Lecture Notes in Computer Science
Edited by G. Goos and J. Hartmanis
Series: GI, Gesellschaft für Informatik e. V.

48

Theoretical Computer Science 3rd GI Conference

Darmstadt, March 1977

Springer-Verlag
Berlin · Heidelberg · New York

CODES ET SOUS-MONOIDES POSSEDANT DES MOTS NEUTRES

D. Perrin - M.-P. Schützenberger

Introduction

Dans tout ce travail, A^* (resp. $A^+ = A^*\setminus 1$) désigne le monoïde libre (resp. le semigroupe libre) engendré par l'ensemble fixe non vide A et on considère un sous-monoide X^* de A^* dont l'ensemble générateur minimal est $X = X^+\setminus X^+X^+$, où $X^+ = X^*\setminus 1$. Une série de recherches se sont attachées à l'étude des rapports entre X, le sous-monoide X^* et le monoïde syntaxique $S = A^*\xi$ de X^* ; en particulier, celles de J-F. Perrot [8], de R. Mc Naughton [7] et de G. Lallement [5] ont montré l'intérêt de la nature des groupes contenus dans S et de la structure des idéaux de ce monoïde. Le cas particulier où X engendre librement X^* (c'est-à-dire où X est un *code*) présente un certain intérêt supplémentaire en raison, notamment, de son interprétation en théorie de l'information et de ses rapports avec les processus stochastiques associés ; il pose divers problèmes algébriques non résolus.

Nous nous occupons ici du cas où X^+ admet des *mots neutres*, c'est-à-dire où il existe des mots $h \neq 1$ ayant même image syntaxique $h\xi$ que le mot vide 1 ; celle-ci est évidemment l'élément neutre du monoïde syntaxique S. Par conséquent, il existe des mots neutres non triviaux dès que S a une sous groupe U (des éléments inversibles ou unités) non-trivial. Formellement, h est un mot neutre ssi les relations $ab \in X^*$ et $ahb \in X^*$ sont équivalentes pour chaque paire de mots a, b de A^*. Cette hypothèse a une signification intuitive immédiate dans le cadre de la théorie du signal puisqu'elle exprime que le bruit sur la ligne est tel qu'on ne peut pas détecter la présence de segments égaux à h qui se trouveraient à l'intérieur des messages. En particulier, le mot $h = c^p$, où p est positif et c est une lettre, est neutre quand les dispositifs physiques ont la propriété que la longueur d'un segment $c\ldots c\ldots c$ formé de la répetition de cette lettre, ne peut être determinée que modulo p (on pourrait dire qu'il s'agit d'un "bruit modulo p"). L'étude de ce problème se rattache aussi à la théorie des polynômes cyclotomiques.

Notre résultat principal concerne la reconnaissabilité de X^*, au sens de S. Eilenberg [4], c'est-à-dire la finitude de son monoïde syntaxique S. Comme on le sait, le théorème de Kleene affirme que X et X^* sont simultanément reconnaissables ou non. Nous établissons ici que, quand X admet des mots neutres non triviaux, *il est reconnaissable ssi l'un de ceux-ci,* soit h, *n'est pas complétable dans* X, c'est-à-dire si l'intersection de X avec A^*hA^* est vide. Un résultat plus fort, basé sur l'existence d'un mot $h \neq 1$ (non nécessairement neutre) tel que l'idéal à gauche A^*h rencontre le stabilisateur de chacun des états de l'automate minimal de X^*, nous a paru trop technique pour que sa preuve mérite d'être donnée ici. On remarquera que, de façon générale, si X^* est reconnaissable, il existe au moins un mot incomplétable dans X mais que, réciproquement, cette hypothèse implique seulement que si tout mot est complétable dans X^*, la densité asymptotique de ce dernier (au sens de Berstel [1] soit non nulle pour toute distribution de probabilités positive sur A.

Il est clair que l'existence de mots non complétables est assurée dans le cas particulier où X est *localement fini,* en ce sens que pour chaque sous-alphabet fini B de A, il n'y a qu'un nombre fini de mots de X dont toutes les lettres sont dans B^*. Dans ce cas, le sous-monoïde X^* est donc reconnaissable dès qu'il possède des mots neutres ; un phénomène curieux est que, si *aucun* des mots neutres n'est complétable dans X (donc en particulier si X est localement fini), le sous-groupe U de S est nécessairement cyclique. Cette situation algébrique correspond à celle du "bruit modulo p" perturbant la détermination des longueurs des segments c...c...c comme on l'a indiqué plus haut et où le paramètre p est évidemment l'ordre de U.

La technique de preuve fait intervenir la représentation de A par un monoïde de relations (c'est-à-dire un automate non déterministe) possèdant un sous groupe *transitif* sur les états. Réciproquement tout monoïde fini de ce type est monoïde syntaxique d'un sous-monoïde X^* ayant des mots neutres incomplétables dans X. Le cas des codes correspond à celui où le monoïde de relations est non-ambigu, au sens de J.M. Böe [2].

Notre second résultat affirme que si X^* (admettant des mots neutres) est engendré librement par un ensemble X localement fini, *le maximum des longueurs des mots de* X *est précisément l'ordre* p *du groupe cyclique* U. Une illustration de ce fait est fournie par la très remarquable famille de codes découverte par A. Restivo, à partir d'hypothèses toutes différentes [9].

Enfin un argument de comptage très simple donne une caractérisation des sous-monoïdes X^* (possèdant des mots neutres) qui sont engendrés par un code X *maximal* (c'est-à-dire qui ne soit pas contenu dans un autre code) : une condition nécessaire et suffisante pour que X ait ces propriétés est que chacune des relations du monoïde construit plus haut ait exactement p entrées non vides, où p est le nombre des états sur lesquels les relations sont définies. Ceci constitue une généralisation d'un fait qui serait banal si l'hypothèse qu'il existe des mots neutres non-triviaux était remplacée par celle que X soit un code préfixe. Cette remarque a une application immédiate au problème de la transmission sur une ligne affectée d'un "bruit modulo p".

Monoïdes de relations

1. Transitivité.

Soit Q un ensemble fini et R le monoïde des relations binaires sur Q ; il est commode d'appeler *états* les éléments de Q . Un monoïde de relations sur Q est un sous-monoïde de R ; en particulier son élément neutre est l'égalité sur Q . On remarquera qu'un sous-semigroupe de R peut être un monoïde (i.e. possèder un élément neutre) sans être, dans notre terminologie, un monoïde de relations ; nous dirons que c'est un semigroupe de relations.

Un monoïde M de relations est *transitif* si pour tout couple (q,q') d'états il existe au moins un m dans M contenant (q,q'). On dit que M est *très transitif* si il existe une *permutation* m dans M contenant (q,q') ; un monoïde de relations M est donc très transitif ssi son sous-groupe est transitif. La proposition suivante montre qu'on n'obtient pas une définition très différente en considérant des semigroupes de relations et sera utile pour la suite :

Proposition 1. Soit S *un semigroupe de relations sur un ensemble fini* Q *possèdant un élément neutre* e *et dont le sous-groupe est transitif. Alors* e *est une équivalence et* S *induit sur le quotient de* Q *par* e *un monoïde de relations très transitif isomorphe à* S .

Démonstration. Tout d'abord la relation e est transitive du fait que e est idempotent: si (q,q') et (q',q") sont dans e , alors (q,q") est dans $e^2 = e$.

Maintenant pour tout q dans Q , il existe un élément inversible s de S contenant (q,q) ; comme Q est fini, l'élément s est d'ordre fini, soit n ;

on a alors : $(q,q) \in s^n = e$, et ceci montre que e est réflexive. Enfin, si $(q,q') \in e$, soit s un élément inversible de S tel que $(q,q') \in s$; si n est l'ordre de s, on a alors $(q',q) \in s\,s^{n-1} = e$, puisque $(q,q) \in es = s$. Ceci montre que e est symétrique et démontre la propriété.

2. Stabilisateurs.

Soit M un monoïde de relations sur Q ; le *stabilisateur* d'un état q de Q est le sous monoïde P de M formé des relations qui contiennent le couple (q,q).

Proposition 2. Si M *est un monoïde de relations très transitif, il est le monoïde syntaxique de chacun des stabilisateurs des états.*

Démonstration. Soit P le stabilisateur de q et supposons que deux éléments m et n de M aient même image dans le monoïde syntaxique de P. Si un couple (q_1, q_2) d'états est dans m, soient g_1 et g_2 des éléments inversibles de M tels que $(q, q_1) \in g_1$ et $(q_2, q) \in g_2$. Alors (q,q) appartient à $g_1 m g_2$ et donc à $g_1 n g_2$; mais ceci implique que $(q_1, q_2) \in n$ et nous avons ainsi montré que $m = n$, ce qui signifie que M est le monoïde syntaxique de P.

Cette proposition montre que si ξ est une représentation de A^* par un monoïde de relations très transitif alors le monoïde syntaxique du stabilisateur dans A^* d'un état est égal à $A^*\xi$.

3. Ambiguité.

Reprenant la terminologie introduite par J.M. Böe, on dira qu'un monoïde de relations M sur un ensemble Q est *non-ambigü* si pour chaque m et n dans M et chaque couple (q,q') dans mn, il existe un *unique* état q'' tel que $(q,q'') \in m$ et $(q'',q') \in n$. Cette condition est évidemment remplie en particulier par les monoïdes d'applications et donc par le sous-groupe d'un monoïde de relations.

On sait que si ξ est une représentation de A^* par un monoïde de relations transitif, l'image réciproque par ξ du stabilisateur d'un état est un sous-monoïde *libre* X^* ssi ce monoïde de relations est non-ambigü.

4. Exemple.

Quand $\mathrm{Card}(Q) = 2$, le monoïde de relations M (resp. M') engendré par les deux permutations de Q et une relation ayant une seule entrée non vide (resp. une seule entrée vide) est très transitif par construction. On notera que M et M' sont des monoïdes isomorphes mais qu'ils ne sont pas équivalents en tant que monoïdes de relations ; de plus M (mais non M') est un exemple de relations non-ambigü.

Le cas général

Reprenant les notations utilisées dans l'introduction, nous établissons l'énoncé suivant, où on dit que X^* est reconnu par un monoïde de relations pour exprimer qu'il existe une représentation de A^* par un monoïde fini de relations telle que X^* soit le stabilisateur d'un état.

Théorème 1. *Une condition nécessaire et suffisante pour que* X^* *soit reconnu par un monoïde très transitif est l'existence d'un mot neutre incomplétable dans* X .

Démonstration. Supposons d'abord que X^* soit le stabilisateur de l'état 0 pour une représentation ξ de A^* par un monoïde de relations très transitif M , sur l'ensemble $Q = \{0, 1, \ldots, p-1\}$. Notons G le sous-groupe de M et définissons par récurrence les mots $w_o, w_1, \ldots, w_p$ en posant : $w_o = 1$ et $w_{i+1} = w_i\, u_i$, où u_i est un mot non vide de $G\xi^{-1}$ tel que : $(i,0) \in w_{i+1}\xi$. Le mot $f = w_p$ est alors incomplétable dans X puisque tous g,h dans A^*, si $g f h$ est dans X^*, alors $(0,0) \in g f h\, \xi$ et il existe donc i et j dans Q tels que : $(0,i) \in g\,\xi$, $(i,j) \in h\,\xi$ et $(j,0) \in h\,\xi$. Mais on a : $h = w_{i+1} r$ et, comme $(i,0) \in w_{i+1}\xi$, et que $h\xi \in G$, on obtient $(0,j) \in r$; ceci montre que les mots $g\,w_{i+1}$ et $r\,h$ sont dans X^* et donc que $g f h$ ne peut être dans X . Maintenant comme G est fini, f a une puissance, soit f^n , qui est l'élément neutre de G . Le mot f^n est alors un mot neutre incomplétable dans X .

Pour établir la réciproque, nous supposons l'existence d'un mot neutre $f \in X^*$ qui est incomplétable dans X , et nous notons R (resp. L) l'ensemble des facteurs droits (resp. gauches) propres de f .

Associons à tout mot u de A^* la partie $u\rho$ de $R \times L$ définie par :

$$(r, l) \in u\rho \Leftrightarrow r\,u\,l \in X^*$$

Notons maintenant π la partie de $L \times R$ définie par :

$$(l, r) \in \pi \Leftrightarrow l\,r = f$$

et démontrons la formule suivante, où les points notent des produits de relations :

$$\forall\, u, v \in A^*, \quad uv\rho = u\rho.\pi.v\rho$$

Tout d'abord, si (r,l) appartient à $u\rho.\pi.v\rho$, il existe par définition (l', r') dans π tels que : $r\,u\,l', r'v\,l \in X^*$ et $f = l'r'$; on a alors $r'\,u\,f\,v\,l' \in X^*$, d'où $r\,u\,v\,l \in X^*$, du fait que f est un mot neutre, et enfin (r,l) appartient à $uv\rho$. Maintenant, si (r,l) appartient à $uv\rho$, alors $r\,u\,v\,l \in X^*$ et donc aussi $r\,u\,f\,v\,l \in X^*$; mais comme f est incomplétable dans X, cela implique l'existence d'une factorisation de f en : $f = l'r'$ telle que : $r\,u\,l', r'\,v\,l \in X^*$, ce qui exprime le fait que $(r,l) \in u\rho.\pi.v\rho$.

Ceci montre que l'application $\xi : u \in A^* \to \pi.u\rho$ (resp. $u\rho\pi$) est un homomorphisme de A^* sur un semigroupe de relations sur l'ensemble *fini* L (resp. R). Le monoïde $M = \xi A^*$ est donc fini et ξf est son élément neutre (mais n'est pas en général l'égalité sur L) ; le sous-groupe (des éléments inversibles) de M est de plus transitif : remarquons en effet tout d'abord que, du fait que M est fini, tout conjugué $g = r\,l$ de $f = l\,r$ est encore dans X^* puisqu'ils ont même image par ξ ; ainsi, pour tous l,l' dans L, si $f = l\,r = l'r'$, alors $r\,l\,r'\,l'$ est dans X et le couple (l,l') appartient donc à $l\,r'\xi$, qui est inversible dans M. Ainsi, d'après la proposition 1 la relation $f\xi$ est une équivalence et le monoïde de relations N induit par M sur le quotient de L par cette équivalence est très transitif. Enfin, l'image réciproque par ξ du stabilisateur de la classe de $1 \in L$ est égale à X^* puisqu'un élément de M stabilise 1 ssi il stabilise tous les éléments de sa classe.

L'énoncé suivant donne des conditions, en apparence beaucoup plus faibles, qui équivalent en fait à celles du théorème précédent. Leur intérêt nous semble être le fait qu'elles ne portent que sur des sous-alphabets finis de A et que chacune d'elles est, en un certain sens, unilatérale ; nous ommettons d'en donner ici la preuve.

Proposition 3. Une condition nécessaire et suffisante pour que X^* *soit reconnu par un monoïde très transitif est l'existence d'un mot* $h \in A^+$ *tel que pour tout sous alphabet fini* B *de* A *satisfaisant* $h \in B^*$ *les conditions suivantes soient remplies :*

(1) L'idéal à gauche B^*h *rencontre le stabilisateur de chacun des états de l'automate minimal reconnaissant* $Y^* = X^* \cap B^*$: $\forall\, b \in B^*, \exists\, g \in B^*: bb' \in Y^* \Leftrightarrow bhgb' \in Y^*$

(2) Pour tout $b \in B^*$ *, il existe un entier* n *tel que* bh^n *soit incomplétable à droite dans* X : $bh^n B^* \cap X = \emptyset$.

Remarque 1. Le théorème 1 implique, sous l'hypothèse supplémentaire que X est un code, que X peut être reconnu par un monoïde de relations non-ambigu isomorphe à son monoïde syntaxique. Cet énoncé est, en fait, vrai de tous les codes reconnaissables, suivant le très important théorème de [3].

Sous monoïdes finiment engendrés

Nous en venons maintenant au cas où l'ensemble X est localement fini, c'est-à-dire que l'intersection de X avec B^* est finie pour tout sous alphabet fini B de A. Tout d'abord, d'après le théorème 1, X^* est alors reconnaissable s'il possède des mots neutres ; en effet, si $h \in A^+$ est un mot neutre il possède une puissance, soit h^n qui est incomplétable dans X, et h^n est encore lui-même neutre. On pourra donc, sans perte de généralité, supposer que A est fini ainsi que X .

Nous établissons le résultat suivant, dans lequel U désigne le sous-groupe (des éléments inversibles) du monoïde syntaxique de X^* et $|X|$ la borne supérieure des longueurs des mots de X :

Théorème 2. Si X *est fini,* U *est cyclique d'ordre au plus égal à* $|X|$.

Démonstration. Tout d'abord, les hypothèses du théorème 1 étant satisfaites, il existe une représentation ξ de A^* par un monoïde M de relations très transirif reconnaissant X^* ; d'après la proposition 2, M est isomorphe au monoïde syntaxique de X^* et U est donc isomorphe au groupe transitif formé des permutations contenues dans M . Notons B l'intersection de l'alphabet A avec $U\xi^{-1}$; la restriction de ξ à B^* est une représentation de B^* par un monoïde de relations qui est évidemment non ambigu et qui reconnaît l'intersection de X^* avec B^* ; la preuve suivra du lemme ci-dessous, dont nous ferons encore usage plus bas :

Lemme. Soit ξ *une représentation de* B^* *par un monoïde transitif de relations non ambigu sur un ensemble* Q *et* Y^* *le stabilisateur de l'état* 0 *. Alors* Y *est fini ssi il existe un ordre sur* Q *tel que pour toute lettre* $a \in A$*, on ait :* $(q,q') \in a\xi$ *seulement si* $q \leq q'$ *ou si* $q = 0$ *.*

Démonstration. La condition est évidemment suffisante puisqu'elle implique que tout mot de Y ait une longueur au plus égale à Card(Q). Réciproquement, il nous suffit de vérifier que la relation sur $Q\backslash 0$ définie par $(q,q') \in a\xi$ pour au moins une lettre a A a une fermeture transitive antisymétrique. Supposons donc qu'il existe $q_1,\ldots, q_k \in Q\backslash 0$ et $a_1,\ldots, a_k \in A$ tels que :

$(q_1, q_2) \in a_1\xi,\ldots, (q_k, q_1) \in a_k\xi$; soient $f,g \in A^*$ deux mots tels que :

$(q,q_1) \in f\xi$, $(q_1, q) \in g\xi$ et que cette relation ne soit vraie pour aucun facteur droit (resp. gauche) de f (resp. g). On a alors $f(a_1 a_2\ldots a_k)^* g \subset Y$ puisque le monoïde $A^*\xi$ est non ambigu, en contradiction avec l'hypothèse que Y est fini.

D'après le lemme, toutes les permutations $b\xi$, pour b dans B doivent être égales à une même permutation circulaire de l'ensemble de tous les états ; ceci montre que le groupe U est cyclique d'ordre $p = \mathrm{Card}(Q)$ et que B^p est inclus dans X , ce qui achève de prouver le théorème.

Dans le cas où X est un code, l'énoncé précédent peut être précisé ainsi :

Corollaire. Si X *est un code fini, le groupe* U *est cyclique d'ordre* $|X|$.

Démonstration. En effet, d'après le lemme précédent, tout mot de X est de longueur au plus égale à $p = \mathrm{Card}(Q)$ et si b est une lettre dont l'image syntaxique est dans U , on a $b^p \in X$.

Remarque 2. Si X n'est pas un code, il peut contenir des mots de longueur supérieure strictement à l'ordre de U comme le montre l'exemple suivant : soit $A = \{a, b\}$ et $X = a^p \cup \{a^i b a^j \mid 0 \leq i,j \leq p-1\}$; on a alors $X = (a^p)^* \cup A^* b A^*$,

a^p est un mot neutre pour X^*, le groupe U est cyclique d'ordre p et $|X| = 2p-1$. Il serait intéressant de donner une borne à la longueur des mots de X en fonction de p.

Une propriété des monoïdes de relations non ambigus

Nommons Valence d'une relation r sur un ensemble Q son cardinal (en tant que partie de $Q \times Q$) ; un monoïde de relations sur Q peut être non-ambigu sans que tous ses éléments non-nuls aient la même valence ; cependant, dans le cas des monoïdes très transitifs, on obtient le résultat suivant :

Théorème 3. Soit M *un monoïde de relations très transitif sur* Q *ne contenant pas la relation vide. Alors* M *est non-ambigu ssi tous ses éléments ont une valence égale à* $\mathrm{Card}(Q)$.

Démonstration. On nommera valence d'une matrice m à éléments dans $\mathbb{N}$ la somme de tous ses éléments, notée $|m|$, et, pour toute relation r sur Q, on notera $\bar{r}$ la matrice à éléments dans $\mathbb{N}$ égaux à 0 ou 1, indexée par Q dont le support est r ; la valence de r est encore égale à $|\bar{r}|$.

Supposons d'abord que tous les éléments de M aient la même valeur p et montrons que M est non-ambigu : cela revient à montrer que pour tous éléments m,m' de M, la matrice $\bar{m}\,\bar{m}'$ n'a que des éléments égaux à 0 ou 1. Supposons donc par l'absurde que $\bar{m}\,\bar{m}'$ a au moins un élément égal à 2 et calculons la somme $s = \sum_{u\in U} |m u m'|$, où U est le sous-groupe de M ; d'une part $s = p\,\mathrm{Card}(U)$ puisque chacun des $m u m'$ a une valence égale à p. D'autre part, s est strictement inférieur à la somme $t = \sum_{u\in U} |\bar{m}\,\bar{u}\,\bar{m}'|$ puisque : $|m m'| < |\bar{m}\,\bar{m}'|$.
Or, on a aussi $t = |\sum_{u\in U} \bar{m}\,\bar{u}\,\bar{m}'| = |\bar{m}\,K\,\bar{m}'|$ où K est la matrice dont tous les éléments sont égaux à $q = \frac{1}{p}\mathrm{Card}(U)$, puisque U est transitif. Ceci montre que $t = p\,\mathrm{Card}(U)$, en contradiction avec le fait que $s < t$.

La réciproque est conséquence directe du lemme ci-dessous :

Lemme. Soit M *un monoïde de relations très transitif sur un ensemble* Q *.*
Si M *contient un élément de valence strictement inférieur à* $p = \mathrm{Card}(Q)$*,*
alors M *contient la relation vide.*

Si M *contient un élément de valence strictement supérieur à* p *, alors* M *est ambigu.*

Démonstration. Soit m un élément de M et K la matrice dont tous les éléments sont égaux à 1. Nous évaluons de deux manières la valence de la matrice $(K\bar{m})^n$, pour un entier n quelconque. D'une part : $|(K\bar{m})^n| = p|m|^n$ puisque $|K\bar{m}| = p\,|m|$ et que $(K\bar{m})^2 = |m|\,K\bar{m}$.

D'autre part : $|(K\bar{m})^n| = \sum_{u_i \in U} \frac{1}{q^n} |\bar{u}_1 \bar{m} \ldots \bar{u}_n \bar{m}|$ puisque la matrice K est égale à $\frac{1}{q} \sum_{u \in U} \bar{u}$.

Tout d'abord, si M ne contient pas la relation vide, chacun des termes de la forme $\bar{u}_1 \bar{m} \ldots \bar{u}_n \bar{m}$ a une valence non nulle et cela implique que $|(K\bar{m})^n| \geq p^n$; on en déduit que l'inégalité $|m|^n \geq p^{n-1}$ est vraie pour tout entier n et cela implique que $|m| \geq p$.

Maintenant, si M est inambigu, chacun des termes de la somme a une valence au plus égale à p^2 et ceci implique que $|(K\bar{m})^n| \leq p^{n+2}$; on en déduit que l'inégalité $|m|^n \leq p^{n+1}$ est vraie pour tout entier n , ce qui implique $|m| \leq p$.

Nous revenons maintenant à un sous monoïde X^* de A^* possèdant des mots neutres incomplétables dans X c'est-à-dire, d'après le théorème 1 que X^* est reconnu par un monoïde M de relations très transitif sur un ensemble Q ; on notera p, comme ci-dessus, le cardinal de Q et on désignera par $|f|$ la valence de la relation sur Q définie par le mot $f \in A^*$.

Corollaire 1. Tout mot de A^* *est complétable dans* X^* *ssi* $|f| \geq p$ *pour tout mot* $f \in A^*$.

En effet, pour que tout mot soit complétable dans X^*, il faut et il suffit que le monoïde M ne contienne pas la relation vide et cet énoncé est donc une reformulation de la première assertion du lemme.

Corollaire 2. Si X^* *est librement engendré par* X *, on a* $|f| \leq p$ *pour tout* $f \in A^*$.

Cet énoncé est une reformulation de la deuxième assertion du lemme puisque X^* est librement engendré par X ssi le monoïde M est non-ambigu. Enfin, on sait que si X est un code reconnaissable, alors tout mot de A^* est complétable dans X^*ssi X est un code maximal (on en trouvera une preuve en [4] ou [6]). On peut donc reformuler le théorème 3 de la façon suivante :

Corollaire 3. X *est un code maximal ssi pour tout* $f \in A^*$*, on a* $|f| = p$.

Cet énoncé a une forme plus frappante dans le cas où X est un code fini puisque, dans ce cas, si a est une lettre dont une puissance est un mot neutre, la valeur de $f \in A^*$ est le nombre de mots de la forme $a^i f a^j$ qui sont dans X^* avec $0 \leq i,j \leq p-1$. Cette formulation fournit une analogie remarquable avec le cas particulier des codes préfixes maximaux où la condition que le nombre de mots de cette forme soit égal à p est trivialement vérifiée.

Références

1 BERSTEL, J.- Sur la densité asymptotique des langages formels, in *Automata Languages and Programming* (M. Nivat ed.) North Holland (1972) 345-58.

2 BOE, J.M.- *Représentations des monoïdes : applications à la théorie des codes*, Thèse de 3ème cycle, Univ. des Sciences et Techniques du Languedoc (1976).

3 BOE, J.M., BOYAT, J. CESARI, Y., LACHENY, A. et M. VINCENT, Automates et monoïdes syntaxiques des sous-monoïdes libres, à paraître dans *Information and Control*.

4 EILENBERG, S.- *Automata, Languages and Machines*, Vol. A, Academic Press (1974).

5 LALLEMENT, G.- On regular semigroups as syntactic monoids of prefix codes, à paraître dans *Theoretical Computer Science*.

6 NIVAT, M.- Eléments de la théorie générale des codes, in *Automata Theory* (E.R. Caianiello ed.) Academic Press (1966).

7 Mc NAUGHTON, R. and PAPERT, S.- *Counter-Free Automata,* MIT Press (1971).

8 PERROT, J-F.- *Contribution à l'Etude des Monoïdes Syntaxiques et de Certains Groupes Associés aux Automates Finis,* Thèse, Paris (1972).

9 RESTIVO, A.- On codes having no finite completions, in *Automata, Languages and Programming* (S. Michaelson ed.) Edinburgh University Press (1976) 38-44.