RAIRO. INFORMATIQUE THÉORIQUE ET APPLICATIONS

BODONIRINA RATOANDROMANANA

Codes et motifs

RAIRO. Informatique théorique et applications, tome 23, n° 4 (1989), p. 425-444

<http://www.numdam.org/item?id=ITA_1989__23_4_425_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 23, n° 4, 1989, p. 425 à 444)

CODES ET MOTIFS (*)

par Bodonirina RATOANDROMANANA (1)

Communiqué par J.-E. PIN

Résumé. – *Nous prouvons, pour deux codes X et Y, l'équivalence entre l'égalité* $XY = YX$ *et l'existence de deux entiers strictement positifs i et j tels que* $X^i = Y^j$. *Si, de plus, l'un des codes est singulier, ces deux conditions sont équivalentes à l'existence d'un motif commun aux deux codes,* i. e. *à l'existence d'un code Z tel que X et Y soient des puissances de Z. Ensuite, nous montrons pour tout langage non vide L commutant avec un code préfixe ou circulaire X, l'existence d'un code Y, d'un entier j et de* $I \subset \mathbb{N}$ *tels que* $L = \bigcup_{i \in I} Y^i$ *et* $X = Y^j$.

En particulier, si X est un code circulaire alors $j = 1$ *et si L est un code alors L est une puissance de X.*

Abstract. – *We prove, for two codes X and Y, the equivalence of the equality* $XY = YX$ *and the existence of two positive integers i and j such that* $X^i = Y^j$. *Moreover, if one of them is singular, these two conditions are equivalent to the existence of a code Z such that X and Y are powers of Z. Then, we show for each non empty language L commuting with a prefix or circular code X, the existence of a code Y, an integer j and* $I \subset \mathbb{N}$ *such that* $L = \bigcup_{i \in I} Y^i$ *and* $X = Y^j$.

In particular, if X is a circular code then $j = 1$ *and if L is a code, L is a power of X.*

I. INTRODUCTION

Un des résultats de base de la théorie combinatoire des mots est dû à Lyndon et Schutzenberger [7]. C'est l'équivalence pour des mots u et v des conditions suivantes :

(1) $uv = vu$

(2) Il existe un mot w et deux entiers i et j tels que $u = w^i$ et $v = w^j$

(3) Il existe deux entiers s et t vérifiant $u^s = v^t$.

(*) Reçu juillet 1987, version finale mai 1988.

Ce travail est supporté par le P.R.C. Mathématiques et Informatique.

(1) C.N.R.S. – U.A. 369, Université de Lille-Flandres-Artois, 59655 Villeneuve-d'Ascq Cedex.

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-3754 89/04 425 20/$4.00/

Perrin [9] a étendu ce résultat sur les mots aux codes préfixes, en montrant que l'ensemble des codes préfixes forme un monoïde libre pour le produit ensembliste.

De façon plus générale, deux éléments d'un monoïde libre commutent si et seulement si ils sont puissances d'un même élément [4].

Un résultat similaire a été établi par Bergman [3], pour les K-algèbres libres :

Soient K un anneau commutatif, A un ensemble et $K\langle A\rangle$ la K-algèbre libre de A; alors, l'ensemble $C(x)=\{y\in K\langle A\rangle / xy=yx\}$ où $x\in K\langle A\rangle$ est un anneau polynomial en une seule variable sur K.

Le but de ce papier est de poursuivre ces extensions à des ensembles de mots. Plus précisément, nous montrons que si deux codes commutent, ils sont prémotifs d'un même code *i. e.* il existe deux puissances égales des deux codes, et réciproquement (proposition 7). En plus, si l'un des deux codes est singulier, alors ils sont puissances d'un même code. Ensuite, nous montrons pour tout langage non vide L commutant avec un code préfixe ou circulaire X, l'existence d'un code Y, d'un entier j et de $I\subset\mathbb{N}$ tels $L=\bigcup_{i\in I} Y^i$ et $X=Y^j$ (propositions 21 et 26).

II. NOTATIONS ET DEFINITIONS

Nous supposons le lecteur familier avec les notions de codes [2, 8, 10]. $\mathbb{N}$ désigne l'ensemble des entiers naturels.

Soit A un ensemble fini de lettres que nous appelons *alphabet.*

Pour tout mot u sur un alphabet A, $|u|$ désigne la longueur de u et ε est le seul mot de longueur nulle.

Deux mots u et v sont dits *conjugués* s'il existe deux mots x et y tels que $u=xy$ et $v=yx$.

Toute partie (finie) de A^* est un langage (fini). Pour tout langage L, tout entier n, nous noterons

$$L_n=\{u\in L/|u|\leqq n\},$$

$$l(L)=\min\{|u|/u\in L\} \quad \text{si} \quad L\neq\varnothing \quad \text{et} \quad L_{\min}=L_{l(L)}.$$

Le produit de deux langages X et Y est dit *non ambigu* (noté $\pi(X, Y)$) si, pour tous x_1, $x_2\in X$ et y_1, $y_2\in Y$, l'égalité $x_1y_1=x_2y_2$ implique $x_1=x_2$ et $y_1=y_2$.

Un *monoïde* est un ensemble muni d'une opération binaire associative et qui a un élément neutre.

Soit M un monoïde. Pour $x, y \in M$ nous définissons

$$x^{-1}y = \{ z \in M / xz = y \}$$

et

$$xy^{-1} = \{ z \in M / x = zy \}.$$

Pour des sous-ensembles X et Y de M, cette notation peut s'étendre à

$$X^{-1}Y = \bigcup_{x \in X} \bigcup_{y \in Y} x^{-1}y$$

et

$$XY^{-1} = \bigcup_{x \in X} \bigcup_{y \in Y} xy^{-1}.$$

Un monoïde (ou semi-groupe) M est *stable* si, pour tous X, Y, Z on a X, Y, XZ, $ZY \in M$ implique $Z \in M$.

Comme caractérisation d'un monoïde libre, nous utiliserons celle de Levi:

LEMME [4, 5, 6] : *Un monoïde M est libre si et seulement si:*

(1) *il existe un homomorphisme μ de M dans le monoïde additif des entiers naturels tel que $\mu^{-1}(0) = \{\varepsilon\}$,*

(2) *pour tous X, Y, Z, T dans M tels que $XY = ZT$, si $\mu(X) \geqq \mu(Z)$ il existe un $U \in M$ tel que $X = ZU$ et $T = UY$* i. e. *M est équidivisible.*

Soient X, Y, Z, T des langages non vides. Alors $XY = ZT$ implique $X_{\min} Y_{\min} = Z_{\min} T_{\min}$. De plus, si $l(Y) = l(T)$ alors $X_{\min} = Z_{\min}$ [11].

Dans le cas des sous-monoïdes d'un monoïde libre, la notion de monoïde stable est équivalente à celle de monoïde libre [2].

Un langage $X \subset A^+$ est un *code* si, pour tous n, $m \geqq 1$, $x_1, x_2, \ldots, x_n$, $y_1, y_2, \ldots, y_m \in X$, l'égalité $x_1 x_2 \ldots x_n = y_1 y_2 \ldots y_m$ implique $n = m$ et $x_i = y_i$ pour tout $i \in [1, n]$.

Pour un alphabet A, $X = A$ est un code. De façon plus générale, l'ensemble des mots de même longueur sur un alphabet constitute un code appelé code *homogène.*

Rappelons que le sous-monoïde X^* engendré par un code X est stable, et que X est un code si et seulement si X^i est un code ($i > 0$) [2].

Dans toute la suite, nous excluerons le cas des codes vides.

Un langage P est un *prémotif* de L si L est une union de puissances de P, *i. e.* $\exists I \subset \mathbb{N}$ tel que $L = \bigcup_{i \in I} P^i = P^I$.

Un langage est *primitif* s'il est son seul prémotif. Un *motif* est un prémotif primitif.

On montre facilement que si $X = L^I$ est un code, alors L est un code et cardinal $(I) = 1$.

Avec ces notions nouvellement introduites par Autebert, Boasson et Latteux [1], nous pouvons établir :

LEMME 1 : *Soient X et Y deux codes. Les conditions suivantes sont équivalentes :*

(1) *Il existe deux entiers $i, j \geqq 1$ tels que $X^i = Y^j$*

(2) *X et Y sont prémotifs d'un même langage non réduit au mot vide.*

Démonstration: L'implication (1) $\Rightarrow$ (2) est évidente.

Pour la réciproque, supposons qu'il existe $I, J \subset \mathbb{N}$, $I \neq \{0\}$ tels que $X^I = Y^J$.

Remarquons que si $X^I = Y^J$, comme X et Y sont des codes, on a $O \in I \Leftrightarrow O \in J$. Ainsi a-t-on $X^I = Y^J \Leftrightarrow X^{I-\{0\}} = Y^{J-\{0\}}$. D'où on peut supposer que $O \notin I$ et $O \notin J$.

Soient i_1, le plus petit élément de I et j_1 celui de J.

Il est facile de montrer que $X^{i_1} \cap Y^{j_1} \neq \varnothing$. En particulier, si $x_0 \in X_{\min}$, $x_0^{i_1} \in Y^{j_1}$ d'où l'existence de $y_1, y_2, \ldots, y_{j_1} \in Y$ tels que $x_0^{i_1} = y_1 \ldots y_{j_1}$.

Montrons que $X^{i_1} \subset Y^{j_1}$.

Soit $x_1 \ldots x_{i_1} \in X^{i_1}$ avec $x_k \in X$ pour $1 \leqq k \leqq i_1$. Comme $X^{i_1} \subset Y^J$, il existe un $j_s \in J$ $(j_s \geqq j_1)$ tel que $x_1 \ldots x_{i_1} \in Y^{j_s}$. D'où $x_1 \ldots x_{i_1} = z_1 \ldots z_{j_s}$ avec $z_k \in Y$ pour $1 \leqq k \leqq j_s$.

Ainsi $x_1 \ldots x_{i_1} x_0^{i_1} = z_1 \ldots z_{j_s} y_1 \ldots y_{j_1} \in Y^{j_s} Y^{j_1} = Y^{j_1} Y^{j_s}$. En utilisant les faits que $Y^{j_s} \subset X^I$, $Y^{j_1} \subset X^I$ et X code, on obtient $x_1 \ldots x_{i_1} \in Y^{j_1}$ et $j_s = j_1$.

De la même façon, on démontre que $Y^{j_1} \subset X^{i_1}$.
Ainsi $X^{i_1} = Y^{j_1}$ avec $i_1, j_1 \geqq 1$. ■

Terminons par quelques définitions de codes particuliers.

Un langage X sur un alphabet A est dit *préfixe* s'il satisfait $XA^+ \cap X = \varnothing$.

Rappelons que le produit de deux codes n'est pas, en général, un code [2]. Cependant, Perrin [9] a montré que le produit de deux codes préfixes est un code préfixe. Plus précisément, l'ensemble des codes préfixes avec $\{\varepsilon\}$, muni du produit ensembliste, est un monoïde libre [4, 9].

Un mot $w \in A^*$ est *préfixe propre* d'un mot $x \in A^*$, s'il existe un mot $u \in A^+$ tel que $x = wu$.

Soit $X \subset A^*$, $x \in X$ est dit *singulier à gauche* dans X si x n'a pas de préfixes propres dans X et s'il n'est pas préfixe propre d'un élément de X. Notons $g(X)$ l'ensemble des mots singuliers de X dans X.

Soit $X \subset A^*$, X est *singulier à gauche* (resp. préfixe) si et seulement si $g(X) \neq \varnothing$ (resp. $g(X) = X$). D'où tout code préfixe est un code singulier à gauche.

Dans toute la suite, nous appelons *code singulier* tout code singulier à gauche.

Un langage $X \subset A^*$ est un *code circulaire* si pour tous n, $m \in \mathbb{N}$, $p \in A^*$, $s \in A^+$ et $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m \in X$, les égalités $sx_2 \ldots x_n p = y_1 \ldots y_m$ et $x_1 = ps$ impliquent $n = m$, $p = \varepsilon$ et $x_i = y_i$ pour tout $i \in [1, m]$.

Un code circulaire est un code mais la réciproque n'est pas toujours vraie.

Rappelons qu'un code circulaire ne contient pas de mots conjugués distincts et que tous les mots d'un code circulaire sont primitifs [2]. Par conséquent, tout code circulaire est primitif.

III. RÉSULTATS

Montrons d'abord :

LEMME 2 : *Soient X, Y deux langages non vides tels que $YX \subset XY$. Alors pour tout $x \in X$, $y \in Y$ il existe deux suites $(x_n)_{n \in N}$, $(y_n)_{n \in N}$ avec $x_0 = x$, $y_0 = y$, $x_n \in X$, $y_n \in Y$ et tels que*

(1) *pour tout $i \in N$*

$$y_0 x_0 x_1 \ldots x_i = x_1 \ldots x_i x_{i+1} y_{i+1}$$

(2) $\forall r, s \in \mathbb{N} : i_s < i_r$

$$x_{i_s} y_{i_s} x_{i_s} \ldots x_{i_r - 1} = x_{i_s} \ldots x_{i_r} y_{i_r}$$

(3) $\exists\, k, r \in \mathbb{N}$: $(x_{i_r} y_{i_r})^k \in X^+$

$$(y_0 x_0)^k x_1 \ldots x_{i_r - 1} = x_1 \ldots x_{i_r - 1} (x_{i_r} y_{i_r})^k \in X^+.$$

Démonstration: On const. les suites $(x_n)_{n\in N}$, $(y_n)_{n\in N}$ par récurrence. En effet, comme $YX \subset XY$ l'on a:

$$\forall i \in \mathbb{N}\ \exists\, x_{i+1} \in X, y_{i+1} \in Y \text{ tels que}$$

$$(\bigstar) \qquad y_i x_i = x_{i+1} y_{i+1}$$

d'où

$$(\bigstar\bigstar) \qquad \forall i \in \mathbb{N}, \quad x_i y_i x_i = x_i x_{i+1} y_{i+1}.$$

Par récurrence, en utilisant (*) et (**), on montre facilement (1) et (2).

Les mots $(x_n y_n)_{n\in N}$, définis par l'équation (*) ont tous la même longueur q. A étant fini, A^q est fini et donc il existe un nombre fini de factorisations des mots de A^q de la forme $x_n y_n$. D'où l'on trouvera un couple (r, s), $i_s < i_r$ vérifiant

$$x_{i_r} = x_{i_s}, \qquad y_{i_r} = y_{i_s}$$

et

$$x_{i_r} y_{i_r} x_{i_s} \ldots x_{i_r-1} = x_{i_s} \ldots x_{i_r-1} x_{i_r} y_{i_r}.$$

D'où il existe $t = x_{i_s} \ldots x_{i_r-1} \in X^+$ tel que $x_{i_r} y_{i_r} t = t x_{i_r} y_{i_r}$.

Comme $x_{i_r} y_{i_r}$ et t commutent, il existe un mot w, deux entiers k et l strictement positifs tels que $t = w^k$ et $x_{i_r} y_{i_r} = w^l$ [4].

Ainsi $(x_{i_r} y_{i_r})^k \in X^+$. Comme $xy = yz$ implique par récurrence $x^n y = y z^n$ pour tout n, en prenant $x = y_0 x_0$, $y = x_1 \ldots x_{i_r-1}$ et $z = x_{i_r} y_{i_r}$, nous retrouvons la propriété 1.

D'où $(y_0 x_0)^n x_1 \ldots x_{i_r-1} = x_1 \ldots x_{i_r-1} (x_{i_r} y_{i_r})^n$ pour tout n. En particulier si $n = k$, $(y_0 x_0)^k x_1 \ldots x_{i_r-1} = x_1 \ldots x_{i_r-1} (x_{i_r} y_{i_r})^k \in X^+$. ■

LEMME 3 : *Soient X un code et Y un langage tels que $YX \subset XY$ (ou $XY \subset YX$) et $X \cap Y \neq \varnothing$. Alors $X \subset Y$.*

Démonstration: Comme $X \cap Y \neq \varnothing$, il existe $y \in X \cap Y$.

Considérons un mot x de X. D'après le Lemme 2, il existe deux suites $(x_n)_{n\in N}$, $(y_n)_{n\in N}$, k, $r \in \mathbb{N}$ tels que $(x_{i_r} y_{i_r})^k \in X^+$ et

$$(yx)^k x_1 \ldots x_{i_r-1} = x_1 \ldots x_{i_r-1} (x_{i_r} y_{i_r})^k \in X^+.$$

X étant un code, $y = x_1$ et $x = y_1$ car $yx = x_1 y_1$. D'où $x \in Y$ et $X \subset Y$.

Dans le cas où $XY \subset YX$, on obtient le résultat en appliquant la première partie de l'énoncé aux images miroir de X et Y. ■

LEMME 4 : *Soient X un code et Y un langage non vide tels que $XY = YX$.*

Alors $X(Y-\{\varepsilon\}) = (Y-\{\varepsilon\})X$.

Démonstration: Si $Y=\{\varepsilon\}$ ou $\varepsilon \notin Y$, le problème est résolu.

Sinon posons $Y_1 = Y-\{\varepsilon\}$. D'où $X \cup XY_1 = X \cup Y_1 X$.

Montrons que $X \cap XY_1 = \varnothing$.

Supposons le contraire *i. e.* qu'il existe $w \in XY_1 \cap X$. Il existe $x \in X$, $y \in Y_1$ tels que $w = yx$. D'après le lemme 2, il existe deux suites $(x_n)_{n \in N}$, $(y_n)_{n \in N}$, k, $r \in \mathbb{N}$ tels que

$$(x_{i_r} y_{i_r})^k \in X^+$$

et

$$(yx)^k x_1 \ldots x_{i_r-1} = x_1 \ldots x_{i_r-1} (x_{i_r} y_{i_r})^k \in X^+.$$

D'où

$$w^k x x_1 \ldots x_{i_r-1} = (xy)^k x x_1 \ldots x_{i_r-1} = x (yx)^k x_1 \ldots x_{i_r-1}$$
$$= x x_1 \ldots x_{i_r-1} (x_{i_r} y_{i_r})^k \in X^+.$$

X étant un code, $w = x$ et $y = \varepsilon$ ce qui est contraire au fait que $y \in Y_1$. D'où $X \cap XY_1 = \varnothing$ et $XY_1 \subset Y_1 X$.

De façon similaire, on démontre que $X \cap Y_1 X = \varnothing$ et $Y_1 X \subset XY_1$. Par conséquent, $X(Y-\{\varepsilon\}) = (Y-\{\varepsilon\})X$. ■

Du lemme 3, on peut établir:

PROPOSITION 5 : *Soient X un code et Y un langage non vide ne contenant pas le mot vide tels que $YX \subset XY$. Alors il existe deux entiers strictement postiifs i et j tels que $X^i \subset Y^j$. En plus, si Y est un code, on a l'égalité.*

Démonstration: Posons $i = l(Y)$ et $j = l(X)$. Il est facile de montrer par récurrence que $Y^n X^m \subset X^m Y^n$ pour tous n, $m \in N$.

En particulier, pour $n = j$ et $m = i$, on obtient $Y^j X^i \subset X^i Y^j$.

Comme $\varepsilon \notin Y$ et $Y \neq \varnothing$, soient $y \in Y_{\min}$, $x \in X_{\min}$ d'où $y^j x^i \in Y^j_{\min} X^i_{\min} \subset Y^j X^i \subset X^i Y^j$.

Comme $|y^j| = |x^i| = l(X^i_{\min}) = l\ (Y^j_{\min})$, alors $y^j \in X^i$ et $x^i \in Y^j$ d'où $X^i \cap Y^j \neq \varnothing$. D'après le lemme 3, $X^i \subset Y^j$.

Si, en plus Y est un code, Y^j l'est aussi et $Y^j \subset X^i$. Par conséquent $X^i = Y^j$. ■

COROLLAIRE 6 : *Soient X un code et Y un langage contenant un mot non vide tels que $XY = YX$. Alors il existe deux entiers $i, j \geq 1$ tels que $X^i \subset Y^j$.*

Démonstration: D'après le lemme 4, $X(Y-\{\varepsilon\}) = (Y-\{\varepsilon\})X$. Comme Y contient un mot non vide, $Y-\{\varepsilon\}$ et X vérifient les hypothèses de la proposition 5. Ainsi, il existe deux entiers i, $j \geq 1$ tels que $X^i \subset (Y-\{\varepsilon\})^j \subset Y^j$. ■

PROPOSITION 7 : *Etant donnés deux codes X et Y sur un alphabet A, les conditions suivantes sont équivalentes:*

(1) $XY \subset YX$

(2) X et Y commutent

(3) X et Y sont prémotifs d'un même langage non réduit au mot vide

(4) Il existe deux entiers i, j ≥ 1 *tels que* $X^i = Y^j$.

Démonstration: On obtient l'équivalence entre (3) et (4) par le lemme 1.

La proposition 5 nous permet d'avoir (1) $\Rightarrow$ (4). Comme (2) $\Rightarrow$ (1), il suffit de montrer que (4) implique (2).

Il est facile de vérifier que $X_{\min}^i = Y_{\min}^j$. D'où

$$X_{\min}^{2i} = X_{\min} Y_{\min}^j X_{\min}^{i-1} = Y_{\min}^{2j} = Y_{\min} X_{\min}^i Y_{\min}^{j-1}.$$

Comme $X_{\min} \subset A^{l(X)}$ et $Y_{\min} \subset A^{l(Y)}$, nous pouvons en déduire que $X_{\min} Y_{\min} = Y_{\min} X_{\min}$.

Montrons par récurrence sur n que $(XY)_n = (YX)_n$.

C'est vrai pour $n = l(X) + l(Y)$.

Supposons que c'est vrai pour $p < n$ et montrons-la pour n.

Soient $x \in X$ et $y \in Y$ avec $n = |xy| > l(X) + l(Y)$, $x_0 \in X_{\min}$ et $y_0 \in Y_{\min}$. Alors $u = xyy_0^{j-1} x_0^{i-1} \in XY^j X^{i-1} = YX^i Y^{j-1}$. D'où il existe $y_1 \in Y$, $x_1 \in X$ et $z \in X^{i-1} Y^{j-1}$ tels que $u = y_1 x_1 z$. Ainsi $|z| \geq |y_0^{j-1} x_0^{i-1}| = k$.

Ce qui nous donne deux possibilités:

1. $|z| = k$, $xy = y_1 x_1 \in YX$.

2. $|z| > k$ et $|y_1 x_1| < n$ et par hypothèse de récurrence $y_1 x_1 = x_2 y_2$ avec $x_2 \in X$ et $y_2 \in Y$.

En plus $y_0^{j-1} x_0^{i-1} \in Y_{\min}^{j-1} X_{\min}^{i-1} = X_{\min}^{i-1} Y_{\min}^{j-1}$. D'où

$$u \in xy X^{i-1} Y^{j-1} \cap x_2 y_2 X^{i-1} Y^{j-1} \qquad \text{avec} \quad |x_2 y_2| < |xy|.$$

Si on prend $v \in Y$ et $w \in X$, $uv \in xy X^{i-1} Y^j \cap x_2 y_2 X^{i-1} Y^j$ et

$$uvw \in xy Y^j X^i \cap x_2 y_2 Y^j X^i = xy Y^{2j} \cap x_2 y_2 Y^{2j}.$$

Ainsi $uvwy^{j-1} \in x\, Y^{3j} \cap x_2\, Y^{3j} = x\, X^{3i} \cap x_2\, X^{3i}$. Comme X est un code alors $x = x_2$. D'où $x^{-1} uvw = yy_0^{j-1} x_0^{i-1} vw \in y\, Y^{2j} \cap y_2\, Y^{2j}$ et comme Y est un code l'on a $y = y_2$, d'où la contradiction.

Par conséquent $xy \in (YX)_n$.

De façon similaire, $yx \in (XY)_n$. ■

Ainsi pouvons-nous retrouver le

COROLLAIRE 8 : *Soient X et Y deux codes et n un entier strictement positif. Alors les conditions suivantes sont équivalentes*:

(1) $X = Y$

(2) $X^n = Y^n$.

Démonstration: L'implication directe est évidente. Pour la réciproque, X *et* Y commutent d'après la proposition 7.

Comme il est facile de vérifier que $X \cap Y \neq \varnothing$, on obtient le résultat en utilisant le lemme 3. ■

Cette proposition 7 nous permet d'énoncer quelques propriétés des codes qui commutent:

COROLLAIRE 9 : *Si X et Y sont deux codes qui commutent, alors*

(1) XY est un code

(2) $\pi(X, Y)$ *et* $\pi(Y, X)$ i. e. *les produits XY et YX sont non ambigus.*

Démonstration: D'après la proposition 7, il existe deux entiers strictement positifs i et j tels que $X^i = Y^j$.

Considérons $(XY)^j$, $X^{i+j} = X^i X^j = Y^j X^j = (XY)^j$. Comme X est un code, X^{i+j} et $(XY)^j$ le sont ainsi que XY.

Soient $x_1, x_2 \in X$ et $y_1, y_2 \in Y$ tels que $x_1 y_1 = x_2 y_2$. Alors

$$x_1 y_1^j = x_2 y_2 y_1^{j-1} \in XY^j = X^{i+1}.$$

Comme X est un code, $y_1^j \in X^i$ et $y_2 y_1^{j-1} \in X^i$, $x_1 = x_2$ et $y_1 = y_2$. D'où $\pi(X, Y)$.

De façon similaire, on démontre $\pi(Y, X)$. ■

LEMME 10 : *Soit X un code. $C(X) = \{ Y / Y$ est un code et $XY = YX \}$ est un semi-groupe commutatif stable.*

Remarques: Par la proposition 7, l'on a:

1. $C(X) = \{ Y / \exists\, i, j \geqq 1$ tels que $X^i = Y^j \}$.

En effet, il est inutile de préciser que Y est un code car X l'est ainsi que X^i, Y^j et par conséquent Y.

2. $C(X) = C(Y)$ pour tout $Y \in C(X)$.

Démonstration: (1) $C(X)$ *est un semi-groupe commutatif.*

Soient Y, $Z \in C(X)$. D'après la remarque 2, l'on a $C(X) = C(Y)$ d'où $Z \in C(Y)$ et $ZY = YZ$. Ainsi YZ est un code (corollaire 9).

$$X(YZ) = (XY)Z = (YX)Z = Y(XZ) = Y(ZX) = (YZ)X,$$

par conséquent $YZ \in C(X)$.

(2) $C(X)$ *est stable.*

Soient Y, Z, ZT, $TY \in C(X)$. Par la remarque 2, l'on a

$$(YZ)T = Y(ZT) = (ZT)Y = Z(TY) = (TY)Z = T(YZ).$$

Remarquons que $\varepsilon \notin T$.

En effet, supposons que $\varepsilon \in T$, alors $Z \cap ZT \neq \varnothing$ et $Y \cap TY \neq \varnothing$. Comme Z, ZT, Y, $TY \in C(X)$, $Z = ZT$ et $Y = TY$ d'après le lemme 3. Supposons que $T - \{\varepsilon\} \neq \varnothing$, d'où il existe $t \in T - \{\varepsilon\}$ tel que

$$z_1 t = z_2 \qquad \text{avec} \quad z_1, z_2 \in Z,$$
$$t y_2 = y_1, \qquad \text{avec} \quad y_1, y_2 \in Y.$$

Par conséquent, on a une double décomposition de $z_1 t y_2$ dans ZY qui est en contradiction avec le point (2) du corollaire 9. D'où $T = \{\varepsilon\}$ qui n'est pas un sous-ensemble du semi-groupe. Comme YZ est un code, il existe deux entiers $i, j \geqq 1$ tels que $(YZ)^i \subset T^j$ (corollaire 6).

Puisque $T^j (j \geqq 1)$ code implique T code, il suffit de montrer que $(YZ)^i = T^j$. Nous pouvons supposer $i \geqq j$ sans nuire à la généralité de la démontration. En effet, si $i < j$, il suffit de prendre le plus petit entier multiple de i supérieur ou égal à j. Il est facile de montrer par récurrence que $(YZ)^i T^j = (YZ)^{i-j} (YZT)^j$. Ainsi $(YZ)^i T^j$ est un code car YZ et YZT le sont par le corollaire 9 et la remarque 2, d'où $(YZ)^{i-j} (YZT)^j$ est un code par le corollaire 9. Considérons $t_1 \ldots t_j \in T^j$ avec $t_k \in T$ $(1 \leqq k \leqq j)$. Soit $u \in (YZ)^i$, alors $u t_1 \ldots t_j u^2 \in (YZ)^i T^j (YZ)^i T^j$.

Comme $t_i \ldots t_j u \in T^j (YZ)^i = (YZ)^i T^j$, il existe $u_1 \in (YZ)^i$ et $u_2 \in T^j$ tels que $t_1 \ldots t_j u = u_1 u_2$. Alors, comme $(YZ)^i \subset T^j$, le mot $u t_1 \ldots t_j u^2$ a deux factorisations par les éléments de $(YZ)^i T^j$. En effet, $u t_1 \ldots t_j \in (YZ)^i T^j$, $u^2 \in (YZ)^i T^j$ et

$$u u_1 \in (YZ)^i (YZ)^i \subset (YZ)^i T^j, \qquad u_2 u \in T^j (YZ)^i = (YZ)^i T^j.$$

Comme $(YZ)^i T^j$ est un code alors l'on a

$$u t_1 \ldots t_j = u u_1 \quad \Rightarrow \quad t_1 \ldots t_j = u_1 \in (YZ)^i.$$

D'où l'égalité

$$(YZ)^i = T^j. \quad \blacksquare$$

En considérant les codes singuliers, nous établissons :

LEMME 11 : *Soit $i>0$. Les conditions suivantes sont équivalentes :*

(1) *X est un code singulier*

(2) *X^i est un code singulier.*

Démonstration: Comme X code est équivalent à X^i code, pour tout $i>0$, et que le produit de deux langages singuliers est singulier [10], le problème se ramène à X^i singulier $\Rightarrow X$ singulier.

Si $i=1$, le problème est résolu. Supposons $i \geqq 2$. Soit $x=x_1 \ldots x_i$ un mot singulier de X^i où $x_k \in X$ pour $1 \leqq k \leqq i$.

Nous allons montrer que $x_i \in g(X)$.

Supposons le contraire. Deux cas sont possibles :

1. Il existe $u \in A^+$ tel que $x_i u \in X$.

Alors $xu \in X^i$, contraire au fait que $x \in g(X^i)$.

2. Il existe $v \in X$, $u \in A^+$ tel que $x_i = vu$.

Ainsi $x_1 \ldots x_{i-1} v$, $x_1 \ldots x_{i-1} vu \in X^i$, ce qui contredit l'hypothèse sur x.

D'où $x_i \in g(X)$ et X est singulier. $\blacksquare$

COROLLAIRE 12 : Soient X et Y des codes tels que $XY=YX$. Si X est singulier alors Y est singulier.

LEMME 13 : *Soient X, Y, Z des langages non vides tels que $XY=ZY$, $\pi(X, Y)$ et $\pi(Z, Y)$. Alors $X=Z$.*

Démonstration : La démonstration se fait par récurrence sur les longueurs des mots de X et de Z.

Il est facile de vérifier que $X_{\min} = Z_{\min}$.

Supposons que $X_m = Z_m$ avec $m<n$.

Soient $x \in X_n$ tel que $|x|=n$ et $y_0 \in Y_{\min}$, $xy_0 \in XY=ZY$. Il existe $z \in Z$ et $y_1 \in Y$ tels que $xy_0 = zy_1$.

Deux cas sont à considérer :

1. $|z|=|x|$ d'où $x \in Z_n$.

2. $|z|<|x|$. D'après l'hypothèse de récurrence, $z \in X$. Comme $\pi(X, Y)$, alors $x=z$, contraire au fait que $|z|<|x|$.

D'où $x \in Z_n$.

De la même façon $Z_n \subset X_n$. $\blacksquare$

PROPOSITION 14 : *Soient L un code singulier, $C(L)=\{Y/Y$ est un code commutant avec $L\}$. Alors $C=C(L)\cup\{\varepsilon\}$ est un monoïde libre.*

Démonstration: Par le lemme 10, $C(L)\cup\{\varepsilon\}$ est un monoïde. D'après [5], si on prend comme homomorphisme de C sur $\mathbb{N}$, l'application $X\to l(X)$, il suffit de montrer que C est équidivisible.

Soient $X, Y, Z, T\in C$ tels que $XY=ZT$.

Si $l(X)=l(Z)$ alors la conclusion est vraie. En effet, dans ce cas,

$$(\bigstar) \qquad XY=ZT \text{ implique } X_{\min}=Z_{\min}, \quad Y_{\min}=T_{\min}.$$

Par la remarque 2, nous avons $T\in C(Y)$ et $Z\in C(X)$. Par $(*)$ et par le lemme 3, on a $X=Z$ et $Y=T$.

Supposons $l(X)>l(Z)$. On peut remarquer que $l(Y)<l(T)$. Comme Z est un code singulier (corollaire 12), soit $z\in g(Z)$. Considérons le langage U défini par

$$U=\{u\in A^+/zu\in X\}.$$

Nous montrons que $U\in C$ et que $X=ZU$, $UY=T$. D'où la conclusion.

1. $T=UY$ *et* $U\neq\varnothing$.

— Par construction $zU\subset X$ et $zUY\subset XY=CD$. Comme $z\in g(Z)$, $UY\subset T$.

— Soit $t\in T$, $zt\in ZT=XY$. Il existe $x\in X$, $y\in Y$ tels que $zt=xy$. On a 3 possibilités :

• $|x|=|z|$. Alors $X\cap Z\neq\varnothing$. Comme X et Z sont des codes qui commutent (remarque 2) et par le lemme 3 on a $X=Z$. Par conséquent $l(X)=l(Z)$, contraire à l'hypothèse.

• $|x|<|z|$. Considérons $xy_0\in XY=ZT$ avec $y_0\in Y_{\min}$. Il existe $z_1\in Z$ et $t_1\in T$ tels que $xy_0=z_1t_1$ avec $|z_1|<|x|$ car $l(Y)<l(Z)$. Comme z_1 est un préfixe propre de x et x est un préfixe propre de z, alors $z_1\in Z$ est préfixe propre de z. D'où la contradiction $z\notin g(Z)$.

• $|x|>|z|$ i. e. $x=zu$ et $t=uy$ avec $u\in U$, par conséquent $t\in UY$.

2. $\pi(U, Y)$.

Soient $u_1, u_2\in U$ et $y_1y_2\in Y$ tels que $u_1y_1=u_2y_2$. D'où $zu_1y_1=zu_2y_2$. X et Y étant des codes et $Y\in C(X)$ (remarque 2), alors $\pi(X, Y)$ (corollaire 9).

Comme $zu_1, zu_2\in X$, $zu_1=zu_2$ et $\pi(U, Y)$.

3. $\pi(ZU, Y)$.

Soit $z_1u_1, z_2u_2\in ZU$ et $y_1, y_2\in Y$ tels que $z_1u_1y_1=z_2u_2y_2$. Comme $\pi(Y, Z)$ et $UY=T$, alors $z_1=z_2$ et $u_1y_1=u_2y_2$. Ainsi $\pi(ZU, Y)$ car $\pi(U, Y)$ (par 2.).

4. $X=ZU\in C$.

Par hypothèse et par 1., $ZUY=ZT=XY$ avec $\pi(ZU, Y)$. Comme X, Y sont des codes et $Y\in C(X)$ (remarque 2) alors $\pi(X, Y)$ (par 3). D'où $X=ZU\in C$ (lemme 13).

5. $U\in C$.

Car C est stable (lemme 10) et Z, ZU, $Y\in C$ et (par 1) $UY=T\in C$.

D'où il existe $U\in C$ tel que $X=ZU$ et $UY=T$. ■

Comme « deux éléments d'un monoïde libre commutent si et seulement si ils sont puissances d'un même élément » [4], on peut déduire de la proposition 14:

COROLLAIRE 15 : *Deux codes singuliers qui commutent admettent un motif commun.*

COROLLAIRE 16 : *Tout code singulier admet un motif unique.*

Démonstration: Considérons un code singulier X admettant deux motifs Y et Z. D'après la proposition 7, Y et Z commutent. Donc Y et Z admettent un motif commun (corollaire 15). Comme Y et Z sont primitifs, $Y=Z$. ■

Si on veut étendre ce résultat aux codes, il nous semble que l'on puisse conjecturer:

CONJECTURE 1 : *Deux codes qui commutent admettent un motif commun.*

Cette conjecture peut être obtenue à partir de la suivante:

CONJECTURE 2 : *Un code admet un motif unique.*

En effet, considérons deux codes X et Y qui commutent. Il existe deux entiers i, $j\geqq 1$ tels que $X^i=Y^j$ (proposition 7). Soient Z un motif de X et T un motif de Y, *i. e.* il existe deux entiers h, $k\geqq 1$ tels que $X=Z^h$ et $Y=T^k$. Ainsi $X^i=Z^{hi}=T^{kj}=Y^j$. Comme X^i admet un motif unique (conjecture 2), $Z=T$ et X et Y admettent un motif commun.

IV. EXTENSIONS

Dans ce paragraphe, nous essaierons de donner une caractérisation de tout langage non vide qui commute avec un code.

Montrons d'abord:

LEMME 17 : *Soient X un code, i un entier positif, L un langage non vide tels que $X^iL=LX^i$. Alors $X^i(L\setminus X^*)=(L\setminus X^*)X^i$.*

Démonstration: La conclusion est vraie si $i=0$.

Supposons $i>0$. Posons $L_1=L\cap X^*$ et $L_2=L\setminus X^*$ *i.e.* $L=L_1\cup L_2$. Par conséquent, $X^iL=X^iL_1\cup X^iL_2=L_1X^i\cup L_2X^i$.

Montrons que $X^iL_2\cap L_1X^i=\varnothing$.

Supposons le contraire, *i.e.* qu'il existe $x\in X^i$ et $l_2\in L_2$ tels que $xl_2\in L_1X^i$, d'où l'existence de $l_1\in L_1$ et $x_1\in X^i$ tels que $xl_2=l_1x_1$.

Comme $l_1\in X^*$ donc $xl_2\in X^iX^*$, deux cas sont à envisager:

1. $xl_2=xy$ avec $y\in X^*$. D'où $l_2=y\in X^*$, contraire au fait que $L_2\cap X^*=\varnothing$.

2. $xl_2=uv$ avec $u\neq x$, $u\in X^i$ et $v\in X^*$. Considérons le mot l_2x.

D'après le lemme 2, il existe deux entiers positifs r et k tels que $(x_{i_r}y_{i_r})^k\in X^+$,

$$x_1,\ldots,x_{i_r-1}\in X^i$$

et

$$(l_2x)^kx_1\ldots x_{i_r-1}=x_1\ldots x_{i_r-1}(x_{i_r}y_{i_r})^k\in X^+.$$

Par conséquent

$$(xl_2)^kxx_1\ldots x_{i_r-1}=xx_1\ldots x_{i_r-1}(x_{i_r}y_{i_r})^k$$
$$=(uv)^kxx_1\ldots x_{i_r-1}\in X^+,$$

avec u, $x\in X^i$ et $u\neq x$, contraire au fait que X est un code. D'où $X^iL_2\cap L_1X^i=\varnothing$ *i.e.* $X^iL_2\subset L_2X^i$.

On peut obtenir $L_2X^i\subset X^iL_2$ par passage aux images miroir. ■

LEMME 18 : *Soient X un code, L un langage non vide inclus dans X^*, j un entier strictement positif et $I=\{i\in\mathbb{N}/X^i\cap L\neq\varnothing\}$.*

Alors $LX^j=X^jL$ implique $L=X^I$.

Démonstration: Par définition de I, il est clair que $L\subset X^I$. Montrons l'inclusion inverse *i.e.* pour tout $i\in I$, $X^i\subset L$.

Si $i=0$, alors $\varepsilon\in L$.

Soient $i\in I-\{0\}$ et k le plus petit entier multiple de j supérieur ou égal à i.

1. $k=i$.

Alors $X^kL=LX^k$ avec $X^k\cap L\neq\varnothing$. D'où, comme X^k est un code et par le lemme 2, $X^k=X^i\subset L$.

2. $k\neq i$.

Soit $x\in X$. Alors $X^ix^{k-i}\subset X^k$. Comme $X^i\cap L\neq\varnothing$, considérons $l\in L\cap X^i$.

Soit $x_1 \in X^i$, $x_1 x^{k-i} l \in X^k L = LX^k$, d'où il existe $l_2 \in L$ et $x_2 \in X^k$ tels que $x_1 x^{k-i} 1 = l_2 x_2$.

Comme $l_2 \in L \subset X^*$ alors l'on a

$$(\bigstar) \qquad x_1 x^{k-i} l = l_2 x_2 \in X^*.$$

D'autre part, nous avons

$$(\bigstar\bigstar) \qquad x_2, x^{k-i} l \in X^k \qquad \text{et} \qquad x_1, l_2 \in X^*.$$

Alors, comme X est un code, $(*)$ et $(**)$ impliquent $x_1 = l_2 \in L$. Par conséquent, $X^i \subset L$.

Ainsi $X^I \subset L$, d'où l'égalité. ■

LEMME 19 : *Soient X un code et j un entier strictement positif vérifiant la propriété (P):*

Pour tout langage non vide L, $LX^j = X^j L$ implique $L \cap X^* \neq \varnothing$. Alors pour tout langage non vide L, $X^j L = LX^j$ implique l'existence de $I \subset \mathbb{N}$ tel que $L = X^I$.

Démonstration: Soit L un langage non vide tel que $X^j L = LX^j$. Si $L \subset X^*$ alors on conclut par le lemme 18.

Supposons, par l'absurde $L \setminus X^* = L_1 \neq \varnothing$. Par le lemme 17, $X^j L = LX^j$ implique $L_1 X^j = X^j L_1$. Comme X vérifie la propriété (P) alors $X^* \cap (L \setminus X^*) = X^* \cap L_1 \neq \varnothing$, ce qui est absurde. ■

Considérons maintenant les codes dont les éléments minimaux (au point de vue longueur) forment un code circulaire.

LEMME 20 : *Soient X un code, j un entier strictement positif et L un langage non vide tels que $X_{\min}$ est circulaire et $X^j L = LX^j$. Alors $L \cap X^* \neq \varnothing$.*

Démonstration: Si $\varepsilon \in L$, le problème est résolu, sinon $X^j L = LX^j$ implique $X^j_{\min} L_{\min} = L_{\min} X^j_{\min}$ [11].

Comme $X^j_{\min}$ et $L_{\min}$ sont uniformes, donc des codes, par la proposition 7 il existe deux entiers r, $s \geqq 1$ tels que

$$(\bigstar) \qquad (X^j_{\min})^r = L^s_{\min}$$

Soient k et i deux entiers positifs et premiers entre eux tels $jr = kt$ et $s = it$ avec t entier positif.

Par $(*)$, l'on a alors $(X^k_{\min})^t = (L^i_{\min})^t$.

Par cette équation et par corollaire 8, on a $X^k_{\min} = L^i_{\min}$.

Deux cas sont à envisager :

1. $i=1$.

Alors $L \cap X^k \neq \varnothing$.

2. $i>1$.

Alors on a $k>1$ sinon il y a contradiction entre $X^k_{\min}=L^i_{\min}$ et le fait que $X_{\min}$ est circulaire donc primitif.

Soit $x_0 \in X_{\min}$, $x_0^k \in X^k_{\min}=L^i_{\min}$. Il existe $l_1, \ldots, l_i \in L_{\min}$ tels que $x_0^k = l_1 \ldots l_i$.

a. Il existe un entier $t>0$ tel que $l_1 = x_0^t$, par conséquent $L \cap X^t \neq \varnothing$.

b. Il existe $t \in \mathbb{N}$, $u \in A^+$, $v \in A^+$ tels que $x_0 = uv$ et $l_1 = x_0^t u$.

D'où $vx_0^{k-1}u = l_2 \ldots l_i l_1 \in L^i_{\min} = X^k_{\min}$.

Comme $X_{\min}$ est circulaire, $u=\varepsilon$ ce qui est contraire à l'hypothèse.

D'où $L \cap C^* \neq \varnothing$. ■

Comme tout code tel que l'ensemble des mots minimaux forme un code circulaire, vérifie les hypothèses du lemme 19, nous pouvons énoncer :

PROPOSITION 21 : *Soient X un code, j un entier strictement positif et L un langage non vide tels que $X_{\min}$ soit circulaire et $X^j L = LX^j$.*

Alors X est un motif de L i. e. *il existe $I \subset \mathbb{N}$ tel que $L = X^I$ avec X primitif.*

D'où :

COROLLAIRE 22 : *Un langage circulaire est motif de tout code qui commute avec lui.*

Terminons par l'étude des codes préfixes.

LEMME 23 : *Soient X un code et L un langage non vide tels que $XL = LX$ et $\pi(X, L)$. Alors on a $\pi(L, X)$.*

Démonstration : Comme $\pi(X, L)$, le produit $(XL)_n$ est non ambigu $\forall n \in \mathbb{N}$.

Montrons que $\forall n \in \mathbb{N}$, le produit $(LX)_n$ est non ambigu. Pour cela introduisons deux nouveaux ensembles :

$$D_n = \{(x, l)/x \in X, l \in L \text{ et } |xl| = n\},$$

$$E_n = \{(l, x)/x \in X, l \in L \text{ et } |lx| = n\}.$$

Il existe une bijection entre E_n et D_n. Comme le produit $(XL)_n$ est non ambigu, D_n est en bijection avec $(XL)_n = (LX)_n$. D'où $\text{card}((LX)_n) = \text{card}(E_n)$.

Considérons l'application f:

$$E_n \to (LX)_n$$
$$(l, x) \mapsto lx.$$

Il est évident que f est surjective, d'après la définition de E_n. Comme $(LX)_n$ et E_n ont le même cardinal, f est injective et par conséquent bijective.

Ainsi le produit $(LX)_n$ est non ambigu, d'où le résultat. ■

LEMME 24 : *Soient X un code préfixe, L un langage quelconque et k un entier tels que $XL = LX$ et $l(X) = kl(L)$.*

Alors il existe un code préfixe Y tel que $X = Y^k$.

Démonstration: Il est facile de démontrer par récurrence que pour tout n, $XL^n = L^n X$. Comme $X_{\min} = L^k_{\min}$ alors $X \cap L^k \neq \varnothing$.

Ainsi $X \subset L^k$ par le lemme 3.

Pour tout $x = l_1 \ldots l_k \in X \subset L^k$ avec $l_i \in L$ pour tout $i \in [1, k]$, on peut établir les propriétés suivantes:

1. $l_{i+1} \ldots l_k l_0^i \in X$ si $l_0 \in L_{\min}$ et $i \in [0, k]$.

Soit $u = l_{i+1} \ldots l_k l_0^k \in L^{k-i} X = XL^{k-1}$ *i. e.* $u = wy$ avec $x \in X$ et $y \in L^{k-1}$. Comme $l_0 \in L_{\min}$ et que $y \in L^{k-i}$, $|y| \geqq |l_0^{k-i}|$ d'où $l_{i+1} \ldots l_k l_0^i = wv$ et $vl_0^{k-i} = y$.

Comme $l_1 \ldots l_i w \in L^i X = L^i X$ alors

$$xl_0^i = l_1 \ldots l_k l_0^i = l_1 \ldots l_i wv \in XL^i \cap XL^i v.$$

Par cette équation, comme $x \in X$ et que X est préfixe, l'on a $l_0^i \in L^i v$. Par conséquent, comme $l_0 \in L_{\min}$, $v = \varepsilon$ et $l_{i+1} \ldots l_k l_0^i = w \in X$.

2. *La décomposition d'un mot de X dans L^k est unique*

Supposons qu'il existe un mot x de X qui admet une double décomposition dans L^k, *i. e.*

$$x = l_1 \ldots l_i l_{i+1} \ldots l_k = y_1 \ldots y_i y_{i+1} \ldots y_k.$$
$$\text{avec } l_1 \ldots l_i \neq y_1 \ldots y_i \text{ et } l_j, y_j \in L \text{ pour } 1 \leqq j \leqq k$$

D'après 1. $l_{i+1} \ldots l_k l_0^i \in X$ et $y_{i+1} \ldots y_k l_0^i \in X$.

D'où

$$xl_0^i = (l_1 \ldots l_i)(l_{i+1} \ldots l_k l_0^i) = (y_1 \ldots y_i)(y_{i+1} \ldots y_k l_0^i) \in L^i X$$

D'où on n'a pas $\pi(L^i, X)$ qui est en contradiction avec le lemme 23 car si X est préfixe, il est évident que l'on a $\pi(X, L^i)$.

3. $l_0^i l_1 \dots l_{k-i} \in X$ avec $l_0 \in L_{\min}$ et $i \in [0, k]$.

La démonstration se fait par récurrence sur i.

Si $i=0$ alors $l_1 \dots l_k \in X$ par définition.

Supposons $i \neq k$ et $l_0^{i-1} l_1 \dots l_{k-i+1} = u \in X$. Ainsi $l_0 u \in LX = XL$ *i. e.* qu'il existe $y \in Y$ et $z \in L$ tels que $l_0 u = yz$. Comme $|l_0^i| \leqq \min(X)$ alors $y = l_0^i v$ avec $v \neq \varepsilon$ sinon $i=k$ car X est préfixe ($l_0^k \in X$).

D'où $l_0^k v = l_0^{k-i} l_0^i v = l_0^{k-i} y \in L^{k-i} X = XL^{k-i}$. Comme X est préfixe, $l_0^k \in X$ et $v \in L^{k-i}$.

Par hypothèse, $(l_0^{i-1} v) z = (l_0^{i-1} l_1 \dots l_{k-i}) l_{k-i+1} = u \in X \subset L^k$. Le premier terme à gauche et celui du centre donnent deux décompositions de u dans L^k. Comme la décomposition d'un mot de X dans L^k est unique (*voir* 2) et comme z, $l_{k-i+1} \in L$ alors $z = l_{k-i+1}$.

Par conséquent, $l_0^i l_1 \dots l_{k-i} = l_0^i v = y \in X$.

4. $X = Y^k$.

Soit $l_0 \in L_{\min}$. Définissons $Y = (l_0^{k-1})^{-1} X$.

a. Y est préfixe.

Comme l_0^{k-1} est préfixe propre d'un élément de X, Y est préfixe [2].

b. $Y \subseteq L$.

Soit $y \in Y$. Alors $l_0^{k-1} y \in X$.

Considérons $l_0 l_0^{k-1} y \in LX = XL$. Comme X est préfixe et que $l_0^k \in A$ alors $y \in L$.

c. $YX \subseteq XY$.

Soit $y \in Y$ et $x \in X$. Comme $Y \subset L$ (par le point *b*), $yx \in LX = XL$ i. e. $yx = x_1 l$ avec $x_1 \in X$ et $l \in L$. Considérons le mot $l_0^{k-1} yx = l_0^{k-1} x_1 l$ avec $l_0^{k-1} y \in X$. Comme $x_1 \in X$, d'après le point 2, x_1 se décompose de façon unique dans L^k *i. e.* $x_1 = u_1 \dots u_k$ avec $u_i \in L$ pour $i \in [1, k]$.

D'après le point 3, $l_0^{k-1} u_1 \in X$ et comme X est préfixe

$$l_0^{k-1} y = l_0^{k-1} u_1 \qquad \text{et} \qquad x = u_2 \dots u_k l.$$

D'après le point 2, $l l_0^{k-1} \in X$ et le point 3 nous permet d'avoir $l_0^{k-1} l \in X$ d'où $l \in Y$.

d. $YX = XY$ *et* $X = Y^k$.

Comme Y et X sont des codes, alors X et Y commutent par la proposition 7.

Par le lemme 3 et comme X et Y^k sont des codes qui commutent et $l_0^k \in X \cap Y^k$, on a $X = Y^k$. ■

LEMME 25 : *Soient X un code préfixe primitif, i un entier strictement positif, L un langage non vide tels que $X^i L = LX^i$.*

Alors $L \cap X^* \neq \varnothing$.

Démonstration :

— $\varepsilon \in L$. Alors $L \cap X^* \neq \varnothing$.

— $\varepsilon \notin L$. Il est facile de vérifier que $X_{\min}^i L_{\min} = L_{\min} X_{\min}^i$. Par la proposition 7, comme $L_{\min}$ et $X_{\min}^i$ sont des codes, il existe deux entiers α, $\beta > 0$ tels que

$$(\bigstar) \qquad X_{\min}^{\alpha i} = L_{\min}^{\beta} \qquad \text{et} \qquad l(X^{\alpha i}) = \beta l(L).$$

D'après le lemme précédent, il existe un code Y tel que $X^{\alpha i} = Y^{\beta}$. Par la proposition 7, X et Y commutent. Par le corollaire 15 (X et Y sont des codes préfixes), X et Y admettent un motif commun. Comme X est primitif alors X est le motif de Y *i. e.* il existe un entier positif h tel que $Y = X^h$. Alors $X^{\alpha i} = Y^{\beta} = X^{h\beta}$ d'où $i\alpha = h\beta$ *i. e.* β divise αi.

De plus par (*), l'on a $X_{\min}^{\alpha i} = L_{\min}^{\beta} = (X_{\min}^h)^{\beta}$.

Cette équation implique, comme $X_{\min}$ et $L_{\min}$ sont des codes et par le corollaire 8,

$$X_{\min}^{\alpha i/\beta} = X_{\min}^h = L_{\min}.$$

D'où $L \cap X^* \neq \varnothing$. ■

Comme tout code préfixe admet un motif unique (corollaire 15), nous pouvons déduire des lemmes 24 et 25 et du corollaire 15 :

PROPOSITION 26 : *Soit L un langage non vide commutant avec un code préfixe X. Alors X et L admettent un motif commun* i. e. *il existe un code primitif Y, un entier positif j et $I \subset \mathbb{N}$ tels que $X = Y^j$ et $L = Y^I$.*

Reste ouvert le cas où X est un code quelconque. Il semble que :

CONJECTURE 3 : Tout langage non vide commutant avec un code admet un motif commun avec ce dernier.

REMERCIEMENTS

Je tiens à remercier les rapporteurs pour leur lecture très minutieuse de la première version de ce papier, leurs suggestions et remarques et plus particulièrement, pour une meilleure présentation des lemmes 2 et 3. Je remercie également M. Latteux pour ses conseils et remarques tout au long de ce travail.

BIBLIOGRAPHIE

1. J. M. AUTEBERT, L. BOASSON et M. LATTEUX, *Motifs et bases de langages* (à paraître).
2. J. BERSTEL et D. PERRIN, *Theory of Codes*, Academic Press, New York, 1985.
3. P. M. COHN, *Free Rings and their Relation*, Academic Press, New York, 1971.
4. G. LALLEMENT, *Semigroups and Combinatorial Applications*, Wiley, New York, 1979.
5. F. W. LEVI, *On semigroups*, Bull Calcutta Math. Soc., vol. 36, 1944, p. 141-146.
6. M. LOTHAIRE, *Combinatorics on Words*, Reading, Massachussetts, Addison-Wesley, 1983.
7. R. C. LYNDON et M. P. SCHUTZENBERGER, *The equation $a^M = b^N c^P$ in a Free Group*, Michigan Math. J., vol. 9, 1962, p. 289-298.
8. M. NIVAT, *Éléments de la théorie générale des codes*, Automata Theory, E. R. Caianiello éd., p. 279-294, Academic Press, New York, 1966.
9. D. PERRIN, *Codes conjugués*, Information and Control, vol. 20, 1972, p. 222-231.
10. H. J. SHYR, *Free Monoids and Languages*, Lecture Notes, Department of Mathematics, Soochow University, Taipei, Taiwan, R.O.C., 1979.
11. D. WOOD, *A Factor Theorem for Subsets of a Free Monoids*, Information and Control, vol. 21, n° 1, 1972, p. 21-26.