

BULLETIN DE LA S. M. F.

DOMINIQUE PERRIN

Codes asynchrones

Bulletin de la S. M. F., tome 105 (1977), p. 385-404

http://www.numdam.org/item?id=BSMF_1977__105__385_0

© Bulletin de la S. M. F., 1977, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (<http://smf.emath.fr/Publications/Bulletin/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). 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/>

CODES ASYNCHRONES

PAR

par DOMINIQUE PERRIN

[Univ. Rouen]

RÉSUMÉ. — L'article établit l'existence d'une famille nouvelle de sous-monoïdes libres finiment engendrés, dont la base est nommée code asynchrone. Leur construction fait intervenir certaines factorisations du monoïde libre qui sont le relèvement des factorisations en variables commutative obtenues par SCHÜTZENBERGER.

Introduction

Soit A un ensemble, et A^* le monoïde libre sur l'ensemble A ; un *code* sur l'alphabet A est une partie X de A^* qui engendre un sous-monoïde isomorphe au monoïde libre sur l'ensemble X . Les premières études sur ces objets remontent aux travaux de SHANNON, dans les années 1950, sur la théorie de la communication : un tel ensemble peut en effet être utilisé pour coder des suites de messages de telle façon que le résultat soit inambigu. Bien au-delà des problèmes de codage, ces objets se rencontrent en fait dans des domaines assez variés. Tout d'abord, et dans une optique assez proche de celle du codage, les codes préfixes, qui font l'objet de ce travail, donnent naissance aux événements récurrents étudiés par FELLER : un événement récurrent est le couple formé d'un code préfixe X et d'une distribution de probabilités sur X . Cette interprétation probabiliste fournit à la fois une traduction de certaines propriétés des codes ainsi, curieusement, qu'un moyen de prouver certaines d'entre elles.

Ensuite, et surtout, les codes sont un objet important de la théorie des langages formels et de la combinatoire du monoïde libre, qui trouve d'ailleurs des applications à d'autres domaines, comme celui des algèbres de Lie [18]; leur étude fait intervenir, de façon non classique, des propriétés des groupes de permutations ([10], [11]), ainsi que divers problèmes de combinatoire comme celui des factorisations de groupes cycliques.

Les codes *préfixes* (resp. *suffixes*) forment une famille de codes fort simple à construire : ce sont les parties de A^* formées de mots qui ne sont aucun

facteur gauche (resp. droit) l'un de l'autre. Il est plus malaisé de construire directement les codes *bipréfixes* (qui, par définition, sont à la fois préfixe et suffixe) ou, tout au moins, ceux qui sont maximaux; on peut en obtenir des exemples en choisissant un groupe G , un sous-groupe H de G , et un homomorphisme de A^* sur G : l'image réciproque de H est un sous-monoïde engendré par un code bipréfixe maximal; on démontre que le code bipréfixe ainsi obtenu est toujours infini, excepté le cas trivial du code homogène de longueur d , constitué de tous les mots de longueur d (cf. [16], IV. 2); on possède par ailleurs un algorithme direct de construction des codes bipréfixes finis [2].

En contraste avec la notion de code bipréfixe, on définit un code *synchronisant* comme un code préfixe X tel que X^* contienne un idéal à gauche de A^* : $A^*x \subset X^*$. Un code préfixe maximal, qui n'est pas synchronisant, est, par définition, *asynchrone*; on verra qu'on peut associer à tout code préfixe maximal X un entier positif, son *degré* $d(X)$, qui est égal à 1 si, et seulement si, X est synchronisant. Les codes bipréfixes maximaux fournissent un exemple typique de codes asynchrones, et on en obtient d'autres en considérant des inclusions $X^* \subset Y^* \subset A^*$ de sous-monoïdes libres; en effet, le code X n'est alors synchronisant que s'il en est de même de Y et de l'image de X dans le monoïde libre sur l'ensemble Y ; plus précisément, le degré de X est le produit des degrés des deux codes. Par exemple, si les longueurs des mots de X sont divisibles par un entier $d \neq 1$, alors X est un code asynchrone qui correspond à l'inclusion $X^* \subset (A^d)^* \subset A^*$. Un code X est *complètement décomposable* s'il existe une chaîne $Y_1^* \subset Y_2^* \subset \dots \subset Y_n^*$ avec $Y_1 = X$ et $Y_n = A$ telle que Y_i soit, sur l'alphabet Y_{i+1} , ou bien un code bipréfixe, ou bien un code synchronisant.

Le résultat principal de cet article (théorème 4.1) établit l'existence de codes préfixes maximaux finis qui ne sont pas complètement décomposables. Le fait surprenant est que ces codes soient finis: en effet, d'après un théorème de SCHÜTZENBERGER [17], si X est un code maximal fini, et si \mathbf{X} désigne le polynôme caractéristique de X (en les variables *commutatives* a de A), alors $1 - \mathbf{X}$ est divisible par $1 - \mathbf{A}$ et le *quotient n'est irréductible dans $\mathbf{Z}[A]$ que dans les deux cas suivants: soit X est préfixe (resp. suffixe) et synchronisant, soit X est bipréfixe*. On sait [1] qu'il existe cependant des codes maximaux finis indécomposables (i. e. ils engendrent un sous-monoïde libre maximal) qui ne sont ni préfixe ni suffixe; d'après ce qui précède, le polynôme $1 - \mathbf{X}$ a alors au moins trois facteurs non-triviaux dans $\mathbf{Z}[A]$. Et on a pu observer que, dans tous les cas connus, cette factorisation provient d'une factorisation (en variables non commutatives) du

polynôme caractéristique \mathcal{X} de X (qui est un élément de l'algèbre associative libre $\mathbf{Z}\langle A \rangle$). Dans le cas d'un code préfixe, on a toujours une factorisation de la forme $1 - \mathcal{X} = \mathcal{P}(1 - \mathcal{A})$, et si l'on peut trouver de plus une factorisation de la forme $1 - \mathcal{X} = \mathcal{L}(1 - \mathcal{A})\mathcal{K}$, alors X est certainement asynchrone. Notre résultat établit que l'on peut partir de factorisations de ce type pour construire des codes préfixes jouissant des propriétés cherchées : soit en fait X un code bipréfixe maximal fini, et f un mot dans A^* tel que

$$X f^{-1} \cap f^{-1} X = \{f^2\};$$

alors le polynôme non commutatif

$$R = (1 + f)(1 - \mathcal{X} - (1 - \mathcal{X} f^{-1}) f (1 - f^{-1} \mathcal{X}))$$

est de la forme $1 - \mathcal{Y}$, où Y est un code préfixe maximal dont le degré est égal à celui de X ; et si $d(X)$ est un nombre premier impair, alors Y est indécomposable (théorème 4.1). Cette construction présente une analogie frappante avec celle des codes bipréfixes finis décrite en [2]; le point essentiel est le fait que le deuxième facteur de l'expression qui définit R est divisible à droite et à gauche par $1 - \mathcal{A}$, ce qui assure l'existence des deux factorisations évoquées ci-dessus.

Le plan de cet article est odonné de la façon suivante :

Nous avons rassemblé, dans un premier paragraphe, les propriétés connues des codes dont nous aurons à faire usage. Le lecteur pourra aussi se reporter aux différents exposés qui ont été faits de ces questions ([9], [5], chap. IV, [12]).

On démontre, dans la deuxième partie, un résultat de nature combinatoire sur les codes bipréfixes : *un code préfixe maximal fini X est bipréfixe si, et seulement si, l'ensemble des facteurs gauches de ses mots est une union disjointe de $d(X)$ codes suffixes maximaux* (théorème 2.2.1). Ce résultat fournit une preuve directe ainsi qu'une interprétation naturelle d'un énoncé probabiliste établi en [16]; il nous permet aussi d'établir que, pour tout code préfixe X complètement décomposable, il existe deux parties K, L de A^* telles que le polynôme $1 - \mathcal{X}$ se factorise dans $\mathbf{Z}\langle A \rangle$ en $1 - \mathcal{X} = \mathcal{L}(1 - \mathcal{A})\mathcal{K}$, où K est une somme disjointe de $d(X)$ codes préfixes maximaux. Précisant alors le résultat principal de [17], nous montrons, dans une troisième partie, qu'une telle factorisation existe toujours en variables commutatives, même si X n'est pas complètement décomposable (théorème 3.1). Le paragraphe 4 contient notre résultat principal (théorème 4.1); sa preuve utilise le résultat précédent.

Dans une dernière partie, nous établirons une propriété des codes asynchrones finis dont le degré est un nombre premier p (théorème 5.1) : *un tel code contient tous les mots de la forme a^p pour $a \in A$* (le fait que cette propriété des codes bipréfixes finis soit vraie, sans restriction sur le degré, est un corollaire de 2.2.1); la preuve utilise un théorème de Sands sur les factorisations de groupes cycliques [13]. Nous ne savons pas si cette propriété est vraie sans restriction sur le degré du code. Si elle l'était, cela impliquerait que le groupe d'un code asynchrone indécomposable fini (cf. [11]) contient un cycle de longueur égale à son degré, comme dans le cas des codes bipréfixes (cf. [10]).

1. Rappel de propriétés connues

On note A^* le monoïde libre sur l'ensemble (ou alphabet) A , et on désigne par 1 son élément neutre (le mot vide); il est commode de poser $A^+ = A^* \setminus \{1\}$. Pour deux parties L, M de A^* , on désigne par $L^{-1}M$ l'ensemble

$$L^{-1}M = \{u \in A^*; Lu \cap M \neq \emptyset\}$$

et symétriquement,

$$ML^{-1} = \{u \in A^*; uL \cap M \neq \emptyset\}.$$

1.1. *Codes.* — Une partie X de A^* est un *code* sur l'alphabet A si X engendre librement un sous-monoïde de A^* ; c'est-à-dire encore si tout élément du sous-monoïde X^* engendré par X se décompose de façon unique comme produit d'éléments de X .

Une partie X de A^* est *préfixe* si elle ne contient aucun facteur gauche propre d'un de ses éléments; ce qui s'écrit $X^{-1}X = \{1\}$. La proposition suivante, que l'on vérifie directement, montre en particulier qu'une partie préfixe est un code (on dit que c'est un code préfixe).

PROPOSITION 1.1.1. — *Un sous-monoïde M de A^* est engendré par une partie préfixe si, et seulement si, il est unitaire, c'est-à-dire si $M^{-1}M = M$.*

Une partie L de A^* qui rencontre tous les idéaux à droite de A est dite *complète* (à droite); formellement, L est complète si $L(A^*)^{-1} = A^*$. On vérifie alors la propriété suivante :

PROPOSITION 1.1.2. — *Soit X un code préfixe; les conditions suivantes sont équivalentes :*

1° *le sous-monoïde X^* est complet;*

2° l'ensemble XA^* est complet;

3° X est un code préfixe maximal (c'est-à-dire une partie préfixe maximale).

Ainsi, si X est un code préfixe maximal, l'ensemble $P = A^* \setminus XA^*$ des mots qui n'ont pas de facteur gauche dans X s'identifie à l'ensemble $X(A^+)^{-1}$ des facteurs gauches propres des mots de X ; un élément de P est, par définition, un *préfixe* de X , et on vérifie facilement que tout mot $u \in A^*$ se factorise de manière unique en $u = xp$, où $x \in X^*$ et p est un préfixe de X . De ce fait, on définit une action de A^* sur P en posant, pour tout $p \in P$ et $u \in A^*$,

$$p \cdot u = p' \quad \text{si, et seulement si, } pu = xp', \quad \text{avec } x \in X^*, p' \in P.$$

On obtient ainsi un homomorphisme que l'on notera ξ_X , ou simplement ξ , de A^* dans le monoïde des applications de P dans lui-même; et X^* est l'ensemble des $x \in A^*$ tels que $x\xi$ fixe $1 \in P$.

Nous aurons besoin de la propriété suivante, qui est trivialement vraie si X est un ensemble fini.

PROPOSITION 1.1.3. — *Soit X un code préfixe maximal; si X ne rencontre pas tous les idéaux bilatères, le monoïde $A^* \xi$ contient des éléments de rang fini (en tant qu'applications).*

Démonstration. — Soit $u \in A^*$ un mot tel que $A^* u A^* \cap X = \emptyset$; l'image de l'application $u\xi$ est alors contenue dans l'ensemble des facteurs droits de u puisque, pour tout $p \in P$, pu ne peut être dans P et que u est donc dans $A^*(p \cdot u)$. Ainsi le rang de $u\xi$ est au plus égal à la longueur de u . ■

L'hypothèse de la proposition précédente est encore vérifiée si X est reconnaissable (cf. [5]) c'est-à-dire s'il existe un homomorphisme φ de A^* sur un monoïde fini S tel que $X = X\varphi\varphi^{-1}$. Soit en effet, dans ce cas, s un élément de l'idéal minimal de S , et $u \in s\varphi^{-1}$; si $A^* u A^*$ rencontre X en vuw , on a alors $(vuw)^n \in X$ pour tout entier n tel que $(vuw)^n \varphi = vuw\varphi$, en contradiction avec le fait que X est un code.

On déduit de 1.1.3, la propriété suivante, qui n'est pas vraie pour un code quelconque (cf. [15], [5]).

PROPOSITION 1.1.4. — *Soit X un code ne rencontrant pas tous les idéaux bilatères. Les conditions suivantes sont équivalentes :*

1° X est un code préfixe maximal;

2° le sous-monoïde X^* est complet;

3° X est un code maximal qui est préfixe.

Démonstration. — Nous avons vu, en 1.1.2, que 1° entraîne 2° sans hypothèse supplémentaire sur X . Supposons maintenant que 2° soit vérifiée, et soit $Y = X \setminus XA^+$; l'ensemble Y est par définition un code préfixe, et il est maximal puisque $YA^* = XA^*$ et que ce dernier est complet. Soit alors u un mot tel que $u\xi_Y$ soit de rang minimal dans $A^*\xi_Y$; comme Y^* est complet, on peut supposer que $u \in Y^*$. Alors, pour tout mot v de A^* , le mot uvu a une puissance qui est dans X^* , puisqu'il existe un entier k tel que $(uvu)^k \xi_Y = u \xi_Y$; et $Y \cup \{v\}$ n'est donc pas un code. Ceci montre que Y est un code maximal et que $Y = X$, d'où l'assertion 3°. Enfin, 3° implique évidemment 1°. ■

Remarque. — D'après 1.1.3, si X est un code préfixe maximal qui ne rencontre pas tous les idéaux bilatères, le monoïde $A^*\xi$ possède des idéaux minimaux à droite et à gauche, et son groupe de Suškevič (cf. [2]) est fini. En fait, cela est vrai, de façon plus générale, du monoïde syntaxique d'un code qui ne rencontre pas tous les idéaux bilatères; ceci permet de montrer que, sous cette hypothèse, un code est maximal si, et seulement si, X^* rencontre tous les idéaux bilatères (cf. [15], [5]).

1.2. *Synchronisation.* — Soit X un code préfixe maximal, qui ne rencontre pas tous les idéaux bilatères. D'après 1.1.3, l'ensemble des rangs des éléments du monoïde $A^*\xi$ possède un minimum qui est, par définition, le degré de X noté $d(X)$. L'ensemble des éléments de $A^*\xi$ de rang $d(X)$ est une union de groupes de permutations transitifs de degré $d(X)$ tous équivalents à un groupe que l'on nomme groupe de X (cf. [10], [11]).

Si $d(X) = 1$, on dit que X est *synchronisant* et, sinon, qu'il est *asynchrone*. On vérifie que X est synchronisant si, et seulement si, X^* contient un idéal à gauche : $A^*x \subset X^*$.

Remarque. — Dans le cas d'un code X qui n'est pas préfixe, on dit que X est synchronisant s'il existe deux mots $x, y \in X^*$ tels que, pour tous u, v de A^* ,

$$uxyv \in X^* \Rightarrow ux, yv \in X^* \quad (\text{cf. [8], [9]}).$$

Dans le cas où X est préfixe maximal, cette définition coïncide avec la précédente. On observera de plus que la définition du degré de x est, en un sens, indépendante du monoïde $A^*\xi$ construit ci-dessus : en effet, si l'on suppose pour simplifier les choses que X est reconnaissable, soit ϕ un quelconque morphisme de A^* sur un monoïde fini S tel que

$X^* \varphi \varphi^{-1} = X^*$; on démontre alors que l'index dans le groupe de Suškevič de S , du sous-groupe qui est son intersection avec $X^* \varphi$, est égal à $d(X)$. En particulier, X est synchronisant si, et seulement si, le groupe de Suškevič de son monoïde syntaxique est trivial.

1.3. *Décompositions.* — Soient X et Y deux codes sur l'alphabet A ; si X est inclus dans le sous-monoïde Y^* , l'image de X dans le monoïde libre sur l'ensemble Y est encore un code, et on dit que X se *décompose* sur Y . Inversement, si Y est un code sur l'alphabet A , et Z un code sur l'alphabet Y , l'image de Z dans A^* est encore un code que l'on note $X = Z \otimes Y$. Si Y et Z sont préfixes (resp. préfixes maximaux), il en est de même de X ; réciproquement on a le résultat suivant :

PROPOSITION 1.3.1. — *Si X est préfixe maximal et si Y ne rencontre pas tous les idéaux bilatères, alors Y et Z sont préfixes maximaux.*

Démonstration. — Si X est préfixe maximal, Z est préfixe, et Y^* est complet. Mais si Y ne rencontre pas tous les idéaux bilatères, d'après 1.1.4, Y est alors préfixe maximal. Et Z est lui aussi maximal puisque, pour tout $u \in A^*$, il existe un $v \in A^*$ tel que $uv \in X^*$ et que $v \in Y^*$, du fait que Y^* est unitaire. ■

La conclusion de cette proposition est vraie en particulier sous l'hypothèse que X est un code préfixe maximal fini puisque Y est alors lui aussi fini. Supposons, plus généralement, que X et Y soient préfixes maximaux et ne rencontrent pas tous les idéaux bilatères; on a alors le résultat suivant qui montre en particulier que X est synchronisant si, et seulement si, Z et Y le sont aussi.

PROPOSITION 3.2. — *Les degrés se multiplient par composition : $d(X) = d(Z) d(Y)$.*

Démonstration. — Soient P_X, P_Y, P_Z les ensembles de préfixes de X, Y et Z respectivement. On peut identifier P_X au produit $P_Z \times P_Y$ puisque l'application qui à $p \in P_X$ fait correspondre le couple $(r, q) \in P_Z \times P_Y$ tel que $p = rq$ est bijective. Le monoïde $A^* \xi_X$ s'identifie alors à un sous-monoïde du produit en couronne $Y^* \xi_Z \wr A^* \xi_Y$, en faisant correspondre à $u \in A^*$ le couple $(\bar{u}, u \xi_Y)$ où \bar{u} est l'application qui à $q \in P_Y$ fait correspondre l'élément $y \xi_Z$ défini par $qu = yq'$, avec $y \in Y^*, q' \in P_Y$. Or le minimum des rangs des éléments du produit en couronne de deux monoïdes d'applications est le produit des minimums dans les deux monoïdes, d'où le résultat. ■

2. Codes bipréfixes

2.1. *Définition.* — Si X est un code préfixe, il n'en est pas de même, en général, de l'ensemble \tilde{X} des images miroir des mots de X définies par

$$\tilde{x} = a_n \dots a_2 a_1 \quad \text{si } x = a_1 a_2 \dots a_n, \text{ avec } a_i \text{ dans } A;$$

on dit de \tilde{X} qu'il est *suffixe*. Dans le cas où X et \tilde{X} sont simultanément des codes préfixes, on dit que X est *bipréfixe*. La proposition suivante montre que les codes bipréfixes maximaux sont, en particulier quand X est fini, susceptibles de plusieurs définitions équivalentes (cf. [16]).

PROPOSITION 2.1.1. — *Soit X un code qui ne rencontre pas tous les idéaux bilatères; les conditions suivantes sont équivalentes :*

- 1° X est bipréfixe maximal;
- 2° X est préfixe maximal et suffixe;
- 3° X est préfixe et \tilde{X}^* est complet.

Démonstration. — Si X est bipréfixe maximal, et s'il n'est pas maximal en tant que code préfixe, il doit être maximal en tant que code suffixe : en effet, si $X \cup \{w\}$ est préfixe et si $X \cup \{w'\}$ est suffixe, $X \cup \{ww'\}$ est bipréfixe. Mais, d'après 1.1.4, il est alors maximal en tant que code, et donc aussi maximal en tant que code préfixe. Maintenant si 2° est vérifiée, X est alors maximal en tant que code, donc en tant que code suffixe, d'où 3°.

Enfin, si la condition 3° est satisfaite, d'après 1.1.4, X est un code maximal qui est suffixe, d'où l'assertion 1°. ■

Remarque. — Si X est fini (ou, plus généralement, reconnaissable), les conditions de la proposition sont encore équivalentes au fait que tout mot de A^* a une puissance dans X^* . Cette condition implique en effet en particulier que X^* et \tilde{X}^* sont complets, ce qui entraîne que X soit préfixe et suffixe maximal. Réciproquement, si φ est un homomorphisme de A^* sur un monoïde fini S tel que $X^* = X^* \varphi \varphi^{-1}$, tout mot u de A^* possède une puissance u^k dont l'image par φ est un idempotent. Si $v \in A^*$ est un mot tel que $u^k v \in X^*$, on a alors aussi $u^{2k} v \in X^*$, d'où $u^k \in X^*$, du fait que \tilde{X}^* est unitaire.

2.2. *Propriété caractéristique.* — Soit X un code préfixe maximal qui ne rencontre pas tous les idéaux bilatères. Nous prouvons le résultat suivant :

THÉORÈME 2.2.1. — *Le code X est bipréfixe si, et seulement si, l'ensemble de ses préfixes est une union disjointe d'un nombre fini de codes suffixes maximaux. Ce nombre est alors égal au degré de X .*

Démonstration. — Supposons tout d'abord que X est bipréfixe maximal, et montrons que l'ensemble S de ses suffixes (c'est-à-dire de ses facteurs droits propres) est une union disjointe de codes préfixes maximaux; cela établira la partie directe du résultat puisque \tilde{S} est l'ensemble des préfixes de \tilde{X} . Soit pour cela u un mot tel que X ne rencontre pas $A^* u A^*$, et I l'ensemble des facteurs droits de u qui sont dans l'ensemble P des préfixes de X ; posons, pour tout $i \in I$, $R_i = \{i\}^{-1} X$. Du fait que X est préfixe, chacun des R_i est préfixe et, puisque XA^* est complet, $R_i A^*$ l'est aussi; ainsi chaque R_i est un code préfixe maximal inclus dans S . De plus, les R_i sont deux à deux disjoints du fait que X est suffixe. Enfin, tout s de S appartient à l'un des R_i puisque si $v \in A^*$ est tel que vus soit dans X^* , il découle de la définition de u qu'il existe un i dans I tel que is soit dans X . Ainsi S est l'union disjointe des R_i pour i dans I . Enfin, l'ensemble I a $d(X)$ éléments : en effet, l'image de $u\xi$ est égale à I ; et le rang de $u\xi$ est minimal puisque si, pour $i, j \in I$, et $v \in A^*$, on a $i.v = j.v$, on déduit du fait que X est suffixe l'égalité $i = j$.

Réciproquement, supposons que l'ensemble P des préfixes de X soit une union disjointe de codes suffixes maximaux S_i , $1 \leq i \leq n$. Nous montrons que $\tilde{X}A^*$ est complet, ce qui implique que \tilde{X}^* est complet et donc, d'après 2.1.1, que X est bipréfixe. Soit donc v un mot quelconque de A^* et $w = uv$, où u est, comme ci-dessus, un mot tel que $A^* u A^* \cap X = \emptyset$. Posons $w = w' a$, avec $a \in A$, et notons D (resp. D') l'ensemble des facteurs droits de w (resp. w') qui sont dans P . Du fait que les S_i sont des codes suffixes, l'ensemble D (resp. D') a au plus un élément dans chacun des S_i . Et si D (resp. D') ne rencontre pas S_i , on déduit du fait que $\tilde{S}_i A^*$ est complet, l'existence d'un mot $t \in A^*$ tel que $tw \in S_i$ (resp. $tw' \in S_i$); cela entraîne l'existence d'un mot $z \in A^*$ tel que $twz \in X$, en contradiction avec la définition de u . Ainsi D et D' ont tous les deux le même nombre n d'éléments; or D et D' n'ont pas le même nombre d'éléments puisque 1 est dans D mais pas dans D' . Cela implique l'existence d'un $p \in D'$ tel que pa ne soit pas dans D ; mais de $p \in P$, $pa \notin P$, on déduit que $pa \in X$, et donc que $w = uv$ appartient à $A^* X$, ce qui achève de prouver le résultat.

Le corollaire ci-dessous implique en particulier que, si X est fini, tous les idempotents de $A^* \xi$ distincts de 1 sont de rang $d(X)$ (cf. [16], [10]).

COROLLAIRE 2.2.2. — *Si X est un code bipréfixe maximal, tout mot u de A^* tel que $A^* u A^* \cap X = \emptyset$ a $d(X)$ facteurs droits qui sont des préfixes de X .*

En effet, u a au plus un facteur droit dans chacun des $d(X)$ codes suffixes dont l'ensemble des préfixes de X est l'union disjointe; et il en a au moins un dans chacun d'eux sans quoi $A^* u A^* \cap X$ n'est pas vide. On en déduit le résultat suivant :

COROLLAIRE 2.2.3. — *Si X est un code bipréfixe maximal fini, il contient $a^{d(X)}$ pour toute lettre a de A .*

En effet, si X est fini, il existe un entier n tel que $A^* a^n A^* \cap X = \emptyset$, d'où le résultat.

Remarque. — Le théorème précédent donne une preuve directe ainsi qu'une interprétation naturelle du résultat de [16] suivant lequel la longueur moyenne d'un code bipréfixe maximal, relativement à une distribution de probabilités sur l'alphabet, est un entier. En effet, soit $\pi : A \rightarrow]0, 1[$ une application de somme 1 sur A étendue multiplicativement à A^* ; si X est un code préfixe maximal qui ne rencontre pas tous les idéaux bilatères, on a $\pi X = \sum_{x \in X} \pi x = 1$, et la longueur moyenne de X , définie par $\lambda X = \sum_{x \in X} \pi x |x|$, est finie et égale à πP (cf. [5], [6]). Ainsi, si P est l'union des d codes suffixes maximaux S_i , on a

$$\pi P = \sum_{i=1}^d \pi S_i = d.$$

2.3. Codes complètement décomposables. — On dira qu'un code préfixe maximal X est complètement décomposable s'il existe une décomposition de X en $X = Y_1 \otimes \dots \otimes Y_n$, où chacun des Y_i est, soit synchronisant, soit bipréfixe. Cette famille de codes contient donc, en particulier, les codes synchronisants et les codes bipréfixes; nous montrons tout de suite par un exemple (dû à SCHÜTZENBERGER ⁽¹⁾) que tous les codes préfixes maximaux n'y appartiennent pas.

Exemple. — Soit $A = \{a, b\}$, et φ le morphisme de A^* dans le monoïde des applications de l'ensemble $Q = \{1, 2, 3, 4, 5, 6, 7\}$ dans lui-même, défini par

$$a\varphi = \left(\begin{array}{c|c|c} 2 & 3 & 1 \\ \hline 1, 5 & 2, 6 & 3, 4, 7 \end{array} \right), \quad b\varphi = \left(\begin{array}{c|c|c|c} 6 & 1 & 4 & 5 \\ \hline 1 & 2 & 3 & 4, 5 \\ \hline & & & 6 & 7 \end{array} \right).$$

Soit M le sous-monoïde unitaire qui est le stabilisateur du point $1 \in Q$: $M = \{m \in A^*; 1.m\varphi = 1\}$; M est complet car, pour tout $q \in Q$, il existe un $u \in A^*$ tel que $q.u\varphi = 1$. Ainsi M est engendré par un code préfixe maximal X . Ce code n'est pas bipréfixe puisque $b^2 a$ et $b^4 a$ sont

⁽¹⁾ Communication personnelle.

dans X , sans que b^2 soit dans X^* . Il est asynchrone de degré égal à 3; en effet, $A^* a^3$ est inclus dans $X^* \{1, a, a^2\}$, et ceci montre que $a^3 \notin$ de rang 3; ce rang est minimal puisque $\mathcal{Q} \cdot \{1, a, a^2\} = \{1, 2, 3\}$ et que l'on vérifie que la famille de parties de \mathcal{Q} , composée de $\{1, 2, 3\}$, $\{1, 4, 6\}$, $\{5, 6, 7\}$, est stable par l'action de A .

De plus, le code X est indécomposable; supposons en effet que $X = Z \otimes Y$, et distinguons plusieurs cas : tout d'abord, si l'ensemble $1.Y^* \varphi$ contient le point 2; alors $b \in Y$ puisque $2.b \varphi = 1$; mais comme $b^2 a \in X$, on en déduit que $a \in Y$ et donc que $Y = A$. Ensuite, si $1.Y \varphi$ contient un élément de l'ensemble $\{3, 4, 7\}$, alors $a \in Y$ et donc $b \in Y$ puisque $ab \in X$, ce qui entraîne $Y = A$. Enfin, si $5 \in 1.Y^* \varphi$, alors $ba^3 \in Y^*$ et donc $3 \in 1.Y^* \varphi$; et si $6 \in 1.Y^* \varphi$, alors $ba \in Y^*$ et donc $3 \in 1.Y^* \varphi$. Ainsi, si Y est différent de A , l'ensemble $1.Y^*$ est réduit à $\{1\}$, ce qui signifie que $Y = X$.

Nous établissons maintenant, comme corollaire de 2.2, la propriété suivante. Soit X un code préfixe maximal qui ne rencontre pas tous les idéaux bilatères.

PROPOSITION 2.3. — *Si X est complètement décomposable, il existe deux parties K et L de A^* telles que :*

1° *K est une union disjointe de $d(X)$ codes préfixes maximaux;*

2° *tout mot u de A^* se décompose de façon unique en $u = kxl$ avec $k \in K$, $x \in X^*$, $l \in L$.*

Démonstration. — On peut supposer, par hypothèse de récurrence, que $X = Z \otimes Y$ avec Z synchronisant ou bien bipréfixe, et que la propriété est vraie de Y , avec deux parties K' et L' de A^* .

Si Z est synchronisant, soit $M \subset Y^*$ l'ensemble des préfixes de Z ; la propriété est alors vraie de X en posant $K = K'$ et $L = ML'$.

Si Z est bipréfixe, d'après le théorème 2.2, l'ensemble $N \subset Y^*$ des suffixes de Z est une union disjointe de $d(Z)$ codes préfixes maximaux. Ceci implique que l'ensemble $K = K' M$ soit une union disjointe de $d(X) = d(Z) d(Y)$ codes préfixes maximaux et établit la propriété. ■

Remarque. — La propriété ci-dessus est encore vraie pour le code X de l'exemple précédent (bien qu'il ne soit pas complètement décomposable) : on vérifie en effet qu'en posant $L = (b^2)^*$ et $K = 1 + D_2 + D_3$, où D_i est l'ensemble des suffixes de X tels que $i.d = 1$, tout mot $u \in A^*$ se décompose de manière unique en $u = kxl$, avec $k \in K$, $l \in L$.

3. Le théorème de factorisation polynomiale

On note $\mathbf{Z} \ll A \gg$ l'anneau des séries en les variables non commutatives a de A à coefficients dans \mathbf{Z} et $\mathbf{Z} \langle A \rangle$ l'anneau correspondant de polynômes (qui est l'algèbre de A^* sur \mathbf{Z}). Pour une partie L de A^* , on désigne par \mathcal{L} la série caractéristique de L ; avec ces notations, on vérifie que X est un code si, et seulement si, l'inverse de la série $1 - \mathcal{X}$ est égale à la série \mathcal{M} , avec $M = X^*$. De plus, si X est un code préfixe maximal et P l'ensemble de ses préfixes, on a l'égalité : $\mathcal{A}^* = \mathcal{X}^* \mathcal{P}$ ou, de façon équivalente, $1 - \mathcal{X} = \mathcal{P} (1 - \mathcal{A})$. On note encore $\mathbf{Z} [[A]]$ (resp. $\mathbf{Z} [A]$) l'anneau des séries (resp. des polynômes) en les variables commutatives a de A ; pour une partie L de A^* , on note \mathbf{L} l'image de la série \mathcal{L} par le morphisme canonique de $\mathbf{Z} \ll A \gg$ sur $\mathbf{Z} [[A]]$; en particulier, pour tout u dans A^* , \mathbf{u} peut être considéré comme un élément du monoïde commutatif libre sur A .

Soit maintenant X un code maximal fini sur l'alphabet \bar{A} ; le théorème de factorisation polynomiale de Schützenberger [17] affirme que le polynôme $1 - \mathbf{X}$ est divisible par $1 - \mathbf{A}$ et que le quotient n'est irréductible dans $\mathbf{Z} [A]$ que dans les cas suivants :

- 1° X est préfixe et synchronisant;
- 2° X est suffixe et synchronisant;
- 3° X est bipréfixe.

Nous en démontrons une version plus précise : disons pour cela qu'un ensemble H de préfixes de X est une classe de synchronisation s'il existe un mot x de X^* tel que Hx soit inclus dans X^* , et que H soit maximal pour cette propriété. En particulier, X est synchronisant si, et seulement si, $H = P$, et bipréfixe si, et seulement si, $H = \{1\}$.

THÉORÈME 3.1. — *Soit X un code préfixe maximal fini. Le polynôme $1 - \mathbf{X}$ se factorise dans $\mathbf{Z} [A]$ en $1 - \mathbf{X} = L(1 - \mathbf{A}) K$ avec $K \equiv d(X) \pmod{1 - \mathbf{A}}$ et $L \equiv \mathbf{H} \pmod{1 - \mathbf{A}}$ pour toute classe de synchronisation H .*

La démonstration s'appuie sur quatre lemmes; les trois premiers sont des énoncés extraits de [17] dont nous omettons la preuve.

LEMME 3.2 ([17], (4)). — *Pour toute classe de synchronisation H , on a*

$$d(X) \mathbf{H} \equiv P \pmod{1 - \mathbf{A}}.$$

Soit maintenant R la $P \times P$ matrice à éléments dans $\mathbf{Z}[A]$, définie par

$$R_{p,q} = \mathbf{A}_{p,q} \quad \text{où} \quad \mathbf{A}_{p,q} = \{a \in A; p.a = q\},$$

et notons I_p la $P \times P$ matrice identité.

LEMME 3.3 ([17] (1.3)). $1 - \mathbf{X} = \det(I_p - R)$.

Soit maintenant Γ l'ensemble des parties de P de la forme $Q.u$ pour tout $u \in A^*$ tel que $u\xi$ soit de rang $d(X)$. Notons V le $\mathbf{Z}[A]$ -module libre sur P , et W le sous-module de V engendré par les \mathcal{J} , pour tout J dans Γ ; l'action à droite de la matrice R définit un endomorphisme ρ de V qui stabilise W : en effet, pour tout $J \in \Gamma$, on a $\mathcal{J}.R = \sum_{a \in A} \mathbf{a}(\mathcal{J}.a)$ et $J.a$ appartient encore à Γ . Notons σ l'endomorphisme de W qui est la restriction à W de ρ et σ' l'endomorphisme de $W' = V/W$ induit par ρ . D'après 3.3, on a

$$1 - \mathbf{X} = \det(I_W - \sigma) \det(I_{W'} - \sigma').$$

LEMME 3.4 ([17], p. 220). — Il existe deux polynômes $L, L' \in \mathbf{Z}[A]$ tels que :

$$\det(I_W - \sigma) = (1 - \mathbf{A})L \quad \text{et} \quad L \equiv L' \mathbf{H} \pmod{1 - \mathbf{A}}$$

pour toute classe de synchronisation H .

Nous établissons maintenant le quatrième lemme.

LEMME 3.5. — Il existe un polynôme $K' \in \mathbf{Z}[A]$ tel que

$$\det(I_{W'} - \sigma') \equiv d(X)K' \pmod{1 - \mathbf{A}}$$

Démonstration. — Soit Q une partie de P qui forme une base d'un complémentaire de W dans V ; si l'on identifie W' au $\mathbf{Z}[A]$ -module libre sur Q , l'image par σ' d'un $q \in Q$ est l'élément $\sum_{r \in Q} \lambda_r r$ de V , défini par

$$q.\rho - \sum \lambda_r r \in W.$$

Mais, pour tout $w \in W$, le produit scalaire (w, \mathcal{P}) est dans $d(X)\mathbf{Z}[A]$, puisque si $w = \sum_{J \in \Gamma} \lambda_J \mathcal{J}$, alors :

$$(w, \mathcal{P}) = \sum_{J \in \Gamma} \lambda_J (\mathcal{J}, \mathcal{P}) = d(X) \sum_{J \in \Gamma} \lambda_J.$$

Comme, d'autre part $(q.\rho, \mathcal{P}) = \mathbf{A}$, on en déduit que, pour tout q de Q , $(q.\sigma', \mathcal{P})$ appartient à $\mathbf{A} + d(X)\mathbf{Z}[A]$; cela implique que le déterminant de $\mathbf{A}I_{W'} - \sigma'$ soit dans $d(X)\mathbf{Z}[A]$, d'où le lemme. ■

Ainsi, d'après 3.4 et 3.5, $1 - \mathbf{X} = L(1 - \mathbf{A})K$, avec

$$LK \equiv L'K' \mathbf{H} d(X) \pmod{1 - \mathbf{A}};$$

comme, d'après 3.2, on a d'autre part :

$$\mathbf{P} \equiv d(X)H \pmod{(1-\mathbf{A})},$$

on en déduit que $K' L' \equiv 1 \pmod{(1-\mathbf{A})}$, ce qui implique, soit

$$K' \equiv L' \equiv 1 \pmod{(1-\mathbf{A})},$$

et le théorème est démontré, soit

$$K' \equiv L' \equiv -1 \pmod{(1-\mathbf{A})},$$

et le théorème est encore vrai avec $1-\mathbf{X} = (-L)(1-\mathbf{A})(-K)$. ■

Le corollaire suivant montre en particulier que si X contient a^n et b^m pour deux lettres $a, b \in A$ telles que $(n, m) = 1$, alors il est synchronisant.

COROLLAIRE 3.6. — *Soit X un code préfixe maximal fini; pour chaque lettre a de A , l'entier n tel que $a^n \in X$ est un multiple de $d(X)$.*

En effet, il suffit de calculer la valeur du polynôme $1-\mathbf{X}$ au point $\mathbf{a} = 1$, $\mathbf{b} = 0$ pour tout $\mathbf{b} \neq \mathbf{a}$.

4. Une famille remarquable de codes asynchrones finis

Nous présentons maintenant la construction qui permet d'obtenir des codes finis asynchrones indécomposables autres que les codes bipréfixes.

Soit pour cela X un code bipréfixe maximal fini, et $f \in A^*$ un mot qui est à la fois un préfixe et un suffixe de X ; notons G et D les codes respectivement préfixe et suffixe maximaux définis par $G = Xf^{-1}$, $D = f^{-1}X$, et soit Z l'élément de $\mathbf{Z}\langle A \rangle$ défini par

$$Z = \mathcal{X} + (1-\mathcal{G})f(1-\mathcal{D}).$$

On vérifie que si $Gf \cap fD = \emptyset$, Z est le polynôme caractéristique d'un code bipréfixe de même degré que X . Et, d'après le théorème de Césari [2], tout code bipréfixe fini peut être obtenu par de telles transformations à partir d'un code homogène A^d . Par contre, si $Gf \cap fD$ n'est pas vide, les coefficients de Z ne sont plus tous positifs; cependant on a le résultat suivant.

THÉORÈME 4.1. — *Si $Gf \cap fD = \{f^2\}$, alors :*

$$T = 1 - (1+f)(1-Z)$$

est le polynôme caractéristique d'un code préfixe maximal fini Y qui n'est pas bipréfixe et dont le degré d est égal à celui de X ; de plus, si d est un nombre premier distinct de 2, Y est indécomposable.

Démonstration. — Montrons tout d'abord que T est le polynôme caractéristique d'un code préfixe maximal. Posons pour cela $\mathcal{G} = \mathcal{G}_1 + f$, et notons X_1 le code préfixe maximal donné par

$$X_1 = X - \mathcal{G}_1 f + \mathcal{G}_1 f \mathcal{D},$$

on a alors :

$$Z = X_1 + f - f \mathcal{D} + f^2 \mathcal{D} - f^2,$$

d'où on déduit :

$$T = X_1 - f \mathcal{D} + f X_1 - f^3 + f^3 \mathcal{D}.$$

Or, du fait que $Gf \cap fD$ est réduit à f^2 , l'ensemble fD est contenu dans X_1 ; cela entraîne que $X_2 = X_1 - f\mathcal{D} + fX_1$ soit le polynôme d'un code préfixe maximal; et comme X_2 contient f^3 , $T = X_2 - f^3 + f^3 \mathcal{D}$ est donc aussi le polynôme d'un code préfixe maximal Y , qui n'est pas bipréfixe puisque, par exemple, fgd et gd sont tous deux dans Y pour tout g de G_1 .

Désignons par Q l'ensemble des suffixes de X et par R celui de G ; on a alors, du fait que X est bipréfixe

$$1 - Z = (1 - \mathcal{A})(\mathcal{Q} - \mathcal{R}f + \mathcal{R}f\mathcal{D}),$$

d'où on déduit :

$$1 - \mathcal{Y} = (1 + f)(1 - \mathcal{A})(\mathcal{Q} - \mathcal{R}f + \mathcal{R}f\mathcal{D}),$$

où le polynôme $\mathcal{Q} - \mathcal{R}f + \mathcal{R}f\mathcal{D}$ est un polynôme caractéristique puisque Rf est inclus dans Q et que $RfD \cap Q = \emptyset$; si l'on pose

$$\mathcal{K} = \mathcal{Q} - \mathcal{R}f + \mathcal{R}f\mathcal{D},$$

on obtient donc :

$$1 - \mathcal{Y} = (1 + f)(1 - \mathcal{A})\mathcal{K},$$

ou, de façon équivalente :

$$\mathcal{A}^* = \mathcal{K}\mathcal{Y}^*(1 + f).$$

De plus, en variables commutatives, on a $\mathbf{K} \equiv \mathbf{Q} \pmod{1 - \mathbf{A}}$ puisque $\mathcal{K} = \mathcal{Q} + \mathcal{R}f(1 - \mathcal{D})$ et que $1 - \mathbf{D} \equiv 0 \pmod{1 - \mathbf{A}}$; on en déduit que $\mathbf{K} \equiv d(X) \pmod{1 - \mathbf{A}}$. Par ailleurs, $\{1, f\}$ est une classe de synchronisation : supposons en effet qu'il existe un $y_0 \in Y^*$ et un préfixe u de Y tels que $\{1, f, u\}y_0 \subset Y^*$. Posons $u = kyl$ avec $k \in K$, $y \in Y^*$ et $l = 1$ ou f ; si k est distinct de 1, le mot uy_0 a deux factorisations distinctes dans le produit KY^* , ce qui est impossible; ceci montre que $u = yl$, et donc que $u = l$ puisque u est un préfixe de Y .

Ainsi, d'après le lemme 3.2, on a l'égalité $\mathbf{K} \equiv d(Y) \pmod{1 - \mathbf{A}}$, et ceci montre que $d(X) = d(Y)$.

Montrons maintenant que si $d = d(Y)$ est un nombre premier impair, le code Y est indécomposable; remarquons d'abord que, dans le cas, Y contient a^d pour toute lettre a de A : en effet, comme X est bipréfixe fini, il contient a^d ; d'autre part, f ne peut être dans a^* puisque $f^2 \in X$; on en déduit que $a^d \in Y$.

Soit maintenant $Y = Y_1 \otimes Y_2$ une décomposition de Y ; comme d est premier, soit Y_1 , soit Y_2 , est synchronisant. Si Y_2 est synchronisant, alors Y_1 est de degré d , et on a donc, d'après 3.6, $a \in Y_2$ pour tout $a \in A$. Maintenant, si Y_1 est synchronisant, alors $a^d \in Y_2$ pour tout $a \in A$; les seuls préfixes de Y susceptibles d'être dans Y_2 sont donc 1 et f , puisque, pour tout autre préfixe p , l'entier n tel que $pa^n \in Y$, n'est pour aucune lettre $a \in A$ un multiple de d . Mais si $f \in Y_2$, on a aussi $D \subset Y_2^*$ puisque $f^3 D \subset Y$; on obtiendrait alors $D \subset Y^* \{1, f\}$, ce qui est impossible car, pour toute lettre $a \in A$, l'entier n tel que $a^n \in D$ est strictement inférieur à d . On obtient donc, dans ce cas, $Y_2 = Y$, et ceci achève de prouver le théorème. ■

Remarques.

1° Pour tout entier d , il existe au moins un code bipréfixe fini de degré d satisfaisant à la condition $Gf \cap fD = \{f^2\}$. Si $d = 2n$ est pair, on peut prendre $X = A^n$ et $f = a^n$ pour un $a \in A$; on obtient alors $Y = B^2$, avec $\mathcal{B} = \mathcal{A}^n - a^n + a^n \mathcal{A}^n$, ce qui montre que la condition que d soit un nombre premier impair n'est pas entièrement superflue. Pour $d = 2n + 1$, on peut prendre $\mathcal{X} = \mathcal{A}^d + (1 - \mathcal{A}) a^{n-1} b a^n (1 - \mathcal{A})$, où a, b sont deux lettres distinctes, et $f = a^n b$; on a alors en effet $Gf \cap fD = (a^n b)^2$.

2° Soit P l'ensemble des préfixes de Y , et posons $L = \{1, f\}$; on a alors les deux égalités

$$1 - \mathcal{Y} = \mathcal{P}(1 - \mathcal{A}) \quad \text{et} \quad 1 - \mathcal{Y} = \mathcal{L}(1 - \mathcal{A}) \mathcal{K}.$$

Celles-ci suffisent à assurer que le résidu de \mathbf{K} modulo $(1 - \mathbf{A})$ est un entier. En effet, dans $\mathbf{Z} \langle A \rangle$, l'égalité $\mathcal{P}(1 - \mathcal{A}) = \mathcal{L}(1 - \mathcal{A}) \mathcal{K}$ implique l'existence d'un polynôme $K' \in \mathbf{Z} \langle A \rangle$ tel que $\mathcal{P} = \mathcal{L} K'$ et $K'(1 - \mathcal{A}) = (1 - \mathcal{A}) \mathcal{K}$ (cf. [4]); et on déduit de la dernière égalité l'existence d'un entier n et d'un polynôme $F \in \mathbf{Z} \langle A \rangle$ tels que

$$\mathcal{K} = n + F(1 - \mathcal{A}), \quad \mathcal{K}' = n + (1 - \mathcal{A})F.$$

5. Une propriété des codes asynchrones indécomposables

Soit X un code préfixe maximal fini de degré d ; on a vu que si X est bipréfixe, alors a^d est dans X pour tout a dans A (corollaire 2.2.3), et

que cette propriété est aussi vraie pour les codes asynchrones indécomposables définis au paragraphe 4. Nous établissons ici le résultat suivant :

THÉORÈME 5.1. — *Si le degré d de X est un nombre premier, différent de 1, et si X est indécomposable, alors a^d est dans X pour tout a de A .*

Démonstration. — Fixons une lettre $a \in A$, et définissons, pour tout mot f de A^* et $i, j \in \mathbf{N}$, les ensembles

$$U_i(f) = \{k \in \mathbf{N}; a^k f a^i \in X^*\}; \quad V_j(f) = \{l \in \mathbf{N}; a^j f a^l \in X^*\}.$$

On a alors, en désignant par n l'entier tel que $a^n \in X$, la propriété suivante où, rappelons-le, on dit que deux parties U et V de \mathbf{Z}/n forment une factorisation si tout élément de \mathbf{Z}/n s'écrit de façon unique comme somme d'un $u \in U$ et d'un $v \in V$.

LEMME 5.2. — *Si $f \xi$ est de rang minimal, les restes mod n de $U_i(f)$ et $V(f) = \bigcup_{j \in \mathbf{N}} V_j(f)$ forment pour tout $i \in V(f)$ une factorisation de \mathbf{Z}/n dans laquelle le deuxième facteur a d éléments.*

Démonstration du lemme. — Soit $r \in \mathbf{N}$ un entier, et $g = a^{r-i} f a^i$; comme i appartient à $V(f)$, l'image $P.f a^i$ de l'application $f a^i \xi$ contient $1 \in P$ et, puisque $f \xi$ est de rang minimal, il en est de même de l'image de $g \xi$. Il existe donc un entier t tel que $g^t \in X^*$; si $t = 1$, cela signifie que $r-i \in U_i(f)$, et on a donc $r \in V(f) + U_i(f)$; sinon, on peut écrire $g^t = g^{t-2} a^{r-i} f a^i f a^i$. On peut, de plus, quitte à ajouter à r un multiple de n , supposer que $r-i$ est plus grand que la longueur de tout mot de X ; on a alors $r = k+1$ et $r-i = j'+j$ avec $g^{t-2} a^{j'}$, $a^{j'} f a^{j'}$, $a^k f a^i \in X^*$; ce qui signifie que $k \in U_i(f)$ et $l \in V(f)$.

Ainsi, tout entier r assez grand est somme d'un élément de $U_i(f)$ et d'un élément de $V(f)$.

Montrons maintenant l'unicité d'une telle factorisation : supposons que, pour $k, k' \in U_i(f)$ et $l, l' \in V(f)$, on ait $k+1 \equiv k'+l' \pmod n$, et considérons le mot $g = a^k f a^l$. On peut supposer que $l > l'$ et, de même que ci-dessus, que l est plus grand que la longueur de tout mot de X ; d'une part, l'image de $g \xi$ contient 1 et $1.a^{l-l'}$ puisque $P.g = P.f a^l$; d'autre part, $(1.a^{k'-k}).g = 1.g$ puisque

$$(1.a^{k'-k}).g = 1.a^{k'} f a^l = 1.a^{l-i} = 1.a^k f a^l = 1.g.$$

Mais comme $g \xi$ est de rang minimal, il définit une permutation sur son image, et cela implique $1.a^{l-l'} = 1$, c'est-à-dire $l \equiv l' \pmod n$ et donc $k \equiv k' \pmod n$.

Enfin, le fait que le nombre des restes mod n de $V(f)$ soit égal à d résulte du fait qu'un entier l appartient à $V(f)$ si, et seulement si, $l \cdot a^{un-1} \in P \cdot a^{un} f a^{un}$ pour un entier u assez grand. ■

Nous en venons maintenant à la preuve du théorème. Notons \mathcal{J}' l'ensemble des parties de A^* qui sont les images des applications $u\xi$ de rang d , pour tout u dans A^* . Tout $J \in \mathcal{J}'$ est formé de d éléments de la forme a^i , pour $0 \leq i \leq n-1$, et on notera \bar{J} le sous-ensemble de \mathbf{Z}/n formé des i tels que $a^i \in J$. On nommera de plus *période* d'une partie U de \mathbf{Z}/n le p. g. c. d. des entiers i tels que $U+i = U$, et on dira que V est périodique si sa période n'est pas nulle. Distinguons alors deux cas :

Cas 1 : Tous les éléments de \mathcal{J}' sont périodiques. — Comme d est, par hypothèse, un nombre premier, les éléments de $\bar{\mathcal{J}'}$ sont les classes latérales du sous-groupe d'ordre d de \mathbf{Z}/n . Définissons une équivalence π sur l'ensemble P des préfixes de X de la manière suivante : deux préfixes p et p' sont équivalents par π si on a $pa^i \in X$ et $p'a^j \in X$ avec $i \equiv j \pmod{n/d}$. L'image de toute application $u\xi$ de rang d est alors composée d'éléments équivalents par π puisque, si $p, p' \in P \cdot u$ et si r est un entier supérieur à la longueur de tout mot de X , on a : $pa^r, p'a^r \in P \cdot ua^r$ qui est inclus dans \mathcal{J}' . Soit alors σ l'équivalence sur P la plus fine telle que toute image d'un élément de rang minimal soit formée d'éléments équivalents; on vérifie que la classe de 1 pour σ est une partie M telle que X^*M soit un sous-monoïde unitaire, et soit donc Y le code préfixe qui l'engendre. Comme X est indécomposable, soit $Y = X$, soit $Y = A$; dans le premier cas, X est synchronisant, puisqu'il en est de même de Y , ce qui est contraire à l'hypothèse; on a donc $Y = A$, ce qui implique que l'équivalence π , qui est plus grossière que σ , soit l'égalité et donc que n soit égal à d , d'où le résultat dans ce cas.

Cas 2 : Il existe un $\bar{J} \in \bar{\mathcal{J}'}$ qui n'est pas périodique. — Nous montrons que ce cas ne peut pas se produire en utilisant le lemme suivant, qui est une application directe du théorème de Sands [13] et du lemme 5.2 :

LEMME 5.3. — *Pour tout mot $f \in X^*$ tel que $f\xi$ soit de rang d l'ensemble $U_0(f)$ contient dp , où p est le p. g. c. d. des différences d'éléments de \bar{J} .*

Démonstration du lemme. — Soit $g \in A^*$ un mot tel que $g\xi$ ait J pour image. On a alors $V(fg) = V(g) = -\bar{J}$ et $U_0(f) = U_i(fg)$, où i est l'entier déterminé par $ga^i \in X^*$; d'après 5.2, on obtient donc une factorisation de \mathbf{Z}/n entre l'ensemble $L = -\bar{J}$ et l'ensemble K des restes modulo n de $U_0(f)$. Mais le théorème de Sands affirme que, dans toute factorisation

dans laquelle l'un des facteurs a un nombre d'éléments qui est une puissance d'un nombre premier, l'un des deux facteurs est périodique. Comme, par hypothèse, L n'est pas périodique, la période r de K n'est pas nulle. Notons \hat{i} le reste modulo r de tout $i \in \mathbf{Z}/n$; alors $\mathbf{Z}/r = \hat{L} + \hat{K}$ est une factorisation de \mathbf{Z}/r avec $\text{Card}(\hat{L}) = d$ et \hat{K} n'est pas périodique; \hat{L} est donc périodique, et tous ses éléments sont donc congrus modulo r/d . Ainsi, toute différence d'éléments de L est un multiple de r/d , d'où le lemme. ■

Soit maintenant $M = \{m \in A^*; \forall x \in X^*, mx X^* \cap X^* \neq \emptyset\}$; on vérifie que M est un sous-monoïde unitaire de A^* , et soit donc Y le code préfixe qui l'engendre. Comme X est inclus dans M , le code X se décompose sur Y , et, puisque X est indécomposable, ou bien $X = Y$, ou bien $Y = A$. On ne peut avoir $Y = A$ puisque cela implique que X soit synchronisant, contrairement à l'hypothèse, et on a donc $Y = X$. Mais, d'après le lemme 5.3, le mot a^{dp} est dans Y ; en effet, pour tout x de X^* , soit x' un élément de X^* tel que $xx' \xi$ soit de rang d . On a alors $a^{dp} \in U_0(xx')$, c'est-à-dire que $a^{dp}xx' \in X^*$. Cela implique que dp soit un multiple de n , ce qui signifie que L est périodique, contrairement à l'hypothèse, et achève donc de prouver le théorème. ■

Remarques.

1° Le théorème de Sands s'applique aux factorisations dans lesquelles le nombre d'éléments de l'un des facteurs est une puissance d'un nombre premier. Il permet encore d'écartier le cas 2 de la preuve du théorème sous l'hypothèse que d est une puissance d'un nombre premier, en utilisant par surcroît le théorème 1 de [14] qui implique que tous les K tels que $K+L = \mathbf{Z}/n$ ont la même période si $\text{Card}(L) = d$. Cependant, nous ne savons pas résoudre le cas 1 sous cette hypothèse plus générale.

2° On observera que le lemme 5.2 fournit une preuve directe du fait que le degré de X divise, si X est fini, chacun des entiers n tels que $a^n \in X$ pour $a \in A$ (corollaire 3.6).

BIBLIOGRAPHIE

- [1] CESARI (Y.). — Sur l'application du théorème de Suschkevitch à l'étude des codes rationnels complets, *Automata, languages and programming*. [1974, Saarbrücken]. Edited by J. Loeckx, p. 342-350. — Berlin, Springer-Verlag, 1974 (*Lectures Notes in Computer Science*, 14).
- [2] CESARI (Y.). — Sur un algorithme donnant les codes bipréfixes finis, *Math. Syst. Theory*, t. 6, 1972, p. 221-225.

- [3] CLIFFORD (A. H.) and PRESTON (G. B.). — *The algebraic theory of semigroups*. Vol. 1. — Providence, American mathematical Society, 1961 (*Mathematical Surveys*, 7).
- [4] COHN (P. M.). — *Free rings and their relations*. — London, Academic Press, 1971 (*London mathematical Society Monographs*, 2).
- [5] EILENBERG (S.). — *Automata, languages and machines*. Vol. A. — New York, Academic Press, 1974 (*Pure and applied Mathematics*. Academic Press, 59-A).
- [6] FELLER (W.). — *An introduction to probability theory and its applications*. Vol. 1, 2nd edition. — New York, J. Wiley and Sons, 1957 (*Wiley Publications in Statistics*).
- [7] GILBERT (E. N.) and MOORE (E. F.). — Variable length binary encodings, *Bell. Syst. Techn. J.*, t. 38, 1959, p. 933-967.
- [8] GOLOMB (S. W.) and GORDON (B.). — Codes with bounded synchronisation delay, *Information and Control*, t. 8, 1965, p. 355-372.
- [9] NIVAT (M.). — Éléments de la théorie générale des codes, *Automata theory*, p. 278-294. — New York, Academic Press, 1966.
- [10] PERRIN (D.). — La transitivité du groupe d'un code bipréfixe fini, *Mathematische Z.*, t. 153, 1977, p. 283-287.
- [11] PERROT (J.-F.). — Groupes de permutations associés aux codes préfixes finis, *Permutations. Actes du colloque sur les permutations* [1972. Paris], p. 201-235. — Paris, Gauthier-Villars; La Haye, Mouton, 1974.
- [12] PERROT (J.-F.). — Computer science and algebra: the theory of variable length codes, *Theoretical Computer Science*, p. 27-44. — Berlin, Springer-Verlag, 1976 (*Lecture Notes in Computer Science*, 48).
- [13] SANDS (A. D.). — On the factorization of finite abelian groups, *Acta Math. Acad. Sc. Hungaricae*, t. 8, 1957, p. 65-86.
- [14] SANDS (A. D.). — The factorisation of abelian groups, *Quart. J. Math. Oxford Series 2*, t. 10, 1959, p. 81-91.
- [15] SCHÜTZENBERGER (M. P.). — Une théorie algébrique du codage, *Séminaire Dubreil-Pisot : algèbre et théorie des nombres*, 9^e année, 1955-1956, n^o 15, 24 p.
- [16] SCHÜTZENBERGER (M. P.). — On a special class of recurrent events, *Annals of math. Stat.*, t. 32, 1961, p. 1201-1213.
- [17] SCHÜTZENBERGER (M. P.). — Sur certains sous-monoïdes libres, *Bull. Soc. math. France*, t. 93, 1965, p. 209-223.
- [18] VIENNOT (G.). — *Algèbres de Lie libres et monoïdes libres*, Thèse, Sc. math. Univ. Paris-VII, 1974.

(Texte reçu le 10 mars 1977.)

Dominique PERRIN
 Département de Mathématiques,
 Université de Rouen,
 76130 Mont-Saint-Aignan.