Informatique théorique/*Computer Science*

Factorisations dans le monoïde partiellement commutatif libre

Gérard DUCHAMP et Daniel KROB

Résumé — On montre que tout monoïde partiellement commutatif libre se factorise en monoïdes libres et admet donc une factorisation complète. On donne ensuite la décomposition associée de l'algèbre de Lie partiellement commutative libre en somme directe d'algèbres de Lie libres.

Factorisations in the free partially commutative monoid

Abstract — *We show that every free partially commutative monoid can be factorized in free monoids and consequently has a complete factorization. Then, we give the associated decomposition of the free partially commutative Lie algebra in a direct sum of free Lie algebras.*

0. NOTATIONS. — Dans la suite, on notera par A^* le *monoïde libre* construit sur l'alphabet A (*cf.* [1], [7]). On appellera aussi *commutation partielle* sur A la donnée d'une partie symétrique ϑ de $A\times A-\Delta_A$ (où $\Delta_A=\{(a, a),\ a\in A\}$). On associe alors à ϑ la congruence sur A^*, notée $\equiv_\vartheta$, la plus fine (*cf.* [1], [5]) telle que :

$$ab\equiv_\vartheta ba \quad \text{pour tout } (a, b)\in\vartheta.$$

Nous désignerons par $M(A; \vartheta)$ le monoïde quotient $A^*/\equiv_\vartheta$ qui sera appelé *monoïde partiellement commutatif libre* (cf. [3], [8]).

Notons aussi que toute commutation partielle ($ab=ba$) peut s'interpréter comme une relation de Lie ($[a, b]=0$). Cela nous permet donc de construire, pour tout anneau commutatif K, la K-*algèbre de Lie partiellement commutative libre*, qui sera notée $L(A, \vartheta)$, définie comme le quotient de la K-algèbre de Lie libre $L(A)$ par l'idéal de Lie de $L(A)$ engendré par les alternants $[a, b]$ pour tout $(a, b)\in\vartheta$.

Terminons en donnant la définition suivante dont nous aurons besoin pour des raisons techniques : un couple de parties symétriques λ, ϑ de $A\times A-\Delta_A$ étant donné, nous appellerons congruence *alphabétique* associée à (λ, ϑ) la congruence sur A^*, notée $\equiv_{\lambda,\vartheta}$, la plus fine telle que :

$$a\equiv_{\lambda,\vartheta} b \quad \text{pour } (a, b)\in\lambda \qquad \text{et} \qquad ab\equiv_{\lambda,\vartheta} ba \quad \text{pour } (a, b)\in\vartheta.$$

Le lecteur vérifiera aisément que le monoïde quotient $A^*/\equiv_{\lambda,\vartheta}$ est isomorphe à un monoïde partiellement commutatif libre sur un alphabet plus petit. Ainsi, la définition précédente n'étend pas le cadre partiellement commutatif.

1. FACTORISATIONS D'UN MONOÏDE. — La notion de factorisation a été introduite dans le cadre du monoïde libre en [9]. On peut également la définir pour un monoïde quelconque. En effet, on dira qu'une famille $(M_i)_{i\in I}$ de sous-monoïdes d'un monoïde M, indexée par un ensemble totalement ordonné I, est une *factorisation* de M si et seulement si tout élément m de M peut s'écrire d'une manière unique sous la forme suivante :

$$m=m_{i_1}\ldots m_{i_n} \qquad \text{avec} \quad i_1<\ldots<i_n \text{ et } m_{i_k}\in M_{i_k} \text{ pour tout } k$$

On dira de plus que la factorisation $(M_i)_{i\in I}$ est *complète* si et seulement si $M_i\simeq(\mathbb{N}, +)$ pour tout $i\in I$. Il est facile de voir que cela signifie exactement qu'il existe une famille $(l_i)_{i\in I}$ d'éléments de M telle que tout élément m de M s'écrive de manière unique sous la

Note présentée par Marcel-Paul SCHÜTZENBERGER.

0764-4442/91/03120189 $ 2.00 © Académie des Sciences

forme :

$$m = l_{i_1}^{\alpha_{i_1}} \ldots l_{i_n}^{\alpha_{i_n}} \quad \text{avec} \quad i_1 < \ldots < i_n \text{ et } \alpha_{i_k} \in \mathbb{N} \text{ pour tout } k.$$

Rappelons enfin que tout monoïde libre admet une factorisation complète (*cf.* [7], [10]). Par exemple, les mots de Lyndon ordonnés dans l'ordre lexicographique inverse forment une factorisation complète particulièrement importante (*cf.* [7], [10]).

2. Élimination dans le monoïde partiellement commutatif. — Soit A un alphabet muni d'une commutation partielle ϑ. Pour toute partie P de $M(A; \vartheta)$, on notera $\langle P \rangle$ le sous-monoïde de $M(A; \vartheta)$ engendré par P. On pourra remarquer que si $B \subset A$ et si ϑ_B désigne la commutation partielle $\vartheta_B = \vartheta \cap B \times B$, on a alors $\langle B \rangle \simeq M(B, \vartheta_B)$. Rappelons aussi qu'un sous-alphabet B de A est dit *non commutatif* (pour ϑ) si et seulement si pour tout a, $b \in B$, $(a, b) \notin \vartheta$. Enfin, pour tout w dans $M(A, \vartheta)$, on appellera *alphabet terminal* de w l'ensemble :

$$AT(w) = \{ a \in A,\ w \in M(A, \vartheta).a \}.$$

On peut alors donner le théorème suivant (*cf.* [4] pour plus de détails) :

Théorème 1 [procédé d'élimination dans $M(A, \vartheta)$]. — *Soit* A *un alphabet, soit* ϑ *une commutation partielle sur* A *et soit* $Z \subset A$ *un sous-alphabet non commutatif de* A. *Posons alors* $B = A - Z$ *et introduisons :*

$$C_Z = \bigcup_{z \in Z} \{ wz,\ w \in \langle B \rangle \ et\ AT(wz) = \{ z \} \}.$$

On a alors les assertions suivantes :

(1) $\langle C_Z \rangle$ *est un monoïde libre de base* C_Z *: on le notera donc* C_Z^*.

(2) $(C_Z^*, \langle B \rangle)$ *est une factorisation de* $M(A, \vartheta)$.

Preuve. — Pour montrer ce résultat, on prouve en fait que tout mot w de $M(A, \vartheta)$ peut se décomposer d'une manière unique sous la forme :

$$w = c_1 \ldots c_n m \quad \text{avec} \quad c_i \in C_Z \text{ et } m \in \langle B \rangle$$

ce qui établira en même temps les deux points du théorème. L'existence de la décomposition se montre facilement par récurrence sur la longueur de w. Pour prouver l'unicité de la décomposition, on raisonne aussi par récurrence sur la longueur de w en étudiant l'alphabet terminal de w et en se servant de la simplifiabilité de $M(A, \vartheta)$ pour se ramener à un plus petit mot. ■

Exemples. — Dans le cas libre, toute partie est non commutative et on retrouve donc la bisection de Lazard : $A^* = (B^*(B - A))^* B^*$. Au contraire, dans le cas totalement commutatif, les parties non commutatives sont les singletons : le théorème 1 donne alors la décomposition classique $A^{\oplus} = \{ a \}^{\oplus} (A - \{ a \})^{\oplus}$.

Comme $\langle B \rangle \simeq M(B, \vartheta_B)$, le théorème 1 montre immédiatement par récurrence sur $|A|$ que $M(A, \vartheta)$ peut se factoriser en un nombre fini de monoïdes libres, quand A est fini. Comme tous ces monoïdes libres ont une factorisation complète, on en déduit donc qu'il existe aussi une factorisation complète pour $M(A, \vartheta)$.

3. Élimination dans l'algèbre de Lie partiellement commutative libre. — G. Viennot (*cf.* [10]) a mis en évidence les liens profonds qui unissent les factorisations complètes du monoïde libre et les constructions de bases dans l'algèbre de Lie libre associée. Dans le cadre partiellement commutatif, on peut aussi établir un tel lien. Celui-ci est assuré par le théorème suivant, que nous ne prouverons pas ici (*cf.* [4] pour plus de détails), qui

généralise le théorème d'élimination de Lazard pour l'algèbre de Lie libre (*cf.* [2], [6]) :

THÉORÈME 2 (Procédé d'élimination dans $L(A, \vartheta)$). — *Soit* K *un anneau commutatif, soit* A *un alphabet, soit* ϑ *une commutation partielle sur* A *et soit* $Z \subset A$ *un sous-alphabet non commutatif de* A. *Posons alors* $B = A - Z$, *notons* [B] *la sous-algèbre de Lie de* $L(A, \vartheta)$ *engendrée par* B *et introduisons la famille* T_Z *de* $L(A, \vartheta)$ *définie par :*

$$T_Z = \bigcup_{z \in Z} \{ \mathrm{ad}\, w . z,\ w \in \langle B \rangle \text{ et } \mathrm{AT}(wz) = \{z\} \}.$$

On a alors les assertions suivantes :

(1) *La sous-algèbre de Lie de* $L(A, \vartheta)$ *engendrée par* T_Z *est une algèbre de Lie libre de famille basique* T_Z : *on la désignera donc par* $L(T_Z)$.

(2) *L'algèbre de Lie* $L(A, \vartheta)$ *admet la décomposition en somme directe :*

$$L(A, \vartheta) = L(T_Z) \oplus [B].$$

Comme $[B] \simeq L(B, \vartheta_B)$, le théorème précédent nous permet, par une récurrence immédiate sur $|A|$, de décomposer $L(A, \vartheta)$ en une somme directe d'algèbres de Lie libres quand A est fini. Comme une algèbre de Lie libre est un K-module libre (*cf.* [2], [10]), cette décomposition montre donc que le K-module $L(A, \vartheta)$ est libre. De plus, elle permet d'obtenir sans difficulté des bases pour $L(A, \vartheta)$ en se servant des procédés classiques de construction de bases pour les algèbres de Lie libres (*cf.* [10]). Compte tenu des résultats de G. Viennot (*cf.* [10]), le théorème 2 assure donc un lien naturel entre les factorisations complètes de $M(A, \vartheta)$ provenant du procédé décrit au paragraphe 2 et les bases de $L(A, \vartheta)$ obtenues grâce à la méthode que nous venons d'exposer.

Exemple. — Considérons l'alphabet $A = \{a, b, c\}$ muni de la commutation partielle $\vartheta = \{(a, b), (b, a)\}$. Posons $B = \{a, b\}$. Comme $Z = A - B = \{c\}$ est non commutatif, on peut appliquer le théorème 2. Le lecteur vérifiera alors aisément que l'on obtient la décomposition : $L(A, \vartheta) = L(\{\mathrm{ad}\, w . c,\ w \in \{a, b\}^*\}) \oplus K . a \oplus K . b$.

4. UN THÉORÈME DE LIMITATION. — Le fait qu'une congruence partiellement commutative puisse s'interpréter aussi comme une relation de Lie, nous a permis d'associer à cette congruence une algèbre de Lie dont les propriétés sont intimement liées aux propriétés combinatoires du monoïde correspondant. Il est donc naturel de se demander si ce type de phénomène peut se produire pour d'autres congruence sur A^*.

Pour cela, donnons d'abord les définitions suivantes : un anneau commutatif K étant fixé, on dira qu'un idéal bilatère I de l'algèbre associative libre $K\langle A \rangle$ est *monoïdal* si, et seulement si, il existe une congruence $\equiv$ sur A^* telle que I soit engendré comme K-module par les différences $u - v$ pour $u \equiv v$ dans A^*; de même, on dira que I est de *type de Lie*, si, et seulement si, il existe un idéal de Lie J de l'algèbre de Lie libre $L_K(A)$ tel que $I = K\langle A \rangle . J . K\langle A \rangle$.

On peut alors montrer le résultat suivant, que nous ne prouverons pas ici, qui montre (compte tenu de remarques précédentes) que le cadre partiellement commutatif est le cadre maximal dans lequel on peut développer parallèlement une théorie de Lie et une théorie monoïdale (*cf.* [4] pour plus de détails) :

THÉORÈME 3. — *Soit* K *un anneau de* caractéristique 0, *soit* A *un alphabet, soit* $\equiv$ *une congruence sur* A^* *et soit* I *l'idéal bilatère monoidal de* $K\langle A \rangle$ *associé. Alors les deux assertions suivantes sont équivalentes :*

(i) I *est un idéal monoïdal et de type de Lie.*

(ii) $\equiv$ *est une congruence alphabétique.*

Remarques. — (1) Pour montrer ce résultat, nous établissons en fait qu'on ne peut munir $K\langle A; \equiv \rangle = K\langle A \rangle / I$ d'une structure de bigèbre telle que les éléments de A soient primitifs (*cf.* [1], [2]) que si $\equiv$ est une congruence alphabétique. Ainsi, ces congruences sont donc aussi les seules pour lesquelles $K\langle A; \equiv \rangle$ est l'algèbre enveloppante de sa sous-algèbre de Lie engendrée par A.

(2) Le théorème ci-dessus devient faux en caractéristique $p>0$: le lecteur vérifiera en effet aisément que, pour $K=\mathbb{Z}/p\mathbb{Z}$, la congruence $\equiv$ sur $A=\{a, b\}$ la plus fine telle $a^p b \equiv ba^p$ fournit un contre-exemple [car celle-ci peut aussi s'écrire $ad^p a.(b) \equiv 0$].

Note remise le 11 mai 1990, acceptée le 29 octobre 1990.

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] N. BOURBAKI, *Algèbre*, chap. 1 à 3, C.C.L.S., 1970.
[2] N. BOURBAKI, *Groupes et Algèbres de Lie*, chap. 2 et 3, C.C.L.S., 1972.
[3] C. CHOFFRUT, Rapport L.I.T.P., n° 86-20, 1986.
[4] G. DUCHAMP et D. KROB, *Free partially commutative structures*, Rapport L.I.T.P., n° 90-65, 1990.
[5] S. EILENBERG, *Automata, Languages and Machines*, A, Academic Press, 1974.
[6] M. LAZARD, *Groupes, anneaux de Lie et problème de Burnside*, Inst. Mat. dell. Universita Roma, 1960.
[7] M. LOTHAIRE, *Combinatorics on words*, Addison Wesley, 1983.
[8] D. PERRIN, *Lecture Notes in Comp. Sc.*, 372, 1989, p. 637-651.
[9] M.-P. SCHÜTZENBERGER, *Proc. A.M.S.*, 16, n° 1, 1965, p. 21-24.
[10] G. VIENNOT, *Lecture Notes in Math.*, 691, Springer Verlag, 1978.

Laboratoire d'Informatique de Rouen L.I.T.P. et C.N.R.S.,
Université de Rouen, place E.-Blondel, 76134 *Mont-Saint-Aignan Cedex.*