{a^{i+1}b^i \mid 0 \leqslant i\}$$

et Z^* a un délai de déchiffrage infini.

On a cependant, dans le cas des sous-monoïdes *finiment engendrés*, un analogue du Lemme 3.1 et aussi du Théorème 3.2.

Tout d'abord si X est fini, il existe un plus petit sous-monoïde à délai de déchiffrage fini (d.d.f.) Y^* qui contient X et Y est lui aussi fini. En effet, soit $\mathscr{D}$ l'ensemble des sous-monoïdes à d.d.f., engendrés par une partie de l'ensemble F des facteurs de mots de X, et qui contiennent X; cet ensemble est non vide (il contient A^*) et ne contient pas de chaines infinies ordonnées par inclusion. Comme $\mathscr{D}$ est fermé par intersection finie, il possède donc un plus petit élément, soit Y^*; pour tout sous-monoïde d.d.f. Q contenant X, on a $Q \cap F^* \in \mathscr{D}$ et donc $Y^* \subset Q$, ce qui montre que Y est le plus petit sous-monoïde d.d.f. contenant X.

Maintenant, parallèlement au Lemme 3.1, on montre que l'on a les inclusions:

$$Y \subset X(Y^*)^{-1} \cap (Y^*)^{-1}X.$$

Montrons par exemple que tout élément de Y est initiale d'un élément de X: si ce n'est pas le cas pour y on pose:

$$Z = (Y - y)y^*$$

On vérifie que si le délai de déchiffrage de Y est égal à d, celui de Z est égal à $d + 1$ et ceci entraine une contradiction puisque l'on a l'inclusion:

$$X \subseteq Z^* \subset Y^*$$

On déduit de cette propriété le fait que si X n'est pas d.d.f.:

$$\mathrm{Card}(Y) \leqslant \mathrm{Card}(X) - 1,$$

comme dans le Corollaire 1.

Cette inégalité précise un résultat de M. Linna [6] suivant lequel, si X n'est pas d.d.f., il existe un sous-monoïde d.d.f. Y^* tel que l'on ait l'inégalité ci-dessus.

5. Algorithme de Calcul

Dans cette section, nous construisons explicitement le plus petit sous-monoïde libre Y^* contenant une partie X donnée d'un monoïde libre. Cette construction sera utilisée dans la section suivante pour montrer que Y est reconnaissable si X l'est.

Soit X une partie fixée de A^*; définissons une suite S_n de sous-monoïdes de A^* par:

$$S_0 = X^*, \qquad S_{n+1} = [\mathscr{L}(S_n)]^* \qquad n \geqslant 0.$$

Il est clair que la suite est croissante. Posons:

$$S(X) = \bigcup_{n \geqslant 0} S_n$$

PROPOSITION 5.1. *$S(X)$ est le plus petit sous-monoïde libre de A^* contenant X.*

Démonstration. Soit Y la base du plus petit sous-monoïde libre Y^* contenant X. On a $S_n \subset Y^*$ pour tout n. En effet, ceci est vrai pour $n = 0$ et par récurrence, on a:

$$S_{n+1} = [\mathscr{L}(S_n)]^* \subseteq [\mathscr{L}(Y^*)]^* = Y^*,$$

car Y est libre. Par conséquent, $S(X) \subset Y^*$. D'autre part,

$$\mathscr{L}(S(X)) = \bigcup_{n \geqslant 0} \mathscr{L}(S_n) = S(X)$$

puisque la suite des S_n est croissante; le sous-monoïde $S(X)$ est donc libre, ce qui par minimalité de Y^*, implique $S(X) = Y^*$. ∎

Le calcul de Y à partir de X se ramène donc au calcul du libérateur de chacun des S_n. Nous allons voir comment on peut, étant donnée une partie Z de A^*, calculer un ensemble générateur du sous-monoïde $[\mathscr{L}(Q)]^*$, avec $Q = Z^*$. Cela nous permettra de calculer successivement un ensemble générateur de chacun des S_n et de résoudre ainsi le problème du calcul de Y.

Soit donc Z une partie de A^* et $Q = Z^*$. On définit deux suites de parties de A^* par:

$$U_0 = V_0 = \{1\}, \quad U_{j+1} = U_j^{-1}Z \cup Z^{-1}U_j, \quad V_{j+1} = ZV_j^{-1} \cup V_jZ^{-1}, \quad j \geqslant 0.$$

Le calcul de ces suites répond au problème posé puisqu'on a le résultat suivant:

PROPOSITION 5.2. *Soient $U = \bigcup_{i \geqslant 0} U_i$ et $V = \bigcup_{j \geqslant 0} V_j$. On a:*

$$[\mathscr{L}(Q)]^* = (U \cap V)^*$$

c'est à dire que $\mathscr{L}(Q)$ et $U \cap V$ engendrent le même sous-monoïde.

La démonstration fait appel à plusieurs lemmes. Nous donnons d'abord quelques règles de calcul qui serviront constamment dans la suite:

LEMME 5.3. *Soient R, S, T des parties d'un monoïde, M, et soit Q un sous-monoïde de M. Alors*

$$(RS)^{-1}T = S^{-1}(R^{-1}T);\ R(ST)^{-1} = (RT^{-1})S^{-1};$$
$$(R^{-1}S)T^{-1} = R^{-1}(ST^{-1});$$
$$R \subseteq S \Rightarrow T^{-1}R \subseteq T^{-1}S,\ R^{-1}T \subseteq S^{-1}T;$$
$$(Q^{-1}Q)^{-1}Q = Q^{-1}Q = (Q^{-1}Q)Q; \tag{2}$$
$$RQ \cap SQ^{-1} \subseteq (R \cap SQ^{-1})Q;\ QR \cap Q^{-1}S \subseteq Q(R \cap Q^{-1}S). \tag{3}$$

Prouvons par exemple le première des formules (3). Soit $m \in RQ \cap SQ^{-1}$. Alors d'une part $m = rq$ avec $r \in R$, $q \in Q$, et d'autre part $m\bar{q} \in S$ pour un $\bar{q} \in Q$. Par conséquent $r(q\bar{q}) \in S$, et comme $q\bar{q} \in Q$, on a $r \in SQ^{-1}$, d'où $m = rq \in (R \cap SQ^{-1})Q$. ▮

Posons, pour alléger l'écriture,

$$\overline{U}_j = U_0 \cup U_1 \cup \cdots \cup U_j; \qquad \overline{V}_j = V_0 \cup V_1 \cup \cdots \cup V_j$$

LEMME 5.4. *Pour tout* $j \geqslant 0$, $U_{j+1} \subseteq (\overline{U}_j Q)^{-1} Z$ *et* $V_{j+1} \subseteq Z(Q\overline{V}_j)^{-1}$.

Preuve. Par récurrence sur j. Pour $j = 0$, l'inclusion est vraie puisque $U_1 = V_1 = Z$ et $Z \subset Q^{-1}Z$. Si $j > 0$, alors

$$\begin{aligned} U_{j+1} &= U_j^{-1}Z \cup Z^{-1}U_j \subseteq U_j^{-1}Z \cup Z^{-1}((\overline{U}_{j-1}Q)^{-1})Z \\ &= U_j^{-1}Z \cup (\overline{U}_{j-1}QZ)^{-1}Z = (U_j \cup \overline{U}_{j-1}QZ)^{-1}Z. \end{aligned}$$

Or $U_j \cup \overline{U}_{j-1}QZ \subseteq U_jQ \cup \overline{U}_{j-1}Q = \overline{U}_jQ$, ce qui prouve la première inclusion. La deuxième se démontre de la même facon. ▮

LEMME 5.5. *On a* $U = Q^{-1}U$, $V = VQ^{-1}$, $Q^{-1}Q = UQ, QQ^{-1} = QV$.

Preuve. Par définition, $Z^{-1}U_j \subseteq U_{j+1}$ pour $j \geqslant 0$, donc $Z^{-1}U \subseteq U$. De la même manière, $U^{-1}Z \subseteq U_{j+1}$ $(j \geqslant 0)$ implique

$$U^{-1}Z \subseteq U \tag{4}$$

De l'inclusion $Z^{-1}U \subset U$, on obtient par récurrence

$$(Z^{n+1})^{-1}U = (Z^n)^{-1}(Z^{-1}U) \subseteq (Z^n)^{-1}U \subseteq U \qquad n \geqslant 0$$

d'où, puisque $Q = Z^*$, $Q^{-1}U \subseteq U$. L'inclusion $U \subseteq Q^{-1}U$ résulte de ce que $1 \in Q$. Ceci prouve la première égalité. La deuxième se démontre de la même facon.

Pour établir la troisième formule, nous vérifions par récurrence les inclusions

$$U_j \subseteq Q^{-1}Q, \qquad j \geqslant 0 \tag{5}$$

le cas $j = 0$ étant évident. Par le Lemme 3 et par l'hypothèse d'induction, on obtient

$$U_{j+1} \subseteq (\overline{U}_jQ)^{-1}Z \subseteq ((Q^{-1}Q)Q)^{-1}Z.$$

Par (2), et puisque $Z \subseteq Q$, il s'en suit que

$$U_{j+1} \subseteq (Q^{-1}Q)^{-1}Z \subseteq (Q^{-1}Q)^{-1}Q = Q^{-1}Q.$$

L'inclusion $U \subset Q^{-1}Q$ découle immédiatement de (5), d'où

$$UQ \subset (Q^{-1}Q)Q = Q^{-1}Q.$$

Réciproquement, soit $m \in Q^{-1}Q$, de sorte que $qm = q' \in Q$ pour un $q \in Q$. Comme $1 \in UQ$, nous prouvons que $m \in UQ$ pour $m \neq 1$, et procédons pour cela par récurrence sur la longueur $| qq' |$. Si $| qq' | = 0$, alors $m \in Q \subset UQ$. Sinon, comme $Q = Z^*$, il existe deux mots h, h' tels que

$$q = q_1 h, \qquad m = h' q_2 , \qquad \text{avec} \quad q_1 , q_2 \in Q \quad \text{et} \quad hh' \in Z.$$

Comme $m \neq 1$, la première équation implique par récurrence $h \in UQ$, d'où par (4)

$$h' \in (UQ)^{-1}Z = Q^{-1}(U^{-1}Z) \subseteq Q^{-1}U = U$$

Par conséquent, $m = h'q_2 \in UQ$, ce qu'il fallait démontrer. Nous achevons maintenant la preuve de la Proposition 5.2: on a, d'après le Lemme 5.6

$$U \cap V \subseteq UQ \cap QV = Q^{-1}Q \cap QQ^{-1} = \mathscr{L}(Q),$$

donc $(U \cap V)^* \subset \mathscr{L}(Q)$. Réciproquement,

$$\mathscr{L}(Q) = Q^{-1}Q \cap QQ^{-1} = UQ \cap QQ^{-1} \subseteq (U \cap QQ^{-1})Q$$

par le Lemme 5.6 et l'assertion (3) du Lemme 5.3; et de même

$$U \cap QQ^{-1} = U \cap QV = Q^{-1}U \cap QV \subset Q(Q^{-1}U \cap V) = Q(U \cap V),$$

d'où

$$\mathscr{L}(Q) \subseteq Q(U \cap V)Q \tag{6}$$

Comme $Z \subseteq U \cap V$, on a $Q \subseteq (U \cap V)^*$, donc par (6)

$$\mathscr{L}(Q) \subseteq (U \cap V)$$

ce qui achève la vérification. ∎

Remarque. Les calculs qui précèdent se simplifient beacoup si, au lieu du plus petit sous-monoïde libre contenant X, on cherche le plus petit sous-monoïde *unitaire* Y^* contenant X (cf. sect. 4). Si on définit en effet la suite:

$$T_0 = X^*, \quad T_{n+1} = [T_n^{-1}T_n]^* \quad n \geqslant 0$$

on a alors $Y^* = \bigcup_{n \geqslant 0} T_n$. D'autre part, si $Q = Z^*$, comme dans la Proposition 5.2, alors:

$$[Q^{-1}Q]^* = U^* \text{ avec } U = \bigcup_{i \geqslant 0} U_i ;$$

En effet, d'après le Lemme 5.5 $Q^{-1}Q = UQ$ et Q est inclus dans U^* puisque U contient Z.

6. Cas des parties reconnaissables

Rappelons quelques définitions de la théorie des automates (cf. [2] par exemple):

Une partie R d'un monoïde M est *reconnaissable* s'il existe un morphisme

$$\varphi: M \to F$$

sur un monoïde *fini* F qui sature R:

$$\varphi^{-1}\varphi(R) = R.$$

La famille des parties reconnaissables est fermée par toutes les opérations booléennes et, de plus, si S est reconnaissable alors $R^{-1}S$ et SR^{-1} sont reconnaissables pour toute partie R de M. Plus précisément, si $\varphi: M \to F$ sature S, il sature encore ces deux ensembles puisque si $\varphi(m) = \varphi(n)$ et que $m \in R^{-1}S$, il existe par définition un $r \in R$ tel que

$$rm \in S.$$

Mais alors $\varphi(rm) = \varphi(rn) \in \varphi(S)$, ce qui entraine $rn \in S$ et donc $n \in R^{-1}S$. Si $M = A^*$, le théorème de Kleene dit que la famille des parties reconnaissables coïncide avec celle des parties *rationnelles*, qui est par définition la plus petite famille de parties contenant les parties finies et fermée par les trois opérations suivantes: l'*union*, le *produit* et l'*étoile* (i.e. le passage au sous-monoïde engendré) (cf. [2, p. 175]).

Ainsi, en particulier, si X est reconnaissable, X^* l'est encore; de plus, si X est l'ensemble générateur minimal de X^*, la réciproque est vraie; en effet:

$$X = X^+ \backslash X^+X^+, \qquad \text{avec} \quad X^+ = X^* \backslash 1.$$

Nous établissons maintenant le résultat suivant:

Théorème 6.1. *Soit X une partie de A^* et Y la base du plus petit sous-monoïde libre de A^* contenant X. Si X est reconnaissable, Y l'est encore.*

Considérons, pour démontrer le théorème, une partie Z de A^* et soient U_j, V_j, U, V les parties de A^* définies à partir de Z au paragraphe précédent.

Lemme 6.2. *Si Z est saturé par φ, alors $U \cap V$ est saturé par φ.*

Démonstration. Par hypothèse $U_1 = V_1 = Z$ est saturé par φ. Par récurrence,

$$U_{j+1} = U_j^{-1}Z \cup Z^{-1}U_j, \qquad j \geq 0$$

est saturé par φ. Par conséquent

$$U = \bigcup_{j\geq 0} U_j \quad \text{et} \quad V = \bigcup_{j\geq 0} V_j$$

sont saturés par φ, donc $U \cap V$ est saturé par φ. ∎

Le Lemme 6.2 et la Proposition 5.2 fournissent donc, à partir d'un système générateur Z saturé par φ de Q, un système générateur saturé par φ de $[\mathscr{L}(Q)]^*$, à savoir $U \cap V$.

PROPOSITION 6.3. *Soit X une partie de A^* saturée par φ. Alors il existe une partie Y' saturée par φ qui engendre le plus petit sous-monoïde libre Y^* contenant X.*

Démonstration. En vertu du lemme précédent, la partie

$$X_1 = U \cap V$$

construite à partir de $Z = X$ est saturée par φ et

$$S_1 = \mathscr{L}(X^*)^* = X_1^*.$$

Itérant ce procédé, on obtient pour tout n une partie $X_n \subset A^*$ saturée par φ telle que:

$$S_n = \mathscr{L}(S_{n-1})^* = X_n^*.$$

Posons alors $Y' = \bigcup_{n\geq 1} X_n$; on a $Y^* = Y'^*$ et Y' est saturé par φ. ∎

Cette proposition établit le Théorème 6.1 puisque si X est reconnaissable, il existe une partie reconnaissable Y' qui engendre Y^*. Cela montre que Y^* et donc Y sont reconnaissables.

Remarque. Le calcul développé au Section 5 est particulièrement intéressant lorsque X est reconnaissable. En effet, dans ce cas, tout le calcul peut être effectué dans le monoïde fini $F = \varphi(A^*)$ puisque chacun des ensembles générateurs X_n que l'on construit est saturée par φ. En particulier Y' et également Y peuvent être calculés en un nombre fini d'étapes - le résultat étant un morphisme $\psi: A^* \to G$ sur un monoïde fini G et une partie H de G telle que $Y = \psi^{-1}(H)$.

RÉFÉRENCES

1. P. M. COHN, "Free Rings and Their Relations," Academic Press, New York London, 1971.

2. S. EILENBERG, "Automata Languages and Machines," Vol. A, Academic Press, New York/London, 1974.
3. A. EHRENFEUCHT AND G. ROZENBERG, On simplifications of PDOL systems, *in* "Proceedings of a Conference on Theoretical Computer Science, Univ. of Waterloo, 1977," pp. 81–87.
4. A. LENTIN, "Equations dans les monoïdes libres," Gauthier–Villars, Paris, 1972.
5. A. DE LUCA, A note on variable length codes, *Inform. Contr.* **32** (1976), 263–271.
6. M. LINNA, The decidability of the D0L prefix problem, *Internat. J. Comput. Math. A* **6** (1977), 127–142.
7. G. S. MAKANIN, Sur le rang des équations sans coefficients à quatre inconnues dans un demi groupe libre, *Mat. Sb.* **100** (1976), 285–311 (en russe).
8. M. NIVAT, Eléments de la théorie générale des codes, *in* "Automata Theory" (E. R. Caianiello, Ed.), pp. 278–294, Academic Press, New York/London, 1966.
9. J. F. PERROT, La théorie des codes à longueur variable, *in* "Theoretical Computer Science," pp. 27–44, Lecture Notes in Computer Science No. 48, Springer–Verlag, Berlin/New York, 1976.
10. M. SCHÜTZENBERGER, Une théorie algébrique du codage, "Séminaire Dubreil," exposé No. 15, Algèbre et théorie des nombres, année 1955–56.
11. J. C. SPEHNER, Quelques constructions et algorithmes relatifs aux sous-monoïdes d'un monoïde libre, *Semigroup Forum* **9** (1975), 334–353.
12. B. TILSON, The intersection of free submonoids of free monoids is free, *Semigroup Forum* **4** (1972), 345–350.