Daniel Krob

Codes limites et factorisations finies du monoïde libre

Informatique théorique et applications, tome 21, nº 4 (1987), p. 437-467

<http://www.numdam.org/item?id=ITA_1987__21_4_437_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 21, n° 4, 1987, p. 437 à 467)

CODES LIMITES ET FACTORISATIONS FINIES DU MONOÏDE LIBRE *

par Daniel KROB (1)

Communiqué par J.-E. PIN

Résumé. – *Nous introduisons la notion de factorisation monoïdale du monoïde libre. Dans ce cadre, nous étudions la liberté et la limitation des facteurs d'une factorisation monoïdale finie. Puis nous montrons un théorème de recollement pour les quadrisections.*

Abstract. – *We introduce the concept of monoidal factorizations of free monoids. Then we study the freeness and the limitation of the factors of a free monoidal factorization. Finally we prove a pasting theorem for the quadrisections.*

I. INTRODUCTION

L'étude des factorisations d'un monoïde libre A^*, introduites par Schützenberger [4] revenait à poser le problème très naturel de la construction de bases pour A^*. En effet une factorisation de A^* est la donnée d'une famille $(X_i)_{i \in I}$ de codes, indexée par un ensemble I totalement ordonné telle que :

$$\underline{A}^* = \prod_{i \in I} \underline{X}_i^*$$

Schützenberger chercha tout particulièrement des conditions nécessaires et suffisantes pour qu'une famille de codes soit une factorisation de A^* [5] : il montra en particulier que les codes intervenant dans une factorisation étaient circulaires. Il amorça également l'étude des factorisations finies en s'intéressant aux bisections.

(*) Reçu juin 1986, révisé septembre 1986.
(1) Université de Rouen, Faculté des Sciences, Laboratoire d'Informatique, place Emile-Blondel, B.P. n° 67, 76130 Mont-Saint-Aignan.

0296-1598 87/04 437 31/$ 5.10/© Gauthier-Villars

Le lien entre factorisations et algèbres de Lie libres fut ensuite étudié par G. Viennot qui s'intéressa aussi aux factorisations finies et tout particulièrement aux bisections et aux trisections [6]. Il montra que toute trisection pouvait s'obtenir par recollement de bisections et conjectura [6] que de façon générale, toute factorisation finie pouvait se construire par recollement de bisections.

Des travaux de Schützenberger et de Viennot, on pouvait déduire que si (X_1, X_2) était une bisection de A^*, alors X_1 (resp. X_2) était (1, 0) [resp. (0, 1)] limité et que si (X_1, X_2, X_3) était une trisection de A^*, alors X_i était $(3-i, i-1)$-limité. Berstel et Perrin conjecturèrent alors [2] que, pour toute factorisation finie $(X_i)_{i=1,n}$ à n facteurs, les codes X_i étaient $(n-i, i-1)$ limités.

C'est ce dernier problème qui sera le centre de notre article : nous avons réussi en effet à montrer que la conjecture était encore vraie pour $n=4$ et à obtenir des résultats partiels pour n quelconque. Pour arriver à ces résultats, nous nous sommes placés dans un cadre plus général que celui des factorisations au sens usuel et avons introduit la notion de factorisation monoïdale.

Il se trouve également que la conjecture de Viennot sur les recollements de bisections est liée à des problémes de liberté de factorisation monoïdale. Nous avons aussi mis en évidence ces liens et nous montrons en particulier un théorème de recollement pour les quadrisections.

Nous avons donc divisé ce travail en deux parties :

– la premier partie est consacré à l'étude des factorisations monoïdales finies. Nous montrons que les facteurs externes et les premiers facteurs internes d'une telle factorisation sont libres et limités. Nous donnons également une caractérisation des monoïdes qui sont les facteurs externes d'une factorisation monoïdale finie.

– la deuxième et dernière partie est consacrée à la démonstration d'un théorème de recollement pour les quadrisections. Nous signalons aussi que toute généralisation de la méthode employée est liée à la liberté des facteurs d'une factorisation monoïdale finie.

II. NOTATIONS ET DÉFINITIONS

Nous allons donner ici toutes les notations et définitions dont nous aurons besoin par la suite.

A désignera toujours un alphabet et A^* sera le monoïde libre engendré par A.

Pour tout $w \in A^*$, $|w|$ désignera la longueur de w.

Soit X une partie de A^*, nous noterons $\underline{X}$ la série caractéristique de X. Toutes les séries, que nous considérons par la suite, seront toujours prises dans $\mathbb{N}\langle A^* \rangle$ ou si cela s'avère nécessaire dans $\mathcal{N}\langle A^* \rangle$ où $\mathcal{N}$ désigne le semi anneau : $\mathcal{N} = \mathbb{N} \cup \{\infty\}$.

Rappelons que si X et Y sont deux parties de A^*, on ne peut écrire :

$$\underline{XY} = \underline{X}\,\underline{Y}$$

que si le produit XY est non ambigü (i. e. si tout élément de XY ne peut s'écrire que d'une façon et d'une seule comme produit d'un élément de X et d'un élément de Y).

Donnons maintenant quelques définitions sur les codes :

Tout d'abord rappelons qu'une partie X de A^* est dite *préfixielle* si et seulement si elle contient les préfixes de tous ses mots, c'est-à-dire si :

$$\forall u, v \in A^*, \qquad uv \in X \;\Rightarrow\; u \in X$$

De même une partie X et A^* est dite *suffixielle* si et seulement si elle contient les suffixes de tous ses mots, i. e. :

$$\forall u, v \in A^*, \qquad uv \in X \;\Rightarrow\; v \in X.$$

La définition suivante est fondamentale pour la suite :

DÉFINITION : Soient p, q deux entiers. Un sous-monoïde M de A^* vérifie *la condition* $C(p, q)$ si et seulement pour toute suite $u_0, \ldots u_{p+q}$ de mots de A^* telle que :

$$\forall i \in \{1; \ldots; p+q\}, \quad u_{i-1} u_i \in M$$

l'on ait :

$$u_p \in M$$

Remarque : Si M vérifie la condition $C(p, q)$, alors M est libre et engendré par un code circulaire [1].

On dit alors qu'un code X sur A^* est *(p, q)-limité* si X^* vérifie la condition $C(p, q)$. On dira qu'un code est *limité* s'il est (p, q)-limité pour au moins un couple (p, q) de $\mathbb{N}^2$. Notons que le seul code $(0, 0)$-limité est A et qu'un code $(p, 0)$ [resp. $(0,q)$]-limité est toujours préfixe (resp. suffixe).

Terminons en rappelant la notion de factorisation. Soit $(X_i)_{i \in I}$ une famille de codes indexée par un ensemble I totalement ordonné. On dit que $(X_i)_{i \in I}$

est une *factorisation* de A^* si et seulement si tout mot w non vide admet une décomposition et une seule de la forme suivante :

$$w = x_{\alpha_1} \dots x_{\alpha_l} \qquad \text{avec} \quad \alpha_1 < \alpha_2 < \dots < \alpha_l$$

et $x_{\alpha_i} \in X_{\alpha_i}^* \setminus \{1\}$ pour tout $i \in \{1; \dots; l\}$.

Dans la suite, nous serons amenés à ne considérer que des factorisations finies à n facteurs $(X_1, \dots, X_n)$. Les codes X_1 et X_n sont les codes *externes* gauche et droit respectivement, de même les codes X_2 et X_{n-1} seront appelés les *premiers codes internes* (si $n \geqq 3$). Notons que quand nous introduirons la notion de factorisation monoïdale, nous parlerons aussi de facteurs externes et internes d'une telle factorisation quand elle est finie. Mais nous ne répèterons pas les définitions, car elles se transposent facilement.

III. LIBERTÉ ET LIMITATION DES FACTEURS D'UNE FACTORISATION MONOÏDALE FINIE DE A^*

Nous allons introduire un concept généralisant la notion de factorisation au sens usuel, celui de factorisation monoïdale. C'est dans ce cadre plus général que nous étudierons les facteurs d'une factorisation et où nous essaierons de voir leur limitation.

1. Factorisations monoïdales

DÉFINITION : Soit A un alphabet, soit I un ensemble totalement ordonné, soit $(M_i)_{i \in I}$ une famille de sous-monoïdes de A^*. Nous dirons que cette famille forme une *factorisation monoïdale* de A^* si et seulement si : pour tout mot w non vide de A^*, il existe un et seul uplet $(m_{\alpha_1}; \dots; m_{\alpha_n})$ avec $m_{\alpha_i} \in M_{\alpha_i} \setminus \{1\}$ pour tout i et avec $\alpha_1 < \alpha_2 < \dots < \alpha_n$ tel que $w = m_{\alpha_1} \dots m_{\alpha_n}$.

Remarques : 1. Cette définition généralise la notion de factorisation au sens usuel (*cf.* [1]). En effet si $(X_i)_{i \in I}$ est une factorisation au sens usuel, il est clair que $(X_i^*)_{i \in I}$ est une factorisation monoïdale.

2. Soit $(M_i)_{i \in I}$ une famille de sous-monoïdes de A^*, indexée par un ensemble I totalement ordonné. Alors il est clair que $(M_i)_{i \in I}$ est une factorisation monoïdale de A^* si et seulement si on a l'égalité suivante entre séries formelles de $\mathcal{N} \langle A^* \rangle$:

$$\underline{A}^* = \prod_{i \in I} \underline{M}_i$$

DÉFINITION : Soit $(M_i)_{i \in I}$ une factorisation monoïdale de A^*. Les sous-monoïdes M_i sont appelés les facteurs de la factorisation. Si tous les facteurs d'une factorisation monoïdale sont des sous-monoïdes libres de A^*, alors on dira que la factorisation monoïdale est *libre.*

Modulo la remarque (1), nous voyons que les factorisations monoïdales libres sont en fait les factorisations au sens usuel. Un problème apparaît donc très naturellement ; existe-t-il des factorisations monoïdales non libres ? Autrement dit, avons-nous réellement défini une classe de factorisations plus grande que celle des factorisations au sens usuel ? Nous allons apporter des éléments de réponse dans le cas des factorisations monoïdales finies (i. e. celles où I est fini) en montrant comment ce problème est lié à celui de la limitation des codes intervenant dans une factorisation finie au sens usuel.

2. Quelques résultats de symétrisation

Nous allons établir ici quelques résultats qui nous permettrons dans la suite de montrer très rapidement des propositions « symétriques » de propositions déjà prouvées.

DÉFINITION : *Soit* $w \in A^*$, alors on définit $w^\sim$ comme :

(i) si $w=1$, $w^\sim=1$;

(ii) si $w \in A^* \setminus \{1\}$, alors $w=a_1 \ldots a_n$ avec $a_i \in A$ pour $1 \leqq i \leqq n$. On note alors : $w^\sim=a_n \ldots a_1$.

Alors pour tout $X \subset A^*$, on notera : $X^\sim=\{x^\sim, x \in X\}$.

Remarques : 1. Il est clair que :

$$\forall x, y \in A^*, \qquad (xy)^\sim=y^\sim x^\sim \tag{1}$$

$$\forall x \in A^*, \qquad (x^\sim)^\sim=x \tag{2}$$

2. Si M est un sous-monoïde de A^*, alors $M^\sim$ est encore un sous-monoïde de A^*.

LEMME III.1 : *Soit σ l'application de $\mathbb{N}\langle A^*\rangle$ dans $\mathbb{N}\langle A^*\rangle$ définie par :*

$$\sigma\Big(\sum_{w \in A^*} \alpha_w w\Big)=\sum_{w \in A^*} \alpha_{w^\sim} w$$

Alors σ est un antiautomorphisme involutif du semi-anneau $\mathbb{N}\langle A^*\rangle$.

Preuve : Il est clair que $\sigma^2=\mathrm{Id}$ et que σ est un homomorphisme du monoïde additif $\mathbb{N}\langle A^*\rangle$ dans lui-même. Montrons que :

$$\forall \alpha, \beta \in \mathbb{N}\langle A^*\rangle, \qquad \sigma(\alpha\beta)=\sigma(\beta)\sigma(\alpha),$$

ce qui prouvera le lemme.

Soit donc α, β dans $\mathbb{N}\langle A^*\rangle$, on peut alors écrire :

$$\alpha = \sum_{w \in A^*} \alpha_w w \qquad \text{et} \qquad \beta = \sum_{w \in A^*} \beta_w w$$

Alors on a :

$$\sigma(\alpha\beta) = \sigma\Big(\sum_{w \in A^*}\Big(\sum_{mn=w} \alpha_m \beta_n\Big) w\Big) = \sum_{w \in A^*}\Big(\sum_{mn=w^\sim} \alpha_m \beta_n\Big) w$$

On a alors :

$$\sigma(\alpha\beta) = \sum_{w \in A^*}\Big(\sum_{ts=w} \beta_{t^\sim} \alpha_{s^\sim}\Big) w$$

car $mn = w^\sim$ si et seulement si $m = s^\sim$, $n = t^\sim$ avec $ts = w$.

D'où :

$$\sigma(\alpha\beta) = \Big(\sum_{t \in A^*} \beta_{t^\sim} t\Big)\Big(\sum_{s \in A^*} \alpha_{s^\sim} s\Big) = \sigma(\beta)\,\sigma(\alpha). \ \blacksquare$$

On peut maintenant démontrer aisément la proposition suivante :

PROPOSITION II.2. : *Soit* $n \in \mathbb{N}^*$, *soit* $(M_1, \ldots, M_n)$ *une factorisation monoïdale finie de* A^*, *alors* $(M_n^\sim, \ldots, M_1^\sim)$ *est encore une factorisation monoïdale de* A^*.

Preuve : Soit donc $n \in \mathbb{N}^*$ et $(M_1, \ldots, M_n)$ une factorisation monoïdale finie de A^*. On a donc (*cf.* remarque 2) du paragraphe 1)

$$\underline{A}^* = \underline{M}_1 \ldots \underline{M}_n.$$

Appliquons l'homomorphisme σ, défini dans le lemme II.1, à cette égalité entre séries de $\mathbb{N}\langle A^*\rangle$. Compte tenu de ce que σ est un antiautomorphisme, on obtient donc :

$$\underline{A}^* = \sigma(\underline{A}^*) = \sigma(\underline{M}_n) \ldots \sigma(\underline{M}_1) = \underline{M}_n^\sim \ldots \underline{M}_1^\sim$$

ainsi on a : $\underline{A}^* = \underline{M}_n^\sim \ldots\ldots \underline{M}_1^\sim$. Cela prouve que $(M_n^\sim, \ldots, M_1^\sim)$ est une factorisation monoïdale, compte tenu de la remarque 2 du paragraphe précédent et du fait que les $M_n^\sim$ sont bien des sous-monoïdes de A^*. $\blacksquare$

Nous pouvons aussi montrer le résultat suivant :

PROPOSITION III.3 : *Soit* M *un sous-monoïde de* A^* *et soit* p, q *deux entiers. Alors* : M *vérifie la condition* $C(p, q)$ *si et seulement si* $M^\sim$ *vérifie la condition* $C(q, p)$.

Preuve : Comme $(M^{\sim})^{\sim} = M$, il suffit de vérifier que si M vérifie la condition $C(p, q)$, alors $M^{\sim}$ vérifie la condition $C(q, p)$.

Soit donc un sous-monoïde M de A^* vérifiant $C(p, q)$. On va voir que $M^{\sim}$ vérifie $C(q, p)$. Considérons donc des mots $u_0, \ldots, u_{p+q}$ de A^* tels que : $u_{i-1} u_i \in M^{\sim}$ pour i compris entre 1 et $p+q$. On en déduit donc que : pour $1 \leqq i \leqq p+q$,

$$u_i^{\sim} u_{i-1}^{\sim} \in M.$$

Comme M vérifie la condition $C(p, q)$, on en déduit que le $p+1$-ième élément de la suite $u_{p+q}^{\sim}, u_{p+q-1}^{\sim}, \ldots, u_0^{\sim}$ est dans M. Cela nous donne donc :

$$u_q^{\sim} \in M$$

D'où $u_q \in M^{\sim}$. Cela signifie bien que $M^{\sim}$ vérifie la condition $C(q, p)$. ■

3. Liberté et limitation des facteurs externes d'une factorisation monoïdale finie

Le lemme suivant est une généralisation d'un résultat démontré pour $n=3$ (*cf.* [1]).

LEMME III.4 : *Soit $(M_1, \ldots, M_n)$ une factorisation monoïdale finie de A^*, alors $M_1 \ldots M_{n-1}$ est suffixiel et $M_2 \ldots M_n$ est préfixiel.*

Preuve : Soit $w \in M_1 \ldots M_{n-1}$. On peut donc écrire :

$$w = y_1 \ldots y_{n-1} \tag{1}$$

avec $y_i \in M_i$ pour tout $i \in \{1; \ldots; n-1\}$.

Soient alors $u, v \in A^*$ tels que :

$$w = uv \tag{2}$$

Comme $(M_1, \ldots, M_n)$ est une factorisation monoïdale de A^*, nous avons donc :

$$v = x_1 \ldots x_n \tag{3}$$

avec $x_i \in M_i$ pour tout $i \in \{1; \ldots; n\}$. On peut également écrire pour la même raison :

$$u x_1 \ldots x_{n-1} = x'_1 \ldots x'_n \tag{4}$$

avec $x'_i \in M_i$ pour tout $i \in \{1; \ldots, n\}$.

Des relations (1), (2), (3) et (4), on tire donc :

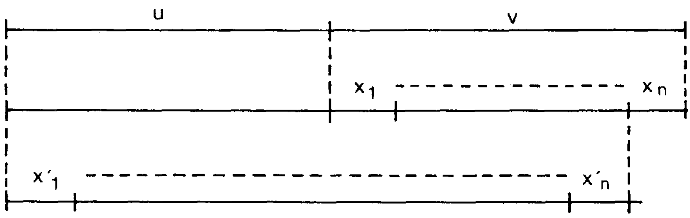
$$y_1 \ldots y_{n-1} = w = uv = (ux_1 \ldots x_{n-1}) x_n = x'_1 \ldots x'_n x_n$$

Par unicité d'une telle décomposition, on a donc :

$$x_n = x'_n = 1$$

Donc, par (3), v appartient à $M_1 \ldots M_{n-1}$, ce qui prouve que $M_1 \ldots M_{n-1}$ est suffixiel.

Une démonstration analogue prouverait que $M_2 \ldots M_n$ est préfixiel. ■



$M_1 \ldots M_{n-1}$ est suffixiel.

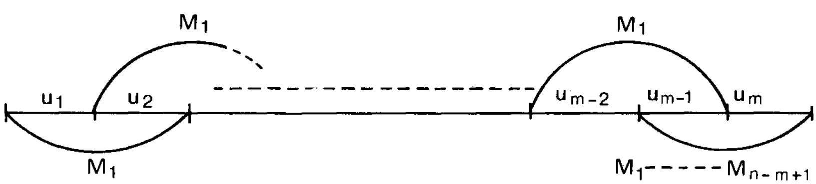
Nous pouvons maintenant établir :

Proposition III.5 : *Soit $n \in \mathbb{N}^*$, soit $(M_1, \ldots, M_n)$ une factorisation monoïdale finie de A^*. Alors pour tout m tel que $2 \leqq m \leqq n$, pour tout $u_1, \ldots, u_m$ mots de A^* vérifiant :*

$$\forall i, \quad 1 \leqq i \leqq m-2, \qquad u_i u_{i+1} \in M_1 \qquad \text{et} \qquad u_{m-1} u_m \in M'_1 \ldots M_{n-m+1}$$

on a :

$$\forall i, \quad 2 \leqq i \leqq m, \qquad u_i \in M_1 \ldots M_{n-i+1}$$



Preuve : On fait une récurrence sur m. Le lemme III.4 nous permet d'écrire :

$$\forall u_1, u_2 \in A^*, \qquad u_1 u_2 \in M_1 \ldots M_{n-1} \quad \Rightarrow \quad u_2 \in M_1 \ldots M_{n-1}$$

Cela établit donc notre proposition pour $m=2$. Supposons donc la proposition établie jusqu'à l'ordre m avec $2 \leqq m \leqq n-1$ et considérons alors

$u_1, \ldots, u_{m+1}$ tel que :

$$\forall i, \quad 1 \leqq i \leqq m-1, \qquad u_i u_{i+1} \in M_1 \qquad \text{et} \qquad u_m u_{m+1} \in M_1 \ldots M_{n-m}.$$

On doit donc démontrer que :

$$\forall i \in \{2; \ldots; m+1\}, \qquad u_i \in M_1 \ldots M_{n-i+1}. \tag{1}$$

Pour $i \in \{2; \ldots m\}$, (1) découle de l'hypothèse de récurrence appliquée à $(u_1, \ldots, u_m)$. De plus on peut aussi appliquer l'hypothèse de récurrence à $(u_2, \ldots, u_{m+1})$ car $M_1 \ldots M_{n-m}$ est inclus dans $M_1 \ldots M_{n-m+1}$. On en déduit donc :

$$u_{m+1} \in M_1 \ldots M_{n-m+1}.$$

Donc il existe des $m_i \in M_i$ pour tout $i \in \{1; \ldots; n-m+1\}$ tels que :

$$u_{m+1} = m_1 \ldots m_{n-m+1} \tag{2}$$

Comme $u_{m-1} u_m m_1 \ldots m_{n-m} \in M_1 \ldots M_{n-m}$, on peut aussi appliquer l'hypothèse de récurrence à $(u_1, \ldots, u_{m-1}, u_m m_1 \ldots m_{n-m})$ et l'on obtient :

$$u_m m_1 \ldots m_{n-m} \in M_1 \ldots M_{n-m+1}$$

On peut donc écrire :

$$u_m m_1 \ldots m_{n-m} = x_1 \ldots x_{n-m+1} \tag{3}$$

avec $x_i \in M_i$ pour tout i, $1 \leqq i \leqq n-m+1$. De (2) et (3), on déduit :

$$u_m u_{m+1} = x_1 \ldots x_{n-m+1} m_{n-m+1}$$

or ce mot appartient à $M_1 \ldots M_{n-m}$ par hypothèse, ce qui implique par unicité d'une telle factorisation :

$$m_{n-m+1} = x_{n-m+1} = 1$$

On a donc alors par (2), $u_{m+1} \in M_1 \ldots M_{n-m}$ ce qui montre (1) pour $i = m+1$. Cela termine donc notre preuve. ■

COROLLAIRE III.6 : *Soit $n \in \mathbb{N}^*$, soit $(M_1, \ldots, M_n)$ une factorisation monoïdale finie de A^*. Alors M_1 vérifie la condition C $(n-1;\ 0)$. Autrement dit M_1 est un sous-monoïde libre dont la base est un code $(n-1;\ 0)$-limité.*

Preuve : Il suffit d'appliquer la proposition III.5 avec $m = n$. ■

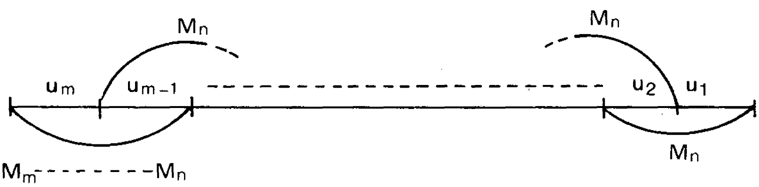
On peut aussi montrer :

Proposition III.7 : *Soit $n \in \mathbb{N}^*$, soit $(M_1, \ldots, M_n)$ une factorisation monoïdale finie de A^*. Alors pour tout $m \in \mathbb{N}$ tel que $2 \leqq m \leqq n$, pour tout $u_1, \ldots, u_m \in A^*$ tels que :*

$$\forall i, \quad 1 \leqq i \leqq m-2, \qquad u_{i+1} u_i \in M_n \qquad \text{et} \qquad u_m u_{m-1} \in M_m \ldots M_n$$

on a :

$$\forall i, \quad 2 \leqq i \leqq m, \qquad u_i \in M_i \ldots M_n$$



Preuve : Soit donc $m \in \mathbb{N}^*$ tel que que $2 \leqq m \leqq n$, soit $u_1, \ldots, u_m \in A^*$ vérifiant :

$$\forall i, \quad 1 \leqq i \leqq m-2, \qquad u_{i+1} u_1 \in M_n \qquad \text{et} \qquad u_m u_{m-1} \in M_m \ldots M_n.$$

On en déduit donc :

$$\forall i, \quad 1 \leqq i \leqq m-2, \qquad u_i^{\sim} u_{i+1}^{\sim} \in M_n^{\sim} \qquad \text{et} \qquad u_{m-1}^{\sim} u_m^{\sim} \in M_n^{\sim} \ldots M_m^{\sim}.$$

Or par la proposition III.2, $(M_n^{\sim}, \ldots, M_1^{\sim})$ est une factorisation monoïdale finie. La proposition III.5, appliquée à cette factorisation, permet donc d'affirmer que :

$$\forall i, \quad 2 \leqq i \leqq m, \qquad u_i^{\sim} \in M_n^{\sim} \ldots M_i^{\sim}$$

c'est-à-dire :

$$\forall i, \quad 2 \leqq i \leqq m, \qquad u_i \in M_i \ldots M_n. \blacksquare$$

Corollaire III.8 : *Soit $n \in \mathbb{N}^*$, soit $(M_1, \ldots, M_n)$ une factorisation monoïdale finie de A^*. Alors M_n est un sous-monoïde de A^* vérifiant la condition $C(0;\, n-1)$. Autrement dit M_n est libre et a pour base un code $(0;\, n-1)$ limité.*

Preuve : Il suffit d'appliquer la proposition III.7, avec $m = n$. $\blacksquare$

Remarque : On aurait pu déduire directement le corollaire III.8 du corollaire III.6 comme suit :

si $(M_1, \ldots, M_n)$ est une factorisation monoïdale finie de A^*, alors par la proposition III.2, $(M_n^\sim, \ldots, M_1^\sim)$ est encore une factorisation monoïdale de A^*. Le corollaire III.6 appliquée à cette dernière montre que $M_n^\sim$ vérifie $C(n-1; 0)$, ce qui est équivalent, grâce à la proposition III.3 au fait que M_n vérifie $C(0; n-1)$. Ainsi une preuve directe est possible. Nous avons préféré cependant procéder comme précédemment car la proposition III.7 montre bien la nature du processus qui conduit à ce que M_n vérifie la condition $C(0; n-1)$.

4. Liberté et limitation des premiers facteurs internes d'une factorisation monoïdale finie

Nous venons de voir que si $(M_1, \ldots, M_n)$ était une factorisation finie alors M_1 et M_n vérifient respectivement $C(n-1; 0)$ et $C(0; n-1)$. Nous allons voir maintenant que M_2 et M_{n-1} vérifient respectivement $C(n-2; 1)$ et $C(1; n-2)$.

Donnons tout de suite la proposition principale :

PROPOSITION III.9 : *Soit $n \in \mathbb{N}^*$, soit $(M_1, \ldots, M_n)$ une factorisation monoïdale finie de A^*. Alors pour tout $m \in \mathbb{N}$ vérifiant $3 \leqq m \leqq n$, pour tout $u_1, \ldots, u_m \in A^*$ tels que :*

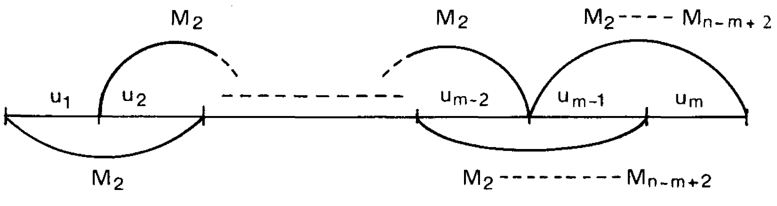
$$\forall i, \quad 1 \leqq i \leqq m-3, \qquad u_i u_{i+1} \in M_2$$

et

$$u_{m-2} u_{m-1},\ u_{m-1} u_m \in M_2 \ldots M_{n-m+2}$$

on a :

$$\forall i, \quad 1 \leqq i \leqq m-1, \qquad u_i \in M_2 \ldots M_{n-i+1}$$



Preuve : Nous allons faire une récurrence sur m.
Pour $m=3$, considérons donc $u_1 u_2$, et u_3 dans A^* tels que :

$$u_1 u_2,\ u_2 u_3 \in M_2 \ldots M_{n-1}$$

Le lemme III.4 montre que :

$$u_1 \in M_2 \ldots M_n \qquad \text{et} \qquad u_2 \in M_1 \ldots M_{n-1} \cap M_2 \ldots M_n.$$

Par l'unicité de la décomposition, on déduit donc que $u_2 \in M_2 \ldots M_{n-1}$; ce qui prouve la proposition pour $m=3$. Supposons maintenant notre proposition vraie à un ordre m avec $3 \leqq m \leqq n-1$ et soient $u_1, \ldots, u_{m+1} \in A^*$ tels que :

$$\forall i, \quad 1 \leqq i \leqq m-2,$$

$$u_i u_{i+1} \in M_2 \qquad \text{et} \qquad u_{m-1} u_m, u_m u_{m+1} \in M_2 \ldots M_{n-m+1}.$$

Il faut donc montrer que :

$$\forall i \in [\![1; m]\!], \qquad u_i \in M_2 \ldots M_{n-i+1} \tag{1}$$

L'hypothèse de récurrence appliquée à $(u_1, \ldots, u_m)$ donne (1) pour $i \in \{1; \ldots; m-1\}$. Mais l'on peut aussi l'appliquer à $(u_2, \ldots, u_{m+1})$ et elle nous dit alors que :

$$u_m \in M_2 \ldots M_{n-m+2}$$

Donc on peut écrire :

$$u_m = x_2 \ldots x_{n-m+2} \tag{2}$$

avec $x_i \in M_i$ pour tout i.

Enfin l'hypothèse de récurrence appliquée à

$$(u_1, \ldots, u_{m-2}, u_{m-1} x_2 \ldots x_{n-m+1}, x_{n-m+2})$$

donne :

$$u_{m-1} x_2 \ldots x_{n-m+1} \in M_2 \ldots M_{n-m+2}$$

Donc il existe des $y_i \in M_i$ pour $i \in \{2, \ldots, n-m+2\}$ tels que :

$$u_{m-1} x_2 \ldots x_{n-m+1} = y_2 \ldots y_{n-m+2} \tag{3}$$

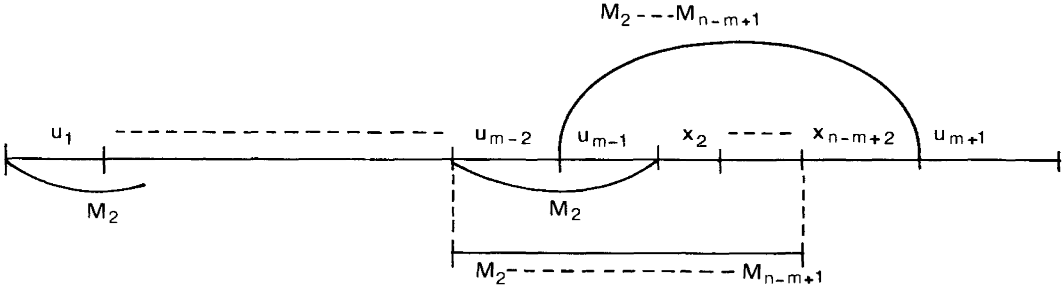
A l'aide de (2) et (3), on a donc :

$$u_{m-1} u_m = u_{m-1} x_2 \ldots x_{n-m+2} = y_2 \ldots y_{n-m+2} x_{n-m+2}$$

Or par hypothèse, $u_{m-1} u_m \in M_2 \ldots M_{n-m+1}$; l'unicité de la décomposition implique donc que :

$$u_{n-m+2} = y_{n-m+2} = 1.$$

D'où par (2), $u_m \in M_2 \ldots M_{n-m+1}$. Cela prouve donc (1) pour $i=m$ et termine notre preuve.



■

On en déduit donc :

COROLLAIRE III.10 : *Soit* $n \in \mathbb{N}$, $n \geqq 3$, *soit* $(M_1, \ldots, M_n)$ *une factorisation monoïdale finie de* A^*. *Alors* M_2 *vérifie la condition* $C(n-2;\ 1)$. *Autrement dit* M_2 *est libre et a une base qui est un code* $(n-2;\ 1)$*-limité.*

Preuve : Il suffit d'appliquer la proposition III.9 avec $m=n$. ■

COROLLAIRE III.11 : *Soit* $n \in \mathbb{N}$, $n \geqq 3$, *soit* $(M_1, \ldots, M_n)$ *une factorisation monoïdale finie de* A^*. *Alors* M_{n-1} *vérifie la condition* $C(1;\ n-2)$. *Autrement dit* M_{n-1} *est libre, de base un code* $(1;\ n-2)$*-limité.*

Preuve: Soit $n \geqq 3$ et $(M_1, \ldots, M_N)$ une factorisation monoïdale finie de A^*. Alors par la proposition III.2, $(M_n^{\sim}, \ldots, M_1^{\sim})$ est encore une factorisation monoïdale de A^*. Le corollaire III.10 appliqué à cette factorisation nous montre que $M_{n-1}^{\sim}$ vérifie $C(n-2;\ 1)$. Alors grâce à la proposition III.3, On montre que M_{n-1} vérifie $C(1;\ n-2)$. ■

Remarque : On aurait pu aussi montrer ce corollaire en établissant d'abord la proposition symétrique de la proposition III.9 et en appliquant cette dernière avec $m=n$.

Conséquences : Les résultats que nous venons d'établir nous permettent donc de répondre à deux types de questions :

1. pour une factorisation $(X_1, \ldots, X_n)$ au sens usuel, on voit donc que X_1, X_2, X_{n-1} et X_n sont des codes respectivement $(n-1;\ 0)$, $(n-2;\ 1)$, $(1;\ n-2)$ et $(0;\ n-1)$ limités. Cela donne donc une réponse partielle à la conjecture de Berstel-Perrin. Remarquons que nous retrouvons donc immédiatement les résultats connus pour les bisections et les trisections et que nous montrons

que, pour une quadrisection (X_1, X_2, X_3, X_4), tous les codes qui y interviennent sont limités, (X_1, X_2, X_3, X_4) étant respectivement (3,0), (2,1), (1,2) et (0,3)-limités;

2. pour une factorisation monoïdale finie $(M_1, \ldots, M_n)$ de A^*, les facteurs M_1, M_2, M_{n-1} et M_n sont libres, de base un code limité. En particulier, nous avons donc montré que pour $n \leqq 4$, toutes les factorisations monoïdales finies à n éléments étaient libres. Signalons que nous pensons, qu'à partir de $n=5$, il doit être possible de construire une factorisation monoïdale à n facteurs qui ne soit pas libre. Mais cela reste pour le moment un problème ouvert.

5. Caractérisation des facteurs externes intervenant dans une factorisation monoïdale finie

Nous avons vu au paragraphe 3 que les facteurs externes M_1 et M_n d'une factorisation monoïdale finie $(M_1, \ldots, M_n)$ de A^* vérifiaient $C(0; n-1)$ respectivement. On peut très naturellement se demander si ces conditions sont suffisantes pour que les sous-monoïdes correspondants de A^* soient les facteurs externes d'une factorisation monoïdale finie : nous allons voir que pour $n \geqq 4$, il n'en est rien. Nous allons en effet trouver une condition nécessaire et suffisante pour qu'un sous-monoïde de A^* soit le facteur externe d'une factorisation monoïdale finie à n facteurs. Nous aurons besoin du lemme :

Lemme III.12 : *Soit M un sous-monoïde de A^*, soit M_1 l'ensemble des facteurs droits des éléments de M, alors M_1^* vérifie la condition $C(1,0)$ dans A^*.*

Preuve : Elle est immédiate puisqu'un facteur droit d'un élément de M_1 est encore dans M_1. ■

Remarque : Il est facile de voir que M_1^*, défini dans le lemme III.12, est le plus petit sous-monoïde de A^*, contenant M et vérifiant la condition $C(1; 0)$ dans A^*.

On peut maintenant donner la définition et la construction suivante. Soit M un sous-monoïde de A^*, on va lui associer une suite $(D_n^*)_{n \geqq 0}$ de sous-monoïdes définie comme suit :

$$D_0^* = A^*.$$

Supposons $n \geqq 0$ et D_n^* défini tel que D_n^* soit un sous-monoïde de A^*, contenant M et étant libre de base le code U_n. On pose alors :

$$D_{n+1} = \{ \alpha \in U_n^*, \exists \beta \in U^*, \beta\alpha \in M \}.$$

Autrement dit D_{n+1} est l'ensemble des facteurs droits des éléments de M dans U_n^*. Par le lemme III.12, D_{n+1}^* vérifie la condition $C(1; 0)$ dans U_n^*. Donc D_{n+1}^* est un sous-monoïde de A^*, libre, contenant M et inclus dans D_n^*. Cela définit donc une suite $(D_n^*)_{n \geqq 0}$ décroissante de sous-monoïdes libres de A^*, contenant tous M. De plus pour tout n, D_{n+1}^* vérifie $C(1, 0)$ dans D_n^*.

DÉFINITION : La suite (D_n^*) ainsi définie s'appellera la suite des facteurs droits associée à M. Si M est un monoïde libre de base le code X, la suite (D_n^*) sera aussi dite associée à X.

Remarque : La suite (D_n^*) associée à un monoïde M peut très bien être stationnaire. Par exemple si $M=(ab+ba)^*$ avec $A=a+b$, on vérifiera que la suite des facteurs droits associée à M est stationnaire constamment égale à A^*.

On peut maintenant énoncer :

PROPOSITION III.13 : *Soit $n \in \mathbb{N}$, $n \geqq 2$, soit $(M_1, \ldots, M_n)$ une factorisation monoïdale finie de A^* et soit $(D_n^*)_{n \geqq 0}$ la suite des facteurs droits associée à M_1. Alors pour tout $k \in [\![0; n-2]\!]$, pour tout $m \in [\![2; n-k]\!]$, pour tout $u_1, \ldots, u_m$ vérifiant :*

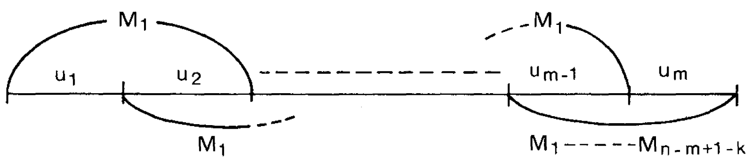
$$u_1, \ldots, u_{m-1} \in D_k^*, \qquad u_m \in A^*$$

et

$$\forall i, \quad 1 \leqq i \leqq m-2, \qquad u_i u_{i+1} \in M_1, \qquad u_{m-1} u_m \in M_1 \ldots M_{n-m+1-k}$$

on a :

$$\forall i, \quad 2 \leqq i \leqq m, \qquad u_i \in M_1 \ldots M_{n+1-i-k}$$



Preuve : On fait une récurrence sur k. Remarquons tout d'abord que pour $k=0$, le résultat n'est autre que celui établi par la proposition III.5. En particulier si $n=2$, la proposition est établie. On supposera donc désormais que $n \geqq 3$.

Supposons donc la proposition établie à l'ordre $k-1$ avec $1 \leqq k \leqq n-2$. On va montrer qu'elle est vraie à l'ordre k par récurrence sur m. Établissons là d'abord pour $m=2$. Considérons donc $u_1 \in D_k^*$ et $u_2 \in A^*$ tels que :

$$u_1 u_2 \in M_1 \ldots M_{n-1-k}$$

On veut établir que :

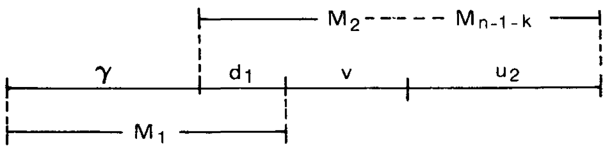
$$u_2 \in M_1 \ldots M_{n-1-k} \tag{1}$$

Nous allons montrer cela par récurrence sur le nombre minimal $\alpha(u_1)$ d'éléments de D_k nécessaire à l'écriture de u_1. Si $\alpha(u_1)=0$, $u_1=1$ et (1) est évident. Sinon supposons que (1) ait été établi pour tous les u_1 dans D_k^* tels que $\alpha(u_1)<l$ où $l \in \mathbb{N}^*$. Montrons alors que (1) est vrai si $\alpha(u_1)=l$. Soit donc u_1 tel que $\alpha(u_1)=l$. On peut donc écrire :

$$u_1 = d_1 \ldots d_1 = d_1 v$$

où les d_i sont tous dans D_k et où donc $v \in D_k^*$.

Par définition de D_k, il existe $\gamma \in D_{k-1}^*$ tel que : $\gamma\, d_1 \in M_1$.



On a $n \geqq 3$, d'où $0 \leqq k-1 \leqq n-3$ et donc $k-1$ existe et $n-(k-1) \geqq 3$. Comme la proposition est supposée établie à l'ordre $k-1$, on peut l'appliquer à cet ordre, avec $m=3$, au triplet (γ, d_1, vu_2) car $d_1 \in D_k \subset D_{k-1}^*$. Cela donne alors :

$$vu_2 \in M_1 \ldots M_{n-1-k}$$

Or il est clair que $\alpha(v)<l$. Donc en raison de notre hypothèse de récurrence appliquée à (v, u_2), on en déduit (1). Cela établit donc la proposition à l'ordre k, au rang $m=2$. Supposons donc la proposition prouvée à l'ordre k, au rang m avec $2 \leqq m \leqq n-k-1$ et montrons qu'elle est alors vraie au rang $m+1$. Cela terminera la preuve.

Soit donc $u_1, \ldots, u_{m+1}$ des mots de A^* tels que :

$$u_1, \ldots, u_m \in D_k^*$$

et vérifiant :

$$\forall i, \quad 1 \leqq i \leqq m-1, \qquad u_i u_{i+1} \in M_1 \qquad \text{et} \qquad u_m u_{m+1} \in M_1 \ldots M_{n-m-k}$$

On veut montrer que :

$$\forall i, \quad 2 \leqq i \leqq m+1, \qquad u_i \in M_1 \ldots M_{n+1-i-k} \tag{2}$$

On remarque qu'on peut appliquer la proposition à l'ordre k, au rang m à $(u_1, \ldots, u_m)$ puisque par hypothèse, elle est établi à ce rang-là. On obtient alors (2) pour tous les i compris entre 2 et m.

On peut aussi appliquer la proposition à l'ordre k, au rang m à $(u_2, \ldots, u_{m+1})$ car $M_1 \ldots M_{n-m-k} \subset M_1 \ldots M_{n+1-m-k}$.

On obtient alors :

$$u_{m+1} \in M_1 \ldots M_{n+1-m-k}$$

On peut donc écrire :

$$u_{m+1} = x_1 \ldots x_{n+1-m-k} \tag{3}$$

où $x_i \in M_i$ pour tout $i \in \{1; \ldots; n+1-m-k\}$.

On remarque qu'on peut alors appliquer la proposition à l'ordre k, au rang m à $(u_1, \ldots, u_{m-1}, u_m x_1 \ldots x_{n-m-k})$. On obtient donc :

$$u_m x_1 \ldots x_{n-m-k} \in M_1 \ldots M_{n+1-m-k}$$

On peut alors écrire :

$$u_m x_1 \ldots x_{n-m-k} = y_1 \ldots y_{n+1-m-k} \tag{4}$$

où $y_i \in M_i$ pour tout $i \in \{1; \ldots; n+1-m-k\}$.

A l'aide de (3) et (4), on peut donc écrire :

$$u_m u_{m+1} = u_m x_1 \ldots x_{n-m-k} x_{n-m-k+1} = y_1 \ldots y_{n+1-m-k} x_{n-m-k+1}$$

or par hypothèse, $u_m u_{m+1} \in M_1 \ldots M_{n-m-k}$. L'unicité de la décomposition montre donc que :

$$y_{n+1-m-k} = x_{n-m-k+1} = 1$$

Compte tenu de (3), on obtient donc $u_{m+1} \in M_1 \ldots M_{n-m-k}$, ce qui prouve (2) pour $i = m+1$.

Cela termine donc notre preuve. ■

COROLLAIRE III.14 : *Soit $n \in \mathbb{N}^*$, $n \geqq 2$. Soit $(M_1, \ldots, M_n)$ une factorisation monoïdale finie de A^* et soit $(D_n^*)_{n \geqq 0}$ la suite des facteurs droits associée à*

M_1. *Alors :*

(i) M_1 *vérifie la condition* C (1; 0) *dans* D_{n-2}^*;

(ii) $M_1 = D_{n-1}^*$.

La condition (i) *signifie donc que le sous-monoïde libre* M_1 *de* A^* *a une base* X_1 *qui est un code* (1, 0)*-limité dans le sous-monoïde libre* D_{n-2}^* *de* A^*.

Preuve : Le (i) résulte immédiatement de la proposition III.13 appliquée avec $k = n-2$ et $m = 2$.

Pour voir le (ii), il suffit de se rappeler que par définition :

$$D_{n-1} = \{ \alpha \in D_{n-2}^*,\ \exists \beta \in D_{n-2}^*,\ \beta\alpha \in M_1 \}.$$

Comme M_1 est $C(1; 0)$ dans le monoïde libre D_{n-2}^* par (i), on voit donc que $D_{n-1} \subset M_1$. L'inclusion contraire étant évidente, on obtient donc bien (ii). ■

Rappelons la définition due à Viennot :

Définition : Soit $\mathscr{F} = (X_1, \ldots, X_n)$ une factorisation (au sens usuel) finie à n facteurs de A^*, avec $n \geqq 2$. On dit que $\mathscr{F}$ est *dichotomique à gauche* si et seulement si il existe des codes $Z_0, \ldots, Z_{n-2}$ de A^* tels que :

(i) (Z_0, X_n) est une bisection de A^*;

(ii) pour tout i, $1 \leqq i \leqq n-2$, (Z_i, X_{n-i}) est une bisection de Z_{i-1};

(iii) $Z_{n-2} = X_1$.

Remarque : On voit donc qu'une factorisation (au sens usuel) est dichotomique à gauche si elle peut s'obtenir par composition successive de bisections.

On peut maintenant énoncer le théorème fondamental de caractérisation des facteurs externes gauches intervenant dans une factorisation monoïdale finie.

Théorème III.15 : *Soit* $n \geqq 2$, $n \in \mathbb{N}$, *soit* X *un code de* A^* *et soit* $(D_n^*)_{n \geqq 0}$ *la suite des facteurs droits associée à* X. *Alors les propositions suivantes sont équivalentes :*

(i) X^* *est le facteur externe gauche d'une factorisation monoïdale finie* $(X^*, M_2, \ldots, M_n)$ *à* n *facteurs de* A^*.

(ii) X *est le facteur externe gauche d'une factorisation* (*au sens usuel*) *finie* $(X, X_2, \ldots, X_n)$ *à* n *facteurs de* A^*.

(iii) X *est le facteur externe gauche d'une factorisation* (*au sens usuel*) *finie* $(X, X_2, \ldots, X_n)$ *à* n *facteurs de* A^*, *dichotomique à gauche.*

(iv) X *est* (1, 0)*-limité dans* D_{n-2}^*;

(v) $X^* = D_{n-1}^*$;

Si de plus $n \geqq 3$, on peut rajouter :

(vi) *X est $(2, 0)$-limité dans D^*_{n-3}.*

Preuve : Il est clair que :

$$(iii) \to (ii) \to (i)$$

De plus le corollaire III. 14 nous montre que :

$$(i) \to (iv) \text{ et } (iv) \to (v)$$

Pour conclure à l'équivalence des cinq premières assertions, il va donc suffire de prouver (v) → (iii). C'est ce que nous allons faire. Soit donc X un code de A^* tel que :

$$X^* = D^*_{n-1}.$$

Rappelons la propriété suivante que nous appelerons la propriété (★) : tout code $(1, 0)$-limité dans un monoïde libre Y^* est le facteur gauche d'une bisection de Y^* (*cf.* [1]).

Notons U_i la base du monoïde libre D^*_i pour tout i. On a donc en particulier $U_{n-1} = X$.

Comme $D^*_1 = U^*_1$, U_1 est $(1,0)$-limité dans A^*. La propriété (★) nous assure donc l'existence d'un code V_n tel que :

$$(U_1, V_n) \text{ est une bisection de } A^* = U^*_0 = D^*_0.$$

Supposons des codes $V_n, V_{n-1}, \ldots, V_i$ construits avec $3 \leqq i \leqq n$ tels que :

$$\forall j \in \{1; \ldots; n-i+1\}, (U_j, V_{n-j+1}) \text{ est une bisection de } U^*_{j-1} = D^*_{j-1}.$$

Comme U_{n-i+2} est $(1,0)$-limité dans D^*_{n-i+1}, la propriété (★) nous permet de construire un code V_{i-1} tel que :

$$(U_{n-i+2}, V_{i-1}) \text{ est une bisection de } U^*_{n-i+1} = D^*_{n-i+1}.$$

Ainsi nous avons donc montré qu'on peut construire des codes : $V_n, \ldots, V_2$ tels que :

$$\forall j \in \{1, \ldots, n-1\}, (U_j, V_{n-j+1}) \text{ est une bisection de } U^*_{j-1} = D^*_{j-1}.$$

Comme $U_{n-1} = X$, compte tenu de la définition précédente, cela signifie donc que $(X, V_2, \ldots, V_n)$ est une factorisation dichotomique à gauche de A^*. Cela prouve donc l'équivalence des cinq premières assertions.

Remarquons qu'on en déduit qu'un code X (2, 0)-limité est toujours le facteur gauche d'une trisection car il est facile de voir qu'un tel code est nécessairement (1,0)-limité dans D_1^* (c'est ce que montre en fait Viennot dans [6]).

Montrons d'abord (vi) $\Rightarrow$ (ii) :

supposons donc $n \geqq 3$ et X (2, 0)-limité dans D_{n-3}^*.

Comme D_{n-3}^* est libre, la propriété citée ci-dessus permet de construire une trisection de D_{n-3}^* de la forme :

(X, W_2, W_3) où W_2 et W_3 sont des codes. Or on a vu qu'il était possible de construire des codes $V_n, \ldots, V_4$ tels que :

$$\forall i \in \{1; \ldots; n-3\},\ (U_i,\ V_{n-i+1}) \text{ est une bisection de } U_{i-1}^* = D_{i-1}^*.$$

On en déduit aisément que $(U_{n-3}, V_4, V_5, \ldots, V_n)$ est une factorisation (au sens usuel) de A^*, puis que : $(X, W_2, W_3, V_4, \ldots, V_n)$ est une factorisation de A^* (au sens usuel). Cela établit donc : (vi) $\Rightarrow$ (ii).

Terminons en remarquant que pour $n \geqq 3$, (iv) $\Rightarrow$ (vi) est clair. En effet si X est (1, 0)-limité dans D_{n-2}^*, comme D_{n-2}^* vérifie $C(1, 0)$ dans D_{n-3}^*, on en déduit que X est (2, 0)-limité dans D_{n-3}^* par composition de codes limités (*cf.* [1]).

Cela termine donc la preuve. ∎

Remarques : 1. Pour $n=2$ et $n=3$, on retrouve donc des résultats classiques établis par Schützenberger et Viennot : à savoir que les codes (1, 0) [resp. (2, 0)]-limités dans A^* sont exactement les facteurs gauches des bisections (resp. des trisections) de A^*.

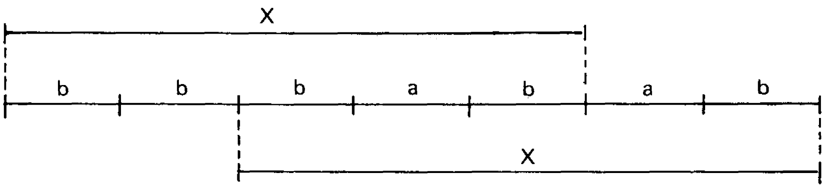
2. Toute la démarche de ce paragraphe peut bien entendu se transposer de façon immédiate pour caractériser les facteurs externes droits d'une factorisation monoïdale finie à n éléments. Il faudrait d'abord définir à la place de $(D_n^*)_{n \geq 0}$ une suite des facteurs gauches $(G_n^*)_{n \geq 0}$ associée à un sous-monoïde de A en remplaçant dans la définition facteur droit par facteur gauche. On pourrait alors énoncer des équivalences similaires à celles du théorème précédent et les démontrer à l'aide de ce théorème et des résultats du paragraphe 2.

Exemple : Nous allons montrer un exemple de code (3,0)-limité qui n'est pas le facteur gauche d'une quadrisection de A^*, ce qui montrera que la remarque 1 précédente devient fausse à partir des quadrisections. Soit donc

$$A = \{a; b\} \qquad \text{et} \qquad X = \{a^4 b,\ ba^3 b,\ b^2 a^2 b,\ b^3 ab,\ a^3 bab,\ babab\}.$$

X est « comma-free » (*cf.* [1], p. 350) donc il est $(3, 0)$-limité (*cf.* [1], p. 336). Mais on peut écrire :

$$(b^2)\, bab \in X, \qquad (bab)\, ab \in X \qquad \text{et} \qquad ab \notin X^*$$



or b, bab, ab sont dans D_1, donc $b^2 \in D_1^*$. Ainsi la relation précédente prouve que X n'est pas $(2, 0)$-limité dans D_1^*. Le théorème III.15 montre donc que X tout en étant $(3, 0)$-limité, ne peut être le code externe gauche d'une quadrisection.

IV. UN THÉORÈME DE RECOLLEMENT POUR LES QUADRISECTIONS

Nous allons consacrer cette partie à l'étude des quadrisections. Comme nous avons vu, en III, que les factorisations monoïdales à 4 facteurs étaient libres, nous allons nous replacer désormais dans un cadre classique. Rappelons que Viennot a montré, en [6], que toute trisection (X, Y, Z) pouvait toujours s'obtenir à l'aide d'une bisection (X', Y') de A^* de telle sorte qu'il existe une bisection (X, X_1) de X'^* et une bisection (Z_1, Z) de Y'^* avec (X_1, Z_1) bisection de Y^*. Nous dirons qu'un tel résultat est un résultat de recollement de bisections.

Signalons que Viennot avait conjecturé qu'un tel résultat pourrait s'étendre à toutes les factorisations finies (ce qui ramènerait en ce sens les factorisations finies aux bisections). Nous allons établir ici un tel théorème pour les quadrisections et voir comment ce problème est relié à ceux étudiés en III.

1. Préliminaires

Nous avons regroupé dans le lemme suivant quelques résultats dont nous aurons besoin par la suite.

LEMME IV.1 : *Soit (X_1, X_2, X_3, X_4) une quadrisection de A^*. Alors :*

1. $X_3^* X_2^* \subset X_1^* X_2^* \cup X_3^* X_4^*$;
2. $X_2^* X_1^* \subset X_1^* X_2^* \cup X_2^* X_3^* \cup X_3^* X_4^*$;

3) $X_4^* X_3^* \subset X_1^* X_2^* \cup X_2^* X_3^* \cup X_3^* X_4^*$.

Preuve : Montrons d'abord l'assertion 1.

Soit donc $w \in X_3^* X_2^*$, alors il existe $x_3 \in X_3^*$, $x_2 \in X_2^*$ et $u_i \in X_i^*$ pour $i \in \{1; \ldots; 4\}$ tels que :

$$w = x_3 x_2 = u_1 u_2 u_3 u_4. \tag{1}$$

Trois cas peuvent se produire :

(*a*) $u_1 \neq 1$;

(*b*) $u_1 = 1$, $u_4 \neq 1$;

(*c*) $u_1 = u_4 = 1$;

Traitons le cas (*a*). Alors il existe α mot de A^* tel que l'on soit dans l'un des deux cas (i) ou (ii) suivants :

(i) $x_3 = u_1 \alpha$, $\alpha x_2 = u_2 u_3 u_4$;

(ii) $x_3 \alpha = u_1$, $x_2 = \alpha u_2 u_3 u_4$.

Le cas (i) ne peut pas se produire. En effet dans ce cas, comme, par le lemme III.4, $X_2^* X_3^* X_4^*$ est préfixiel, on aurait :

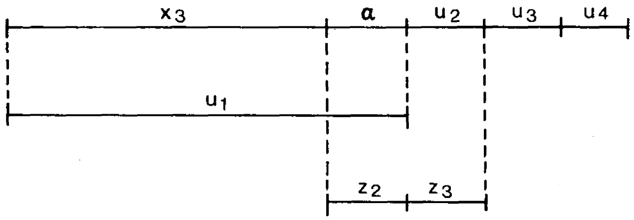
$$\alpha = y_2 y_3 y_4$$

avec $y_i \in X_i^*$ pour tout $i \in \{2; 3; 4\}$. D'ai, par (i) :

$$x_3 = u_1 y_2 y_3 y_4.$$

Ce qui impliquerait par unicité de la décomposition $u_1 = 1$, et donc on aurait une contradiction.

Donc on est nécessairement dans le cas (ii).



Alors αu_2 est à la fois préfixe de X_2 mot de X_2^* et suffixe de $u_1 u_2$, mot de $X_1^* X_2^*$. Par le lemme III.4, αu_2 appartient donc à

$X_2^* X_3^* X_4^* \cap X_1^* X_2^* X_3^* = X_2^* X_3^*$. Donc l'on peut écrire :

$$\alpha u_2 = z_2 z_3$$

avec $z_i \in X_i^*$ pour $i \in \{2; 3\}$. Par (ii), on obtient alors :

$$x_2 = z_2 z_3 u_3 u_4$$

ce qui implique par unicité de la décomposition : $z_3 = u_3 = u_4 = 1$. Donc par (1), l'on a : $w \in X_1^* X_2^*$.

Dans le cas (*b*), on montrerait de même que $w \in X_3^* X_4^*$. Supposons maintenant que l'on soit dans le cas (*c*). Alors par (1), l'on a :

$$w = x_3 x_2 = u_2 u_3. \qquad (2)$$

Alors il existe $\beta \in A^*$ tel que l'on soit dans l'une des deux possibilités suivantes :

(i) $u_2 = x_3 \beta$, $x_2 = \beta u_3$

(ii) $u_2 \beta = x_3$, $\beta x_2 = u_3$

Dans le cas (i), β est préfixe de $x_2 \in X_2^*$ et suffixe de $u_2 \in X_2^*$: par le lemme III.4, il est donc dans $X_2^* X_3^*$. Donc il existe $z_2 \in X_2^*$, $z_3 \in X_3^*$ tels que :

$$\beta = z_2 z_3$$

Par (i), on a donc : $x_2 = z_2 z_3 u_3$.

Par unicité de la décomposition, on obtient donc : $u_3 = z_3 = 1$.

Donc par (2) on a : $x = u_2 \in X_2^*$.

Dans le cas (ii), on montrerait de même que $w \in X_3^*$.

Cela termine donc la preuve de l'assertion 1.

Montrons l'assertion 2.

Soit donc $w \in X_2^* X_1^*$, alors il existe $x_1 \in X_1^*$, $x_2 \in X_2^*$ et $u_i \in X_i^*$ pour tout i, tels que :

$$w = x_2 x_1 = u_1 u_2 u_3 u_4 \qquad (3)$$

Trois cas peuvent donc se produire à nouveau :

(*a*) $u_1 \neq 1$

(*b*) $u_1 = 1$, $u_4 \neq 1$

(*c*) $u_1 = u_4 = 1$.

Traitons le cas (a). Alors il existe α mot de a^* tel que l'on soit dans l'un des deux cas (i) ou (ii) suivant :

(i) $x_2 = u_1 \alpha$, $\alpha x_1 = u_2 u_3 u_4$;

(ii) $x_2 \alpha = u_1$, $x_1 = \alpha u_2 u_3 u_4$.

Le cas (i) ne peut pas se produire car sinon α étant le préfixe d'un mot de $X_2^* X_3^* X_4^*$, qui est préfixiel d'après le lemme III.4, on aurait $\alpha \in X_2^* X_3^* X_4^*$. On peut donc écrire :

$$\alpha = y_2 y_3 y_4$$

avec $y_i \in X_i^*$ pour tout i. Donc on obtient :

$$x_2 = u_1 y_2 y_3 y_4$$

Ce qui impliquerait $u_1 = 1$ par unicité de la décomposition, d'où une contradiction.

Donc on est nécessairement dans le cas (ii). Alors αu_2 est suffixe d'un mot de $X_1^* X_2^*$. Par le lemme III.4, αu_2 appartient à $X_1^* X_2^* X_3^*$, donc on peut écrire :

$$\alpha u_2 = z_1 z_2 z_3$$

avec $z_i \in X_i^*$ pour tout i. D'où on a par (ii) :

$$x_1 = z_1 z_2 z_3 u_3 u_4$$

Par unicité de la décomposition, on a donc : $z_2 = z_3 = u_3 = u_4 = 1$.
Donc par (3), $w \in X_1^* X_2^*$. On montrerait de même dans le cas (b) qu'alors $w \in X_3^* X_4^*$ et pour le cas (c), il est clair que $w \in X_2^* X_3^*$.

Donc 2 est prouvée.

Pour montrer 3, il suffit de voir que si (X_1, X_2, X_3, X_4) est une factorisation de A^*, alors par la proposition III.2 :

$$(X_4^{*\sim}, X_3^{*\sim}, X_2^{*\sim}, X_1^{*\sim})$$

est encore une factorisation monoïdale (donc libre ici) de A^*. Appliquons lui le résultat 2, on obtient :

$$X_3^{*\sim} X_4^{*\sim} \subset X_4^{*\sim} X_3^{*\sim} \cup X_3^{*\sim} X_2^{*\sim} \cup X_2^{*\sim} X_1^{*\sim}$$

et appliquons l'opération $\sim$ à cette inclusion : on obtient alors immédiatement l'assertion 3. ■

2. Le théorème de recollement

On peut donc maintenant énoncer notre résultat principal qui est le théorème de recollement des quadrisections, qui généralise donc le résultat pour les trisections.

THÉORÈME IV.2 : *Soit* (X_1, X_2, X_3, X_4) *une quadrisection de* A^*. *Alors il existe une trisection* (A_1, A_2, A_3) *de* A^*, *une bisection* (U, V) *de* X_2^* *et une bisection* (T, W) *de* X_3^* *telles que :*

(X_1, U) *soit une bisection de* A_1^*, (V, T) *soit une bisection de* A_2^* *et* (W, X_4) *soit une bisection de* A_3^*. *C'est-à-dire :*

$$\underline{A}^*=\underline{X}_1^*\,\underline{X}_2^*\,\underline{X}_3^*\,\underline{X}_4^*=(\underline{X}_1^*\,\underline{U}^*)(\underline{V}^*\,\underline{T}^*)(\underline{W}^*\,\underline{X}_4^*)=\underline{A}_1^*\,\underline{A}_2^*\,\underline{A}_3^*.$$

Remarque : Compte tenu du résultat de Viennot sur le recollement des trisections ([6] ou [1]), on voit que toute quadrisection peut se construire avec des bisections et des recollements.

Preuve : Introduisons :

$$S=\{s\in X_2^*, s X_1^* \subset X_1^* X_2^*\}.$$

Alors l'on a :

LEMME IV.3 : *S est un sous-monoïde de* X_2^* *qui vérifie la condition* $C(1, 0)$ *dans* X_2^*.

Preuve : On a :

$$\forall s, t\in S, \qquad \forall x_1\in X_1^*, \qquad stx_1\in s(X_1^* X_2^*) \subset (X_1^* X_2^*) X_2^*$$

donc $stx_1\in X_1^* X_2^*$. Ainsi $st\in S$ et S est un sous-monoïde de X_2^*.
On veut montrer maintenant que S vérifie la condition $C(1, 0)$ dans X_2^*.
Soient s, $t\in X_2^*$ tels que $st\in S$. Il faut montrer que $t\in S$.
Par définition, l'on a :

$$\forall x_1\in X_1^*, \qquad stx_1\in X_1^* X_2^* \tag{1}$$

Soit donc $x_1\in X_1^*$, alors par le lemme III.4 et (1), on obtient que : $tx_1\in X_1^* X_2^* X_3^*$. Alors par le lemme IV.1, on a donc :

$$tx_1\in X_2^* X_1^* \cap X_1^* X_2^* X_3^* = X_1^* X_2^* \cup X_2^* X_3^* \tag{2}$$

Supposons donc $tx_1\in X_2^* X_3^*$. Alors il existe $y_3\in X_3^*$ et $y_2\in X_2^*$ tels que :

$$tx_1=y_2 y_3. \tag{3}$$

On a donc par (1) et comme $s \in X_2^*$:

$$stx_1 = (sy_2)\, y_3 \in X_1^* X_2^* \cap X_2^* X_3^* = X_2^*.$$

Cela implique par unicité de la décomposition que : $y_3 = 1$. Donc par (3), on a :

$$tx_1 \in X_2^*.$$

Donc par (2), on a bien : $tx_1 \in X_1^* X_2^*$ dans tous les cas.

Ainsi $t \in S$. C'est ce que l'on voulait prouver. ■

Par le lemme IV. 3, on peut donc écrire $S = U^*$ où U est un code (1, 0)-limité dans X_2^*. U est donc le facteur gauche d'une bisection (U, V) de X_2^* avec :

$$V^* = X_2^* \setminus U X_2^* \quad (cf.\ [1]).$$

Posons alors $M = X_1^* U^*$. Alors l'on a :

LEMME IV. 4 : *$M = X_1^* U^*$ est un sous-monoïde de A^*.*

Preuve : Il suffit de montrer que :

$$U^* X_1^* \subset M = X_1^* U^*. \tag{1}$$

Soit $s \in U^*$, $x_1 \in X_1^*$. Par définition de $S = U^*$, il existe $\alpha_1 \in X_1^*$, $\alpha_2 \in X_2^*$ tels que :

$$sx_1 = \alpha_1 \alpha_2. \tag{2}$$

Nous allons montrer que $\alpha_2 \in U^*$, ce qui impliquera (1).

Soit donc $w \in X_1^*$, il faut montrer que l'on a :

$$\alpha_2 w \in X_1^* X_2^*. \tag{3}$$

Comme $s \in S = U^*$ et $x_1 w \in X_1^*$, par (2) et la définition de S, l'on a :

$$sx_1 w = \alpha_1 (\alpha_2 w) \in X_1^* X_2^*. \tag{4}$$

Donc comme $X_1^* X_2^* X_3^*$ est suffixiel par le lemme III. 4, l'on a :

$$\alpha_2 w = y_1 y_2 y_3 \tag{5}$$

avec $y_i \in X_i^*$ pour $i \in \{1;\ 2;\ 3\}$. Cela implique par (4).

$$\alpha_1 \alpha_2 w = \alpha_1 y_1 y_2 y_3 \in X_1^* X_2^*.$$

Par l'unicité factorisation, l'on a : $y_3 = 1$ et par (5), on a donc que (3) est vrai. ■

Posons maintenant :

$$S' = \{s \in X_3^*,\ X_4^* s \subset X_3^* X_4^*\}$$

On a alors :

LEMME IV.5 : *S' est un sous-monoïde de X_3^* qui vérifie la condition $C(0, 1)$ dans X_3^*.*

Preuve : Par la proposition III.2, on sait que $(X_4^{*\sim}, X_3^{*\sim}, X_2^{*\sim}, X_1^{*\sim})$ est une factorisation monoïdale finie (donc libre) de A^*. Appliquons lui le lemme IV.3. On déduit que

$$F = \{s \in X_3^{*\sim},\ s X_4^{*\sim} \subset X_4^{*\sim} X_3^{*\sim}\}$$

est un sous-monoïde de $X_3^{*\sim}$ vérifiant la condition $C(1, 0)$ dans $X_3^{*\sim}$. Il est facile de vérifier que $F^{\sim} = S'$. Donc par la proposition III.3, S' est un sous-monoïde de X_3^* vérifiant la condition $C(0, 1)$. ■

Par le lemme IV.5, on peut donc écrire : $S' = W^*$ où W est un code $(0, 1)$-limité dans X_3^*. C'est donc (*cf.* [1]) le facteur droit d'une bisection (T, W) de X_3^* et l'on a :

$$T^* = X_3^* \setminus X_3^* W.$$

Posons alors $N = W^* X_4^*$. Comme dans le cas précédent, l'on a :

LEMME IV.6 : *$N = W^* X_4^*$ est un sous monoïde de A^*.*

Preuve : Identique à celle du lemme IV.4 ou alors on peut obtenir ce lemme comme conséquence du lemme IV.4 à l'aide de l'opération $\sim$. ■

Posons maintenant

$$R = \{s \in X_2^*,\ s X_1^* \cap X_3^* X_4^* \neq \varnothing\}$$

$$Z = \{s \in X_3^*,\ X_4^* s \cap X_1^* X_2^* \neq \varnothing\}$$

Alors l'on a :

LEMME IV.7 : *On a alors les assertions suivantes :*

(1) $R^* = V^*$;

(2) $Z^* = T^*$;

(3) $ZR \subset Z \cup R$.

Preuve : Montrons d'abord l'assertion 1.

(i) Montrons que $R \subset V^*$.

Soit donc $r \in R$, comme par définition, $r \in X_2^*$ et que (U, V) est une bisection de X_2^*, on peut écrire avec $u \in U^*$ et $v \in V^*$:

$$r = uv. \tag{1}$$

Il suffit donc de montrer que $u = 1$. Supposons, par l'absurde, $u \neq 1$. Par (1) et par définition de R, l'on a :

$$\exists\, x \in X_1^*, \qquad rx = uvx \in X_3^*\, X_4^*. \tag{2}$$

Mais $v \in V^*$, donc $vx \in X_2^*\, X_1^*$, d'où par le lemme IV. 1 on obtient :

$$vx \in X_1^*\, X_2^* \cup X_2^*\, X_3^* \cup X_3^*\, X_4^*. \tag{3}$$

Par (2) et (3), comme $u \in X_2^* \setminus \{1\}$ et par l'unicité de la factorisation, on a aisément :

$$vx \in X_1^*\, X_2^*$$

donc il existe $x_1 \in X_1^*$ et $x_2 \in X_2^*$ tels que :

$$vx = x_1\, x_2. \tag{4}$$

Mais d'autre part, par définition de $S = U^*$, l'on a :

$$ux_1 \in X_1^*\, X_2^*. \tag{5}$$

Donc par (2), (4) et (5), l'on obtient :

$$rx = uvx = (ux_1)\, x_2 \in X_1^*\, X_2^* \cap X_3^*\, X_4^* = \{1\}.$$

Cela contredit donc $u \neq 1$. Ainsi $u = 1$ et par (1), $r \in V^*$.

(ii) Montrons par récurrence sur la longueur, que $V^* \subset R^*$:

Soit $v \in V^*$, si $|v| = 0$, alors $v \in R^*$. Supposons qu'on ait prouvé :

$$\forall\, v \in V^*, \qquad |v| < n \quad \Rightarrow \quad v \in R^*$$

et soit $v \in V^*$ de longueur n.

Comme (U, V) est une factorisation de X_2^*, l'on a $v \notin U^*$. Donc il existe $\alpha_1 \in X_1^*$ tel que : $v\,\alpha_1 \notin X_1^*\, X_2^*$.

Cela implique par le lemme IV. 1, comme $v\,\alpha_1 \in X_2^*\, X_1^*$, que :

$$v\,\alpha_1 \in (X_2^*\, X_3^* \setminus X_2^*) \cup X_3^*\, X_4^*. \tag{6}$$

Si $v\alpha_1 \in X_3^* X_4^*$, alors $v \in R$ par définition et c'est terminé. Sinon par (6), l'on a :

$$\exists x_2 \in X_2^*, \qquad \exists x_3 \in X_3^* \setminus \{1\}, \qquad v\alpha_1 = x_2 x_3. \tag{7}$$

Par (7), il existe $\alpha \in A^*$ tel que l'on soit dans l'un des deux cas :

(a) $\alpha_1 = \alpha x_3$ et $v\alpha = x_2$;

(b) $x_3 = \alpha\alpha_1$ et $v = x_2 \alpha$.

Le cas (a) ne peut se réaliser car sinon, α étant un suffixe de $x_2 \in X_2^*$, par le lemme III.4, on aurait $\alpha \in X_1^* X_2^* X_3^*$. On pourrait donc écrire :

$$\alpha = y_1 y_2 y_3 \qquad \text{avec} \quad y_i \in X_i^* \quad \text{pour } i \in \{1;\ 2;\ 3\}.$$

Donc par (a), on aurait :

$$\alpha_1 = y_1 y_2 y_3 x_3. \tag{8}$$

De (8), on tire, par unicité de la factorisation, que $x_3 = 1$, ce qui est en contradiction avec (7).

Donc on est dans le cas (b). Par (b), α est un préfixe de $x_3 \in X_3^*$, donc par le lemme III.4, l'on a :

$$\forall i \in \{2;\ 3;\ 4\}, \qquad \exists \delta_i \in X_i^*, \qquad \alpha = \delta_2 \delta_3 \delta_4. \tag{9}$$

Par (b) et par (9), on a donc :

$$v = x_2 \alpha = x_2 \delta_2 \delta_3 \delta_4 \in X_2^*.$$

Par unicité de la factorisation, on obtient $\delta_3 = \delta_4 = 1$. Donc par (9), on a $\alpha \in X_2^*$ et par (b), on a :

$$\alpha\alpha_1 = x_3 \in X_3^* \cap \alpha X_1^*.$$

Par définition de R, on a donc : $\alpha \in R$.

Par (b), on a aussi : $x_2 \alpha = v \in V^*$.

Comme V est (0, 1)-limité dans X_2^* [(U, V) est une bisection de X_2^*] cette équation implique que : $x_2 \in V^*$.

Or $|x_2| < |v|$ car $\alpha \neq 1$ [sinon dans (b), on aurait $\alpha_1 = x_3 \in X_3^* \cap X_1^* = \{1\}$, en contradiction avec (7)]. Par hypothèse de récurrence, on a donc :

$$x_2 \in R^*.$$

Alors par (b), comme $\alpha \in R$ et $x_2 \in R^*$, on obtient bien :

$$v = x_2 \alpha \in R^*.$$

Cela prouve donc bien que $V^* \subset R^*$ et termine la preuve de l'assertion 1.

L'assertion 2 s'obtient facilement à partir de l'assertion 1 en utilisant l'opération $\sim$ (on applique (1) à la factorisation $(X_4^{*\sim}, X_3^{*\sim}, X_2^{*\sim}, X_1^{*\sim})$).

Il reste donc à montrer l'assertion 3.

Soient donc $z \in Z$ et $r \in R$. Par définition de R et Z l'on a : $zr \in X_3^* X_2^*$ et d'après le lemme IV. 1, on a donc deux cas :

(*a*) $zr \in X_1^* X_2^*$;

(*b*) $zr \in X_3^* X_4^*$.

Supposons que (*a*) soit vérifié, alors :

$$\exists x_1 \in X_1^*, \qquad \exists x_2 \in X_2^*, \qquad zr = x_1 x_2. \tag{10}$$

Par définition de R, il existe $\alpha_1 \in X_1^*$ tel que :

$$r \alpha_1 \in X_3^* X_4^*.$$

Comme $z \in Z \subset X_3^*$, on a donc :

$$zr \alpha_1 \in X_3^* X_4^*. \tag{11}$$

Par le lemme III. 4, cela implique :

$$zr \in X_2^* X_3^* X_4^*.$$

Par (10), cela implique que $zr \in X_2^*$. De plus par (11), il existe $\alpha_1 \in X_1^*$ tel que $(zr) \alpha_1 \in X_3^* X_4^*$.

Cela signifie donc que $zr \in R$.

On montrerait de même que si on était dans le cas (*b*), alors $zr \in Z$. ■

Posons alors $P = V^* T^*$.

COROLLAIRE IV. 8 : *$P = V^* T^*$ est un sous-monoïde de A^*.*

Preuve : C'est immédiat car par le lemme IV. 7, on peut écrire $P = R^* Z^*$ et comme par ce même lemme, on a $ZR \subset R \cup Z$, on en déduit que :

$$Z^* R^* \subset P. \ \blacksquare$$

On peut maintenant terminer la preuve de théorème. En termes de séries caractéristiques dans $\mathbb{N} \langle A^* \rangle$, on peut écrire :

$$\begin{aligned} \underline{A}^* &= \underline{X}_1^* (\underline{U}^* \underline{V}^*)(\underline{T}^* \underline{W}^*) \underline{X}_4^* \\ &= (\underline{X}_1^* \underline{U}^*)(\underline{V}^* \underline{T}^*)(\underline{W}^* \underline{X}_4^*) \\ &= \underline{M}\, \underline{P}\, \underline{N}. \end{aligned}$$

La dernière égalité vient du fait que les produits $X_1^* U^*$, $V^* T^*$ et $W^* X_4^*$ sont non ambigüs puisque $U^* \subset X_2^*$, $V^* \subset X_2^*$, $T^* \subset X_3^*$ et $W^* \subset X_3^*$.

Ainsi (M, P, N) est une factorisation monoïdale de A^* à 3 facteurs. Compte tenu des résultats de la partie III, elle est libre. Autrement dit M, N et P sont des sous-monoïdes libres de base A_1, A_2 et A_3 respectivement. Cela termine la preuve du théorème. ■

Remarque : Nous voyons donc que la méthode que nous avons utilisée conduit finalement à l'utilisation des résultats de la partie III sur les factorisations monoïdales finies libres. Même si cette méthode était généralisable, compte-tenu de ce que nous savons sur les factorisations monoïdales finies du point de vue de leur liberté, nous ne pourrions donc de toute façon pas dépasser le cas du recollement des pentasections.

Notons également qu'on peut se demander, compte tenu des résultats de cette partie, si le cadre adéquat pour démontrer des résultats de recollement n'est pas en fait celui des factorisations monoïdales finies au lieu de celui des factorisations finies usuelles.

BIBLIOGRAPHIE

1. Berstel-Perrin, *Theory of Codes*, Academic Press, 1985.
2. Berstel-Perrin, *Codes Circulaires*, Combinatorics on Words, Progress and Perspectives, Academic Press, 1984.
3. Lothaire, *Combinatorics on Words*, Addison-Wesley, 1983.
4. Schutzenberger, *Sur une propriété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de mathématiques appliquées*, Séminaire Dubreuil-Pisot, année 58-59, I.H.P., Paris, 1959.
5. Schutzenberger, *On a Factorisation of Free Monoids*, Proc. Amer. Math. Soc., vol. 16, 1965, p. 21-24.
6. Viennot, *Algèbres de Lie libres et monoïdes libres*, Thèse d'état, Paris-VII, 1974.
7. Viennot, *Algèbres de Lie libres et monoïdes libres*, Lecture Notes in Math., n° 691, Springer-Verlag, 1978.