INFORMATIQUE THÉORIQUE ET APPLICATIONS

MIREILLE CLERBOUT

Compositions de fonctions de commutation partielle

Informatique théorique et applications, tome 23, n° 4 (1989), p. 395-424

<http://www.numdam.org/item?id=ITA_1989__23_4_395_0>

© AFCET, 1989, tous droits réservés.

L'accès aux archives de la revue « Informatique théorique et applications » 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/

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 23, n° 4, 1989, p. 395 à 424)

COMPOSITIONS DE FONCTIONS DE COMMUTATION PARTIELLE (*)

par Mireille CLERBOUT (1)

Communiqué par J.-E. PIN

Résumé. – *Nous étudions les fonctions obtenues en composant des fonctions de commutation partielle. Nous donnons des règles de « réduction » et d'« amélioration » de ces fonctions pour aboutir à la définition d'une forme normale. Nous explicitons toutes les fonctions possibles que l'on obtient sur un alphabet de quatre lettres.*

Abstract. – *We study functions which are defined by composition of partial commutation functions. We give "reduction" rules and "improvement" rules for these functions in order to establish a normal form. We list every function which can be constructed on an alphabet of four letters.*

INTRODUCTION

Pour modéliser les comportements de processus exécutés en parallèle, ou encore pour représenter les différents accès possibles à une information dans une base de données, on utilise de plus en plus les commutations partielles. Dans le premier cas, les lettres de l'alphabet représentent les actions à exécuter (les processus), et certaines d'entre elles, étant indépendantes, peuvent « commuter » (être exécutées dans un ordre quelconque, ou en parallèle); dans le deuxième cas, une lettre représente une fonction d'accès et un mot la composition de ces fonctions.

D'où l'intérêt d'étudier en profondeur le monoïde partiellement commutatif et les commutations partielles. Ceci explique pourquoi un grand nombre

(*) Reçu juillet 1987, version finale juillet 1988.
Ce travail est en partie supporté par le PRC Mathématiques et Informatique du Ministère de la Recherche et de la Technologie.
(1) C.N.R.S.-U.A. n° 369, L.I.F.L., Université de Lille-Flandres-Artois, 59655 Villeneuve-d'Ascq Cedex.

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-3754 89/04 395 30/$5.00/© Gauthier-Villars

d'articles ont été, ces dernières années, consacrés à cette étude ([2], [3], [5], [6], [8], [9], [10], [11], [13]).

On pourra trouver un « survey » des principaux résultats dans [1] et [12].

Dans ce papier, nous étudions la composition de fonctions de commutation partielle, définies à partir de relations de commutation: à un mot, ou à un langage, on applique successivement plusieurs fonctions de commutation.

En nous attachant à des fonctions d'un type particulier (les fonctions de commutation partitionnée), nous donnons des critères permettant de réduire le nombre de fonctions qui sont composées, et nous définissons une forme normale de composée de fonctions. Nous démontrons ainsi son unicité sur un alphabet de quatre lettres, et nous donnons une condition nécessaire et suffisante pour qu'une fonction qui est la composée de deux fonctions de commutation partitionnée soit sous forme normale.

PRÉLIMINAIRES

Soit X un alphabet.

Une *relation de commutation partielle* sur X est une relation antirefléxive et symétrique.

Une *relation de commutation partitionnée* sur X est associée à une partition de X: $\Pi = \{X_1, X_2, \ldots, X_k\}$. Elle est alors définie par: (x, y) est dans $\bar{\Theta}$ (le complémentaire de Θ) si et seulement si il existe un élément X_i de la partition Π qui contient à la fois x et y.

De manière équivalente, on peut définir une relation de commutation partitionnée comme le complémentaire d'une relation d'équivalence sur X. Les éléments de la partition correspondent alors aux classes d'équivalence.

Pour deux mots w et w' de X^*, on dit que w *se dérive directement en* w' par Θ, et on note $w \Rightarrow_\Theta w'$ si il existe une décomposition $w = uabv$, $w' = ubav$ avec (a, b) dans Θ. La propriété « x *se dérive en* » est alors la clôture reflexive et transitive de « se dérive directement en », et on notera $w \Rightarrow_\Theta^* w'$. Si Y est un sous-ensemble de X, la projection de X sur Y qu'on notera $\Pi(X, Y)$ est la substitution définie sur X par $\Pi(X, Y)(x) = \{x\}$ si $x \in Y$, $\Pi(X, Y)(x) = \{\varepsilon\}$ sinon. Quand aucune ambiguité n'existe au niveau de l'alphabet de définition X, on notera plus simplement Π_Y la projection de X sur Y.

A une relation de commutation Θ, on associe une fonction de commutation f_Θ définie sur X^* par:

$$\forall w \in X^*, \quad f_\Theta(w) = \{w' \in X^* / w \Rightarrow_\Theta^* w'\},$$

cette définition s'étend à un langage:

$$\forall L \subset X^*, \quad f_\Theta(L) = U_{w \in L} f_\Theta(w).$$

Pour une relation de commutation partitionnée Θ, cette définition devient plus simplement:

$$f_\Theta(w) = \Pi_{x1}(w) \sqcup \Pi_{x2}(w) \sqcup \ldots \sqcup \Pi_{xk}(w),$$

en d'autres termes, $f_\Theta(w)$ est le shuffle des k projections de w sur les k éléments de la partition.

Le monoïde commutatif est isomorphe à $X_1^* \times X_2^* \times \ldots \times X_p^*$.

Le résultat suivant est important, car il permet de résoudre simplement de nombreux problèmes.

LEMME DE PROJECTION ([4], [7]). — *Soient u et v deux mots de X^+ et Θ une relation de commutation partielle sur X. Sont équivalentes les deux propriétés suivantes*:

(1) $v \in f_\Theta(u)$.

(2) $\forall (a, b) \in \bar{\Theta}$, $\Pi_{\{a,b\}}(u) = \Pi_{\{a,b\}}(v)$.

Il est clair qu'une fonction de commutation partielle f_Θ n'est une transduction rationnelle que si Θ est vide ($f_\Theta = \mathrm{Id}$). En effet, si Θ n'est pas vide, il existe deux lettres a et b qui commutent, et alors

$$f_\Theta((ab)^*) = U_{n \geqq 0} f_\Theta((ab)^n) = D_1^*$$

(le langage de Dyck): l'image d'un rationnel par f_Θ n'est pas rationnel.

Par contre le lemme de projection permet d'établir que:

PROPOSITION 1 : *L'application τ définie sur X^* par $\tau(u) = \{ v \in X^* / v \notin f_\Theta(u) \}$ est toujours une transduction rationnelle.*

En effet $\tau(u) = \bigcup_{(a,b) \in \Theta} \{ v \in X^* / \Pi_{\{a,b\}}(v) \neq \Pi_{\{a,b\}}(u) \}$

D'autre part, pour une relation Θ sur X donnée, et deux mots u et v de X^*, il est facile de décider si v est dans $f_\Theta(u)$.

D'après le lemme de projection, il suffit de contrôler l'égalité des projections de u et de v sur tous les couples (a, b) de $\bar{\Theta}$.

Mais le problème devient plus complexe quand on cherche à composer des fonctions de commutation: pour k fonctions de commutation données: f_1, $f_2 \ldots f_k$ et deux mots u et v, comment décider si v est dans $f_1 \ldots f_2 \ldots f_k(u)$ [on applique à u f_1, puis f_2 à chaque mot de $f_1(u)$, etc.]. Cette propriété est évidemment décidable: il suffit de trouver une suite de mots w_1, $w_2 \ldots w_k$

vérifiant:

$$w_1 = u, \qquad w_i \in f_i(w_{i-1}), \qquad \forall 2 \leqq i \leqq k \quad \text{et} \quad w_k = v.$$

Il n'y a qu'un nombre fini de mots à tester, mais cela risque d'être long et coûteux.

De même, peut-on décider si la composition de k fonctions de commutation permet d'obtenir la commutation totale, ou comment trouver une suite plus «courte» de p fonctions ($p<k$) vérifiant $f_1 . f_2 . . . f_k = g_1 . g_2 . . . g_p$.

Nous allons dans ce papier donner des règles de simplification de la composée de fonctions de commutation et définir une forme normale, en nous restreignant toutefois au cas des fonctions de commutation partitionnée.

On sait déjà qu'il ne sera pas toujours possible de réduire la composée de k fonctions, grâce au résultat suivant: [4]:

PROPOSITION 2 : *Si*

$$P^k(\mathrm{RAT}) = \{ g_1 . . . g_2 . . . g_k(R)/R \in \mathrm{RAT}, \forall 1 \leqq i \leqq k, g_i$$

est une fonction de commutation partitionnée $\}$,

$$\forall k \geqq 0, \quad P^k(\mathrm{RAT}) \subset P^{k+1}(\mathrm{RAT}) \subset H_{s\alpha} \circ H^{-1}(P(\mathrm{RAT}))$$

où

$$H_{s\alpha} \circ H^{-1}(P(\mathrm{RAT})) = \{ \mathrm{hog}^{-1}(L)/L \in P(\mathrm{RAT}),$$

g est un homomorphisme, h est un homomorphisme strictement alphabétique $\}$.

C'est-à-dire, on peut construire un langage rationnel R et $k+1$ fonctions de commutation partitionnée qui successivement appliquées aux mots de R permettent d'obtenir un langage qu'on ne peut pas décrire comme le résultat de la composition de k fonctions de commutation partitionnée sur un langage rationnel quelconque.

Le rationnel R construit dans la preuve de ce résultat est défini sur un alphabet dont le cardinal dépend de k. Mais, en fixant la taille de l'alphabet, a-t-on encore une hiérarchie infinie? Nous allons voir très vite que la réponse est négative.

Pour cela, nous donnons, dans la première partie, des règles d'effacement: les fonctions apparaissant dans la composée d'une fonction peuvent être supprimées sans changer la fonction; ces règles nous permettront d'établir que, sur un alphabet fixé, le nombre de fonctions qu'on peut définir est fini; dans la deuxième partie nous énonçons des règles de réduction: une fonction

peut parfois être redéfinie comme la composée de fonctions de commutation partitionnée, mais en plus petit nombre. La quatrième partie contient des règles d'amélioration: les fonctions apparaissant dans la composée sont remplacées par des fonctions plus grandes au sens où $f \geqq g$ si $\forall w \in X^*$, $f(w) \supset g(w)$. Cela nous permet, dans le chapitre 5, de définir une forme normale: la composée de fonctions est sous forme normale si on ne peut ni la réduire ni l'améliorer. Nous montrons qu'une fonction composée de deux fonctions a une forme normale unique, et nous donnons une condition nécessaire et suffisante pour décider si la composée de deux fonctions de commutation est sous forme normale.

Enfin, dans la dernière partie, nous étudions les composées de fonctions définies sur un alphabet de quatre lettres: ces fonctions se réduisent toutes à la composée de deux fonctions au maximum.

I Le monoïde engendré par les fonctions de commutation partielle sur l'alphabet X

Si X est un alphabet fixé, notons Z l'ensemble des relations de commutation partitionnée définies sur X et Z^* le monoïde libre engendré par Z.

A z de Z, correspond la fonction de commutation f_z, à $z_1 z_2 \ldots z_k$ de Z^* correspond le produit $f_{z_1} . f_{z_2} \ldots f_{z_k}$: à un mot w de X^*, on applique f_{z_1}, puis à chaque mot de $f_{z_1}(w)$, on applique f_{z_2}, etc.

Exemple: Soient

$$X = \{a, b, c\}, \qquad z_1 = \{\{a\}, \{b, c\}\}, \qquad z_2 = \{\{b\}, \{a, c\}\},$$

$$f_{z_1} f_{z_2}((abc)^n) = \bigcup_{w \in L} f_{z_2}(w) \qquad \text{avec} \quad L = a^n \sqcup (bc)^n = f_{z_1}((abc)^n)$$

il est facile de voir qu'ici, $f_{z_1} . f_{z_2}((abc)^n) = a^n \sqcup b^n \sqcup c^n$.

On peut définir sur Z^* une relation d'ordre partiel:

- si $z_1, z_2 \in Z$, $z_1 \leqq z_2 \Leftrightarrow \forall w \in X^*$, $f_{z_1}(w) \subseteq f_{z_2}(w)$;
- si $u_1 = z_1 z_2 \ldots z_k$ et $u_2 = t_1 . t_2 \ldots t_p$ sont deux mots de Z^*,

$u_1 \leqq u_2 \Leftrightarrow \forall w \in X^*$, $f_{z_1} . f_{z_2} \ldots f_{z_k}(w) \subseteq f_{t_1} . f_{t_2} \ldots f_{tp}(w)$. Il est clair que cette relation est compatible avec le produit:

- si $u, u_1, u_2 \in Z^*$;
- si $u_1 \leqq u_2 \Leftrightarrow$

$u_1 u \leqq u_2 u$; on en déduit une congruence sur Z^*:

Soient: $u_1 = z_1 z_2 \ldots z_k$ et $u_2 = t_1 t_2 \ldots t_p$ deux mots de Z^*,

$$u_1 \equiv u_2 \Leftrightarrow u_1 \leqq u_2 \quad \text{et} \quad u_2 \leqq u_1 \Leftrightarrow f_{z_1} f_{z_2} \ldots f_{zk} = f_{t_1} f_{t_2} \ldots f_{tp}.$$

Enfin, la relation $\leqq$ confère à Z une structure de treillis. Le plus petit élément, noté 0, correspond à la relation où rien ne commute (c'est la partition $\{X\}$), et le plus grand élément, noté 1, est associé à la commutation totale (c'est la partition $\{\{x\}, x \in X\}$). Pour deux éléments de Z, z_1 et z_2, on notera $z_1 \vee z_2$ le plus petit majorant de $\{z_1, z_2\}$ (union des relations) et $z_1 \wedge z_2$ le plus grand minorant de $\{z_1, z_2\}$ (intersection des relations).

Exemple: Soit $X = \{a, b, c, d\}$.

En notant plus simplement (a, b, c, d) la partition $\{\{a\}, \{b\}, \{c\}, \{d\}\}$ ou (ab, cd) la partition $\{\{a, b\}, \{c, d\}\}$, on a:

$$Z = \{(a, b, c, d), (abcd)\}$$
$$U\{(x, y, zt), \{x, y, z, t\} = X\}$$
$$U\{(xy, zt), \{x, y, z, t\} = X\}$$
$$U\{(x, yzt), \{x, y, z, t\} = X\}$$
$$\forall z \in Z, \quad z \leqq (a, b, c, d) (= 1)$$

$(ab, cd) \leqq (a, b, cd)$ (les a et b peuvent commuter dans un cas et pas dans l'autre).

On a alors

$$(ab, cd) \vee (a, b, cd) = (a, b, cd)$$

et

$$(ab, cd)(a, b, cd) \equiv (a, b, cd).$$

Par contre, (ab, cd) (ac, bd) n'est pas équivalent à un mot de Z^* plus court. Si c'était le cas, on aurait forcément (ab, cd) $(ac, bd) \equiv 1$ car, chaque lettre peut commuter à un moment ou à un autre avec toutes les autres.

Or, (ab, cd) (ac, bd) n'est pas la commutation totale car, à partir du mot $w = abcd$, on ne peut pas obtenir $w' = cabd$: si c'était le cas, on pourrait trouver un mot x de X^* vérifiant:

$$x \in f_{(ab, cd)}(w) \quad \text{donc} \quad \Pi_{ab}(x) = \Pi_{ab}(w) = ab \quad \text{et} \quad \Pi_{cd}(x) = \Pi_{cd}(w) = dc$$

$x \in f_{(ac,\, bd)}(w')$ [ce qui est la même chose que $w' \in f_{(ac,\, bd)}(x)$] donc

$$\Pi_{ac}(x) = \Pi_{ac}(w') = ca \qquad \text{et} \qquad \Pi_{bd}(x) = \Pi_{bd}(w') = bd.$$

Il est alors clair qu'on ne peut pas reconstruire le mot x (le graphe d'ordonnancement des lettres conduit à un cycle).

Nous allons maintenant énoncer quelques propriétés élémentaires de simplification de mots de Z^*, qui sont en fait des règles d'effacement, puisqu'elles permettent de supprimer des lettres d'un mot de Z^*. Dans la suite du papier, nous noterons z ou z_i les lettres de Z, u ou v les mots de Z^*, x ou x_i les lettres de X et w ou w_i les mots de X^*.

Règle E 0:

(1) $\forall z \in Z,\ zz \equiv z.$

(2) $\forall z_1, z_2 \in Z,\ z_1 \leqq z_2 \Rightarrow z_1 z_2 \equiv z_2 z_1 \equiv z_2.$

Preuve: (1) En notant f_z la fonction de commutation associée à z, nous avons de manière évidente:

$$\forall w \in X^*, \quad f_z(w) = \{ w' \in X^*,\ w \Rightarrow^* w' \} = f_z . f_z(w) = \{ w' \in X^*,\ w \Rightarrow_z^* w_1 \Rightarrow_z^* w' \}.$$

(2) $0 \leqq z_1 \leqq z_1 z_2$ implique $z_2 \leqq z_1 z_2 \leqq z_2 z_2 \equiv z_2$ donc $z_1 z_2 \equiv z_2$.

De même, on a $z_2 \leqq z_2\ z_1 \leqq z_2\ z_2$ donc $z_2 z_1 \equiv z_2$.

Nous pouvons alors énoncer la règle suivante, permettant de «réduire» des mots de z et de conclure que $Z^*/\equiv$ est fini:

Règle E 1: Soient $z \in Z$ et $u, v \in Z^*$. On a $zuzvz \equiv zuvz$,

Preuve: Nous allons nous placer dans le cas où z est une partition de deux éléments de l'alphabet X: $z = \{ Y, \bar{Y} \}$. La démonstration serait tout à fait identique pour une partition quelconque.

Notons f_u et f_v les fonctions associées à u et v (ce sont en fait des composées de fonctions de commutation partitionnée) et f_z la fonction associée à z.

$\forall w \in X^*$, $\forall w' \in f_z f_u f_z f_v f_z(w)$, il existe des mots w_1, w_2, w_3, w_4 de X^* vérifiant:

$$w \ \Rightarrow_z^* \ w_1 \ \rightarrow_u \ w \ \Rightarrow_z^* \ w_3 \ \rightarrow_v \ w_4 \ \Rightarrow_z \ w'$$

$w \Rightarrow_z^* w_1$ est équivalent à

$$w \ \Rightarrow_z^* \ x_1 x_2 \ \Rightarrow_z^* w_1 \qquad \text{avec} \quad x_1 \in Y^*, \quad x_2 \in \bar{Y}^*$$

de même $w_4 \Rightarrow_z^* w'$ est équivalent à

$$w_4 \quad \Rightarrow_z^* \quad y_1 y_2 \quad \Rightarrow_z^* \quad w' \qquad \text{avec} \quad y_1 \in Y^*, \quad y_2 \in \bar{Y}^*$$

donc $y_1 y_2 \in f_z f_u f_z f_v f_z (x_1 x_2)$
on en déduit que:

$$\Pi_Y (y_1 y_2) = y_1 \in f_z f_u f_z f_v f_z (\Pi_Y (x_1 x_2))$$
$$= f_z f_u f_z f_v f_z (x_1) = y_1$$

et

$$y_2 \in f_z f_u f_z f_v f_z (x_2).$$

Mais, pour obtenir y_1 (resp. y_2) à partir de x_1 (resp. x_2), aucune commutation relative à z ne sera utilisée puisque $x_1 \in Y^*$ et $x_2 \in \bar{Y}^*$. Donc

$$y_1 \in f_u f_v (x_1) \qquad \text{et} \qquad y_2 \in f_u f_v (x_2),$$

donc $y_1 y_2 \in f_u f_v (x_1 x_2)$ et on en conclut que $w' \in f_z f_u f_v f_z (w)$, ainsi $zuzvz \leqq zuvz$.

L'inégalité inverse étant évidente, on a le résultat.

Un mot de Z^* est ainsi toujours équivalent à un mot qui ne contient pas plus de deux occurences de la même lettre. On a donc:

PROPOSITION 3 : $Z^*/\equiv$ *est fini.*

Mais peut-on décider de l'équivalence de deux mots? Pour cela, on voudrait pouvoir obtenir une forme normale dans Z^*: un mot serait toujours équivalent à un unique mot qui aurait de bonnes propriétés (celle d'être le plus petit, par exemple). Pour cela, il faut se donner des règles pour réduire la longueur des mots d'une part, et d'autre part, essayer de trouver des critères simples permettant de dire si un mot est sous forme normale ou pas. Nous allons tout de suite énoncer quelques règles permettant de réduire la longueur d'un mot de Z^*.

II. Mots irréductibles dans Z^*

DÉFINITION : Un mot z de Z^* est irréductible si il n'existe pas de mot z' plus court: $|z| > |z'|$ tel que $z \equiv z'$ (sinon il sera réductible).

Les premières règles que nous allons énoncer ont rapport à la présence dans un mot z de lettres identiques ou comparables.

Règle R 2: Soient z, z_1, z_2, ..., z_k, $k+1$ lettres de Z.

Alors, $z z_1 z_2 \ldots z_k z \equiv (z \vee z_1)(z \vee z_2) \ldots (z \vee z_k)$.

Exemple: Soit $X = \{a, b, c, d, e, f, g, h\}$ et

$$z_1 = (abcd, efgh), \qquad z_2 = (abef, cdgh), \qquad z_3 = (aceg, bdfh).$$

Alors,

$$\begin{aligned} z_1 z_2 z_3 z_2 z_1 &\equiv (z_1 \vee z_2)(z_1 \vee z_3)(z_1 \vee z_2) \\ &\equiv (z_1 \vee z_2 \vee z_3) = 1 \end{aligned}$$

avec

$$z_1 \vee z_2 = (ab, cd, ef, gh)$$

et

$$z_1 \vee z_3 = (ac, eg, bd, fh)$$

Preuve: Comme précédemment, nous allons démontrer le résultat dans le cas où les z_i sont des partitions à deux éléments. L'extension au cas quelconque se fait sans difficulté.

Le raisonnement est basé sur une récurrence sur k.

Posons

$$z = (Y, \bar{Y}) \qquad \text{et} \qquad z_1 = (X_1, \bar{X}_1).$$

Nous allons montrer que

$$z z_1 z \equiv (z \vee z_1) \qquad \text{où} \quad z \vee z_1 = (Y \cap X_1, Y \cap \bar{X}_1, \bar{Y} \cap X_1, \bar{Y} \cap \bar{X}_1).$$

Tout d'abord, on a de manière évidente

$$z z_1 z \leqq (z \vee z_1)(z \leqq z \vee z_1 \qquad \text{et} \qquad z_1 \leqq z \vee z_1).$$

Montrons que $z \vee z_1 \leqq z z_1 z$, c'est-à-dire que $\forall w \in X^*$, $f_{z \vee z_1}(w) \subseteq f_z f_{z_1} f_z(w)$:

$\forall w \in X^*$, $\forall w' \in f_{z \vee z_1}(w)$, il existe une dérivation $w \Rightarrow^*_{z \vee z_1} w'$. Si cette dérivation est de longueur nulle, alors $w' \in f_z f_{z_1} f_z(w)$.

Supposons alors le résultat vrai pour une dérivation de longueur inférieure ou égale à l.

Si $w \Rightarrow^{l+1}_{z \vee z_1} w'$, on peut écrire $w \Rightarrow^1_{z \vee z_1} w_1 \Rightarrow^l_{z \vee z_1} w'$.

$w \Rightarrow^1_{z \vee z_1} w_i$ implique $w \Rightarrow^1_z w_1$ ou $w \Rightarrow^1_{z_1} w_1$ implique $w_1 \in f_z f_{z_1} f_z(w)$

$w_1 \Rightarrow^l_{z \vee z_1} w'$ implique $w' \in f_z f_{z_1} f_z(w_1)$ par hypothèse de récurrence

donc

$$w' \in f_z f_{z_1} f_z f_z f_{z_1} f_z(w) \qquad \text{et} \qquad z \vee z_1 \leqq z z_1 z z z_1 z$$

comme $zz \equiv z$, on a

$$z \vee z_1 \leqq z z_1 z z_1 z \equiv z z_1 z$$

d'après la règle E 1.

Supposons maintenant que

$$\forall \alpha \leqq k, \quad z z_1 z_2 \ldots z_\alpha z \equiv (z \vee z_1) \ldots (z \vee z_\alpha)$$

alors,

$$\begin{aligned} z z_1 z_2 \ldots z_{k+1} z &\equiv z z_1 z_2 \ldots z_k z z z_{k+1} z \,(\text{règles E 1 et E 0}) \\ &\equiv (z \vee z_1)(z \vee z_2) \ldots (z \vee z_k)(z \vee z_{k+1}) \end{aligned}$$

d'après l'hypothèse de récurrence.

La règle R 3 est un corollaire de la règle R 2:

Règle R 3: Soient z, z', z_1, $z_2 \ldots z_k$ des éléments de Z.

Si $z \leqq z'$, $z z_1 z_2 \ldots z_k z' \equiv (z_1 \vee z) \ldots (z_k \vee z) z'$.

Preuve:

$$\begin{aligned} z z_1 z_2 \ldots z_k z' &\equiv z z_1 z_2 \ldots z_k z z' \quad (\text{règle E 0}) \\ &\equiv (z_1 \vee z)(z_2 \vee z) \ldots (z_k \vee z) z' \quad (\text{règle R 2}) \end{aligned}$$

Un exemple: Soient $X = \{a, b, c, d, e, f, g\}$ et

$$z_1 = (ab, cd, efg), \qquad z_2 = (bc, de, fga), \qquad z_3 = (ac, bd, efg),$$
$$z_4 = (bc, def, ga)$$

alors, on a

$$z = (z_2 \vee z_4) = (bc, defga) \leqq z_2 \qquad \text{et} \qquad \leqq z_4$$

et

$$\begin{aligned} u = z_1 z_2 z_3 z_4 &\equiv z_1 z_2 z_3 z z_4 \\ &\equiv z_1 z_2 (z_3 \vee z) z_4 \quad (\text{règle R 3 et } z_2 \vee z \equiv z_2) \end{aligned}$$

avec

$$z_3 \vee z = (a, b, c, d, efg) = z'_3$$

donc

$$u \equiv z_1 z_2 z'_3 z_4$$

et $z_1 \leqq z'_3$ donc

$$u \equiv z'_2 z'_3 z_4 \qquad \text{avec} \quad z'_2 = (z_1 \vee z_2) = (a, b, c, d, e, fg)\, 3$$

Comme

$$z'_2 \geqq z'_3, \qquad u \equiv z'_2 z_4 = (a, b, c, d, e, fg)\,(bc, def, ga).$$

En fait, $u \equiv 1$.

Pour arriver à cette conclusion, il nous faut des règles de réduction liées à la valeur même des partitions. C'est ce type de règles que nous allons énoncer maintenant.

Règle R 4: Si

$$z_1 = (X_1, X_2, X_3 \cup X_4, X_5, \ldots, X_k)$$

et

$$z_2 = (X_1 \cup X_2, X_3, X_4, X_5, \ldots, X_k),$$

alors

$$z_1 z_2 \equiv z_2 z_1 \equiv z = (X_1, X_2, X_3, X_4, X_5, \ldots, X_k).$$

Preuve: $z_1 \leqq z$ et $z_2 \leqq z$ donc $z_1 z_2 \leqq z$, de même $z_2 z_1 \leqq z$.

Montrons la relation inverse: $z \leqq z_1 z_2$.

$$\forall w \in X^*, \quad \forall w' \in f_z(w), \quad \forall i \in \{1, k\}, \qquad \Pi_{X_i}(w) = \Pi_{X_i}(w')$$

Alors,

$$w \Rightarrow^*_{z_1} \Pi_{X_1}(w)\, \Pi_{X_2}(w)\, \Pi_{X_3 \cup X_4}(w)\, \Pi_{X_5}(w) \ldots \Pi_{X_k}(w)$$
$$\Rightarrow^*_{z_1} \Pi_{X_1 \cup X_2}(w')\, \Pi_{X_3 \cup X_4}(w)\, \Pi_{X_5}(w') \ldots \Pi_{X_k}(w')$$

car

$$\Pi_{X_1 \cup X_2}(w') \in \Pi_{X_1}(w) \sqcup \Pi_{X_2}(w) \qquad \text{et} \qquad \forall i \geqq 5, \quad \Pi_{X_i}(w) = \Pi_{X_i}(w')$$
$$\Rightarrow^*_{z_2} \Pi_{X_1 \cup X_2}(w') \Pi_{X_3}(w) \Pi_{X_4}(w) \Pi_{X_5}(w') \ldots \Pi_{X_k}(w')$$
$$= \Pi_{X_1 \cup X_2}(w') \Pi_{X_3}(w') \Pi_{X_4}(w') \ldots \Pi_{X_k}(w')$$

soit w_1 ce mot:

$$w_1 \in f_{z_1} . f_{z_2}(w)$$

et

$$f_{z_2}(w_1) = \Pi_{X_1 \cup X_2}(w_1) \sqcup \Pi_{X_3}(w_1) \ldots \sqcup \Pi_{X_k}(w_1)$$
$$= \Pi_{X_1 \cup X_2}(w') \sqcup \Pi_{X_3}(w') \ldots \sqcup \Pi_{X_k}(w')$$

donc

$$w' \in f_{z_2}(w_1) = f_{z_1} f_{z_2} f_{z_2}(w) = f_{z_1} f_{z_2}(w)$$

on a ainsi $z_1\, z_2 \leqq z$.

On montrera de même que $z_2\, z_1 \leqq z$.

Règle R 5: Si

$$z_1 = (X_1, X_2 \cup X_3, X_4, \ldots, X_k) \qquad \text{et} \qquad z_2 = (X_1 \cup X_2, X_3, X_4, \ldots, X_k),$$

alors

$$z_1 z_2 \equiv z_2 z_1 \equiv z = (X_1, X_2, \ldots, X_k).$$

Preuve: Puisque $z_1 \leqq z$ et $z_2 \leqq z$, on a immédiatement $z_1 z_2 \leqq z$ et $z_2 z_1 \leqq z$.

Montrons que $z \leqq z_1 z_2$:

$$\forall w \in X^* \; w' \in f_z(w), \quad \text{on a } \forall i \in \{1, \ldots, k\}, \qquad \Pi_{X_i}(w) = \Pi_{X_i}(w').$$

Alors:

$$w \quad \Rightarrow^*_{z_1} \quad \Pi_{X_1}(w) \Pi_{X_2 \cup X_3}(w) \Pi_{X_4}(w) \ldots \Pi_{X_k}(w) \quad \Rightarrow^*_{z_1} \quad u_1 \Pi_{X_4}(w) \ldots \Pi_{X_k}(w)$$

où u_1 est défini par:

$$\Pi_{X_1 \cup X_2}(u_1) = \Pi_{X_1 \cup X_2}(w') \subseteq \Pi_{X_1}(w) \sqcup \Pi_{X_2}(w)$$

et $\Pi_{X_3}(u_1)=\Pi_{X_3}(w)$

$$\Rightarrow^*_{z_2} \quad \Pi_{X_1 \cup X_2}(u_1)\,\Pi_{X_3}(u_1)\,\Pi_{X_4}(w')\ldots\Pi_{X_k}(w')$$
$$=\Pi_{X_1 \cup X_2}(w')\,\Pi_{X_3}(w')\,\Pi_{X_4}(w')\ldots\Pi_{X_k}(w')=w_1$$

et

$$f_{z_2}(w_1)=\Pi_{X_1 \cup X_2}(w') \sqcup \Pi_{X_3}(w') \sqcup \Pi_{X_4}(w')\ldots \sqcup \Pi_{X_k}(w')$$

contient donc w' donc $w' \in f_{z_1} f_{z_2}(w)$ et $z_1\ z_2 \leqq z$.

Pour exemple, reprenons le précédent:

Nous en étions à

$$u \equiv z'_2\, z_4 \qquad \text{avec} \qquad z'_2=(a,b,c,d,e,fg) \quad \text{et} \quad z_4=(bc,def,ga)$$

alors

$$z'_2 \geqq z''_2=(bc,de,afg)$$

donc

$$u \equiv z'_2\, z''_2\, z_4 \qquad \text{et} \qquad z''_2\, z_4 \equiv (bc,de,f,ga)=z'_4 \quad \text{(règle R 5)}$$

alors

$$z'_2 \geqq z''_4=(bc,de,a,fg)$$

et

$$u \equiv z'_2\, z''_4\, z'_4 \equiv z'_2\,(bc,de,a,f,g)=z'_2\, z_5.$$

Enfin, $u \equiv z'_2\, z_5$ avec

$$z'_2 \geqq z'_5=(bc,d,e,a,fg)$$

et

$$z'_5\, z_5 \equiv (a,bc,d,e,f,g)=z_6 \quad \text{(règle R 4)}$$

donc

$$u \equiv z'_2\, z_6 \equiv (a,b,c,d,e,f,g) \quad \text{(règle R 4)}$$

Voici un autre exemple:

Soit

$$u = z_1 z_2 = (a, bc, d, ef, gh)(ab, cd, eg, fh).$$

On a

$$z_1 \geqq z'_1 z''_1 = (a, bc, d, efgh)(a, bcd, efgh)$$

et

$$z_2 \geqq z'_2 = (ab, cd, efgh).$$

Donc

$$u \equiv z_1 z'_1 z''_1 z'_2 z_2$$

$$z''_1 z'_2 \equiv z''_2 = (a, b, cd, efgh) \quad \text{(règle R 5)}$$

et

$$z'_1 z''_2 \equiv z_3 = (a, b, c, d, efgh) \quad \text{(règle R 5)}$$

Donc

$$u \equiv z_1 z_3 z_2 = (a, bc, d, ef, gh)(a, b, c, d, efgh)(ab, cd, eg, hf).$$

$$z_1 z_3 \equiv t_1 = (a, b, c, d, ef, gh) \quad \text{(règle R 4)}$$

et

$$z_3 \geqq z'_3 = (a, b, cd, efgh).$$

Alors

$$u \equiv z_1 z_3 z_3 z'_3 z_2 \equiv t_1 z_3 z'_3 z_2 \equiv t_1 z_3 z''_3$$

car

$$z'_3 z_2 \equiv z''_3 = (a, b, cd, eg, hf) \quad \text{(règle R 4)}$$

enfin

$$z_3 z''_3 \equiv t_2 = (a, b, c, d, eg, hf) \quad \text{(règle R 4)}$$

et

$$u \equiv t_1 t_2 = (a, b, c, d, ef, gh)(a, b, c, d, eg, hf).$$

Ici, nous n'avons pas réduit le mot de départ, au sens où le mot obtenu n'est pas plus court. Mais, on obtient un mot qui représente sans doute mieux ce que fait la fonction associée à u. Chaque lettre du mot de départ a en fait été remplacée par une lettre plus grande, et dans le cas présent, on ne peut pas faire mieux: ni réduire le mot en longueur (nous avons vu que (ef, gh) (eg, hf) est irréductible), ni remplacer une lettre par une lettre plus grande (sinon, on obtient la commutation totale) c'est ce qui peut donner l'idée d'une forme normale. Mais avant d'énoncer des règles qui permettent de transformer un mot en «améliorant» ses lettres, nous allons donner un critère permettant de reconnaître si un mot peut se réduire à une lettre:

PROPOSITION 4 : *Soit u un mot de Z^*. Il est équivalent d'écrire que:*

(1) *u est équivalent à une lettre z de Z.*

(2) $u \equiv u^2$.

(3) $u \equiv u^R$.

Preuve: (1) $\Rightarrow$ (2) est évident (règle E 0).

(2) $\Rightarrow$ (3).

Posons $u = z_1 . z_2 \ldots z_k$, avec $\forall\, 1 \leqq i \leqq k$, $z_i \in Z$. Écrire que $u \equiv u^2$ implique que $u \equiv u^k$ donc $u \leqq u^R$ [dans u^k, on enlève dans chaque occurrence de $u\,(k-1)$ lettres]. D'autre part, $\forall\, 1 \leqq i \leqq k$, $z_i \leqq u$, donc $z_k z_{k-1} \ldots z_1 = u^R \leqq u^k \equiv u$.

On en déduit que $u \equiv u^R$.

(3) $\Rightarrow$ (1)

Posons $u = z_1 z_2 \ldots z_k (k \geqq 1)$ et raisonnons par induction sur k.

Si $k = 1$, $u \in Z$.

Si le résultat est vrai pour les mots de longueur inférieure ou égale à k, prenons:

$u = z_1 z_2 \ldots z_{k+1} \equiv z_{k+1} z_k \ldots z_1$ alors:

$$
\begin{aligned}
u &\equiv z_1 z_2 \ldots z_{k+1} z_{k+1} && \text{(règle E 0)} \\
&\equiv z_1 z_1 z_2 \ldots z_{k+1} z_{k+1} && \text{(règle E 0)} \\
&\equiv z_1 z_{k+1} z_k \ldots z_1 z_{k+1} && \text{(hypothèse)} \\
&\equiv (z_{k+1} \vee z_1)(z_k \vee z_1) \ldots (z_2 \vee z_1) z_{k+1} && \text{(règle R 2)} \\
&\equiv (z_{k+1} \vee z_1)(z_k \vee z_1 \vee z_{k+1}) \ldots (z_2 \vee z_1 \vee z_{k+1}) && \text{(règle R 3).}
\end{aligned}
$$

Nous avons ainsi réduit u à un mot v de k lettres;

de même:

$$u^R \equiv z_{k+1} z_{k+1} z_k \ldots z_1 z_1 \quad \text{(règle E 0)}$$
$$\equiv z_{k+1} z_1 z_2 \ldots z_{k+1} z_1 \quad \text{(hypothèse)}$$
$$\equiv z_{k+1}(z_1 \vee z_2)(z_1 \vee z_3)(z_1 \vee z_{k+1}) \quad \text{(règle R 2)}$$
$$\equiv (z_1 \vee z_2 \vee z_{k+1})(z_1 \vee z_3 \vee z_{k+1}) \ldots (z_1 \vee z_k \vee z_{k+1})(z_1 \vee z_{k+1}) = v^R.$$

Nous avons donc $v \equiv v^R$, puisque $u \equiv u^R$.

Par hypothèse de récurrence, on a donc $v \equiv z \in Z$ et donc $u \equiv z \in Z$.

Remarque: il est clair, qu'ici, $z = z_1 \vee z_2 \vee \ldots \vee z_{k+1}$.

COROLLAIRE : *Les seules fonctions de commutation partielle qui s'expriment comme le produit de fonctions de commutation partitionnée sont les fonctions de commutation partitionnée.*

Preuve: Si g est une fonction de commutation partielle, $g = g^2$. Donc, si $g = f_{z_1} f_{z_2} \ldots f_{z_p}$, on a forcément $z_1 z_2 \ldots z_p \equiv z$ (proposition 4).

III. Mots améliorables dans Z^*

DÉFINITION : Soit $u = z_1 z_2 \ldots z_p$ un mot de Z^*.

u est k-améliorable si on peut remplacer la k-ième lettre de u par une lettre plus grande, pour obtenir un mot équivalent à u, c'est-à-dire si il existe $z \in Z$ tel que $z > z_k$ et $u \equiv z_1 z_2 \ldots z_{k-1}\, z z_{k+1} \ldots z_p$.

u est améliorable si il existe un indice k pour lequel u est k-améliorable.

Nous allons énoncer des règles qui permettent d'améliorer un mot, et tout de suite une règle qui est à associer à la règle R 3:

Règle A 6: Soient z, z', z_1, z_2, ..., z_k des lettres de Z.

Soit $z'' = z \wedge z'$.

On a

$$z z_1 z_2 \ldots z_k z' \equiv z(z_1 \vee z'')(z_2 \vee z'') \ldots (z_k \vee z'') z'.$$

Remarque: Dans le cas où $z \leqq z'$, on a $z'' = z$ et $z \leqq z_1 \vee z$, et on retrouve la règle R 3.

Preuve:

$$z'' = z' \vee z' \leqq z \text{ et } z'' \leqq z'$$

donc:

$$zz_1 \ldots z_k z' \equiv zz'' z_1 z_2 \ldots z_k z'' z' \quad \text{(règle E 0)}$$
$$\equiv z(z_1 \vee z'')(z_2 \vee z'') \ldots (z_k \vee z'') z' \quad \text{(règle R 2).}$$

La règle suivante généralise les règles R 4 et R 5.

Règle A 7: Si

$$z_1 = (X, X_1, X_2, \ldots, X_p) \qquad \text{et} \qquad z_2 = (X \cup Y, Y_1, Y_2, \ldots, Y_k),$$

alors

$$z_1 z_2 \equiv (X, X_1, X_2, \ldots, X_p)(X, Y, Y_1, Y_2, \ldots, Y_k) = z_1 z_2'$$

et

$$z_2 z_1 \equiv z_2' z_1.$$

Un exemple:

$$u = z_1 z_2 = (ab, cd, ef, gh)(a, bc, de, fg, h)$$
$$\equiv (a, b, cd, ef, gh)(a, bc, de, fg, h) \quad \text{(règle A 7)}$$
$$\equiv (a, b, cd, ef, gh)(a, b, c, de, fg, h) \quad \text{(A 7)}$$
$$\equiv (a, b, c, d, ef, gh)(a, b, c, de, fg, h) \quad \text{(A 7)}$$
$$\equiv (a, b, c, d, ef, gh)(a, b, c, d, e, fg, h) \quad \text{(A 7)}$$
$$\equiv (a, b, c, d, e, f, gh)(a, b, c, d, e, fg, h) \text{(A 7)}$$
$$\equiv (a, b, c, d, e, f, g, h) \quad \text{(règle R 5).}$$

Mais on pourra vite s'apercevoir que le mot (ab, cd, ef, gh) (bc, de, fg, ha) n'est pas équivalent à la commutation totale.

Preuve: Montrons que

$$z_1 z_2 \equiv z_1 z_2' \qquad \text{avec} \quad z_2' = (X, Y, Y_1, Y_2, \ldots, Y_k).$$

posons

$$z_1'' = \left(X, \bigcup_{i=1}^{p} X_i\right) \qquad \text{et} \qquad z_2'' = \left(X \cup Y, \bigcup_{i=1}^{k} Y_i\right)$$

alors $z_1 \geqq z_1''$ et $z_2 \geqq z_2''$,

Donc

$$u = z_1 z_2 \equiv z_1 z_1'' z_2'' z_2 \qquad \text{et} \qquad z_1'' z_2'' \equiv z_3 = \left(X, Y, \bigcup_{i=1}^{k} Y_i\right)$$

en utilisant la règle R 5.

Il reste à montrer que $z_3 z_2 \equiv z_2'$, soit

$$\left(X, Y, \bigcup_{u=1}^{k} Y_i\right)(X \cup Y, Y_1, Y_2, \ldots, Y_k) \equiv (X, Y, Y_1, \ldots, Y_k).$$

Faisons une récurrence sur k:

Si $k = 1$, le résultat est clair puisque $(X, Y, Y_1) \geqq (X \cup Y, Y_1)$.

Si le résultat est vrai pour toute valeur plus petite que k, alors à l'indice $k+1$:

$$z_3 z_2 \equiv z_3 \left(X \cup Y, Y_1, \bigcup_{i=2}^{k+1} Y_i\right) z_2$$

et

$$z_3 \left(X \cup Y, Y_1, \bigcup_{i=2}^{k+1} Y_i\right) \equiv \left(X, Y, Y_1, \bigcup_{i=2}^{k+1} Y_i\right) = z_4 \quad \text{(règle R 4)}$$

alors

$$\begin{aligned} z_3 z_2 &\equiv z_4 z_2 \\ &\equiv z_4 \left(X, Y \cup Y_1, \bigcup_{i=2}^{k+1} Y_i\right)(X \cup Y \cup Y_1, Y_2, Y_3, \ldots, Y_{k+1}) z_2 \\ &\equiv z_4 (X, Y \cup Y_1, Y_2, Y_3, \ldots, Y_{k+1}) z_2 \end{aligned}$$

en appliquant l'hypothèse de récurrence

$$\begin{aligned} &\equiv z_4 z_2' \quad \text{(règle R 4)} \\ &\equiv z_2' \text{ car } z_4 \leqq z_2'. \end{aligned}$$

La dernière règle de ce paragraphe permet d'améliorer les extrémités d'un mot.

Règle A 8: Soient $t, u, v, \in Z^*$ et $z_1, z_2, z_3, z_4 \in Z$.

Si

$$t \equiv z_1 u z_2 \equiv z_3 v z_4$$

alors

$$t \equiv (z_1 \vee z_3) u (z_2 \vee z_4) \equiv (z_1 \vee z_3) v (z_2 \vee z_4).$$

Preuve:

$$\begin{aligned} t \equiv z_1 u z_2 &\equiv z_1 z_1 u z_2 z_2 \\ &\equiv z_1 z_3 v z_4 z_2 \\ &\equiv z_1 z_3 z_3 v z_4 z_4 z_2 \\ &\equiv z_1 z_3 z_1 u z_2 z_4 z_2 \\ &\equiv (z_1 \vee z_3) u (z_2 \vee z_4) \quad \text{(règle R 2).} \end{aligned}$$

IV. Mots normalisés dans Z*

Il semble maintenant naturel de donner la définition suivante:

DÉFINITION : Un mot u de Z^* est sous forme normale ou normalisé si il est irréductible et s'il n'est plus améliorable.

On peut maintenant se demander si l'équivalence de deux mots normalisés implique leur égalité et puis essayer de trouver des critères simples permettant de décider rapidement si un mot est sous forme normale ou pas.

L'unicité est vraie pour les mots qui se réduisent à deux lettres:

PROPOSITION 5 : *Tout mot de Z^* de longueur inférieure ou égale à deux à une forme normale unique.*

Preuve: Soit $u \in Z^*$. Si u se réduit à une lettre, cette lettre est de manière évidente la forme normale unique de u.

Supposons maintenant que u a deux formes normales (de deux lettres):

Si $u \equiv z_1 z_2 \equiv z_3 z_4$, avec $z_1, z_2, z_3, z_4 \in Z$, $z_1 z_2$ et $z_3 z_4$ sous forme normale, alors

$$\begin{aligned} z_1 z_2 &\equiv z_1 z_1 z_2 \\ &\equiv z_1 z_3 z_4 \\ &\equiv z_1 z_3 z_3 z_4 \\ &\equiv z_1 z_3 z_1 z_2 \\ &\equiv (z_1 \vee z_3) z_2 \quad \text{(règle R 2)} \end{aligned}$$

donc $(z_1 \vee z_3) \leqq z_1 \leqq (z_1 \vee z_3)$ (la première inégalité venant du fait que $z_1 z_2$ est sous forme normale). On en déduit que $z_1 \equiv (z_1 \vee z_3)$ et symétriquement on montre que $z3 \equiv (z_1 \vee z_3)$.

Ainsi $z_1 = z_3$ est de même $z_2 = z_4$.

Nous allons maintenant nous intéresser à une condition nécessaire et suffisante permettant de décider si un mot de deux lettres est sous forme normale ou pas:

PROPOSITION 6 : *Soit* $u = z_1 z_2$ *avec* $z_1, z_2 \in Z$.

Alors u est 1*-améliorable si et seulement si il existe* $R_3 \subseteq X$ *et des sous-ensembles* X_1', X_1'', R_1, R_2 *tel que*:

- $X_1 = X_1' \cup X_1''$ *soit un élément de* z_1;
- $z_1 > (X_1, R_1, R_2, R_3)$;
- $z_2 > (X_1' \cup R_1, X_1'' \cup R_2, R_3)$.

Preuve: Montrons que la condition est suffisante:
posons:

$$y_1 = (X_1, R_1, R_2, R_3), \qquad y_2 = (X_1' \cup R_1, X_1'' \cup R_2, R_3)$$

et

$$y_1' = (X_1 \cup R_1, R_2, R_3)$$

alors

$$\begin{aligned} z_1 z_2 &\equiv z_1 y_1 y_1' y_2 z_2 \\ &\equiv z_1 y_1 (X_1' \cup R_1, X_1'', R_2, R_3) z_2 \quad \text{(règle R 5)} \\ &\equiv z_1 (X_1', X_1'', R_1, R_2, R_3) z_2 \quad \text{(règle R 5)} \end{aligned}$$

et en posant $z_1=(X_1, X_2, X_3, \ldots, X_k)$, on a:

$$z_1(X_1', X_1'', R_1, R_2, R_3)\equiv(X_1', X_1'', X_2, X_3, \ldots, X_k)>z_1 \quad \text{(règle A 7)}.$$

Montrer que la condition est nécessaire est un peu plus long:

z_1 est 1-améliorable implique qu'il existe une lettre $z'>z_1$ telle que $z_1 z_2\equiv z_1' z_2$.

Si $z_1=(X_1, X_2, \ldots, X_k)$, on a:

$$z_1'=(X_{1,1}, X_{1,2}, \ldots, X_{1,p_1}, X_{2,1}, \ldots, X_{k,1}, X_{k,2}, \ldots, X_{k,pk})$$

avec

$$\forall 1\leqq i\leqq k, \quad \forall 1\leqq i\leqq p_i, \qquad X_{i,j}\neq\varnothing, \quad p_i\geqq 1,$$

et pour au moins un indice i, $p_i\geqq 2$ $(z_1'>z_1)$.

Supposons que p_1 soit plus grand que 2 et posons:

$$X_1'=X_{1,1}, \qquad X_1''=\bigcup_{j=2}^{p_1} X_{1,j} \quad \text{et} \quad z_1''=(X_1', X_1'', X_2, X_3, \ldots, X_k)$$

alors on a $z_1<z_1''\leqq z_1'$, donc

$$z_1 z_2<z_1'' z_2\leqq z_1' z_2\equiv z_1 z_2.$$

On en déduit que $z_1 z_2\equiv z_1'' z_2$.

Il nous faut maintenant construire les ensembles R_1, R_2, R_3.

Posons $z_2=(Y_1, Y_2, \ldots, Y_p)$.

Soient

$$R_1^0=U\{Y_\alpha, Y_\alpha\cap X_1'\neq\varnothing\}\setminus X_1'$$
$$R_1^1=U\{X_\beta, X_\beta\cap R_1^0\neq\varnothing\}$$

et plus généralement, pour $p\geqq 1$

$$R_1^{2p}=U\{Y_\alpha, Y_\alpha\cap R_1^{2p-1}\neq\varnothing\}\setminus X_1'$$
$$R_1^{2p+1}=U\{X_\beta, X_\beta\cap R_1^{2p}\neq\varnothing\}.$$

Soit $R_1=R_1^{2p}$, p étant le premier indice vérifiant $R_1^{2p}=R_1^{2p+1}$ (p existe car X est fini et la suite des R_1^i est croissante)

R_2 est construit de manière analogue, en remplaçant X_1' par X_1''.

Par construction, il est clair que $R_1 \cup X'_1$ et $R_2 \cup X''_1$ sont chacun des unions d'éléments Y_i de la partition z_2 et de même, R_1 et R_2 sont deux unions d'éléments X_j de la partition z_1.

Posons $R_3 = X \setminus (X_1 \cup R_1 \cup R_2)$.

Ainsi, il est clair que $X = X_1 \cup R_1 \cup R_2 \cup R_3$, et pour montrer que (X_1, R_1, R_2, R_3) est une partition de X, il suffit d'établir que

$$R_1 \cap R_2 = \varnothing, \qquad R_1 \cap X_1 = \varnothing \quad \text{et} \quad R_2 \cap X_1 = \varnothing.$$

(1) $R_1 \cap X_1 = \varnothing$ (et symétriquement $R_2 \cap X_1$).

Tout d'abord, par construction, on a $R_1 \cap X'_1 = \varnothing$.

Supposons que R_1 contienne une lettre x''_1 de X''_1.

Cela veut dire qu'il existe une suite de lettres $(x_0, x_1, x_2, \ldots, x_{2p+1})$ avec $p \geqq 1$ vérifiant:

- $x_0 \in X'_1$;
- $\exists\, \alpha_0$ tel que $\{x_0, x_1\} \subset Y_{\alpha 0}$ (construction de R_1^0);
- $\exists\, \beta_0$ tel que $\{x_1, x_2\} \subseteq X_{\beta 0}$ (construction de R_1^1);
- $\{x_{2i}, x_{2i+1}\} \subseteq Y_{\alpha i}$, $\{x_{2i+1}, x_{2i+2}\} \subseteq X_{\beta i}$;
- et $x_{2p+1} = x''_1 \in X''_1$ (c'est la première lettre de X''_1 qu'on rencontre dans la suite).

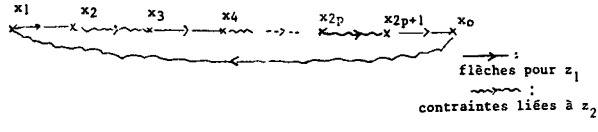
Alors, soient

$$w = x_1 x_2, \ldots, x_{2p+1} x_0 \qquad \text{et} \qquad w' = x_0 x_1 x_2, \ldots, x_{2p+1}.$$

Il est clair que w' peut-être obtenu à partir de w par les fonctions $f_{z''_1}$ et f_{z_2}:

$$w \quad \to^*_{z''_1} \quad w_1 \to^*_{z_2} w' \qquad \text{avec} \quad w_1 = w'$$

mais il n'est pas possible d'obtenir w' à partir de w par z_1 puis z_2: en essayant de reconstruire le mot w_1, on obtient:



ce qui est cyclique:

w_1 n'existe donc pas.

Comme on a supposé que $z_1 z_2 \equiv z_1'' z_2$, nous obtenons une contradiction et il est donc impossible de trouver une lettre de X_1'' dans R_1.

(2) Pour montrer que $R_1 \cap R_2 = \varnothing$, le raisonnement est analogue:

Supposons qu'il existe une lettre x de X appartenant à $R_1 \cap R_2$.

De part son appartenance à R_1, on peut construire une suite de lettres $(x_0, x_1, \ldots, x_{2p+1})$ avec $p \geqq 0$ et

- $x_0 \in X_1'$;
- $\{x_0, x_1\} \subseteq Y_{\alpha 0}$ (construction de R_1^0);
- $\{x_1, x_2\} \subset X_{\beta 0}$ (construction de R_1^1);
- $\{x_{2i}, x_{2i+1}\} \subseteq Y_{\alpha i}$, $\{x_{2i+1}, x_{2i+2}\} \subseteq X_{\beta i}$, $\forall i \geqq 1$.
- $x_{2p+1} = x$.

De même, parce que x appartient à R_2, on peut construire une suite $(y_0, y_1, \ldots, y_{2k})$ avec $k \geqq 0$ et

- $\{y_{2i}, y_{2i+1}\} \subseteq Y_{\alpha' i}'$ et $\{y_{2i+1}, y_{2i+2}\} \subseteq X_{\beta' i}'$, $\forall i \geqq 0$;
- $y_0 \in X_1''$;
- $y_{2k} = x$.

Alors posons

$$w = x_1 x_2, \ldots, x_{2p} x y_{2k-1} \ldots y_1 y_0 x_0$$

et

$$w' = x_0 x_1 x_2 \ldots x_{2p} x y_{2k-1} \ldots y_1 y_0.$$

Il est clair, d'après les constructions que w' s'obtient à partir de w avec la fonction associée à z_1' ($x_0 \in X_1'$ commute avec toutes les autres lettres de w qui ne peuvent être dans X' — ni dans X_1 d'ailleurs, sauf y_0), mais il n'est pas possible, comme précédemment, d'obtenir w' à partir de w en appliquant les fonctions associées à z_1 puis z_2.

La démonstration est alors finie puisqu'il est clair que:

$$z_1 > (X_1, R_1, R_2, R_3)$$

et

$$z_2 > (X_1' \cup R_1, X_1'' \cup R_2, R_3).$$

On peut évidemment donner un critère tout à fait analogue pour la propriété « 2-améliorable » :

$z_1\ z_2$ est 2-améliorable si et seulement si il existe un élément $Y_1 = Y_1' \cup Y_1''$ de z_2, vérifiant :

$$Y_1' \neq \varnothing, \qquad Y_1'' \neq \varnothing, \qquad z_2 > (Y_1, R_1, R_2, R_3)$$

et

$$z_1 > (Y_1' \cup R_1, Y_1'' \cup R_2, R_3).$$

Exemples : Soit

$$X = \{a, b, c, d, e, f, g, h, i, j, k, l\}$$

et

$$z_1 = (abcd, ef, gh, ij, kl), \qquad z_2 = (abeg, fh, cdik, jl)$$

* on a

$$z_1 \geqq (abcd, efgh, ijkl) = z_1'$$
$$z_2 \geqq (abefgh, cdikjl) = z_2',$$

Posons

$$X_1 = \{a, b, c, d\}, \qquad X_1' = \{a, b\}, \qquad X_1'' = \{c, d\}.$$
$$R_1 = \{e, f, g, h\}, \qquad R_2 = \{i, j, k, l\}, \qquad R_3 = \varnothing.$$

$z_1\ z_2$ est donc 1-améliorable et

$$z_1\ z_2 \equiv (ab, cd, ef, gh, ij, kl)\ (abeg, fh, cdik, jl).$$

* on a alors :

$$z_1 > (ab, efgh, cdijkl)$$
$$z_2 > (abeg, fh, cdijkl)$$

et posons

$$Y_1 = \{a, b, e, g\}, \qquad Y_1' = \{a, b\}, \qquad Y_1'' = \{e, g\}, \qquad R_1 = \varnothing,$$
$$R_2 = \{f, h\} \qquad \text{et} \qquad R_3 = \{c, d, i, j, k, l\},$$

on a $z_1\ z_2$ est 2-améliorable, et $z_1\ z_2 \equiv z_1\ (ab, eg, fh, cdik, jl)$.

* et en réitérant l'opération avec les six lettres c, d, i, j, k, l, on a $z_1 z_2 \equiv (ab, cd, ef, gh, ij, kl)\ (ab, eg, fh, cd, ik, jl)$.

* $z_1 z_2$ est maintenant sous forme normale.

V. Les commutations sur un alphabet de quatre lettres

Avec les propriétés et les règles énoncées jusqu'à présent, nous allons pouvoir montrer que sur un alphabet de quatre lettres, un mot de Z^* se réduit toujours, et de manière unique, à un mot de longueur inférieure où égale à deux.

Soit $X = \{a, b, c, d\}$ — outre les éléments 1 (commutation totale) et 0 (rien ne commute), les éléments de Z sont du type 1: (x, yzt) avec $\{x, y, z, t\} = \{a, b, c, d\}$, ou 2: (xy, zt), ou 3: (x, y, zt).

Il faut regarder comment se réduisent les mots formés de ces trois types de lettres:

Un mot $z_1 z_2$ où z_1 et z_2 sont du type 1 se réduit à une lettre grâce à la règle R 5:

$$(x, yzt)(y, xzt) \equiv (x, y, zt)$$

de même pour un mot $z_1 z_2$ où z_1 est du type 1 et z_2 de type 2:

$$(x, yzt)(xy, zt) \equiv (x, y, zt) \quad \text{(règle R 5)}$$

et aussi pour un mot $z_1 z_2$ où z_1 est de type 1 et z_2 de type 3:
soit $z_1 \leqq z_2$, soit

$$z_1 z_2 = (x, yzt)(y, z, xt) \equiv 1 \quad \text{(règle A 7)}.$$

Un mot $z_1 z_2$ où z_1 est du type 2 et z_2 du type 3 se réduit ainsi:
soit $z_1 \leqq z_2$, soit

$$z_1 z_2 = (xy, zt)(x, z, yt) \equiv 1 \quad \text{(règle A 7)}.$$

Un mot composé de lettres de type 3 se réduit également:

$$(x, y, zt)(xy, z, t) \equiv 1 \qquad \text{et} \qquad (x, y, zt)(x, z, yt) \equiv 1.$$

Par contre un mot de deux lettres différentes de type 2 est sous forme normale. On a déjà vu qu'un tel mot est irréductible. Il est facile de voir qu'il n'est pas améliorable.

Il est alors clair que les mots de longueur supérieure ou égale à 3 vont se réduire sans problème, sauf celui formé des trois lettres de type 2. Mais nous

pouvons écrire:

PROPOSITION 7 : $z_1 z_2 z_3 = (ab, cd)\ (ac, bd)\ (ad, bc) \equiv 1$,

Preuve: Nous allons montrer que pour tout mot w de X^*, $f_1\ f_2\ f_3(w) = \mathrm{com}(w)$, où f_1 (resp. f_2, f_3) est la fonction de commutation partitionnée associée à z_1 (resp. z_2, z_3) et com (w) est l'ensemble des mots qui ont le même nombre d'occurrences de chaque lettre de X que w.

Pour cela, nous allons, pour tout mot w' de com (w), construire deux mots: x et y tels que:

$$w \Rightarrow_{z_1}^* x \Rightarrow_{z_2}^* y \Rightarrow_{z_3}^* w'$$

x et y ont donc les propriétés suivantes:

(1) $\Pi_{\{a,b\}}(x) = \Pi_{\{a,b\}}(w)$ et $\Pi_{\{c,d\}}(x) = \Pi_{\{c,d\}}(w)$.

(2) $\Pi_{\{a,d\}}(y) = \Pi_{\{a,d\}}(w')$ et $\Pi_{\{b,c\}}(y) = \Pi_{\{b,c\}}(w')$.

(3) $\Pi_{\{a,c\}}(x) = \Pi_{\{a,c\}}(y)$ et $\Pi_{\{b,d\}}(x) = \Pi_{\{b,d\}}(y)$.

Posons

$$u_1 = \Pi_{\{a,b\}}(w), \qquad u_2 = \Pi_{\{c,d\}}(w)\ (x \in u_1 \sqcup u_2)$$

et

$$v_1 = \Pi_{\{a,d\}}(w'), \qquad v_2 = \Pi_{\{b,c\}}(w')\ (y \in v_1 \sqcup v_2).$$

Pour définir la première lettre de x et celle de y, on peut comparer les premières lettres de u_1 et u_2 avec celles de v_1 et v_2: par exemple, si $u_1 = au_1'$ et $v_1 = av_1'$, on peut poser $x = ax'$, $y = ay'$ et se ramener à un problème plus simple: la longueur des mots à définir diminue.

Par contre, si $u_1 = au_1'$, $u_2 = cu_2'$ d'une part et $v_1 = dv_1'$, $v_2 = bv_2'$ d'autre part, alors, on peut avoir $u_1 = a^k bu_1''$, $x = a^k bx'$ et $y = by'$, et il faut alors «conserver» le mot a^k qui devra apparaître dans y' (dans le passage de x à y, les occurrences de la lettre «a» commute avec le «b»).

D'où l'algorithme et l'invariant suivants pour construire x et y:

On peut trouver x', x'', u_1', u_1'', u_2', u_2'', y', y'' et s dans X^* tels que:

$$x = x'x'' \quad (x' \text{ est la partie du mot } x \text{ déjà construite})$$

$$u_1 = u_1' u_1''$$

$$u_2 = u_2' u_2''$$

$$x' \in u_1' \sqcup u_2'$$

$$y = y' y''$$

et

(1) $x' \Rightarrow^* y's$ (s est le sous mot de y qui n'a pu être placé immédiatement — *voir* exemple ci-dessus),

(2) $s \in (a+c)^* \cup (b+d)^*$,

(3) $\Pi_{\{a,d\}}(y') \in FG(v_1)$ (l'ensemble des facteurs gauches de y_1)

$$\Pi_{\{b,c\}}(y') \in FG(v_2).$$

(4) y' est le plus grand facteur gauche de $y's$ vérifiant la condition (3).

Ces conditions étant vérifiées (elles le sont au départ), comment définir la lettre qui sera derrière x'?

Supposons $u_1'' u_2'' \neq \varepsilon$ (il reste une lettre à traiter).

Si $u_1'' = a u_1'''$ (les autres cas sont traités de manière symétrique).

Alors: (1) s contient une occurrence de a. Alors le traitement consiste à ajouter «a» au bout de s ($s \leftarrow sa$) et au bout de x' ($x' \leftarrow x'a$). On vérifie aisément que toutes les conditions restent vérifiées.

(2) s ne contient aucune occurrence de a.

Alors

(2.1) s peut être vide; dans ce cas, soit la lettre «a» peut être placée dans y' car $\Pi_{\{a,d\}}(y'a) \in FG(v_1)$ et alors $x' \leftarrow x'a$, $y' \leftarrow y'a$, soit la lettre «a» ne peut être placée dans y' car $\Pi_{\{a,d\}}(y'a) \notin FG(v_1)$ (on attend un «d») alors, on ajoute a à s ($s \leftarrow sa$) et dans les deux cas, $x' \leftarrow x'a$.

(2.2) s peut être un mot de c^+. Alors, on ajoute a à s et à x ($s \leftarrow sa$, $x \leftarrow xa$)

(2.3) s peut être un mot de $(b+d)^+$.

(2.3.1) Si $\Pi_{\{a,d\}}(y'a) \in FG(v_1)$, on peut comme précédemment ajouter a à y', ($y' \leftarrow y'a$), puis le prolonger par le plus grand facteur gauche s' de s tel que $\Pi_{\{a,d\}}(y's') \in FG(v_1)$. Ainsi, en éliminant s' de s, les conditions 3 et 4 sont vérifiées, et on a encore $x'a \Rightarrow_{z_2}^* y'as$ car a commute avec b et d dans z_2. Donc

$$\begin{array}{ccccccc} x'a & \Rightarrow_{z_2}^* & y'sa & \Rightarrow_{z_2}^* & y'as \\ \| & & & & \| \\ x' & & & & y's \end{array}$$

(2.3.2) $\Pi_{\{a,d\}}(y'a) \notin FG(v_1)$. Cela veut dire que $\Pi_{\{a,d\}}(y'd) \in FG(v_1)$. (On attend un d avant le a qu'on vient de lire dans u_1), et donc $s \in b(b+d)^*$ (sinon la condition (4) ne serait pas vérifiée). Prenons alors en compte la

première lettre de u_2'' plutôt que celle de u_1''. Si $u_2''=du_3''$, alors s devient sd ($s \leftarrow sd$), x' est remplacé par $x'd$; sinon, on a $u_2''=cu_2''$ et on déduit que $\Pi_{\{b,c\}}(y'c) \in FG(v_2)$ (s commence par un b et la condition 3 est vérifiée par y'). Alors, on prolonge y' par c puis par le plus grand facteur gauche de s: s' qui permet de garder la condition 3, et on prolonge également x' par c ($x' \leftarrow x'c$).

Reste à étudier le cas où $u_2''=\varepsilon$: toutes les occurrences de la lettre c ont donc été prises en compte dans y' et comme 3) est vérifiée, on devrait avoir $\Pi_{\{b,c\}}(y'b) \notin FG(v_2)$. Mais comme il n'y a plus que des «b» à prendre en compte pour définir $\Pi_{\{b,c\}}(y)$, on a ici une impossibilité.

Quand $u_1''=\varepsilon$, on peut prolonger x' et y' en étudiant la première lettre de u_2'', de manière tout à fait analogue. Quand $u_1''=u_2''=\varepsilon$ (on a épuisé la lecture de u_1 et u_2), il faut alors montrer que $s=\varepsilon$, et ainsi on aura construit x et y répondant au problème.

Supposons que $s \neq \varepsilon$, $s=as'$ par exemple.

Alors, toutes les occurrences de la lettre d ont été lues et placées dans y' ($s \in (a+c)^*$); il n'y a donc que des occurrences de la lettre «a» à placer dans $\Pi_{\{a,d\}}(y')$ or $\Pi_{\{a,d\}}(y'a) \notin FG(v_1)$ car y' vérifie la condition (4), il y a donc une contradiction.

Si s commence par une des lettres b, c, ou d, on obtient par symétrie le même résultat.

On a donc:

COROLLAIRE 8 : *Le monoïde engendré par les commutations partitionnées définies sur l'alphabet* $\{a, b, c, d\}$ *contient exactement* 21 *éléments.*

Preuve: Outre la commutation totale et la fonction où rien ne commute (les éléments 0 et 1 du treillis Z^*), nous avons vu qu'il y avait les partitions du type (x, yzt): au nombre de 4, celles au nombre de 3 du type (xy, zt) et celles du type (x, y, zt) au nombre de 6.

Nous avons vu, qu'en composant deux fonctions associées à deux partitions de type (xy, zt) différentes, nous obtenions des nouvelles fonctions (les mots de Z^2 sont d'ailleurs sous forme normale).

Il est facile de voir que ces six fonctions ainsi obtenues sont toutes différentes:

par exemple:
(ab, cd) $(ac, bd) \neq (ac, bd)$ (ab, cd) à cause de la proposition 4 (ab, cd) $(ac, bd) \neq (ab, cd)$ (ad, bc)

car si

$$(ab, cd)(ac, bd) \equiv (ab, cd)(ad, bc),$$

on a alors

$$\begin{aligned}(ab, cd)(ac, bd)(ac, bd) &\equiv (ab, cd)(ac, bd) \\ &\equiv (ab, cd)(ad, bc)(ac, bd) \\ &\equiv 1\end{aligned}$$

ce qui est faux.

Les autres cas se traitent de manière analogue.

CONCLUSION

Pour étudier les compositions de fonctions de commutation partitionnée, nous avons prouvé la validité d'un certain nombre de règles et nous avons introduit la notion de forme normale.

Dans le cas d'un alphabet contenant au plus 4 lettres, ces règles et la proposition 7 permettent de construire pour toute composition de fonctions de commutation partitionnée, une composition de fonctions de commutation partitionnée unique, sous forme normale, de longueur plus petite où égale à 2. Il est alors possible de comparer deux compositions de fonctions.

Par contre, pour un alphabet de plus de quatre lettres, même si les règles énoncées permettent souvent des simplifications importantes, de nombreuses questions restent posées. Rappelons-en quelques unes:

(1) décider si $f_{z_1} f_{z_2} \ldots f_{z_k} = \text{com}$.

(2) Peut-on avoir $u \equiv v$, avec u et v deux mots de Z^* différents et sous forme normale.

(3) Décider si un mot u de Z^* est sous forme normale...

BIBLIOGRAPHIE

1. I. J. Aalbersberg et G. Rozenberg, *Theory of traces*, rep n° 85-16, University of Leiden.
2. A. Bertoni, G. Mauri et N. Sabadini, *Equivalence and membership problems for regular trace languages*, 9e I.C.A.L.P., Aarhus, Lecture Note in Computer Science, vol. 140, 1982, p. 61-71.
3. P. Cartier et D. Foata, *Problèmes Combinatoires de Commutation et réarrangements*, Lectures Notes in Math., vol. 85, Springer Verlag, 1969.

4. M. CLERBOUT, *Commutations partielles et familles de langages*, Thèse de 3e cycle, Lille, 1984.
5. M. CLERBOUT et M. LATTEUX, *Semi-Commutations*, Information and Computation, n° 73, p. 15-24, 1987.
6. R. CORI et Y. METIVIER, *Recognizable Subsets of some partially abelian monoïds*, Theoretical Computer Sciences, vol. 35, 1985, p. 179-189.
7. R. CORI et D. PERRIN, *Sur la reconnaissabilité dans les monoïdes partiellement commutatifs libres*, R.A.I.R.O. Informatique Théorique, vol. 19, 1985.
8. C. DUBOC, *Commutations dans les monoïdes libres: un cadre théorique pour l'étude du parallélisme*, Thèse 3e cycle, Rouen, 1986.
9. M. P. FLÉ et G. ROUCAIROL, *Maximal serializability of iterated transactions*, Theoretical Computer Science, vol. 38, 1985, p. 1-16.
10. A. MAZURKIEWICZ, *Concurrent program schemes and their interpretations*, D.A.I.M.I., PB 78, Aarhus University, 1977.
11. E. OCHMANSKI, *Regular Behaviour of concurrent Systems*, E.A.T.C.S. Bulletin, octobre 1985.
12. D. PERRIN, *Words over a partially commutative alphabet*, Rapport L.I.T.P., n° 84-59.
13. W. ZIELONKA, *Notes on Finite Asynchronous Automata*, R.A.I.R.O. Info. Théorique, n° 21, p. 99-135, 1987.