

GROUPE D'ÉTUDE D'ALGÈBRE

JEAN MARIE BOÉ

Reconnaisseurs pour les sous-monoïdes libres

Groupe d'étude d'algèbre, tome 1 (1975-1976), exp. n° 14, p. 1-9

http://www.numdam.org/item?id=GEA_1975-1976__1__A14_0

© Groupe d'étude d'algèbre
(Secrétariat mathématique, Paris), 1975-1976, tous droits réservés.

L'accès aux archives de la collection « Groupe d'étude d'algèbre » 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/>

RECONNAISSEURS POUR LES SOUS-MONOÏDES LIBRES

par Jean Marie BOÉ

L'étude des sous-monoïdes d'un monoïde libre qui sont eux-même libres a fait l'objet de nombreux travaux et notamment sous le nom de théorie des codes ([4], [5], [9]). Elle fait intervenir de façon cruciale les monoïdes de matrices à éléments 0 ou 1 (considérés comme des entiers). En effet, pour tout sous-monoïde reconnaissable P d'un monoïde libre X^* , il existe une représentation μ de X^* par des matrices $n \times n$ telle que le coefficient $(1, 1)$ de la matrice μf correspondant au mot f soit égal au nombre de factorisations de f en éléments de l'ensemble générateur minimal de P ([8], [10]). On en déduit qu'une partie reconnaissable P de X^* est un sous-monoïde libre si, et seulement si, elle est le stabilisateur d'un indice dans une représentation μ de X^* par des matrices à éléments 0 ou 1 : $P = \{p \in X^*, (\mu p)_{1,1} = 1\}$. Ces représentations ont notamment été utilisées pour étudier les sous-monoïdes libres maximaux (qui correspondent à la notion de codes indécomposables) [2], [11]. Dans le cas particulier où les matrices sont monomiales, on obtient la notion classique d'automate déterministe qui correspond au cas des sous-monoïdes libres qui sont préfixes [6], [7].

Notre but est ici d'étudier et de classifier les représentations de X^* par matrices $(0, 1)$ reconnaissant un sous-monoïde libre P (c'est-à-dire telles que P soit le stabilisateur d'un indice). Nous établissons ici, (2.8), que parmi ces représentations il en existe une, soit μ , telle que le monoïde μX^* soit le monoïde syntaxique de P [1]. Contrairement au cas des automates déterministes, il n'existe pas de représentation unique de dimension minimale, et le résultat signifie donc qu'il existe cependant des représentations μ telles que le monoïde μX^* soit minimal.

Nous introduisons ici une définition de morphisme de monoïde de matrices $(0, 1)$ correspondant à la notion intuitive de réduction de ces représentations et adaptée à l'étude des décompositions de codes. (Cette définition se confond, dans le cas des matrices monomiales, avec celle de congruence d'automate [7]).

Nous démontrons alors que toutes les représentations μ de X^* reconnaissant un sous-monoïde libre P telle que μX^* soit un monoïde M fixé sont image par un morphisme d'une représentation que nous nommons standard.

Ce résultat donne, en vertu de ce qui précède, une représentation canonique du monoïde syntaxique d'un sous-monoïde libre par des matrices $(0, 1)$ qui, comme nous le verrons, permet d'étudier la décomposition des codes.

1. Codes et sous-monoïdes libres.

1.1. X^* désignant le monoïde libre sur l'alphabet X , une partie $A \subset X^*$ est un

code si elle engendre librement un sous-monoïde libre de X^* que nous noterons A^* . Parmi les codes, les codes préfixes (suffixes) sont les parties qui vérifient

$$AXX^* \cap A = \emptyset, \quad (X^*XA \cap A = \emptyset).$$

Un code bipréfixe est un code préfixe et suffixe.

Exemple. -- $X = \{x, y\}$, $A = \{xx, xy, xxy, xyy, yy\}$.

A est un code qui n'est ni préfixe ni suffixe.

1.2. Définition.

Un sous-monoïde P d'un monoïde M est dit libérable s'il vérifie pour tout $m \in M$, $mP \cap P \neq \emptyset$ et $Pm \cap P \neq \emptyset$ entraînent $m \in P$.

Cette définition trouve sa justification dans l'importante proposition [5].

1.3. PROPOSITION. -- Un sous-monoïde d'un monoïde libre est libre si, et seulement si, il est libérable.

1.4. Etant donnée une partie P d'un monoïde M , on appelle reconnaisseur de P toute image homomorphe N de M pour laquelle P est saturé, c'est-à-dire que le morphisme φ de M sur N vérifie $\varphi^{-1} \varphi(P) = P$.

1.5. Remarquons alors que, si P est un sous-monoïde libérable, il en est de même de $\varphi(P)$.

1.6. P est dit reconnaissable s'il existe un reconheisseur fini.

1.7. Un sous-monoïde P d'un monoïde M est dit complet si P intersecte tous les idéaux bilatères, soit

$$\forall m \in M, \quad P \cap mM \neq \emptyset.$$

1.8. Un code A sur X^* est maximal s'il est maximal en tant que code, c'est-à-dire

$$A \subset B \subset X^*, \quad B \text{ est un code} \implies B = A.$$

Ces notions s'articulent dans l'important résultat [9] suivant, dont on trouvera une démonstration dans [3] ainsi qu'un exposé détaillé des différentes notions présentées dans ce paragraphe.

PROPOSITION. -- Soit A un code. Alors,

- (i) A^* complet reconnaissable $\implies A$ maximal,
- (ii) A maximal $\implies A^*$ complet.

1.9. Enfin le monoïde syntaxique d'une partie $P \subset M$ est le reconheisseur minimal de P (pour les images homomorphes). C'est aussi le quotient de M par la congruence syntaxique

$$m \equiv m' \iff (\forall u, v \in M, \quad umv \in P \iff um'v \in P).$$

2. Représentations des reconheisseurs des sous-monoïdes libres

Notations. -- Etant donné un monoïde M de relations sur un ensemble S , soient

2.3.2. Définition.

Un m. r. n. a. M sur S est dit transitif si $\forall s, t \in S$, il existe $m \in M$ tel que $s \langle m \rangle t$.

Remarquons que si M est un m. r. n. a. sur S transitif et $\equiv$ une congruence de M , alors $M/\equiv$ est un m. r. n. a. transitif sur $S/\equiv$.

Par la suite nous n'utiliserons que des m. r. n. a. transitifs et le mot transitif sera sous-entendu.

2.4. Représentation des monoïdes par relations non-ambigües.

Une représentation d'un monoïde M par relations non-ambigües est un homomorphisme de M sur un m. r. n. a. N sur S . Les représentations du monoïde libre par r. n. a. sont donc des automates non déterministes particuliers (qu'on nomme automate non-ambigu dans [1]).

2.5. Monoïde de relation non-ambigu reconnaisseur.

2.5.1. PROPOSITION. - Soit M un m. r. n. a. sur S . Alors le stabilisateur d'un élément de S est un sous-monoïde libérable de M .

C'est l'étude de la réciproque de cette proposition qui est l'objet de notre étude et nous amène à poser la définition suivante.

2.5.2. Définition.

Etant donné $P \subset M$ un sous-monoïde libérable d'un monoïde M , on dira qu'une représentation de M par un m. r. n. a. N sur S reconnait P si l'image de P est le stabilisateur d'un élément de S (généralement noté 1).

Le résultat principal s'énonce alors :

2.6. THÉOREME. - Soit P un sous-monoïde libérable d'un monoïde M . Alors il existe une représentation de M par un m. r. n. a. M_0 sur S_0 reconnaissant P qui vérifie la propriété universelle suivante.
Pour toute représentation de M par un m. r. n. a. N sur T reconnaissant P , il existe un morphisme f qui fait commuter le diagramme suivant.

$$\begin{array}{ccc}
 M & \xrightarrow{\quad} & M_0 \text{ sur } S_0 \\
 & \searrow & \downarrow f \\
 & & N \text{ sur } T.
 \end{array}$$

On nommera représentation standard de M reconnaissant P l'unique m. r. n. a. reconnaissant P défini par le théorème ci-dessus.

2.6.1. Preuve du théorème.

Avec les mêmes notations qu'en 2.6 posons $S_1 = \{(u, v) \in M \times M ; uv \in P\}$ et soit $\sim$ la fermeture de la relation $\mathcal{R}$ définie sur S_1 par

$$(u, v) \mathcal{R} (u', v') \iff Pu \times vP \cap Pu' \times v'P \neq \emptyset.$$

Posons $S_0 = S_1/\sim$.

2.6.2. LEMME. - Les classes d'équivalence modulo $\sim$ sont des produits cartésiens de parties de M , c'est-à-dire

$$s \in S_0 = S_1 / \sim \quad s = A_s \times B_s \quad \text{avec} \quad A_s, B_s \subset M.$$

2.6.3. LEMME. - Avec les mêmes notations qui précédemment $m_1, m_2 \in M$

$$\left. \begin{array}{l} A_s m_1 \times m_2 B_t \cap A_r \times B_r \neq \emptyset \\ A_s m_1 m_2 B_t \subset P \end{array} \right\} \Rightarrow A_s m_1 \times m_2 B_t \subset A_r \times B_r.$$

Ces deux lemmes permettent de définir le m. r. n. a. M_0 sur S_0 .

2.6.4. PROPOSITION. - Soit φ l'application de M dans le monoïde des relations sur $S_0 = S_1 / \sim$ définie par

$$s, t \in S_0, \quad s \langle \varphi(m) \rangle t \iff A_s m \subset A_t \quad \text{et} \quad m B_t \subset B_s.$$

Alors φ est un homomorphisme de monoïde et $M_0 = \varphi(M)$ est un m. r. n. a. sur S_0 reconnaissant P . Plus précisément, P est le stabilisateur de $1 = A_1 \times B_1 = P \times P$.

2.6.5. Enfin, pour montrer la propriété universelle de la représentation standard, on montre, que toute représentation par un m. r. n. a. N sur T reconnaissant P , induit sur S_1 une partition plus grossière que la partition $\sim$ définie en 2.6.1. On en déduit donc une application f de S_0 sur T et on montre que cette application est un morphisme de m. r. n. a. selon la définition 2.3.

2.6.6. Le théorème 2.6. généralise et précise les assertions de [10] et [8] (voir l'introduction). En effet il ne nécessite par l'hypothèse "reconnaissable" pour le sous-monoïde libre et il affirme d'autre part que le monoïde syntaxique peut être représenté par un m. r. n. a. reconnaissant P . Ce qui donne les deux corollaires suivants.

2.7. COROLLAIRE. - Un sous-monoïde P de X^* est libre (reconnaissable) si, et seulement si, il existe une représentation de X^* par relations non ambiguës (finie) reconnaissant P .

2.8. COROLLAIRE. - Etant donné un sous-monoïde libre $A^* \subset X^*$, il existe une représentation μ de X^* par r.n.a. reconnaissant A^* , telle que μX^* soit isomorphe au monoïde syntaxique de A^* .

3. Quelques représentations particulières - exemples.

3.1. La représentation standard de X^* .

Etant donné A^* un sous-monoïde libre de X^* , appliquons le théorème 2.6. à X^* . On en déduit une représentation de X^* par r. n. a. qui, d'après la propriété universelle, est élément maximal du treillis des m. r. n. a. reconnaisseurs de A^* . Cependant, on peut donner explicitement ce m. r. n. a., ce qui fait l'objet de ce paragraphe.

Soit $A \subset X^*$ le code engendrant A^* , posons

$$\Sigma = \{\sigma = (\sigma_1, \sigma_2) \in X^+ \times X^+, \sigma_1 \sigma_2 \in A\} \cup \{(e, e)\}$$

en convenant que $1 = (e, e)$.

Soit φ l'application de X^* dans le monoïde des relations sur Σ définie par

$$\sigma \langle \varphi(m) \rangle \tau \iff \sigma_1 m \in A^* \tau_1 \text{ et } m \tau_2 \in \sigma_2 A^*.$$

On vérifie que cette dernière condition est équivalente à

$$\sigma_1 m \tau_2 \in \sigma_1 \sigma_2 A^* \cap A^* \tau_1 \tau_2$$

(à composer à 1.2.). Avec ces notations, on a la proposition suivante.

3.1.1. PROPOSITION.

- (i) $M = \varphi(X^*)$ est un m. r. n. a. sur Σ , reconnaisseur de A^* .
- (ii) M est la représentation standard de X^* reconnaissant A^* .
- (iii) Toute représentation de X^* par r. n. a. reconnaissant A^* est image homomorphe du m. r. n. a. M sur Σ .

Remarque. - Cette proposition est un corollaire du théorème 2.6. Cependant, on peut démontrer directement (i). En effet, de $(\sigma_1, \sigma_2) \langle ff' \rangle (\tau_1, \tau_2)$ pour $f, f' \in X^*$, on déduit l'existence d'un unique $(\rho_1, \rho_2) \in \Sigma$ tel que

$$(\sigma_1, \sigma_2) \langle f \rangle (\rho_1, \rho_2) \langle f' \rangle (\tau_1, \tau_2).$$

Il suffit d'observer que $\tau_1 ff' \tau_2 \in A^*$ entraîne l'existence d'un unique mot $a \in A^* \cup \{e\}$, $a = \rho_1 \rho_2$, $(\rho_1, \rho_2) \in \Sigma$ et $\sigma_1 f \in A^* \rho_1$, $f' \tau_2 \in \rho_2 A^*$.

3.1.2. Exemple. - $X = \{x, y\}$, $A = \{xx, xy, xxy, xyy, yy\}$
 posons $1 = (e, e)$, $2 = (x, y)$, $3 = (x, y)$, $4 = (x, xy)$,
 $5 = (xx, y)$, $6 = (x, yy)$, $7 = (xy, y)$, $8 = (y, y)$.

$$\varphi(x) = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & . & . & . & . & . & 0 \\ 0 & . & . & . & . & . & . & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & . & . & . & . & . & . & 0 \\ 0 & . & . & . & . & . & . & 0 \\ 0 & . & . & . & . & . & . & 0 \\ 0 & . & . & . & . & . & . & 0 \end{bmatrix} \quad \varphi(y) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & . & . & . & . & . & . & 0 \\ 1 & 0 & . & . & . & . & . & 0 \\ 0 & . & . & . & . & . & . & 0 \\ 1 & 0 & . & . & . & . & . & 0 \\ 0 & . & . & . & 0 & 1 & 0 & 0 \\ 1 & 0 & . & . & . & . & . & 0 \\ 1 & 0 & . & . & . & . & . & 0 \end{bmatrix}$$

3.2. Représentation du monoïde syntaxique.

Soit $A^* \subset X^*$ un sous-monoïde libre de X^* , et soit M son monoïde syntaxique. D'après le théorème 2.6. et la syntaxicité de M , toutes les représentations de M par r. n. a. reconnaissant A^* sont fidèles. Cependant, contrairement à ce qui se passe lorsque l'on a des monoïdes d'applications (cas des monoïdes de transition des automates déterministes), il n'y a pas de représentation minimale unique (minimal pour card S), comme le montre les exemples suivants.

3.2.1. Exemple. - Considérons le sous-monoïde libre décrit en 3.1.2. La représentation standard μ_0 du monoïde syntaxique est la suivante :

$$\mu_0 x = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \mu_0 y = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

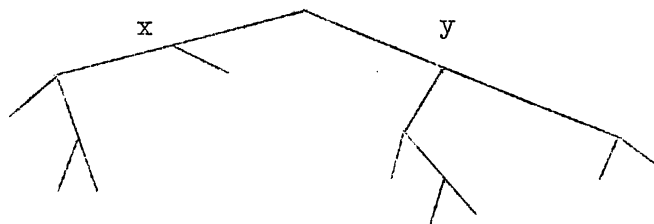
$\mu_0 X^*$ admet deux quotients (de m. r. n. a.) reconnaissant eux-aussi A^* et dont les monoïdes sont isomorphes au monoïdes syntaxiques.

$$\mu_1 x = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \mu_1 y = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{correspondant à l'équivalence } 1/2, 4/3.$$

$$\mu_2 x = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \mu_2 y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{correspondant à l'équivalence } 1/2/3, 4.$$

On pourra aussi remarquer que le m. r. n. a. $\mu_0 X^*$ est le quotient du m. r. n. a. ϕX^* défini en 3.1.2. par la congruence $1/246/578/3$.

3.2.2. Exemple. - Considérons le code bipréfixe de longueur moyenne 3, non uniforme, sur l'alphabet $X = \{x, y\}$ décrit par l'arbre suivant



La représentation standard μ_0 du monoïde syntaxique donne un m. r. n. a.

$\mu_0 X^* = M$ sur S_0 où $\text{card } S_0 = 9$.

Posons $S_0 = \{1, 2, \dots, 9\}$.

M est le sous-monoïde du monoïde des relations sur S_0 engendré par

$$\mu_0 x = \{4, 8\} \times \{1\} \cup \{1\} \times \{2, 3\} \cup \{2, 6\} \times \{4, 5\}$$

$$\mu_0 y = \{3, 9\} \times \{1\} \cup \{1\} \times \{6, 7\} \cup \{5, 7\} \times \{8, 9\}.$$

M admet deux congruences :

$\equiv_R$ définie par l'équivalence sur S_0 $1/23/45/67/89$.

$\equiv_L$ définie par l'équivalence sur S_0 $1/39/57/48/26$.

$M/\equiv_R$ est le monoïde de transition de l'automate minimal de gauche à droite, tandis que $M/\equiv_L$ correspondant à l'automate minimal de droite à gauche.

4. Applications à la décomposition des codes.

4.1. Définition.

Un code A sur X se décompose sur le code B si $A^* \subset B^* \subset X^*$. On vérifie, alors, que A est un code sur l'alphabet B . L'étude des décompositions des codes trouve un appui dans la proposition suivante.

4.2. PROPOSITION. - Soient $P \subset Q \subset M$ deux sous-monoïdes libérables du monoïde M avec P complet dans Q , et Q complet dans M . Désignons par N le m. r. n. a.

sur S , représentation standard de M reconnaissant P . Alors il existe une congruence $\equiv$ du m. r. n. a. N telle que :

(i) La représentation standard de M reconnaissant Q est le quotient $N/\equiv$, m. r. n. a. sur $S/\equiv$.

(ii) La représentation standard de Q reconnaissant P est de m. r. n. a. restriction de N à la classe de $1 \pmod{\equiv}$.

Cette proposition s'appliquant à la décomposition des codes donne le corollaire suivant.

4.3. COROLLAIRE. - A toute décomposition d'un code $A^* \subset X^*$ complet correspond une congruence du m. r. n. a. image de la représentation standard de X^* reconnaissant A^* .

On peut aussi démontrer la proposition suivante.

4.4. PROPOSITION. - A toute congruence d'un m. r. n. a. reconnaissant un sous-monoïde libre correspond une décomposition du code qui engendre ce dernier.

4.5. Exemple. - Avec les notations de 3.2.1. on constate que $\mu_0 X^*$ admet deux congruences correspondant à des décompositions propres :

12/34 qui donne comme quotient $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ce qui correspond à la décomposition :

$$A \subset \{x, xy, yy\}^*.$$

13/24 qui donne comme quotient $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ correspondant à la décomposition :

$$A \subset \{xx, xy, y\}^*.$$

Il est à noter que μ_1 et μ_2 ne supportent chacune qu'une seule congruence donnant une décomposition. Seule la représentation standard μ_0 supporte les deux congruences correspondant aux deux décompositions possibles du code A .

4.6. Problème. - On est amené à se poser le problème suivant, résolu par D. PERRIN et J. F. PERROT dans le cas préfixe (voir [6]).

A chaque décomposition d'un code fini complet correspond-il une congruence de la représentation standard du monoïde syntaxique. (congruence non triviale, si la décomposition ne l'est pas).

La proposition 4.3. assure cette correspondance lorsqu'on considère la représentation standard de X^* (et non du monoïde syntaxique). Cependant si A est un code reconnaissable non fini, cette représentation n'est pas finie. On a toutefois la proposition suivante.

4.7. PROPOSITION. - Soient A et B deux codes reconnaissables sur X . Supposons que A se décompose sur B .

Alors il existe une représentation de X^* par m. r. n. a. fini reconnaissant A^* qui admette un quotient reconnaissant B^* .

BIBLIOGRAPHIE

- [1] BOÉ (J. M.), BOYAT (J.), CÉSARI (Y.) et LECHENY (A.). - Automates et monoïdes syntactiques des sous-monoïdes libres (à paraître).
- [2] CÉSARI (Y.). - Sur l'application du théorème de Susshkewitsch à l'étude des codes rationnels complets, "Automata, languages and programming", 2nd Colloquium [1974. Saarbrücken], Edited by J. Loeckx. - Berlin, Springer-Verlag, 1974 (Lecture Notes in computer Science, 14).
- [3] EILENBERG (S.). - Automata, languages and machines, Vol. A. - New York, Academic Press, 1974 (Pure and applied Mathematics, Academic Press, 59-A).
- [4] GILBERT (E. N.) et MOORE (E. F.). - Variable-length binary encodings, Bell Syst. techn. J., 38, 1959, p. 933-967.
- [5] NIVAT (M.). - Eléments de la théorie générale des codes, "Automata theory", p. 278-294. - New York, Academic Press, 1966.
- [6] PERRIN (D.). - Le langage engendré par un code préfixe et son monoïde syntaxique, Thèse 3e cycle, Paris, 1970
- [7] PERROT (J. f.). - Une série algébrique des automates finis monogènes, "Informatica teorica [1973. Roma]", p. 201-244. - London, Academic Press, 1975 (Symposia Mathematica, 15).
- [8] RICHARD (J.). - Représentations matricielles des séries rationnelles en variables non commutatives, C. R. Acad. Sc. Paris, t. 270, 1970, Série A, p. 224-227.
- [9] SCHÜTZENBERGER (M. P.). - Une théorie algébrique du codage, Séminaire Dubreil-Pisot : Algèbre et théorie des nombres, 9e année, 1955/56, n° 15, 24 p.
- [10] SCHÜTZENBERGER (M. P.). - On the definition of a family of automata, Inf. and Control, t. 4, 1961, p. 245-270.
- [11] SCHÜTZENBERGER (M. P.). - Sur certains sous-monoïdes libres, Bull. Soc. math. France, t. 93, 1965, p. 209-223.

Jean Marie BOÉ
 Mathématiques
 Université du Languedoc
 Place Eugène Bataillon
 34060 MONTPELLIER CEDEX
