Groupe d'étude d'algèbre

Antonio Restivo

Sur les sous-monoïdes très purs

Groupe d'étude d'algèbre, tome 1 (1975-1976), exp. n° 18, p. 1-7

<http://www.numdam.org/item?id=GEA_1975-1976__1__A18_0>

Groupe d'étude d'ALGÈBRE
(Marie-Paule MALLIAVIN)
1re année, 1975/76, n° 18, 7 p.

28 mai 1976

SUR LES SOUS-MONOÏDES TRÈS PURS

par Antonio RESTIVO

1. Introduction.

Un des thèmes principaux de la théorie combinatoire du monoïde libre est d'étudier les propriétés des sous-monoïdes du monoïde libre qui sont eux-mêmes libres. Cette étude a été développée sous le nom de théorie des codes. En effet, les bases des sous-monoïdes libres d'un monoïde libre correspondent de façon toute naturelle aux codes à longueur variable introduits par C. SHANNON dans les premiers travaux sur la théorie de l'information. Bien au-delà des problèmes de codage, ces objets interviennent aussi dans des domaines assez variés comme la théorie des langages formels et la théorie des probabilités.

Le but du présent article est de donner quelques détails sur une classe particulière de sous-monoïdes dont la définition est la suivante. Un sous-monoïde M de X^* est très pur si, et seulement si,

$$\forall\, u, v \in X^*, \quad uv \in M \text{ et } vu \in M \Longrightarrow u \in M \text{ et } v \in M .$$

L'intérêt de considérer les sous-monoïdes très purs vient de ce qu'on les rencontre dans les problèmes classiques comme la factorisation des monoïdes libres, et la construction des bases des algèbres de Lie (cf. [9], [11], [12]). D'un autre côté, ces objets interviennent aussi dans les problèmes de synchronisation de la théorie du codage (cf. [5], [4]).

Dans la théorie des sous-monoïdes libres, le cas où le sous-monoïde est finiment engendré, joue un rôle particulier. Sous cette hypothèse, on montre qu'il existe un lien entre les sous-monoïdes très purs et les parties locales d'un monoïde libre (théorème 1). Ce résultat permet de développer des techniques pour étudier les sous-monoïdes très purs finiment engendrés. Nous verrons alors comment on peut construire les bases d'une famille particulière en utilisant les factorisations des polynômes cyclotomiques (théorème 2).

Les mêmes techniques permettent aussi de prouver, dans la dernière partie du travail, un résultat général sur les sous-monoïdes libres maximaux (théorème 3).

Nous n'avons pas fait figurer ici toutes les preuves des propriétés énoncées, pour lesquelles on pourra se reporter à [6], [7].

2. Définitions et propriétés générales.

Soient X un ensemble fini, appelé alphabet, et X^* le monoïde libre engendré par X. Ses éléments seront ici appelés mots et son élément neutre, le mot vide sera noté 1. Si A est une partie de X^*, A^* est le sous-monoïde engendré par A.

Etant donné un sous-monoïde M de X^*, M est lui-même libre s'il satisfait la condition suivante (cf. [8], [10], [1]) :

$$\forall\, u \in X^*\,,\ \forall\, v \in M\,,\ uv \in M \text{ et } vu \in M \Longrightarrow u \in M\,.$$

La plus petite partie A de X^* engendrant M est appelée, pour des raisons historiques, code à longueur variable ou simplement code.

Il n'est pas difficile de vérifier que si A est un code, toute partie de A est aussi un code. Ceci justifie la définiton suivante.

Un code $A \subseteq X^*$ est maximal s'il est élément maximal de l'ensemble des codes sur X ordonné par inclusion, i. e. pour tout $w \in X^* \backslash A$, $A \cup \{w\}$ n'est pas un code. De la même façon, les éléments maximaux de l'ensemble des sous-monoïdes libres de X^* ordonné par inclusion seront appelés sous-monoides libres maximaux. Un sous-monoïde libre maximal est évidemment engendré par un code maximal. La réciproque n'est généralement pas vraie.

Soient maintenant A et B deux codes sur l'alphabet X. Si A est inclus dans B^*, alors l'image de A dans le monoïde libre sur l'ensemble B est encore un code, notons-le C. On dit alors que A est obtenu par composition des codes C et B, on note $A = C \otimes B$. On dira qu'un code A est indécomposable s'il admet seulement des décompositions triviales. Les codes indécomposables sont alors les bases des sous-monoïdes libres maximaux.

Il est évident que tout code est obtenu par composition de codes indécomposables. Si le code est fini on montre que ses décompositions ne contiennent qu'un nombre fini de facteurs. Cela montre l'intérêt tout particulier pour l'étude des sous-monoïdes libres maximaux finiment engendrés.

3. Sous-monoïdes très purs et sous-monoïdes locaux.

Soit M un sous-monoïde de X^*. M est très pur s'il satisfait la condition suivante.

$$\forall\, u\,,\ v \in X^*\,,\ uv \in M \text{ et } vu \in M \Longrightarrow u \in M \text{ et } v \in M\,.$$

D'après la condition de liberté donnée ci-dessus, tout sous-monoïde très pur est aussi libre. Un code A engendrant un sous-monoïde très pur est appelé code très pur.

Rappelons que deux mots $f\,,\ g \in X^*$ sont dits conjugués (proprement conjugués), s'il existe $u\,,\ v \in X^*$ (XX^*), tels que $f = uv$ et $g = vu$. Si $A \subset X^*$ est un code, deux mots $f\,,\ g \in A^*$ sont dits A-conjugués (proprement conjugués), s'il sont conjugués (proprement conjugués) dans le monoïde libre sur l'ensemble A. Il est évident que deux mots A-conjugués sont aussi conjugués. La réciproque n'est généralemenr pas vraie. Il en résulte qu'un code A est très pur si, pour tous $f, g \in A^*$, l'hypothèse que f est proprement conjugué à g entraine que f est proprement A-conjugué à g. Il n'est pas alors difficile de vérifier les propriétés suivantes.

PROPRIÉTÉ 1. - Toute partie d'un code très pur est un code très pur.

PROPRIÉTÉ 2. - La composition de deux codes très purs est un code très pur.

Les propriétés 1 et 2 montrent comment on peut obtenir des sous-monoïdes très purs "plus petits" à partir de ceux "plus grands" avec les opérations de compositions et de passage aux sous-ensembles. Cela pose le problème de définir les sous-monoïdes très purs maximaux.

Nous donnons maintenant quelques définitions.

Une partie L de X^* est dite locale s'il existe un entier positif k et trois sous-ensembles U, V, W de X^k tels que

$$L \cap X^k X^* = (UX^* \cap X^* V) \setminus X^* W X^* .$$

Le plus petit k tel que la condition donnée soit satisfaisante est appelé l'ordre de L, et L sera aussi dit, dans ce cas k-local.

Remarque. - Les parties locales de X^* ont été introduites dans la théorie des langages formels et sont connues, dans la littérature de langue anglaise, comme langages "locally testable". Le contenu intuitif de la définition est le suivant : un mot $f \in X^*$ appartient à L si, et seulement si, son facteur gauche de longueur k est élément de V, son facteur droit de longueur k est élément de V et aucun de ses facteurs de longueur k n'est élément de W. W est aussi appelé ensemble des facteurs interdits de longueurs k.

Un sous-monoïde M de X^* est dit local, s'il est local comme sous-ensemble de X^*. Le théorème suivant représente le point de départ de notre étude.

THÉORÈME 1. - Soit M un sous-monoïde libre et finiment engendré de X^*. M est très pur si, seulement si, M est local.

Les hypothèses sur M d'être libre et finiment engendré sont effectivement nécessaires comme le montrent les exemples suivants.

Exemple 1.

Soit $X = \{x, y\}$, $A = (x^2)^* y$ et $M = A^*$. M est libre mais il n'est pas finiment engendré. Il est facile de vérifier que M est très pur, mais il n'est pas local.

Exemple 2.

Soit $X = \{x, y\}$, $A = \{x^2, x^3, y^2, y^3\}$ et $M = A^*$. M est finiment engendré, mais il n'est pas libre. Evidemment M n'est pas très pur, mais il est 3-local avec : $U = \{x^3, y^3, x^2 y, y^2 x\}$

$V = \{x^3, y^3, xy^2, yx^2\}$

$W = \{xyx, yxy\}$

Le théorème 1 donne une représentation des sous-monoïdes très purs au moyen des trois ensembles finis U, V, W. Nous étudions en particulier les liens entre M

et l'ensemble W des facteurs interdits de longueur k. Pour rendre explicite le lien entre M et W, W sera aussi noté W_M. On a le lemme suivant.

LEMME. - Soit M un sous-monoïde de X^*, k-local, finiment engendré, et soit W_M l'ensemble de facteurs interdits de longueur k. Alors il existe une lettre $x \in X$ telle que $x^k \in W_M$.

Preuve. - Si $x \in X$ et $x^k \in W_M$, alors le mot x^n, avec n assez grand, est facteur d'un mot de M. M étant finiment engendré, la longueur des mots de sa base A est bornée. On peut alors conclure qu'il existe un entier m tel que $x^m \in A$. La seule valeur de m compatible avec la condition M très pur est $m = 1$. Donc pour tout $x \in X$, $x^k \in W_M$ entraine $x \in A$. La thèse du lemme est alors une conséquence triviale du fait que $M \neq X^*$.

Remarque. - Le lemme n'est pas vrai si M n'est pas finiment engendré, comme montre l'exemple suivant.
Soit $X = \{x, y, z\}$, $A = x^* z \cup \{y\} \cup \{z\}$ et $M = A^*$. Il est facile de vérifier que M est 2-local avec $W_M = \{xy\}$.

Comme corollaire du lemme précédent on obtient la proposition 1.

PROPOSITION 1. - La famille des sous-monoïdes très purs, finiment engendrés de X^*, ordonnée par inclusion, ne contient pas d'éléments maximaux.

Preuve. - Soit M très pur et finiment engendré. M est alors aussi k-local pour quelque k. Par le précédent lemme, il existe au moins une lettre $x \in X$ telle que $x^k \in W_M$. Si A est la base de M et y un élément de X différent de x, il n'est pas difficile de vérifier que $A \cup \{x^k y\}$ est la base d'un sous-monoïde M' très pur, qui contient proprement M.

4. La construction d'une classe particulière.

Le but de cette section est de donner des méthodes de construction pour les bases d'une classe particulière de sous-monoïdes très purs. Les preuves ne sont pas données ici, et le lecteur pourra les trouver dans [7]. Dans la suite, nous emploierons simplement le mot "sous-monoïde" pour désigner un sous-monoïde libre finiment engendré.

Les propriétés 1 et 2 des codes très purs données dans la section 3, établissent l'importance des sous-monoïdes, dans quelque manière, maximaux, aux fins de la construction des codes très purs. D'autre part, la proposition 1 affirme qu'il n'existe pas de sous-monoïde très pur maximal. Nous considérons alors une condition de maximalité relative à l'ordre k donné par la propriété d'un sous-monoïde d'être local. On a la définition suivante.

Définition 1. - Soit M un sous-monoïde k-local de X^*. M est k-maximal s'il est un élément maximal de l'ensemble des sous-monoïdes k-locaux de X^* ordonné par inclusion.

La relation d'inclusion entre deux sous-monoïdes M et M' k-locaux induit une relation d'inclusion entre les ensembles correspondants W_M et $W_{M'}$ des facteurs interdits.

$$M \subset M' \Longrightarrow W_{M'} \subset W_M$$

L'implication réciproque n'est pas généralement vérifiée. Ce qui empêche de conclure que, à tout sous-monoïde M k-maximal correspond un ensemble W_M minimal. D'après le lemme 1, les ensembles W_M contiennent nécessairement au moins un élément de la forme x^k pour quelque $x \in X$. Cela suggère la définition suivante.

Définition 2. - Soit $\mathcal{P}$ la classe des sous-monoïdes M k-locaux tels que W_M soit de la forme $W_M = \{x^k\}$ pour quelque $x \in X$.

Remarque. - Tous les sous-monoïdes de $\mathcal{P}$ sont k-maximaux, mais, comme on verra ensuite, $\mathcal{P}$ ne contient pas tous les sous-monoïdes k-maximaux.

On a la proposition suivante.

PROPOSITION 2. - *Soit* $M \in \mathcal{P}$, avec $W_M = \{x^k\}$, *soit* A *la base de* M. *On a l'inclusion* $A \subset x^* Yx^*$ *avec* $Y = X \backslash \{x\}$.

Nous donnons maintenant l'exemple d'un sous-monoide très pur qui n'est inclus dans aucun élément de $\mathcal{P}$. Soit $X = \{x, y\}$ et $M = A^*$ avec $A = \{xy, xxyy, yyx\}$. M est très pur, mais d'après la proposition 2, on vérifie sans peine, que M n'est pas inclus dans un élément de $\mathcal{P}$.

Pour donner la construction des bases des éléments de $\mathcal{P}$, il faut maintenant introduire des définitions.

Soit $P_k(x)$ le polynôme cyclotomique d'ordre k en l'indéterminée x

$$P_k(x) = x^{k-1} + x^{k-2} + \ldots + x + 1 .$$

On considère le problème de trouver deux polynômes $Q(x)$, $R(x)$ à coefficients 0 et 1 tels que

$$P_k(x) = Q(x)R(x) .$$

Le couple $(Q(x), R(x))$ est appelé une factorisation de $P_k(x)$. Le problème de trouver toutes les factorisations d'un polynôme cyclotomique a été résolu par KRASNER et RANULAC [3], lesquels ont donné une méthode pour construire ces factorisations.

Soit maintenant $X = \{x_1, x_2, \ldots, x_n\}$. A chaque partie finie $A \subset X^*$ on peut associer son polynôme caractéristique $\sum_{a \in A} a$ en les indéterminées non commutatives $x_1, x_2, \ldots, x_n$. L'union et le produit finis des parties finies de X^* ont alors une interprétation naturelle dans le calcul des polynômes en variables non commutatives.

Avec cette notation on peut alors énoncer le théorème suivant.

THÉORÈME 2. Soit $M \in \mathcal{P}$ avec $W_M = \{x^k\}$ et soit A la base de M. Alors

$$A = Q(x)(\sum_{x \neq y \in X} y)R(x) .$$

où $(Q(x) , R(x))$ est une factorisation de $p_k(x)$. Toutes les bases des éléments de $\mathcal{P}$ sont obtenues avec cette procédure.

Remarque. - Le théorème 2 et le résultat de Krasner et Ranulac donnent une méthode effective pour construire toutes les bases des éléments de $\mathcal{P}$.

Exemple. - Soit $X = \{x , y , z\}$ et soit $M \in \mathcal{P}$ tel que $W_M = \{x^4\}$. On considère la factorisation :

$$P_4(x) = x^3 + x^2 + x + 1 = (x^2 + 1)(x + 1) .$$

On obtient la base :

$$A = (x^2 + 1)(y + z)(x + 1) = x^2 yx + x^2 y + yx + y + x^2 zx + x^2 z + zx + z .$$

5. Un résultat général sur les sous-monoïdes maximaux.

Dans la théorie des sous-monoïdes d'un monoïde libre, comme nous avons déjà observé, une place particulière est occupée par le cas des sous-monoïdes finiment engendrés. En effet, beaucoup des théorèmes qu'on peut trouver sous cette condition de finitude ne se vérifient plus dans le cas général. D'autre part, nous avons aussi remarqué le rôle important que jouent dans la théorie, les sous-monoïdes libres maximaux. De leurs propriétés on peut déduire beaucoup de propriétés de tous les autres sous-monoïdes libres. On peut alors comprendre l'intérêt d'étudier les sous-monoïdes libres qui sont à la fois maximaux et finiment engendrés.

Nous considérons ici la question suivante. Si M est un sous-monoïde libre finiment engendré, existe-t-il un sous-monoïde libre maximal finiment engendré M' tel que $M \subset M'$?

Les techniques développées dans la section 4 permettent de donner une réponse négative à cette question. Soit $X = \{x , y\}$ et soit t un nombre premier plus grand que 3. Si $(Q(x) , R(x))$ est une factorisation du polynôme cyclotomique $P_{t-1}(x)$, on considère le sous-monoïde libre M engendré par l'ensemble $A = x^t + Q(x)yR(x)$. On peut vérifier [7] qu'il n'existe aucun sous-monoïde libre maximal finiment engendré contenant M. On a alors le théorème suivant.

THÉORÈME 3. - Soit X^* un monoïde libre sur un alphabet de deux lettres au moins. Il existe des sous-monoïdes libres finiment engendrés qui ne sont inclus dans aucun sous-monoïde libre maximal finiment engendré.

Le théorème 3 pose le problème de trouver une condition, sur un sous-monoïde, plus faible que "finiment engendré", telle que tout sous-monoïde libre, satisfaisant cette condition, soit inclus dans un sous-monoïde libre maximal satisfaisant la même condition.

Pour finir la section, nous proposons alors le problème suivant. Si M est un sous-

monoïde libre rationnel [2] , existe-t-il un sous-monoïde libre maximal rationnel qui le contient ?

BIBLIOGRAPHIE

[1] COHN (P. M.). - On semigroups of free semigroups, Proc. Amer. math. Soc., t. 13, 1962, p. 347-351.

[2] EILENBERG (S.). - Automata languages and machines, Vol. A. - New York, Academic Press, 1974 (Pure and applied Mathematics. Academic Press, 59-A).

[3] KRASNER (M.) et RANULAC (B.). - Sur une propriété des polynômes de la division du cercle, C. R. Acad. Sc. Paris, t. 204, 1937, Série A, p. 397-399.

[4] LASSEZ (J. L.). - Circular words and synchronization, Intern. J. of Comp. and Inf. Sc. (to appear).

[5] RESTIVO (A.). - A combinatorial property of codes having finite synchronization delay, Theor. Comp. Sc., t. 1, 1975, p. 95-101.

[6] RESTIVO (A.). - On a question of Naughton and Papert, Inf. and Control, t. 25, 1974, p. 93-101.

[7] RESTIVO (A.). - On codes having no finite completions, Discrete Math. (to appear)

[8] SCHUTZENBERGER (M. P.). - Sur certains sous-demigroupes qui interviennent dans un problème de mathématiques appliquées, Publ. scient. Univ. Alger, Série A, t. 6, 1959, p. 85-90.

[9] SCHÜTZENBERGER (M. P.). - Sur une propriété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de mathématiques appliquées, Séminaire Dubreil-Pisot : Algèbre et théorie des nombres, 12e année, 1958/59, n° 1, 23 p.

[10] SEVRIN (L. N.). - On subsemigroups of free semigroups [en russe], Doklady Akad. Nauk SSSR, t. 133, 1960, p. 537-539 ; [en anglais] Soviet Math., t. 1, 1960, p. 892-894.

[11] VIENNOT (G.). - Factorisations régulières des monoïdes libres et algèbres de Lie libres, C. R. Acad. Sc. Paris, t. 277, 1973, Série A, p. 493-496.

[12] VIENNOT (G.). - Algèbres de Lie libres et monoïdes libres, Thèse Doct. Etat, Université Paris-VII, 1974.

Antonio RESTIVO
Laboratorio di Cibernetica
Arco Felice
NAPOLI (Italie)