Marcel-Paul Schützenberger

ŒUVRES COMPLÈTES

éditées par
Jean Berstel, Alain Lascoux et Dominique Perrin

*

Tome 9 : 1976–1978

Institut Gaspard-Monge, Université Paris-Est
2009

Introduction
Tome IX : 1976–1978

L'année 1976 est celle de la sortie du volume B de *Automata, Languages and Machines* [3]. Les relations avec Eilenberg se sont beaucoup tendues et l'introduction dit cette fois simplement : « M.-P. Schützenberger made valuable contributions which are specifically acknowledged in the reference sections ». On est bien loin du temps du volume A. Eilenberg renoncera d'ailleurs à rédiger les deux volumes suivants C (langages algébriques) et D (calculabilité).

L'article *Sur le produit de concaténation non ambigu* [1976-3] commence par une phrase qui est un hommage appuyé (et sûrement ironique) « Cet article est une application des méthodes développées par S. Eilenberg... ». Le sujet est la variété des semigroupes finis dont toute $\mathcal{D}$-classe régulière est un semigroupe. L'article établit un lien très étonnant entre cette variété et le produit non ambigu (ou sa variante latéralisée nommée produit déterministe). Bien qu'il soit moins connu que celui sur les langages sans étoile [1965-4], cet article a eu lui aussi une influence considérable sur les développements ultérieurs. On en trouvera une synthèse dans l'article de P. Tesson et D. Thérien [6], au titre évocateur, "Diamonds are Forever : The Variety DA".

L'article *Sur les relations rationnelles entre monoïdes libres* [1976-4] est un complément à [1975-2] qui commence par la palinodie usuelle « L'objet du présent travail est de préciser un point de la théorie des relations rationnelles entre monoïdes libres développée par Eilenberg dans le chapitre IX de son traité... ». Il montre que les relations rationnelles entre monoïdes libres qui ne sont pas des unions finies de fonctions rationnelles sont à croissance soit polynomiale soit exponentielle.

Les articles *Sur une caractérisation des parties reconnaissables d'un monoïde libre* [1976-5] et *Une caractérisation des parties reconnaissables* [1976-6] sont des variantes de la définition usuelle des parties reconnaissables. La deuxième est inspirée par la notion de matrice de Hankel et sera généralisée dans *Une propriété de Hankel des relations fonctionnelles entre monoïdes libres* [1977-2], à des relations rationnelles.

Le bref texte *Quelques problèmes posés par l'étude combinatoire des semigroupes* [1976-7] est issu d'une présentation au séminaire d'algèbre de M.-P. Malliavin du résultat qui paraîtra plus tard en [1979-1] (voir tome 10).

L'article [1976-1] dégage une propriété de dualité de l'opération d'*évacuation*, qui consiste, dans un ensemble étiqueté par des entiers tous différents, à choisir un sous-ensemble, puis à éliminer la plus petite valeur y apparaissant et à déplacer successivement toutes les autres valeurs. Le *jeu de taquin* sur les tableaux

de Young est une procédure de ce type.

L'article [1977-4] sur *La correspondance de Robinson* est un texte fondamental, quoique de lecture quelque peu ardue. Il présente la théorie des *tableaux de Young* par l'intermédiaire de glissements planaires (essentiellement le *jeu de taquin*). Ceci permet de réinterpréter les constructions de Robinson, Schensted, Knuth, les tableaux apparaissant comme représentants canoniques de chaque classe de congruence. Cette construction permet de plonger l'algèbre des polynômes symétriques dans l'*algèbre plaxique* (quotient de l'algèbre libre par les *relations plaxiques* dues à Knuth).

Les polynômes de Hall-Littlewood sont une base linéaire de l'anneau des polynômes symétriques. Leur décomposition dans la base des fonctions de Schur s'obtient en définissant une fonction à valeurs entières, *la charge*, sur l'ensemble des tableaux de Young. Ce résultat, annoncé dans [1978-4], est developpé dans [1978-1]. Une correction a été apportée par L. Butler [2].

L'introduction de la communication *Codes et sous-monoïdes possédant des mots neutres* [1977-1], avec Dominique Perrin, au colloque STACS se termine par une évocation du « bruit modulo p » qui n'a pas donné lieu à des explications beaucoup plus détaillées par la suite.

L'article *Un problème élémentaire de la théorie de l'information* [1978-2] contient une formulation de la conjecture qui apparaît déjà dans le séminaire de Royan [1965-8] : tout code est commutativement équivalent à un code préfixe. Cette conjecture n'est pas vraie sous cette forme (sans l'hypothèse que le code est maximal), comme l'a montré Shor en 1983 (voir le commentaire de [1981-3]). Il contient par contre la preuve de la conjecture pour les codes circulaires.

L'article *Major index and inversion number of permutations* [1978-3], avec Dominique Foata, fait suite à l'article de D. Foata [4] qui contient la description d'une transformation, donnant une démonstration "bijective" du vieux théorème de MacMahon, qui disait que l'indice majeur et le nombre d'inversions étaient équidistribuées sur toute classe de réarrangements de mots. On peut également décrire le groupe des symétries d'une statistique multivariée liée à l'indice majeur, lorsqu'on restreint cette transformation au groupe symétrique. Il a fallu attendre presque vingt ans pour qu'une transformation analogue, non plus sur les mots, mais sur les mots signés, puisse être construite [5]. Indice majeur et nombre d'inversions sont alors remplacés par indice majeur-drapeau et fonction longueur, respectivement et le groupe symétrique par le groupe hyperoctaedral.

L'article [1978-5] *Une application de la théorie ergodique au problème du codage*, avec François Blanchard et Dominique Perrin, est une version préliminaire d'un article signé des seuls deux premiers auteurs paru en 1980 [1].

---

[1] François Blanchard and Dominique Perrin. Relèvement d'une mesure ergodique par un codage. *Z. Wahrsch. Verw. Gebiete*, 54 :303–311, 1980.

[2] Lynne M. Butler. *Combinatorial properties of partially ordered sets associated with partitions and finite abelian groups*. PhD thesis, MIT, 1986.

[3] Samuel Eilenberg. *Automata, Languages, and Machines. Vol. B*. Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976. With two chapters ("Depth decomposition theorem" and "Complexity of semigroups and morphisms") by Bret Tilson, Pure and Applied Mathematics, Vol. 59.

[4] Dominique Foata. On the Netto inversion number of a sequence. *Proc. Amer. Math. Soc.*, 19 :236–240, 1968.

[5] Dominique Foata and Guo-Niu Han. Signed words and permutations, I : a fundamental transformation. *Proc. Amer. Math. Soc.*, 135 :31–40, 2007.

[6] Pascal Tesson and Denis Thérien. Diamonds are forever : the variety DA. In *Semigroups, algorithms, automata and languages (Coimbra, 2001)*, pages 475–499. World Sci. Publ., 2002.

Année 1976

Bibliographie

[1] Marcel-Paul Schützenberger. Evacuations. In *Colloquio Internazionale sulle Teorie Combinatorie (Rome, 1973), Tomo I*, pages 257–264. Atti dei Convegni Lincei, No. 17. Accad. Naz. Lincei, Rome, 1976.

[2] Samuel Eilenberg and Marcel-Paul Schützenberger. On pseudovarieties. *Adv. in Math.*, 19(3) :413–418, 1976.

[3] Marcel-Paul Schützenberger. Sur le produit de concaténation non ambigu. *Semigroup Forum*, 13(1) :47–75, 1976.

[4] Marcel-Paul Schützenberger. Sur les relations rationnelles entre monoïdes libres. *Theoret. Comput. Sci.*, 3(2) :243–259, 1976.

[5] Marcel-Paul Schützenberger. Sur une caractérisation des parties reconnaissables d'un monoïde libre. In *Journées algorithmiques (École Norm. Sup., Paris, 1975)*, pages 247–251. Astérisque, No. 38–39. Soc. Math. France, Paris, 1976.

[6] Marcel-Paul Schützenberger. Une caractérisation des parties reconnaissables. In *Formal languages and programming (Proc. Sem., UAM-IBM Sci. Center, Univ. Autónoma Madrid, Madrid, 1975)*, pages 77–82. North-Holland, Amsterdam, 1976.

[7] Marcel-Paul Schützenberger. Quelques problèmes posés par l'étude combinatoire des semigroupes. In *Groupe d'étude d'algèbre, Marie-Paule Malliavin, année 1975-76*, Exposé No. 19, 28 mai 1976, 1 page. Inst. H. Poincaré, Paris, 1976.

ACCADEMIA NAZIONALE DEI LINCEI

ATTI DEI CONVEGNI LINCEI

17

Colloquio Internazionale sulle

TEORIE COMBINATORIE

con la collaborazione della

AMERICAN MATHEMATICAL SOCIETY

(Roma, 3–15 settembre 1973)

Tomo I

(*ESTRATTO*)

R O M A
ACCADEMIA NAZIONALE DEI LINCEI
1 9 7 6

Année 1976 1976-1. Evacuations

M. P. SCHÜTZENBERGER

EVACUATIONS

RIASSUNTO. — Si introduce un algoritmo, detto di « evacuazione » che trova applicazione nelle teorie combinatorie delle rappresentazioni del gruppo simmetrico.

I. INTRODUCTION

La Théorie des représentations linéaires du groupe symétrique utilise toute une série de constructions remarquables sur les Tableaux de Young. Les plus connues sont peut être l'algorithme de Richardson et Littlewood pour déterminer la multiplicité des composantes irréductibles et la correspondance de G. de B. Robinson qui sert de base à la méthode des « rising operators » de Young. L'analyse des preuves fait apparaître deux niveaux bien distincts: dans le premier, n'interviennent que les propriété le plus élémentaires des ensembles ordonnés finis cependant que dans le second le fait que les tableaux de Young puissent être considérés comme des configurations *planaires* joue un rôle absolument essentiel qui ne semble permettre aucune généralisation. Evidement un troisième niveau est requis pour rattacher ces objets aux représentations elles même.

Dans le présent travail je me limiterai à la définition et à l'étude d'un algorithme dit « d'évacuation » qui ne relève que du premier niveau mais qui posséde déja plusieurs des propriétés remarquables de celui de G. de B. Robinson, introduit en 1938 (« American J. of Math. », *60*, pp. 745–60) et étudié depuis dans une toute autre optique (C. Schensted (1961), « Canadian J. of Math. », *13*, pp. 179–192 et D. Knuth (1970), « Pacific J. of Math. », *34*, pp. 709–727).

II. NOTATIONS ET DÉFINITION DE L'ALGORITHME

Dans tout ce qui suit nous considérerons un ensemble fini fixe P de *points* et des *fonctions* (c'est à dire d'applications partielles) *injectives* α de P dans la chaine standard $[n] = \{1 < 2 < \cdots < n\}$. Le nombre de éléments du domaine d'une telle fonction α sera noté $|\alpha|$ et, comme d'usage, O désiquera la fonction dont le domaine est vide.

La notion de base sera celle d'une action $\alpha \to \alpha V$ d'une partie V de P sur une fonction α que nous définissons de la façon suivante. Soit $V' = (v_1, v_2, \cdots, v_s)$ la suite de éléments de $V \cap \mathrm{Dom}(\alpha)$ indexés de telle sorte que l'on ait $v_1\alpha > v_2\alpha > \cdots > v_s\alpha$.

L'action αV est la fonction β de P telle que:

(1) $p\beta = p\alpha$ pour tout $p \in P \setminus V$;

(2) $v_1 \beta = \varnothing$;

(3) $v_k \beta = v_{k-1} \alpha$ pour chaque $v_k \in V$ $(h \geq 2)$;

On a donc

(4) $\mathrm{Dom}\ (\alpha V) = \mathrm{Dom}\ (\alpha) \setminus \{v_1\}$;

(5) $Im\ (\alpha V) = Im\ (\alpha) \setminus \{v_1\ \alpha\}$.

Et il est clair que αV est injective. Nous dirons pour abréger que V est une *trainée pour* α quand V est contenue dans le domaine de α. Par conséquent la donnée de deux fonctions (injectives) α et β determine au plus une trainée V pour α dont l'action sur α soit β.

De façon graphique on peut figurer P comme un systéme de « cases » et $[n]$ comme un ensemble de « piéces » classés par ordre de grandeur. Chaque fonction injective α représente alors une disposition de $|\alpha|$ (= Card Dom (α)) piéce sur les cases. V étant supposée être une trainée pour α, son action consiste à déplacer les piéces situées sur les cases qui la composent en commencant pur la plus grande (soit $v_1 \alpha$) et en suivant la régle que chaque piéce $v_k \alpha$ vient prendre la place occupée par la piéce immediatement plus petite, c'est à dire v_{k-1}, sauf en ce qui concerne la derniére piéce $v_s \alpha$ qui est éliminée. Par conséquent dans la disposition représenteé par $\beta = \alpha V$, la case v_1 est devenue vide et, par construction, l'on a $p\beta^{-1} \geq p\alpha^{-1}$ pour chaque point $p \in \mathrm{Dom}\ (\beta)$.

Une *evacuation* A de α sera une suite de $m = |\alpha|$ semblables actions menant de $\alpha = \alpha_m$ à $\alpha_0 = 0$. On la décrira en se donnant la suite $(V_m, V_{m-1}, \cdots, V_1)$ de ses m trainés, chaque V_k ètant une trainée pour $\alpha_k = \alpha_{k-1}\ V_{k-1}$, ou, aussi bien, par la suite des m fonctions $(\alpha_m = \alpha, \alpha_{m-1}, \cdots, \alpha_1)$ liés par les relations précédente qui impliquent $\alpha_1\ V_1 = 0$.

Pour des raisons de symétrie qui apparaitront dans la suite, il sera commode de considérer une partie quelconque I de m éléments distincts de $[n]$ et d'indexer le trainés par le éléments de I pris en ordee décroissant. On parlera alors d'une *I–évacuation*.

La deuxiéme notion de base est la suite $(U_j : j \in J)$ des *trajectoire* des piéces $j \in J = \mathrm{Im}\ (\alpha)$ dans une évacuations A de α. Intuitivement, U_j est la suite des cases *distinctes* occupées par la piéce j dans la suite de dispositions représentée par les fonctions α_i $(i \in I)$ de l'evacuation A. Formellement, soit $I\ (j) = (i_1, > i_2 > \cdots > i_s)$ la sous–suite des indice $i \in I$ pour lesquels $j\alpha_i^{-1}$ appartient à la trainée V_i de α_i. Il est clair que si j appartient à l'image d'une fonction α_i de A, l'on a $j\alpha_i^{-1} = j\alpha_{i'}^{-1}$, pour au moins un $i' \in I\ (j)$ car toute piéce finit par être éliminée. En oùtre tous les points $j\alpha_{i_k}^{-1}$ $(i_k \in I(s))$ sont différents puisque comme ou l'a fait observer plus haut, chaque relation $p\alpha_i = j$ $(p \in P)$

implique $p\alpha_{i'} \leq j$ pour tout $i' \geq i$. La suite $U_j = (j\alpha_{i_1}, j\alpha_{i_2}, \cdots, j\alpha_{i_s})$ est donc bien la suite de cases *distinctes* occupés par j au cours de l'évacuation.

Nous notons que les trainés et les trajectoires ont la même structure: ce sont des suite de points distincts. Notre résultat principal est l'établissement d'une dualité qui les échange. Le chapître suivant considère le cas indispensable pour les applications où les fonctions α sont de morphisme (d'ensemble ordonné).

L'exemple suivant tente d'illustrer ce notions. L'ensemble P est formé de 5 cases a, b, c, d, e.

Les dispositions successive des α_i d'une évacuation de α_5 sont le suivants:

	a	b	c	d	e
$\alpha_5 =$	1	2	3	4	5
$\alpha_4 =$	1	4	3	·	5
$\alpha_3 =$	1	·	4	·	5
$\alpha_2 =$	4	·	5	·	·
$\alpha_1 =$	4	·	·	·	·
$\alpha_0 =$	·	·	·	·	·

Les 5 trainés sont (d, b), (b, c), (e, c, a), (c), (a) et les 5 trajectoires sont $U_5 = (e, c)$; $U_4 = (d, b, c, a)$; $U_3 = (c)$; $U_2 = (b)$; $U_1 = (a)$.

Le lecteur aura peut être moins d'impatience en parcourant les sections suivantes s'il veut bien se convainance lui même qu'il y a quelque chose à prouver: partant de la disposition initiale $\beta_5 = 1\,4\,2\,5\,3$, il peut vérifier que $U_5, U_4, \cdots, U_1$ constituent bien les *trainées* successives d'une évacuation B dont les *trajectoires* se trouvent être (dans l'ordre même) les trainées de l'évacuation précédente.

III. Dualité

Nous considérons une $\dot{I}$–évacuation fixe $A = (\alpha_i : i \in I)$ $(I = (i_m > \cdots > i_{m-1} > \cdots > i_1))$ d'une fonction $\alpha = \alpha_{i_m}$ $(m = |\alpha|)$ de domaine $D \subset P$ et d'image $J \subset [n]$. Par hypothèse, I, D et J out m éléments et les trainés successives V_i de A sont indexés de façon decroissante. Les trajectoires son: les U_j $(j \in \dot{J})$.

Définition. Le *plan* de l'évacuation A est la fonction $a : I \times \dot{J} \to P$ définie par $(i, j)\, a = V_i \cap j\alpha_i^{-1}$ pour chaque $(i, j) \in I \times \dot{J}$.

De façon plus explicite, $(i, j)\, a = p$ ssi la trainée V_i contient un point p pour lequel $p\alpha_i = j$, ce qui entraine que pour chaque $i \in I$ l'ensemble $\{a(i, j) : j \in J\}$ $(= a(i, \dot{J}))$ soit précisement l'ensemble des points de la trainée V_i. Ceci entraine que la donnée de plan a determine completement l'evacuation A une fois connue la fonction initiale α. Mais celle–ci elle même est aussi

fournie par le plan a puisque pour chaque point p de domaine, la piéce $j = p\alpha$ peut être déterminée par la relation $a(i_j, j) = p$ où $i_j \in I$ est obtenu à son tous comme le plus grand $i \in I$ pour lequel $p \in V_i$.

De façon symétrique, la définition des trajectoires montre que pour chaque $j \in \dot{J}$ ou a $U_j = a(I, j)$. Cette deuxième remarque indique la marche générale de la discussion qui suit: elle revient à établir que la fonction transposée $\tilde{a}$ définie par l'identité $\tilde{a}(j, i) = a(i, j)$ est aussi le plan d'une évacuation B d'une certaine fonction initiale β.

Pour simplifier nous traitons d'abord tout ce qui concerne le *support* S′ du plan a c'est à dire la relation $S \subset I \times J$ formée des pairs (i, j) pour lesquelles $(i, j)\, a \neq \varnothing$. Comme d'usage, quelque soit la relation $R \subset I \times \dot{J}$ nous desiquons par $j R_1$ (resp. $i R_2$) pour chaque $j \in \dot{J}$ (resp. $i \in I$) l'ensemble des $i \in I$ (resp. des $j \in \dot{J}$) tels que $(i, j) \in R$.

III.1. Le support S du plan a satisfait la condition suivante:

(E). Il existe une bisection $E \subset S$ telle que pour chaque $(i, j) \in S'$ ou ait

$$jE_1 \leq i \qquad \text{et} \qquad iE_2 \leq j.$$

Preuve. Soit $i \in I$ et soit V_i le dernier élément de la trainée V_i, c'est à dire celui des points de V_i tel que $v_i\, \alpha_i = \mathrm{Max}\ (V_i\, \alpha_i)$.

D'aprés la definition de l'action $\alpha_i \to \alpha_i\, V_i$, la piéce $v_i\, \alpha_i$ n'appartenent plus à l'image d'aucune des fonctions $\alpha_{i'}$ pour $i' < i$. Comme toute les piéces $j \in J$ appartiennent à $I_m(\alpha)$ et que chacune d'elles est finalement évacuée, ceci montre que la fonction $i \to v_i\, \alpha_i$ est une bijection de $\dot{I}$ sut $\dot{J}$ dont nous designons le graphe par E. Ou a identiquement comme ou vient de voir que $(i, j) \in S$ entraine $i \geq jE_1$ et par consèquent aussi la condition symétrique $j \geq iE_2$. Q.E.D.

Pour abréger nous dirons qu'une relation $R \subset I \times J$ est une *relation d'évacuation* si elle satisfait la condition (E) ci dessus. Les deux énoucés suivants concernant une relation d'évacuation quelconque R ne requèrent pas de preuve:

– La relation transposeé $\tilde{R}$ ($(j, i) \in \tilde{R}$ ssi $(i, j) \in R$, identiquement) est aussi une relation d'évacuation.

– Quelque soit $(i, j) \in E$ la restriction de R à $(I \setminus i) \times (J \setminus j)$ est encore une relation d'évacuation.

Nous etablissons maintenant une deuxième propriété du plan a dont l'énoncé utilise le fait que S est une relation d'évacuation ou plus exactement une notation déduite de ce fait. Soit donc $R \subset I \times J$ une relation d'évacuation quelconque contenant la bijection E. Pour chaque paire $(i, j) \in R \setminus E$ nous appelons I–*successeur* de i (selon j) l'élément $i_j^+ = \mathrm{Max}\ \{i' \in {}^{f} R_1 : i' < i\}$ et, de même, J–*successeur* de j (selon i) l'élément $j_i^+ = \mathrm{Max}\ \{j' \in i\, R_2 : j' < j\}$. Ces deux éléments existent toujours en raison de l'hypothése que $(i, j) \notin E$.

III.2. Le plan a satisfait la relation de *symétrie locale* suivante:

(S_y). Pour chaque $(i, j) \in S \setminus E$ on a $(j, j_i^+)\, a = (i_j^+, j)\, a$.

Preuve. En raison de la façon dont les points sont indexés sur les trajectoires, ceci équivaut à l'assertion suivante:

Si v et v' sont deux points immédiatement consécutifs sur une trainée V_i ces deux points sont aussi immédiatement consécutifs sur la trajectoire de la piéce $v\alpha_i$.

Mis sous cette forme l'énonce est donc une conséquence immédiate de la définition de l'action $\alpha_i \to \alpha_i V_i$ qui « déplace » la piéce $v\alpha_i$ de la case v à la case v'. Q.E.D.

Il reste encore une propriété caractéristique à vérifier. Considérant une fonction $b : I \times J \to P$ quelconque assujétie à la seule consition que $(i, \dot{J})\, b \neq \varnothing$ et $(I, j)\, b \neq \varnothing$ pour chaque paire (i, j), nous appelons I-*application* de b l'application envoyant chaque $i \in I$ sur $(i, \mathrm{Max}\,(i\, R_2))\, b$, où R designe le support de B. De même la J-*application* de b envoye chaque $j \in \dot{J}$ sur $(\mathrm{Max}\,(j\, R_1), j)\, b$.

Nous avons vu au début de cette section que la fonction initiale à évacuer $\alpha : D \to J$ ($D = \mathrm{Dom}\,(\alpha)$) (et qui est par définition une bisection) est l'inverse de la J-application du plan a. Cette derniére est donc aussi une bijection. En ce qui concerne la I-application de a elle envoye chaque indice $i \in I$ sur le premier élément v_i ($= \alpha_i^{-1}\ \mathrm{Max}\,(V_i \alpha_i)$) de la trainée V_i: c'est aussi une bijection $I \to D$ puisque, d'après la définition de l'action $\alpha_i \to \alpha_i V_i$, ce point v_i n'appartent pas au domaine de $\alpha_i V_i$, ni par conséquent, à celui des fonctions $\alpha_{i'}$ pour $i' < i$.

Nous établissons maintenant la réciproque.

III.3. Soit $b : I \times J \to P$ une fonction d'image D satisfaisant les trois conditions suivantes:

(1) Son support R est une relation d'évacuation;

(2) La condition de symétrie locale (S_y).

(3) Sa J-application γ est une bijection $J \to D$.

Il existe une évacuation B de la fonction initiale $\beta = \gamma^{-1}$ dont b est le plan.

Preuve. L'enoncé est trivial quand $m = \mathrm{Card}\,(J) = \mathrm{Card}\,(\dot{I}) = \mathrm{Car}\,(D)$ est égal à un. Nous pouvons donc procéder par induction sur $m \geq 2$. Pour simplifier l'écriture nous supposons que $\dot{I} = \dot{J} = [m]$. Le maximum de I est donc m et, E étant la relation bijective contenue dans le support R de b nous désignons par j^* le minimum de mR_2, c'est à dire l'élément mE_2. Posant $I' = I \setminus \{m\} = [m - 1]$ et $J' = J \setminus \{j^*\}$ nous notons b' la restriction de b à $I' \times J'$. Ou sait déjà que le support R' de b' est une relation d'évacuation (sur $I' \times J'$) et il est immédiat que b' satisfait la condition de symétrie locale (S_y). Il nous suffit donc de vérifier que la J'-application γ' de b' est une bijection

$J' \to D'$ où $D' \subset D$ et que son inverse γ'^{-1} est précisement égale à $\beta' = \beta V_m$ où V_m designe la trainée pour β dont l'ensemble de points est l'ensemble $(m\ ,\ J)\ b$, c'est à dire l'ensemble $mR_2\ \gamma$ d'aprés la définition de γ et $m = \mathrm{Max}\ (I)$.

De nouveau ceci est trivial quand mR_2 se réduit au singolet $\{j^*\}$ car dans ce cas D' est égal à D privé du point $(m\ , j^*)\ b = j^*\ \gamma$ et γ' est la restriction de γ à J' c'est à dire l'inverse de la restriction de β à D'. Nous supposons donc désormais que $mR_2 = \{j_1 > j_2 > \cdots > j_s = j^*\}$ où $s \geq 2$. Ou a $V_m = (V_k = J_k\ \gamma : h = 1, 2, \cdots, s)$ et la J'–application γ' de b' est définie par les relations suivante pour chaque $j \in J' : j\gamma' = j\ \gamma$ si $j \notin mR_2$;

$$= (m_1^+\ , j)\ b \quad \text{si} \quad j \in mR_2 \setminus \{j^*\}.$$

D'aprés la condition de symétrie locale on a identiquement $(m_i^+\ , j)\ b = (m\ , j_m^+)\ b$ dans le deuxiéme cas ce qui équivant à la condition que $\gamma^{1-1} = (\gamma^{-1})\ V_m$ et ceci établit l'énoncé. Q.E.D.

Une discussion un peu plus longue permet de montrer que la donnée d'une relation d'évacuation $R \subset I \times J$ et d'une bisection $\gamma : J \to D$ suffit pour déterminer de façon unique une fonction $b : I \times J \to D$ de support R et de J–application γ qui satisfasse les condition de symétrie locale et qui soit donc comme ou vient de le voir le plan d'une évacuation (necessairement unique) de la fonction initiale $\gamma^{-1} : D \to \dot{J}$. Nous n'autores pas besoin de ce résultat et nous passons directement à notre enoncé principal.

III.4. *Propriété de dualité.* Il existe une *involution* envoyant chaque $\dot{I}$–évacuation A d'image $\dot{J}$ sur l'unique $\dot{J}$–évacuation B d'image I dont la suite des trainés est la suite des trajectoires de A.

Preuve. Soit $\tilde{a}$ la transposée de plan a de A (c'est à dire $\tilde{a}\ (j\ , i) = a\ (i\ , j)$ identiquement). Etant donnée la symétrie de conditions (1) et (2) de III. 3, celles–ci sont satisfaites par $\tilde{a}$ puisquélles le sont par a. De plus on a vu plus haut que la I–application de a est une bisection γ sur $Im(a)$. Par conséquent, d'aprés III. 3, (eu échangeau I et J), $\tilde{a}$ est le plan d'une évacuation B de la fenction initiale γ^{-1} et il est clair que cette opération A $\to$ B est une involution échangeant les trainés et les trajectoires. L'unicité est évidente.

Q.E.D.

Nous appelerons B l'*évacuation transposée* de A et β la *fonction adjointe* de A. Il est commode pour les applications d'expliciter certaine des notions qui sont préservées ou échangées dans cette involution. En particulier, appelons *transitions de* A les paire de points qui sont consécutifs sur au moins une des trainés de A et *points finaux* les points qui sont le dernier point d'au moins une des trainées de A.

Appelons aussi (abusivement) *permutation* de A l'application π_A envoyant chaque $i \in I$ sur l'image par α, de dernier point de la trainée V_i, c'est à dire sur $\mathrm{Min}\ (V_i\ \alpha_i)$.

III.5. L'évacuation A et sa transposée B ont les même transitions, et les mêmes points finaux et leurs permutations sont deux bijectiones inverses l'une de l'autre.

Prevue: Ceci est clair en ce qui concerne les transitions car sous cette forme l'enoncé est un cas particulier de la condition de symétrie locale. En ce qui concerne les points finaux et les permutations, il suffit d'observer que π_A est simplement la bijection $i \to iE_2$ où E est la bisection contenue dans le support de plan a de A et que l'ensemble des points finaux de A et de B est l'ensemble $Ea = \{(i,j)\, a : (i,j) \in E\}$. Q.E.D.

Une autre formulation utile résulte de la consideration par chaque I-évacuation $A = (\alpha_m, \alpha_{m-1}, \cdots, \alpha_1)$ de l'*évacuation derivée* $A' = (\alpha_{m-1}, \cdots, \alpha_1)$ dont la fonction initiale α_{m-1} est la deuxiéme fonction de A. Pour obtenir une notion duale, soient $j^* = \mathrm{Max}(J)$ et $J' = J \setminus j^*$. A chaque fonction α_i de A nous pouvons associer une autre fonction α_i^* par la condition que pour chaque point p on ait $p\,\alpha_i^* = p\alpha_i \setminus \{j^*\}$ c'est à dire $p\alpha_i^* = p\alpha_i$ si $p\alpha_i \neq j^*$ et $= \varnothing$ sinon. Cette correspondance envoye sur O l'une de fonctions de la suite A et nous notons A* la suite de fonctions (α_i^*) privée de cette dernière. A* sera appelée la restriction de A.

III.6. La restriction A* de la I–évacuation A est une évacuation dont la transposée est la dérivée B′ de la transposée B de A.

Preuve. Il suffit de vérifier que A* est l'évacuation dont le plan est la restriction de plan a de A à l'ensemble $(I \setminus i_*) \times (J \setminus j^*)$ où $j^* = \mathrm{Max}(J)$ et où $i_* = J^* E$. Q.E.D.

IV. Evacuations ordonnées

En vue d'applications évidentes nous supposons désormais que l'ensemble de base P est muni d'une relation d'ordre (partiel) fixe notéé $\leq$. Par abus de langage nous appelerons *morphisme* toute fonction $\varphi : P \to [n]$ telle que pour deux points p, p' de son domaine la relation $p \leq p'$ implique $p\varphi \leq p'\varphi$.

Considérons maintenant le deux conditions suivantes sur une I–évacuation A de la bijection initiale $\alpha : D \to J$:

(Morph). Toute les fonctions α_i de A sont des morphismes.

(Max). Le premier point de chaque trainée V_i est un point maximal du domaine de α_i.

On voit sans peine que la condition (Max) équivaut à l'hypothése que tous les ensembles $\mathrm{Dom}(\alpha_i)$ $(i \in I)$ sont des *idéaux* de D c'est à dire que $\mathrm{Dom}(\alpha_i)$ contient tous les points $p' \in D$ tels que $p' \leq p$ pour au moins un point $p \in \mathrm{Dom}(\alpha_i)$. Une propriété plus interessante est la suivante.

IV.1. L'évacuation A satisfait la condition (Max) ssi sa fonction adjointe β est un morphisme.

Preuve. Par définition, β est la bijection de D sur I telle que pour chaque $i \in I$, le point $v_i = i\,\beta^{-1}$ soit le premier point de la trainée V_i. L'énoncé en resulte puisque (Max) équivant à la condition que pour chaque paire d'indices i et i' la relation $v_i \leq v_{i'}$ entre les premiers éléments des deux trainées V_i et $V_{i'}$ entraine que l'ou ait $i \leq i'$. Q.E.D.

Nous appelerons *evacuation ordonnée* toute évacuation $A=(\alpha_m, \alpha_{m-1}, \cdots, \alpha_1)$ satisfaisant à la fois les deux conditions (Morph) et (Max). Nous notons que ceci est réalisé de façon triviale quand $m = 1$ et que quand A est ordonnée il en est de même de sa derivée $A' = (\alpha_{m-1}, \cdots, \alpha_1)$ (dans la terminologie de l'énoncé III. 6) d'aprés la structure même des conditions (Morph) et (Max).

Sous cette même hypothése, la restriction A^* de A est aussi ordonnée puisque d'une part la restriction d'un morphisme est un morphisme et que, d'autre part, le premier point v_i^* de chaque trainée V_i^* de A^* est maximal dans Dom (α_i^*) d'aprés l'a double hypothése qu'il en est de même du premier point de V_i et que α_i est un morphisme.

Cette observation nous permet d'etablir la proprieté suivante.

IV. 2. La classe des évacuations ordonnées est fermée par transposition.

Preuve. Supposons que $A = (\alpha_m, \cdots, \alpha_1)$ soit ordonnée est soit $B = (\beta_m, \cdots, \beta)$ l'évacuation transposée. D'aprés IV. I. β_m est un morphisme et d'aprés le dual de cet enouncé, B satisfait la condition (Max) puisque α_m est un morphisme. Maintenant, d'aprés III. 6, l'evacuation transposés de $B'=(\beta_{m-1}, \cdots \beta_1)$ est la restriction A^*.

Comme cette derniére est une évacuation ordonnée, une induction sur m montre que toutes les fonctions de B' sont des morphismes ce qui achéve les preuve. Q.E.D.

Reprinted from ADVANCES IN MATHEMATICS
Vol. 19, No. 3, March 1976
Printed in Belgium

On Pseudovarieties

SAMUEL EILENBERG* AND M. P. SCHÜTZENBERGER

Columbia University and University of Paris VII

DEDICATED TO GARRETT BIRKHOFF

Birkhoff's Theorem [1] asserts that a family of algebras is an equational variety if and only if the family is closed under the operations of passing to subalgebras and quotient algebras and also under arbitrary direct products. The objective of this paper is to study what happens to this notion and the theorem above if one restricts ones attention to finite algebras only. This is motivated by applications to the theory of automata.

In the body of the paper, we shall only consider monoids. At the end, we shall remark how the results can be extended to more general species of algebras.

A family $\mathbf{V}$ of finite monoids is called a *pseudovariety* if the following conditions hold

(1) If $S \in \mathbf{V}$ and T is a submonoid of S, then $T \in \mathbf{V}$.

(2) If $S \in \mathbf{V}$ and T is a homomorphic image of S, then $T \in \mathbf{V}$.

(3) If $S, T \in \mathbf{V}$, then $S \times T \in \mathbf{V}$.

There are two points in which this definition differs from that of a (Birkhoffian) variety. One is that all the monoids in $\mathbf{V}$ are assumed to be *finite*. The second one (implied by the first) is that $\mathbf{V}$ is closed only under finite direct products. For example finite groups form a pseudovariety, but groups do not form a variety of monoids. Indeed, a submonoid of an (infinite) group need not be a group. It should however be noted that a finite monoid S is a group if and only if, for all n sufficiently large, and for all $x \in S$, the equation

$$x^n = 1$$

* Research partially supported by NSF Grant DCR 72-03703 A01.

holds, where $\bar{n}$ is the least common multiple of all the integers $1 < i \leqslant n$. The objective of this paper is to show that such a phenomenon holds for all pseudovarieties.

Let Ξ^* be the free monoid generated by the infinite sequence of letters $x_1, \ldots, x_n, \ldots$ and let $u, v \in \Xi^*$. We shall say that a monoid S *satisfies* (u, v) (or that the equation $u = v$ *holds* in S) if $u\varphi = v\varphi$ for every morphism $\varphi: \Xi^* \to S$. Finite monoids satisfying (u, v) clearly from a pseudovariety that we shall denote by $\mathbf{V}(u, v)$.

Given a sequence of pairs

$$(u_i, v_i) \in \Xi^* \times \Xi^*, \qquad i \geqslant 1,$$

we may consider two pseudovarieties

$$\mathbf{V}' = \bigcap_{i=1}^{\infty} \mathbf{V}(u_i, v_i),$$

$$\mathbf{V} = \bigcup_{k=1}^{\infty} \bigcap_{i=k}^{\infty} \mathbf{V}(u_i, v_i).$$

A (finite) monoid is in $\mathbf{V}'$ if it satisfies all of the equations $u_i = v_i$, while it is in $\mathbf{V}$ if it satisfies the equations $u_i = v_i$ for all i sufficiently large. We shall say that $\mathbf{V}'$ is *defined* by the equations $u_i = v_i$, and that $\mathbf{V}$ is *ultimately defined* by the equations $u_i = v_i$.

Our main result is

THEOREM 1. *Each nonempty pseudovariety* $\mathbf{V}$ *is ultimately defined by a sequence of equations.*

We denote by Ξ_n^* the submonoid of Ξ^* generated by the letters $x_1, \ldots, x_n$. In Ξ_n^*, we shall consider congruences. Such a congruence $\sim$ in Ξ_n^* is said to be finite provided the quotient monoid $\Xi_n^*/\sim$ is finite. An important fact in the proof of Theorem 1 is

PROPOSITION 2. *A finite congruence* $\sim$ *in* Ξ_n^* *is finitely generated, i.e., there exists a finite set* $W \subset \Xi_n^* \times \Xi_n^*$ *such that* $u \sim v$ *for all* $(u, v) \in W$, *and such that* $\sim$ *is the smallest congruence with this property.*

Proof. Since the congruence $\sim$ is finite, there exists an integer $k > 0$ such that each congruence class contains an element w with length $|w| < k$. Define

$$W = \{(u, v) \mid u \sim v, |u| \leqslant k, |v| < k\}.$$

Clearly, card $W < (1 + n)^{2k-1}$. Let $\equiv$ be the congruence generated by W. Clearly, $u \equiv v$ implies $u \sim v$. To prove the opposite implication, we need the following assertion

(4) For each $w \in \Xi_n^*$, there exists $w' \in \Xi_n^*$ such that $|w'| < k$ and $w \equiv w'$.

We prove this by induction with respect to $|w|$. If $|w| < k$, there is nothing to prove since $(w, w) \in W$. Assume now that $l > k$ and that (4) holds for all w with $|w| < l$. Consider $w \in \Xi_n^*$, $|w| = l$. Then, $w = u\sigma$ with $|u| = l - 1$. Consequently $u \equiv u'$ for some u' with $|u'| < k$. This implies $w \equiv u'\sigma$. Since $|u'\sigma| = k$, the definition of W implies that $(u'\sigma, w') \in W$ for some w' such that $|w'| < k$. It follows that $w \equiv w'$ as required.

Now, assume $u \sim v$. By (4) we have $u \equiv u'$ and $v \equiv v'$ with $|u'| < k$, $|v'| < k$. Since $u' \sim v'$, it follows that $(u', v') \in W$ and thus, $u' \equiv v'$. Consequently, $u \equiv v$. This proves that $\sim$ and $\equiv$ coincide and thus, $\sim$ is finitely generated.

Having proved Proposition 2, we now proceed with the proof of Theorem 1.

We first construct a sequence

$$S_1, S_2, \ldots, S_n, \ldots,$$

in $\mathbf{V}$ with the following two properties

(5) S_n is isomorphic to a quotient of S_{n+1}.

(6) If $S \in \mathbf{V}$, then S is isomorphic to a quotient of S_n for some $n \geqslant 1$.

To construct such a sequence, we write a sequence $T_1, T_2, \ldots, T_n, \ldots$, which contains all the elements of $\mathbf{V}$ up to an isomorphism, and then define $S_n = T_1 \times \cdots \times T_n$.

For each $n \geqslant 1$, we define the congruence $\sim_n$ in Ξ_n^* as follows: $u \sim_n v$ iff $u\varphi = v\varphi$ for all morphisms $\varphi: \Xi_n^* \to S_n$. Consider the quotient monoid V_n[3] of Ξ_n^* by the congruence $\sim_n$. The following facts are clear

(7) V_n is isomorphic to a submonoid of some finite product of S_n with itself.

This implies

(8) $V_n \in \mathbf{V}$.

Since V_n is finite, Proposition 2 may be applied to the congruence

$\sim_n$, yielding a finite set $W_n \subset \Xi_n^* \times \Xi_n^*$, such that $\sim_n$ is generated by W_n. Since Ξ_n^* is a subset of Ξ^*, we obtain the countable set

$$W = \bigcup_{n=1}^{\infty} W_n$$

in $\Xi^* \times \Xi^*$. We assert that W ultimately defines $\mathbf{V}$.

First, assume that $S \in \mathbf{V}$. Since S is isomorphic to a quotient of S_n for some $n \geqslant 1$, and since S_n satisfies the equations W_n, it follows that S satisfies the equations W_n. However, S_n is isomorphic to a quotient of S_{n+k} for all $k \geqslant 0$ and thus, S also satisfies all the equations W_{n+k} for all $k \geqslant 0$. Thus, S satisfies all but a finite number of equations in W.

Conversely, assume that S is a finite monoid satisfying all but a finite number of equations in W. Choose $n \geqslant 1$ with the following two properties

(9) $n \geqslant \operatorname{card} S$,

(10) S satisfies the equations W_n.

Let

$$\varphi: \Xi_n^* \to S,$$

be a surjective morphism. If $(u, v) \in W_n$, then $u\varphi = v\varphi$ since S satisfies the equation $u = v$. Since the pairs (u, v) in W_n generate the congruence $\sim_n$, it follows that $u \sim_n v$ implies $u\varphi = v\varphi$. This implies that φ admits a factorization

$$\Xi_n^* \longrightarrow V_n \xrightarrow{\psi} S,$$

and that ψ is a surjective morphism. Since $V_n \in \mathbf{V}$, it follows that $S \in \mathbf{V}$. This concludes the proof of Theorem 1.

A pseudovariety $\mathbf{V}$ is said to be *equational* if it is defined by a family of equations. This holds if and only if $\mathbf{V}$ is the class of all finite monoids in some (Birkhoffian) variety of monoids. However, two distinct varieties may yield the same pseudovariety.

An immediate consequence of Theorem 1 is

COROLLARY 3. *Each pseudovariety is the union of an ascending sequence of equational pseudovarieties.*

A pseudovariety $\mathbf{V}$ is said to be *finitely generated*, if there exists a finite sequence of monoids $M_1, \ldots, M_k$ such that $\mathbf{V}$ is the smallest

pseudovariety containing $M_1, \ldots, M_k$. Replacing this sequence by the single monoid $M = M_1 \times \cdots \times M_k$, shows that each finitely generated pseudovariety is generated by a single monoid M. A consequence of Corollary 3 is

COROLLARY 4. *Each finitely generated pseudovariety is equational.*

The remarks above lead in a natural way to consider the following two properties of a finite monoid M

(11) The variety generated by M is defined by a finite number of equations.

(12) The pseudovariety generated by M is defined by a finite number of equations.

The implication (11) $\Rightarrow$ (12) is clear. Whether the implication (12) $\Rightarrow$ (11) holds is an open question. Oates and Powell [3] have shown that (11) holds for any finite group. This easily implies (12) for any finite group. Perkins [4] has constructed a monoid containing six elements for which (11) fails. It is an open question whether (12) holds for this monoid. Perkins' monoid may be described as the monoid of all partial functions $f: \{0, 1\} \to \{0, 1\}$, but excluding the two constant functions and the function that interchanges 0 and 1.

Although we have limited our attention to monoids, the entire development can be carried out for any algebraic theory based on a finite number of finitary operations. The role of Ξ^* and Ξ_n^* is then taken over by the free algebras generated by $x_1, \ldots, x_n, \ldots$, and by $x_1, \ldots, x_n$. For $u \in \Xi^*$ or $u \in \Xi_n^*$, the integer $|u|$ must be defined in such a way that the proof of Proposition 2 remains valid. A fact needed in this proof is the finiteness of the sets $\{u \mid u \in \Xi_n^*, |u| \leqslant k\}$. This follows from the assumption that there is only a finite number of basic operations.

Pseudovarieties of monoids and of semigroups have applications in the theory of automata. The interested reader is referrred to Eilenberg [2], where the ultimate equations of many interesting pseudovarieties are derived.

In connection with pseudovarieties of semigroups, the following interesting fact should be noted. Finite groups form a pseudovariety **G** of monoids. However, **G** is not a pseudovariety of semigroups because it does not contain the empty semigroup. If, however, the empty semigroup is adjoined to **G**, a pseudovariety **G'** of semigroups is obtained. Its ultimate equations are obtained by replacing each equation $x^n = 1$

used to ultimately define **G** by the pair of equations $x^{\bar{n}}y = y = yx^{\bar{n}}$. These new equations ultimately define **G′** as a pseudovariety of semigroups, and **G** as a pseudovariety of monoids. This method of eliminating the unit element is quite general.

References

1. Garrett Birkhoff, On the structure of abstract algebras, *Proc. Cambridge Phil. Soc.* **31** (1935), 433–454.
2. Samuel Eilenberg, "Automata, Languages and Machines, Vol. B," Academic Press, New York, 1976.
3. Sheila Oates and M. B. Powell, Identical relations in finite groups, *J. Algebra* **1** (1964), 11–39.
4. Peter Perkins, Bases for equational theories of semigroups, *J. Algebra* **11** (1968), 298–314.

Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium.

Semigroup Forum 13, 47-75 (1976)

RESEARCH ARTICLE

SUR LE PRODUIT DE CONCATENATION NON AMBIGU

M.P. Schützenberger

Communiqué par G. Lallement

I. INTRODUCTION

Cet article est une application des méthodes développées par S. Eilenberg [5, Vol B] pour caractériser certaines familles de semi-groupes au moyen de constructions sur les parties de semi-groupes ou de monoïdes libres. Nous nous permettrons dans cette introduction de rappeler quelques éléments des concepts et des notations de ce traité plutôt que d'y multiplier les références.

Une *variété* (de semi-groupes ou de monoïdes) est une famille d'objets contenant chaque *diviseur* (= objet quotient d'un sous objet) du produit direct de deux quelconques de ses membres. On notera la différence entre ce concept et celui de "variété au sens de Birkhoff". Pour nous limiter à des exemples qui interviendront par la suite, citons la variété des semi-groupes commutatifs, et celle des semi-groupes idempotents (qui sont toutes les deux des variétés au sens de Birkhoff), la variété de semi-groupes union de groupes finis (qui n'en n'est pas une), celle des semi-groupes finis G-triviaux (c'est-à-dire dans lesquels chaque G-classe est un singolet) en prenant pour G l'une quelconque des relations $\mathcal{J}$, $\mathcal{R}$, $\mathcal{L}$ ou $\mathcal{H}$ de Green.

La variété des semi-groupes $\mathcal{J}$-triviaux est caractérisée par un théorème profond de I. Simon [14] ; celles des semi-groupes $\mathcal{R}$ ou $\mathcal{L}$ triviaux jouent un rôle dans la théorie de la hiérarchie de J. Brzozowski ([1], [2]). Les semi-groupes $\mathcal{H}$-triviaux ont été introduits par R. Mc Naughton (cf. [8]). Nous suivrons S. Eilenberg qui les nomme *apériodiques*. L'objet du présent article sera la variété, notée $\underline{\underline{\mathrm{Df}}}$, des semi-groupes *finis* dont chaque $\mathcal{J}$-classe contenant un idempotent est un semi-groupe. Elle contient évidemment celle des semi-groupes finis dont chaque idéal principal idempotent est un idéal principal

à gauche (ou à droite) qui se rencontre dans la théorie de la complexité ([14]), et qui a été récemment étudiée par G. Lallement [6], [7].

Dans la première partie de cet article on examine quelques propriétés formelles des monoïdes de $\underline{\underline{Df}}$. En particulier on vérifie que $\underline{\underline{Df}}$ est l'ensemble des monoïdes *finis* d'une famille plus générale $\underline{\underline{D}}$ qui, de façon intuitive, est constituée par les semi-groupes dont la structure des idéaux n'est pas complètement oblitérée par passage à leur quotient commutatif (ou idempotent). Pour être plus précis, disons qu'un morphisme ϕ d'un semi-groupe S dans un semi-groupe T est *injectif sur les idéaux principaux idempotents* ssi deux tels idéaux de S sont égaux quand leurs images par ϕ engendrent le même idéal de T. On a alors la :

DEFINITION. $\underline{\underline{D}}$ est la famille des semi-groupes tels que le morphisme naturel sur leur plus grand quotient commutatif et idempotent soit injectif sur les idéaux principaux idempotents.

Cette condition est trivialement satisfaite par les semi-groupes idempotents et des théorèmes classiques de Clifford montrent que tous les semi-groupes commutatifs de même que les semi-groupes union de groupes appartiennent à $\underline{\underline{D}}$.

On distinguera dans $\underline{\underline{D}}$ la sous-famille $\underline{\underline{D}}1$ (resp. $\underline{\underline{D}}r$, resp. $\underline{\underline{D}}1r$) des semi-groupes dont la $\mathcal{J}$-classe de chaque idéal idempotent est une $\mathcal{L}$-classe (resp. $\mathcal{R}$-classe, resp. un groupe). Un autre cas particulier sera la famille $\underline{\underline{D}}^{o}$ des semi-groupes ayant un et un seul idéal idempotent qui est leur idéal minimum.

Ces considérations dépendent de façon essentielle de la théorie de la décomposition en semi-treillis de Tamura et Kimura [15], Yamada [20] et M. Petrich [10] à laquelle nous avons fait de larges emprunts

Venons-en aux monoïdes libres.

Rappelons que si $X, Y, \ldots$ sont des parties d'un semi-groupe S on note X^{+} (resp. $X^{*} = \{1\} \cup X^{+}$) le sous semi-groupe (resp. sous monoïde) engendré par X ; $XY = \{xy \in S : x \in X, y \in Y\}$ $X^{-1}YZ^{-1} = \{s \in S : Y \cap XsZ \neq \emptyset\}$. Suivant Eilenberg, un sous semi-groupe P de S sera dit *unitaire* (en symbole $P \in \mathcal{U}(S)$) ssi $P^{-1}P = P \neq 0$; nous l'appellerons *bi-complet* ($P \in \mathcal{B}(S)$) ssi de plus $S = S^{-1}P$.

Enfin on sait qu'étant donnée une collection $\{X_i : i \in I\}$ de parties de S, il existe une congruence maximale sur S dont chaque X_i est une union de classes ; le quotient correspondant de S est le *semi-groupe syntaxique* $\mathrm{Synt}(X_i : i \in I)$ de la collection. Une partie X

est dite *reconnaissable* ssi Synt(X) est fini.

PROPRIETE 1. $\underline{\underline{Df}}$ est la plus petite variété $\underline{\underline{V}}$ qui contienne pour chaque alphabet fini A le semi-groupe syntaxique de tout sous semigroupe *reconnaissable unitaire bi-complet* $P \in \mathcal{B}(A^+)$ satisfaisant la condition supplémentaire :

(#). Chaque sous semi-groupe unitaire Q contenu dans P et tel que Synt(Q) soit un quotient de Synt(P) vérifie $(A^+)^{-1}Q \subset Q(A^+)^{-1}$.

On notera que si l'on remplace la condition $(A^+)^{-1}Q \subset Q(A^+)^{-1}$ par $A^+ = Q(A^+)^{-1}$ (resp. par $A^+ = (A^+)^{-1}Q$) on caractérise de la même façon la sous variété $\underline{\underline{D}}^o_f$ (resp. $\underline{\underline{D}}^o_f 1$) des semi-groupes finis dont tous les idempotents sont dans l'idéal minimum (resp. dans un idéal à gauche principal minimum).

Comme le semi-groupe syntaxique d'une partie d'un monoïde libre A^* est automatiquement un monoïde, on obtient une caractérisation des monoïdes de $\underline{\underline{Df}}$ en remplaçant partout A^+ par A^* dans l'énoncé précédent. En particulier la variété des groupes finis est obtenue en imposant la condition $A^* = Q(A^*)^{-1}$ dans (#), ainsi qu'on le vérifie facilement en prenant $Q = \{1\}$.

D'autre part, en utilisant les travaux de Y. Cesari [3] et de D. Perrin [8], on pourrait montrer que $\underline{\underline{D}}^o_f$ contient la variété engendrée par les semi-groupes syntaxiques des sous semi-groupes P de $\mathcal{B}(A^+)$ qui sont *finiment engendrés* et que cette dernière contient la variété des semi-groupes union de groupes de $\underline{\underline{D}}^o_f$.

La sous variété $\underline{\underline{Df}} \cap \underline{\underline{Ap}}$ des semi-groupes de $\underline{\underline{Df}}$ qui sont apériodiques (c'est-à-dire dont tous les groupes sont triviaux) admet une caractérisation plus immédiate. Il en est de même de la famille des monoïdes finis $\mathcal{R}$ (resp. $\mathcal{L}$) triviaux (qui sont les monoïdes apériodiques finis de $\underline{\underline{D}}1$ (resp. $\underline{\underline{D}}1r$).

Les énoncés de cette partie du travail sont indépendants des résultats obtenus au cours de la preuve de la Propriété 1. Suivant S. Eilenberg nous employons la notation $A^*\text{-}\underline{\underline{V}}$ pour désigner la famille des parties du monoïde libre A^* dont le monoïde syntaxique appartient à un ensemble donné $\underline{\underline{V}}$ de monoïdes.

Rappelons qu'un produit XY de deux parties d'un monoïde libre A^* est *non ambigu* ssi chaque a de A^* admet au plus une factorisation $a = xy$ avec $x \in X$ et $y \in Y$ et appelons *completion polynomiale non ambiguë* $UPol(\underset{\sim}{X})$ d'une famille $\underset{\sim}{X}$ de parties de A^* la plus petite famille $\underset{\sim}{Y}$ qui contienne $\underset{\sim}{X}$ et les parties suivantes :

(i) Chaque lettre a de A et chaque sousmonoïde B^* où $B \subset A$;

(ii) Chaque union *disjointe* $Y_1 \cup Y_2$ et chaque produit *non ambigu* $Y_1 Y_2$ où $Y_1, Y_2 \in \underset{\sim}{Y}$.

Nous établirons la :

PROPRIETE 2. Pour chaque alphabet A, la famille $A^* - (\underline{\underline{D}}_f \cap \underline{\underline{A}}_p)$ est la plus petite famille de parties de A^* égale à sa complétion polynomiale non ambiguë.

On peut imposer au produit XY des conditions plus strictes que d'être non ambigu. Nous introduirons ainsi sans la section IV un "*produit déterministe*" et un "*produit bidéterministe*" et les complétions polynomiales correspondantes.

En application directe de la théorie des produits en couronne de J. Rhodes et de Bret Tilson ([14] [12], [13], [16], [17]) on obtiendra l'énoncé suivant dans lequel $\underline{\underline{G}}$ est une variété donnée de groupes finis et, où par abus de notations, $\underline{\underline{G}}\ \underline{\underline{D1}}$ (resp. $\underline{\underline{G}}\ \underline{\underline{D1r}}$) désigne la famille des monoïdes finis de $\underline{\underline{D1}}$ (resp. de $\underline{\underline{D1r}}$) dont tous les groupes appartiennent à $\underline{\underline{G}}$.

PROPRIETE 3. Pour chaque alphabet A, $A^*-\underline{\underline{G}}\ \underline{\underline{D1}}$ (resp. $\underline{\underline{A}}^*-\underline{\underline{G}}\ \underline{\underline{D1r}}$) est la plus petite famille $\underset{\sim}{X}$ de parties de A^* qui soit égale à sa complétion polynomiale déterministe (resp. bidéterministe) et qui contienne chaque intersection de la forme $X \cap Y$ où $X \in \underset{\sim}{X}$ et $Y \in A^*-\underline{\underline{G}}$.

Ceci suggère la question plus intéressante suivante qui se rattache à la théorie des semi-groupes orthodoxes de Clifford. Dans celle-ci $\mathrm{Pol}\ (A^*- \underline{\underline{G}})$ désigne la plus petite algèbre booléene de parties de A^* contenant le produit (de concaténation) de deux de ses membres et chaque partie finie dont le monoïde syntaxique est un groupe de la variété $\underline{\underline{G}}$.

Est-ce que $\mathrm{Pol}\ (A^*- \underline{\underline{G}}) = A^*- \underline{\underline{G}}\ \underline{\underline{E}}$ où $\underline{\underline{G}}\ E$ désigne la variété des monoïdes finis dont les groupes sont dans $\underline{\underline{G}}$ et dont les idempotents engendrent un sous monoïde apériodique ?

II. GENERALITES

Pour des raisons de commodité typographiques tous les énoncés de cette section sont formulés dans le langage des monoïdes. Ils s'appliquent aussi bien à un semi-groupe quelconque en considérant celui-ci comme l'idéal propre maximal du monoïde formé en lui adjoignant un

un élément neutre.

Nous réservons la notation $\xi = \xi_S$ pour désigner pour chaque semi-groupe S le morphisme naturel de celui-ci sur son plus grand quotient commutatif et idempotent, c'est-à-dire sur $S/\equiv$ où $\equiv$ est la plus petite congruence sur S telle que l'on ait identiquement $ss' \equiv s's$ et $s \equiv s^2$ $(s,s' \in S)$.

Une partie X d'un monoïde M est dite consistante ssi $M^{-1}XM^{-1} \subset X$ c'est-à-dire ssi toute relation $mm'm'' \in X$ implique $\{m,m',m''\} \subset X$ $(m,m',m'' \in M)$; elle est dite *fermée par conjugaison* (ou "reflexive" selon Clifford) ssi pour chaque $m \in M$ on a $m^{-1}X = Xm^{-1}$; enfin on pose $\sqrt{X} = \{m \in M : X \cap m^+ \neq \emptyset\}$ où, on le rappelle, $m^+ = \{m,m^2,\ldots, m^n,\ldots\}$ est le sous semi-groupe engendré par m.

L'énoncé suivant résume les propriétés du morphisme $\xi = \xi_M$ qui nous serviront par la suite. Dans celui-ci M est un monoïde quelconque.

II.1. (1) Chaque classe d'équivalence E de la congruence $\equiv$ est un semi-groupe $E = \sqrt{E}$, fermé par conjugaison et contenant chaque J-classe qu'il rencontre ;

(2) Un sous-monoïde unitaire P de M est une union de $\equiv$ classes ssi il est consistant.

PREUVE. (1) Comme $m \equiv m^2$ identiquement, chaque classe E est égale à $\sqrt{E}$; en outre $m \equiv m'$ implique $m \equiv m^2 \equiv mm'$ et E est donc un semi-groupe ; enfin E est fermé par conjugaison d'après l'identité $mm' \equiv m'm$.

Il est trivial que les J-classes de $M\xi = M/\equiv$ sont précisément les éléments de ce monoïde. Comme tout morphisme de M envoye chaque J-classe D de M dans une partie d'une J-classe de l'image, il en résulte que $D\xi$ est un élément de $M\xi$ ce qui achève la preuve de (1).

(2) Soit P un sous-monoïde unitaire de M. S'il est une union de $\equiv$ classes, chaque relation $m'm \in P$ implique que $m'mm \in P$ donc que $m \in (m'm)^{-1}(m'mm) \subset P^{-1}P$ appartienne à P. On a de même $mm' \in P$ d'où $m' \in m^{-1}P \subset P$ ce qui montre que P est consistant. Réciproquement si P est consistant et si $m_1m_2m_3m_4 \in P$ on a $m_1, m_2, m_3, m_4 \in P$, d'où $m_1m_3m_2m_4 \in P$. On vérifie de même que $m_1m_2m_3 \in P$ ssi $m_1m_2m_2m_3 \in P$ ce qui montre que P contient chaque

Ξ -classe qu'il rencontre.

Q.E.D.

Nous désignons par Jid = Jid(M) la famille des J-classes D de M qui engendrent un idéal idempotent. En application des remarques précédentes on a :

II.2. Deux conditions nécessaires et suffisantes équivalentes pour que M appartienne à la famille $\underline{\underline{D}}$ sont :
(1). $D \to D\xi$ est une injection de Jid(M) dans $M\xi$:
(2). Il existe un semi-groupe T de $\underline{\underline{D}}$ et un morphisme $\phi : M \to T$ qui est injectif sur les idéaux idempotents.

PREUVE. (1) Résulte immédiatement de l'énoncé précédent puisque $Jid(M\xi) = M\xi$. Pour vérifier (2) rappelons qu'un idéal principal est idempotent ssi sa J-classe D satisfait $DD \cap D \neq \emptyset$, ce qui montre que tout morphisme $\phi : M \to T$ induit une application de Jid(M) dans Jid(T). D'autre part le caractère naturel des morphismes ξ_M et ξ_T fait qu'il existe un morphisme Ψ de $M\xi_M$ dans $T\xi_T$ tel que $\phi\xi_T = \xi_M\psi$. Par conséquent si $T \in \underline{\underline{D}}$ et si ϕ est injectif sur les idéaux principaux idempotents, le morphisme ξ_M doit être une injection de Jid(M) dans $M\xi_M$ et par conséquent M appartient à $\underline{\underline{D}}$. La condition (2) est donc suffisante. On vérifie qu'elle est trivialement nécessaire en prenant $T = M\xi_M$ et $\phi = \xi_M$.

Q.E.D.

II.3. Une condition nécessaire et suffisante pour qu'une partie non vide D de M soit l'idéal minimum d'un sous monoïde consistant I de M est qu'elle soit à la fois une J-classe et un semi-groupe. On a alors $P = D^{-1}D = DD^{-1}$.

PREUVE. (1). La condition est nécessaire car, d'une part chaque idéal minimum d'un sous monoïde de M est un semi-groupe, et d'autre part, d'après II.1(2), chaque J-classe d'un sous monoïde consistant de M est une J-classe de M.

(2) Réciproquement, soit D une J-classe de M. D est l'intersection de l'idéal MDM avec l'ensemble $C = M^{-1}D\,M^{-1}$ des éléments de M qui engendrent un idéal contenant MDM. Ce deuxième ensemble C est consistant.

Posons $P = D^{-1}D$ et soit $p \in P$. Il existe $d \in D$ pour lequel $dp \in D$. Si $p = mm'$ on a $(dm)\,m' \in D$ donc $dm \in MDM \cap C = D$ ce qui montre que $m \in P$ et $m' \in (dm)^{-1}D \subset D^{-1}D$, établissant ainsi qu

P est consistant.

Supposons désormais que la J-classe D est un semi-groupe. On a $D \subset P$ puisque $DD \subset D$. De plus chaque relation $dp \in D$ $(d \in D)$ entraîne $dpD \subset DD \subset D$ donc $pD \subset MDM \cap C = D$ et l'on a donc la double inclusion $PD \subset D \subset P$.

Il en résulte que P est un semi-groupe car si $p, p' \in P$, $d \in D$ et $dp \in D$, on a $dpp'D = (dp)(p'D) \subset DD \subset D$ d'où $pp'D \subset d^{-1}D \subset P$ et enfin $pp' \in P$ puisque P est consistant.

Maintenant, le fait que D soit une J-classe dans M et que $P \subset M^{-1}D\,M^{-1}$ entraîne qu'elle soit une J-classe dans P. Comme $DD \subset PD \subset D$, D est l'idéal minimum de P et la relation $P = DD^{-1}$ découle de $PD \subset D$, par symétrie gauche-droite.

Q.E.D.

II.4. Soit M un monoïde tel que chaque m^+ $(m \in M)$ rencontre au moins une classe de Jid(M). Chacune des deux conditions suivantes est nécessaire et suffisante pour que $M \in \underline{\underline{D}}$.

(1) $D \to D\xi$ est une bijection de Jid(M) sur $M\xi$.

(2) Chaque classe de Jid(M) est un semi-groupe.

PREUVE. (1) Ceci résulte immédiatement de II.2(1) et de l'hypothèse supplémentaire sur M, puisque cette dernière entraîne que l'image inverse de chaque élément de M rencontre au moins une classe de Jid(M).

(2) Si $D \in$ Jid(M) n'est pas un semi-groupe, il existe $d,d' \in D$ tels que pour chaque $n \geq 1$ l'idéal principal $M(dd')^nM$ soit une partie *propre* de MDM. Comme $(dd')^n\xi = D\xi$, on en déduit immédiatement que sous l'hypothèse supplémentaire faite sur M, la condition (2) est nécessaire pour que M appartienne à $\underline{\underline{D}}$. Réciproquement, si chaque classe D de Jid(M) est un semi-groupe, l'énoncé précédent montre que $D \to D^{-1}D$ est une injection de Jid(M) dans la famille des sous-monoïdes consistant de M, donc d'après II.1.2., que $D \to (D^{-1}D)\xi \cap D\xi = D\xi$ est une injection de Jid(M) dans $M\xi$ et par conséquent que M appartient à $\underline{\underline{D}}$.

Q.E.D.

Comme les J-classes des idéaux idempotents des semi-groupes commutatifs sont des groupes, ainsi qu'il est bien connu, l'énoncé précédent montre que $\underline{\underline{D}}$ contient tous ces semi-groupes. Il en est de même pour les autres familles mentionnées dans l'introduction.

M.P. Schützenberger

Nous considérons maintenant exclusivement les semi-groupes S satisfaisant la condition suivante :

(Gp) Chaque semi-groupe s^+ $(s \in S)$ rencontre un groupe dans S .

Les théorèmes classiques de Clifford prouvent que chaque J-classe D d'un tel semi-groupe et une $\mathcal{D}$-classe complètement 0-simple. En particulier $DD \cap D \neq \emptyset$ (resp. $DD \subset D$) ssi D contient un groupe (resp. est une union de groupes).

Pour chaque $s \in S$ nous désignerons par s^ω l'idempotent du groupe (nécessairement unique) rencontrant s^+. Il est clair que $s^\omega = s^{n!}$ pour tout $n \in N$ assez grand quand tous les éléments des groupes dans S ont un ordre fini.

Nous rappelons la notation $\underline{D}^o$ pour désigner la famille des semi-groupes dont tous les idempotents sont contenus dans l'idéal minimum.

II.5. Soit M un semi-groupe satisfaisant (Gp). Il appartient à $\underline{D}$ ssi il admet une partition en semi-groupes fermés par conjugaison, satisfaisant (Gp) et appartenant à $\underline{D}^o$. Ces semi-groupes sont alors les classes de la congruence Ξ.

PREUVE. (1). Soit E une classe de Ξ. On a vu dans II.1(1) que $E = \sqrt{E}$ est un semi-groupe fermé par conjugaison qui contient chaque J-classe de M qu'il rencontre. Il satisfait donc (Gp) en même temps que M. Comme cette condition implique l'hypothèse supplémentaire de l'énoncé précédent et comme, trivialement, chaque idempotent est contenu dans la J-classe d'un idéal idempotent, ce même énoncé montre que si $M \in \underline{D}$, il existe exactement une classe D de $Jid(M)$ qui soit contenue dans E et que tous les idempotents de E se trouvent dans D. D'après II.3. D est l'idéal minimum de $P = D^{-1}D$ donc de E puisque $D \subset E \subset P$.

La condition énoncée est donc nécessaire.

(2) Réciproquement soit E un composant d'une partition $\{E_i : i \in I\}$ de M en semi-groupes. Ceci implique que $E = \sqrt{E}$. Si de plus chaque E_i satisfait (Gp) chaque élément m de M appartient au composant E_i qui contient l'idempotent m^ω. Donc E contient $\sqrt{G}$ pour chaque groupe G qui le rencontre.

Introduisons l'hypothèse que E est fermé par conjugaison et soient $u = u^2 \in E$ et D la J-classe de M contenant u. En raison de l'hypothèse que M satisfait (Gp), D est une $\mathcal{D}$-classe. Par conséquent pour chaque idempotent $v \in D$ on peut trouver $x \in uM \cap Mv$

et $y \in Mu \cap vM$ tels que $xy = u$, $yx = v$, donc $v \in E$ montrant que E contient tous les groupes dans D.

Faisant jouer la dernière condition que $E \in \underline{\underline{D}}^{o}$, on vérifie que l'union des groupes dans D est contenue dans l'idéal minimum de E. Donc D est cet idéal minimum (et par conséquent un semi-groupe). En outre E ne peut rencontrer aucune autre classe de $Jid(M)$ puisque chaque J-classe d'un sous semi-groupe de M est contenue dans une J-classe de M.

Supposons pour finir que ces deux conditions de fermeture par conjugaison et d'appartenance à $\underline{\underline{D}}^{o}$ sont satisfaites par chacun des composants E_i. Le raisonnement précédent montre que toutes les classes de $Jid(M)$ sont des semi-groupes, donc que $M \in \underline{D}$.

(3) La construction qui vient d'être effectuée établit une bijection à travers $Jid(M)$ entre les E_i et les classes de la congruence Ξ. Comme tous les composants de ces deux partitions sont des semi-groupes fermés par $m \to m^{\omega}$ d'après l'hypothèse (Gp), on voit facilement que les E_i sont les classes de Ξ.

Q.E.D.

II.6. Soit M un semi-groupe satisfaisant (Gp). Il appartient à $\underline{\underline{D}}$ ssi il satisfait l'identité

$$((xy)^{\omega}\,(yx)^{\omega}\,(xy)^{\omega})^{\omega} = (xy)^{\omega} \qquad (x,y \in M).$$

Donc quand $M \in \underline{\underline{D}}$ tout semi-groupe quotient de M appartient aussi à $\underline{\underline{D}}$ et il en est de même de ceux de ses sous semi-groupes qui satisfont (Gp).

PREUVE. (1). Supposons que M appartient à $\underline{\underline{D}}$. Les deux idempotents $u = (xy)^{\omega}$ et $v = (yx)^{\omega}$ sont dans une même J-classe D. Comme celle-ci est une $\mathcal{D}$-classe complètement simple, le produit uvu appartient à la même R-classe et à la même L-classe que u, c'est-à-dire au groupe dont u est l'idempotent, ce qui établit l'identité.

(2). Réciproquement, supposons que celle-ci est satisfaite par M. Soit x un élément quelconque d'une classe D de $Jid(M)$. En raison de l'hypothèse (Gp), D est une $\mathcal{D}$-classe contenant des idempotents et d'après un théorème classique de Clifford on peut trouver $y \in D$ tel que $xy = u$ et $yx = v$ soient deux idempotents de D. On a donc $(xy)^{\omega} = u$; $(yx)^{\omega} = v$. L'identité entraîne que le produit $xy.yx.xy$, donc xx, soient contenus dans D. Puisque les conditions de Green sont satisfaites par M, les relations $x, x^2 \in D$ impliquent que x soit un élément d'un groupe. Donc D est une union

de groupes. La théorie classique de Clifford montre alors que D est un semi-groupe ce qui donne la conclusion cherchée que $M \in \underline{\underline{D}}$.

(3). Chaque identité satisfaite par M est aussi satisfaite par chaque quotient et chaque sous semi-groupe de M. Comme il est trivial que les quotients de M satisfont (Gp) la dernière partie de l'énoncé découle directement de la première.

Q.E.D.

Il est clair que le produit direct de deux semi-groupes de $\underline{\underline{D}}$ satisfaisant (Gp) a aussi ces deux propriétés.

C'est un théorème connu ([5]) que les semi-groupes de $\underline{\underline{D}}1$ (resp. de $\underline{\underline{D}}1r$), satisfaisant (Gp) sont caractérisés par l'identité $(xy)^{\omega}x^{\omega} = (xy)^{\omega}$ (resp. $(xy)^{\omega} = (yx)^{\omega}$). Par conséquent les familles $\underline{\underline{D}}_f$, $\underline{\underline{D}}_f1$ et $\underline{\underline{D}}_f1r$ sont des variétés.

Les énoncés suivants sont des cas particuliers de théorèmes beaucoup plus généraux dus à J. Rhodes [13] et développés par B. Tilson [17]. Nous rappelons la notation $\underline{\underline{D}}^o1$ pour la sous-famille des semi-groupes de $\underline{\underline{D}}^o$ dont tous les idempotents sont dans un idéal à gauche minimum et nous notons $\mathcal{L}id(M)$ la famille des $\mathcal{L}$-classes de M qui engendrent un idéal à gauche idempotent.

II.7. *Soient P un semi-groupe satisfaisant (Gp) et $\pi : P \to M$ un morphisme surjectif tel que $u\pi^{-1} \in \underline{\underline{D}}^o$ (resp. $\in \underline{\underline{D}}^o1$) pour chaque idempotent u de M. Le morphisme π induit une application bijective de $\mathcal{J}id(P)$ sur $\mathcal{J}id(M)$ (resp. $\mathcal{L}id(P)$ sur $\mathcal{L}id(M)$). Donc $P \in \underline{\underline{D}}$ quand $M \in \underline{\underline{D}}$.*

PREUVE. Il est clair que l'application induite par π est surjective. Il suffit donc de montrer que si les idempotents r et s de P sont tels que leurs images $u = r\pi$ et $s\pi$ appartiennent à la même $\mathcal{J}$-classe D (resp. $\mathcal{L}$-classe L) de M on a $r \in PsP$ (resp. $r \in Ps$) puisque, par symétrie entre r et s ceci entraînera que ces deux éléments appartiennent à la même $\mathcal{J}$-classe (resp. $\mathcal{L}$-classe) de P.

Soit E la $\mathcal{J}$-classe de $r = r^2$. Comme $r \in u\pi^{-1}$ où $u = u^2$, E est l'idéal minimum du semi-groupe $u\pi^{-1}$ puisque celui-ci appartient à $\underline{\underline{D}}^o$ par hypothèse. Donc $r \in PtP$ pour chaque $t \in u\pi^{-1}$. Si de plus, $u\pi^{-1} \in \underline{\underline{D}}^o1$ on a de même $r \in Pt$.

Si $s\pi$ est dans la même $\mathcal{J}$-classe (resp. $\mathcal{L}$-classe) que u il existe $m,m' \in M$ tels que $u = m.s\pi.m'$ (resp. $u = m.1\pi$). Comme π est surjectif on peut prendre des éléments quelconques $p \in m\pi^{-1}$ et

$p' \in m'\pi^{-1}$ et l'on obtient l'élément $t = p.s.p' \in u\pi^{-1} \cap PsP$ (resp. $= ps \in u\pi^{-1} \cap Ps$) ce qui achève la preuve.

Q.E.D.

Nous rappelons enfin le cas particulier suivant des théorèmes généraux sur le produit en couronne.

II.8. Soient M un semi-groupe, S un semi-groupe de $\underline{\underline{D}}^o$ (resp. de $\underline{\underline{D}}^o 1$) satisfaisant (Gp) et π le morphisme naturel sur M du produit en couronne P de S dans M. Pour chaque idempotent u de M le semi-groupe $P_u = u\pi^{-1}$ appartient à $\underline{\underline{D}}^o$ (resp. à $\underline{\underline{D}}^o 1$).

PREUVE. Il suffit de vérifier que $p \in pp'P$ (resp. $p = pp'$) pour deux idempotents quelconques p et p' de P_u.

Soit F l'ensemble des applications de M dans S. Par définition P est l'ensemble $F \times M$ muni du produit $(f,m)(f',m') = (f'',mm')$ où, à son tour, l'application f'' est définie par la condition que pour chaque $m'' \in M$ on ait $m''f'' = (m''f)((m''m)f')$. Les idempotents de P sont donc les paires (f,m) dans lesquelles m est un idempotent et f satisfait $m''f = (m''f)((m''m)f)$ pour tout $m'' \in M$. Supposant $m = m^2$, on note que cette dernière condition implique que $m''f$ soit un idempotent pour chaque $m'' \in Mm$ puisque $m'' = m''m = m''mm$ quand $m'' \in Mm$.

Donc, d'après l'hypothèse $S \in \underline{\underline{D}}^o$ qui implique que chaque idempotent de S soit contenu dans son idéal minimum D, une condition nécessaire pour que (f,u) soit idempotent est que f envoie Mu sur le sous-ensemble D_1 des idempotents de D. De plus, comme S satisfait (Gp), D est un semi-groupe union de groupes et pour chaque $s \in S$ on a $s = se$ $(e \in D_1)$ ssi s appartient à la L-classe de e. Soient maintenant $p = (f,u)$ et $p' = (f',u)$ deux idempotents. Pour chaque m de M_u les éléments mf et mf' sont des idempotents de D. Donc $(mf)(mf')(mf) = h_m$ est un élément du groupe contenant mf et l'on peut trouver dans ce dernier un élément $\bar{h}_m$ tel que $h_m\bar{h}_m = mf$. Nous définissons l'élément $\bar{p} = (\bar{f},u)$ de P_u par la condition que $m\bar{f} = \bar{h}_{mu}$ pour chaque m de M. Soit $p'' = (f'',u) = pp'\bar{p}$. Pour chaque $m \in M$, $mf = s$ est égal à se où $e = (mu)f$ et on calcule directement que $mf'' = s.(mu)f'.\bar{h}_{mu} = s.e = s$. Donc $p'' = p \in pp'P$.

Dans le cas particulier où $S \in \underline{\underline{D}}^o 1$, l'idéal D se réduit à une seule L-classe. Donc si $p'' = pp' = (f'',u)$, on a pour chaque

$m \in M$ que $mf = s$; $muf = e = e^2$; $muf' = e' = e'^2$ où $s = e$ et où $ee' = e$, $se' = see' = e$ ce qui donne directement $p'' = pp' = p$.

Q.E.D.

III. LA PROPRIETE 1.

Nous commençons par rappeler quelques faits concernant la famille $U(S)$ des sous semi-groupes unitaires de S c'est-à-dire, on le rappelle des sous semi-groupes T tels que $T = T^{-1}T$. Dans ce qui suit G est un groupe maximal dans S , L sa $\mathcal{L}$-classe et L' le sous semi-groupe $\mathcal{L}$-simple union des groupes dans L .

III.1. (1) Si $T \in U(S)$ rencontre G , l'intersection $T \cap G$ est un groupe de $T \cap L'$ est un semi-groupe $\mathcal{L}$-simple contenant tous les idempotents dans L .

(2) Réciproquement, si H est un sous groupe de G, l'intersection T de tous les $T' \in U(S)$ contenant H est un sous semi-groupe de $U(S)$ tel que $T \cap G = H$. Si la $\mathcal{J}$-classe de G est complètement 0-simple on a de plus $T \cap MGM = T \cap L'$.

PREUVE. (1). Soient $g \in T \cap G$ et h l'inverse de g dans G . L'idempotent $u = hg$ appartient à T puisque $ghg = g$ implique $hg \in \{g\}^{-1}\{g\} \subset T^{-1}T \subset T$. Comme $u = gh$ on obtient $h \in \{g\}^{-1}\{u\} = T^{-1}T \subset T$ ce qui montre que $T \cap G = H$ est un sous groupe de G puisque T , donc $T \cap G$ est un semi-groupe.

Si v est un autre idempotent dans L on a $uv = u$, donc, comme ci-dessus, $v \in T$. Par conséquent, puisque T est un semi-groupe, son intersection avec L contient le semi-groupe $\mathcal{L}$-simple V formé par l'union des groupes vH où v parcourt l'ensemble des idempotents dans L .

(2). Réciproquement, étant donné le sous groupe H de G , posons $T = H^{-1}H$. Tout sous semi-groupe unitaire de S contenant H doit contenir T . Soit $t \in T$. Il existe $h \in H$ tel que $ht = h' \in H$. Multipliant à gauche par H on obtient $Ht = H$, puisque H est un groupe. On a donc d'une part $TT \subset T$ (puisque $Htt' = Ht' = H$ pour chaque $t' \in T$), et, d'autre part $T^{-1}T \subset T$ (puisque, si $s \in S$ et $ts \in T$, on a $Hts = Hs = H$ d'où $s \in T$). Par conséquent T est bien le plus petit sous semi-groupe unitaire contenant H .

Le reste de la preuve découle de la première partie qui montre

que T contient le semi-groupe $\mathcal{L}$-simple $V = T \cap L'$ et des résultats classiques sur les $\mathcal{J}$-classes complètement 0-simples qui impliquent $Hx \cap H = \emptyset$ donc $x \notin T$ pour tout $x \in MGM \setminus V$.

Q.E.D.

Nous désignons par $\mathcal{U}^1(S)$ la famille des sous semi-groupes unitaires de la forme $H^{-1}H$ où $H = \{u\}$ est un groupe trivial (c'est-à-dire réduit à un idempotent u) dans S. On rappelle que $\mathcal{B}(S)$ désigne la sous famille des sous semi-groupes unitaires T qui sont *bi-complets* en ce sens que $S \subset S^{-1}T$. Cette sous famille n'est pas vide car elle contient toujours au moins S lui-même. Nous utiliserons le fait que chaque $T \in \mathcal{B}(S)$ contient tous les $Q \in \mathcal{U}^1(S)$. En effet, si u est un idempotent dans S, l'hypothèse que T est bicomplet implique $su = t \in T$ pour au moins un $s \in S$. Comme $tu = suu = su = t$ et comme T est unitaire, ceci implique $u \in T$ donc $u^{-1}u \in T$.

III.2. Soit M un semi-groupe satisfaisant (Gp).

(1) Si $M \in \underline{\underline{D}}$ on a $M^{-1}Q \subset QM^{-1}$ pour tout $Q \in \mathcal{U}(M)$.

(2) Si $M^{-1}Q \subset QM^{-1}$ pour chaque $Q \in \mathcal{U}^1(M)$ on a $M \in D$.

PREUVE. (1). Supposons ces hypothèses satisfaites et soit $x \in M^{-1}Q$, c'est-à-dire $mx \in Q$ pour un certain $m \in M$. Puisque M satisfait (Gp), une puissance positive $q = (mx)^n$ $(n \geq 1)$ de mx appartient à un groupe dans M. Comme Q est un semi-groupe il contient q, donc, ainsi qu'on l'a vu en III.1., un groupe H dans lequel se trouve l'élément q.

D'autre part puisque M appartient à $\underline{\underline{D}}$, il existe un sous semi-groupe premier R dont l'idéal minimum est la $\mathcal{J}$-classe D contenant H. On a $x \in R$ puisque R est premier et $(mx)^n \in H \subset R$.

De plus, D est un semi-groupe union de groupes. Prenons $h \in H$ quelconque. On a $x \in D$ ce qui signifie que $xh = vg$ où v est un idempotent dans la $\mathcal{L}$-classe L de H et où g est un élément du groupe maximal G contenant H. On a vu dans III.1. que $v \in Q$. Prenant l'inverse g' de g dans G, on a $xhg' = v \in Q$, ce qui est la conclusion cherchée $x \in QM^{-1}$.

(2). Supposons inversement que M n'appartienne pas à $\underline{\underline{D}}$. C'est-à-dire en raison de l'hypothèse (Gp) qu'il existe une classe $D \in \mathrm{Jid}(M)$ qui ne soit pas un semi-groupe. D'après un théorème classique de Clifford D a une $\mathcal{L}$-classe L qui contient à la fois un idempotent u et un élément x n'appartenant pas à un groupe dans

M. Plus précisément l'idéal à droite xM ne rencontre aucun des groupes dans L. Considérons $Q = u^{-1}u$. D'après III.1., c'est un semi-groupe unitaire dont l'intersection avec MLM est formée des idempotents dans L. De nouveau d'après la théorie des inverses de Clifford on peut trouver un élément $y \in D$ pour lequel $yx = u$. On a par conséquent $x \in M^{-1}Q\backslash QM^{-1}$ prouvant que la condition (2) est suffisante pour que $M \in \underline{\underline{D}}$.

Q.E.D.

III.3. Tout semi-groupe S' est contenu dans un semi-groupe T admettant un sous semi-groupe $R \in \mathcal{B}(T)$ pour lequel $T = \mathrm{Synt}(R)$. Quand $S' \in \underline{\underline{D}}_f$ on peut choisir un tel T dans $\underline{\underline{D}}_f$.

PREUVE. (1). Nous transformons S' en un monoïde S en lui ajoutant un élément neutre e. Nous prenons un groupe G et un sous groupe $H \neq G$ de G ayant au moins autant d'éléments que S et ne contenant aucun sous groupe invariant $\neq \{1\}$ de G. Il est clair que quand S est fini on peut prendre un groupe G fini. Nous considérons le monoïde M des $S \times S$ matrices à entrées dans l'algèbre de G ayant exactement une entrée non nulle par colonne, celle-ci appartenant de plus à G lui-même. Soit μ le morphisme injectif de S dans M envoyant chaque $s \in S$ sur la matrice $s\mu$ telle que chacune de ses entrées $s\mu(s',s'')$ soit égale à 1 $(= 1_G)$ ou 0 selon que $s' = ss''$ ou non. Nous notons M_e le sous semi-groupe des matrices de M dont toutes les entrées non nulles sont dans la ligne e. A chaque g de G nous associons la matrice $u^g \in M_e$ telle que $u(e,s) = g$ pour tout $s \in S$. Enfin, nous choisissons arbitrairement une matrice v $v \in M_e$ telle que ses entrées $v(e,s)(s \in S)$ soient des éléments de H tous distincts, ce qui est possible puisque $\mathrm{Card}(H) \geq \mathrm{Card}(S)$ par hypothèse.

Ceci fait T est défini comme le sous semi-groupe de M engendré par les s $(s \in S)$, les u^g $(g \in G)$ et v et son semi-groupe R comme celui des matrices de T dont toutes les entrées non nulles sont dans H.

(2). Il est clair que T est fini quand S est fini. Montrons que $T \in \underline{\underline{D}}$ quand $S \in \underline{\underline{D}}$. Pour cela il suffit de vérifier que toutes les classes de $\mathrm{Jid}(T)$ sont des sous semi-groupes. Comme T est l'union de S et d'un ensemble D de matrices lignes, il suffit de montrer que D est l'idéal minimum de T c'est-à-dire, par exemple

ue $u^1 d = d$ (pour tout $d \in D$) ce qui est trivial, et que u^1 ap-
artient à tous les idéaux de T, ce qui résulte du calcul immédiat
$^1 = u^g.t.s.u^1$ pour chaque $t \in T$ en prenant une de ses entrées
on nulles quelconque $t(s';s) = g'$ et pour g l'inverse de g' dans
.

(2). Nous vérifions $R \in \mathcal{B}(T)$. Tout d'abord c'est un
emi-groupe puisque $HH \subset H$. Il est unitaire car si $t \in T$ et $p \in R$
ont tels que $q = pt \in T$ on a $pt \in R$ puisqu'à chaque entrée non
ulle $t(s';s)$ correspond au moins une entrée non nulle $p(s'';s')$, qui
st dans H, par hypothèse de même que le produit $q(s'';s) = p(s'';s')$
$(s';s)$ ce qui implique $t(s';s) \in H^{-1}H \subset H$.

Pour montrer que R est bi-complet nous considérons un t de T
uelconque et une de ses entrées non nulles $t(s';s) = g'$. Si $g = g'^{-1}$
a matrice $s\mu.u^g$ a toutes ses entrées non nulles dans la ligne s.
n vérifie facilement que $t.s\mu.u^g = s'\mu.u^1$ où ce dernier produit ap-
artient à R puisque $s'\mu$ et u^1 appartiennent à R par défini-
ion. Donc $tT \cap R \neq \emptyset$ pour tout $t \in T$ et $T = T^{-1}R$.

(4). Il reste à établir $T = \mathrm{Synt}(R)$, c'est-à-dire
u'étant donnés deux éléments distincts t et $t' \neq t$ de T on peut
rouver $t_1, t_2 \in T$ tels que $t_1 t t_2 \in R$ et $t_1 t' t_2 \notin R$.

Par hypothèse on a $0 \neq t(s';s) \neq t'(s';s)$ pour au moins une paire
$s';s)$. D'après notre choix de v une relation analogue est encore
raie pour $u^1 t$ et $u^1 t'$ et pour vt et vt'. Ceci permet désormais
e supposer que $t,t' \in M_e$ et que l'on a $f = t(e,s) \neq f' = t'(e,s)$
$f,f' \in G$). Comme H ne contient pas de sous groupe normal non tri-
ial de G, on peut trouver au moins un $g \in G$ tel que $f^{-1}f' \notin g^{-1}Hg$.
ar conséquent $gf^{-1}fg^{-1} = 1 \in H$, $gf^{-1}f'g^{-1} \notin H$.

Un calcul direct donne alors $u^x tu^y \in R$, $u^x t' u^y \notin R$ en prenant
$= gf^{-1}$, $y = g^{-1}$.

Q.E.D.

PREUVE DE LA PROPRIETE 1. Il sera commode de dire qu'un morphisme
$\phi : S \to T$ *reconnaît* une partie X d'un semi-groupe S ssi $X\phi\phi^{-1} = X$,
'est-à-dire, de façon équivalente, ssi il existe un morphisme de
'image $S\phi$ sur le semi-groupe syntaxique de X.

Nous utiliserons couramment la remarque que quand ϕ est un mor-
hisme surjectif qui reconnaît les parties X et Y de S on a
$Y^{-1}X)\phi = (Y\phi)^{-1}(X\phi)$ et $(Xy^{-1})\phi = (X\phi)(Y\phi)^{-1}$. Par conséquent, suppo-
ant toujours ϕ surjectif, les relations $P \in U(S)$ et $P\phi \in U(S\phi)$

M.P. Schützenberger

sont équivalentes pour chaque sous semi-groupe P reconnu par ϕ. Il en est de même pour la condition d'être bi-complet ou de satisfa la relation $S^{-1}P \subset PS^{-1}$.

Nous prions le lecteur de se rapporter à l'énoncé de la Propri té I donné dans l'introduction. Comme tous les semi-groupes finis s tisfont (Gp), il résulte immédiatement de II.6 que $\underline{\underline{Df}}$ est une varié Par conséquent, pour établir l'égalité $\underline{\underline{Df}} = \underline{\underline{V}}$ qui constitue la Pr priété I il suffit de vérifier les deux assertions (1) et (2) ci-de sous. On rappelle que P est *reconnaissable* si son semi-groupe syn taxique est *fini*.

(1). Soient A un alphabet fini et $P \in \mathcal{B}(A^+)$ reconnaissable et sa tisfaisant la condition supplémentaire (#). Son semi-groupe synta- xique $M = \mathrm{Synt}(P)$ est dans $\underline{\underline{D}}$.

PREUVE. Soit $\phi : A^+ \to M$ le morphisme syntaxique de P. Ainsi qu'on vient de le dire, $P\phi$ appartient à $\mathcal{B}(M)$. Chacun des sous s groupes $Q \in \mathcal{U}^1(M)$ est reconnu par ϕ, par définition, et par con quent chaque semi-groupe syntaxique $\mathrm{Synt}(Q\phi^{-1})$ est un quotient de $M = A^+\phi = \mathrm{Synt}(P)$. Donc en raison de la condition (#) chaque Q (est égal à $Q\phi^{-1}\phi$) satisfait $M^{-1}Q \subset QM^{-1}$. La conclusion désirée $M \subset \underline{\underline{D}}$ résulte alors de II.2.(2).

Q.E

(2). Soit $S' \in \underline{\underline{Df}}$. Il existe un alphabet fini A et un semi-grou reconnaissable $P \in \mathcal{B}(A^+)$ satisfaisant la condition (#) tel que S divise $\mathrm{Synt}(P)$.

PREUVE. Nous appliquons à S' la construction décrite dans III.3. Le semi-groupe obtenu T est fini et appartient à $\underline{\underline{D}}$. On peut donc prendre un ensemble fini A et étendre une surjection $\phi : A \to T$ à un morphisme ϕ de A^+ sur T. Soit $P = R\phi^{-1}$. Le morphisme ϕ reconnaît P, par construction et, d'autre part, d'après l'hypothèse $T = \mathrm{Synt}(R)$ on a $P \neq P\Psi\Psi^{-1}$ pour tout morphi Ψ de la forme $\phi\tau$ où τ est un morphisme de T sur un de ses quotients propres. Donc $T = \mathrm{Synt}(P)$.

En raison de $R \in \mathcal{B}(T)$ on a $P \in \mathcal{B}(A^+)$. En outre chaque sou semi-groupe $Q \subset P$, $Q \in \mathcal{U}(A^+)$ tel que $\mathrm{Synt}(Q)$ soit un quotient de $\mathrm{Synt}(P)$ vérifie $Q = Q\phi\phi^{-1}$, donc $Q\phi \subset R$, $Q\phi \in \mathcal{U}(T)$, ce qui impliq $T^{-1}.Q\phi \subset Q\phi.T^{-1}$ d'après III.2.(1) et, par conséquent, $(A^+)^{-1}Q \subset Q(A^+)^{-1}$. Donc P satisfait (#) et comme S' est un sou

semi-groupe de T le résultat est prouvé.

Q.E.D.

IV. LES PROPRIETES 2 ET 3.

Nous commençons par préciser une construction connue. Si X et Y sont deux parties d'un monoïde libre A^*, le produit XY est *d'ambiguïté bornée* ssi il existe un entier k tel que chaque mot de A^* admette au plus k factorisations distinctes comme produit d'un mot de X par un mot de Y. Une partie X est dite *préfixe* ssi elle est contenue dans le semi-groupe libre A^+ et si $XA^+ \cap X = \emptyset$, c'est-à-dire, de façon équivalente, ssi $X'Y$ est un produit non ambigu différent de Y pour tout $X' \cup X$ et $Y \subset A^*$. De façon symétrique, X est *suffixe* (ou *préfixe opposé*) ssi $X \subset A^+$ et $A^+X \cap X = \emptyset$.

Nous considérons maintenant un monoïde fini M et deux de ses éléments x et y. Soient T $(= T_{x,y})$ l'ensemble des paires $(m,m') \in M \times M$ telles que $x \in Mm$ et $y \in m'M$ et 2^T le monoïde commutatif des parties de T par rapport à l'union. Nous définissons selon [5] une action bilatère $M \times 2^T \times M \to 2^T$ en posant pour chaque $m_1, m_2 \in M$; $q \in T$ et $t = (m, m') \in T$:

$m_1 \, t \, m_2 = (m_1 m, m' m_2)$ si cette paire est dans T ; $= \emptyset$ sinon.

Comme d'usage $m_1 \, q \, m_2 = \{m_1 \, t' \, m_2 : t' \in q\}$ et mq et qm sont des abréviations pour $mq1$ et $1qm$. L'union est notée $+$ par commodité. Ceci permet de définir un produit sur $M \times 2^T$ par l'identité $(m,q)(m',q') = (mm', mq' + qm')$ $((m,q), (m',q') \in M \times 2^T)$ dont on vérifie immédiatement l'associativité en calculant

$$(m,q)(m',q)(m'',q'') = (mm'm'', mm'q'' + mq'm'' + qm'm'').$$

On désignera par π et τ les projections naturelles de $M \times 2^T$ sur M et sur 2^T respectivement.

IV.1. Soit $\mu : A^* \to M$ un morphisme. Le produit $E = x\mu^{-1}.y\mu^{-1}$ est reconnu par un morphisme ϕ sur un monoïde P contenu dans $M \times 2^T$.

Pour chaque idempotent u de M le semi-groupe $u\pi^{-1} \cap P$ est apériodique. De plus, il appartient à D^o quand E est d'ambiguïté bornée. Quand $x\mu^{-1}$ est préfixe, il appartient à $D^o 1$. Enfin, quand E est préfixe et $y\mu^{-1} \subset A$ il se réduit à $\{u\}$.

PREUVE. (1). L'application de A dans $M \times 2^T$ envoyant chaque lettre a sur $(a\mu, \ (a\mu,1) + (1, a\mu))$ se prolonge en un morphisme ϕ de A^* sur un monoïde P contenu dans $M \times 2^T$ dont l'élément neutre

est $(1, (1,1))$. Pour chaque mot b on a $b\phi = (b\mu, b\phi\tau)$ où :

$$b\phi\tau = \Sigma\ \{(b'\mu, b''\mu) \in T : b', b'' \in A^*\ ;\ b = b'b''\}.$$

Donc $b \in E = x\mu^{-1}.y\mu^{-1}$ ssi $(x,y) \in b\phi\tau$ ce qui montre que ϕ reconnaît E.

(2). Soient maintenant u un idempotent de M et $V = u\mu^{-1} \cap P$.

Si $P = (u,q) \in V$, on a $p^2 = (u,uq + qu)$ et $p^n = (u,uq + uqu + qu)$ pour chaque $n \geq 3$ ce qui montre que V est apériodique.

Soit T_u l'ensemble des $t \in T$ tels que $t \in q$ pour au moins un $(u,q) \in V$. Supposons qu'il existe un $t = (m,m') \in T$ tel que $utu\ utu = t$, c'est-à-dire tel que $um = n$ et $m'u = m'$. Cette hypothèse est satisfaite si $u = 1$ ou si $ut'u \neq \emptyset$ pour un $t' \in T_u$ puisqu'il suffit alors de prendre $t = ut'u$. Prenons $c \in m\mu^{-1}$, $d \in m'\mu^{-1}$. D'après la définition $T = (M^{-1}x) \times (yM^{-1})$ il existe $f,g \in A^*$ tel que $fc \in x\mu^{-1}$ et $dg \in y\mu^{-1}$ et $mm' = u$. On a $f(cd)^ic \in x\mu^{-1}$, $d(cg)^jg \in y\mu^{-1}$ pour tout $i,j \geq 0$ ce qui montre que $f(cd)^ng$ a $n+1$ factorisations distinctes comme produit d'un mot de $x\mu^{-1}$ et d'un mot de $y\mu^{-1}$ quand $cd \in A^+$.

Par conséquent, quand E est un produit d'ambiguïté bornée on a $uT_uu = \emptyset$ pour chaque idempotent $u \in A^+\mu$, ce qui entraîne en particulier que le sous monoïde $A^*\mu$ de M soit l'union d'un élément neutre $1 = 1\mu$ et d'un semi-groupe $A^+\mu$. On en déduit immédiatement que $V \in \underline{D}^o$ puisque si $p = (u,q)$, $p' = (u,q')$ et $p'' = (u,q'')$ sont trois éléments de V, le produit $pp'p'' = (u,uq'' + uq'u + qu)$ est égal à $pp'' = (u,uq'' + qu)$ en raison de $uq'u \subset u.T_u.u = \emptyset$, ce qui montre que $pVp'' = pp''$ $(p,p'' \in V)$ identiquement.

(3). Gardant les mêmes notations, supposons que $t = (m,m') \in T_u$ soit tel que $ut = t$. On a $f(cd)^ic \in x\mu^{-1}$ pour tout $i \geq 0$ et par conséquent la partie $X = x\mu^{-1}$ est telle que $X^{-1}X$ contient le semi-groupe $(dc)^+$ ce qui est impossible quand $cd \in A^+$ et quand X est une partie préfixe, comme nous le supposons maintenant. On a donc $uT_u = \emptyset$ pour chaque idempotent $u \in A^+\mu$. Sous cette hypothèse, prenant $p,p'' \in V$ comme ci-dessus, on trouve que $pp'' = (u,qu) = p^2$, c'est-à-dire que $pV = p^2$ identiquement ce qui établit que $V \in \underline{\underline{D}}^o 1$.

(4). Supposons enfin que $Y = y\mu^{-1}$ est une partie de A. On a donc $y \notin ym'M$ pour tout $m' \neq 1$ et, en revenant à la définition

du morphisme ϕ, on voit que si $b \neq 1$ est tel que $E \cap A^*bA^* \neq \emptyset$, il n'y a que deux cas possibles, à savoir : $b\phi = (b\mu, (b\mu, 1))$ et $b\phi = (b\mu, (b\mu, 1) + (b'\mu, y))$ selon que $b \notin A^*Y$ ou que $b = b'a \in A^*Y$ $(a \in Y \subset A)$ où, dans le second cas, $b\mu = b'\mu.y$. Si l'on introduit l'hypothèse supplémentaire que $E = XY$ est une partie préfixe, il est exclus que $b\mu$ soit un idempotent dans le deuxième cas puisque ceci impliquerait $fb^+ \subset E$ pour au moins un mot f. Par conséquent les seuls idempotents de $P = A^*\phi$ sont $(1, (1,1)) = 1\phi$ et les $(u, (u\mu, 1))$ $(u = u^2 \in M)$ d'où l'on conclut que $u\pi^{-1} \cap P = \{u\}$ ce qui achève la vérification de l'énoncé.

Q.E.D.

G. Lallement m'a fait observer que les calculs ci-dessus équivalent à l'usage des identités $x^\omega y z^\omega = x^\omega z^\omega$ et $x^\omega y = x^\omega$ pour caractériser les variétés des semi-groupes apériodiques de $\underline{\underline{D}}_f^o$ et $D_f^o 1$ respectivement.

Nous dirons que le produit XY est *déterministe* ssi X est préfixe ou si XY est préfixe et $Y \subset A$. Symétriquement, YX est *déterministe opposé* ssi X est suffixe ou si YX est suffixe et $Y \subset A$. Plus généralement, un produit $X_1 X_2 \ldots X_k$ sera déterministe (resp. déterministe opposé) ssi ceci est vrai de chacun des produits $X_1 X_2$, $(X_1 X_2) X_3$, $(X_1 X_2 X_3) X_4$,... etc. (resp. $X_{k-1}X_k$, $X_{k-2}(X_{k-1} X_k)$, ... etc). Ces conditions impliquent trivialement que ce produit soit non ambigu.

Nous rappelons que nous avons défini dans l'introduction la *complétion polynomiale non ambiguë* $\mathrm{UPol}(\underset{\sim}{X})$ d'une famille $\underset{\sim}{X}$ de partie de A^* comme la plus petite famille $\underset{\sim}{Y}$ contenant $\underset{\sim}{X}$ telle que :

(i) $\underset{\sim}{Y}$ contient chaque lettre de l'alphabet A et chaque sous monoïde B^* engendré par une partie B de A.

(ii) $\underset{\sim}{Y}$ contient l'union disjointe de deux de ses membres.

(iii) $\underset{\sim}{Y}$ contient tout produit *non ambigu* de ses membres.

On définit de même la *complétion polynomiale déterministe* $\mathrm{DPol}(\underset{\sim}{X})$ en remplaçant dans (iii) l'adjectif *non ambigu* par *déterministe*. Enfin on aura la *complétion polynomiale bidéterministe* $\mathrm{BDPol}(\underset{\sim}{X})$ en remplaçant (iii) par :

(iii B). $\underset{\sim}{Y}$ contient chaque partie de A^* qui est à la fois une union disjointe finie de produits déterministes de parties de $\underset{\sim}{Y}$ et

une union disjointe finie de produits déterministes opposés de parties de $\underset{\sim}{Y}$. (On a par conséquent les inclusions $\underset{\sim}{X} \subset BDPol(\underset{\sim}{X}) \subset DPol(\underset{\sim}{X}) \subset UPol(\underset{\sim}{X})$).

D'autre part, afin d'unifier les preuves des Propriétés 2 et 3, nous considérons comme dans l'introduction une variété $\underline{\underline{G}}$ de groupes finis et nous notons $\underline{\underline{G}}\,\underline{\underline{D}}_f$ la famille des monoïdes finis de $\underline{\underline{D}}$ dont tous les groupes appartiennent à $\underline{\underline{G}}$ et qui satisfont l'identité :

(#) $(x^\omega y^\omega)^\omega = (x^\omega y^\omega)(x^\omega y^\omega)^\omega$.

(avec ω comme dans l'énoncé II.6). D'après la théorie de S. Eilenberg, $\underline{\underline{G}}\,\underline{\underline{D}}_f$ est une variété. De façon plus explicite, la condition exprimée par l'identité supplémentaire (#) signifie que le sous monoïde engendré par deux idempotents est apériodique. Elle est donc trivialement satisfaite par les monoïdes finis apériodiques et la variété $\underline{\underline{D}}_f \cap A_p$ de la Propriété 2 est la variété $\underline{\underline{G}}\,\underline{\underline{D}}_f$ correspondant au cas où $\underline{\underline{G}}$ est la variété triviale de groupes formés du seul groupe $\{1\}$.

IV.2. Pour tout alphabet fini A, chacune des familles $\underset{\sim}{Y} = A^*\text{-}\underline{\underline{D}}_f$ ou $A^*\text{-}\underline{\underline{G}}\,\underline{\underline{D}}_f$ (resp. $= A^*\text{-}\underline{\underline{G}}\,\underline{\underline{D}}_f 1$; resp. $= A^*\text{-}\underline{\underline{G}}\,\underline{\underline{D}}_f 1r$) est égale à sa complétion polynomiale non ambiguë (resp. déterministe ; resp. bidéterministe) et contient les intersections de ses membres avec les parties de $A^*\text{-}\underline{\underline{G}}$.

PREUVE. (1) C'est un théorème de S. Eilenberg [5] que pour chaque variété $\underline{\underline{V}}$ la famille $A^*\text{-}\underline{\underline{V}}$ est une algèbre booléenne : en effet le monoïde syntaxique de toute partie X de A est égal à celui de son complément $A^*\backslash X$ et celui d'une union $X \cup Y$ divise le produit direct des monoïdes syntaxiques de X et de Y. Comme la variété $\underline{\underline{G}}$ est contenue dans $\underline{\underline{D}}1r$ (et que tous les groupes satisfont trivialement l'identité (#)), ceci prouve que $\underset{\sim}{Y}$ contient l'union disjointe de deux de ses membres et l'intersection de chacun de ceux-ci avec une partie quelconque de $A^*\text{-}\underline{\underline{G}}$.

(2) Chaque partie de A^* formée d'une seule lettre ou égale au sous monoïde engendré par un sous alphabet possède un monoïde syntaxique qui divise le monoïde à trois éléments $\{1, m, m^2 = m^3\}$. Ce dernier est apériodique et appartient à $\underline{\underline{D}}^o_f 1r$. Par conséquent $\underset{\sim}{Y}$ contient toutes les parties de A^* de cette forme.

(3) Soient X et Y deux parties de $\underset{\sim}{Y}$. Elles sont reconnues par un morphisme μ de A^* dans un sous monoïde M du pro-

duit direct de leurs monoïdes syntaxiques. Le produit XY est une somme disjointe de produits de la forme $(x\mu^{-1})(y\mu^{-1}) = E$ $(x \in X_\mu, y \in Y_\mu)$ dont chacun est non ambigu (resp. déterministe ; resp. déterministe opposé) quand E lui-même a cette propriété. D'après IV.1, E est reconnu par un morphisme $\phi : A^* \to P$ où la projection $\pi : P \to M$ est telle que $u\pi^{-1}$ soit un semi-groupe apériodique de D_f^o (resp. de $D_f^o 1$ pour chaque idempotent u de M quand le produit est non ambigu (resp. déterministe).

Le fait que $u\pi^{-1}$ soit apériodique implique que chaque groupe dans P soit isomorphe à un groupe dans M donc qu'il appartienne à la variété $\underline{G}$. Elle entraîne aussi que P satisfasse l'identité (#) quand celle-ci est satisfaite par M.

Le second fait que $u\pi^{-1} \in \underline{\underline{D}}_f^o$ (resp. $\in D_f^o 1$) entraîne d'après II. 7, que l'on ait $P \in \underline{\underline{D}}_f$ (resp. $\in \underline{\underline{D}}_f^1$) quand M appartient à cette variété.

Procédant par induction sur le nombre des produits de concaténation effectués, ceci établit l'énoncé en ce qui concerne les familles $A^* - \underline{\underline{D}}_f$, $A^* - \underline{\underline{G}}\ \underline{\underline{D}}_f$ et $A^* - \underline{\underline{G}}\ \underline{\underline{D}}_f 1$ et il nous reste seulement à examiner le cas de $\underline{\underline{D}}_f 1r$.

(4) Soit donc F une partie de A^* satisfaisant les hypothèses de (iii B) c'est-à-dire telle que $F = F^1 = F^r$ où F^1 (resp. F^r) est une union disjointe finie de produits déterministes de termes $X_i^1 \in A^* - \underline{\underline{D}}_f 1r$, $(i \in I)$ (resp. de produits déterministes opposés de termes $X_j^r \in A^* - \underline{\underline{D}}_f 1r$ $(j \in J)$).

Soit N le monoïde syntaxique simultané de toutes les parties X_i^1 et X_j^r $(i \in I, j \in J)$, c'est-à-dire le quotient de A^* par la plus grande congruence pour laquelle chacune de ces parties est une union de classes. N est un monoïde fini appartenant à $\underline{\underline{D}} 1r$.

Utilisant l'expression $F = F^1$, il résulte de (3) qu'il existe un morphisme $\lambda : A^* \to Q^1$ reconnaissant F où Q^1 appartient à la variété $\underline{\underline{D}}_f 1$ Symétriquement, utilisant $F = F^r$, on vérifie que F est reconnu par un morphisme ρ de A^* dans un monoïde Q^r de la variété $\underline{\underline{D}}_f r$ des semi-groupes finis dont chaque J-classe contenant un idempotent est une R-classe.

Par conséquent, le monoïde syntaxique de F appartient à l'intersection de D_f^1 et $\underline{\underline{D}}_f^r$ c'est-à-dire à $\underline{\underline{D}}_f 1r$.

O.E.D.

M.P. Schützenberger

Le même énoncé IV.1 permet facilement de vérifier que la famille des parties reconnaissables de A^* dont le monoïde syntaxique n'admet aucun diviseur égal au monoïde à trois éléments $\{1, u = u^2 = vu, v = v^2 = uv\}$ (resp. ni au monoïde symétrique $\{1, u = u^2 = uv, v = v^2 = vu\}$) est égale à sa complétion polynomiale déterministe (resp. bidéterministe) (Cf. [5] Chap. VI).

Nous considérons maintenant un alphabet (fini) A, un monoïde fini fixe $M \neq \{1\}$, l'ensemble ΔM de ses diviseurs *propres* (c'est-à-dire $\neq M$) et la famille $A^* - \Delta M$ des parties de A^* dont le monoïde syntaxique appartient à ΔM. Nous considérons aussi la complétion polynomiale non ambiguë UPol (resp. déterministe, DPol ; resp. bidéterministe, BDPol) de $A^*-\Delta M$ et nous notons PolB la famille des unions finies de parties de A^* de la forme X, A^*X ou $X\backslash Y$ avec $X \in$ UPol et $Y \in$ PolB.

Dans l'énoncé suivant l'*idéal 0-minimal* K de M est l'intersection de tous les idéaux de M ayant deux éléments ou plus. Comme $M \neq \{1\}$ est fini, K est un idéal non vide qui peut être réduit au zéro, 0, de M.

Dans le cas contraire $K\backslash 0 = D$ ($= K$ si M n'a pas de zéro) est une J-classe. On sait que si $K \neq 0$ chaque élément $k \in K\backslash 0$ engendre un idéal à droite kM (resp. à gauche Mk) qui est *0-minimal* en ce sens que $kM = k'M$ (resp. $Mk = Mk'$) pour chacun de ses éléments $k' \neq 0$. Si de plus K est apériodique, on a $kM \cap Mk = \{k,0\}$ ou $K = k$ selon que M a ou non un zéro. Enfin dans le cas particulier où K est apériodique et où D est réduit à une seule L-classe (resp. H-classe) on a $kM = \{k,0\}$ ou $= k$ dans les mêmes conditions (resp. $D = kM\backslash 0 = Mk\backslash 0 = \{k\}$).

IV.3. Soit μ un morphisme du monoïde libre A^* dans un monoïde fini $M \neq \{1\}$, K l'idéal 0-minimal de M, $x \in M$ et $X = x\mu^{-1}$.

On a les relations suivantes :

(i) $X \in A^*-\Delta M$ pour chaque $x \in M\backslash K$.

Soit désormais $x \in K$.

(ii) $X \in$ BDPol si $K^2 = 0$ ou si $x = 0$ et $D^2 = D$ $(\neq \emptyset)$.

Soit désormais K apériodique.

(iii) $X \in$ UPol si $D^2 = D$ avec, plus précisément, $X \in$ DPol (resp. $\in$ BDPol) quand D est réduit à une seule L-classe (resp. H-classe).

(iv) $X \in$ PolB pour chaque $x \in K$ dans le cas restant, l'hypothèse

K apériodique n'étant pas requise pour $x = 0$.

PREUVE. Elle requiert la considération de cas particuliers dont l'ordre ne coincide pas exactement avec celui de l'énoncé.

(1). Soit d'abord $x \in M\backslash K$. Par hypothèse il existe un idéal W ne contenant pas x qui a deux éléments ou plus. Par conséquent, il existe un morphisme ρ de M sur un monoïde quotient qui reconnaît x et envoie W sur un zéro. On a donc $X = x\rho(\mu\rho)^{-1}$ où $M\rho \in \Delta M$ ce qui établit l'assertion (i).

Nous supposons donc toujours désormais que $x \in K$ et nous posons $\bar{M} = M\backslash M \times M$.

(2). Soit $K = 0$ et $x = 0$.

On a $1 \notin X$ puisque $M \neq \{1\}$. Soit f un mot de X. Il admet un plus long facteur gauche g tel que $g\mu = m \in \bar{M}$, donc une factorisation $f = gag'$ où $a \in A$, $g' \in A^*$ et $(ga)\mu = x = 0$. Si $E = (m\mu^{-1})a$ on a $EA^* \subset X$ puisque $x = xM$. Puisque $m \in \bar{M} = M\backslash M \times M$ et $E\mu = x$, E est une partie préfixe. Donc EA^* est un produit déterministe appartenant à DPol. Il est clair que X est l'union disjointe finie de tels produits $(m'\mu^{-1}).a'.A^*$ étendue à toutes les paires $(m', a') \in \bar{M} \times A$ telles que $x = m'.a'\mu$.

Une construction symétrique à partir des plus longs facteurs *droits* dans $\bar{M}\mu^{-1}$ des mots de X montre que X est aussi une union disjointe finie de produits déterministes opposés. Par conséquent $X \in$ BDPol.

Nous supposons désormais $K \neq 0$.

(3). Soit $K^2 = 0$ et $x \in D = K\backslash 0$.

Comme dans (2) on a $1 \notin X$. Soient f un mot de X, et g son plus long facteur gauche dans $\bar{M}\mu^{-1}$. On a encore $f = gag'$ ($a \in A$, $g' \in A^*$) où $(ga)\mu \in K$. Comme $(gag')\mu = x \neq 0$ et $K^2 = 0$ on a aussi $g' \in \bar{M}\mu^{-1}$. De la même manière que dans (2) on voit que si $g\mu = m$, $g'\mu = m'$, le produit $(m\mu^{-1})$ a est une partie préfixe et que le produit $(m\mu^{-1})a\,(m'\mu^{-1})$ est une partie déterministe contenue dans X. On en déduit $X \in$ DPol et, comme la construction est symétrique $X \in$ BDPol.

(4). $K^2 = 0$ et $x = 0$.

La vérification que $X \in$ BDPol se fait comme dans (2) puisque l'on vient de voir que cette famille contient toutes les parties de la

forme $k\mu^{-1}$ où $k \in K\backslash 0$.

Nous supposons désormais $K^2 \neq 0$ et par conséquent $D = K\backslash 0 \neq \emptyset$. Les arguments sont différents selon que D est un semi-groupe ($D^2 = D$) ou non. Nous considérons d'abord le premier cas.

D'après II.3., $D^{-1}D$ est un sous semi-groupe premier P de M. Soit $B = A \cap P\mu^{-1}$. Puisque P est premier on a $P \subset B^*\mu = M'$ et puisque P est un monoïde $P = M'$. Par conséquent D est l'idéal minimum de M'.

(5). $D^2 = D$ et $x = 0$.

Comme $0 \notin P$, ces hypothèses impliquent que $C = A\backslash B$ ne soit pas vide. Soit $Q = (A^* C A^*)\mu$. Q est un idéal de M qui contient x et d'après la définition du sous monoïde premier P, son intersection avec P est vide. Donc $Q \cap D = \emptyset$. Puisque $D = K\backslash 0$ où K est l'intersection de tous les idéaux de M ayant deux éléments ou plus, ceci entraîne que Q soit un singolet, c'est-à-dire que $Q = 0 = x$. Donc $X = A^* C A^*$. On peut écrire X comme un produit déterministe, $B^* C A^*$, ou déterministe opposé, $A^* C B^*$, et par conséquent $X \in$ BDPol ce qui termine la preuve de l'assertion (ii).

Nous supposons toujours désormais que K est apériodique.

(6). $D^2 = D$ et $x \in D$.

Si $1 \in X$ on a $x = 1$ c'est-à-dire que x appartient au sous-groupe de M. Comme K est apériodique, ce dernier est réduit à 1 et l'on a $X = B^*$ pour un sous alphabet B de A. Donc dans ce cas $X \in$ BDPol.

Supposons désormais $1 \notin X$ et soit f un mot de X. Il admet un plus long facteur gauche g tel que $g\mu = m \in \bar{M}$ et une factorisation $f = gag'$ avec $a \in A$, $g' \in A^*$. De fait, $g, g' \in B^*$ et $a \in B$ d'après les remarques faites au début de la discussion du cas $D^2 = D$.

Si D est réduit à une seule L-classe le produit déterministe $(m\mu^{-1})a B^*$ est contenu dans X et $X \in$ DPol puisque X est une union disjointe finie de tels produits. Si D est réduit à une seule H-classe, c'est-à-dire ssi $D = \{x\}$, on conclut $X \in$ BDPol par symétrie.

Revenant au cas général et au même mot f, il se peut que $m'' = g'\mu$ appartienne à $\bar{M}$. Dans ce cas f appartient au produit déterministe $(m\mu^{-1})a (m''\mu^{-1}) \in$ DPol. Si cette circonstance particulière n'est pas réalisée, c'est-à-dire si $g'\mu \in K$, le mot g' a un plus long facteur droit h tel que $h\mu = m' \in \bar{M}$, donc une factorisation $g = f'a'h$ avec $a' \in B$, $f' \in B$ et $(a'h)\mu \in K$.

M.P. Schützenberger

Comme D est l'idéal minimal du sous monoïde $B^*\mu = M'$, tous les mots de $m.a\mu.M'$ (resp. de $M'.a'\mu.m'$) appartiennent à l'idéal à droite minimum xM' de M' (resp. à l'idéal minimum à gauche $M'x$). Comme K est apériodique, l'intersection de ces deux idéaux se réduit à x ce qui montre que le produit $X' = (m\mu^{-1}).a.B^*.a'.(m'\mu^{-1})$ est contenu dans X. Par construction le produit $m\mu^{-1}.a$ est une partie préfixe. Donc le produit $(m\mu^{-1}).a.B^*$ est déterministe. Comme la partie $a'.(m'\mu^{-1})$ est suffixe (par construction), le produit X' est non ambigu.

Il est clair que X est une union disjointe finie de tels produits et de produits décrits au début de la discussion ce qui achève la preuve de l'assertion (iii) que $X \in UPol$.

Nous supposons désormais que $D^2 \neq D$, ce qui entraîne que M ait un zéro.

(7). $D^2 \neq D$ et $x = 0$.

Soit $C = X \cap A$. Si C n'est pas vide, X contient la partie $A^* C A^*$ qui appartient à BDPol par définition. Considérons un mot $f \in X \backslash A^* C A^*$. Il admet un plus long facteur gauche $g \in \bar{M}\mu^{-1}$, donc une factorisation $f = gag'$ avec $a \in A$, $g' \in A^*$ et $0 = x\,(ga)\mu$. Comme $a \notin C$, le mot g admet un plus long facteur droit h tel que $(ha)\mu \in \bar{M}$ et une factorisation $g = f'a'h$ où $f' \in A^*$, $a' \in A$, $(a'ha)\mu = x = 0$.

Nous vérifions que $h\mu = p$ n'appartient pas à K. Pour cela, supposons le contraire et posons $m = a\mu$, $m' = a'\mu$. Comme $pm \neq 0$, p et pm engendrent le même idéal à droite 0-minimum de M. Il existe donc $m'' \in M$ tel que $p = pmm''$. Comme $m'p \neq 0$ par hypothèse, on obtient les relations contradictoires $0 = m'pm = m'pmm''$ et $0 \neq m'pmm'' = m'p$.

Par conséquent le produit $a'.(p\mu^{-1}).a$ (qui est non ambigu puisque $a, a' \in A$) appartient à UPol et le produit $Y = A^*.a'.(p\mu^{-1}).a.A^*$ appartient à PolB par construction puisque $a'.p\mu^{-1}.a.A^* \in UPol$. Il est clair que $X \backslash A^* C A^*$ est une union finie (non nécessairement disjointe) de tels produits et nous avons donc établi $X \in PolB$ pour $X = 0\mu^{-1}$.

Le lecteur notera que l'hypothèse que K est apériodique n'a pas été utilisée. Bien plus, quand K n'est pas apériodique, un théorème classique de J. Rhodes et B. Tilson montre qu'il existe un morphisme χ de M sur un monoïde quotient *propre* $M' \in \Delta M$ pour lequel $0\chi\chi^{-1} = 0$ et que l'on a donc alors $X = 0\mu^{-1} \in A^* - \Delta M$.

M.P. Schützenberger

Nous supposons de nouveau K apériodique.

(8). $D^2 \neq D$ et $x \in D$.

L'hypothèse que K est apériodique entraîne que $xM \cap Mx = \{x,0\}$. Reprenant la discussion de (6) et remplaçant partout B par A on obtient une partie X' de $X \cup 0\mu^{-1}$ contenant X comme union fine de produits $(m\mu^{-1})\ a\ (m'\mu^{-1})$ $(a \in A\ ;\ m, m' \in \bar{M},\ m(a\mu)\ m' = x)$ et de produits $(m\mu^{-1})\ a\ A^*\ a'\ (m'\mu^{-1}) \in UPol\ (a, a' \in A\ ;\ m, m' \in \bar{M}\ ;\ m\ (a\mu),\ (a'\mu)\ m' \in K)$. On en déduit $X = X'\backslash 0\mu^{-1}$ par complémentation, d'où $X \in PolB$ d'après (7) et la définition de cette famille.

Q.E.D.

Nous avons encore besoin d'une remarque qui est un corollaire des théorèmes fondamentaux de la théorie moderne des semi-groupes finis de J. Rhodes et B. Tilson et nous faisons référence aux travaux de ces auteurs pour la preuve de la plupart des faits utilisés ci-dessous.

IV.4. Soient $M \in \underline{\underline{G}}\,\underline{\underline{D}}_f \cup \underline{\underline{G}}\,\underline{\underline{D}}_f 1$ un monoïde sans zéro et G un groupe maximal dans son idéal 0-minimal K. M admet un monoïde quotient M' dont l'idéal 0-minimal est apériodique qui est tel que M soit un sous-monoïde du produit direct $M' \times G$.

PREUVE. (1). L'hypothèse que M n'a pas de zéro entraîne que $K = D = D^2$ dans les notations de IV.3. D'après J. Rhodes et B. Tilson il existe un morphisme de M sur un monoïde quotient M' dont la restriction à $M\backslash K$ est bijective et celle à K envoit bijectivement chaque $\mathcal{H}$-classe sur un idempotent. M' a un idéal 0-minimal apériodique (qui est l'image de K). C'est le monoïde mentionné dans l'énoncé.

Soit d'autre part $\{L^i : i \in I\}$ l'ensemble des idéaux à gauche minimaux de M, leur union est K. D'après les mêmes auteurs il existe un monoïde P d'applications de I dans lui-même, un sous monoïde Q du produit en couronne GoP et un morphisme surjectif ρ de M sur Q dont la restriction à chaque idéal minimal à droite de M est bijective. Ceci entraîne que M soit isomorphe à un sous monoïde du produit direct $M' \times Q$. Comme P est un monoïde quotient de M' il suffit donc de montrer que sous l'hypothèse $M \in \underline{\underline{G}}\,\underline{\underline{D}}_f \cup \underline{\underline{G}}\,\underline{\underline{D}}_f 1$, Q se trouve être un sous monoïde du produit *direct* $G \times P$ (qui est lui-même un sous monoïde de GoP).

(2). Ceci est trivial quand M appartient à $\underline{\underline{D}}_f 1$ car cette hypothèse implique que J soit un singolet et que par conséquent

P soit le monoïde trivial {1}.

Nous supposons donc désormais $M \in \underline{G}\,\underline{D}_f$.

(3). Soit $\bar{e}_1 = (f_1, e_1)$ un idempotent fixe dans l'idéal minimum K' de Q. Son support $e \in P$ est une application de I sur un élément i_1 de cet ensemble et f_1 est une application de S dans G telle que $i_1 f_1 = 1 (= 1_G)$. On peut supposer que $if_1 = 1$ pour chaque $i \in I$ car sinon on se ramenerait à ce cas en prenant deux éléments convenablement choisis (d,1) et (d',1) du sous-groupe de GoP et en effectuant l'isomorphisme interne $p \to (d,1)p\,(d',1)$ $(p \in GoP)$.

Supposons qu'il existe un autre idempotent $\bar{e}_2$ dans l'idéal à gauche engendré par $\bar{e}_1$. On a $\bar{e}_2 = (f_2, e_1)$ et, si $\bar{e}_2 \neq \bar{e}_1$, il existe un $i \in I$ pour lequel $if_2 = g \neq 1$. Soit $\bar{e}_3$ l'idempotent du groupe H_1^i intersection de L^i et de l'idéal à droite $R_{1,i}$ engendré par $\bar{e}_1$. On a que $\bar{e}_3\,\bar{e}_2$ est l'élément g du groupe $L^{i1} \cap R_1$.

Ceci est impossible quand M appartient à $\underline{G}\,\underline{D}_f$ puisque l'identité (#) implique que le produit de deux idempotents soit apériodique, et on en conclut que sous cette hypothèse K' est constitué par l'idéal minimum à droite R_1. Par conséquent, K' est l'ensemble des paires (f, e_j) où e_j est l'application de J sur j $(j \in J)$ et où chaque application f envoie J sur un seul élément du groupe G.

Considérant un élément quelconque $\bar{q} = (f, p) \in Q$ et calculant $q\,\bar{e}_1$ on en déduit que l'image de son application f est encore un élément unique $\bar{q}\gamma \in G$. Il est clair que γ est un morphisme ce qui conclut la preuve.

Q.E.D.

Il résulte de la preuve que l'on a les inclusions :

$$\underline{G} \subset G\,\underline{D}_f 1r \subset G\,\underline{D}_f 1 \subset \underline{D}_f$$

PREUVE DES PROPRIETES 2 ET 3.

Ainsi qu'on l'a dit plus haut elle résultera de celle de l'énoncé suivant.

IV.5. Soit $\underline{G}$ une variété de groupes finis. Pour chaque alphabet A, la famille $A^*\text{-}G\,\underline{D}_f$ (resp. $A^*\text{-}G\,\underline{D}_f 1$; resp. $A^*\text{-}G\,\underline{D}1r$) est la plus petite famille de parties de A^* égale à sa complétion polynomiale non ambiguë (resp. déterministe ; resp. bi-déterministe) qui contienne les intersections de ses membres avec les parties de $A^*\text{-}\underline{G}$.

PREUVE. En raison de IV.2. il reste seulement à vérifier que si

une partie X de A^* a son monoïde syntaxique $M = A^*\mu$ dans les variétés mentionnées dans l'énoncé on peut l'obtenir par les opérations permises. Ceci est trivial quand $M = \{1\}$ puisque dans ce cas $X = A^*$ et on peut donc procéder par induction sur le nombre d'éléments de M. De plus, comme les completions polynomiales sont fermées par union disjointe finie on peut supposer que $X\mu = x$ où, d'après IV.3 (i), cet élément appartient à l'idéal 0-minimal K de M. Si K est apériodique (et en particulier si $K^2 = 0$) le résultat découle de IV.3 (ii) et (iii) puisque l'hypothèse $M \in \underline{D}_f$ implique que D soit un semi-groupe quand $K^2 \neq 0$. Sinon, d'après IV.4., il existe un morphisme γ de A^* dans un groupe G de $\underline{G}$ et un élément $g \in G$ tel que $X = X' \cap g\gamma^{-1}$ où X' a pour monoïde syntaxique un quotient du monoïde $M' \in \Delta M$ et ou par conséquent il satisfait les conditions requises en vertu de l'hypothèse d'induction.

Q.E.D.

REFERENCES

1. Brzozowski J.A., Culik II, K. and Gabriellian A, Classification of non counting events, J. of Computer and System Sci, 5 (1971) 41-53.
2. Brzozowski J., Run languages à paraître dans Discrete Maths.
3. Césari Y., Sur un algorithme donnant les codes bipréfixes finis, Math. Syst. Theory 6 (1972) 221-223.
4. Clifford A.H. and G.B. Preston, The algebraic theory of semigroups, Amer. Math. Soc., Providence, R.I., Vol I, 1961.
5. Eilenberg S., Automata, languages and machines, Vol B, Academic Press, New York and London, 1976.
6. Lallement G., Regular semigroups with $\mathcal{D}=\mathcal{R}$ as syntactic monoids of finite prefix codes, à paraître dans Theoretical Computer Science.
7. Lallement G. and E. Milito, Recognizable languages and finite semilattices of groups, Semigroup Forum, 11 (1975), 181-184.
8. Nc Naughton R. and S. Pappert., Counter free automata. MIT Press (1971).
9. Perrin D., Codes bipréfixes et groupes de permutations. Thèse Paris (1975).
10. Petrich M., The maximal semilattice decomposition of semigroups. Math. Zeit. 85 (1964) 68-82.
11. Rhodes J.L., Algebraic theory of finite semigroups, in Semigroups, K.W. Folley Ed., Academic Press, 1969.

12. Rhodes J.L. and B.R. Tilson, Local Structure theorems for finite semigroups, in Algebraic theory of machines, languages, and semigroups, M.A. Arbib Ed., Academic Press, 1968.
13. Rhodes J.L. and D. Allen Jr., Synthesis of the classical and modern theory of finite semigroups, Advances in Math. 11 (1973), 238-266.
14. Simon I., Piecewise testable events, Second Conf. on Automata Theory, Kaiserslautern, 1975, à paraître dans Lecture Notes in Computer Science (Springer Verlag).
15. Tamura T. and N. Kimura, Existence of greatest decomposition of semigroups, Kodai Math. Sem. Rep. 7 (1955) 83-84.
16. Tilson B., Decomposition and complexity of finite semigroups, Semigroup Forum, 3 (1971), 189-250.
17. Tilson B., Depth decomposition theorems, Chapter XI in Reference 5.
18. Tilson B., Complexity of two J-classes semigroups, Advances in Math 11 (1973), 215-237.
19. Tilson B., On the p-length of p-solvable semigroups, in Semigroups, K.W. Folley Ed., Academic Press, 1969.
20. Yamada M., On the greatest semilattice decomposition of semigroups. Kodai. Math. Sem. Rep. 7 (1955), 59-62.

Université de Paris VII
U.E.R. de Mathématiques
Tour 45-55, 5e Etage
2, place Jussieu
Paris 75005

Received Feb. 15, 1976; in revised and final form 15 July, 1976

Theoretical Computer Science 3 (1976) 243–259.

SUR LES RELATIONS RATIONNELLES ENTRE MONOIDES LIBRES

M.P. SCHÜTZENBERGER
Université de Paris VII, Paris, et I.R.I.A., Le Chesnay, Yvelines, France

Communiqué par Maurice Nivat
Reçu en mars 1976

Résumé. On applique la théorie de S. Eilenberg au moyen de la méthode des transducteurs de M. Nivat pour obtenir quelques indications sur la vitesse de croissance en fonction de la longueur du mot du nombre de mots de l'image d'une relation rationnelle.

1. Introduction

(1) L'objectif du présent travail est de préciser un point de la théorie des relations rationnelles entre monoïdes libres développée par Eilenberg dans le chapitre IX de son traité [1] auquel nous ferons de larges emprunts et auquel nous nous permettons de renvoyer le lecteur pour la motivation et un historique de sujet depuis les travaux fondamentaux de Elgot et Mezei [2].

On rappelle qu'étant donnés deux monoïdes libres A^* et B^* (engendrés respectivement par les alphabets finis A et B), une relation rationnelle $\rho : A^* \to B^*$ est une application de A^* dans le semi-anneau 2^{B^*} des parties de B^* dont le graphe est une partie *rationnelle* [1, chapitre VII] du produit direct $A^* \times B^*$. Ces relations forment elles-mêmes un semi-anneau si l'on définit la somme $\sigma = \rho + \rho'$ et le produit $\pi = \rho\rho'$ de deux d'entre elles par la condition que pour chaque mot a de A^* on ait:

$$a\sigma = a\rho + a\rho' \quad \text{et} \quad a\pi = \{(a'\rho)(a''\rho') : a', a'' \in A^* ; a'a''\}$$

(où $(a'\rho)(a''\rho')$ désigne le produit dans le semi-anneau 2^{B^*} des parties $a'\rho$ et $a''\rho'$ de B^*). La restriction d'une relation ρ à une partie D de A^* est la relation $\rho' : A^* \to B^*$ telle que pour chaque mot a on ait $a\rho = a$ ou $= 0$ selon que $a \in D$ ou non. Quand ρ est rationnelle il en est de même de sa restriction à chaque partie *reconnaissable* D de A^* (c'est-à-dire à chaque D tel que $D\varphi\varphi^{-1} = D$ pour un morphisme φ de A^* dans un monoïde fini). Nous ne considérerons ici que les relations ρ telles que l'image $a\rho$ de chaque mot a de A^* soit une partie *finie* de B^*. Pour abréger on notera $\| X \|$ le nombre d'élément de chaque partie X de B^* et on appelera *norme* de ρ le supremum de $\| a\rho \|$ sur tous les mots a de A^*. Un rôle particulier est joué par les relations de norme un que nous appelerons *fonctionnelles*

puisque ce sont des fonctions (= applications partielles) de A^* dans B^*. Notre résultat principal est la propriété ci-dessous. Dans celle-ci, $A^+ = A^*\backslash 1$ est le semi-groupe libre engendré par A et, comme d'usage, $|a|$ désigne la longueur du mot a.

Propriété. *Toute relation rationnelle $\rho : A^* \to B^*$ satisfait l'une des trois conditions suivantes*:

(i) *Il existe trois mots, $a', p, a'' \in A^*$ tels que l'on ait $\|(a'p^n p'')\rho\| \geqslant 2^n$ pour tout $n \in \mathbf{N}$.*

(ii) *Il existe des entiers d et K tels que l'on ait $\|a\rho\| \leqslant K|a|^d$ pour tout mot a de A^+ et trois mots tels que $\|(a'p^n a'')\rho\| \geqslant n+1$ $(n \in \mathbf{N})$.*

(iii) *ρ est une somme finie de relations rationnelles fonctionnelles (et a donc une norme finie).*

Nous dirons qu'une relation ρ est *cyclique* ssi son image est contenue dans un sous monoïde h^* de B^* engendré par un seul mot h. Une telle relation peut aussi être considérée comme une relation de A^* dans le semi-groupe additif des entiers. On constatera que les relations satisfaisant (ii) ou (iii) sont les polynomes (= sommes finies de produits finis) en des relations fonctionnelles et cycliques. J'ignore si toute relation cyclique est un polynome en des relations fonctionnelles. La distinction entre (i) et (ii) introduit une certaine complication et la preuve de la Propriété ne se trouvera achevée qu'à la fin de la Section 3.

Dans la Section 2 on examinera préalablement les relations fonctionnelles dont on retrouve après Nivat et Eilenberg une représentation maniable. Ces résultats sont nécessaires pour la preuve de la Propriété. Ils sont repris dans la Section 4 où l'on montre notament que quand ρ a une norme finie, on peut la représenter comme la somme d'une relation de domaine fini et de d relations fonctionnelles où $d = \min\{\|A^n A \cap \rho\| : n \in \mathbf{N}\} = \overline{\lim}_{n\to\infty}\{\|a\rho\| : |a| \geqslant n\}$.

(2) Dans tout ce travail nous employerons la méthode des *transducteurs* de Nivat [4]. Compte-tenu de l'hypothèse selon laquelle la relation rationnelle ρ considérée envoye chaque mot sur une partie *finie* de B^*, ceci signifie que ρ est définie par un ensemble fini Q, deux éléments distingués q_1, q_m de Q, et un morphisme de semi-groupe μ de A^* dans le monoïde $\mathbf{F}$ des $Q \times Q$ matrices ayant pour entrées des parties *finies* du semi-anneau 2^{B^*}. Pour chaque mot a de A^* on a $a\rho = a\mu(q, q_m)$ = l'entrée (q_1, q_m) de la matrice $a\mu$. Le *support* de cette dernière est la relation binaire $a\mu\#$ sur Q formée des paires (q, q') pour lesquelles l'entrée $a\mu(q, q')$ n'est pas nulle. Les théorèmes fondamentaux de la théorie des relations rationnelles permettent de supposer que le transducteur $\mu(q_1, q_m)$ de ρ est *émondé* ("Trim") en ce sens que pour chaque $q \in Q$ il existe $a, a' \in A^*$ tels que $(q_1, q) \in a\mu$ et $(q, q_m) \in a'\mu \neq$. On sait en outre que quand $1\rho = 0$ et $q^1 \neq q_m$ ou quand $1\rho = 1$ et $q_1 = q_m$ le morphisme μ est un morphisme de monoïde.

Nous concluons cette introduction par l'énoncé suivant qui couvre une partie des assertions avancées dans la Propriété.

1.1. *Soit ρ une relation rationnelle telle que $a\rho$ soit fini pour tout mot a et que $1\rho = 0$. Il existe un entier K tel que l'on ait identiquement $\|a\rho\| \leqslant K^{|a|}$ $(a \in A^*)$. Si ρ est cyclique cette inégalité peut être remplacée par $\|a\rho\| \leqslant K|a|$ $(a \in A^*)$.*

Enfin si ρ est un polynome en des relations cycliques ou fonctionnelles, il existe un entier d pour lequel $\|a\rho\| \leqslant K|a|^d$ $(a \in A^*)$.

Preuve. On vient de voir que ρ peut être définie par un morphisme μ de A^* dans le monoïde **F**. Soit L le maximum de la longueur des mots de B^* figurant dans les entrées des matrices génératrices $a\mu$ $(a \in A)$. Pour chaque mot a de A^*, tous les mots figurant dans $a\mu$ sont de longueur au plus $|a|L$. Ceci établit la première inégalité puisque posant $m = \mathrm{card}(B)$, le monoïde B^* a exactement $(m-1)^{-1}(m^{n+1}-1)$ mots de longueur au plus n pour chaque $n \in \mathbf{N}$. Le même argument donne la seconde inégalité puisque, quand ρ est cyclique, son image est contenue dans un sous monoïde cyclique h^* de B^* qui contient au plus $n+1$ mots de longueur $\leqslant n|h|$.

Considérons maintenant un produit $\rho = \rho_1\rho_2\cdots\rho_k$ où chaque ρ_i est une relation cyclique ou fonctionnelle. L'image $a\rho$ d'un mot quelconque est par définition la somme des produits $(a_1\rho_1)(a_2\rho_2)\cdots(a_k\rho_k)$ sur toutes les factorisations $a = a_1a_2\cdots a_k$ du mot a. Le nombre de celles-ci est borné par une fonction polynomiale de degré $k-1$ en $|a|$ ce qui établit la dernière inégalité. □

2. Le cas fonctionnel

(1) Nous considérons un morphisme de monoïde μ de A^* dans le semi-anneau **F** qui a été défini dans l'introduction et $q, q' \in Q$ étant une paire fixe quelconque, nous établissons d'abord le fait suivant:

2.1. *On a $\|a\mu(q,q')\| \leqslant 1$ pour tout $a \in A^*$ ssi cette inégalité est vérifiée par tous les mots de longueur au plus $1+2m(m-1)$ où $m = \mathrm{card}(Q)$.*

Preuve. Il suffit de vérifier que si $a = a_1a_2\cdots a_n$ $(a_1, a_2, \ldots, a_n \in A)$ est un mot de longueur minimum $|a| = n$ pour lequel $\|a\mu(q,q')\| \geqslant 2$, l'hypothèse $n > L = 1+2m(m-1)$ conduit à une contradiction.

Comme $|a|$ est minimum, il existe au moins une suite de $n-1$ paires (q_j, q'_j) $(1 \leqslant j \leqslant n-1\,;\, q_j \neq q'_j)$ telles que posant $q_0 = q'_0 = q$, $q_n = q'_n = q'$ et $b_j = a_j\mu(q_{j-1}, q_j)$, $b'_j = a_j\mu(q'_{j-1}, q'_j)$, les produits $b = b_1b_2\cdots b_n$ et $b' = b'_1b'_2\cdots b'_n$ (qui sont des éléments de $a\mu(q,q')$) sont deux mots distincts.

Supposons $n > L$. Il existe trois indices $i < j < k$ tels que $(q_i, q'_i) = (q_j q'_j) = (q_k, q'_k)$ ce qui détermine une factorisation $a = f_1 f_2 f_3 f_4$ où $f_1 = a_1 a_2 \cdots a_i$; $f_2 = a_{i+1} \cdots a_j$; $f_3 = a_{j+1} \cdots a_k$; $f_4 = a_{k+1} \cdots a_n$. Nous définissons de même les factorisations $b = g_1 g_2 g_3 g_4$ et $b' = g'_1 g'_2 g'_3 g'_4$ en remplaçant dans les expressions ci-dessus les a_s par les b_s ou les b'_s $(1 \leqslant s \leqslant n)$. Par construction on a les trois inclusions:

$$g_1 g_4, g'_1 g'_4 \in (f_1 f_4)\mu(q, q'); \quad g_1 g_2 g_4, g'_1 g'_2 g'_4 \in (f_1 f_2 f_4)\mu(q, q');$$

$$g_1 g_3 g_4, q'_1 q'_3 q'_4 \in (f_1 f_3 f_4)\mu(q, q').$$

En raison du caractère minimal de a, on en déduit les équations

$$g_1 g_4 = g'_1 g'_4; \quad g_1 g_2 g_4 = g'_1 g'_2 g'_4; \quad g_1 g_3 g_4 = g'_1 g'_3 g'_4;$$

où l'on peut supposer que, par exemple, $|g_1| \leqslant |g'_1|$.

La première équation équivaut alors à l'existence d'un mot h tel que $g'_1 = g_1 h$ et $g_4 = h g'_4$. En reportant ceci dans les deux autres, on obtient après simplification, $h g_2 = g'_2 h$ et $h g_3 = g'_3 h$.

Par conséquent $b = g_1 g_2 g_3 g_4 = g_1 g_2 g_3 h g'_4 = g_1 g_2 h g'_3 g'_4 = g_1 h g'_2 g'_3 g'_4 = g'_1 g'_2 g'_3 g'_4 = b'$ en contradiction avec $b \neq b'$. □

(2) Nous dirons qu'un morphisme μ est *fonctionnel* ssi la norme

$$\|a\mu\| = \max\{\|a\mu(q, q')\| : (q, q') \in Q \times Q\}$$

de toutes les matrices $a\mu$ $(a \in A^*)$ est au plus 1, c'est à dire ssi toutes les entrées non nulles des matrices $a\mu$ sont des mots. On voit facilement que si μ est émondé et $\rho = \mu(q_1, q_m)$ l'hypothèse que ρ est fonctionnelle entraine qu'il en soit de même de μ.

Nous nous proposons ici de déduire d'un morphisme fonctionnel μ un autre morphisme λ, qui soit aussi un transducteur pour ρ et qui possède la propriété supplémentaire que son caractère fonctionnel résulte a priori de la structure des supports $a\lambda\#$ des matrices $a\lambda$ $(a \in A^*)$ et des conditions initiales $\|a\lambda\| \leqslant 1$ $(a \in A)$.

C'est à quelques détails près la théorie développée par Nivat [3, Section 7]. Au moyen d'une construction plus compliquée, nous retrouvons les *bimachines* de Eilenberg [1, chapitre XI, 7] et une partie de son Théorème 7.1. Tout ceci sera utilisé pour étudier la norme d'un polynome en des relations fonctionnelles dans les Sections 2(3) et 4.

Considérons d'abord un monoïde M de $Q \times Q$ matrices sur un semi-anneau unitaire quelconque $\mathbf{B}$. Suivant Nivat [4, Section 7] nous dirons que M est un *monoïde* $\{0, 1\}$ ssi les supports $m\#$ de ses éléments satisfont la condition (ZU): Pour chaque paire $m, m' \in M$ et chaque entrée $(q, q') \in (mm')\#$, il existe exactement un $q'' \in Q$ pour lequel $(q, q'') \in m\#$ et $(q'', q') \in m'\#$.

La condition (ZU) a pour conséquence que seule la structure multiplicative de $\mathbf{B}$

(et le fait que 0 soit un élément neutre additif) interviennent dans le calcul du produit de deux matrices de M. Il en résulte que si μ est un morphisme de A^* dans un sous monoïde $\{0,1\}$ de $\mathbf{F}$ il est fonctionnel ssi chacune des matrices génératrices $a\mu$ $(a \in A)$ a norme au plus 1.

La condition (ZU) est satisfaite en particulier par les matrices dites *monomiales* (resp. *monomiales par colonne*) caractérisées par la propriété que chaque ligne (resp. colonne) a au plus une entrée non nulle. Nous aurons besoin de la généralisation suivante de cette notion. Disons qu'une matrice m est *semi-monomiale* ssi son ensemble d'indice est un produit direct $I \times J$ et si en outre:

(i) il existe une application partielle $i \to i \cdot m$ de I dans lui-même;

(ii) pour chaque $(i,i') \in I \times I$, la $(J \times J)$-sous matrice bloc $m_{ii'} = (m(ij,i'j'))(j,j' \in J)$ est une matrice monomiale par colonne quand $i' = i \cdot m$ et nulle, sinon.

Il est clair que l'ensemble des $(I \times J) \times (I \times J)$ matrices semi-monomiales à entrées dans $\mathbf{B}$ forme un monoïde de matrices $\{0,1\}$.

Il en est de même dans le cas encore plus particulier où toutes les $J \times J$ sous matrices blocs non nulles $m_{ii'}$ de chaque matrice m ont le même support et où nous dirons alors qu'il s'agit d'un *semi-groupe de matrices de bimachines*. De façon équivalente, une $(I \times J) \times (I \times J)$ matrice m est semi-monomiale (resp. de bimachine) ssi elle appartient au produit en couronne (resp. kroneckerien) des $(J \times J)$-matrices monomiales par colonne dans les $(I \times I)$-matrices monomiales.

Pour abréger, si Ket K' sont deux parties de $I \times J$, nous désignons par $m(K,K')$ pour chaque $(I \times J) \times (I \times J)$ matrice m, la somme des entrées $m(ij,i'j')$ pour $(i,j) \in K$, $(i',j') \in K'$.

2.2. *Soit $\rho = \mu(q_1, q_m)$ une relation rationnelle fonctionnelle. Il existe un ensemble fini V, un morphisme fonctionnel λ de A^* dans le monoïde des $(V \times Q) \times (V \times Q)$ matrices semi-monomiales, un $v_1 \in V$ et une partie V_m de V tels que l'on ait identiquement $a\rho = a\lambda(v_1 q_1, V_m q_m)$.*

Preuve. En raison de l'hypothèse faite dans l'introduction que μ est émondé, le caractère fonctionnel de ρ implique que toutes les matrices $a\mu$ $(a \in A^*)$ soient de norme au plus 1.

Soient u le Q-vecteur égal à la ligne q_1 de la matrice 1μ et $v_1 = u\#$ son support. Nous désignons par V l'ensemble des supports non nuls des lignes q_1 des matrices $a\mu$ $(a \in A^*)$ (c'est à dire des vecteurs $u \cdot a\mu$) et nous introduisons une action partielle $V \times A \to V$ en définissant $v' \cdot a$ comme le support commun des vecteurs $u \cdot (a'a\mu)$ pour tous les mots a' tels que $u(a'\mu) = v' \cdot (v' \in V)$.

Nous construisons maintenant le morphisme λ en deux étapes. Tout d'abord pour chaque lettre $a \in A$, $v \in V$ et $q \in Q$ tels que $v \cdot a(q) = 0$, on peut choisir arbitrairement un q' pour lequel on a à la fois $v(q') \neq 0$ et $a\mu(q',q) \neq 0$. Ceci permet de définir la $Q \times Q$ matrice $a\mu'_v$ en posant $a\mu'_v(q'',q) = a\mu(q'',q)$ ou $= 0$

selon que $q'' = q'$ ou non. Il est clair que toutes ces matrices $a\mu'_v$ sont monomiales par colonne et de norme $\leqslant 1$.

Ensuite nous définissons pour chaque lettre a la $(V \times Q) \times (V \times Q)$ matrice $a\lambda$ par la condition que chacun de ses (v, v') blocs $a\lambda_{v,v'}$ $(v, v' \in V)$ soit égal à $a\mu'_v$ où à 0 selon que $v' = v \cdot a$ ou non. Comme $v \to v \cdot a$ est une action partielle, les matrices $a\lambda$ sont bien semi-monomiales et de norme au plus 1.

On vérifie directement (par induction sur la longueur du mot) que pour chaque $a \in A^*$, la ligne $v_1 q_1$ de la matrice $a\lambda$ est un vecteur dont les coordonnées non nulles ont pour index les paires $(v_1 \cdot a, q)$ où $v_1 \cdot a(q) \neq 0$.

Comme le vecteur $u \cdot a\mu$ est par hypothèse un vecteur de norme au plus 1, il en résulte instantanément que la ligne $v_1 q_1$ de a est le $V \times Q$ vecteur dont chaque coordonnée (v, q) est égal à la coordonnée q du vecteur $u \cdot a$ quand $v = v_1 a$ et à 0 sinon. □

(3) Venons en aux bimachines. Modifiant très légèrement la définition de Eilenberg [1, XI, 7] nous appelerons *bimachine* toute application partielle $\nu : A^* \times A^* \times A^* \to B^*$ satisfaisant les deux conditions suivantes:

(i) Pour tout $a_1, a_2, a_3, a_4 \in A^*$ on a

$$(a_1; a_2 a_3; a_4)\nu = (a_1; a_2; a_3 a_4)\nu \cdot (a_1 a_2; a_3; a_4)\nu.$$

(ii) Il existe un morphisme ϕ de A^* dans un monoïde fini tel que pour tout $a, a_1, a_2, a_3, a_4 \in A^*$, les équations $a_1\phi = a_3\phi$ et $a_2\phi = a_4\phi$ impliquent $(a_1; a; a_2)\nu = (a_3; a; a_4)\nu$.

La *relation définie par la bimachine* ν est l'application partielle $\bar{\nu}$ envoyant chaque mot a sur $(1, a, 1)\nu$.

On vérifie facilement que, réciproquement, étant donné un morphisme ϕ de A^* dans un monoïde fini S, toute application partielle $\nu' : S \times A \times S \to B^*$ définit la restriction à A^+ d'une bimachine. En effet, l'identité (i) équivaut à la condition que pour chaque mot $a = a_1 a_2 \cdots a_n$ $(n \geqslant 1, a_1, a_2, \ldots, a_n \in A)$ la valeur de $a\bar{\nu}$ soit le produit sur $i = 1, 2, \ldots, n$ des termes

$$((a_1 \cdots a_{i-1})\phi\ ;\ a_i\ ;\ (a_{i+1} \cdots a_n)\phi)\nu'$$

(avec la convention habituelle que pour $i = 1$ ou $i = n$, le produit vide vaut 1). La même identité détermine presque complètement les valeurs des $(a; 1; a)\nu$ qui ne peuvent être que $1 = 1_{B^*}$ ou 0. Si (comme on peut toujours le supposer) $1\phi\phi^{-1} = 1$, on peut choisir arbitrairement $1\bar{\nu} = 1$ ou $1\bar{\nu} = 0$.

Enfin nous réserverons le nom de *morphisme de la bimachine* ν aux morphismes ϕ de A^* dans un monoïde fini qui, en plus de (ii) satisfont $1\phi\phi^{-1} = 1$ et la condition que pour chaque paire de mots $a_1, a_2 \in A^*$, le domaine D' de la relation $\rho' \mapsto (a_1; a; a_2)\nu$ soit reconnaissable par ϕ (c'est à dire que $D' = D'\phi\phi^{-1}$). Comme ρ' ne dépend que de a_1 et a_2 il n'existe qu'un nombre fini de tels domaines D' et chacun d'eux est reconnaissable. Comme en outre $\{1\}$ est reconnaissable, on peut

définir de façon naturelle pour tout morphisme $\phi' : A^* \to S'$ satisfaisant (ii) un morphisme $\phi = \phi' \times \psi : A^* \to S = S' \times T$ qui soit un morphisme de ν.

2.3. *Soit $\rho : A^* \to B^*$ une relation rationnelle fonctionnelle. Il existe un morphisme ϕ de A^* dans un monoïde fini S tel que ρ puisse être définie par l'un quelconque des trois objets suivants*:

(a) *un morphisme μ de A^* dans un monoïde $\{0,1\}$ de matrices tel que $\mu\# = \phi$*;

(b) *une bimachine ν dont ϕ est un morphisme*;

(c) *un morphisme π de A^* dans un monoïde de bimachine de $(S \times S) \times (S \times S)$ matrices tel que $\phi = \pi\#$.*

Preuve. Nous partons d'un morphisme μ de A^* dans un monoïde $\{0,1\}$ de $Q \times Q$ matrices de norme $\leqslant 1$ telle que l'on ait identiquement $a\rho = a\mu(q_1, q')$ pour une certaine paire $q_1 \in Q$, $q' \subset Q$. Pour abréger nous désignons par ϕ le morphisme $\mu\#$ envoyant chaque mot sur le support de la matrice $a\mu$.

Soient a, a', et a'' trois mots dont le produit $aa'a''$ est dans le domaine de ρ. En raison de la propriété (ZU) et du caractère fonctionnel de ρ il existe un et un seul triple $(q, q', q'') \subset Q \times Q \times Q'$ pour lequel les trois entrées $b = a\mu(q_1, q)$, $b' = a'\mu(q_1 q')$ et $b'' = a''\mu(q', q'')$ sont simultanément non nulles. On a alors $(aa'a'')\rho = bb'b''$. Il est clair que le mot b' ne dépend que de la matrice $a'\mu$ et des supports $s = a\phi$ et $s'' = a''\phi$ des matrices $a\mu$ et $a''\mu$. Nous pouvons donc définir une application partielle ν' de $S \times A^* \times S$ dans B^* $(S = A^*\phi)$ en posant $b = (s; a'; s'')\nu'$. Prenant $a = a'' = 1$, le calcul précédent montre que $a'\rho = (1; a', 1)\nu'$ pour tout mot a' de A^*. Prenons maintenant a et a'' quelconques et supposons $a' = a_2 a_3$ $(a_2, a_3 \in A^*)$. On vérifie l'identité

$$(a\phi\,;\, a_2a_3\,;\, a''\phi)\nu' = (a\phi\,;\, a_2\,;\, (a_3a''\phi)\nu' \cdot ((aa_2)\phi\,;\, a_3\,;\, a''\phi)\nu'$$

qui montre que $\nu = (\phi\,;\,;\,\phi)\nu'$ est une bimachine dont ϕ est un morphisme.

Supposons maintenant donnés ν et ϕ. Pour chaque $s, s'' \in S$, $a' \in A^*$ nous désignons par $(s; a'; s'')\nu'$ la valeur commune de $(a; a'; a'')\nu$ pour n'importe quels mots $a \in s\phi^{-1}$ et $a'' \in s''\phi^{-1}$. Nous associons à chaque mot à $1a\,(S \times S) \times (S \times S)$ matrice $a\pi$ par la condition que pour tout $s_1, s', s_2, s_2' \in S$ on ait $a\pi(s_1, s_2\,;\, s_1's_2') = (s_1; a\,;\, s_2')\nu'$ ou 0 selon que la double condition $s_1' = s_1 \cdot (a\phi)$ et $s_2 = (a\phi) \cdot s_2'$ est ou non satisfaite.

On vérifie facilement que π est un morphisme de A^* dans un monoïde de matrices de bimachine (de norme $\leqslant 1$) tel que $a\rho$ soit identiquement égal à $a\pi(1, S; S, 1)$ et plus précisement à l'entrée $(1, s\,;\, s, 1)$ où $s = a\phi$. Le morphisme $\pi\#$ coincide avec ϕ puisque l'on peut considérer $a \to a\pi\#$ comme le produit kronekerien des représentations régulières gauches et droites de A sur $S = A^*\varphi$. Ceci achève la preuve puisque tout monoïde de bimachine est un monoïde (ZU). □

On en déduit:

Théorème (Eilenberg). *Toute relation rationnelle fonctionnelle peut être réalisée par une bimachine.*

Preuve. Ceci découle immédiatement de 2.2 et de l'énoncé précédent. □

(4) Nous terminons cette section en considérant les produits de relations fonctionnelles.

2.4. *Soit $\pi : A^* \to B^*$ un produit de relations rationnelles fonctionnelles qui n'est pas une somme finie de relations rationnelles fonctionnelles. Il existe trois mots $a', p, a'' \in A^*$ tels que $\|(a'p^n a'')\pi\| \geq n+1$ pour tout entier positif n.*

Preuve. Par induction sur le nombre de facteurs de produit, il suffit de considérer le cas de $\pi = \bar{\mu} \cdot \bar{\nu}$ où $\bar{\mu}$ et $\bar{\nu}$ sont les relations fonctionnelles définies respectivement par les bimachines μ et ν. Nous pouvons construire un morphisme ϕ de A^* dans un monoïde fini S qui est simultanément un morphisme de μ et de ν. Soit $s \in S$ quelconque. Nous engendrons une bimachine μ_s en posant pour chaque $a \in A$ et $a_1, a_2 \in A^*$,

$$(a_1, a, a_2)\mu_s = 0 \quad \text{si } (a_1 a)\phi \neq s \quad \text{et} \quad (a_1, a_2, a_2)\mu \text{ sinon.}$$

Par définition, le domaine de la relation $\bar{\mu}_s$ est contenu dans $s\phi^{-1}$ et $\bar{\mu}_s$ est égale à $\bar{\mu}$ sur son domaine. La même construction s'applique à ν et nous avons donc que π est égale à la somme finie des produits de relation $\bar{\mu}_s \bar{\nu}_{s'}$, $(s, s' \in S)$. Nous pouvons donc supposer pour simplifier que $\mu = \mu_s$ et $\nu = \nu_t$ pour une certaine paire $s, t \in S \backslash 1$.

Si chacun des mots du domaine de $\pi = \mu\nu$ admet exactement une factorisation comme produit d'un mot de $s\phi^{-1}$ par un mot de $t\phi^{-1}$, le résultat est établi puisqu'alors π est fonctionnelle. Dans le cas contraire, soit a un mot du domaine de π ne satisfaisant pas les conditions d'unicité ci-dessus. Il admet une factorisation maximale unique $a = a' p_1 p_2 \cdots p_n a''$ $(p, \cdots, p_n \in A^+, n \geq 1)$ telle que l'on ait identiquement $a' p_1 \cdots p_i \in s\phi^{-1}$; $p_{i+1} \cdots p_n a'' \in t\phi^{-1}$ $(0 \leq i \leq n)$.

Son image par π est constituée par les $n+1$ mots $b' q_1 \cdots q_i r_{i+1} \cdots r_n b''$ où pour abréger on a posé $b' = (1; a'; a'')\mu$; $b'' = (a'; a''; 1)\nu$; $q_i = (a'; p_i; a'')\mu$; $r_i = (a'; p_i; 1)\nu$ $(1 \leq i \leq n)$.

Désignons par P^* le sous monoïde de A^* formé des mots p tels que $s \cdot p\phi = s$ et $p\phi \cdot t = t$. C'est une partie reconnaissable de A^* et nous pouvons tester si les relations rationnelles fonctionnelles $\bar{\mu}' : p \mapsto (a'; p; a'')\mu$ et $\bar{\nu} : p \mapsto (a'; p; a'')\nu$ sont ou non égales sur P^*.

Dans le premier cas on a évidemment $q_i = r_i$ $(1 \leq i \leq n)$ et par conséquent π est fonctionnelle. Dans le second cas soit $p \in P^*$ tel que $q = p\bar{\mu}' \neq p\bar{\nu}'$. L'image par π du mot $a' p^n a''$ est formée des $n+1$ mots $b' q^m i^{n-m} b''$ $(0 \leq m \leq n)$ que l'on vérifie

immédiatement être distincts puisque toute égalité entre deux d'entre eux entrainerait une équation de la forme $q^k = r^k$ $(k \geqslant 1)$ en contradiction avec $q \neq r$. □

3. Le cas général

Nous continuons à faire tacitement l'hypothèse que chaque relation considérée donne une image *finie* à chaque mot de son domaine.

(1) Une relation $\rho : A^* \to B^*$ sera dite *minimale* ssi son domaine est $\{1\}$ ou une lettre de A. Elle sera dite *unitaire* ssi elle peut être mise sous la forme $\rho = \mu(q, q)$ où μ est un morphisme de monoïde de A^* dans un semi-anneau de $Q \times Q$ matrices et q un élément quelconque de Q.

Il est clair que chaque relation unitaire ρ satisfait $1\rho = 1$ et est sous-multiplicative en ce sens que $(a\rho)(a'\rho) \subset (aa')\rho$ pour tout $a, a' \in A^*$. Son domaine est donc un sous monoïde P^* de A^* (engendré par un ensemble minimal $P \subset A^+$, qui est vide ssi ρ est *triviale*). On rappelle qu'un morphisme μ de A^* dans un anneau de $Q \times Q$ matrices est *irréductible* ssi $Q \times Q$ est l'union sur tous les mots a des supports des matrices $a\mu$. Par conséquent si $\rho = \mu(q, q)$ où μ est émondé au sens donné à ce terme dans l'introduction, le morphisme μ est irréductible, puisque pour tout $q' \in Q$ il doit exister $a, a' \in A^*$ tels que $(q, q') \in a\mu \neq$ et $(q', q) \in a'\mu \neq$.

Un produit $\rho = \rho_1\rho_2 \cdots \rho_k$ de relations est *non ambigu* ssi tout mot a de son domaine admet exactement une factorisation $a = a_1a_2 \cdots a_k$ où chaque a_i est dans le domaine de ρ_i. Plus généralement, un polynome $\rho = \rho'_1 + \rho'_2 + \cdots \rho'_k$ est *non ambigu* ssi tous les produits ρ'_j sont non ambigus et ont des domaines deux à deux disjoints.

3.1. *Soit $\rho = \mu(q_1, q_m)$ une relation rationnelle. Il existe un algorithme ne dépendant que du morphisme $\mu \neq$ dans le monoïde des relations binaires sur Q qui permet d'exprimer ρ comme un polynome en des relations rationnelles minimales ou unitaires. Quand μ est un morphisme dans un monoïde $\{0, 1\}$, le polynome obtenu est non ambigu.*

Preuve. Nous pouvons supposer que μ est un morphisme de monoïde dans le semi-anneau **F** (de $Q \times Q$ matrices) et que $q_1 \neq q_m$. Soit ρ_1 la relation rationnelle unitaire $\mu(q_1, q_1)$.

Nous considérons d'abord le cas ù ρ_1 est triviale (en ce sens que son domaine est $\{1\}$). Ceci équivaut à l'hypothèse que toutes les colonnes q_1 des matrices $a\mu$ $(a \in A^+)$ sont nulles.

Soit $Q' = Q \backslash q_1$. Pour chaque $q \in Q'$, $a \in A$ nous posons $\rho'_q = \mu(q, q_m)$ et $\rho_{a,q}$ = la relation de domaine $\{a\}$ égale à $a\mu(q_1, q)$ sur celui-ci. La relation ρ est la somme sur tous les $q \in Q'$, $a \in A$ des produits non ambigus $\rho_{a,q}\rho'_q$ et chaque $\rho_{a,q}$ est

une somme de relations minimales. Soit maintenant μ' la restriction de μ à $Q' \times Q'$, c'est à dire soit $a\mu'(q,q') = a\mu(q,q')$ pour chaque $a \in A^*, q, q' \in Q'$. En raison de l'hypothèse faite sur μ c'est un morphisme de A^* dans un semi-anneau de $Q' \times Q'$ matrice et l'on a $\rho'_q = \mu'(q, q_m)$ pour chacun des q de Q'.

Ceci conclut la preuve par induction sur card (Q) dans ce cas. En effet, quand μ est un morphisme dans un monoïde $\{0,1\}$ il en est encore de même de μ', chaque $\rho_{a,q}$ est minimale et la condition (ZU) montre que les produits $\rho_{a,q}\rho'_q$ ont des domaines disjoints.

Supposons maintenant que ρ_1 n'est pas triviale et définissons un morphisme μ'' de A^* dans F par sa restriction à A en remplaçant par 0 toutes les entrées de la colonne q_1 de chaque matrice $a\mu$ $(a \in A)$. La relation rationnelle $\rho'' = \mu''(q_1, q_m)$ satisfait les hypothèses du premier cas traité et il nous suffit donc de montrer que l'on a $\rho = \rho_1\rho''$ où le produit est non ambigu quand ρ est fonctionnelle puisque $A^*\mu''$ et un monoïde $\{0,1\}$ quand μ a la même propriété.

Soit donc $a = a_1 \cdots a_n$ $(n \geqslant 1, a_1, a_2, \ldots, a_n \in A)$ un mot du domaine de ρ. L'entrée $a\mu(a_1, q_m)$ est la somme du produit des entrées $a_i(q'_i, q'_{i+1})$ $(1 \leqslant i \leqslant n)$ sur toutes les suites $(q'_1 = q_1, q'_2, \ldots, q'_{n+1} = q_m)$ de $n+1$ états q'_j pour lesquelles ces entrées sont toutes non nulles. Pour chaque telle suite il existe un plus grand indice j $(1 \leqslant j \leqslant n)$ tel que $q'_j = q_1$. Le produit correspondant est contenu dans le produit des deux entrées $(a_i \cdots a_j)\mu(q_i, q_i)$ et $(a_{j+1} \cdots a_n)\mu''(q_1, q_m)$. Donc $\rho_1\rho'' \subset \rho$, d'où l'égalité cherchée puisque réciproquement toute relation $a'\rho_1 \neq 0$, $a''\rho'' \neq 0$ implique $(a'a'')\rho \neq 0$. Dans le cas fonctionnel, $a(q_1, q_m)$ est de façon unique un produit d'entrées non nulles et la factorisation $\rho = \rho_1\rho'$ est donc non ambigue. □

On notera que la construction précédente de la suite $(q'_1, \ldots, q'_{n+1})$ montre que quand ρ est fonctionnelle le domaine P^* de ρ_1 est engendré librement par l'ensemble générateur minimal P de P^*.

(2) Nous aurons besoin en outre de quelques résultats propres au semi-anneau 2^{B^*}. Nous les extrayons sans démonstration du livre de Lentin [2].

Pour chaque mot $b \in B^*$ soit $\sqrt{b}$ le plus court mot $h \in B^*$ tel que b soit contenu dans le monoïde cyclique $h^* = \Sigma_{0 \leqslant n} h^n$. On a évidement $h = \sqrt{h}$, c'est à dire que h est un mot *primitif*. Plus généralement, nous dirons qu'une partie P de B^* est *cyclique* ssi il existe un mot h (que l'on peut supposer primitif et noter $\sqrt{P}$) tel que $P \subset h^*$. Donc toute partie P' d'une partie cyclique P est aussi cyclique et $\sqrt{P} = \sqrt{P'}$ sauf si $P' \backslash 1 = \emptyset$.

Soit $P = \{b, c\}$ où $b, c \neq 1$. On sait que les assertions suivantes sont équivalentes:

(a) P n'est pas cyclique;

(b) $\sqrt{b} \neq \sqrt{c}$;

(c) $b^* \cap c^* = \{1\}$;

(d) P^* est isomorphe au monoïde libre à *deux* générateurs.

Nous utiliserons plus loin la remarque suivante:

3.2. *Soient $b \in B^+$ et P une partie cyclique de B^* qui n'est pas un singolet. Les parties $b + P$ et bP sont simultanément cycliques ou non.*

Preuve. Il est clair que $b + P$ est cyclique ssi $\sqrt{b} = \sqrt{P}$ et que ceci entraine que $\sqrt{bP} = \sqrt{P}$. Réciproquement, supposons que bP soit cyclique. Comme P n'est pas un singolet, P contient h^r et h^s où $h = \sqrt{P}$, $0 \leqslant r \leqslant s$, et bP contient les mots $bh^r = g^{r'}$, $bh^s = g^{s'}$ où $g = \sqrt{bP}$. On a $r' < s'$. Par conséquent $h^{s-r} = g^{s'-r'}$ ce qui entraine $h = g$ puisque ces deux mots sont primitifs et, enfin, $b = h^{r'-r}$. □

(3) Pour alléger l'écriture nous supposons ici que $Q = \{1, 2, \ldots, m\}$. Un morphisme μ de A^* dans F sera dit de *type cyclique* ssi il est possible de réindexer les éléments de Q de telle sorte que la matrice $A^*\mu$ (somme des matrices $a\mu$ pour $a \in A^*$) soit contenue dans une $Q \times Q$ matrice H satisfaisant les conditions suivantes:

Il existe m mots $b_j \in B^*$ tels que, posant $h_j = b_j b_{j+1} \cdots b_m b_1 \cdots b_{j-1}$ $(1 \leqslant j \leqslant m)$, on ait pour tout i, j, $H(i, i) = h_i^*$, et pour $i \neq j$, $H(i, j) = h_i^* H'(i, j)$ avec $H'(i, j) = b_i b_{i+1} \cdots b_{j-1}$ si $i < j$ ou si $i < j$ et $h_i = h_j$ et $H'(i, j) = b_i b_{i+1} \cdots b_m b_1 \cdots b_{j-1}$ sinon.

On vérifie directement que $H(i, j) = H'(i, j) h_j^*$ et que par conséquent $HH = H$.

Soit maintenant μ un morphisme irréductible au sens donné à ce terme à la fin de 3.1. Nous posons $A\mu = \Sigma\{a\mu = a \in A\}$, $A^*\mu = \Sigma\{a\mu : a \in A^*\}$, $\bar{M} = A\mu + A^2\mu + \cdots + A^{2m-1}\mu$ et $P = \bar{M}(1, 1)$. Il est clair que P est une partie cyclique de B^* quand μ est de type cyclique.

Réciproquement:

3.3. *Une condition suffisante pour que le morphisme irréducible μ soit de type cyclique est que P soit une partie cyclique de B^*.*

Preuve. L'énoncé est trivial si aucune des entrées de $A\mu$, (donc de $A^*\mu$) ne rencontre B^+ car il suffit de prendre alors tous les b_j égaux à 1 dans la définition de H. Nous supposons donc ce cas écarté.

Soient q et q' deux états *distincts* de Q. Comme μ est irréductible, la paire (q, q') est dans le support de la matrice $A^*\mu$, ce qui signifie qu'il existe une suite $(q'_1 = q, q'_2, \ldots, q'_n = q')$ et n lettres $a_i \in A$ tels que les entrées $a_i\mu\,(q'_i, q'_{i+1})$ $(1 \leqslant i \leqslant n-1)$ sont non nulles. On peut choisir les q'_i distincts et, puisque $m = \mathrm{Card}\,(Q)$, ceci montre que la matrice $M' = A\mu + A^2\mu + \cdots + A^{m-1}\mu$ a toutes ses entrées non diagonales non nulles. Comme au moins une des entrées de $A\mu$ rencontre B^+ il en résulte que la même chose est vraie de l'entrée $(1, 1)$ de $\bar{M} = M'(A\mu)M'$ et que le mot $h = \sqrt{P}$ appartient à B^+.

Considérons un état $q \neq 1$. On a l'inclusion $M'(1, q) \cdot M'(q, 1) \subset \bar{M}(1, 1) \subset h^*$.

Si $M'(1, q)$ n'est pas contenue dans h^*, ceci implique l'existence d'une factorisation bien définie $h = g'_q g''_q$ pour laquelle $M'(1, q) \subset h^* g'_q$ et $M'(q, 1) \subset g''_q h^*$. Dans le cas contraire, on doit avoir aussi $M'(q, 1) \subset h^*$ et nous posons $g'_q = g''_q = 1$.

Nous choisissons maintenant un indexage de Q tel que la suite des longueurs des mots g'_q soit non décroissante. Les $m-1$ équations $g'_q g''_q = h$ (ou $=1$) déterminent sans ambiguité m mots b_j tels que $g'_j = b_1 \cdots b_{j-1}$ $(2 \leqslant j \leqslant m)$. Maintenant pour chaque $(i,j)(i,j \neq 1)$ on a l'inclusion:

$$M'(1,i) \cdot A\mu(i,j) \cdot M'(j,1) \subset \bar{M}(1,1) \subset h^*$$

où $M'(1,i)$ et $M'(j,1)$ sont des parties non vides de $h^* g'_i$ et de $g''_j h^*$ respectivement. Exprimant ceci en fonction des mots b_h, on obtient la relation $A(i,j) \subset H(i,j)$ d'où le résultat puisque $HH = H$. □

3.4. *Soit $\mu : A^* \to \mathbf{F}$ un morphisme irréductible qui n'est pas fonctionnel. Il existe trois mots p, a', a'' tels que l'on ait $\|(a'p^n a'')\mu\| \geqslant \alpha(n)$ $(n \in \mathbf{N})$ avec $\alpha(n) = n+1$ ou $= 2^n$ selon que μ est ou non de type cyclique.*

Preuve. L'hypothèse que μ n'est pas fonctionnelle implique l'existence d'un mot p et d'états q, q' tels que $P = \rho\mu(q,q')$ contienne au moins deux mots distincts b et c. D'autre part quelques soient q_1 et q'_1 l'hypothèse que μ est irréductible implique l'existence de mots a' et a'' tels $a'\mu(q_1,q)$ et $a''\mu(q',q'_1)$ ne soient pas nuls et que par conséquent $\|(a'pa'')\mu(q_1,q'_1)\| \geqslant \|P\|$.

Il suffit donc de considérer une seule paire (q,q') et on peut même supposer que $q = q'$ ce que nous ferons désormais.

Pour chaque entier n on a $\{b,c\}^n \subset P^n \subset P^n \mu(q,q)$. Ceci établit l'inégalité cherchée quand P n'est pas cyclique puisque l'on peut alors prendre $b, c \in P$ tels que $\{b,c\}^*$ soit isomorphe au monoïde libre à deux générateurs, c'est à dire que $\|\{b,c\}^n\| = 2^n$ identiquement.

Si P est cyclique mais que μ ne l'est pas, nous pouvons trouver deux mots a_1 et a_2 tels que $\{d_1 = a_1\mu(q,q),\ d_2 = a_2\mu(q,q)\}$ ne soit pas cyclique. On a $d_i P \subset (a_i p)\mu(q,q)$, $i = 1,2$, et d'après 3.2, l'un au moins de ces deux ensembles n'est pas cyclique. Ceci achève la preuve quand μ n'est pas cyclique.

Supposons maintenant P cyclique c'est à dire $b = h^r$, $c = h^s$ $(r,s \in \mathbf{N})$ où $h = \sqrt{P}$. Pour chaque $n \in \mathbf{N}$, P^n contient les $n+1$ mots distincts h^{n_i} où $n_i = ir + (n-i)s$ $(0 \leqslant i \leqslant n)$ concluant la preuve. □

Ceci achève d'établir la Propriété énoncée dans l'introduction. En effet, soit $\rho : A^* \to B^*$ une relation rationnelle. S'il existe un mot de A^* dont l'image par ρ est infinie, l'eventualité (i) est réalisée (avec $p = 1$). Sinon (comme nous le supposons désormais) nous savons d'après 1.1 que ρ est un polynome en des relations fonctionnelles ou unitaires et nous distinguons deux cas selon que ces dernières sont toutes fonctionnelles ou que l'une au moins ne l'est pas.

Compte tenu de 1.2, l'énoncé 2.4 (resp. 3.4) montre alors que dans le premier (resp. second) cas l'une des éventualités (i) ou (ii) ou (iii) est réalisée.

Nous terminons la discussion dans la section suivante, en utilisant le résultat (qui

vient d'être établi) qu'une relation rationnelle a une nomme finie ssi elle est la somme d'un nombre fini de relations rationnelles fonctionnelles.

4. Les relations de norme finie

(1) Faisant référence à la terminologie introduite au début de la Section 3, nous considerons une relation rationnelle fonctionnelle ρ de domaine infini qui est un produit non ambigu de relations minimales ou unitaires. Regroupant les termes et omettant ceux qui sont triviaux, on en déduit de façon unique une expression de ρ comme un produit non ambigu $p = \tau_0\sigma_1 \cdots \tau_{k-1}\sigma_k\tau_k$ $(k \geqslant 1)$ où chaque τ_i est une relation dont le domaine est un mot $y_i \in A^*$ et chaque σ_i une relation fonctionnelle unitaire dont le domaine est le sous-monoïde X_i^* engendré librement par la partie non vide X_i de A^+.

Nous appelerons $(X) = (y_0, X_1, y_1, \ldots, X_k, y_k)$ $(k \geqslant 1)$ un *monome*. Son *domaine* sera la partie infinie $y_0X_1^*y_1 \cdots x_k^*y_k = x$ de A^* et nous dirons que la relation ρ est *compatible* avec (X). La suite $(\sigma) = (\tau_0, \sigma_1, \ldots, \sigma_k, \tau_k)$ sera dite *induite* par (X) sur ρ.

Nous montrons d'abord que l'ensemble Σ des suites induites par (X) sur ρ contient un élément distingué σ.

4.1. *La condition que la séquence* $(|y_0\tau_0|, |y_1\tau_1|, \ldots, |y_{k-1}\tau_{k-1}|)$ *soit minimale pour l'ordre léxicographique caractérise de façon unique une suite* σ *de* Σ. *Celle-ci jouit de la propriété que pour* $i = 0, 1, \ldots, h-1$ *les mots* $y_i\tau_i$ *et* $x\sigma_{i+1}$ $(x \in X_{i+1})$ *de* B^+ *n'ont pas de facteur droit commun non trivial.*

Preuve. Soient (σ) et (σ') deux suites de Σ, (σ) étant choisie de telle sorte que $t = y_0\tau_0$ soit de longueur minimale. Quelque soit le mot x de X_1 on a identiquement: $(y_0x^hy_1 \cdots y_h)\rho = ts^hu = t's'^hu'$ $(n \in \mathbf{N})$ où $s = x\sigma_1$, $u' = (y_1\tau_1) \cdots (y_h\tau_h)$; $t' = y_0\tau_0'$; $s' = x\sigma_1'$, $u' = (y_1\tau_1') \cdots (y_k\tau_k')$. Considérant ces équations pour $n = 0$ et pour $n = 1$ on obtient $tu = t'u'$ et $|s| = |s'|$.

Par conséquant t (donc t et s) est déterminé de façon unique par la condition que t soit le facteur gauche commun de tous les mots de la forme $y_0\tau_0''$ $(\sigma'' \in \Sigma)$.

Ceci entraine qu'il n'existe pas de lettre b de B qui soit facteur gauche commun des mots t et $x\sigma_1$ $(x \in X_1)$. En effet, si tel était le cas, on pourrait remplacer t par tb^{-1}, $y_1\tau_1$ par $b(y_1\tau_1)$ et chaque $x\sigma_1 \in B^+$ par $b((x\sigma_1)b^{-1})$, en contradiction avec le caractère minimal de $|t|$.

Le résultat est établi pour $k = 1$. Si $k \geqslant 2$, on le vérifie par induction sur k en considérant le monome $(y_1, X_1, y_2, \ldots, X_k, y_k)$ et la relation définie par la suite induite $(\tau_1, \sigma_1, \ldots, \tau_k)$. □

Ceci nous permettra une économie de notations puisque, pour tout segment $X_i^*y_i \cdots X_j^*$ (ou $y_{i-1}^*X_i^*y_i \cdots X_j^*$ ou $X_i^*y_i \cdots X_j^*y_j$ etc.) du domaine X et tout mot

x de celui-ci nous pourrons sans ambiguité désigner par $x\rho$ le produit correspondant des images de ses facteurs par les relations de la suite distinguée (σ) que l'on vient de définir.

(2) Nous vérifions d'abord un résultat technique.

4.2. *Soit $\rho = \rho_1 + \rho_2 + \cdots + \rho_d$ une somme finie de relations rationnelles fonctionnelles ρ_i. Il existe une relation ρ_0 de domaine fini et un système fini de monomes disjoints $(X^{(j)})$ et de relations rationnelles ρ_{ji} telles que chaque paire $(X^{(j)}, \rho_{ji})$ soit compatible et que ρ soit la somme de ρ_0 et des ρ_{ji}.*

Preuve. Chacune des relations initiales ρ_i peut être définie par une bimachine ν_i. Celles-ci étant en nombre fini, on peut choisir un morphisme ϕ de A^* dans un monoïde fini S qui en soit simultanément un morphisme. Donc pour tout ρ_i et $s \in S$ la partie $s\phi^{-1}$ est contenue dans le domaine de ρ_i ou dans son complément.

On définit maintenant la relation ρ_0 comme la restriction de ρ à l'union D de celles des parties $s\phi^{-1}$ $(s \in S)$ qui sont finies. Remplaçant ρ par sa restriction au complément de D, on peut désormais supposer $\rho_0 = 0$ et même, pour simplifier, que toutes les relations ρ_i ont le même domaine $s\phi^{-1}$ pour un certain $s \in S$.

D'après 2.3 et ses corollaires, on peut trouver des morphismes μ_i dans des monoïdes $\{0,1\}$ de $Q \times Q$ matrices $(Q = S \times S)$ qui définissent les ρ_i et satisfont identiquement $\mu_i \# = \phi$.

Appliquons maintenant la construction de 3.1 à l'une quelconque des relations ρ_i. Elle permet d'exprimer cette relation come une somme finie de produits ρ_{j1} $(j = 1, 2, \ldots, k)$ de relations et chacun de ceux-ci donne de façon unique une paire compatible $(X^{(j)}, \rho_{j1})$. Par construction les domaines des monomes $(X^{(j)})$ sont deux à deux disjoints. En vertu des égalités $\phi = \mu_i \#$, les mêmes monomes $(X^{(j)})$ auraient été obtenus si cette construction avait été effectuée à partir de l'une quelconque des autres relations ρ_i. □

Nous considérons désormais un monome fixe (X) avec lequel toutes les relations considérées seront supposées compatibles. Puisque chaque segment X_i^* de (X) est engendré librement par X_i, le monoïde $M = X_1^* \times X_2^* \cdots \times X_k^*$ est isomorphe à un produit direct de monoïdes libres. Il existe donc une bijection η de M sur le domaine X de (X) envoyant chaque $m = (x_1, \ldots, x_h)$ sur $y_0 x_1 y_1 \cdots x_h y_k$. En particulier $1\eta = y_0 y_1 \cdots y_k$.

Enfin pour chaque relation fonctionnelle ρ compatible avec (X) nous désignons par $\hat{\rho}$ le morphisme de M dans $\mathbf{N}$ tel que $m\hat{\rho} = |m\eta\rho| - |1\eta\rho| = |x_1\rho| + |x_2\rho| + \cdots + |x_k\rho|$ pour chaque $m = (x_1, \ldots, h_k) \in M$. On a donc identiquement

$$|(m^n w m'^{n'})\eta\rho| = |w\eta\rho| + (n + n') \cdot m\hat{\rho}$$

pour tout $m, w, m' \in M$ et $n, n' \in \mathbf{N}$.

L'énoncé 2.1 permet de tester si deux relations rationnelles fonctionnelles ρ et ρ' sont telles que $\hat{\rho} = \hat{\rho}'$ c'est-à-dire telles que $|x\rho| = |x\rho'|$ pour tout mot x appartenant à l'union des X_i. En effet il suffit pour cela de prendre un morphisme β de B^* envoyant l'alphabet B sur une lettre unique et de vérifier pour $l = 1, 2, \ldots, k$ l'égalité sur X_l^* des relations induites sur $\rho\beta$ et $\rho'\beta$.

4.3. *Soient ρ et ρ' deux relations fonctionnelles distinctes compatibles avec le monome (X) et satisfaisant $\hat{\rho} = \hat{\rho}'$. Il existe un idéal non vide W de M tel que $w\mu\rho \neq w\mu\rho'$ pour chacun de ses éléments w.*

Preuve. Soit $\delta = |1\eta\rho| - |1\eta\rho'|$. Si $\delta \neq 0$ on a $|m\eta\rho| - |m\eta\rho'| = \delta \neq 0$ pour chaque m de M en raison de $\hat{\rho} = \hat{\rho}'$ et on peut donc prendre $W = M$. Soient $b = y_0\rho$ et $b' = y_0\rho'$. Si l'un de ces deux mots n'est pas facteur gauche de l'autre, les idéaux à droite bB^* et $b'B^*$ sont disjoints. Il en est donc de même de $X\rho$ et de $X\rho'$ et on peut encore prendre $W = M$.

Nous supposons donc désormais ces deux cas écartés, c'est-à-dire $\delta = 0$ et par exemple, en simplifiant à gauche, $b' = y_0\rho' = 1$.

Soit V l'ensemble des mots v de X_1^* pour lesquels $|v\rho| \geqslant |b|$. On définit quatre relations α', β, β' et γ de domaine V par les équations suivantes pour chaque v de V : $v\rho = (v\beta)(v\gamma)$; $v\rho' = (v\alpha')(v\beta')$; $|v\gamma| = |v\alpha| = |b|$, $(b = y_0\rho)$. Autrement dit $v\gamma$ et $v\gamma'$ sont respectivement le facteur droit et le facteur gauche de longueur $|b|$ de $v\rho$ et de $v\rho'$ et $v\beta = (v\rho)(v\gamma)^{-1}$ et $v\beta' = (v\alpha')^{-1}(v\rho')^{-1}$ sont les cofacteurs associés. Donc $|v\gamma| = |v\alpha'|$ et comme V est un idéal non vide X_1 on a identiquement $(xv)\beta = x\rho \cdot v\beta$; $(vx)\beta' = v\beta' \cdot x\rho'$ pour chaque $v \in V$, $x \in X_1^*$.

On vérifie facilement que V est une partie reconnaissable et que les relations α', β, β', γ sont rationnelles en même temps que ρ et ρ'. Ceci permet de tester si l'ensemble V' des mots v de V pour lesquels $v\beta \neq v\beta'$ est vide ou non.

Supposons maintenant $v \in V' \neq \emptyset$. Quelque soit le mot x de X_1^*, l'égalité de longueur des mots $x\rho$ et $x\rho'$ entraîne celle des mots $b(x\rho)(v\beta)$ et $(x\rho'')(v\rho') = (x\rho')(v\alpha')(v\beta')$.

Comme $v\beta \neq v\beta'$ ces deux mots engendrent des idéaux à droite dans B^* disjoints. Par conséquent $w\mu\rho \neq w\mu\rho'$ pour tout $w \in M$ appartenant à l'idéal (bilatère) de ce monoïde engendré par $v\eta^{-1} = (v, 1, \ldots, 1)$. Le résultat est donc établi dans ce cas et nous pouvons désormais supposer que V' est vide, c'est-à-dire que $\beta = \beta'$.

Prenant deux mots quelconques u et v dans V, le calcul:

$$u\beta \cdot u\gamma \cdot v\beta = u\rho \cdot v\beta = (uv)\beta = (uv)\beta' = u\beta' \cdot v\rho' = u\beta' \cdot v\alpha' \cdot v\beta'$$

établit l'existence d'un mot c de longueur $|b|$ tel que l'on ait identiquement $u\gamma = v\alpha' = c$, c'est-à-dire $v\rho = v\beta \cdot c$; $v\rho' = c \cdot v\beta$ pour chaque $v \in V$. Si $c \neq b$ on a évidemment $m\eta\rho \neq m\eta\rho'$ pour chaque $m \in M$. Il ne reste donc à considérer que le cas ou $c = b$.

Comme $V = VX_1^*$, les relations $b = y_0\rho$ et $v = v\beta \cdot b$ $(v \in V)$ montrent que si b était différent de 1, les mots $y_0\rho$ et $x\rho$ $(x \in X_1)$ auraient un facteur droit commun non trivial en contradiction avec les conventions adoptées à la fin de 4.1. Par conséquent $b = 1$ et β est la valeur commune des restrictions à V de ρ et de ρ'. Comme $V^* = V^*X_1^*$ on en conclut que de fait ρ et ρ' ont même restriction à X_1.

Il est clair que seul ce dernier cas est à considérer pour achever la preuve. Si $k = 1$ l'hypothèse $\rho \neq \rho'$ implique $y_1\rho \neq y_1\rho'$ ce qui entraîne que $X\rho$ et $X\rho'$ soient disjoints. Si $k \geqslant 2$ le résultat énoncé découle de la même manière des remarques précédentes par induction sur k en considérant les restrictions à $(y_1, X_2, \ldots, y_k)$ de ρ et de ρ'. □

Gardant le même monome (X) nous considérons enfin un ensemble R de $d < \infty$ relations rationnelles fonctionnelles compatibles avec lui et la somme σ de ces dernières.

4.4. *Le monoïde M contient un sous semi-groupe non vide S' tel que $\| s\eta\sigma \| = d$ pour chacun de ses éléments s.*

Preuve. Comme la famille des idéaux non vides de M contient l'intersection de deux de ses membres, l'énoncé précédent permet de trouver un idéal $W \neq \emptyset$ tel que pour chacun de ses éléments w et $\rho, \rho' \in R$ on ait $w\eta\rho = w\eta\rho'$ seulement si $\rho = \rho'$ ou $\hat{\rho} \neq \hat{\rho}'$.

Soit d'autre part $R' = \{\rho_1, \ldots, \rho_p\}$ une partie maximale de R telle que $\hat{\rho}_i \neq \hat{\rho}_j$ pour deux quelconques de ses éléments distincts. Comme chaque $\hat{\rho}$ est un morphisme de M dans $\mathbf{N}$ on peut trouver un élément m de M et un indexage de R' tels que $m\hat{\rho} < m\hat{\rho}_2 \cdots < m\hat{\rho}_p$.

Ces inégalités restent vérifiées par n'importe quelle puissance de m et, prenant un w dans W quelconque on peut trouver une puissance m'' de m telle qu'en posant $s' = wm''$ on ait $|s\eta\rho_1| < |s\eta\rho_2| \cdots < |s\eta\rho_p|$ pour chaque élément s du sous semi-groupe S de M engendré par s' ce qui établit le résultat puisque S est contenu dans l'idéal W de M. □

Nous avons terminé la preuve des propriétés énoncées dans l'introduction.

En effet si la relation rationnelle ρ n'admet aucun triple de mots a', ρ, a'' pour lequel $\|(a'p''a'')\rho\| \geqslant n + 1$ identiquement, la première partie de la preuve montre quelle est la somme d'un nombre fini de relations rationnelles fonctionnelles. D'après 4.2 nous pouvons la représenter comme la somme d'une relation ρ_0 de domaine fini et de relations fonctionnelles ρ_{ji} dont les domaines sont ceux de monomes disjoints $(X^{(j)})$. Sur chacun de ceux-ci, le dernier énoncé montre que la norme de ρ est la même que celle de la restriction de ρ à tous les mots de longueur supérieure à une valeur finie arbitraire. Si donc d est le maximum de la norme de $X^{(j)} \cap \rho$ sur tous les domaines $(X^{(j)})$ on peut regrouper ceux-ci et exprimer ρ comme somme de ρ_0 et d'exactement d relations fonctionnelles.

On notera que les constructions effectuées permettraient de vérifier si une relation rationnelle ρ' de norme finie satisfait ou non $a\rho \subset a\rho'$ pour tous les mots assez longs. Il serait curieux que ceci ne reste pas vrai pour des relations rationnelles ρ et ρ' satisfaisant seulement la condition (ii) de la Propriété.

Références

[1] S. Eilenberg, *Automata, Languages and Machines*, Vol. A (Academic Press, New York, 1974).
[2] C. Elgot and G. Mezei, On operations defined by generalised automata, *IBM J. Res. Dev.* **9** (1965) 47–68.
[3] A. Lentin, *Equations dans les monoïdes libres* (Gauthier Villars, Paris, 1972).
[4] M. Nivat, Transductions des languages de Chomsky, *Ann. Institut Fourier* **18** (1968) 335–455.

Société Mathématique de France
Astérisque 38-39 (1976) p.247-251

SUR UNE CARACTÉRISATION DES PARTIES RECONNAISSABLES D'UN MONOÏDE LIBRE

par

M.P. SCHÜTZENBERGER

1.- INTRODUCTION

Une partie S d'un monoïde M est reconnaissable ssi il existe un morphisme φ de M dans un monoïde fini pour lequel $S = S\varphi\varphi^{-1}$. Une caractérisation remarquable de ces parties est donnée par S. Eilenberg (vol. A ; chap. XIII, Prop. 12.3) dans son traité "Automata, Languages and Machines". On se propose ici de montrer que dans le cas où M est le monoïde libre A^* (engendré par l'ensemble A), on peut légèrement affaiblir les hypothèses de cet énoncé. Plus précisément, nous établirons la :

PROPRIÉTÉ .- Une condition nécessaire et suffisante pour que la partie S de A^* soit reconnaissable est l'existence d'un entier naturel n et de deux applications $\lambda : A^* \to \mathbb{N}^n$ et $\rho : A^* \setminus A^{n+1} A^* \to \mathbb{N}^n$ satisfaisant la condition que pour chaque $a \in A^*$, $f \in A^* \setminus A^{n+1} A^*$ le produit scalaire $a\lambda . f\rho$ ait la valeur 1 ou 0 selon que $af \in S$ ou non.

Il est trivial que la condition est nécessaire. En effet, soit $S = S\varphi\varphi^{-1}$ où φ est un morphisme dans un monoïde P ayant $n < \infty$ éléments. On peut considérer P comme un monoïde d'applications de P dans lui-même et associer à chaque mot a de A^* le P-vecteur ligne $a\lambda$ (resp. colonne $a\rho$) tel que pour chaque $p \in P$ sa coordonnée $a\lambda_p$ (resp. $a\rho_p$) soit égale à 1 ou

à 0 selon que $a\varphi = p$ ou non (resp. $a\varphi.p \in S$ ou non). On a donc $a\lambda.f\rho = 1$ ou 0 puisque $a\lambda$ a exactement une coordonnée non nulle et $a\lambda.f\rho = 1$ ssi $a\varphi.f\varphi \in S\varphi$.

Nous ne nous occuperons plus désormais que de la réciproque.

2.- VÉRIFICATION DE LA RÉCIPROQUE

Nous supposons remplies les conditions de l'énoncé. On pose $F = A^* \setminus A^{n+1} A^*$ et on note σ la fonction caractéristique de S ($a\sigma = 1$ ou 0 selon que $a \in S$ ou non pour chaque mot a de A^*). Il est clair que l'on peut supposer qu'aucune des coordonnées des vecteurs $a\lambda$ ($a \in A^*$) ou $f\rho$ ($f \in F$) n'est identiquement nulle. Comme $(af)\sigma = a\lambda.f\rho$, ceci entraîne que ces vecteurs aient toutes leurs coordonnées égales à 1 ou à 0.

Définissons deux relations d'équivalence sur A^* par les conditions : $a \sim a'$ (resp. $a(\sim)a'$) ssi $(af)\sigma = (a'f)\sigma$ pour chaque $f \in A^*$ (resp. $f \in F$).

Il est bien connu que chaque relation $a \sim a'$ implique $ab\,(\sim)a'b$ et $ab \sim a'b$ pour tout $b \in A^*$ et que réciproquement $ab\,(\sim)a'b$ pour tout $b \in A^*$ entraîne $a \sim a'$. L'essentiel de la preuve est la remarque suivante :

2.1.- La relation $a(\sim)a'$ implique $a \sim a'$.

Preuve.- Pour chaque indice $j \leqslant n$, soit r_j le F-vecteur ligne dont chaque coordonnée f est égale à la coordonnée j du n-vecteur colonne $f\rho$ ($f \in F$). Le sous-module R de $\mathbb{Z}^F$ sous-tendu par les r_j ($1 \leqslant j \leqslant n$) a donc dimension au plus n.

Soit, d'autre part, $a\alpha$ pour chaque mot a de A^* le F-vecteur ligne dont chaque coordonnée f est égale à $(af)\sigma$. Comme $(af)\sigma = a\lambda.f\rho$ ce vecteur est égal à la combinaison linéaire $\sum_j a\lambda_j.r_j$ des vecteurs r_j et appartient donc à R. Pour la même raison, on a que chaque relation $ab(\sim)a'b$ équivaut à $(ab)\alpha - (a'b)\alpha = 0$.

Supposons donc $a(\sim)a'$ et qu'il existe un mot b pour lequel $(ab)\alpha - (a'b)\alpha \neq 0$. On peut prendre $b = b_1, b_2, \ldots, b_m$ ($m \geqslant 1$; $b_1, b_2, \ldots, b_m \in A$) de longueur minimale, ce qui fait que si $f \in F$ est tel que les coordonnées $(ab)\alpha_f$ et $(a'b)\alpha_f$ sont différentes, on a $f \in A^n$. En effet, sinon on aurait : $(ab')\alpha_{f'} \neq (a'b')\alpha_{f'}$ avec $b' = b_1, \ldots, b_{m-1}$ et $f' = b_m f \in F$.

Soit π_j le morphisme de R dans lui-même annulant les coordonnées correspondant aux $f' \in F$ de longueur $> n - j$ ($0 \leqslant j \leqslant n$). On vient de montrer que $w_o = (ab)\alpha - (a'b)\alpha$ satisfait $w_o \pi_1 = 0$ et $w_o \pi_o \neq 0$.

Plus généralement, soit $f = a_1 a_2 \ldots a_n$ ($a_1, a_2, \ldots, a_n \in A$) et pour chaque i, $b_i = b a_1 \ldots a_i$, $w_i = (ab_i)\alpha - (a'b_i)\alpha$. Si $f' \in F$ est de longueur au plus $n - i$, on a l'égalité $(ab_i)\alpha_{f'} = (ab)\alpha_{f''}$ avec $f'' = a_1 \ldots a_i f' \in F$ puisque la valeur commune des deux membres est 1 ou 0 selon que $ab_i f' = ab f''$ appartient ou non à S. La même observation s'applique aux $(a'b_i)\alpha$ et il en résulte immédiatement que l'on a $w_i \pi_{i+1} = 0$; $w_i \pi_i \neq 0$ pour $i = 0, 1, \ldots, n$.

Ceci montre que les w_i constituent un système de $n + 1$ vecteurs linéairement indépendants de R en contradiction avec $\dim R \leqslant n$. Par conséquent, $ab(\sim)a'b$ pour tout $b \in A^*$, c'est-à-dire $a \sim a'$.

Q.E.D.

D'après la définition même de cette équivalence, S est une union de classe de $\sim$. Comme cette relation admet la multiplication à droite il suffit, d'après la théorie classique, de vérifier qu'elle n'a qu'un nombre fini de classes. Pour cela, supposons que $a\lambda = a'\lambda$. Pour chaque $f \in F$, on a $(af)\sigma = (a'f)\sigma$, c'est-à-dire que $a(\sim)a'$ et donc $a \sim a'$ comme on vient de le montrer. Autrement dit, chaque classe de $\sim$ est une union de parties de la forme $v\lambda^{-1}$ où $v \in V = \{a\lambda : a \in A^*\}$, ce qui conclut la preuve puisque V a au plus 2^n éléments.

Q.E.D.

3.- CAS AMBIGU

Nous considérons maintenant une formulation un peu différente de la

M. P. SCHÜTZENBERGER

propriété et nous supposons qu'il existe n paires de parties $X_i' \subset A^*$ et $Y_i' \subset A^* \setminus A^{2^n} A^* = F'$ telles que, pour chaque $(a,f) \in A^* \times F'$, on ait $af \in S$ ssi $a \in X_i'$ et $f \in Y_i'$ pour au moins un indice i.

Observation.- Sous les hypothèses indiquées, S est une partie reconnaissable.

Preuve.- Pour chaque $a \in A^*$, soit $a\lambda' = \{i \in [n] : a \in X_i\}$ où $[n] = \{1 < 2 < \ldots < n\}$. Posons $m = \mathrm{Max}\,\{\mathrm{Card}\, a\lambda' : a \in A^*\}$ et définissons Q comme l'ensemble des paires de la forme $(i,\bar{q})$ où $i \in [n]$ et où $\bar{q}$ est une partie de $[i-1]$ $(= \emptyset$ pour $i = 1)$ ayant au plus $m-1$ éléments. Puisque Q est en bijection avec les parties non vides de $[n]$ ayant m éléments au plus, on a $\mathrm{Card}\, Q \leqslant 2^n - 1$.

A chaque mot a de A^*, on associe le Q-vecteur ligne $a\lambda$ par la condition que si $q = (i,\bar{q}) \in Q$, sa coordonnée $a\lambda_q$ soit 1 ou 0 selon que l'on a ou non $i \in a\lambda'$ et $\bar{q} = a\lambda' \cap [i-1]$.

De façon analogue, si $f \in F$, on pose $f\rho' = \{j \in [n] : f \in Y_j\}$ et on définit le Q-vecteur colonne $f\rho$ par la condition que $f\rho_q = 1$ ou 0 selon que l'on a ou non $j \in f\rho'$ et $\bar{q} \cap f\rho' = \emptyset$ $(q = (j,\bar{q}))$.

Considérons un produit scalaire $s = a\lambda . f\rho$. Par hypothèse $af \notin S$ ssi l'intersection $I = a\lambda' \cap f\rho'$ est vide et dans ce cas $s = 0$ d'après la définition des vecteurs $a\lambda$ et $f\rho$. Dans le cas contraire où I est non vide, soit i son plus petit élément. Si $\bar{q} = [i-1] \cap a\lambda'$, les vecteurs $a\lambda$ et $f\rho$ ont tous les deux leur coordonnée $(i,\bar{q})$ égale à 1, et par conséquent, $s \geqslant 1$. De fait, on a exactement $s = 1$. En effet, suppsons que $a\lambda_{q'} = a\rho_{q'} = 1$ pour un certain $q' = (i',\bar{q}')$ de Q. On doit avoir $i' \in I$ et $\bar{q}' = [i'-1] \cap a\lambda'$ (d'après la définition de λ). Ceci implique $i' = i$ et donc $\bar{q}' = \bar{q}$ puisque $i' \geqslant i$ (d'après le choix initial de $i = \mathrm{Min}\, I$) ou en cas d'inégalité stricte, on aurait $i \in \bar{q}' \cap f\rho'$ en contradiction avec $f\rho_{q'} = 1$ (d'après la défini-

tion de ρ). Par conséquent, on a identiquement $(af)\sigma = a\lambda.f\rho$ pour tout $a \in A^*$, $f \in A^* \setminus A^{2^n} A^*$ et comme $\mathrm{Card}\, Q < 2^n$, le résultat découle de la Propriété en remplaçant n par $\mathrm{Card}\, Q$.

Q.E.D.

On notera que dans la Propriété il n'est pas possible de remplacer F par $A^* \setminus A^{n'+1} A^*$ où $n' < n$. Considérons, en effet, le cas où A consiste en une seule lettre a, et, posant $D = \{2^p : p \in \mathbb{N}\}$, définissons les applications λ et ρ dans $\mathbb{N}^2$ par :

$a^m\lambda = (1,0)$ si $m \in D$; $= (0,1)$ si $m \in D+1$; $= (0,0)$ dans les autres cas.

$$a\rho = (0,1) \ ; \ a^2\rho = (1,0).$$

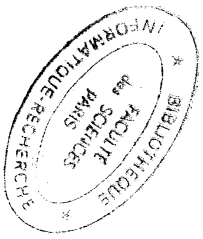
On a donc que $a^{m+2}\sigma = a^{m+1}\lambda.a\rho = a^m\lambda.a^2\rho$ est égal à 1 ou à 0 selon que $m \in D+2$ ou non, ce qui donne la partie $S = 1\sigma^{-1} = \{a^{2+d} : d \in D\}$ qui n'est évidemment pas reconnaissable.

***

Marcel Paul SCHÜTZENBERGER
Département de Mathématiques
Université de Paris VII
Tour 45-55
2 place Jussieu
75005 PARIS

FORMAL LANGUAGES AND PROGRAMMING

Proceedings of a Seminar
Organized by UAM-IBM Scientific Center
Madrid, April 23-25, 1975



edited by

R. Aguilar

Director of the IBM Scientific Center/Universidad Autónoma de Madrid

1976

NORTH-HOLLAND PUBLISHING COMPANY
AMSTERDAM - NEW YORK - OXFORD

R. Aguilar (ed.), Formal Languages and Programming

UNE CARACTERISATION DES PARTIES RECONNAISSABLES

M.P. Schützenberger

Dans la théorie de S. Eilenberg ([1], p. 68), une partie X d' un semi-groupe S est dite reconnaissable ssi il existe un morphisme de S dans un semi-groupe fini pour lequel $X = X\phi\phi^{-1}$.

La méthode des matrices de Hankel introduite par M. Fliess et en particulier le théorème 2.11 de cet auteur ([2]), suggèrent les caractérisations suivantes des parties reconnaissables du semi-groupe S voisine de la Propriété 12.2 de [1] chapitre IV. On supnose donné un corps commutatif K et on rappelle que la fonction caractéristique $\chi = \chi_X$ d'une partie X de S est l'application de S dans K telle que pour chaque élément s de S on ait $s\chi = 1$ ou 0 selon que s appartient ou non à X.

Propriété: Une condition nécessaire et suffisante pour que la partie X du semi-groupe S soit reconnaissable est qu'il existe une famille finie $\{\lambda_i,\rho_i\}(1\leq i\leq n<\infty)$ de paires l'application de S dans K telles que sa fonction caractéristique χ satisfasse l'identité suivante pour tout $s,s' \in S$:

$$(1) \qquad (ss')\chi = \sum_{1\leq i\leq n} (s\lambda_i)\,(s'\rho_i).$$

Un cas typique où une telle identité est satisfaire est celui où il existe un morphisme μ de S dans un monoïde de $n\times n$ matrices ($n<\infty$) sur le corps K et deux indices distingués i_1,i_n tels que l'entrée (i_1,i_n) de chaque matrice $s\mu$, soit $s\chi$, ne prenne que les valeurs 1 ou 0. On obtient alors (1) en prenant le produit scolaire de la ligne i_1 de la matrice $s\mu$ par la colonne i_n de $s'\mu$.

Nous établissons maintenant cette propriété.

I. La condition est sufissante.

Supposons que l'on ait $X = X\phi\phi^{-1}$ où ϕ est un morphisme de S dans un semi-groupe fini M. Soit Q l'ensemble des paire $(m,m') \in M \times M$ telles que $mm' \in X\phi$. C'est un ensemble fini et pour chaque $s,s' \in S$ les relations

$(ss')\chi = 1$; $ss' \in X$; $(ss')\phi = (s\phi)\,(s'\phi) \in X\phi$ et $(s\phi,s'\phi) \in Q$

sont équivalentes.

Pour chaque $q = (m,m') \in Q$ nous considérons maintenant la fonction caractéristique λ_q (resp. ρ_q) de la partie $m\phi^{-1}$ (resp. $m'\phi^{-1}$) de S. Si s et s' sont deux éléments quelconques de S, le produit $(s\lambda_q)\,(s'\rho_q)$ est égal à s si $(s\phi,s'\phi) = q$ et à 0, sinon. Par conséquent la somme finie

$$\sum_{q \in Q} (s\lambda_q)\,(s'\rho_q)$$

est égale a 1 ou 0 selon que $ss' \in X$ ou non, ce qui établit le résultat cherché.

Q.E.D.

II. La condition est nécessaire.

Nous considérons le cas un peu plus général où sont données deux familles $\{\lambda_q\}$, $\{\rho_q\}$ d'applications de S dans K indexées par les éléments d'un ensemble fini Q et une application χ satisfaisant la condition que l'identité (1) soit vraie et que l'image $\{s\chi : s \in S\}$ de χ soit une partie finie du corps K.

Nous nous proposons de vérifier que chaque partie donnée J de I définit une partie reconnaissable.

$$X_J = J_\chi^{-1} = \{s \in S : s\chi \in J\}$$

de S.

Nous commençons par trois remarques introduisant des hypothèses supplémentaires qui allègent la preuve proprement dite.

(1). S est un semi-groupe infini et $X = X_J$ n'est ni vide ni égal à S.

Preuve: En effet, dans le cas contraire, le résultat est déjà établi car, par définition, toute partie X d'un semi-groupe fini est reconnaissable et la partie X = ∅ ou X = S de tout semi-groupe S est une partie reconnaissable de ce dernier.

Q.E.D.

(2). J est le singleton formé de l'élement unité 1 de corps K. De plus il n'existe aucun $q \in Q$ pour lequel λ_q ou ρ_q soit identiquement nulle.

Preuve: Toute partie X de S est reconnaissable en même temps que son complément S\X. On peut donc supposer $0 \notin J$ en remplaçant au besoin J par son complément dans l'image I de χ puisque cette dernière est supposée être finie.

D'autre part, si pour chaque $k \in J$, il existe un morphisme ϕ_k de S d'image finie tel que $X_k \phi_k \phi_k^{-1}$ où $X_k = k_\chi^{-1}$, on a $X\phi\phi^{-1} = X$ ou ϕ est le morphisme évident de S dans le produit direct des semi-groupes S_{ϕ_k}. Il suffit donc d'établir que chaque X_k est reconnaissable. On se ramène au cas où k = 1 en remplaçant chaque ρ_q par ρ_q^{k-1} et χ par χ^{k-1}.

Enfin si λ_q ou ρ_q était identiquement nulle, il en serait de même de chaque terme $s_q.s'_q$ dans (x) et celui-ci pourrait être omis.

Q.E.D.

Nous supposons donc désormais $\{1\} = J \subset I$

(3). S est un monoïde.

Preuve: S'il n'est est pas ainsi, nous adjoignons à S un nouvel élément neutre 1, obtenant ainsi un monoïde $\bar{S} = \{1\} \cup S$.

Nous définissons $1\lambda_q = 1\rho_q = 0$ pour chaque $q \in Q$. Nous ajoutons aussi deux nouveaux éléments r et r' à Q et nous définissons les applications $\lambda_r = \rho_{r'}$ et $\lambda_{r'} = \rho_r$ comme étant respectivement les fonctions caractéristiques des parties

X et {1} de $\bar{S}$. on a donc que pour chaque s,s' ϵ S le nouveau terme $(s\lambda_r)\,(s'\rho_r) + (s\lambda_{r'})\,(s'\rho_{r'})$ de la somme est égal à 1 ou à 0 selon que (s,s') appartient ou non à l'union de X x {1} et de {1} x X, ce qui montre que l'identité (1) (et les autres hypothèses) sont encore satisfaites.

Il est clair que X est reconnaissable à la fois comme partie de $\bar{S}$ et comme partie de S. En effet si $X\phi\phi^{-1} = X$ où ϕ est un morphisme d'image finie du monoïde $\bar{S}$, on a aussi $X\Psi\Psi^{-1} = X$ où Ψ est la restriction de ϕ à S puisque, par construction, le nouvel élément 1 n'appartient pas à X

Q.E.D.

Nous en venons maintenant à la preuve que X est reconnaissable. Nous désignons par $s\lambda$ (resp. $s\rho$) pour chaque s ϵ S, le Q-vecteur ligne (resp. colonne) dont les coordonnées sont les $s\lambda_q$(resp. $s\rho_q$) ce qui fait que le membre de droite de (1) est simplement le produit scalaire $s\lambda.s'\rho$.

Soit d($\leq$ Card(Q)) la dimension du K-module R sous-tendu par tous les vecteurs $s\rho$(s ϵ S). On peut trouver une partie T de d élément de S et une Q×Q matrice inversible M tels que, posant $s\lambda' = s\lambda.M^{-1}$ $s\rho' = M.s\rho$(s ϵ S) les vecteurs $t\rho'$(t ϵ T) forment une base de R constituée de vecteurs ayant toutes leurs coordonnées nulles sauf une égale à 1.

On a identiquement $s\lambda.s'\rho = s\lambda'.s'\rho'$ et nous pourrons donc désormais supposer que $\lambda = \lambda', \rho = \rho'$.

D'après l'hypothèse (2), on a donc d = Card(Q). En raison de notre choix des vecteurs $t\rho$(t ϵ T), l'hypothèse que $s\lambda.t\rho$soit identiquement contenu dans la partie I de K implique que toutes les coordonnées non nulles des vecteurs $s\lambda$ (s ϵ S) soient aussi dans I.

Nous en concluons que la relation d'équivalence $\approx$ sur S définie par $\lambda^{-1}(s_1 \approx s_2$ ssi $s_1\lambda = s_2\lambda)$ n'a qu'un nombre fini ($\leq(1+\mathrm{Card}(I))^d$) de classes.

Posons $X_k = k_X^{-1}$ et $s^{-1}X_k = \{s' \epsilon S\ ;\ ss' \epsilon X_k\}$ pour chaque k ϵ I et s ϵ S et désignons par $\sim$ la relation d'équivalence sur S définie par $s_1 \sim s_2$ ssi $s_1^{-1} X_k = s_2^{-1} X_k$ pour chaque K ϵ I. Il est clair que $s_1 \approx s_2$ implique $s_1 \sim s_2$ et que, réciproquement, d'apres notre choix de vecteurs t (t ϵ T) on ne peut avoir

$s_1 \approx s_2$ que si $s_1 \sim s_2$.

De plus, chaque X_k est une union de $\sim$ - classes puisque, S étant un monoïde, on a:

$$X_k = \{ s \in S : 1 \in s^{-1} X_k \}$$

Ceci permettrait d'achever la preuve en utilisant la Proposition 12.1 de [1]. Par souci d'être complet, nous en reproduisons la partie pertinente.

Soient $s, s_1, s_2 \in s_2 \in S$, $k \in I$ tels que $s_1^{-1} X_k = s_2^{-1} X_k$. L'ensemble $(s_1 s)^{-1} X_k$ est égal à $s^{-1}(s_1^{-i} X)$ puisque $1 \in S$, et il est par conséquent égal à $(s_2 s)^{-1} X_k$ ce qui montre que l'équivalence $\sim = \approx$ admet la multiplication à droite.

Il existe donc un morphisme ϕ de S dans le monoïde fini des applications dans lui-même de l'ensemble $S/\sim$ qui est en bijection avec $\{s\lambda : s \in S\}$. Comme S est un monoïde, on a $Y_{\phi\phi}{}^{-1} = Y$ pour chaque $\sim$ - classe ou union de $\sim$ - classes $Y \subset S$. Donc en particulier $X = X\phi\phi^{-1}$ est reconnaissable.

Q.E.D.

REFERENCES:

[1] S. Eilenberg. Automata, languages and machines. (vol A). Academie Press. New-York 1974.

[2] M. Fliess (1974). Matrices de Hankel. J.Math. Pures et Appli. 53 pp. 197-222.

GROUPE D'ÉTUDE D'ALGÈBRE

MARCEL P. SCHÜTZENBERGER

Quelques problèmes posés par l'étude combinatoire des semigroupes

Groupe d'étude d'algèbre, tome 1 (1975-1976), exp. n° 19, p. 1-1.

<http://www.numdam.org/item?id=GEA_1975-1976__1__A19_0>

Groupe d'étude d'ALGÈBRE
(Marie-Paule MALLIAVIN)
1re année, 1975/76, n° 19, 1 p.

19-01

28 mai 1976

QUELQUES PROBLÈMES POSÉS PAR L'ÉTUDE COMBINATOIRE DES SEMIGROUPES

par Marcel P. SCHÜTZENBERGER

Résumé.

Divers travaux au premier rang desquels figurent ceux de J.-F. PERROT et de D. PERRIN ont montré l'intérêt de l'étude des groupes contenus dans le monoïde syntaxique d'un sous-monoïde X^* du monoïde libre A^* engendré par une partie X ayant un nombre fini k d'éléments. Le but de cette communication est d'établir l'énoncé suivant.

PROPRIÉTÉ. - Les seuls groupes (maximaux) dans $\mathrm{Synt}\,(X^*)$ qui ne sont pas sous-groupe du groupe symétrique γ_{2k} sont cycliques, et leur nombre est au plus k.

La vérification utilise la théorie des équations dans les monoïdes libres de A. LENTIN. Il semble possible de montrer par la même technique que le nombre d'idéaux principaux idempotents de $\mathrm{Synt}(X^*)$ est borné supérieurement en fonction de k. La valeur $2k$ figurant dans la propriété est vraisemblablement extravagante.

Notations. - Dans tout l'exposé, X est une partie du semi-groupe libre $A^+ = A^*\setminus 1$, et l'on pose

$$(1)\quad \begin{cases} P = XA^{+(-1)} = \{p \in A^* : pA^+ \cap X \neq \emptyset\} ; \\ Q = A^{+(-1)}X = \{q \in A^* : A^+ q \cap X \neq \emptyset\} ; \\ W = A^*\setminus A^{*(-1)}XA^{*(-1)} = \{w \in A^* : A^* wA^* \cap X = \emptyset\} ; \end{cases}$$

selon les notations de S. EILENBERG.

On considère un morphisme fixe α dans A^* du monoïde libre B^*, engendré par un ensemble B tel que la restriction de α à B soit une bijection sur X. Pour chaque mot a de A^*,

$$(2)\qquad a\bar{\alpha} = \{(q\ ,\ b\ ,\ p) \in Q \times B^* \times P\ ;\ a = q.b\alpha.p\}$$

est l'ensemble des lectures de a. Deux lectures $(q\ ,\ b\ ,\ p)$ et $(q'\ ,\ b'\ ,\ p')$ de a sont séparées si, et seulement si, il n'existe pas de factorisations $b = b_1\ b_2$, $b' = b'_1\ b'_2$ pour lesquelles

$$(3)\qquad q.b_1\ \alpha = q'.b'_1\ \alpha \quad (\Longleftrightarrow b_2\ \alpha.p = b'_2\ \alpha.p')\ .$$

On rappelle que deux mots a et a' sont dits conjugués si, et seulement si, il existe des mots c, d tels que $a = cd$, $a' = dc$. Un mot a est primitif si, et seulement si, $a \in b^*$ pour tout $b \in A^*\setminus a$. C'est une sesquipuissance de thème cd $(= \sqrt{a})$ et d'ordre p si, et seulement si, il existe une paire (nécessairement unique) $(c\ ,\ d) \in A^* \times A^+$ et un entier $p \geqslant 2$ tels que

$$(4)\qquad a = (cd)^p\ c\ ;\quad cd \text{ primitif.}$$

Marcel P. SCHÜTZENBERGER, 97 rue du Ranelagh, 75016 PARIS.

Année 1977

Bibliographie

[1] Dominique Perrin and Marcel-Paul Schützenberger. Codes et sous-monoïdes possédant des mots neutres. In *Theoretical Computer Science (Third GI Conf., Darmstadt, 1977)*, volume 48 of *Lecture Notes in Comput. Sci.*, pages 270–281. Springer, Berlin, 1977.

[2] Marcel-Paul Schützenberger. Une propriété de Hankel des relations fonctionnelles entre monoïdes libres. *Adv. in Math.*, 24(3) :274–280, 1977.

[3] Marcel-Paul Schützenberger. Sur une variante des fonctions séquentielles. *Theoret. Comput. Sci.*, 4(1) :47–57, 1977.

[4] Marcel-Paul Schützenberger. La correspondance de Robinson. In *Combinatoire et représentation du groupe symétrique (Actes Table Ronde CNRS, Univ. Louis-Pasteur Strasbourg, Strasbourg, 1976)*, volume 579 of *Lecture Notes in Math.*, pages 61–115. Springer-Verlag, 1977.

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis
Series: GI, Gesellschaft für Informatik e. V.

48

Theoretical Computer Science
3rd GI Conference

Darmstadt, March 1977

Springer-Verlag
Berlin · Heidelberg · New York

CODES ET SOUS-MONOIDES POSSEDANT DES MOTS NEUTRES

D. Perrin - M.-P. Schützenberger

Introduction

Dans tout ce travail, A^* (resp. $A^+ = A^* \setminus 1$) désigne le monoïde libre (resp. le semigroupe libre) engendré par l'ensemble fixe non vide A et on considère un sous-monoide X^* de A^* dont l'ensemble générateur minimal est $X = X^+ \setminus X^+X^+$, où $X^+ = X^* \setminus 1$. Une série de recherches se sont attachées à l'étude des rapports entre X, le sous-monoide X^* et le monoïde syntaxique $S = A^*\xi$ de X^* ; en particulier, celles de J-F. Perrot [8], de R. Mc Naughton [7] et de G. Lallement [5] ont montré l'intérêt de la nature des groupes contenus dans S et de la structure des idéaux de ce monoïde. Le cas particulier où X engendre librement X^* (c'est-à-dire où X est un *code*) présente un certain intérêt supplémentaire en raison, notamment, de son interprétation en théorie de l'information et de ses rapports avec les processus stochastiques associés ; il pose divers problèmes algébriques non résolus.

Nous nous occupons ici du cas où X^+ admet des *mots neutres*, c'est-à-dire où il existe des mots $h \neq 1$ ayant même image syntaxique $h\xi$ que le mot vide 1 ; celle-ci est évidemment l'élément neutre du monoïde syntaxique S. Par conséquent, il existe des mots neutres non triviaux dès que S a une sous groupe U (des éléments inversibles ou unités) non-trivial. Formellement, h est un mot neutre ssi les relations $ab \in X^*$ et $ahb \in X^*$ sont équivalentes pour chaque paire de mots a, b de A^*. Cette hypothèse a une signification intuitive immédiate dans le cadre de la théorie du signal puisqu'elle exprime que le bruit sur la ligne est tel qu'on ne peut pas détecter la présence de segments égaux à h qui se trouveraient à l'intérieur des messages. En particulier, le mot $h = c^p$, où p est positif et c est une lettre, est neutre quand les dispositifs physiques ont la propriété que la longueur d'un segment $c...c...c$ formé de la répetition de cette lettre, ne peut être déterminée que modulo p (on pourrait dire qu'il s'agit d'un "bruit modulo p"). L'étude de ce problème se rattache aussi à la théorie des polynômes cyclotomiques.

Notre résultat principal concerne la reconnaissabilité de X^*, au sens de S. Eilenberg [4], c'est-à-dire la finitude de son monoïde syntaxique S. Comme on le sait, le théorème de Kleene affirme que X et X^* sont simultanément reconnaissables ou non. Nous établissons ici que, quand X admet des mots neutres non triviaux, *il est reconnaissable ssi l'un de ceux-ci*, soit h, *n'est pas complétable dans* X, c'est-à-dire si l'intersection de X avec A^*hA^* est vide. Un résultat plus fort, basé sur l'existence d'un mot $h \neq 1$ (non nécessairement neutre) tel que l'idéal à gauche A^*h rencontre le stabilisateur de chacun des états de l'automate minimal de X^*, nous a paru trop technique pour que sa preuve mérite d'être donnée ici. On remarquera que, de façon générale, si X^* est reconnaissable, il existe au moins un mot incomplétable dans X mais que, réciproquement, cette hypothèse implique seulement que si tout mot est complétable dans X^*, la densité asymptotique de ce dernier (au sens de Berstel [1] soit non nulle pour toute distribution de probabilités positive sur A.

Il est clair que l'existence de mots non complétables est assurée dans le cas particulier où X est *localement fini*, en ce sens que pour chaque sous-alphabet fini B de A, il n'y a qu'un nombre fini de mots de X dont toutes les lettres sont dans B^*. Dans ce cas, le sous-monoïde X^* est donc reconnaissable dès qu'il possède des mots neutres ; un phénomène curieux est que, si *aucun* des mots neutres n'est complétable dans X (donc en particulier si X est localement fini), le sous-groupe U de S est nécessairement cyclique. Cette situation algébrique correspond à celle du "bruit modulo p" perturbant la détermination des longueurs des segments $c...c...c$ comme on l'a indiqué plus haut et où le paramètre p est évidemment l'ordre de U.

La technique de preuve fait intervenir la représentation de A par un monoïde de relations (c'est-à-dire un automate non déterministe) possèdant un sous groupe *transitif* sur les états. Réciproquement tout monoïde fini de ce type est monoïde syntaxique d'un sous-monoïde X^* ayant des mots neutres incomplétables dans X. Le cas des codes correspond à celui où le monoïde de relations est non-ambigu, au sens de J.M. Böe [2].

Notre second résultat affirme que si X^* (admettant des mots neutres) est engendré librement par un ensemble X localement fini, *le maximum des longueurs des mots de* X *est précisément l'ordre* p *du groupe cyclique* U. Une illustration de ce fait est fournie par la très remarquable famille de codes découverte par A..Restivo, à partir d'hypothèses toutes différentes [9].

Enfin un argument de comptage très simple donne une caractérisation des sous-monoïdes X^* (possèdant des mots neutres) qui sont engendrés par un code X *maximal* (c'est-à-dire qui ne soit pas contenu dans un autre code) : une condition nécessaire et suffisante pour que X ait ces propriétés est que chacune des relations du monoïde construit plus haut ait exactement p entrées non vides, où p est le nombre des états sur lesquels les relations sont définies. Ceci constitue une généralisation d'un fait qui serait banal si l'hypothèse qu'il existe des mots neutres non-triviaux était remplacée par celle que X soit un code préfixe. Cette remarque a une application immédiate au problème de la transmission sur une ligne affectée d'un "bruit modulo p".

Monoïdes de relations

1. Transitivité.

Soit Q un ensemble fini et R le monoïde des relations binaires sur Q ; il est commode d'appeler *états* les éléments de Q. Un monoïde de relations sur Q est un sous-monoïde de R ; en particulier son élément neutre est l'égalité sur Q. On remarquera qu'un sous-semigroupe de R peut être un monoïde (i.e. possèder un élément neutre) sans être, dans notre terminologie, un monoïde de relations ; nous dirons que c'est un semigroupe de relations.

Un monoïde M de relations est *transitif* si pour tout couple (q,q') d'états il existe au moins un m dans M contenant (q,q'). On dit que M est *très transitif* si il existe une *permutation* m dans M contenant (q,q') ; un monoïde de relations M est donc très transitif ssi son sous-groupe est transitif. La proposition suivante montre qu'on n'obtient pas une définition très différente en considérant des semigroupes de relations et sera utile pour la suite :

Proposition 1. Soit S un semigroupe de relations sur un ensemble fini Q possèdant un élément neutre e et dont le sous-groupe est transitif. Alors e est une équivalence et S induit sur le quotient de Q par e un monoïde de relations très transitif isomorphe à S.

Démonstration. Tout d'abord la relation e est transitive du fait que e est idempotent: si (q,q') et (q',q'') sont dans e, alors (q,q'') est dans $e^2 = e$.

Maintenant pour tout q dans Q, il existe un élément inversible s de S contenant (q,q) ; comme Q est fini, l'élément s est d'ordre fini, soit n ;

on a alors : $(q,q) \in s^n = e$, et ceci montre que e est réflexive. Enfin, si $(q,q') \in e$, soit s un élément inversible de S tel que $(q,q') \in s$; si n est l'ordre de s, on a alors $(q',q) \in s\, s^{n-1} = e$, puisque $(q,q) \in es = s$. Ceci montre que e est symétrique et démontre la propriété.

2. Stabilisateurs.

Soit M un monoïde de relations sur Q ; le *stabilisateur* d'un état q de Q est le sous monoïde P de M formé des relations qui contiennent le couple (q,q).

Proposition 2. Si M est un monoïde de relations très transitif, il est le monoïde syntaxique de chacun des stabilisateurs des états.

Démonstration. Soit P le stabilisateur de q et supposons que deux éléments m et n de M aient même image dans le monoïde syntaxique de P. Si un couple (q_1, q_2) d'états est dans m, soient g_1 et g_2 des éléments inversibles de M tels que $(q, q_1) \in g_1$ et $(q_2, q) \in g_2$. Alors (q,q) appartient à $g_1 m g_2$ et donc à $g_1 n g_2$; mais ceci implique que $(q_1, q_2) \in n$ et nous avons ainsi montré que $m = n$, ce qui signifie que M est le monoïde syntaxique de P.

Cette proposition montre que si ξ est une représentation de A^* par un monoïde de relations très transitif alors le monoïde syntaxique du stabilisateur dans A^* d'un état est égal à $A^*\xi$.

3. Ambiguïté.

Reprenant la terminologie introduite par J.M. Böe, on dira qu'un monoïde de relations M sur un ensemble Q est *non-ambigü* si pour chaque m et n dans M et chaque couple (q,q') dans mn, il existe un *unique* état q'' tel que $(q,q'') \in m$ et $(q'',q') \in n$. Cette condition est évidemment remplie en particulier par les monoïdes d'applications et donc par le sous-groupe d'un monoïde de relations.

On sait que si ξ est une représentation de A^* par un monoïde de relations transitif, l'image réciproque par ξ du stabilisateur d'un état est un sous-monoïde *libre* X^* ssi ce monoïde de relations est non-ambigü.

4. Exemple.

Quand Card(Q) = 2, le monoïde de relations M (resp. M') engendré par les deux permutations de Q et une relation ayant une seule entrée non vide (resp. une seule entrée vide) est très transitif par construction. On notera que M et M' sont des monoïdes isomorphes mais qu'ils ne sont pas équivalents en tant que monoïdes de relations ; de plus M (mais non M') est un exemple de relations non-ambigü.

Le cas général

Reprenant les notations utilisées dans l'introduction, nous établissons l'énoncé suivant, où on dit que X^* est reconnu par un monoïde de relations pour exprimer qu'il existe une représentation de A^* par un monoïde fini de relations telle que X^* soit le stabilisateur d'un état.

Théorème 1. *Une condition nécessaire et suffisante pour que* X^* *soit reconnu par un monoïde très transitif est l'existence d'un mot neutre incomplétable dans* X.

Démonstration. Supposons d'abord que X^* soit le stabilisateur de l'état 0 pour une représentation ξ de A^* par un monoïde de relations très transitif M, sur l'ensemble $Q = \{0, 1, \ldots, p-1\}$. Notons G le sous-groupe de M et définissons par récurrence les mots $w_0, w_1, \ldots, w_p$ en posant : $w_0 = 1$ et $w_{i+1} = w_i u_i$, où u_i est un mot non vide de $G\xi^{-1}$ tel que : $(i,0) \in w_{i+1}\xi$. Le mot $f = w_p$ est alors incomplétable dans X puisque tous g,h dans A^*, si gfh est dans X^*, alors $(0,0) \in gfh\xi$ et il existe donc i et j dans Q tels que : $(0,i) \in g\xi$, $(i,j) \in h\xi$ et $(j,0) \in h\xi$. Mais on a : $h = w_{i+1}r$ et, comme $(i,0) \in w_{i+1}\xi$, et que $h\xi \in G$, on obtient $(0,j) \in r$; ceci montre que les mots gw_{i+1} et rh sont dans X^* et donc que gfh ne peut être dans X. Maintenant comme G est fini, f a une puissance, soit f^n, qui est l'élément neutre de G. Le mot f^n est alors un mot neutre incomplétable dans X.

Pour établir la réciproque, nous supposons l'existence d'un mot neutre $f \in X^*$ qui est incomplétable dans X, et nous notons R (resp. L) l'ensemble des facteurs droits (resp. gauches) propres de f.

Associons à tout mot u de A^* la partie $u\rho$ de $R \times L$ définie par :

$$(r, l) \in u\rho \Leftrightarrow rul \in X^*$$

Notons maintenant π la partie de $L \times R$ définie par :

$$(l, r) \in \pi \Leftrightarrow lr = f$$

et démontrons la formule suivante, où les points notent des produits de relations :

$$\forall u, v \in A^*, \quad uv\rho = u\rho . \pi . v\rho$$

Tout d'abord, si (r,l) appartient à $u\rho . \pi . v\rho$, il existe par définition (l', r') dans π tels que : $rul', r'vl \in X^*$ et $f = l'r'$; on a alors $r'ufvl' \in X^*$, d'où $ruvl \in X^*$, du fait que f est un mot neutre, et enfin (r,l) appartient à $uv\rho$. Maintenant, si (r,l) appartient à $uv\rho$, alors $ruvl \in X^*$ et donc aussi $rufvl \in X^*$; mais comme f est incomplétable dans X, cela implique l'existence d'une factorisation de f en : $f = l'r'$ telle que : $rul', r'vl \in X^*$, ce qui exprime le fait que $(r,l) \in u\rho . \pi . v\rho$.

Ceci montre que l'application $\xi : u \in A^* \to \pi . u\rho$ (resp. $u\rho$) est un homomorphisme de A^* sur un semigroupe de relations sur l'ensemble *fini* L (resp. R). Le monoïde $M = \xi A^*$ est donc fini et ξf est son élément neutre (mais n'est pas en général l'égalité sur L) ; le sous-groupe (des éléments inversibles) de M est de plus transitif : remarquons en effet tout d'abord que, du fait que M est fini, tout conjugué $g = rl$ de $f = lr$ est encore dans X^* puisqu'ils ont même image par ξ ; ainsi, pour tous l, l' dans L, si $f = lr = l'r'$, alors $rlr'l'$ est dans X et le couple (l,l') appartient donc à $lr'\xi$, qui est inversible dans M. Ainsi, d'après la proposition 1 la relation $f\xi$ est une équivalence et le monoïde de relations N induit par M sur le quotient de L par cette équivalence est très transitif. Enfin, l'image réciproque par ξ du stabilisateur de la classe de $l \in L$ est égale à X^* puisqu'un élément de M stabilise l ssi il stabilise tous les éléments de sa classe.

L'énoncé suivant donne des conditions, en apparence beaucoup plus faibles, qui équivalent en fait à celles du théorème précédent. Leur intérêt nous semble être le fait qu'elles ne portent que sur des sous-alphabets finis de A et que chacune d'elles est, en un certain sens, unilatérale ; nous ommettons d'en donner ici la preuve.

Proposition 3. *Une condition nécessaire et suffisante pour que* X^* *soit reconnu par un monoïde très transitif est l'existence d'un mot* $h \in A^+$ *tel que pour tout sous alphabet fini* B *de* A *satisfaisant* $h \in B^*$ *les conditions suivantes soient remplies :*

(1) L'idéal à gauche B^*h *rencontre le stabilisateur de chacun des états de l'automate minimal reconnaissant* $Y^* = X^* \cap B^*$: $\forall\, b \in B^*, \exists g \in B^*$: $bb' \in Y^* \Leftrightarrow bhgb' \in Y^*$

(2) Pour tout $b \in B^*$, *il existe un entier* n *tel que* bh^n *soit incomplétable à droite dans* X : $bh^n B^* \cap X = \emptyset$.

Remarque 1. Le théorème 1 implique, sous l'hypothèse supplémentaire que X est un code, que X peut être reconnu par un monoïde de relations non-ambigu isomorphe à son monoïde syntaxique. Cet énoncé est, en fait, vrai de tous les codes reconnaissables, suivant le très important théorème de [3].

Sous monoïdes finiment engendrés

Nous en venons maintenant au cas où l'ensemble X est localement fini, c'est-à-dire que l'intersection de X avec B^* est finie pour tout sous alphabet fini B de A. Tout d'abord, d'après le théorème 1, X^* est alors reconnaissable s'il possède des mots neutres ; en effet, si $h \in A^+$ est un mot neutre il possède une puissance, soit h^n qui est incomplétable dans X, et h^n est encore lui-même neutre. On pourra donc, sans perte de généralité, supposer que A est fini ainsi que X.

Nous établissons le résultat suivant, dans lequel U désigne le sous-groupe (des éléments inversibles) du monoïde syntaxique de X^* et $|X|$ la borne supérieure des longueurs des mots de X :

Théorème 2. *Si* X *est fini,* U *est cyclique d'ordre au plus égal à* $|X|$.

Démonstration. Tout d'abord, les hypothèses du théorème 1 étant satisfaites, il existe une représentation ξ de A^* par un monoïde M de relations très transirif reconnaissant X^* ; d'après la proposition 2, M est isomorphe au monoïde syntaxique de X^* et U est donc isomorphe au groupe transitif formé des permutations contenues dans M. Notons B l'intersection de l'alphabet A avec $U\xi^{-1}$; la restriction de ξ à B^* est une représentation de B^* par un monoïde

de relations qui est évidemment non ambigu et qui reconnaît l'intersection de X^* avec B^* ; la preuve suivra du lemme ci-dessous, dont nous ferons encore usage plus bas :

Lemme. *Soit* ξ *une représentation de* B^* *par un monoïde transitif de relations non ambigu sur un ensemble* Q *et* Y^* *le stabilisateur de l'état* 0 . *Alors* Y *est fini ssi il existe un ordre sur* Q *tel que pour toute lettre* $a \in A$, *on ait :* $(q,q') \in a\xi$ *seulement si* $q \leq q'$ *ou si* $q = 0$.

Démonstration. La condition est évidemment suffisante puisqu'elle implique que tout mot de Y ait une longueur au plus égale à $\mathrm{Card}(Q)$. Réciproquement, il nous suffit de vérifier que la relation sur $Q \setminus 0$ définie par $(q,q') \in a\xi$ pour au moins une lettre a A a une fermeture transitive antisymétrique. Supposons donc qu'il existe $q_1,\ldots, q_k \in Q\setminus 0$ et $a_1,\ldots, a_k \in A$ tels que : $(q_1, q_2) \in a_1\xi,\ldots, (q_k, q_1) \in a_k\xi$; soient $f,g \in A^*$ deux mots tels que : $(q,q_1) \in f\xi$, $(q_1, q) \in g\xi$ et que cette relation ne soit vraie pour aucun facteur droit (resp. gauche) de f (resp. g). On a alors $f(a_1 a_2 \ldots a_k)^* g \subset Y$ puisque le monoïde $A^*\xi$ est non ambigu, en contradiction avec l'hypothèse que Y est fini.

D'après le lemme, toutes les permutations $b\xi$, pour b dans B doivent être égales à une même permutation circulaire de l'ensemble de tous les états ; ceci montre que le groupe U est cyclique d'ordre $p = \mathrm{Card}(Q)$ et que B^p est inclus dans X , ce qui achève de prouver le théorème.

Dans le cas où X est un code, l'énoncé précédent peut être précisé ainsi :

Corollaire. *Si* X *est un code fini, le groupe* U *est cyclique d'ordre* $|X|$.

Démonstration. En effet, d'après le lemme précédent, tout mot de X est de longueur au plus égale à $p = \mathrm{Card}(Q)$ et si b est une lettre dont l'image syntaxique est dans U , on a $b^p \in X$.

Remarque 2. Si X n'est pas un code, il peut contenir des mots de longueur supérieure strictement à l'ordre de U comme le montre l'exemple suivant : soit $A = \{a, b\}$ et $X = a^p \cup \{ a^i b a^j \mid 0 \leq i,j \leq p-1 \}$; on a alors $X = (a^p)^* \cup A^* b A^*$,

a^p est un mot neutre pour X^*, le groupe U est cyclique d'ordre p et $|X| = 2p - 1$. Il serait intéressant de donner une borne à la longueur des mots de X en fonction de p.

Une propriété des monoïdes de relations non ambigus

Nommons Valence d'une relation r sur un ensemble Q son cardinal (en tant que partie de $Q \times Q$) ; un monoïde de relations sur Q peut être non-ambigu sans que tous ses éléments non-nuls aient la même valence ; cependant, dans le cas des monoïdes très transitifs, on obtient le résultat suivant :

Théorème 3. Soit M un monoïde de relations très transitif sur Q ne contenant pas la relation vide. Alors M est non-ambigu ssi tous ses éléments ont une valence égale à $\mathrm{Card}(Q)$.

Démonstration. On nommera valence d'une matrice m à éléments dans N la somme de tous ses éléments, notée $|m|$, et, pour toute relation r sur Q, on notera $\bar{r}$ la matrice à éléments dans N égaux à 0 ou 1, indexée par Q dont le support est r ; la valence de r est encore égale à $|\bar{r}|$.

Supposons d'abord que tous les éléments de M aient la même valeur p et montrons que M est non-ambigu : cela revient à montrer que pour tous éléments m,m' de M, la matrice $\bar{m}\,\bar{m}'$ n'a que des éléments égaux à 0 ou 1. Supposons donc par l'absurde que $\bar{m}\,\bar{m}'$ a au moins un élément égal à 2 et calculons la somme $s = \sum_{u \in U} |m u m'|$, où U est le sous-groupe de M ; d'une part $s = p\,\mathrm{Card}(U)$ puisque chacun des $m u m'$ a une valence égale à p. D'autre part, s est strictement inférieur à la somme $t = \sum_{u \in U} |\bar{m}\,\bar{u}\,\bar{m}'|$ puisque : $|m m'| < |\bar{m}\,\bar{m}'|$. Or, on a aussi $t = |\sum_{u \in U} \bar{m}\,\bar{u}\,\bar{m}'| = |\bar{m} K \bar{m}'|$ où K est la matrice dont tous les éléments sont égaux à $q = \frac{1}{p}\,\mathrm{Card}(U)$, puisque U est transitif. Ceci montre que $t = p\,\mathrm{Card}(U)$, en contradiction avec le fait que $s < t$.

La réciproque est conséquence directe du lemme ci-dessous :

Lemme. *Soit* M *un monoïde de relations très transitif sur un ensemble* Q . *Si* M *contient un élément de valence strictement inférieur à* p = Card(Q), *alors* M *contient la relation vide.*

Si M *contient un élément de valence strictement supérieur à* p , *alors* M *est ambigu.*

Démonstration. Soit m un élément de M et K la matrice dont tous les éléments sont égaux à 1. Nous évaluons de deux manières la valence de la matrice $(K\bar{m})^n$, pour un entier n quelconque. D'une part : $|(K\bar{m})^n| = p|m|^n$ puisque $|K\bar{m}| = p|m|$ et que $(K\bar{m})^2 = |m|K\bar{m}$.

D'autre part : $|(K\bar{m})^n| = \sum_{u_i \in U} \frac{1}{q^n} |\bar{u}_1 \bar{m} \ldots \bar{u}_n \bar{m}|$ puisque la matrice K est égale à $\frac{1}{q} \sum_{u \in U} \bar{u}$.

Tout d'abord, si M ne contient pas la relation vide, chacun des termes de la forme $\bar{u}_1 \bar{m} \ldots \bar{u}_n \bar{m}$ a une valence non nulle et cela implique que $|(K\bar{m})^n| \geq p^n$; on en déduit que l'inégalité $|m|^n \geq p^{n-1}$ est vraie pour tout entier n et cela implique que $|m| \geq p$.

Maintenant, si M est inambigu, chacun des termes de la somme a une valence au plus égale à p^2 et ceci implique que $|(K\bar{m})^n| \leq p^{n+2}$; on en déduit que l'inégalité $|m|^n \leq p^{n+1}$ est vraie pour tout entier n , ce qui implique $|m| \leq p$.

Nous revenons maintenant à un sous monoïde X^* de A^* possèdant des mots neutres incomplétables dans X c'est-à-dire, d'après le théorème 1 que X^* est reconnu par un monoïde M de relations très transitif sur un ensemble Q ; on notera p, comme ci-dessus, le cardinal de Q et on désignera par |f| la valence de la relation sur Q définie par le mot $f \in A^*$.

Corollaire 1. *Tout mot de* A^* *est complétable dans* X^* *ssi* $|f| \geq p$ *pour tout mot* $f \in A^*$.

En effet, pour que tout mot soit complétable dans X^*, il faut et il suffit que le monoïde M ne contienne pas la relation vide et cet énoncé est donc une reformulation de la première assertion du lemme.

Corollaire 2. *Si* X^* *est librement engendré par* X, *on a* $|f| \leq p$ *pour tout* $f \in A^*$.

Cet énoncé est une reformulation de la deuxième assertion du lemme puisque X^* est librement engendré par X ssi le monoïde M est non-ambigu. Enfin, on sait que si X est un code reconnaissable, alors tout mot de A^* est complétable dans X^* ssi X est un code maximal (on en trouvera une preuve en [4] ou [6]). On peut donc reformuler le théorème 3 de la façon suivante :

Corollaire 3. X *est un code maximal ssi pour tout* $f \in A^*$, *on a* $|f| = p$.

Cet énoncé a une forme plus frappante dans le cas où X est un code fini puisque, dans ce cas, si a est une lettre dont une puissance est un mot neutre, la valeur de $f \in A^*$ est le nombre de mots de la forme $a^i f a^j$ qui sont dans X^* avec $0 \leq i,j \leq p-1$. Cette formulation fournit une analogie remarquable avec le cas particulier des codes préfixes maximaux où la condition que le nombre de mots de cette forme soit égal à p est trivialement vérifiée.

Références

1 BERSTEL, J.- Sur la densité asymptotique des langages formels, in *Automata Languages and Programming* (M. Nivat ed.) North Holland (1972) 345-58.

2 BOE, J.M.- *Représentations des monoïdes : applications à la théorie des codes*, Thèse de 3ème cycle, Univ. des Sciences et Techniques du Languedoc (1976).

3 BOE, J.M., BOYAT, J. CESARI, Y., LACHENY, A. et M. VINCENT, Automates et monoïdes syntaxiques des sous-monoïdes libres, à paraître dans *Information and Control*.

4 EILENBERG, S.- *Automata, Languages and Machines*, Vol. A, Academic Press (1974).

5 LALLEMENT, G.- On regular semigroups as syntactic monoids of prefix codes, à paraître dans *Theoretical Computer Science*.

6 NIVAT, M.- Eléments de la théorie générale des codes, in *Automata Theory* (E.R. Caianiello ed.) Academic Press (1966).

7 Mc NAUGHTON, R. and PAPERT, S.- *Counter-Free Automata*, MIT Press (1971).

8 PERROT, J-F.- *Contribution à l'Etude des Monoîdes Syntaxiques et de Certains Groupes Associés aux Automates Finis*, Thèse, Paris (1972).

9 RESTIVO, A.- On codes having no finite completions, in *Automata, Languages and Programming* (S. Michaelson ed.) Edinburgh University Press (1976) 38-44.

Reprinted from ADVANCES IN MATHEMATICS
All Rights Reserved by Academic Press, New York and London

Vol. 24, No. 3, June 1977
Printed in Belgium

Une Propriété de Hankel des Relations Fonctionnelles entre Monoïdes Libres

M. P. SCHÜTZENBERGER

Department of Mathematics, Université de Paris VII, 2 Place Jussieu, 75016 Paris V, France

EN MÉMOIRE DE N. LEVINSON

1. INTRODUCTION

La théorie des automates et, plus précisément, le théorème de Kleene ont montré que la notion de *rationalité* était susceptible d'interprétations non commutatives au delà du cadre classique de la théorie des fonctions. Nous faisons référence au volume A du Traité de S.E. Eilenberg [1] pour un exposé définitif des méthodes et des résultats et leur historique. Le présent travail s'insère dans cette perspective et son résultat principal est une variante du théorème de Hankel relative à l'étude des relations fonctionnelles (= application partielles) d'un monoïde libre A^* dans un autre, B^*(cf. [1], chap. IX et XI).

Rappelons que sous sa forme classique le théorème de Hankel caractérise une série rationnelle $r(x) = \sum r_n x^n$ par la condition que la $\mathbb{N} \times \mathbb{N}$-matrice H telle que $H(n, m) = r_{n+m}$, identiquement, ait un rang fini. Ceci revient à définir la rationalité de la série formelle $\sum r_n x^n$ par l'existence d'une relation de récurrence linéaire constante entre les coefficients r_n, c'est-à-dire encore par la possibilité d'exprimer ceux-ci par la projection sur l'anneau des coefficients des puissances $(x\mu)^n$ d'une matrice $x\mu$ de dimension finie; il est commode de prendre par projecteur le produit de $(x\mu)^n$ par deux vecteurs fixes v et v' et l'on a alors formellement:

$$r(x) = \sum r_n x^n = \sum v \cdot (x\mu)^n \cdot v' \cdot x^n = v \cdot (1 - x\mu \cdot x)^{-1} \cdot v'.$$

De façon équivalente, introduisant les vecteurs $x^n\lambda = v \cdot (x\mu)^n$ et $x^m\rho = (x\mu)^m \cdot v'$, on voit que chaque entrée $H(n, m)$ de la matrice de Hankel H est égale au produit scalaire $x^n\lambda \cdot x^m\rho = r_{n+m}$.

Cette définition de la rationalité $r(x)$ conduit immédiatement à une double généralisation:

(a) d'une part on peut prendre les entrées de la matrice $x\mu$ et des vecteurs v et v', donc des vecteurs $x^n\lambda$, $x^m\rho$ et les coefficients r_n eux-même, dans un semi-anneau quelconque S;

(b) d'autre part, on peut remplacer la variable unique x et ses puissances successives x^n par un ensemble (fini) A et les mots du monoïde libre A^* qu'il engendre.

ISSN 0001–8708

Les coefficients r_n deviennent alors une fonction α de A^* dans S et l'on considère la série formelle $\sum\{a\alpha \cdot a : a \in A^*\}$. En conformité avec le cas d'une variable unique, cette série sera dite *rationelle* (sur S) ssi il existe un morphisme μ de A^* dans un monoïde de matrices de *dimension finie* à entrées dans S et deux vecteurs fixes v et v' tels que $a\alpha = v \cdot a\mu \cdot v'$ pour chaque mot a de A^*; le triple (μ, v, v') est appelé un *transducteur* pour α par M. Nivat(3); comme ci-dessus on a $\sum\{a\alpha \cdot a\} = v \cdot (1 - M)^{-1} \cdot v'$ où $M = \sum\{a\mu \cdot a : a \in A\}$. Cette présentation n'est d'ailleurs qu'un cas particulier d'une construction abstraite plus générale développée par Elgot et Mezei (2). Elle a pour nous l'avantage de s'interpréter directement du point de vue de Hankel. En effet, on peut associer à l'application α de A^* dans S la $A^* \times A^*$-matrice H dont chaque entrée $H(a, a')$ est égale au coefficient $(aa')\,\alpha = v \cdot (aa')\,\mu \cdot v'$ du mot a et, introduisant comme précédemment les vecteurs $a\lambda = v \cdot a\mu$ et $a'\rho = a'\mu \cdot v'$ de même dimension *finie* d que μ, on a identiquement $H(a, a') = a\lambda \cdot a'\rho$. Par conséquent la matrice de Hankel H est de rang fini puisqu'elle est le produit $H_\lambda' \cdot H_\rho'$ de la $A^* \times d$-matrice H_λ' dont les lignes sont les vecteurs $a\lambda$ par la $d \times A^*$-matrice H_ρ' dont les colonnes sont les $a\rho$. De façon plus rapide, on vient donc de montrer que quand l'application α est définie par un transducteur, elle admet ce que nous appelerons une *factorisation* c'est-à-dire une paire de fonctions vectorielles (λ, ρ) de dimension finie satisfaisant l'identité:

(1) $(aa')\,\alpha = a\lambda \cdot a'\rho$ pour tous les mots a, a' de A^*;

qui permet l'existence de la matrice de Hankel.

Il est clair que la condition essentielle est la finitude de la dimension puisque l'on peut toujours (trivialement) associer à n'importe quel α une paire d'applications(λ, ρ) dans les A^*-vecteurs satisfaisant l'identité (1).

Ceci constitue la partie directe du théorème de Hankel pour α et elle n'est donc ici que la simple conséquence de la définition adoptée pour la rationalité de la série formelle $\sum a\alpha \cdot a$. Reste la partie réciproque qui consisterait à établir que α est définie par un transducteur quand α: $A^* \to S$ est une application donnée admettant une factorisation. Nous donnons une réponse positive dans le cas très particulier où α est une relation fonctionnelle entre A^* et un autre monoïde libre B^*; le semi-anneau S étant alors le semi-anneau booléen des parties de B^* et α une application de A^* dans S telle que, pour chaque mot a de A^*, $a\alpha$ est soit un mot de la base B^* de S, soit la partie vide, qui est le zéro, 0, de S. Ce cas correspond à celui des *bimachines* de S. Eilenberg ([1, chap. XI, sect. 7]). Les méthodes linéaires du cas classique (qui sont exclues par le caractère booléen de S) sont remplacées par les méthodes de [1, Proposition 12.3, chap. III, et Théorème 4.2, chap. XII] dont l'usage est rendu possible par l'hypothèse initiale que α est une fonction (= application partielle) de A^* dans B^*. Cette même hypothèse permet de supposer que tous les vecteurs $a\lambda$ et $a\rho$ de la factorisation (λ, ρ) de α ont leurs coordonnées non nulles dans B^*; de fait on supposera même seulement (par commodité) que ces coordonnées sont des éléments du

groupe libre $B^{(*)}$ engendré par le même ensemble B que le monoïde B^*. L'hypothèse que A^* est finiment engendré ne sera pas utilisée. Le résultat principal de ce travail est donc la:

PROPRIÉTÉ. *Soit* $\alpha: A^* \to B^*$ *une fonction. Une condition suffisante (et nécessaire) pour quelle soit définie par un transducteur est qu'elle admette une factorisation* (λ, ρ) *dont les vecteurs ont leurs coordonnées non nulles dans le groupe libre* $B^{(*)}$.

2. VÉRIFICATION DE LA PROPRIÉTÉ

On considère une application partielle de rang finie $\alpha: A^* \to B^*$ fixe et une de ses factorisations (λ, ρ) de dimension n. On commence par vérifier que l'on peut imposer à (λ, ρ) des conditions supplémentaires (0), (2), (3), (4) en montrant pour chacune de celles-ci que si elle n'était pas remplie par (λ, ρ) on pourrait trouver une autre factorization (λ', ρ') qui la satisfasse ainsi que les conditions précédentes.

Pour chaque indice $i \in I = \{1, 2, \ldots, n\}$ on note λ_i (resp., ρ_i) l'application envoyant chaque mot a de A^* sur la valeur de la i-ème coordonnée du vecteur $a\lambda$ (resp., $a\rho$); $L_i = \{a \in A^* : a\lambda_i \neq 0\}$ et $R_i = \{a \in A^* : a\rho_i \neq 0\}$.

Comme d'usage, le *support* d'un vecteur $v(=a\lambda$ ou $a\rho$, $a \in A^*)$ est l'ensemble noté $v\#$ des indices de ses coordonnées non nulles.

Venons en à la première condition supplémentaire.

(0) *Pour chaque* $i \in I$ *on a* $L_i \neq \varnothing$ *et* $R_i \neq \varnothing$.

Preuve. Soit $I' = \{i \in I : L_i \neq \varnothing$ et $R_i \neq \varnothing\}$. Pour chaque $i \in I \backslash I'$ et $a, a' \in A^*$ le terme $a\lambda_i \cdot a'\rho_i$ du produit scalaire $a\lambda \cdot a\rho$ est nul puisque $a\lambda_i = 0$ ou $a'\rho_i = 0$. Donc la paire (λ', ρ') où λ' et ρ' sont les restrictions à I' de λ et de ρ est encore une factorisation de α et satisfait (0). Q.E.D.

(2). *Pour tout* $a, a' \in A^*$ (resp., $i, j \in I$) *les supports* $a\rho\#$ *et* $a'\rho\#$ (resp., *les parties* R_i *et* R_j *de* A^*) *sont égaux ou disjoints.*

Preuve. L'équivalence des deux conditions énoncées est claire. En effet, chacune d'elles signifie que pour tout $a, a' \in A^*$; $i, j \in I$ les relations $a\lambda_i \neq 0$, $a\lambda_j \neq 0$, $a'\lambda_i \neq 0$ impliquent $a'\lambda_j \neq 0$.

Supposons qu'elles ne sont pas satisfaites et soit I' l'ensemble des paires de la forme (i, q) où $i \in I$ et où q est une partie de I contenant i telle que $q = a\rho\#$ pour au moins un mot a.

On définit deux applications λ' et ρ' de A^* dans les I'-vecteurs en posant pour chaque $a \in A^*$ et $i' = (i, q) \in I'$:

$$a\lambda'_{i'} = a\lambda_i ;$$

$$a\rho'_{i'} = a\rho_i \quad \text{si} \quad a\rho\# = q; = 0 \text{ sinon}$$

Il est clair que I' est fini et que (λ', ρ') satisfait (0) et (2). Soient a, $a' \in A^*$. Les termes non nuls du produit scalaire $a\lambda' \cdot a'\rho'$ sont ceux de la forme $a\lambda'_{i'} \cdot a'\rho'_{i'}$, où $i' = (i, a'\rho\#)$ avec, par définition, $i \in a'\rho\#$, c'est-à-dire $a'\rho_i \neq 0$. Ils sont donc en correspondance biunivoque avec les termes non nuls de $a\lambda \cdot a'\rho$. Comme $a\lambda'_{i'} \cdot a'\rho'_{i'} = a\lambda_i \cdot a'\rho_i$ par définition pour i' et i comme ci-dessous, on a identiquement $a\lambda' \cdot a'\rho' = a\lambda \cdot a'\rho$ ce qui montre que (λ', ρ') est une factorisation de α. Q.E.D.

(3). *Pour chaque paire f, f' de mots de A^* il existe au plus un indice $i \in I$ tel que $f\lambda_i \cdot f'\rho_i \neq 0$.*

Preuve. Supposons au contraire que les termes $x_j = f\lambda_j \cdot f'\rho_j$ et $x_k = f\lambda_k \cdot f'\rho_k$ soient non nuls pour deux indices distincts j et k. Comme x_j et x_k figurent dans le produit scalaire $f\lambda \cdot f'\lambda = (ff')\alpha$ qui d'après (1) est un mot b de B^*, on doit avoir $b = x_j = x_k$ ce qui entraîne l'existence d'un élément c du groupe $B^{(*)}$ pour lequel $f\lambda_k = f\lambda_j \cdot c$ et $f'\rho_k = c^{-1} \cdot f'\rho_j$.

On a $j, k \in f'\rho\#$ et d'après (2) l'ensemble $F = \{a \in A^* : a\rho\# = f'\rho\#\}$ contient tous les mots dont le support du vecteur ρ rencontre $\{j, k\}$. De plus si $a' \in F$ il existe un $b' \in B^*$ tel que $b' = (fa')\alpha = f\lambda \cdot a'\rho = f\lambda_j \cdot a'\rho_j = f\lambda_k \cdot a'\rho_k$ ce qui implique que $a'\rho_k = c^{-1} \cdot a'\rho_j$ avec le même c que plus haut. Autrement dit, l'ensemble $\{a\rho_j \cdot (a\rho_k)^{-1} : a \in R_j = R_k\}$ est un élément unique, $c \in B^{(*)}$. Nous utiliserons désormais exclusivement cette condition sur les indices j et k et nous notons qu'elle implique que si $a \in A^*$ et $a\lambda_k \neq 0$ on a $a\lambda_k \cdot a'\rho_k = a\lambda_k \cdot c \cdot a'\rho_j$ pour chaque $a' \in R_j = R_k$.

Soient maintenant ρ' la restriction de ρ à $I' = I\backslash k$ et λ' l'application de A^* dans les I'-vecteurs telle que pour chaque $a \in A^*$ et $i \in I'$ on ait $a\lambda_i' = a\lambda_k \cdot c$ si $i = j$ et $a\lambda_k \neq 0$ et $a\lambda_i' = a\lambda_i$ dans tous les autres cas. Les remarques précédentes montrent que (λ', ρ') est une factorisation de α et on vérifie facilement qu'elle remplit les conditions (0) et (2). Le résultat en découle par induction sur Card I. Q.E.D.

(4) *Si j et k sont deux indices distincts pour lesquels $R_j = R_k$, l'ensemble $G_{jk} = \{a\rho_j \cdot (a\rho_k)^{-1} \in B^{(*)} : a \in R_j = R_k\}$ est infini.*

Preuve. Notons $M(\lambda, \rho)$ l'ensemble des paires d'indices distincts j, k pour lesquels G_{jk} est fini, $M_1(\lambda, \rho)$ le nombre de celles pour lesquelles G_{jk} est un singolet et $M_2(\lambda, \rho) = \text{Card } M(\lambda, \rho) - M_1(\lambda, \rho)$. On vérifie facilement que quand Card $G_{jk} = 1$ la transformation $(\lambda, \rho) \to (\lambda', \rho')$ par restriction à $I\backslash k$ décrite dans la preuve précédente a la propriété que $M_1(\lambda', \rho') < M_1(\lambda, \rho)$ et $M_2(\lambda', \rho') \leqslant M_2(\lambda, \rho)$.

Il suffit donc, par induction, de construire une autre transformation $(\lambda, \rho) \to (\lambda', \rho')$(entre factorisations de α) pour laquelle $M_2(\lambda', \rho')$ est strictement moindre que $M_2(\lambda, \rho)$(au prix d'un accroissement éventuel de M_1). C'est ce que nous faisons maintenant en supposant que $M_1(\lambda, \rho) = 0$ ainsi qu'il est loisible d'après ce qui précède.

Soit (j_1, k_1) une paire fixe dans $M(\lambda, \rho)$. Par hypothèse $R_{j1} = R_{k1}(=R)$ et il existe donc une partie K de I contenant ces deux indices telle que $R = \{a \in A^* : a\rho\# = K\}$.

Notons E l'union de la restriction à K de la relation binaire $M(\lambda, \rho)$ sur I et de la diagonale de K, c'est-à-dire de $\{(k, k): k \in K\}$. Comme $\mathrm{Card}(G_{ik}) \leqslant \mathrm{Card}(G_{ij}) \times \mathrm{Card}(G_jk)$ pour tout $i, j, k \in K$, la relation E est une équivalence sur R et nous pouvons en choisir une section $\overline{K} \subset K$.

Pour chaque a de R soit $a\gamma$ le K-vecteur tel que pour chaque $j \in K$, sa coordonnée $a\gamma_j$ soit égale à l'élément $a\rho_j \cdot a\rho_k^{-1}$ de $B^{(*)}$ où $k = k_j$ est l'unique élément de la section $\overline{K}$ qui appartienne à la même classe de E que j.

L'ensemble $C = \{a\gamma : a \in R\}$ est fini, par définition, puisque E est une équivalence.

Soit maintenant I' l'union des ensembles $I\backslash K$ et $K \times C$. Pour chaque mot a de A^*, on définit les I'-vecteurs $a\lambda'$ et $a\rho'$ par les conditions suivantes:

$a\lambda'_{i'} = a\lambda_{i'}$ et $a\rho'_{i'} = a\rho_{i'}$ si $i' \in I\backslash K$; et pour $i' = (k, c) \in K \times C$: $a\lambda'_{i'} = a\lambda_k$; $a\rho'_{i'} = a\rho_k$ si $a\gamma = c$ et $= 0$ sinon.

La vérification que (λ', ρ') est encore une factorisation de α satisfaisant (0), (2) et (3) est immédiate et peut être omise. La contribution à $M_2(\lambda', \rho')$ des paires $j', k' \in I\backslash K$ est la même que pour (λ, ρ) et, par construction, celle des paires dans $K \times C$ est nulle. Donc $M_2(\lambda', \rho')$ est strictement moindre que $M(\lambda, \rho)$. Q.E.D.

(5). *Il existe un morphisme μ de A^* dans un monoide de $I \times I$-matrices à entrées dans $B^{(*)} \cup 0$ tel que $a\lambda = 1\lambda \cdot a\mu$ pour chaque mot a.*

Preuve. Soit Q l'ensemble des supports des vecteurs $a\lambda (a \in A^*)$. D'après (0) et (2) on peut choisir une partie minimale fixe S de A^* telle que $\{s\rho\# : s \in S\}$ forme une partition de I.

(5.1.). Soit maintenant $a \in A^*$ donné. Nous montrons d'abord qu'il existe une application partielle $q \to q \cdot a$ de Q dans lui-même telle que $(fa)\lambda\# = q \cdot a$ pour chaque $q \in Q$ et $f \in F_q = \{f' \in A^* : f'\lambda\# = q\}$. Soient donc $q \in Q$, $f \in F_q$ et supposons pour commencer que $(fa)\lambda\#$ contient un indice j.

D'après (0) on peut prendre un mot $g \in S \cap R_j$ et l'on a $(fag)\alpha = (fa)\lambda j \cdot g\rho_j = b$ pour un certain mot b de B^*. Comme (λ, ρ) est une factorisation de α on a aussi $b = f\lambda \cdot (ag)\rho$ donc d'après (3) $b = f\lambda_i \cdot (ag)\rho_i$ pour un indice unique i.

Prenons un autre mot $f' \in F_q$. L'indice i appartient à q et l'on a donc $f'\lambda_i \cdot (ag)\rho_i = b' \in B^*$. Appliquant de nouveau (3) on obtient un indice unique k tel que $b' = (f'ag)\alpha = (f'a)\lambda_k \cdot g\rho_k$.

Les équations qui viennent d'être écrites donnent:

$$g\rho_j = (fa)\lambda_j^{-1} \cdot f\lambda_i \cdot (ag)\rho_i \ (\neq 0);$$

$$g\rho_k = (f'a)\lambda_k^{-1} \cdot f'\lambda_i \cdot (ag)\rho_i \ (\neq 0).$$

Par conséquent $g\rho_j \cdot g\rho^{-1}$ est égal au produit:

$$\rho_i = (fa)\,\lambda_j^{-1} \cdot f\lambda_i \cdot f'\lambda_i^{-1} \cdot (f'a)\,\lambda_k\,.$$

De plus $j, k \in g\rho\#$ ce qui implique $R_j = R_h$ d'après (2).

Gardant f et f', soit g' un autre mot de R_j. Le même raisonnement que ci-dessus donne un indice i' et une équation:

$$f\lambda_{i'} \cdot (ag')\,\rho_{i'} = (fa)\,\lambda_j \cdot g'\rho_j \neq 0.$$

Comme k (resp. i') appartient d'après (2) au support commun de $g\rho$ et $g'\rho$ (resp. $f\lambda$ et $f'\lambda$) on a aussi l'équation:

$$f'\lambda_{i'} \cdot (ag')\,\rho_{i'} = (f'a)\,\lambda_k \cdot g'\rho_k \neq 0.$$

On en déduit que $g'\rho_j \cdot g'\rho_k^{-1}$ est égal au produit $p_{i'}$ obtenu en remplaçant par i' l'indice i dans l'expression de p_i.

Donc l'ensemble $G_{jk} = \{g''\rho_j \cdot g''\rho_k^{-1} : g'' \in R_j = R_h\}$ contient au plus Card I éléments. Comme I est fini, la condition (4) montre que l'on doit avoir $j = k$. Ceci établit l'assertion annoncée.

(5.2.). Revenant aux calculs précédents, on voit que (S étant fixée) l'indice i ne dépend que de a, j et q. L'équation $b = (fa)\,\lambda_j \cdot g\rho_j = f\lambda_i \cdot (ag)\,\rho_i$ montre que, de même, le rapport:

$$f\lambda_i^{-1} \cdot (fa)\,\lambda_j = (ag)\,\rho_i \cdot g\rho_j^{-1}\ (= x_{ji})$$

est indépendant du choix de f dans F_q. On peut donc définir une $q \times q \cdot a$— matrice notée am_q ayant une et une seule entrée non nulle ($= x_{ji}$) dans chaque colonne qui satisfasse identiquement $(fa)\,\lambda = f\lambda \cdot am_q$ pour chaque $f \in F_q$.

(5.3.). Posons $I' = Q \times I$ et pour chaque mot a définissons la $I' \times I'$ matrice $a\mu$ par la condition que pour tout $q, q' \in Q$ son bloc (q, q') soit la matrice nulle si $q' \neq qa$ et sinon qu'il soit la matrice am_q qui vient d'être écrite. Par construction toutes les entrées non nulles de $a\mu$ sont dans $B^{(*)}$ et on vérifie directement que $(aa')\,\mu = a\mu \cdot a'\mu$ pour tout $a, a' \in A^*$. On vérifie de même que l'on a identiquement $a\lambda' = 1\lambda' \cdot a\mu$ où $a\lambda'$ est le I'-vecteur tel que $a\lambda'_{(q,i)} = a\lambda_i$ ou 0 selon que $q = a\lambda\#$ ou non.

Enfin, d'après (3) il correspond à chaque $q \in Q$ un indice unique $i = i_q$ pour lequel $f\lambda_i \cdot 1\rho_i \neq 0$ quand $f \in F_q$. On définit les I'-vecteurs $a\rho'$ par $a\rho' = a\mu \cdot 1\rho (a \in A^* \backslash 1)$ et $1\rho'_{(q,i)} = 1\rho_i$ ou $= 0$ selon que $i = i_q$ ou non.

On a donc identiquement:

$$(aa')\,\alpha = (aa')\,\lambda \cdot 1\rho = (aa')\,\lambda' \quad 1\rho' = 1\lambda' \cdot (aa')\,\mu \cdot 1\rho'$$
$$= 1\lambda' \cdot a\mu \cdot a'\mu \cdot 1\rho' = a\lambda' \cdot a'\rho'$$

ce qui montre que (λ', ρ') est une factorisation de α. Il suffit de la substituer à (λ, ρ) pour satisfaire (5). Q.E.D.

La construction précédente ne conserve que les conditions (0) et (3). Nous supposerons donc désormais que (λ, ρ) satisfait (0), (3) et (5), et nous faisons enfin jouer l'hypothèse que l'image de α appartient au sous-monoïde B^* du groupe $B^{(*)}$.

(6). *Pour chaque indice i de I l'ensemble $L_i\lambda_i(=\{a\lambda_i : a \in L_i\})$ est contenue dans B^* et ses mots n'ont pas de facteur droit commun non trivial (c'est-à-dire dans BB^*).*

Preuve. Par induction sur le nombre des indices pour lesquels (6) n'est pas remplie en remplaçant la factorisation (λ, ρ) par une factorisation $(\lambda\delta, \delta^{-1}\rho)$ où δ est une certain $I \times I$ matrice diagonale dont les entrées non nulles sont dans $B^{(*)}$ et au plus une de ces dernières est différente de 1. Il est clair qu'une telle transformation préserve (0), (3) et (5). Soit donc $i \in I$ fixe.

Prenons un mot $g \in R_i$ quelconque et soit d le plus long facteur droit commun (dans B^*) des mots de $(L_ig)\alpha$. On définit la matrice δ par $\delta_{ii} = (g\rho_i)^{-1}\, d$ et on effectue la transformation correspondante. Ceci permet de supposer désormais $g\rho_i = d$. On a $(ag)\,\alpha = a\lambda_i \cdot d \in B^*$ pour tout $a \in L_i$. Donc, d'après le choix fait de d, tous les $a\lambda_i$ sont des mots de B^* et ils n'ont pas de facteur droit commun dans $BB^* = B^*\backslash 1$. Q.E.D.

Fin de la vérification de la Propriété

Il reste seulement à montrer que si $a \in A^*$, $i, j \in I$ et $a\mu(i, j) = c \in B^{(*)}$, on a bien $c \in B^*$. Soit donc $f \in L_i$. On a $f\lambda_i \cdot c = (fa)\,\lambda_j$ où $f\lambda_i$ et $(cfa)\,\lambda_j$ sont des mots de B^* d'après la première partie de (6). La seconde partie de cette même condition montre que, ou bien $L_i\lambda_i$ est un mot unique qui est nécessairement 1, auquel cas $c = (fa)\,\lambda_j \in B^*$, ou bien il existe un autre mot $f' \in L_i$ tel que $f\lambda_i = b$ et $f'\lambda_i = b'$ ne se terminent pas par la même lettre de B. Dans ce second cas, supposant c écrit sous forme réduite, l'un au moins des deux produits $f\lambda_i \cdot c$ et $f'\lambda_i \cdot c$ est aussi sous forme réduite. Comme ces produits sont égaux respectivement aux mots $(fa)\,\lambda_j$ et $(f'a)\,\lambda_j$ de B^* ceci implique que $c \in B^*$ et achève la preuve de la propriété. Q.E.D.

References

1. S. Eilenberg, "Automata Languages and Machines," Vol. A, Academic Press, New York, 1975.
2. C. C. Elgot et G. Mezei, "On relations defined by generalised finite automata," *IBM J. Res. Develop.* **9** (1965), 47–65.
3. M. Nivat, "Transduction des langages de Chomsky," *Ann. Inst. Fourier (Grenoble)* **18** (1968), 339–455.

Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium

Theoretical Computer Science 4 (1977) 47–57.

SUR UNE VARIANTE DES FONCTIONS SEQUENTIELLES

M.P. SCHÜTZENBERGER
Université de Paris VII, Paris et I.R.I.A., Rocquencourt, France

Communiqué par M. Nivat
Reçu en juillet 1976

1. Introduction

Nous faisons référence aux Chapitres XI et XII du Traité de Eilenberg [1] pour la définition et la Théorie des fonctions (partielles) rationnelles et séquentielles généralisées d'un monoïde libre dans un autre. Nous nous proposons de montrer ici qu'au prix d'une perte de simplicité dans leur formulation certaines parties des théorèmes classiques de Ginsburg et Rose [3] et de Eilenberg s'appliquent à une famille un peu différente que nous appellerons famille des fonctions *sous-séquentielles* (sSq).

Dans ce qui suit A^* et B^* sont les monoïdes libres engendrés par les ensembles A et B ; B^* est considéré comme un sous-monoïde du groupe libre $B^{(*)}$ (engendré par B) et 0 est le zéro de l'algèbre de $B^{(*)}$ sur $\mathbf{Z}$. Si X est une partie de A^*, on appellera pour abréger *fonction de* X toute application de X dans l'union de B^* et de 0 et on notera $\mathbf{0}$ n'importe quelle function dont l'image est 0.

Soit, dorénavant, $k \geqslant 0$ un entier naturel fixe. Pour chaque $n \geqslant 0$ on désigne par F_n l'ensemble $A^k A^* \setminus A^{k+n+1} A^*$ des mots de A^* dont la longueur est comprise entre k et $k+n$. La famille sSq est l'union sur tous les n *finis* des sous-familles sSq(n) des *fonctions sous-séquentielles* de *dimension au plus* n dont la définition est la suivante:

Définition. sSq(n) est la famille des fonctions α de $A^k A^*$ telles qu'il existe une fonction β de A^* et une application $a \to \rho_a$ de A^* dans l'union de $\mathbf{0}$ et d'un ensemble R de n fonctions ρ ($\neq \mathbf{0}$) de F_n satisfaisant l'identité:

$$(af)\alpha = a\beta \cdot f\rho_a \qquad (a \in A^*, \quad f \in F_n). \tag{1}$$

Par conséquent sSq(0) se réduit à $\mathbf{0}$, et on supposera désormais que n est positif. Le Théorème 4.2. du Chapitre XII de [1] montre que les hypothèses de cette dèfinition sont satisfaites (avec $k = 0$, $\beta = \alpha$ et n assez grand) par n'importe quelle fonction séquentielle généralisée ("generalized sequential partial function") et donne une réciproque remarquable de cette propriété.

La motivation pour envisager la possibilité que α et β soient différentes provient du cas des fonctions ayant un domaine fini, des restrictions de fonctions séquentielles généralisées à un domaine (reconnaissable) arbitraire ou de l'exemple 8.2. du Chapitre XI de [1].

Les résultats principaux sont les Propriétés 2 et 3 qui constituent des adaptations au cas sous-séquentiel d'une partie des Théorèmes classiques de Ginsburg et Rose [4]. La Propriété 1 situe ces fonctions parmi les fonctions définies par des transducteurs finis au sens de Nivat [7].

2. Une autre définition

Nous commençons par construire certaines fonctions de A^kA^* ($k \geqslant 0$, fixe) dont la Propriété 1 à la fin de cette section établit l'équivalence avec les fonctions sous-séquentielles.

Soit Q un ensemble fini (non vide). Un *Q-transducteur sous-séquentiel* est un triple $(\mu, 1\lambda, v)$ où:

μ est un morphisme du monoïde A^* dans un monoïde de $Q \times Q$-matrices ayant leurs entrées dans $B^* \cup 0$ et au plus une entrée non nulle par ligne;

1λ est un Q-vecteur ligne à coordonnées dans $B^* \cup 0$ ayant exactement une coordonnée non nulle;

v est une application de $F_0 = A^k$ dans les Q-vecteurs colonnes à coordonnées dans $B^* \cup 0$.

Les conditions sur μ signifient que ce morphisme est monomial et impliquent que pour chaque mot a le vecteur $a\lambda = 1\lambda.\ a\mu$ ait au plus une coordonnée non nulle, qui est alors un mot de B^*. Il en résulte que le transducteur (μ, λ, v) définit une fonction α de A^kA^* par l'identité:

$$(af)\alpha = 1\lambda \cdot a\mu \cdot fv \qquad (a \in A^*, f \in F_0). \tag{2}$$

Evidemment on retrouve (pour A et B finis) les machines séquentielles généralisées classiques en prenant $k = 0$ (donc $F = \{1\}$), pour 1λ le Q-vecteur ayant une coordonnée égale à 1 et les autres à 0 et pour $1v$ le Q-vecteur dont toutes les coordonnées sont égales à 1.

2.1. *La fonction α définie par le Q-transducteur sous-séquentiel (μ, λ, v) est sous-séquentielle de dimension au plus* Card Q.

Preuve. Pour chaque mot a de A^* on note $a\beta$ et q_a la valeur de la coordonnée non nulle du vecteur $a\lambda$ et son indice si ce vecteur n'est pas nul; sinon $a\beta = 0$ et $q_a = \mathbf{0}$. On étend maintenant v à une fonction de A^hA^* en posant $(af)v = a\mu \cdot fv$ ($a \in A^*$, $f \in F_0$) et on convient que chaque q désigne la fonction de A^hA^* égale à la valeur de la coordonnée q du vecteur fv ($f \in A^kA^*$). On a donc identiquement:

$$(af)\alpha = a\lambda \cdot fv = a\beta \cdot fq_a$$

pour tout $a \in A^*$, $f \in A^h A^*$, donc, en particulier, pour tout $a \in A^*$, $f \in F_n$ $(= A^h A^* \setminus A^{h+n+1} A^*)$ ce qui achève la vérification. □

Notre objectif est d'établir une réciproque de cet énoncé (Propriété 1 cidessous). Afin de ne pas trop restreindre la généralité, nous considérons une partie G de A^* contenant tous les mots de longueur au plus $2n$ et les facteurs gauches de ses membres et une fonction α fixe de l'ensemble GF_n $(= \{gf \in A^* : g \in G, f \in F_n\})$.

Nous supposons qu'il existe une fonction β de G et une application $g \to \rho_g$ de G dans l'union de $\mathbf{0}$ et d'un ensemble R de n fonctions $(\neq \mathbf{0})$ de F_n telles que l'on ait:

$$(gf)\alpha = (g\beta)\cdot(f\rho_g) \qquad (g \in G, \quad f \in F_n). \tag{1}$$

Quand $G = A^*$, α est par définition une fonction sous-séquentielle de dimension $\leqslant n$. Nous supposons que n est minimum (par rapport à α) c'est-à-dire que l'on ne peut pas effectuer un autre choix de β tel que (1) soit satisfaite par un système de $n' \leqslant n$ fonctions ρ. Ceci implique évidemment que $D_\rho = \{g \in G : \rho = \rho_g\}$ soit non vide pour chaque $\rho \in R$. La donnée de α ne détermine pas complètement β et R. En particulier, d'après (1), chacune des relations $g\beta = 0$ ou $F_n\rho_g$ $(= \{f\rho_g : f \in F_n\}) = 0$ pour un mot g de G équivaut à $(gF_n)\alpha = 0$. On pourra donc supposer qu'elles sont toujours simultanément vérifiées ou non, c'est-à-dire que β et R satisfont la *première condition de normalisation*:

(0). Pour chaque $g \in G$, $g\beta = 0$ ssi $\rho_g = \mathbf{0}$.

Une second condition est la suivante:

(Min). Pour chaque $\rho \in R$, les mots de $(D_\rho)\beta$ n'ont pas de facteur droit commun dans $B^* \setminus 1$ (où D_ρ désigne comme toujours le domaine *propre* de ρ).

Supposons en effet que $b \in B^* \setminus 1$, soit un facteur droit commun de tous les mots de la forme $d\beta$ $(d \in D_\rho)$. Sans altérer la validité de (1) on peut remplacer chaque $d\beta$ par le mot $d\beta \cdot b^{-1}$ de B^* à condition de substituer à ρ la fonction, notée $b[\rho]$, envoyant chaque f sur $b \cdot (f\rho) \cdot (f \in F_n)$.

Cette notation $b[\rho]$ sera constamment utilisée dans la suite. En particulier, pour $j = 0, 1, \ldots, n$ nous désignerons par E_{n-j} la relation sur l'ensemble des fonctions de F_n telle que $(\rho, \rho') \in E_{n-j}$ ssi il existe un élément b de groupe libre $B^{(*)}$ pour lequel ρ' et $b[\rho]$ ont même restriction à F_{n-j} $(= A^h A^* \setminus A^{n+1-j} A^*)$. Comme $B^{(*)}$ est un groupe, chaque E_{n-j} est une relation d'équivalence et, par construction, les E_{n-j} forment une suite croissante. L'emploi de ces relations est dû à Eilenberg [1].

2.2. *La relation E_n se réduit à l'identité sur $R \cup \mathbf{0}$.*

Preuve. Supposons $(\rho, \sigma) \in E_n$, c'est-à-dire $\sigma = b[\rho]$ pour un $b \in B^{(*)}$.

Si $\rho = \mathbf{0}$ on a $f\sigma = b(f\rho) = 0$ pour chaque $f \in F_n$ donc $\sigma = \mathbf{0} = \rho$ et réciproquement.

Soient maintenant $\rho, \sigma \in R$ et $f \in F_n$ tels que $f\rho = r \neq 0$. On a $s = f\sigma = br$ donc $b = sr^{-1}$ où $r, s \in B^*$. Si t est le plus long facteur droit commun dans B^* de r et s, c'est-à-dire si $r = ut$, $s = vt$ où les mots u, v de B^* n'ont pas de facteur droit commun dans $B^* \setminus 1$, on a $b = vu^{-1}$ sous forme réduite. Ceci montre d'une part que $b = 1$, c'est-à-dire que $\rho = \sigma$ quand $u = v = 1$ et, d'autre part, que u (resp. v) est un facteur gauche commun des mots de $F_n\rho$ (resp. $F_n\sigma$).

Il reste donc seulement à vérifier que n ne serait pas minimal si l'on avait $u, v \neq 1$. Supposons donc $u \neq 1$. On peut substituer à ρ la fonction $\rho' = u^{-1}[\rho]$ quitte à remplacer chaque $d\beta$ par $d\beta \cdot u$ ($d \in D_\rho$) et de même pour σ. On a alors $\rho' = \sigma'$ ce qui achève la preuve. □

Nous désignons maintenant par G_1 le sous-ensemble formé des mots g de G pour lesquels gA^n est contenu dans G. Il est non vide puisque G contient tous les mots de longueur $\leqslant 2n \cdot R_1 = \{\rho_g : g \in G_1\}$.

2.3.0. *Soit $\rho \in R_1 \cup \mathbf{0}$ tel que $F_{n-1}\rho = 0$. On a $\rho = \mathbf{0}$.*

Preuve. Supposons au contraire $\rho \neq \mathbf{0}$, c'est-à-dire qu'il existe un mot h de F_n pour lequel $h\rho \neq 0$. Puisque $F_{n-1}\rho = 0$ on doit avoir $h \in F_n \setminus F_{n-1} = A^{k+n}$ ce qui permet de l'écrire sous la forme $h = a_1 a_2 \cdots a_n h_n = h_0$ avec $a_1, a_2, \ldots, a_n$ des letters de A et $h_n \in A^k$.

Comme $\rho \in R_1$ on peut prendre un mot $d = d_0$ dans $D_\rho \cap G_1$ ce qui fait que $dh \in G$. Posons $d_i = da_1 \cdots a_i$; $\rho_i = \rho_{d_i}$ ($\rho = \rho_0$); $h_i = a_{i+1} \cdots a_n h_n$ pour $0 \leqslant i \leqslant n$.

Utilisant l'identité (1) et $d_i\, h_i = dh$ on a:

$$0 \neq d\beta \cdot h\rho = (dh)\alpha = (d_i h_i)\alpha = d_i\beta \cdot h_i \rho_i.$$

Ceci implique $d_i\beta \neq 0$ et $h_i\rho_i \neq 0$. Comme $h_i \in F_{n-i}$, on en déduit que les ρ_i appartiennent à R et satisfont $F_{n-i}\rho_i \neq 0$ pour $0 \leqslant i \leqslant n$.

Prenons maintenant $i \leqslant n-1$, $f \in F_{n-1-i}$ et $g = a_1 \cdots a_i$ $f \in F_{n-1}$. D'après l'hypothèse $F_{n-1}\rho = 0$ on a:

$$0 = d\beta \cdot g\rho = (dg)\alpha = (d_i f)\alpha = d_i\beta \cdot f\rho_i.$$

On vient d'observer que $d_i\beta \neq 0$ et que, par conséquent, $f\rho_i = 0$. Comme ceci est vrai de tout mot f de F_{n-1-i}, on voit que $F_{n-1-i}\rho_i = 0$ ($0 \leqslant i \leqslant n-1$).

Comparant ces relations avec les relations établies plus haut on en conclût que les ρ_i forment un système de $n+1$ fonctions *distinctes* de R ce qui contredit le fait que Card $R = n$ et établit $F_n\rho = 0$, c'est-à-dire $\rho = 0$. □

2.3.1. *Soient $\rho, \rho' \in R_1$ et $b \in B^{(*)}$ tels que ρ' et $b[\rho]$ aient même restriction à F_{n-1}. On a $\rho = \rho'$.*

Preuve. En raison de $\rho \neq \mathbf{0}$ et de la remarque précédente on a $f\rho \neq 0$ pour au moins

un $f \in F_{n-1}$. Par conséquent $b = (f\rho')(f\rho)^{-1} \in B^{(*)}$ est déterminé par les restrictions de ρ et ρ' à F_{n-1}.

Procédant de la même façon que pour 2.2.0, nous supposons que $h\rho' \neq b \cdot (h\rho)$ pour un mot h de F_n. L'énoncé étant symétrique en ρ et ρ' (puisque $B^{(*)}$ est un groupe), on peut supposer $h\rho \neq 0$ et, par conséquent, $c = (h\rho')(h\rho)^{-1}$ est un élément bien défini de $B^{(*)} \cup 0$.

Soit $h = a_1 \cdots a_n$ $h_n = h_0$ comme dans la preuve précédente et, de même, $d = d_0 \in D_\rho \cap G_1$, $d' = d'_0 \in D_{\rho'} \cap G_1$, d_i; ρ_i; $d'_i = d'\ a_1 \cdots a_i$; $\rho'_i = \rho_{d'_i}$ $(0 \leqslant i \leqslant n)$; $\rho = \rho_0$; $\rho' = \rho'_0$. On a:

$$(dh)\alpha = d\beta \cdot h\rho = d_i\beta \cdot h_i\rho_i$$

$$(d'h)\alpha = d'\beta \cdot h\rho' = d'_i\beta \cdot h_i\rho'_i \qquad (0 \leqslant i \leqslant n),$$

où $d\beta, d'\beta \neq 0$ et $h\rho' = c \cdot (h\rho)$. La première série d'équations montre que les $d_i\beta$ sont différents de 0 et que les ρ_i sont dans R. La deuxième série mène à la même conclusion en ce qui concerne les $d'_i\beta$ et les ρ'_i quand $c \neq 0$, et l'on trouve alors que $h_i\rho'_i = y_i \cdot (h_i\rho_i)$ où y_i est l'élément de $B^{(*)}$ égal à $(d_i\beta)^{-1} \cdot (d'\beta) \cdot c \cdot (d\beta)^{-1} \cdot (d_i\beta)$ $(0 \leqslant i \leqslant n)$. Si au contraire $c = 0$, on a $(d'h)\alpha = 0$ donc $h_i\rho'_i = 0$ et on peut écrire la même relation en prenant tous les y_i égaux à 0 $(0 \leqslant i \leqslant n)$.

Soient maintenant $i \leqslant n-1$, $f \in F_{n-1-i}$, $g = a_1 \cdots a_i\ f \in F_{n-1}$ comme dans 2.2.0. On a:

$$(dg)\alpha = d\beta \cdot g\rho = d_i\beta \cdot f\rho_i,$$

$$(d'g)\alpha = d'\beta \cdot g\rho' = d'_i\beta \cdot f\rho'_i,$$

où ici $g\rho' = b \cdot (g\rho)$ avec $b \neq 0$.

Comme $d\beta, d'\beta \neq 0$ on a $f\rho'_i = 0$ ssi $f\rho_i = 0$. Par conséquent, quand $d'_i\beta \neq 0$, on peut écrire $f\rho'_i = x_i \cdot (f\rho_i)$ où x_i est l'élément de $B^{(*)}$ obtenu en substituant b à c dans l'expression de y_i. Si $d'_i\beta = 0$ on a $f\rho'_i = f\rho_i = 0$ et on peut prendre $x_i = 1$. Dans les deux cas x_i est indépendant du choix de f dans F_{n-1-i}.

On déduit de ce calcul que chaque paire (ρ_i, ρ'_i) appartient à la relation E_{n-1-i} pour $0 \leqslant i \leqslant n-1$ cependant que le calcul précédent avec le mot h avait montré que $(\rho_i, \rho'_i) \notin E_{n-i}$ pour les mêmes valeurs de l'indice i. De fait, dans le cas particulier où $c = 0$, on peut même être sur que $(\rho_n, \rho'_n) \notin E_0$ puisque $h_n\rho_n \neq 0 = h_n\rho'_n$.

Etant donnée la définition des équivalences E_{n-i} ceci montre que leurs restrictions E'_{n-i} à $\{\rho_i, \rho'_i\colon\ 0 \leqslant i \leqslant n\}$ forment une suite strictement croissante: $\emptyset \neq E'_n \not\subseteq E''_{n-1} \cdots \not\subseteq E'_1$ ce qui contredit Card $R \neq n$ quand $c \neq 0$ puisqu'alors toutes les fonctions ρ_i et ρ'_i sont dans R. Quand $c = 0$ ces fonctions sont dans $R \cup \mathbf{0}$ et on aboutit de la même manière à une contradiction puisque l'on a en plus l'inclusion stricte de E_1 dans E_0. Par conséquent, $\rho' = b[\rho]$ ce qui implique $\rho = \rho'$ d'après 2.2. □

On pourrait résumer les deux remarques qui précèdent par l'assertion unique:

2.3.2. *La restriction de* E_{n-1} *à* $R \cup \mathbf{0}$ *est l'identité.*

Nous introduisons désormais l'hypothèse supplèmentaire que $R_1 = R$. Elle est trivialement satisfaite quand $G = A^*$ puisque dans ce cas G_1 est lui aussi égal à A^*.

2.4. *Soient* $a \in A$ *et* $\rho \in R \cup \mathbf{0}$. *Il existe une et une seule fonction* σ *de* $R \in \mathbf{0}$, (*notée* $\rho \cdot a$) *pour lequel* $(D_\rho)_a \cap D_\sigma \neq \emptyset$. *On a* $\rho \cdot a = \mathbf{0}$ *pour* $\rho = \mathbf{0}$. *Quand* $\rho \cdot a \neq \mathbf{0}$, *il existe un mot* b *de* B^*, (*noté* $a\mu(\rho, \sigma)$), *tel que* $(ga)\beta = g\beta \cdot b$ *pour tout* $g \in D_\rho$ (*tel que* $ga \in G$).

Preuve. Puisque $R_1 = R$ on peut prendre un mot g dans $D_\rho \cap G_1$. Soit $\sigma = \rho_{ga}$. Pour chaque $f \in F_{n-1}$ on a:

$$(gaf)\alpha = g\beta \cdot (af)\rho = (ga)\beta \cdot f\sigma.$$

Par conséquent, quand $(aF_{n-1})\rho = 0$ on a $F_{n-1}\sigma = 0$, d'où l'on conclut $\sigma = \mathbf{0}$ *grâce à* 2.3.0 *et* $\sigma \in R_1 = R$.

Dans le cas contraire, $\rho \neq \mathbf{0}$, $g\beta \neq 0$ et, d'après 2.3.0, on peut trouver un $f \in F_{n-1}$ pour lequel $(af)\rho \neq 0$, ce qui entraîne $f\sigma \neq 0$ et permet de définir $b = (g\beta)^{-1}((ga)\beta) = ((af)\rho)(f\sigma)^{-1} \in B^{(*)}$. La première équation montre que b ne dépend pas du choix de f dans F_{n-1} et la seconde qu'il est aussi indépendant de choix de g dans $D_\rho \cap D_\sigma a^{-1}$ ($= \{g \in D_\rho : ga \in D_\sigma\}$). Prenons un autre mot g' dans D_ρ et soit $\sigma' = \rho_{g'a}$. On a de même $b' = ((af)\rho)(f\sigma')^{-1} \in B^{(*)}$ et par conséquent $f\sigma' = b'b^{-1}(f\sigma)$ pour chaque $f \in F_{n-1}$ d'où l'on conclut que $\sigma' = \sigma$ d'après 2.3.1. Ceci établit l'existence de l'application $(\rho, a) \to \rho \cdot a$ et le fait que $\mathbf{0} \cdot a = \mathbf{0}$. Il nous reste à vérifier que b est bien un mot de B^*.

Tous les termes de l'équation $g\beta \cdot (af)\rho = (ga)\beta \cdot f\sigma$ sont dans B^*. Il existe donc un mot c de B^* tel que l'une des alternatives suivantes soit réalisée:

$$\text{soit } g\beta = (ga)\beta \cdot c; \quad f\sigma = c((af)\rho) \quad \text{et } b = c^{-1},$$

$$\text{soit } (ga)\beta = g\beta \cdot c; \quad (af)\rho = c(f\sigma) \quad \text{et } b = c.$$

Dans la seconde on a directement $b \in B^*$. Dans la première c est un facteur droit de tous les mots de $D_\rho\beta$ puisque D_ρ a est contenu dans D_σ ainsi qu'on vient de le voir. En vertu de l'hypothèse de normalisation (Min) faite au début de la discussion on a alors $c = 1$ ce qui montre que $b \in B^*$ dans les deux cas. □

Nous soulignons une conséquence utile pour la suite:

2.4 bis. *Pour chaque fonction* ρ *de* R (*resp. de* $R \cup \mathbf{0}$), *l'ensemble* D_ρ *contient un mot de longueur au plus* $n - 1$ (*resp. au plus* n).

Preuve. On vient d'établir l'existence d'une application $(R \cup \mathbf{0}) \times A \to R \cup \mathbf{0}$

satisfaisant $\mathbf{0} \cdot a = \mathbf{0}$ $(a \in A)$. Elle s'étend à une action de A^* sur $R \cup \mathbf{0}$ et par définition chaque fonction ρ de $R \cup \mathbf{0}$ a la forme $\rho = \rho_1 \cdot a$ pour au moins un mot a de A^*. La remarque résulte alors immédiatement de ce aue $\mathrm{Card}(R) \leqslant n$. □

2.5. *Il existe un R-transducteur sous-séquentiel (μ, λ, v) tel que α soit la restriction à G de la fonction définie par celui-ci.*

Preuve. C'est une conséquence directe de l'énoncé précédent. A chaque lettre a de A on associe la $R \times R$ matrice $a\mu$ dont chaque entrée (ρ, σ) est égale à $a\mu(\rho, \sigma)$ ou à 0 selon que $\sigma = \rho \cdot a$ ou non $(\rho, \sigma \in R)$. Cette application s'étend à un morphisme monomial.

Pour chaque mot a de A^* on note $a\lambda$ le R-vecteur Ligne dont la coordonnée ρ est égale à $a\beta$ si $\rho = \rho_a$ et à 0 sinon $(\rho \in R)$ avec $a\lambda = 0$ quand $a\beta = 0$. Par induction sur la longueur de a on vérifie que $a\lambda = 1\lambda \cdot a\mu$ $(a \in G)$.

Enfin on définit le R-vecteur fv $(f \in F_0)$ par la condition que sa coordonnée ρ soit $f\rho$ $(\rho \in R)$. Par définition on a identiquement

$$(gf)\alpha = g\beta \cdot f\rho_g = g\lambda \cdot fv = 1\lambda \cdot g\mu \cdot fv \quad (g \in G, f \in F_0)$$

ce qui établit le résultat. □

Compte tenu de 2.1, on a donc comme corollaire immédiat la:

Propriété 1. Les fonctions sous-séquentielles de dimension au plus n sont les fonctions définies par les Q-transducteurs sous-séquentiels où $\mathrm{Card}(Q) \leqslant n$.

Nous concluons cette section par une dernière remarque. Dans la preuve de celle-ci, étant donnée une fonction α et une partie Y de A^* on note $Y\hat{\alpha}$ le plus long facteur gauche commun des mots de $Y\alpha$ avec la convention que $Y\hat{\alpha} = 0$ quand $Y\alpha = 0$.

2.6. *Deux fonctions sous-séquentielles de dimension $\leqslant n$ ayant même restriction à F_{2n} sont égales.*

Preuve. Posons $G_0 = A^* \setminus A^{n+1}A^*$ de telle sorte que $F_{2n} = G_0F_n$. Soit α (avec ρ, μ et c comme ci-dessus) une fonction sous-séquentielle de dimension $\leqslant n$. Nous rappelons tout d'abord que l'existence d'un morphisme monomial μ et le fait que $\mathrm{Card}\, R \leqslant n$ impliquent que chaque fonction $\rho \in R$ (resp. $\in R \cup \mathbf{0}$) ait la forme ρ_g pour au moins un mot g de longueur au plus $n-1$ (resp. au plus n), ainsi qu'on l'a vu en 2.4 bis. Nous observons aussi que d'après 2.1 la fonction v dans les R-vecteurs et, par conséquent, les fonctions ρ, peuvent être étendues à des fonctions de F_n même si la dimension minimale de α est strictement moindre que n.

Définissons pour chaque $g \in G_0$ une fonction σ_g de F_n par la condition que $f\sigma_g = 0$ ou $= ((gF_n)\hat{\alpha})^{-1}((gf)\alpha)$ selon que $(gF_n)\alpha = 0$ ou non $(f \in F_n)$. Il existe des mots b_g de B^* tels que $\rho_g = b_g[\sigma_g]\,(g \in G)$ et, posant $S = \{\sigma_g : g \in G_0\}\backslash 0$, on déduit de 2.2 et de la définition de l'équivalence E_n que celle-ci se réduit à l'identité sur $S \cup \mathbf{0}$. Il y a donc bijection entre R et S où, par construction ce dernier ensemble est complètement déterminé par la restriction de α à F_{2n}. Ceci permet de définir une application v' de F_n dans les R-vecteurs colonne par la condition que la valeur de la coordonnée ρ de fv' soit $f\sigma$ $(f \in F_n, \rho \in R)$ où $\sigma \in S \cup \mathbf{0}$ est la fonction correspondant à ρ. De fait $fv = \boldsymbol{b} \cdot fv'$ où $\boldsymbol{b}$ est la $R \times R$ matrice diagonale dont les entrées non nulles sont les mots b_g définis plus haut.

A chaque mot g de G_0 on associe aussi le R-vecteur ligne $g\lambda'$ égal à zéro si $(gF_n)\alpha = 0$ et dont, sinon, la seule coordonnée non nulle a pour indice ρ_g et est choisie de telle sorte que $g\lambda' \cdot fv' = (gf)\alpha$ $(f \in F_n)$. Ceci est possible (de façon unique) puisque de fait $g\lambda' = g\lambda \cdot \boldsymbol{b}^{-1}$.

Compte tenu de la remarque faite au début de la preuve et de la bijection entre R et S, on peut maintenant construire pour chaque lettre $a \in A$ une $R \times R$ matrice monomiale $a\mu'$ à entrées dans $B^{(*)} \cup 0$ unique qui satisfasse $(ga)\lambda' = g\lambda' \cdot a\mu'$ $(ga \in G_0)$. Par construction $a\mu' = \boldsymbol{b}^{-1}(a\mu)\boldsymbol{b}$ et l'on a donc $(af)\alpha = 1\lambda' \cdot a\mu' \cdot fv'$ pour tous les $f \in F_n$ et $a \in A^*$ ce qui achève de montrer que α est entièrement déterminée par sa restriction à F_{2n}. □

3. Connection avec les fonctions rationnelles et séquentielles

Dans toute cette section, nous supposons que les ensembles A et B sont finis.

Le premier énoncé de cette section peut être considéré comme l'application au cas particulier des fonctions sous-séquentielles d'une partie d'un théorème classique de Ginsburg et Rose [4].

La théorie de Eilenberg ([1], Chap. IX, 7), établit qu'une fonction rationnelle α est définie par un morphisme μ de A^* sur un monoïde de $Q \times Q$ matrices (Q, fini) à entrées dans $B^* \cup 0$, un Q-vecteur ligne 1λ et un Q-vecteur colonne v, ayant une coordonnée égale à 1 et les autres nulles, ces objects satisfaisant la condition que $a\alpha = 1\lambda \cdot a\mu \,.\, v \in B^* \cup 0$ pour chaque mot a de A^*. La même théorie permet de supposer que pour chaque $q \in Q$ il existe des mots $a \cdot a' \in A^*$ tels que les vecteurs $a\lambda = 1\lambda \cdot a\mu$ et $a'v = a\mu \cdot v$ aient leur coordonnée d'indice q non nulle. Soit $n = \mathrm{Card}\, Q = \dim(\alpha)$. On garde la notation $Y\,\hat{\alpha}$ introduite à la fin de la section précédente pour noter le plus long facteur gauche commun des note de $Y\alpha$. Comme d'usage $|b|$ désigne la longueur du mot b.

Propriété 2. Une condition nécessaire et suffisante pour qu'une fonction rationelle α de domaine A^kA^* soit sous-séquentielle est que pour chaque mot f de $F_n = A^kA^*\backslash A^{k+n+1}A^*$ $(n = \dim \alpha)$ on ait:

$$\mathrm{Sup}\{|(af)\alpha| - |(aF_n)\hat{\alpha}| : a \in A^*\} < \infty \tag{3}$$

où $(aF_n)\,\hat{\alpha}$ désigne le plus long facteur commun gauche des mots de la forme $(af)\alpha$ $(f \in F_n)$.

Preuve. Il est immédiat que la condition (3) est nécessaire. Pour établir qu'elle est suffisante on utilise les notations introduites ci-dessus pour décrire la fonction rationnelle α et pour tout mot a on désigne par $a\beta$ le plus long facteur gauche commun des coordonnées non nulles du vecteur $a\lambda = 1\lambda \cdot a\mu$. On note $a\lambda'$ le Q-vecteur $(a\beta)^{-1}[a\lambda]$ dont chaque coordonnée $a\lambda' q$ est égale à $(a\beta)^{-1}$. $a\lambda q$ $(q \in Q)$ en convenant que $a\beta$ et $a\lambda'$ sont nuls quand $a\lambda = 0$. Enfin π désigne l'extension naturelle aux vecteurs du morphisme envoyant B^* sur le monoïde trivial $\{1\}$ et P est l'ensemble des Q-vecteurs $\{a\lambda\pi : a \in A^*\}$.

Soit $p \in P \setminus 0$ tel que $p = a\lambda\pi$ pour une infinité de mots a. Comme Card $Q = n$ on peut trouver des mots a de longueur $\leqslant 2^n - 1$ et g de longueur $\leqslant 2^n$ tels que $a\lambda\pi = (ag)\lambda\pi = p$. On a donc $(ag^m)\lambda\pi = p$ pour tout $m \geqslant 0$.

Supposons que le vecteur $(ag)\lambda'$ ne soit pas égal à $a\lambda'$ à une permutation près de ses coordonnées. Comme $(ag)\lambda = a\lambda \cdot g\mu$, il existe une puissance $g' = h$ $(1 \leqslant v \leqslant n-1)$, deux indices distincts $q, q' \in Q$ et un mot $b \in B^* \setminus 1$ tels que $bm = (ah^m)$ $\lambda'_q = a\lambda'_q \cdot b_m$ et $b'_m = (ah^m)\lambda'_{q'}$ soient pour tout $m \geqslant 0$ deux mots différents de 0 n'ayant aucun facteur gauche commun non trivial. Utilisant de nouveau Card $Q = n$, on peut trouver $f, f' \in F_n$ tels que $(ah^m f)\alpha = b_m c$, $(ah^m f')\alpha = b'_m c'$ $(c, c' \in B^*)$ ce qui montre que la condition (3) est violée.

Supposons au contraire que les hypothèses précédentes ne sont satisfaites par aucun $p \in P \setminus 0$. Chaque mot a assez long admet un facteur gauche a' de longueur $\leqslant 2^n - 1$ pour lequel $a\lambda' = a'\lambda'$. Par conséquent $a\alpha = a\beta \cdot (a'\lambda' \cdot v) = a\beta \cdot 1\rho'_a$ où $1\rho'_a \in B^*$ ne dépend que de a'. L'ensemble $R \cup \mathbf{0} = \{1\rho'_a : a \in A^*\}$ est donc un système *fini* de fonctions de $F_0 = A^k$ pour $k = 0$ ce qui établit le résultat. □

On peut noter le contre-exemple suivant dans lequel $A = \{a_1, a_2\}$ et $B = \{b\}$. Soient ϕ_1 et ϕ_2 les morphismes de A^* dans B^* définis par:

$$a_1\phi_1 = a_2\phi_2 = 1; \quad a_2\phi_1 = a_1\phi_2 = b.$$

La fonction α envoyant chaque mot g de A^* sur $g\phi_2$ ou $g\phi_1$ selon que la longueur de g est paire ou impaire est rationnelle. Quelque soit n positif on a $(gF_n)\,\hat{\alpha} = b^m$ avec $m = \mathrm{Min}\{m_1, m_2\}$ où m_i est le nombre d'occurences de a_i dans g $(i = 1, 2)$. Par conséquent pour tout $a \in A$ on voit que $(gaF_n)\hat{\alpha} \in (gF_n)\hat{\alpha}(1 \cup b)$ bien que $\hat{\alpha}$ ne soit manifestement pas une fonction rationnelle.

Nous caractérisons maintenant les fonctions séquentielles généralisées parmi les fonctions sous-séquentielles. La condition (4) de l'énoncé ci-dessous signifie que α "préserve les segments initiaux" selon la terminologie classique et il s'agit donc encore d'une variante des théorèmes connus.

Propriété 3. Soit α une fonction sous-séquentielle de dimension au plus n telle que:

$$(fa)\alpha \in 0 \cup (fa)B^* \tag{4}$$

pour tout mot f de $F_{n-1} = A^k A^* \setminus A^{k+n} A^v$ et toute lettre a de A.

Il existe une fonction séquentielle généralisée ayant même restriction que α à $A^{k+1}A^*$.

Preuve. Utilisant les notations de la section précédente, nous vérifions d'abord l'existence d'une application $(\rho, f; a) \to a\tau_{\rho,f}$ de $(R \times F_0) \times A$ dans $B^* \cup 0$ telle que l'on ait:

$$(gfa)\alpha = (gf)\alpha \cdot a\tau_{\rho,f} \quad (a \in A;\ g \in D_\rho). \tag{4.1}$$

Pour cela nous utilisons l'application $(\rho, a) \to \rho \cdot a$ (de $(R \cup \mathbf{0}) \times A$ dans $R \cup \mathbf{0}$ construite dans 2.4 et le fait déjà observé que D_ρ contient toujours au moins un mot g de longueur $\leqslant n-1$ ($\rho \in R$)).

En vertu de l'hypothèse (4) on a dans (4.1) soit $(gfa)\alpha = 0$ soit $(gfa)\alpha = (gf)\alpha \cdot b$ avec $(gf)\alpha \neq 0$ et $b \in B^*$. On conviendra que $b = 0$ si $(gf)\alpha = 0$. Maintenant l'identité (1) montre que $(g'f)\alpha = g'\beta \cdot f\rho$ et $(g'fa)\alpha = g'\beta \cdot (fa)\rho$ quelque soit $g' \in D_\rho$. Donc $(fa)\rho = f\rho \cdot b$ et, identiquement, $(g'fa)\alpha = (g'f)\alpha \cdot b$ ($g' \in D_\rho$). On peut donc définir $a\tau_{\rho,f} = b$.

Soit maintenant Q l'ensemble des suites de $k+1$ fonctions de $R \cup \mathbf{0}$. Posons $q_1 = (0, 0, \ldots, \rho_1)$ et définissons une application $Q \times A \to Q$ par la condition que si $q = (\rho_{i_1}, \rho_{i_2}, \ldots, \rho_{i_{k+1}})$ et $a \in A$, $q \cdot a = (\rho_{i_2}, \rho_{i_3}, \ldots, \rho_{i_{k+1}}, \rho')$ avec $\rho' = \rho_{i_{k+1}} \cdot a$ dans la notation de 2.4 si $\rho' \neq \mathbf{0}$ et sinon $q \cdot a = (\mathbf{0}, \mathbf{0}, \ldots, \mathbf{0})$ $(= q_0)$.

Cette application s'étend à une action $Q \times A^* \to Q$. On pose $Q = \{q_1 \cdot a : a \in A^* \setminus A^k A^*\}$ et $Q'' = \{q_1 \cdot a : a \in A^k A^*\}$. Comme chaque $q \in Q'' \setminus q_0$ a toutes ses composantes différentes de $\mathbf{0}$ par construction on voit que les ensembles Q' et $Q'' \setminus q_0$ sont disjoints.

Pour terminer nous nous construisons une application τ de $Q \times A$ dans $B^* \cup 0$ (notée $a\tau_q$, $a \in A$, $q \in Q$) de la façon suivante:

D'abord $a\tau_q = 0$ si $q = q_0$ ou $q \notin Q' \cup Q''$ ($a \in A$). Si $q \in Q'' \setminus q_0$, on peut écrire $q = q_1 \cdot gf$ où $g \in A^*$ et $f \in A^k$ et on pose alors $a\tau_q = a\tau_{\rho,f}$ avec $\rho = \rho_g$. Si $q = q_1 \cdot g \in Q' \setminus q_0$, on pose $a\tau_q = (ga)\alpha$ ou $= 1$ selon que $ga \in A^k$ ou $\in A^* \setminus A^k A^*$.

La théorie des fonctions séquentielles généralisées montre que les deux applications $Q \times A \to Q$ et $\tau : Q \times A \to B^* \cup 0$ définissent une telle fonction σ. On vérifie facilement par induction sur la longueur du mot a que si k est positif on a $a\sigma = 1$ ou $a\sigma = a\alpha$ selon que $|a| < k$ ou $\geqslant k$ et que si k est nul, on a $a\sigma = a\alpha$ pour tout $a \in A\ A^*$. □

Références

[1] S. Eilenberg, *Automata, Languages and Machines* Vol. A (Academic Press, NY, 1975).
[2] C. Elgot and J.E. Mezei, On relations defined by generalized finite automata, *IBM. J. Res.* **9** (1965) 47–68.
[3] S. Ginsburg, *An Introduction to Mathematical Machine Theory* (Addison-Wesley, Reading, MA, 1962).
[4] S. Ginsburg and G.F. Rose, A characterisation of machine mappings, *Canad. J. Math.* **18** (1966) 381–388.
[5] J. Hartmanis and R.E. Stearns, *Algebraic Theory of Sequential Machines* (Prentice-Hall, Engelwood Cliffs, NJ, 1966).
[6] M. Minsky, *Computation Finite and Infinite Machines* (Prentice-Hall, Englewood Cliffs, NJ, 1967).
[7] M. Nivat, Transduction des languages de Aiousky, *Ann. Inst. Fourier* (*Grenoble*) **18** (1968).

61

Combinatoire et représentation
du groupe symétrique, Strasbourg, 1976

LA CORRESPONDANCE DE ROBINSON.

M.-P. Schützenberger

1. Introduction.

1.1. La correspondance R entre permutations et tableaux standards de Young introduite en 1938 par G. de B. Robinson [12] dans la théorie des représentations du groupe symétrique a été depuis étudiée en elle-même par divers auteurs qui lui ont découvert une série de propriétés combinatoires curieuses, ou utiles pour l'étude des fonctions symétriques. Dans le présent travail nous nous proposons de donner un exposé systématique des principaux résultats basé sur la théorie de C. Green ([5], [6], [7]) grâce à laquelle il devient possible de montrer que la correspondance R est naturelle sur l'ensemble de tous les tableaux gauches ("skew" de Young, appelés ici tableaux) muni d'une structure convenable.

J'ai utilisé de nombreuses idées de G. Thomas et de A. Lascoux pour simplifier ces preuves et organiser les énoncés de façon à réduire autant que j'ai pu la partie combinatoire.

La technique est la suivante. On considère le plan entier $\underset{\sim}{P} = Z \times Z$ muni de son ordre naturel $\leq((x,y) \leq (x',y')$ ssi $x \leq x'$ et $y \leq y')$ et on identifie chaque tableau (gauche, "skew") de Young à un morphisme (de structure d'ordre) bijectif d'un intervalle du plan sur une chaîne standard $[n] = \{1 < 2 < \ldots < n\}$. On associe une certaine relation d'ordre C_φ sur $[n]$ à chaque tableau φ d'image $[n]$ et pour $j \geq 0$, $k \geq 1$ on définit $L_j(\varphi; k)$ comme le maximum du nombre des éléments parmi les parties de $[n-j]$ qui sont unions de k C_φ-chaînes.

La fonction L induit une équivalence $\equiv$ sur l'ensemble des tableaux ($\varphi \equiv \psi$ ssi $L(\varphi) = L(\psi)$) dont chaque classe contient un et un seul élément qui soit un tableau standard c'est-à-dire dont la forme soit celle d'un diagramme de Ferrers : c'est la correspondance de Robinson et on peut caractériser les transformations entre tableaux (les "glissements") qui commutent avec $\equiv$.

La famille des tableaux peut être munie d'un produit associatif pour lequel $\equiv$ est une congruence. De ce point de vue les permutations peuvent être considérées comme des produits σ dont chaque terme a pour domaine un point. Il se trouve que les ordres C_σ et $C_{\sigma^{-1}}$ sont isomorphes et on en déduit aisément le théorème fondamental de G. de B. Robinson que la correspondance $\sigma \rightarrow (\sigma R, \sigma^{-1} R)$ est une bijection des permutations sur les paires de tableaux standards de même forme.

Cet énoncé fournit le substrat combinatoire aux résultats classiques connus sous le nom de "règle de Littlewood-Richardson" et "théorème d'Aitken". Le lien avec la théorie des fonctions de Schur s'effectue en vérifiant que les manipulations précédentes équivalent au calcul dans le quotient de l'anneau des polynômes en n variables x_i (non commutatives) par la congruence $x_i^2 \equiv 0$ $(i = 1, 2, \ldots, n)$.

Nous ferons référence aux travaux de G. Thomas ([18], [19]) qui montrent de façon plus précise, que le relèvement de la structure multilinéaire seule considérée ici peut être réalisé au moyen des opérateurs de Baxter introduits en algèbre par G.-C. Rota.

Une partie importante des propriétés que nous venons de résumer résulte de ce que la congrence $\equiv$ commute avec les involutions naturelles induite par la structure d'ordre sur le plan $\underset{\sim}{P}$. Pour profiter au maximum des simplifications que procurent ces opérations nous avons rassemblé dans la seconde partie de cette introduction l'ensemble des définitions et des notions géométriques, au demeurant parfaitement triviales, qui seront utilisées par la suite. Le chapitre 2 contient la définition des glissements. Le chapitre 3 montre d'après C. Green que ces opérations entre tableaux préservent la fonction L et qu'elles peuvent être obtenues en composant des transformations encore plus simples dues à D. E. Knuth [8]. La correspondance de Robinson est définie dans le même chapitre et le théorème fondamental sur les permutations est établi dans le chapitre 4. Le dernier chapitre établit la connexion avec les fonctions de Schur.

Les lecteurs de ce mémoire devront remercier le Professeur D. Foata qui a consacré beaucoup d'efforts à son amélioration et sans lequel je n'aurais pu le terminer.

1.2. NOTATIONS.

Intervalles. Dans tout ce travail nous désignerons par J la famille des parties finies F du plan entier $\underset{\sim}{P} = Z \times Z$ qui sont des intervalles par rapport à l'ordre naturel $\leq$ c'est-à-dire qui satisfont la condition

(1) $$p, p' \in F\ ,\quad p'' \in \underset{\sim}{P},\quad p \leq p'' \leq p' \Rightarrow p'' \in F\ .$$

Un interval F sera dit principal ($F \in \hat{J}$) ssi il possède un point minimum (par rapport à l'ordre naturel) unique c'est-à-dire ssi il a la forme d'un diagramme de Ferrers. Chaque intervalle F est contenu dans un plus petit intervalle principal $\hat{F}$ que l'on peut définir comme la plus petite partie F' du plan qui contienne F et qui soit telle que

(2) $$p, p' \in F' \Rightarrow \mathrm{Min}\ \{p,\ p'\} \in F'\ .$$

Il sera commode de désigner par $\hat{J}^1$ la sous-famille des intervalles F dont $(1, 1)$ est le point minimum de $\hat{F}$, c'est-à-dire de disposer d'une section de J par rapport aux translations.

Ordre croisé. Concurremment avec l'ordre naturel $\leq$, nous utiliserons un second ordre sur le plan $\underset{\sim}{P}$, dit ordre croisé dont le graphe $C \subset \underset{\sim}{P} \times \underset{\sim}{P}$ sera défini par l'identité :

(3) $\qquad ((x, y), (x', y')) \in C$ ssi $x \leq x'$ et $y \geq y'$.

Autrement dit, l'involution $(x, y) \to (x, -y)$ sur le plan établit un isomorphisme entre les ordres naturels et croisés. La transposition $p = (x, y) \to p^T = (y, x)$ est un anti-isomorphisme entre C et l'ordre opposé $\overline{C}$. Il en est de même de la symétrie par rapport à l'origine $p = (x, y) \to -p = (-x, -y)$ c'est-à-dire que pour toute paire (p, p') de points les relations :

(4) $\qquad (p, p') \in C$; $(p', p) \in \overline{C}$; $(p'^T, p^T) \in C$; $(-p', -p) \in C$; $(-p^T, -p'^T) \in C$;

sont équivalentes.

Nous dirons qu'une partition ordonnée $(F_1, F_2, \ldots, F_n)$ d'une partie F du plan est une C-partition ssi, d'une part deux points de F sont incomparables pour l'ordre naturel quand ils appartiennent à deux composantes distinctes et, d'autre part, $(p, q) \in C$ pour tout $p \in F_i, q \in F_j$ quand $i < j$. Par exemple la suite ordonnée des points $\{(n, 1)\}, \{(n-1, 2)\}, \ldots \{(n-i, i+1)\}, \ldots \{(1, n)\}$ forme une C-partition de leur union F.

On voit facilement qu'une condition nécessaire et suffisante pour que $(F_1, \ldots, F_r)$ soit une C-partition est qu'il existe des points (x_i, y_i) $(i = 2, \ldots, r)$ tels que pour chaque $j = 1, \ldots, r$ et $(x, y) \in F_j$ on ait :

$x \leq x_i$, $y \geq y_i$ si $j \leq i$ et $x_i < y$, $y_i > y$ si $j > i$.

Manifestement chaque composante F_i d'une C-partition d'un intervalle F est elle-même un intervalle.

Morphisme. Dans tout ce travail un morphisme sera une application partielle φ du plan P dans une chaîne dont la restriction à son domaine est un morphisme de structure d'ordre, c'est-à-dire qui est telle que $p\varphi \leq p'\varphi$ pour toute paire ordonnée $p \leq p'$ de points de son domaine. Pour l'essentiel nous n'aurons à faire qu'à une famille plus restreinte, à savoir la famille $\mathcal{M}$ des morphismes qui satisfont les deux conditions supplémentaires suivantes :

(1) leur domaine F est un intervalle fini du plan ;
(2) leur restriction à celui-ci est une bijection sur leur image A .

Si besoin est, on précisera le domaine ou l'image par des écritures telles que $\mathcal{M}_A$, $\mathcal{M}(F)$ ou $\mathcal{M}_A(F)$.

Comme les morphismes de $\mathcal{M}$ sont des bijections, il n'y aura pas d'inconvénient à désigner par la même notation $\varphi|F'$ ou $\varphi|A'$ leur restriction à une partie F' de leur domaine ou A' de leur image.

Nous ferons un usage constant de la remarque triviale que si le domaine F d'un morphisme φ (non nécessairement bijectif) est un intervalle (resp. un intervalle principal) et si B est un intervalle (resp. un intervalle initial) de son image, le domaine de la restriction $\varphi|B$ est encore un intervalle (resp. un intervalle principal).

Nous supposerons en général que la chaîne $A = \{a_1 < a_2 \cdots < a_n\}$ est fixée. Ses éléments seront appelés pièces. Enfin on notera $a \to -a$ l'anti-isomorphisme de A sur la chaîne opposée $-A = \{-a_n < \cdots < -a_2 < -a_1\}$.

La transposition et la symétrie par rapport à l'origine permettent d'associer à chaque application $\varphi : F \to A$ trois autres applications $\varphi^T : F^T \to A$, $\bar{\varphi} : -F \to -A$ et $\overline{\varphi^T} = \varphi^{-T} : -F^T \to -A$ en posant

(5) $$p^T\varphi^T = p\varphi \; ; \; (-p)\bar{\varphi} = -(p\varphi) \quad \text{et} \quad (-p^T)\varphi^{-T} = -(p\varphi)$$

pour chaque point p de F.

Il est clair que ces opérations sont des involutions sur $\mathcal{M}$ et que si φ est principal (c'est-à-dire si son domaine est principal) il en est de même de son transposé φ^T.

DEFINITION. Etant donnée une bijection $\varphi : F \to A$, la relation d'ordre C_φ sur A est définie par la condition que pour toute paire de pièces a, b de A on ait :

(6) $$(a, b) \in C_\varphi \text{ ssi } a \leq b \text{ et } (a\varphi^{-1}, b\varphi^{-1}) \in C .$$

On définit de même $\bar{C}_\varphi$ en remplaçant C par l'ordre opposé $\bar{C}$.

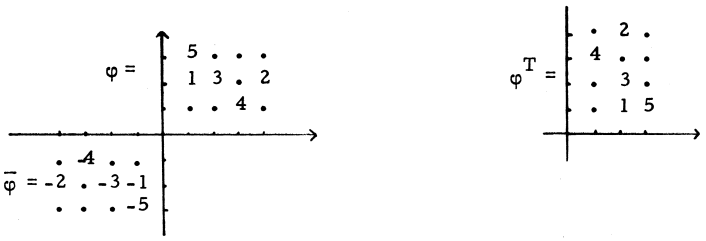
En raison de son importance pour la suite nous isolons la remarque suivante :

1.1. <u>On a $\bar{C}_\varphi = C_{\varphi T}$ et la bijection $a \to -a$ de A sur $-A$ établit un anti-isomorphisme entre les ordres C_φ sur A et $C_{\bar{\varphi}}$ sur $-A$.</u>

<u>Preuve.</u> L'isomorphisme entre $\bar{C}_\varphi$ et C_{φ^T} résulte de ce que $(p, q) \in \bar{C}$ équivaut à $(q^T, p^T) \in C$. L'anti-isomorphisme entre C_φ et $\bar{C}_{\bar{\varphi}}$, de ce que si $a\varphi^{-1} = p$ et, $b\varphi^{-1} = q$, la double condition $a \leq b$, $(p, q) \in C$ équivaut à $-b \leq -a$, $(-q, -p) \in C$.

Q. E. D.

L'exemple suivant peut aider le lecteur à visualiser ces notations. (Conformément à l'usage courant dans le reste des mathématiques les coordonnées X (resp. Y) vont en croissant de gauche à droite (resp. de bas en haut)). La bijection φ n'est pas un morphisme (à cause de la paire (3, 2)) et son domaine n'est pas un intervalle.



On a :

$$C_{\varphi} = \{(1, 2), (1, 3), (1, 4), (3, 4)\} ;$$
$$\bar{C}_{\varphi} = C_{\varphi^T} = \{(1, 5), (2, 3), (2, 5), (3, 5), (4, 5)\} ;$$
$$C_{\bar{\varphi}} = \{(-2, -1), (3, -1), (-4, -1), (-4, -3)\} ;$$
$$C_{\bar{\varphi}^T} = \{(-5, -1), (-3, -2), (-5, -3), (-5, -4)\} .$$

Par contre la bijection

$$\psi = \begin{matrix} 2 & 5 & . & . \\ . & 1 & 4 & . \\ . & . & . & 3 \end{matrix}$$

est un morphisme dont le domaine est un intervalle qui, d'ailleurs, admet la C-partition (F_1, F_2) où F_1 a la forme $\begin{matrix} * & * & . \\ . & * & * \end{matrix}$ et où F_2 est réduit au point portant la pièce 3 . On a

$$C_{\psi} = \{(1, 3), (1, 4), (2, 3), (2, 4), (2, 5)\} .$$

Produit. Deux applications $\psi : F \to A$ et $\psi' : F' \to A$ ne diffèrent que par une translation ssi leurs domaines F et F' ont le même nombre de points et s'il existe $(u, v) \in Z \times Z$ tel que $(x+u, y+v)\psi' = (x, y)\psi$ pour chaque point (x, y) de F.

Considérons maintenant une suite $(\varphi_1, \ldots, \varphi_r)$ de morphismes $\varphi_i \in \mathcal{M}_{A_i}(F_i)$. Nous écrirons $\varphi_1\varphi_2 \ldots \varphi_r = 0$ quand les A_i ne forment pas une partition de leur union B. Dans le cas contraire nous dirons qu'une application $\varphi : F \to B$ est un produit des φ_i (et nous écrirons $\varphi \in \varphi_1\varphi_2 \ldots \varphi_r$) ssi F admet une C-partition $(F'_1, \ldots, F'_r)$ telle que chaque restriction $\varphi'_i = \varphi \mid F'_i$ ne diffère de φ_i que par une translation $(i = 1, 2, \ldots, r)$.

Pour illustrer ceci considérons par exemple les trois morphismes principaux $\varphi_1 = \begin{matrix}3\\1\end{matrix}$; $\varphi_2 = 5$; $\varphi_3 = 34$. Un produit $\varphi \in \varphi_1\varphi_2\varphi_3$ serait par exemple :

$$\varphi = \begin{matrix} 3 & . & . & . \\ 1 & . & . & . \\ . & 5 & . & . \\ . & . & 3 & 4 \end{matrix} \qquad \text{ou aussi bien} \qquad \varphi' = \begin{matrix} 3 & . & . & . & . \\ 1 & . & . & . & . \\ . & 5 & . & . & . \\ . & . & . & 3 & 4 \end{matrix}$$

Soit F le domaine d'un produit $\varphi \in \varphi_1 \ldots \varphi_r$ où chaque φ_i appartient à $\mathcal{M}$. Par hypothèse F est un intervalle, φ est bijectif et enfin φ est un morphisme puisque deux points de F sont incomparables pour l'ordre naturel quand ils appartiennent à deux composantes distinctes. Donc $\varphi \in \mathcal{M}$.

Posant $0\psi = \psi 0 = 00 = 0$, $(\psi \in \mathcal{M})$ il en résulte immédiatement que la notion de produit que nous venons de définir munit $\mathcal{M} \cup \{0\}$ d'une structure de semigroupe. De fait, c'est même une structure de monoïde puisque $\mathcal{M}$ contient le morphisme de domaine vide (à ne pas confondre avec le zéro 0) qui est élément neutre du produit.

Il est clair que les relations $\varphi \in \varphi_1\varphi_2$; $\varphi^T \in \varphi_2^T\varphi_1^T$; $\bar{\varphi} \in \bar{\varphi}_2\bar{\varphi}_1$; $\bar{\varphi}^T \in \bar{\varphi}_1^T\bar{\varphi}_2^T$ sont identiquement équivalentes. Nous soulignons la remarque suivante :

1.2. Soit $\varphi \in \varphi_1 \cdots \varphi_r$ un produit. L'ordre C_φ ne dépend que de la suite $(C_{\varphi_1}, \ldots, C_{\varphi_r})$ des ordres associés à ses facteurs.

Preuve. Comme chaque point du domaine de φ_i est en relation C avec tous les points de celui de φ_j pour $i < j$, le graphe C_φ est l'union des graphes C_{φ_i} et des paires (a_i, a_j) où a_i (resp. a_j) appartient à l'image de φ_i (resp. de φ_j) et $i < j$ $(i, j = 1, 2, \ldots, r)$.

Q.E.D.

Permutations. Une bijection σ d'image A sera dite une permutation de A $(\sigma \in S_A^1)$ ssi son domaine est constitué des points $(n+1-i, i)$ $(1 \leq i \leq n = \text{Card } A)$, ce qui entraîne qu'il soit un intervalle et que $\sigma \in \mathcal{M}$; nous la représenterons le plus souvent par la suite $(1\sigma)(2\sigma)\ldots(n\sigma)$ des pièces de A lues dans l'ordre C.

L'énoncé suivant sera utilisé plusieurs fois par la suite.

1.3. A chaque morphisme bijectif φ d'image A correspond une et une seule permutation $\sigma = \sigma(\varphi)$ telle que $C_\sigma = C_\varphi$. Une condition suffisante pour qu'un autre morphisme bijectif ψ de même image A satisfasse $C_\varphi = C_\psi$ est que chaque pièce de A se trouve dans la même ligne dans φ et dans ψ.

Preuve. Nous définissons un ordre total C^L contenant l'ordre croisé C par l'identité :

$$((x, y), (x', y')) \in C^L \quad \text{ssi} \quad (x \leq x' \text{ et } y = y') \text{ ou } (y > y')$$

et à chaque morphisme bijectif φ d'image A nous associons l'ordre C_φ^L contenant C_φ par la condition que $(a, b) \in C_\varphi^L$ ssi $a \leq b$ et $(a\varphi^{-1}, b\varphi^{-1}) \in C^L$.

Puisque C^L est un ordre total il correspond à φ une et une seule permutation $\sigma = \sigma(\varphi)$ de S_A^1 pour laquelle $C_\varphi^L = C_\sigma^L$, à savoir celle représentée par la suite $s_k s_{k-1} \cdots s_1$ où chaque s_i est la suite des pièces (lues dans l'ordre naturel) sur la ligne y_i de φ et où $y_k > y_{k-1} \cdots > y_1$. Par conséquent $\sigma(\varphi) = \sigma(\psi)$ dans les conditions de l'énoncé. De plus $C_\sigma^L = C_\sigma$ puisque les deux ordres C^L et C coïncident sur le domaine de toute permutation.

Supposons $(a, b) \in C_\varphi^L \backslash C_\varphi$. On a $a \leq b$ et les points $p = (x, y) = a\varphi^{-1}$ et $p' = (x', y') = b\varphi^{-1}$ sont tels que d'une part $x \leq x'$ et $y = y'$ ou $y > y'$ et d'autre part on n'ait pas $x \leq y'$ et $y \geq y'$. On a donc $x > x'$ et $y \geq y'$, c'est-à-dire $b\varphi = (x', y') < a\varphi = (x, y)$ ce qui montre que φ n'est pas un morphisme.

Par conséquent sous l'hypothèse contraire, on a $C_\varphi = C_\varphi^L$ (puisque $C_\varphi \subset C_\varphi^L$ par construction) ce qui achève la preuve.

Q. E. D.

Pour des raisons évidentes on peut appeler <u>connexe</u> toute partie du plan qui n'admet pas de C-partition non triviale. Nous laissons au lecteur de vérifier l'observation (que nous n'utiliserons pas) qu'à chaque morphisme $\varphi \in \mathcal{M}$ correspond un morphisme ψ de $\mathcal{M}$, unique à une translation près dans le plan, dont le domaine est connexe et pour lequel $C_\varphi = C_\psi$ et $C_{\varphi^T} = C_{\psi^T}$.

2. Les Glissements.

Disons qu'une partie F et un point p du plan sont un quasi-intervalle et un complément de celui-ci si $F \cup p$ est un intervalle et $p \notin F$, ce qui n'exclut pas la possibilité que F soit déjà lui-même un intervalle.

Soient maintenant $\varphi \in \mathcal{M}$ un morphisme bijectif sur A dont le domaine est l'intervalle F et $p = (x, y)$ un complément de F tel que F contienne au moins un des deux points $p^X = (x+1, y)$, $p^Y = (x, y+1)$. Nous construisons une suite $(\varphi_0, p_0) = (\varphi, p), \ldots, (\varphi_k, p_k)$ de paires dans lesquelles chaque φ_i est une bijection sur A dont le domaine F_i est un quasi-intervalle de complément p_i par les trois conditions suivantes :

(1) k est le premier indice pour lequel $F_i \cap \{p_i^X, p_i^Y\} = \emptyset$;

(2) Pour chaque $i = 0, 1, \ldots, k-1$ on a : $F_{i+1} = (F_i \backslash p_{i+1}) \cup p_i$ où $p_{i+1} \in \{p_i^X, p_i^Y\}$ est défini par la condition que $p_{i+1}\varphi_i = \mathrm{Min}\{p_i^X\varphi_i, p_i^Y\varphi_i\}$;

(3) $p_i\varphi_{i+1} = p_{i+1}\varphi_i$ et $p'\varphi_{i+1} = p'\varphi_i$ pour tous les autres points p'.

Autrement dit, φ_{i+1} se déduit de φ_i en amenant au point p_i la plus petite des pièces $p_i^X\varphi_i$ et $p_i^Y\varphi_i$ si F_i contient les deux points p_i^X et p_i^Y et sinon la seule de ces pièces qui existe. Comme les points p_i forment une suite strictement croissante, le processus s'arrête puisqu'il finit par donner un point p_k qui se trouve être un point maximal du domaine F_k.

Nous poserons $\varphi_k = \varphi\Gamma_p$ (ou pour préciser s'il le faut $(\varphi_k, p_k) = \varphi\Gamma_p$) et nous appelerons φ_k le glissement de φ de sommet p.

L'exemple suivant où $k = 3$, $q = p_k$ illustre cette construction :

$$\varphi = \begin{matrix} 1\ 5\ 8\ . \\ .\ 3\ 4\ 7 \\ .\ p\ 2\ 6 \end{matrix} \quad ; \quad \varphi_1 = \begin{matrix} 1\ 5\ 8\ . \\ .\ 3\ 4\ 7 \\ .\ 2\ p_1\ 6 \end{matrix} \quad ; \quad \varphi_2 = \begin{matrix} 1\ 5\ 8\ . \\ .\ 3\ p_2\ 7 \\ .\ 2\ 4\ 6 \end{matrix} \quad ; \quad \varphi_3 = \begin{matrix} 1\ 5\ 8\ . \\ .\ 3\ 7\ p_3 = 9 \\ .\ 2\ 4\ 6 \end{matrix}$$

Nous rassemblons en un seul énoncé les propriétés des glissements qui nous serviront par la suite en posant $\psi = \varphi_k$, $q = p_k$. Les opérations $\varphi \to \varphi^T$ ou $\bar{\varphi}$ sont celles définies dans la section précédente et pour chaque point $q = (x, y)$ on note $q^{-X} = (x-1, y)$; $q^{-Y} = (x, y-1)$.

2.1. On a les propriétés suivantes :

(1) Chaque φ_i est un morphisme bijectif et $a\varphi_i^{-1} \leq a\varphi^{-1}$ pour chaque a de A ;

(2) Le domaine G de ψ est un intervalle tel que $G \cup q = F \cup p$ et $G \cap \{q^{-X}, q^{-Y}\} \neq \emptyset$;

(3) $\psi^T = \varphi^T \Gamma_{p^T}$;

(4) $\bar{\psi} \Gamma_{-q}$ est défini et est égal à $(\bar{\varphi}, -p)$;

(5) Si B est un intervalle de A et $\psi \mid B \neq \varphi \mid B$ il existe un point p' pour lequel $\psi \mid B = (\varphi \mid B)\Gamma_{p'}$.

Preuve. Par hypothèse $\varphi_0 = \varphi$ est un morphisme et on peut donc procéder par induction sur i. Par construction φ_{i+1} satisfait identiquement $a\varphi_{i+1}^{-1} \leq a\varphi_i^{-1}$ ($a \in A$) avec égalité pour toutes les pièces sauf une, qui passe du point p_{i+1} au point $p_i < p_{i+1}$ et qui, d'après l'hypothèse que φ_i est un morphisme peut être définie par la condition d'être la pièce minimum de l'ensemble $\{p'\varphi_i : p_i \leq p'\}$. Ceci suffit pour vérifier que φ_{i+1} est un morphisme.

(2) En effet, par construction tous les $F_i \cup p_i$ sont égaux à l'intervalle initial $F \cup p$ et le point $q = p_k$ est un point maximal propre de celui-ci.

(3) Immédiat.

(4) On a $F_k \cap \{p_k^{-X}, p_k^{-Y}\} \neq \emptyset$, ce qui équivaut à $-G \cup \{(-q)^X, (-q)^Y\} \neq \emptyset$ où $-G \cup -q$ est un intervalle. L'énoncé équivaut donc à l'assertion que pour chaque $i = k, k-1, \ldots, 0$ la donnée de φ_i et du point $p_i = (x, y)$ détermine le point

p_{i-1} par la condition duale que $p_{i-1}\varphi_i = \text{Max}\{p_i^{-X}\varphi_i , p_i^{-Y}\varphi_i\}$. Or ceci est clair car si $p_{i-1} = p_i^{-X} = (x-1, y)$ (resp. $= p_i^{-Y}$) on a $p_{i-1}\varphi_i = p_i\varphi_{i-1} \geq (x, y-1)\varphi_{i-1}$ (resp. $\geq p_i^{-X}\varphi_{i-1}$) puisque φ_{i-1} est un morphisme.

(5) Comme $\varphi \mid B \in \mathcal{M}$ ceci résulte immédiatement du caractère local de la construction.

Q. E. D.

D'après (4) , la paire finale (ψ, q) $(= (\varphi_k, p_k))$ détermine de façon unique la paire initiale (φ, p) que nous appelerons le glissement inverse $\varphi = \psi \bar{\Gamma}_q$ de sommet q de ψ . Les glissements et les glissements inverses constituent donc une famille de bijections sur l'ensemble $\mathcal{M}_A$ contenant l'inverse de chacun de ses membres [15] .

La semi-orbite $\varphi\Gamma^*$ d'un morphisme φ sera définie comme le plus petit ensemble fermé par glissement qui le contienne ; son orbite sera la plus petite union de semi-orbites fermée par glissements inverses qui contienne $\varphi\Gamma^*$.

Disons pour abréger que φ est un morphisme principal de point minimum (x, y) ssi son domaine est un intervalle principal ayant cette propriété (cf. Introduction).

2.2. Chaque semi-orbite $\varphi\Gamma^*$ contient un morphisme principal de point minimum (x, y) pour tous $x, y \in Z$ assez petits.

Preuve. Soient F le domaine de φ et $\hat{F}$ le plus petit intervalle principal contenant F . Si F lui-même n'est pas principal, $\hat{F}\backslash F$ contient au moins un point maximal. On vérifie facilement que $p \cup F$ est un intervalle et que si G est le domaine du glissement $\varphi\Gamma_{p'}$, l'ensemble $\hat{G}\backslash G$ est contenu dans $\hat{F}\backslash(F \cup p)$. Donc, par induction sur Card $\hat{F}\backslash F$, la semi-orbite de φ contient un morphisme principal ψ dont le point minimum (x, y) est contenu dans $\hat{F}$.

Pour achever la preuve il suffit de montrer que la semi-orbite de ψ

contient des morphismes principaux de point minimum (x-1, y) et (x, y-1). En raison de la symétrie par rapport à la transposition, il suffit de vérifier ceci pour (x-1, y). Soit H le domaine de ψ. Il contient un point maximum de la forme (x, y') avec $y' \geq y$. L'union de H et du point p' = (x-1, y') est un intervalle. Appliquant la construction précédente au glissement $\psi = \psi\Gamma_{p'}$, on obtient un morphisme principal de point minimum (x-1, y) appartenant à la semi-orbite de ψ', donc de φ.

Q. E. D.

Soient $a < b < c$ trois pièces et $\varphi_1 = \begin{matrix} b & c \\ . & a \end{matrix}$. Le glissement de sommet (1, 1) fait passer du morphisme φ_1 au morphisme $\varphi_1 K = \begin{matrix} b & . \\ a & c \end{matrix}$ et du morphisme $\varphi_2 = \begin{matrix} a & c \\ . & b \end{matrix}$ au morphisme $\varphi_2 K = \begin{matrix} c & . \\ a & b \end{matrix}$. Nous appellerons φ_1 et φ_2 tableaux élémentaires et l'opération $\varphi_i \to \varphi_i K$ transformation (élémentaire) de Knuth. Cet auteur a montré que ces transformations et leurs inverses engendrent pour l'essentiel toutes les opérations entre tableaux qui nous intéressent. Nous nous proposons de donner une forme un peu plus stricte de ce résultat (en évitant les inverses). Plus précisément, nous appellerons semi-orbite de Knuth χK^* d'un morphisme χ le plus petit ensemble de morphismes X contenant χ qui satisfasse les deux conditions suivantes :

(1) $\varphi \in X$, $C_\varphi = C_\psi \Rightarrow \psi \in X$;

(2) Si $\varphi \in X$ est un produit de la forme $\varphi'\varphi_i\varphi''$ où φ_i est un des deux morphismes φ_1 ou φ_2 ci-dessus on a $\varphi'(\varphi_i K)\varphi'' \in X$.

Rappelons la notation $\sigma(\varphi)$ pour désigner la permutation associée à un morphisme φ ainsi qu'il a été expliqué dans l'énoncé 1.3. La permutation $\sigma(\varphi_1)$ (resp. $\sigma(\varphi_2)$) est bca (resp. acb) et $\sigma(\varphi_1 K)$ = bac (resp. $\sigma(\varphi_2 K)$ = cab).

Il est immédiat que la semi-orbite χK^* est caractérisée par la condition que $\varphi \in \chi K^*$ implique $\psi \in \chi K^*$ quand il existe deux permutations σ' et σ'' et

trois pièces $a < b < c$ telles que

(3) Soit $\sigma(\varphi) = \sigma' bca\sigma''$ et $\sigma(\psi) = \sigma' bac\sigma''$;
Soit $\sigma(\varphi) = \sigma' acb\sigma''$ et $\sigma(\psi) = \sigma' cab\sigma''$.

D'après la définition de χK^* chaque morphisme de cette semi-orbite peut être obtenu par une suite de glissements à partir de χ . Il est un peu plus difficile de vérifier le théorème de Knuth qui affirme la réciproque de cette propriété. Nous commençons par examiner en détail le cas où χ est un produit $(\lambda)(b)$ où λ est un morphisme dont le domaine est une ligne, $\lambda = b_1 b_2 \dots b_m$ $(b_1, \dots, b_m \in A)$ et où b est une pièce unique.

Si $b_m < b$ le morphisme φ formé de la ligne $b_1 \dots b_m b$ peut être obtenu par glissement à partir de χ et il appartient à χK^* puisque φ et χ correspondent à la même permutation $b_1 \dots b_m b$.

Supposons donc $b_m > b$. Soit b_r la plus petite des pièces de l'image de λ qui soit plus grande que b .

2.3. Le produit $\varphi = (b_r)(\lambda')$ où λ' est le morphisme obtenu en remplaçant b_r par b dans λ appartient à χK^* et peut être obtenu par glissements à partir de χ .

Preuve. On peut supposer que dans χ chaque b_i se trouve au point $(i, 1)$ $(1 \le i \le m)$ et b au point $(m+1, 0)$. On passe par glissement au morphisme φ_m qui ne diffère de χ que par le fait que b se trouve au point $(m, 0)$. Définissons $\varphi_i = \varphi_{i+1} \Gamma_{(i,1)}$ $(i = m-1, \dots, 1)$. Chaque glissement $\varphi_{i+1} \to \varphi_i$ consiste quand $i > r$ (resp. $i \le r$) à déplacer b (resp. b_r) d'un pas vers la gauche et à abaisser la pièce b_{i+1} (resp. b_i) . Chacun d'eux est une opération K ce qui établit le résultat puisque $\varphi_1 = \varphi$ a bien la forme indiquée.

Q. E. D.

EXEMPLE. Soient $\lambda = 1\ 2\ 3\ 5\ 6$; $b = 4$. On a $b_r = 5$ et

$$\varphi_5 = \begin{matrix} 1 & 2 & 3 & 5 & 6 \\ . & . & . & . & 4 \end{matrix} \quad ; \quad \varphi_4 = \begin{matrix} 1 & 2 & 3 & 5 & . \\ . & . & . & 4 & 6 \end{matrix} \quad ; \quad \varphi_3 = \begin{matrix} 1 & 2 & 5 & . & . \\ . & . & 3 & 4 & 6 \end{matrix} \quad ;$$

$$\varphi_2 = \begin{matrix} 1 & 5 & . & . & . \\ 1 & 2 & 3 & 4 & 6 \end{matrix} \quad ; \quad \varphi_1 = \begin{matrix} 5 & . & . & . & . \\ 1 & 2 & 3 & 4 & 6 \end{matrix} \quad .$$

Nous considérons maintenant un cas plus compliqué. Soient φ_i et φ_{i+1} deux des morphismes consécutifs construits dans un glissement et supposons que l'on se trouve dans le cas où φ_{i+1} diffère de φ_i par le déplacement de la pièce c du point (x, y) au point adjacent en dessous (x, y-1) . On peut représenter la ligne y de φ_i par un produit $s_3 c s_4$ où s_3 et s_4 sont des suites croissantes de pièces ; de la même manière la ligne y-1 de φ_{i+1} peut être notée $s_1 c s_2$. Par hypothèse, les longueurs de ces suites satisfont $|s_1| \leq |s_3|$; $|s_2| \geq |s_4|$. De plus si $s_2 = a_1 a_2 \ldots a_m$ et $s_4 = b_1 \ldots b_p$ où les a_j, b_j sont des pièces, on a par hypothèse $c < a_1$ et $a_i < b_i$ pour $i = 1, 2, \ldots, p \leq m$; des relations similaires valent pour s_1 et s_3 . Un exemple avec $c = 6$ est fourni par $s_1 = 1\ 3$; $s_2 = 7\ 8$; $s_3 = 2\ 4\ 5$; $s_4 = 9$ ce qui correspond aux lignes y et y-1 de φ_i et de φ_{i+1} représentées par

$$\begin{matrix} 2 & 4 & 5 & 6 & 9 & . \\ . & 1 & 3 & \times & 7 & 8 \end{matrix} \qquad \text{et} \qquad \begin{matrix} 2 & 4 & 5 & \times & 9 & . \\ & 1 & 3 & 6 & 7 & 8 \end{matrix}$$

2.3. bis <u>On a</u> $\psi \in \varphi K^*$ <u>où</u> φ <u>est le produit des deux lignes</u> $s_3 c s_4$ <u>et</u> $s_1 s_2$, <u>et</u> ψ <u>celui des deux lignes</u> $s_3 s_4$ et $s_1 c s_2$.

<u>Preuve</u>. Par induction sur le nombre des pièces, le cas initial étant trivial. Si $|s_3| > |s_1|$ on peut écrire $s_3 = s'_3 s''_3$ où $|s''_3| = |s_1|$ et l'on voit que φ et ψ sont les produits de s'_3 par φ' et par ψ' obtenus en remplaçant s_3 par s''_3 . Le résultat découle alors de l'hypothèse d'induction sauf si $|s'_3| = 0$, c'est-à-dire sauf si $|s_1| = |s_3|$ comme nous le supposons désormais. On distingue deux cas :

(1) $|s_1| = |s_3| = 0$

Soient $s_2 = a_1 \dots a_m$ et $s_4 = b_1 \dots b_p$ comme ci-dessus. On peut considérer φ comme le produit de cs_4 par les singolets $a_1, a_2, \dots, a_m$, ce que nous écrirons

$$\varphi = (c\, s_4)(a_1)(a_2) \dots (a_m) .$$

D'après $c < a_1 < b_1$ et 2.3, on voit que la semi-orbite de Knuth du produit $(c\, s_4)(a_1)$ contient le morphisme $\varphi_1 = \begin{matrix} b_1 \cdot \cdot \cdot \cdot \cdot \cdot \\ ca_1 b_2 \cdot \cdot \cdot \cdot \cdot b_p \end{matrix}$. Donc $\varphi_1 \in \varphi K^*$ où

$$\varphi_1 = (b_1)(ca_1 b_2 \dots b_p)(a_2) \dots (a_m) .$$

On obtient de même $\varphi_2 \in \varphi_1 K^* \subset \varphi K^*$ où :

$$\varphi_2 = (b_1)(b_2)(ca_1 a_2 b_3 \dots b_p)(a_3) \dots (a_m)$$

et où on peut aussi bien écrire $(b_1 b_2)$ que $(b_1)(b_2)$. Répétant la même opération on obtient enfin $\varphi_m \in \varphi K^*$ où :

$$\varphi_m = (b_1 \dots b_m)(c_1 a_1 \dots a_m b_{m+1} \dots a_p) = \psi .$$

Ce qui achève la vérification dans ce cas.

(2) $|s_1| = |s_3| \geq 1$

On peut poser $s_1 = as'_1$ et $s_3 = b s'_3$ où $a < b$ sont deux pièces. Considérant φ comme le produit $(b\, s'_3\, c\, s_4)(a)(s'_1 s_2)$ et appliquant 2.3 aux deux premiers facteurs, on trouve que φK^* contient le produit $(b)(a\, s'_3\, c\, s_4)(s'_1\, s_2)$. Donc, appliquant l'hypothèse d'induction aux deux derniers facteurs de ce produit, on obtient que φK^* contient le produit $(b)(a\, s'_3\, s_4)(s'_1\, c\, s_2) = \varphi'$. Maintenant comme a est la plus petite de toutes les pièces, le morphisme formé par les deux dernières lignes de φ' a la forme $(\bar{c}\,\bar{s}_3)\bar{s}_2$ avec $\bar{c} = a$ $\bar{s}_3 = s'_3 s_4$ et $\bar{s}_2 = s'_1 c\, s_2$. On

peut donc lui appliquer la même opération que dans le cas 1 ci-dessus. On trouve que le produit de b, $\bar{s}_3$ et $\bar{c}\, s_2$ est dans $\varphi' K^*$, donc dans φK^*, c'est-à-dire que l'on a :

$$\varphi'' = (b)(s'_3\, s_4)(a\, s'_1\, c\, s_2) \in \varphi K^* \ .$$

Ceci conclut la preuve car comme b est plus petit que toutes les pièces de $s'_3\, s_4$, la permutation de φ'' est la même que celle du produit des deux lignes $(b\, s'_3\, s_4)(a\, s'_1\, c\, s_2) = (s_3\, s_4)(s_1\, c\, s_2) = \psi$.

Q. E. D.

THÉORÈME 2.4 (D. E. Knuth [8]). Chaque semi-orbite de glissement est une semi-orbite de Knuth.

Preuve. D'après nos définitions, il suffit de montrer que $\chi' \in \chi K^*$ quand χ' est obtenu par un seul glissement à partir du morphisme χ .

Considérons la suite $\chi_1 = \chi, \chi_2, \ldots, \chi_h = \chi'$ des morphismes construits pour définir ce glissement. Il suffit d'établir $\chi_{i+1} \in \chi_i K^*$ pour tout i. La permutation $\sigma(\chi_i)$ est la même que la permutation associée au produit des lignes de χ_i . Donc si χ_{i+1} ne diffère de χ_i que par le déplacement de la pièce c du point (x, y) au point $(x-1, y)$, on a $\sigma(\chi_i) = \sigma(\chi_{i+1})$ et le résultat est établi pour cette paire. Si au contraire χ_{i+1} est obtenu en faisant passer c de (x, y) en $(x, y-1)$, on peut se borner à considérer le produit des lignes y et $y-1$ de χ_i et χ_{i+1} et le résultat découle de l'énoncé 2.3 bis.

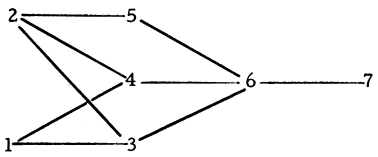
Q. E. D.

3. Le théorème de C. Green.

Etant donnés $k \geq 1$ et $\varphi \in \mathcal{M}_A$, soit $\mathcal{E}(\varphi ; k)$ l'ensemble des parties de A qui sont unions de k C_φ-chaînes et, comme indiqué dans l'introduction :

$$L_j(\varphi, k) = \text{Max } \{\text{Card } E : E \in \mathcal{E}(\varphi | A_j ; k)\}$$

où A_j est l'intervalle initial de A obtenu en lui enlevant ses j plus grandes pièces ($j \geq 0$) (et où, par conséquent, $A_0 = A$; $A_m = \emptyset$ pour $m \geq \text{Card } A$). Par exemple, si $\varphi = \begin{matrix} 2 & 5 & . & . \\ 1 & 4 & . & . \\ . & 3 & 6 & 7 \end{matrix}$, le graphe de C_φ est représenté par



et la partie significative de la fonction $L(\varphi)$ est fournie par la Table :

$j =$	0	1	2	3	4	5	6	7	.	.	.
$k = 1$	4	3	2	2	2	1	1	0	.	.	.
$k = 2$	6	5	4	4	3	2	1	0	.	.	.
$k = 3$	7	6	5	4	3	2	1	0	.	.	.
$k = 4$	7	6	5	4	3	2	1	0	.	.	.
...	.	.	.	.	.	.	.	.	.	.	.

THÉORÈME 3.1 (C. Green [5]). On a $L(\varphi) = L(\psi)$ pour chaque ψ de l'orbite de φ.

Preuve. Puisque les orbites sont définies par itération de glissements et de glissements inverses il suffit de considérer le cas où ψ est un glissement de φ. D'après 2.1 (5) on a alors que chaque $\psi | A_j$ est égal à un glissement de $\varphi | A_j$ ou à $\varphi | A_j$ lui-même. Par conséquent, il suffit d'établir $L_0(\varphi) = L_0(\psi)$ ce qui a

été démontré par C. Green dont nous reproduisons le raisonnement pour la commodité du lecteur.

D'après le théorème 2.4 de D. E. Knuth et le fait que $\mathcal{E}(\varphi ; k)$ ne dépend que de l'ordre C_φ, on peut se limiter au cas où φ et ψ sont respectivement des produits de la forme $\varphi_1\varphi_2\varphi_3$ et $\varphi_1(\varphi_2\, K)\varphi_3$ ainsi qu'on l'a dit pour définir K^*.

Supposons d'abord $\varphi_2 = \begin{matrix} a & c \\ \cdot & b \end{matrix}$ et $\varphi_2\, K = \begin{matrix} c & \cdot \\ a & b \end{matrix}$ où, on le rappelle, $a < b < c$. On a $C_\psi \subset C_\varphi$ et $C_\varphi \backslash C_\psi = \{(a, c)\}$. Par conséquent, pour chaque $k \geq 1$, l'ensemble $\mathcal{E}(\psi, k)$ est contenu dans $\mathcal{E}(\varphi, k)$ (d'où $L_0(\psi ; k) \leq L_0(\varphi ; k)$) et la partie E ne peut appartenir au second mais non au premier de ces ensembles que si elle contient une chaîne de la forme $sacs'$. Si b n'appartient pas à une chaîne de E, le fait que $a < b < c$ entraîne que $sabs'$ soit une C_ψ-chaîne, donc que $E' = (E \backslash sacs') \cup sabs'$ soit une union de k C_ψ-chaînes disjointes. Si au contraire E contient une chaîne tbt', on voit de même que $sabt'$ et tcs' sont deux C_ψ-chaîne. Donc $E' = (E \backslash \{sacs', tbt'\}) \cup \{sabt', tcs'\}$ appartient à $\mathcal{E}(\psi ; k)$. Dans les deux hypothèses Card E = Card E' et l'on a donc vérifié $L_0(\psi) = L_0(\varphi)$, dans le premier cas de Knuth.

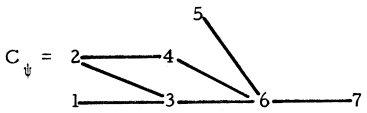
Le second cas où $\varphi_2 = \begin{matrix} b & c \\ \cdot & a \end{matrix}$ et $\varphi_2\, K = \begin{matrix} b & \cdot \\ a & c \end{matrix}$ est traité de façon symétrique puisque l'on a alors $C_\varphi \subset C_\psi \backslash C_\varphi = \{(a, c)\}$. Le résultat est donc prouvé dans tous les cas.

Q. E. D.

Par exemple, faisant subir au morphisme φ ci-dessus le glissement de sommet (1, 1) on obtient

$$\psi = \begin{matrix} 5 & & & \\ 2 & 4 & & \\ 1 & 3 & 6 & 7 \end{matrix}$$

pour lequel



Le lecteur pourra vérifier l'invariance de la fonction L associée.

On observera qu'un résultat légèrement plus fort a été établi, à savoir que si ψ appartient à la semi-orbite de φ, il correspond à chaque $E \in \mathcal{E}(\varphi, k)$ un $E' \in \mathcal{E}(\psi, k)$ ayant la propriété qu'il existe une bijection $a \to a'$ de E sur E' telle que $a' \leq a$, identiquement. J'ignore si cette propriété suffit pour caractériser les morphismes de l'orbite de φ qui appartiennent à sa semi-orbite. Elle montre en tout cas que $\begin{smallmatrix} a & c \\ . & b \end{smallmatrix}$ n'appartient pas à la semi-orbite de $\begin{smallmatrix} c & . \\ a & b \end{smallmatrix}$ $(a < b < c)$, ce qui présente un certain intérêt en raison du fait (établi plus bas) que ceci reste vrai pour tout morphisme contenant ces configurations.

Dans la suite de ce travail nous désignerons par $\mathcal{L} = \bigcup_{0 \leq n} \mathcal{L}_n$ la famille des fonctions $L(\varphi)$ $(\varphi \in \mathcal{M})$, $\mathcal{L}_n$ étant la sous-famille de celles qui, de façon équivalente, satisfont $L_0(k) = n$ pour tout $k \geq n$ ou $L_j(k) = 0$ pour tout $j \geq n$, $k \in \mathbb{N}$, c'est-à-dire qui correspondent à des morphismes dont le domaine a n points.

Introduisons la notation $\mathcal{P}_A$ pour désigner les morphismes de $\mathcal{M}$ d'image A dont le domaine est un intervalle principal de point minimum $(1, 1)$. Soit $n = \text{Card } A$.

3.2. A chaque $L \in \mathcal{L}_n$ correspond un et un seul morphisme principal ψ de $\mathcal{P}_A$ pour lequel $L = L(\psi)$. Son domaine est déterminé par L_0 et la position de la pièce Max A est déterminée par L_0 et L_1 seulement.

Preuve. Par hypothèse $L = L(\varphi)$ où $\varphi \in \mathcal{M}_A$. D'après 2.2, la semi-orbite de φ contient au moins un morphisme principal ψ et d'après le théorème précédent on

a $L(\psi) = L(\varphi)$.

Nous pouvons supposer que $\psi \in \mathcal{P}_A$ et il ne reste plus qu'à montrer que ψ est déterminé de façon unique par sa fonction L . Tout d'abord, puisque ψ est un morphisme, toutes les pièces d'une C_ψ-chaîne doivent se trouver dans des colonnes différentes. Donc $L_0(\psi ; k)$ est au moins égal à la somme des longueurs de k lignes de ψ $(k \geq 1)$. De fait $L_0(\psi ; k)$ est exactement égal à la somme des longueurs des k plus longues lignes de ψ puisque chaque ligne est une C_ψ-chaîne. Comme par hypothèse le domaine F de ψ a la forme d'un diagramme de Ferrers ceci montre qu'il est entièrement déterminé par la fonction L_0 .

Soit maintenant $A_1 = A \backslash a$ où $a = \operatorname{Max} A$. Le point $p = a\psi^{-1}$ est un point maximal de F . Donc le domaine $F' = F \backslash p$ de $\psi | A_1$ est aussi principal. D'après la première partie de la preuve, il est déterminé par $L_1(\psi) = L_0(\psi | A_1)$ et l'on a donc $a\psi^{-1} = F \backslash F'$, le résultat s'en déduit par induction sur $\operatorname{Card} A$.

Q. E. D.

Par exemple tous les morphismes φ dont le domaine est l'intervalle principal
x
x x
x x x x
satisfont

$$L_0(\varphi ; 1) = 4 \quad ; \quad L_0(\varphi ; 2) = 4 + 2 = 6 \quad ; \quad L_0(\varphi ; k \geq 3) = 4 + 2 + 1 = 7 \ .$$

Selon que la pièce $\operatorname{Max} A$ se trouve dans la première, deuxième ou troisième ligne, on a :

$L_1(\varphi, 1) = 3$ ou 4 ou 4 ; $L_1(\varphi, 2) = 5$ ou 5 ou 6 et $L(\varphi_1, k \geq 3) = 6$ dans les trois cas.

Notons $\equiv$ l'équivalence sur $\mathcal{M}$ telle que $\varphi \equiv \psi$ ssi $L(\varphi) = L(\psi)$ et si les deux morphismes ont même image. Le corollaire suivant résume les propriétés

dont nous aurons besoin. Nous faisons référence à l'introduction pour la définition des involutions $\varphi \to \varphi^T$ et $\varphi \to \bar{\varphi}$.

3.3. Les classes de l'équivalence $\equiv$ sont les orbites. Supposant $\varphi \equiv \psi$ on a :

(1) φ et ψ ne diffèrent que par une translation si leurs domaines sont principaux ;

(2) $\varphi^T \equiv \psi^T$; $\bar{\varphi} = \bar{\psi}$ et $\varphi|B \equiv \psi|B$ pour tout intervalle B de leur image ;

(3) $\varphi\varphi' \equiv \psi\psi'$ quels que soient φ' et ψ' tels que $\varphi' \equiv \psi'$.

Preuve. Le théorème de C. Green montre que $\varphi \equiv \psi$ quand ces deux morphismes appartiennent à la même orbite et 3.2 montre que cette équivalence satisfait (1).

Réciproquement, d'après 2.2 on peut trouver dans les semi-orbites de deux morphismes quelconques φ et ψ des morphismes principaux ayant même point minimum de leur domaine. Si de plus $L(\varphi) = L(\psi)$, ces morphismes principaux sont égaux d'après (1) et par conséquent φ et ψ sont dans une même orbite.

Les relations (2) découlent directement des assertions (3), (4) et (5) de 2.1. puisque les classes de $\equiv$ sont les orbites.

Pour vérifier (3) nous pouvons supposer que les domaines F et F' de φ et de φ' forment une C-partition de leur union. Il existe alors des morphismes principaux $\rho \equiv \varphi$ et $\rho' \equiv \varphi'$ dont un produit $\rho\rho'$ est contenu dans la semi-orbite de $\varphi\varphi'$ et satisfait $\rho\rho' \equiv \varphi\varphi'$. Ceci permet de supposer désormais que $\varphi = \rho$, $\varphi' = \rho'$ et que ψ et ψ' eux aussi sont principaux. D'après (1), φ et ψ sont égaux à des translations près et il en est de même de φ' et ψ'. On a donc $C_\varphi = C_\psi$, $C_{\varphi'} = C_{\psi'}$ d'où enfin $C_{\varphi\varphi'} = C_{\psi\psi'}$ d'après 1.2. ce qui implique l'équivalence cherchée.

Q. E. D.

Rappelons la notation $\mathcal{P}$ pour désigner la sous-famille des morphismes principaux de $\mathcal{M}$ dont $(1, 1)$ est le point minimum de domaine. L'énoncé précédent justifie la

DÉFINITION. La correspondance de Robinson est la projection R de $\mathcal{M}$ sur $\mathcal{P}$ envoyant chaque morphisme sur l'unique morphisme de son orbite qui appartienne à $\mathcal{P}$.

3.4. On a les formules :

(1) $\varphi^{T}R = (\varphi R)^{T}$; $\bar{\varphi}R = (\overline{\varphi R})R$;

(2) $(\varphi | A')R = (\varphi R | A')R$ pour chaque intervalle A' de l'image de φ où $(\varphi R | A')R = \varphi R | A'$ quand A' est un intervalle initial ;

(3) $(\varphi\psi)R = (\varphi R . \psi R)R$ où le domaine de $(\varphi\psi)R$ contient celui de φR et de ψR.

Preuve. Par définition les relations $\varphi \equiv \psi$ et $\varphi R = \psi R$ sont équivalentes. Donc (1) et (2) sont seulement une reformulation de l'énoncé précédent, puisque $\varphi R | A'$ est principal avance A' est un intervalle initial de l'image de φ. La seconde assertion de (3) résulte de 3.2 et du fait évident que quelques soient les les morphismes φ et ψ (d'images disjointes) on a $L_0(\varphi\psi) \geq L_0(\varphi)$, $L_0(\psi)$.

Q. E. D.

On observera que le théorème de Green montre directement à travers son corollaire 3.4 que le sous-ensemble $\mathcal{P}$ de $\mathcal{M}$ peut être muni d'une structure de monoïde en définissant le produit π de deux morphismes φ, ψ de $\mathcal{M}$ par $\pi = (\varphi\psi)R$ (avec la convention $OR = O$) . Il serait convenable de nommer ce résultat théorème de Schensted puisque l'associativité de ce produit peut être facilement établie en établissant le cas particulier $((a\varphi)Rb)R = (a((\varphi b)R))R$ $(a, b \in A , \varphi \in \mathcal{P})$ ce qui a été effectué directement par cet auteur [13] .

Nous complétons cette section par quelques remarques.

3.5. Soient $\varphi, \psi \in \mathcal{M}_A$. Une condition nécessaire et suffisante pour que $\varphi \equiv \psi$ est que $L_0(\varphi|B_j) = L_0(\psi|B_j)$ pour tous les termes B_j d'une suite strictement décroissante maximale $B_0 = A \supset B_1 \supset \ldots \supset B_n = \emptyset$ d'intervalles de A.

Preuve. D'après (2) de 3.3 cette condition est nécessaire. Réciproquement, chaque B_i est par hypothèse un intervalle de B_j pour $j \leq i$. On peut donc procéder par induction sur $n = \text{Card } A$ et supposer que $\varphi|B_1 \equiv \psi|B_1$. Si $A \setminus B_1 = a$ est la plus grande pièce de A, l'énoncé résulte directement de 3.2. Sinon, comme B_1 est un intervalle de A, la pièce a doit être la plus petite de celui-ci. Toujours d'après 3.2, on peut supposer que φ, ψ, $\varphi|B_1$ et $\psi|B_1$ ont des domaines principaux de point minimum $(1, 1)$. Donc $\varphi|B_1 = \psi|B_1$ ont même domaine F' et comme $\varphi = \varphi|B_0$, $\psi = \psi|B_0$, on déduit de $L_0(\varphi|B_0) = L_0(\psi|B_0)$ et de 3.2 que φ et ψ ont le même domaine principal F. On a évidemment $L_0(\varphi|B) = L_0(\varphi)$ et par conséquent $F \setminus F'$ est un point maximal p de F. Par définition, $\varphi|B_1$ est déduit de φ en enlevant la pièce $a = \text{Min } A$ du point $(1, 1)$ et en effectuant le glissement de sommet $(1, 1)$. Comme cette opération est invertible on retrouve $\varphi = \psi$ en appliquant à $\varphi|B_1 = \psi|B_1$ le glissement inverse de sommet p.

Q. E. D.

Une partie substantielle des preuves des résultats des chapitres suivants utilise la transformation envoyant chaque morphisme φ de $\mathcal{P}$ (c'est-à-dire tel que $\varphi = \varphi R$, $\varphi \in \mathcal{M}$) sur le morphisme $\bar{\varphi} R$ qui appartient évidemment aussi à $\mathcal{P}$. Cette opération change en $-A$ l'image A de φ ce qui peut être incommode et pour y remédier nous définirons φ^J comme l'image de $\bar{\varphi} R$ par l'isomorphisme Ω de la chaîne $-A$ sur la chaîne A. Autrement dit $a \to (-a)\,\Omega\,(= \bar{a})$ est l'anti-isomorphisme $a \to \bar{a}$ de la chaîne A sur elle-même.

Par exemple si $\varphi = \begin{matrix} 2 & 4 \\ 1 & 3 \; 5 \end{matrix}$ on a $\bar{\varphi} = \begin{matrix} -3 & -1 \\ -5 & -4 \; -2 \end{matrix}$ et par conséquent $\varphi^J = \begin{matrix} 3 & 5 \\ 1 & 2 \; 4 \end{matrix}$ puisqu'ici $-i\Omega = 6-i$ $(1 \leq i \leq 5)$.

Dans l'énoncé suivant on note $A^{(m)}$ (resp. A_m) l'intervalle final (resp. initial) de A formé des $n-m$ plus grandes (resp. plus petites) pièces de A et on emploie le même symbole Ω pour désigner l'isomorphisme entre $A^{(m)}$ et A_m $(m = 0, 1, \ldots, n = \mathrm{Card}\ A)$. En application des formules de 3.4 on a :

3.6. L'opération $\varphi \to \varphi^J$ est une involution sur chaque $\mathcal{P}_A(F)$ qui commute avec la transposition et qui satisfait identiquement les relations

$$\varphi^J|A_m = ((\varphi|A^{(m)})R\Omega)^J \quad \text{équivalentes à} \quad \bar{\varphi}R|{-A^{(m)}} = \overline{(\varphi|A^{(m)})}R \quad (0 \leq m \leq n).$$

Preuve. Soient φ un morphisme de $\mathcal{P}_A(F)$ et $\psi = \bar{\varphi}R$. On sait (1.1.) que l'involution $a \to -a$ établit un anti-isomorphisme entre l'ordre C_φ (sur A) et l'ordre $C_{-\varphi}$ (sur $-A$). Donc $L_0(\varphi) = L_0(\bar{\varphi}) = L_0(\psi)$ et comme le domaine F de φ est principal par hypothèse on conclut en vertu de 3.2 que F est aussi le domaine de ψ. Donc φ^J appartient à $\mathcal{P}_A(F)$.

Comme l'application $\chi \to \bar{\chi}$ $(\chi \in \mathcal{M})$ est une involution sur la famille des orbites et qu'elle commute avec la transposition, on a immédiatement que $\varphi = \bar{\psi}R$ d'où $\varphi^{JJ} = \varphi$ et que $\bar{\varphi}^T R = \psi^T$ d'où $\varphi^{JT} = \varphi^{TJ}$.

Maintenant comme $-A^{(m)}$ est un intervalle initial de l'image $-A$ de ψ et que $\psi = \psi R$, on a $\psi|{-A^{(m)}} \in \mathcal{P}$, c'est-à-dire que $\psi|{-A^{(m)}}$ est l'image par R de la restriction à $-A^{(m)}$ d'un morphisme quelconque de l'orbite de ψ (en raison de 3.3(2))donc en particulier de $\bar{\varphi}$.

Comme $\bar{\varphi}|{-A^{(m)}}$ est trivialement égal à $\overline{\varphi|A^{(m)}}$, on a par conséquent $\psi|{-A^{(m)}} = (\bar{\varphi}|{-A^{(m)}})R = \overline{(\varphi|A^{(m)})}R$ ce qui est la seconde des identités énoncées. La première s'en déduit facilement en observant que $\varphi^J|A_m$ ne diffère de $\bar{\varphi}R|{-A^{(m)}}$ que par un isomorphisme entre les images et qu'il en est de même des membres de droites des deux relations de par la définition même de l'isomorphis-

me Ω.

Q.E.D.

Cet énoncé fournit une justification directe de l'algorithme suivant de calcul de φ^J (cf. [14] p. 57-59). Soient $A = \{a_1 < a_2 \ldots < a_n\}$ et $\varphi_0 = \varphi$. Pour chaque $m = 1, \ldots, n$, on calcule φ_m en enlevant la pièce a_m du point minimum (1, 1) du domaine de φ_{m-1} et en effectuant ensuite le glissement de φ_{m-1} de sommet (1, 1), ce qui libère un point maximum q_m du domaine de φ_{m-1}. On pose alors $q_m \varphi^J = \bar{a}_m = a_{n+1-m}$.

Par exemple si $\varphi = \begin{matrix} 3 & 4 & \cdot \\ 1 & 2 & 5 \end{matrix} = \varphi_0$ on obtient $\varphi^J = \begin{matrix} 4 & 5 \\ 1 & 2 & 3 \end{matrix}$ à la suite des opérations suivantes :

$$\varphi_1 = \begin{matrix} 3 & * \\ 2 & 4 & 5 \end{matrix} \quad ; \quad \varphi_2 = \begin{matrix} * \\ 3 & 4 & 5 \end{matrix} \quad ; \quad \varphi_3 = 4\ 5\ * \quad ; \quad \varphi_5 = 5\ * \ .$$

Le lecteur pourra vérifier que le morphisme $\overline{\varphi R}$ est (à une translation près) l'unique morphisme de l'orbite de φ dont le domaine est co principal (c'est-à-dire possède un point maximum unique) ce qui est une autre manière de formuler la dualité $\varphi \to \varphi^J$.

La structure de celle-ci est loin d'être entièrement éclaircie. Ainsi j'ai observé (sans pouvoir le démontrer) que si deux morphismes φ et ψ de $\mathcal{P}$ ne diffèrent que par la transposition de deux pièces consécutives (dans leur image) les morphismes φ^J et ψ^J ne diffèrent que par une permutation de leurs pièces consistant en un cycle de longueur paire et des points fixes. Par exemple :

$$\varphi = \begin{matrix} 6 & \cdot & \cdot & \cdot \\ 4 & 5 & 7 & \cdot \\ 1 & 2 & 3 & 8 \end{matrix} \qquad \text{et} \qquad \psi = \begin{matrix} 6 & \cdot & \cdot & \cdot \\ 4 & 5 & 8 & \cdot \\ 1 & 2 & 3 & 7 \end{matrix}$$

diffèrent par la transposition (7, 8) cependant que

$$\varphi^J = \begin{matrix} 6 & . & . & . \\ 4 & 7 & 8 & . \\ 1 & 2 & 3 & 5 \end{matrix} \qquad \text{et} \qquad \psi^J = \begin{matrix} 6 & . & . & . \\ 2 & 4 & 7 & . \\ 1 & 3 & 5 & 8 \end{matrix}$$

se déduisent l'un de l'autre par la permutation circulaire (2, 3, 5, 8, 7, 4).

L'algorithme précédent peut être formulé dans un cadre moins spécial (qui contient aussi celui décrit au début de la section suivante). La technique est discutée dans un travail (à paraître) présenté au Colloque d'analyse combinatoire de l'Accademia dei Lincei en 1974.

Le dernier énoncé de cette section utilise la dualité $\varphi \to \varphi^J$ pour établir un résultat combinatoire servant de base au théorème d'Aitken. Nous rappelons que $\hat{J}^1$ désigne la famille des domaines principaux de point minimum (1, 1). Une écriture telle que $\lambda \in \mathcal{P}_m(F)$ signifiera que le domaine de λ est l'intervalle principal F de la famille $\hat{J}^1$ et que $m = \mathrm{Card}\, F$.

3.7. Soient F, G et H trois intervalles de $\hat{J}$, $\lambda_1 \in \mathcal{P}_m(F)$ et $\rho_1 \in \mathcal{P}_p(G)$. On suppose que H contient F et G. Il existe une bijection entre les ensembles $V(\lambda_1 ; G ; H) = \lambda_1 R^{-1} \cap \mathcal{M}_m(H\backslash G)$ et $V(\rho_1 ; F ; H) = \rho_1 R^{-1} \cap \mathcal{M}_p(H\backslash F)$.

Preuve. Par définition on a $m = \mathrm{Card}\, F$, $p = \mathrm{Card}\, G$ et les ensembles considérés sont vides sauf si $\mathrm{Card}\, H = m+p\ (= n)$ ainsi que nous le supposerons désormais. Soit $A = [n]$. Soit $U(\lambda_1, \rho_1)$ l'ensemble des morphismes $\varphi \in \mathcal{P}_A(H)$ tels que $\varphi|G = \rho_1^J$ et $(\varphi|H\backslash G)R\Omega = \lambda_1$ où Ω est l'isomorphisme de l'intervalle $A^{(m)} = A\backslash[p]$ sur $A_m = [m]$ dans les notations de 3.6. L'ensemble $U(\rho_1, \lambda_1)$ est défini de façon symétrique.

Il y a bijection entre $V(\lambda_1; G ; H) = V$ et $U(\lambda_1, \rho_1)$ puisque nous pouvons associer à chaque $\lambda \in V$ l'unique $\varphi \in U(\lambda_1, \rho_1)$ tel que $\varphi|G = \rho_1^J$ et $\varphi|H\backslash G = \lambda\Omega^{-1}$ et réciproquement. Il en est de même pour $V(\rho_1, F, H)$ et $U(\rho_1, \lambda_1)$ et il suffit de montrer $\varphi^J \in U(\rho_1, \lambda_1)$ pour chaque $\varphi \in U(\lambda_1, \rho_1)$ pour obtenir la bijection cherchée puisque J est une involution et que les ensembles sont

définis de façon symétrique.

Soit donc φ comme ci-dessus. D'après 3.6 , la restriction de φ^J à A_m est égale à $((\varphi|A^{(m)})R\,\Omega)^J$ donc à λ_1^J puisque par construction

$$\varphi|A^{(m)} = \varphi|H\backslash G = \lambda\,\Omega^{-1} \quad \text{où} \quad \lambda R = \lambda_1 .$$

On en déduit que $\varphi^J|A_m = \varphi|F$ donc que $\varphi|A^{(p)} = \varphi|H\backslash F$ puisque $A^{(p)} = [n]\backslash[m] = A\backslash A_m$. Appliquons le même énoncé à φ^J et p au lieu de φ et m .

Comme $\varphi^{JJ} = \varphi$ on obtient que $\varphi^{JJ}|A^{(p)} = ((\varphi^J|A^{(p)})R\,\Omega)^J$ (avec ici $\Omega : A^{(p)} \to A_p = [p]$) . Dans cette relation on a $\varphi^{JJ} = \varphi$ et, par construction, $\varphi|A_p = \rho_1^J$. En outre, comme on vient de le voir, $\varphi^J|A^{(p)} = \varphi^J|H\backslash F$. Comme J est une involution on a la conclusion désirée $\rho_1 = (\varphi^J|H\backslash F)R\,\Omega$.

Q. E. D.

Comme les deux ensembles V ont le même nombre d'éléments et que le premier (resp. le second) ne dépend pas du choix du morphisme ρ_1 (resp. λ_1) , ce nombre,que nous désignerons par g(F, G ; H), ne dépend que des intervalles F, G et H et ceci de façon symétrique en F et G . Comme de plus R commute avec la transposition on peut résumer l'énoncé précédent par l'identité suivante, dans laquelle on suppose g(F, G ; H) = 0 si les conditions de 3.7 ne sont pas satisfaites.

3.7. bis $\qquad g(F, G ; H) = g(G, F ; H) = g(F^T, G^T ; H^T)$.

Nous verrons plus loin que les g sont les paramètres de structure de la multiplication des fonctions de Schur.

Je mentionne enfin une construction dont le seul intérêt est de manifester une propriété de continuité curieuse de l'opération R .

Considérons un intervalle F du plan, un morphisme bijectif $\varphi : F \to [n]$, deux entiers positifs p et q et un système (ρ) de n morphismes bijectifs

$\rho_{i,j}$ ($(i, j) \in F$) dont les domaines sont l'intervalle rectangulaire du plan $[p] \times [q]$ et les images, la chaîne $[pq]$.

Soit G l'intervalle du plan formé des points de la forme $(ip+k, jq+k')$ où $(i, j) \in F$ et $(k, k') \in [p] \times [q]$. On définit le produit en couronne de (ρ) dans φ comme le morphisme bijectif ψ de domaine G tel que l'on ait identiquement :

$$(ip+k, jq+k')\psi = (i, j)\varphi . n + (k, k')\rho_{i,j}$$

Ceci fait on a la remarque suivante dont la preuve ne fait pas intervenir d'idées nouvelles et est omise :

3.8. Si ψ est le produit en couronne de (ρ) dans φ, alors ψR est le produit en couronne de (ρ) dans φR.

4. Le théorème de Robinson.

Nous commençons par un calcul dû initialement à G. de B. Robinson qui l'a présenté dans [12] au moyen du formalisme des "lattice permutations" (dont la possibilité de la traduction immédiate en termes de tableaux ne semble pas toujours avoir été perçue). La formulation ci-dessous est celle de Schensted [4] avec une simplification due à Knuth [9]. Nous rappelons que $\mathcal{P}$ est l'ensemble des morphismes φ de $\mathcal{M}$ tels que $\varphi = \varphi R$, c'est-à-dire dont le domaine est un intervalle principal de point minimum $(1, 1)$.

4.1. (1) Si $b \in A$ et $\varphi \in \mathcal{P}_{A \setminus b}$, le domaine de $(\varphi b)R$ est l'union de celui de φ et d'un point ;

(2) Réciproquement, si $\psi \in \mathcal{P}_A(F)$ il correspond à chaque point maximal p de son domaine une et une seule paire $b \in A$, $\varphi \in \mathcal{P}(F \setminus p)$ telle que $\psi = (\varphi b)R$.

Preuve. Supposons que b et φ satisfont les conditions de (1).

Si b est plus grande que toutes les pièces de la première ligne φ_1 de φ on a $C_{\varphi b} = C_\psi$ où $\psi = \psi R$ est obtenu en mettant b à la fin de φ_1. Donc $\psi = (\varphi b)R$ et le résultat est établi dans ce cas.

Dans le cas contraire on construit une suite $b_0 = b, b_1, \ldots, b_k$ par la condition que chaque b_{i+1} soit la plus petite pièce $> b_i$ de la ligne i de φ et que b_k soit le premier terme pour lequel la pièce obtenue soit plus grande que toutes les pièces de la ligne supérieure ou soit située sur la plus haute ligne de φ. Ceci fait, on définit ψ en remplaçant dans φ chaque b_{i+1} par b_i et en plaçant b_k à la fin de la ligne $k+1$. On vérifie que $\psi = \psi R \in \mathcal{M}$. Le fait que $\psi = (\varphi b)R$ est établi par induction en observant que $\varphi \equiv \varphi' \varphi_1$ où φ' est la restriction de φ aux lignes 2, 3, ... et en faisant appel à 2.3 qui montre que $\varphi_1 b \equiv b_1 \psi_1$ d'où $\varphi b \equiv \varphi' b_1 \psi_1$.

(2) Réciproquement si le point p se trouve à l'extrémité de la ligne $k+1$ de ψ on construit la suite $b_k = p\psi^{-1}$, $b_{k-1}, \ldots, b_0 = b$ où chaque b_i est la plus grande pièce $< b_{i+1}$ de la ligne i de ψ. Effectuant la substitution inverse de celle faite dans (1) on trouve un morphisme $\varphi = \varphi R$ et on vérifie que l'on a bien $\psi = (\varphi b_0)R$ par le même argument que ci-dessus.

Q.E.D.

EXEMPLE.

$$\varphi = \begin{matrix} 7 & . & . & . & . \\ 3 & 8 & . & . & . \\ 1 & 2 & 4 & 6 & 9 \end{matrix} \qquad (\varphi 5)R = \begin{matrix} 7 & 8 & . & . & . \\ 3 & 6 & . & . & . \\ 1 & 2 & 4 & 5 & 9 \end{matrix}$$

Nous avons défini dans le chapitre des notations à la fin de l'introduction le sous-ensemble $S^1_A \subset \mathcal{M}$ des permutations d'image A comme l'ensemble des $\sigma \in \mathcal{M}$ dont le domaine est formé des points $p_i = (n+1-i, i)$ $(1 \leq i \leq n = \mathrm{Card}\ A)$. Chaque permutation est donc un produit $(p_1\sigma)(p_2\sigma)\ldots(p_n\sigma)$. Nous définissons son inverse σ^{-1} comme le produit $\tau = c_1 c_2 \ldots c_n \in S^1_n$ où pour chaque $r = 1, 2, \ldots, n$, on a $c_r = j$ ssi $p_j \sigma$ est la r-ième pièce de A (par ordre

croissant). C'est donc l'inverse habituel quand A est la chaîne standard $[n]$. On a la formule importante :

4.2. Les ordres C_σ sur A et $C_{\sigma^{-1}}$ sur $[n]$ sont isomorphes.

Preuve. Soit $b = p_i\sigma$ et $b' = p_j\sigma$ respectivement la r-ième et la s-ième pièce de A. Par définition on a $(b, b') \in C_\sigma$ ssi d'une part $b \leq b'$, c'est-à-dire $r \leq s$, et d'autre part $(p_i, p_j) \in C$, c'est-à-dire $i \leq j$ et ces deux conditions équivalent donc à $(c_r, c_s) \in C_{\sigma^{-1}}$.

Q. E. D.

L'énoncé 4.2 est donc une simple reformulation du fait connu que $\sigma \to \sigma^{-1}$ induit une bijection sur l'ensemble des paires en inversion.

Nous établissons maintenant le résultat le plus important de la théorie. Dans son énoncé $\mathcal{L}_n^{(2)}$ désigne l'ensemble des paires de fonctions $(L, L') \in \mathcal{L}_n \times \mathcal{L}_n$ telles que $L_0 = L'_0$. Comme d'habitude Card A = n.

THÉORÈME 4.3 (G. de B. Robinson). L'application $\sigma \to (L(\sigma), L(\sigma^{-1}))$ est une bijection de S_A^1 sur $\mathcal{L}_n^{(2)}$.

Preuve. On vient de voir que les ordres C_σ et $C_{\sigma^{-1}}$ sont isomorphes ce qui entraîne immédiatement $L_0(\sigma) = L_0(\sigma^{-1})$ et l'application est donc une application de S_A^1 dans $\mathcal{L}_n^{(2)}$.

Réciproquement, considérons une paire $(M, N) \in \mathcal{L}_n^{(2)}$ et montrons qu'il lui correspond une et une seule permutation $\sigma \in S_A^1$ telle que $M = L(\sigma)$, $N = L(\sigma^{-1})$.

Ceci est trivial pour $n = 1$ et nous procédons par induction sur $n \geq 2$.

D'après 3.3 il existe une et une seule paire $\varphi = \varphi R$, $\psi = \psi R$ d'image $[n]$ telle que $M = L(\varphi)$, $N = L(\psi)$. Puisque $M_0 = L_0$, les morphismes φ et ψ ont même domaine F . De plus, d'après 3.2 , la fonction M_1 détermine le point maximum p de F où se trouve la pièce n dans ψ . D'après 4.1 , il existe une et une seule paire (φ', b) où $\varphi' = \varphi' R$ a pour domaine $F \setminus p$ et $b \in [n]$ telle que $(\varphi' b)R = \varphi$. Par construction la paire de fonctions $(L(\varphi'), L(\psi|[n-1]))$ appartient à $\mathcal{L}^{(2)}_{n-1}$. D'après la définition des fonctions L , la fonction $L(\psi|[n-1])$ est déterminée par M puisque c'est simplement la fonction M^+ telle que $M^+_j = M_{j+1}$ $(j = 0, 1, \ldots)$.

D'après l'hypothèse d'induction il existe une et une seule permutation $\tau' = b'_1 \ldots b'_{n-1}$ de S^1_{n-1} qui soit telle que

$$L(\tau') = L(\varphi') \quad \text{et} \quad L(\tau'^{-1}) = M^+ .$$

Nous définissons maintenant la permutation $\tau = b_1 \ldots b_n$ de S^1_n en posant $b_n = b$ (où b est la pièce obtenue plus haut) et pour chaque $i \leq n-1$, $b_i = b'_i$ où $1+b'_i$ selon que $b_i < b$ ou $b_i > b$. Comme $b'_i \to b_i$ est un isomorphisme on a bien $\varphi = \tau R$, donc $N = L(\tau)$ et comme $b_n = b$ est le dernier élément du produit τ on a $M = L(\tau^{-1})$.

L'unicité de cette permutation τ est une conséquence immédiate du caractère biunivoque de chacune des étapes de sa construction. On obtient enfin $\sigma \in S'_A$ en posant $\sigma = \tau\Omega^{-1}$ où Ω est l'isomorphisme de $[n]$ sur A .

Q.E.D.

Une formulation équivalente de ce théorème est l'assertion que l'application $RR : \sigma \to (\sigma R, \sigma^{-1} R)$ est une bijection de S^1_n sur l'ensemble des paires de morphismes de ρ_n ayant même domaine. Je fais référence au remarquable travail de G. Viennot [20] pour une interprétation géométrique de ces résultats.

Nous signalons maintenant quelques propriétés de cette correspondance en employant les notations J et Ω définies à la fin de la section 3. On pose $\bar{b} = (-b)\Omega$ $(b \in [n])$ où Ω est ici l'isomorphisme de $-[n]$ sur $[n]$. Par conséquent $b \to \bar{b}$ est simplement l'anti-isomorphisme de la chaîne $[n]$ sur elle-même. Les relations de (1) ci-dessous dans lesquelles J n'intervient pas sont dues à Schensted [14].

4.3. Soient $\sigma = b_1 b_2 \dots b_n \in S_A^1$ une permutation et $(\varphi, \psi) = \sigma RR$. On a :

(1)
$$(\bar{b}_n \bar{b}_{n-1} \dots \bar{b}_1)RR = (\varphi^J, \psi^J)$$
$$(b_n b_{n-1} \dots b_1)RR = (\varphi^T, \psi^{JT})$$
$$(\bar{b}_1 \bar{b}_2 \dots \bar{b}_n)RR = (\varphi^{JT}, \psi^T).$$

(2) Si $\beta = b_1 \dots b_p$ et $\gamma = b_{p+1} \dots b_n$ sont une factorisation de σ, on a $\beta^{-1}R = \psi|[p]$ et $\gamma^{-1}R = (\psi|[n]\backslash[p])R\Omega$ où $\Omega : [n]\backslash[p] \to [n-p]$.

Preuve. Comme $b_n \dots b_1 = \sigma^T$ et comme la transposition commute avec R on a $(b_n \dots b_1)R = \varphi^T$. D'autre part, d'après les définitions de l'involution $\chi \to \bar{\chi}$ $(\chi \in \mathcal{M})$ et de l'isomorphisme $\Omega : -[n] \to [n]$ on a $\bar{\sigma}\Omega = \bar{b}_n \dots \bar{b}_2 \bar{b}_1$, donc $(\bar{b}_n \dots \bar{b}_2 \bar{b}_1)R = \varphi^J$ en raison de la définition de J et de l'identité $\bar{\chi}R = (\overline{\chi R})R$. La troisième formule $(\bar{b}_1 \dots \bar{b}_n)R = \varphi^{JT}$ résulte des deux précédentes puisque J et T commutent.

Pour établir les formules concernant ψ il suffit de vérifier l'une d'elles et d'utiliser la dualité $\sigma \to \sigma^{-1}$. Le plus simple est de noter que si $\sigma' = \bar{b}_n \dots \bar{b}_2 \bar{b}_1$ on a de façon équivalente, $\sigma'^{-1} = (\sigma^{-1})^T$ d'où $(\bar{b}_n \dots \bar{b}_2 \bar{b}_1)RR = (\varphi^{JT}, \psi^T)$.

La deuxième partie de l'énoncé résulte de ce que β^{-1} est la restriction de σ^{-1} à l'intervalle initial $[p]$ de son image et que, de même, γ^{-1} est la restriction de σ^{-1} au complément de $[p]$.

Q. E. D.

4.4. La correspondance $\sigma \to \sigma R$ établit une bijection entre les involutions sur $[n]$ et la famille $\mathcal{P}$ telle que le nombre des points fixes de σ est égal au nombre des colonnes de longueur impaire de σR.

Preuve. La permutation σ est une involution ssi $\sigma = \sigma^{-1}$, donc d'après le théorème de Robinson, ssi $\sigma R = \sigma^{-1} R$ ce qui établit la première partie de l'énoncé.

En ce qui concerne la seconde nous procédons par induction sur $[n]$ et nous considérons une involution $\sigma = b_1 b_2 \dots b_n$. Si $b_n = n$, σ a un point fixe de plus que l'involution $\sigma' = b_1 \dots b_{n-1}$ et le morphisme σR a une colonne impaire de plus que $\sigma' R$ puisque d'après 4.1, $\sigma R = (\sigma' n) R$ est obtenu en ajoutant la pièce n à la fin de la première ligne de $\sigma' R$, ce qui crée une nouvelle colonne de longueur 1.

Soit maintenant $b_n = m \neq n$. Nous considérons σ' comme ci-dessus et l'involution τ sur $A = [n] \setminus \{n, m\}$ obtenue en supprimant $b_m = n$ et $b_n = m$ dans le produit σ. Comme n est une pièce maximale, τR est la restriction de $\sigma' R$ à A ; c'est-à-dire que τR se déduit de $\sigma' R$ en retranchant la pièce $n = b_m$ qui se trouve au point q du domaine F de σ'.

D'autre part, toujours d'après 4.1, on voit que $\sigma R = (\sigma' m) R$ a pour domaine l'union de F et d'un point p. Comme $\sigma R = \sigma^{-1} R$ ce point p porte la pièce maximale n de l'image $[n]$ de σ^{-1}. Autrement dit, l'opération $\sigma' R \to (\sigma' m) R$ déplace la pièce n du point q au point p qui se trouve donc dans la ligne immédiatement supérieure à celle de q. Si p et q sont dans la même colonne, les domaines $F \cup p$ de σ et $F \setminus q$ de τ ont le même nombre de colonnes impaires, d'où le résultat par induction puisque τ a, par construction, le même nombre de points fixes que σ.

Si au contraire $p = (i, j)$ et $q = (i', j')$ sont dans deux colonnes distinctes, c'est-à-dire si $i \neq i'$, ces deux points sont des points maximaux de $F \cup p$ et les

longueurs de ces colonnes sont j et $j' = j-1$, donc de parités différentes. Par conséquent le domaine $F\backslash q$ de τ a encore le même nombre de colonnes impaires que celui de σ.

Q. E. D.

En particulier R établit une bijection entre les involutions sans points fixes et les morphismes φ de P dont toutes les colonnes du domaine ont une longueur paire. Une autre bijection a été découverte par W. H. Burge ([3]) entre ces involutions et les morphismes φ de P dont le domaine a la forme $\{\alpha\}$ de Littlewood (cf. [3]). Je n'ai pas réussi à trouver le cadre dans lequel la construction de Burge est naturelle.

L'énoncé suivant est associé à 3.7.

4.5. Soient F, G deux domaines principaux de $\hat{J}^1$ de cardinaux respectifs m et p, $\chi \in \mathcal{P}_n(H)$ et $\lambda_1 \in \mathcal{P}_m(F)$. L'ensemble $W(F, G;\chi) = \{(\rho, \lambda) \in \mathcal{P}(G) \times \mathcal{P}(F) : (\rho\lambda)R = \chi\}$ est non vide ssi $n = m+p$ et F, $G \subset H$. S'il en est ainsi, il est en bijection avec l'ensemble $\lambda_1 R^{-1} \cap \mathcal{M}_m(H\backslash G)$.

Preuve. Supposons $(\rho, \lambda) \in W$. La condition $(\rho\lambda)R = \chi \in P_n(H)$ implique évidemment que les images B et C de ρ et de λ forment une partition de $A = [n]$, donc que $n = m+p$. Le fait que H contient F et G résulte de 3.4 (2).

Choisissons arbitrairement un morphisme $\rho_1 \in \mathcal{P}_p(G)$. D'après le théorème de Robinson il existe une et une seule permutation β d'image B telle que $\beta RR = (\rho, \rho_1)$ (resp. γ d'image C telle que $\gamma RR = (\lambda, \lambda_1)$). Soit σ un produit $\beta\gamma$. Par construction on a $\sigma R = (\beta R.\gamma R)R = (\rho\lambda)R = \chi$. Considérons $\psi = \sigma^{-1}R$. D'après 4.3 $(\psi|[p])R = \beta^{-1}R = \rho_1$ et $(\psi|[n]\backslash[p])R\Omega = \gamma^{-1}R = \lambda_1$. Par conséquent pour chaque ρ_1 arbitrairement choisi la correspondance $(\rho, \lambda) \to (\psi|[n]\backslash[p])\Omega$ est une application de W dans $\lambda_1 R^{-1} \cap \mathcal{M}_m(H\backslash G)$.

Réciproquement, supposant donné λ dans ce dernier ensemble, on définit $\psi \in \mathcal{P}_n(H)$ par ses restrictions $\psi|[p] = \rho_1$; $\psi|[n]\setminus[p] = \lambda\Omega^{-1}$ et on obtient σ comme l'unique permutation telle que $\sigma RR = (\varphi, \psi)$. La factorisation $\sigma = \beta\gamma$ est déterminée sans ambiguité par les longueurs p et $n-p = m$ de β et de γ et on obtient la paire $(\beta R, \gamma R)$ de $W(F, G; \chi)$.

Q. E. D.

Il résulte de l'existence de cette bijection que W est indépendant du choix de χ dans H et on écrira plutôt $W(F, G ; H)$. Il existe une bijection évidente avec $W(F^T, G^T ; H^T)$. L'énoncé 3.7 permet d'en établir une autre avec $W(G, F ; H)$. Enfin 4.5 lui-même signifie que $g(F, G ; H) = \mathrm{Card}\, W(F, G ; H)$.

On indiquera dans la section suivante comment ces relations se traduisent en termes d'identités dans l'algèbre des fonctions de Schur. Ceci motive la recherche d'un algorithme facilitant le calcul des nombres $g(F, G ; H)$ c'est-à-dire, essentiellement, du nombre des tableaux ψ de domaine $H\setminus G$ tels que ψR ait pour domaine l'intervalle principal F. Cet algorithme est connu sous le nom de "règle de Littlewood-Richardson". Nous en exposons maintenant la base combinatoire en utilisant une idée de A. Lascoux et une technique de preuve suggérée par D. Foata.

Nous considérons désormais une partition <u>non croissante</u> fixe $\nu = \{n_1 \geq n_2 \geq \ldots \geq n_k > 0\}$ de l'entier $n = n_1+n_2+ \ldots + n_k$. Elle définit une partition de la chaîne $[n]$ en intervalles successifs $I_1, \ldots, I_k$ de longueurs respectives $n_1, \ldots, n_k$ et un intervalle principal $F = F_\nu$ dont les longueurs des colonnes sont les n_i. Le morphisme $\chi = \chi_\nu$ de domaine F tel que les pièces de l'intervalle I_i soient dans la i-ème colonne de F $(1 \leq i \leq k)$ sera appelé le <u>morphisme naturel</u> de ν.

Par exemple le morphisme naturel de $\nu = (3, 2, 2, 1)$ est

$$\chi = \begin{matrix} 3 & . & . & . \\ 2 & 5 & 7 & . \\ 1 & 4 & 6 & 8 \end{matrix} .$$

Soit maintenant A une chaîne ayant n éléments.

4.6. Si $\varphi : F \to A$ est un morphisme bijectif, la permutation $\tau = \tau_\varphi$ telle que $(\tau R, \tau^{-1} R) = (\varphi, \chi)$ est celle obtenue en lisant φ par colonnes (de haut en bas et de gauche à droite).

Preuve. La pièce n se trouve au point (k, n_k) du tableau naturel χ. Donc, d'après l'algorithme de Robinson, le dernier élément de la permutation τ est la pièce $a' = (k, 1)\varphi$. Soient $\nu' = (n_1, n_2, \ldots, n_k - 1)$ et φ' le morphisme de domaine $F_{\nu'}$ et d'image $A \backslash a'$ obtenu en enlevant a' et en abaissant d'un pas toutes les autres pièces situées dans la k-ième colonne de φ. On a $\tau = \tau' a'$ où τ' est la permutation de $A \backslash a'$ telle que $(\tau' R, \tau'^{-1} R) = (\varphi', \chi_{\nu'})$ (où $\chi_{\nu'}$ dénote évidemment le morphisme naturel de ν'). Par induction sur n, τ' a la forme voulue, ce qui établit le résultat.

Q. E. D.

Par exemple si $\varphi = \begin{matrix} 7 & . & . & . \\ 3 & 5 & 8 & . \\ 1 & 2 & 4 & 6 \end{matrix}$ on trouve que $\tau = \tau_\varphi = (7\ 3\ 1\ 5\ 2\ 8\ 4\ 6)$.

Le lecteur observera que la permutation $\tau = \tau_\varphi$ qui vient d'être construite en lisant φ "par colonnes" n'est pas la permutation $\sigma = \sigma(\varphi)$ définie dans l'introduction par la lecture successives des lignes de φ (de gauche à droite et de bas en haut). Dans l'exemple précédent on aurait $\sigma(\varphi) = (7\ 3\ 5\ 8\ 1\ 2\ 4\ 6)$. C'est $\sigma(\varphi)$ qui sera utilisée dans l'énoncé suivant. Auparavant nous associons à la même partition ν le morphisme $\omega = \omega_\nu$ de $[n]$ sur $[k]$ envoyant chaque intervalle $I_i \subset [n]$ sur $i \in [k]$. Par conséquent si $\sigma = s_1 s_2 \ldots s_n$ est une permutation de $[n]$ son image $\sigma\omega = s_1\omega \cdot s_2\omega \ldots s_n\omega$ a pour multidegré ν (en ce sens que le nombre $|\sigma\omega|_i$ d'occurrences de chaque $i \in [k]$ dans $\sigma\omega$ est exactement n_i). De plus nous désignons

par Y l'ensemble des mots $x = x_1 x_2 \dots x_n$ sur l'alphabet $[k]$ qui satisfont la condition que pour chaque $m \leq n$ et $i \leq k-1$ le nombre des occurrences de i dans le facteur gauche $x_1 \dots x_m$ soit au moins égal à celui des occurrences de $i+1$. Ces mots sont les "lattice permutations" de MacMahon et G. de B. Robinson. Suivant l'usage des physiciens nous les appellerons mots de Yamanouchi.

Par exemple si $k = 2$, le sous-ensemble des mots de Y de multidegré $(3,2)$ est formé des 5 mots :

$$\{1\,1\,1\,2\,2,\ 1\,1\,2\,1\,2,\ 1\,1\,2\,2\,1,\ 1\,2\,1\,1\,2,\ 1\,2\,1\,2\,1\}.$$

La condition Y implique que le multidegré soit une partition ordonnée et signifie que, pour chaque lettre i, la j-ème occurrence de celle-ci dans le mot précède la j-ème occurrence de la lettre $i+1$ pour tout $j \leq n_{j+1}$.

Ceci permet de définir la famille Y'_ν des permutations $\sigma = s_1 s_2 \dots s_n$ de $[n]$ telles que, d'une part, $\sigma\omega$ soit un mot de Yamanouchi de multidegré ν et que, d'autre part, on ait $s_i > s_j$ quand $i < j$ et $s_i\omega = s_j\omega$. On a alors :

4.7. L'ensemble χR^{-1} est formé des morphismes bijectifs ψ d'image $[n]$ et de domaine quelconque tels que leur permutation (par ligne) $\sigma = \sigma(\psi)$ appartienne à Y'_ν.

Preuve. Comme $(\sigma(\psi))R$ est égal à ψR il suffit d'établir que la condition $\sigma \in Y_\nu$ caractérise les permutations σ pour lesquelles σR est le morphisme naturel χ. D'après l'énoncé précédent on sait d'autre part que $\sigma R = \chi$ ssi son inverse σ^{-1} est la permutation τ_φ obtenue en lisant "par colonne" un tableau φ de domaine F et d'image $[n]$.

Considérons d'abord une telle permutation $\tau = \tau_\varphi$ et vérifions que son inverse $\sigma = \tau^{-1}$ appartient bien à Y_ν. Par définition τ envoie chaque intervalle I_i de $[n]$ sur l'ensemble C_i des pièces figurant dans la i-ème colonne de φ. Donc

$C_i\sigma = I_i$ et $C_i\sigma\omega = i$ $(i \in [k])$ ce qui montre que σ a le multidegré ν. De plus pour chaque $i \leq k-1$ et $j \leq n_{i+1}$, la pièce x située dans φ dans la colonne j et la ligne i est plus petite que la pièce y située juste en dessus. Comme x (resp. y) est la j-ième lettre de σ dont l'image par ω soit i (resp. $i+1$), la condition Y est vérifiée par $\sigma\omega$.

Réciproquement, soient $\sigma \in Y'_\nu$ et τ son inverse. La dernière condition caractérisant Y'_ν montre que la restriction de τ à chaque $C_i = \{j : j\sigma\omega = i\}$ est un mot dont les lettres vont en décroissant de gauche à droite et que C_i a n_i éléments puisque $\sigma\omega$ est de multidegré ν.

La condition que $\sigma\omega$ est un mot de Yamanouchi implique que pour chaque $i \leq k-1$ et $j \leq n_{j+1}$ la j-ième lettre x de σ dont l'image par ω est i soit plus petite que la j-ième lettre y dont l'image est $i+1$. Il en résulte que la bijection $\varphi : F \to [n]$ dont les colonnes sont les C_i est un morphisme et le résultat est établi puisque $\tau = \tau_\varphi$ par construction.

Q. E. D.

Reprenant le même exemple que plus haut où $\tau = (7\ 3\ 1\ 5\ 2\ 8\ 4\ 6)$, on a $\tau^{-1} = \sigma = (3\ 5\ 2\ 7\ 4\ 8\ 1\ 6)$ dont l'image par ω est $(1\ 2\ 1\ 3\ 2\ 4\ 1\ 3) \in Y_\nu$).

5. Connexion avec les fonctions de Schur.

Nous commençons par compléter l'outillage combinatoire. Si φ est un morphisme de $\mathcal{M}$, une file de φ est un intervalle maximal B de son image qui est une C_φ-chaîne. Par exemple les files de

$$\varphi = \begin{matrix} 10 & . & . & . & . \\ 5 & 9 & 12 & . & . \\ . & 1 & 4 & 7 & 8 \end{matrix}$$ sont

$B_1 = (1, 4)$, $B_2 = (5, 7, 8)$, $B_3 = (9)$, $B_4 = (10, 12)$.

Il est clair que les files de φ constituent une partition ordonnée (de façon naturelle) de son image A et qu'elles sont déterminées sans ambiguité par la donnée de A et de la suite (dite suite de files) $N(\varphi) = (n_1, n_2, \ldots, n_k)$ du nombre de leurs éléments ($N(\varphi) = (2, 3, 1, 2)$ dans l'exemple ci-dessus).

5.1. Soit $N(\varphi) = (n_1, \ldots, n_k)$ la suite de files d'un morphisme φ de $\mathcal{M}_n$. Alors :

(1) $N(\varphi) = N(\varphi R)$;

(2) $N(\bar{\varphi}) = (n_k, \ldots, n_1)$ et $N(\varphi^T)$ sont déterminées par $N(\varphi)$;

(3) Quand φ est une permutation σ, les longueurs des facteurs croissants maximaux de σ^{-1} sont $n_1, \ldots, n_k$.

Preuve. (1) Soit B un intervalle de l'image $[n]$ de φ. Il est contenu dans une file de φ ssi il est contenu dans une C_φ-chaîne, c'est-à-dire, de façon équivalente ssi $(\varphi|B)R$ se réduit à une seule ligne d'où le résultat d'après la formule $(\varphi R|B)R = (\varphi|B)R$ de 3.4.2 .

(2) La première assertion résulte immédiatement de l'anti-isomorphisme entre les ordres C_φ et $C_{\bar{\varphi}}$. La seconde utilise une observation qui présente un intérêt plus général.

Soient $a < b$ deux pièces de A qui n'appartiennent ni à une file de φ ni à une file du morphisme transposé φ^T. Posant $p = a\varphi^{-1} = (x, y)$ et $q = b\varphi^{-1} = (x', y')$, ceci équivaut à $(p, q) \notin C$ et $(p^T, q^T) \notin C$, c'est-à-dire à :

NON ($x \leq x'$ et $y \geq y'$) et NON ($y \leq y'$ et $x \geq x'$)

c'est-à-dire encore à :

($x > x'$ ou $y < y'$) et ($x < x'$ ou $y > y'$)

soit enfin à :

($x > x'$ et $y > y'$) ou ($x < x'$ et $y < y'$).

La première alternative est exclue puisque φ est un morphisme et puisque $a\ (= (x, y)\varphi) < b\ (= (x', y')\varphi)$. On a donc $x < x'$ et $y < y'$ et comme le domaine de φ est un intervalle ce dernier contient deux points $r = (x, y')$ et $s = (x', y)$ satisfaisant $p < r$, $s < q$. Utilisant de nouveau le fait que φ est un morphisme, on en déduit enfin qu'il existe deux pièces $c = r\varphi$ et $d = s\varphi$ telles que $a < c$, $d < b$.

Par conséquent deux pièces consécutives de la chaîne A appartiennent à une file de φ ou à une file de φ^T. Comme de plus les ordres C_φ et C_{φ^T} ont une intersection triviale on obtient le résultat que les files de φ^T sont les intervalles maximaux de A pour lesquels toutes les pièces appartiennent à des files de φ différentes, et vice versa.

(3) Ceci résulte immédiatement de l'isomorphisme entre C_σ et $C_{\sigma^{-1}}$ et du fait que les intervalles initiaux de longueur m $(m \leq n)$ de l'image de σ correspondent aux facteurs gauches de même longueur de la permutation inverse σ^{-1}.

Q.E.D.

Soit par exemple $\varphi = \begin{matrix} 7 & 9 & . & . \\ 3 & 4 & 8 & . \\ 1 & 2 & 5 & 6 \end{matrix}$. Ses files sont (1 2), (3 4 5 6), (7 8), (9) et $N(\varphi) = (2, 4, 2, 1)$. La permutation associée $\sigma = \sigma(\varphi)$ est 7 9 3 4 8 1 2 5 6 dont l'inverse σ^{-1} est 6 7 3 4 8 9 1 5 2. Les facteurs croissants maximaux de σ^{-1} ont bien pour longueur 2, 4, 2 et 1. Le morphisme transposé φ^T a pour files (1) (2 3) (4) (5) (6 7) (8 9) $(N(\varphi^T) = (1, 2, 1, 1, 2, 2))$. La permutation associée est 6 5 2 1 8 4 3 9 7 dont l'inverse est 4 3 7 6 2 1 9 5 8 dont les longueurs des facteurs croissants maximaux sont bien 1, 2, 1, 1, 2, 2. (cf. les relations discutées dans 4.3).

En raison de son importance pour la suite nous isolons le fait suivant.

5.2. Tous les morphismes (bijectifs) de chaque orbite de glissement ont la même suite de files.

Preuve. Ceci résulte immédiatement de (1) ci-dessus.

Q.E.D.

La réciproque est évidemment fausse comme le montre l'exemple (minimal) des deux morphismes principaux $\begin{matrix} 4 & . & . \\ 2 & 6 & . \\ 1 & 3 & 5 \end{matrix}$ et $\begin{matrix} 6 & . & . \\ 2 & 4 & . \\ 1 & 3 & 5 \end{matrix}$ qui ont la même suite de files (1, 2, 2, 1).

Ces notions permettent d'appliquer une partie de considérations développées dans les sections précédentes à une famille $\tilde{\mathfrak{M}}$ généralisant celle des morphismes bijectifs. Nous appellerons les éléments de $\tilde{\mathfrak{M}}$ les morphismes verticalement injectifs. Comme on le verra ils correspondent aux monômes intervenant dans les fonctions de Schur.

DÉFINITION. A étant une chaîne et F un intervalle du plan, $\tilde{\mathfrak{M}}_A(F)$ est la famille des morphismes α de domaine F dont l'image est une partie de A et dont la restriction à chaque colonne de F est injective.

Autrement dit α appartient à $\tilde{\mathfrak{M}}$ ssi aucune pièce ne figure plus d'une fois dans une même colonne. Par exemple le morphisme $\alpha = \begin{matrix} 6 & . & . \\ 2 & 2 & 6 \\ . & . & 2 & 5 \end{matrix}$ appartient à $\tilde{\mathfrak{M}}_A$ pour toute chaîne A contenant 2, 5 et 6.

Le multidegré $|\alpha|$ d'un morphisme α de la famille $\tilde{\mathfrak{M}}_A$ des morphismes

de $\tilde{\mathcal{M}}$ dont l'image est contenue dans A est la fonction donnant le nombre d'occurrences $|\alpha|_a$ de chaque $a \in A$ dans α .

Il est clair que la notion de produit définie dans l'introduction s'étend de façon naturelle à $\tilde{\mathcal{M}}$ et que le multidegré d'un produit est la somme des multidegrés de ses facteurs. Les morphismes de $\mathcal{M}$ peuvent donc être caractérisés comme les éléments multilinéaires de $\tilde{\mathcal{M}}$.

Nous établissons maintenant une correspondance très simple entre les deux familles.

Soit $\alpha \in \tilde{\mathcal{M}}_A(F)$. L'ensemble $A \times \mathbb{N}$ est une chaîne pour l'ordre lexicographique : ses éléments sont simplement les pièces de A indexées. On associe à α un morphisme bijectif α' de domaine F dont l'image est une partie A' de $A \times \mathbb{N}$ en indexant pour chaque pièce chacune de ses occurrences dans l'ordre croissant en lisant α de gauche à droite. Par exemple si

$$A = \{a, b, c, d, e, f\} \quad \text{et} \quad \alpha = \begin{matrix} c & . & . & . \\ b & e & f & f \\ . & b & b & c \end{matrix}$$

on obtient

$$\alpha' = \begin{matrix} c1 & . & . & . \\ b1 & e1 & f1 & . \\ . & b2 & b3 & c2 \end{matrix} \quad .$$

Ceci fait, si Ω est le morphisme bijectif de A' sur $[n]$ (n = Card F), l'application $\varphi = \alpha'\Omega$ est un morphisme bijectif de F sur $[n]$ que l'on notera αP . De plus si γ' est le morphisme naturel de A' dans A consistant à oublier les indices et $\gamma = \Omega^{-1}\gamma'$, on a la relation

$$\alpha P \Omega^{-1} \gamma' = \alpha' \gamma' = \alpha \ .$$

Dans l'exemple précédent on trouve $\alpha P = \begin{matrix} 4 & . & . & . \\ 1 & 6 & 7 & . \\ . & 2 & 3 & 5 \end{matrix}$ et γ est défini par $a\gamma^{-1} = d\gamma^{-1} = \emptyset$; $b\gamma^{-1} = \{1, 2, 3\}$ $c\gamma^{-1} = \{4, 5\}$, $e\gamma^{-1} = \{6\}$, $f\gamma^{-1} = \{7\}$.
Par construction chaque $a\gamma^{-1}$ $(a \in A)$ est un intervalle de $[n]$ et le multidegré

de α est défini par γ.

Par construction aussi chaque $a\gamma'^{-1}$ $(a \in A)$ est contenu dans une file de α' et comme celles-ci sont en bijection par Ω avec celles de αP on a la remarque importante que chaque file de αP est une union de parties de la forme $a\gamma^{-1}$ $(a \in A)$.

Il en résulte que l'on peut retrouver pour chaque morphisme bijectif $\varphi : F \to [n]$ l'ensemble φP^{-1} des morphismes $\alpha \in \tilde{\mathcal{M}}_A(F)$ tels que $\varphi = \alpha P$. Pour ceci il suffit de considérer la suite $(B_1, \ldots, B_k)$ des files de φ et la famille Γ_φ des morphismes γ de $[n]$ dans A tels que $a\gamma^{-1}$ soit contenu dans une file, B_i, pour chaque $a \in A$. Comme les pièces d'une même file sont dans des colonnes distinctes par définition, le morphisme $\varphi\gamma = \alpha$ $(\gamma \in \Gamma_\varphi)$ est verticalement injectif et en construisant α' on vérifie directement que αP est bien égal à φ.

Nous étendons aussi aux morphismes verticalement injectifs les opérations de glissement. Etant donné un tel morphisme α, soit α' le morphisme bijectif obtenu en indexant les occurrences d'une même pièce comme expliqué plus haut. Si β' appartient à l'orbite de α', l'énoncé 5.2 montre que ses files sont les mêmes que celles de α'. Par conséquent le morphisme $\beta'\gamma' = \beta$ obtenu en oubliant les indices dans β' est verticalement injectif et a même multidegré que α. Nous dirons que β appartient à l'orbite de α. De fait on voit sans peine que chaque opération de glissement peut être réalisée directement sur α à condition d'appliquer la convention que si a' et a'' sont deux occurrences d'une même pièce a de A, l'on considère que $a' < a''$ chaque fois que a' se trouve à gauche de a''. Ainsi, par exemple, avec $A = \{a, b\}$ les deux transformations élémentaires de Knuth (cf. section 2, énoncé 2.3) deviennent

$$\begin{matrix} a & b \\ \cdot & a \end{matrix} \to \begin{matrix} b & \cdot \\ a & a \end{matrix} \quad \text{et} \quad \begin{matrix} b & b \\ \cdot & a \end{matrix} \to \begin{matrix} b & \cdot \\ a & b \end{matrix} .$$

Nous résumons cette discussion par l'énoncé suivant :

5.3. P est une projection de $\tilde{\mathcal{M}}$ sur $\mathcal{M}$ qui commute avec la correspondance R de Robinson et qui satisfait la condition que si $\alpha_1 P = \alpha_2 P$ on a $\alpha_1 = \alpha_2$ ssi α_1 et α_2 ont même multidegré.

Preuve. Le fait que P commute avec R résulte immédiatement de ce que P commute avec les glissements qui ont été définis ci-dessus pour les morphismes de $\tilde{\mathcal{M}}$.

Supposons que $\alpha_1, \alpha_2 \in \tilde{\mathcal{M}}$ soient tels que $\alpha_1 P = \alpha_2 P = \varphi$. Ainsi qu'on l'a vu, $\alpha_i = \varphi\gamma_i$ $(i = 1, 2)$ où γ_i est un morphisme de la chaîne $[n]$ $(n = \text{Card Dom } \varphi)$ dans A. Comme $|\alpha_i|_a = \text{Card}\,(a\gamma_i^{-1})$ pour chaque $a \in A$, la donnée de ces nombres détermine entièrement γ_i puisque cette application est un morphisme. Donc $|\alpha_1| = |\alpha_2|$ implique $\alpha_1 = \alpha_2$.

Q.E.D.

Une formulation plus intéressante consiste à considérer $\tilde{\mathcal{M}}_A$ comme un monoïde par rapport au produit défini dans l'introduction et généralisé de la façon indiquée plus haut. Comme P commute avec R, on peut prendre le quotient de ce monoïde par la congruence dont les classes sont les orbites et puisque l'ensemble $\tilde{\mathcal{M}}_A R = \{\alpha R : \alpha \in \tilde{\mathcal{M}}_A\}$ est une section de cette congruence d'après l'énoncé précédent, il est tolérable de désigner ce quotient par $\tilde{\mathcal{M}}_A \tilde{R}$. Autrement dit, $\tilde{\mathcal{M}}_A \tilde{R}$ désigne si l'on veut l'ensemble $\tilde{\mathcal{M}}_A R$ muni d'un produit défini par l'identité $\alpha_1 \cdot \alpha_2 = (\alpha_1\alpha_2) R$.

Dans ce qui suit on utilisera largement P et P^{-1} pour passer du cas général au cas multilinéaire (bijectif) qui est souvent plus commode à traiter. Une technique plus profonde (mais basée aussi implicitement sur la notion de file) est due à G. Thomas. L'outil essentiel est alors constitué par les opérateurs de Baxter ([18], [19]).

Soit d'autre part A^* le monoïde libre engendré par les éléments de la chaîne A (considérée comme un alphabet totalement ordonné).

THÉORÈME 5.4 (D. E. Knuth, A. Lascoux). Il existe un isomorphisme naturel (préservant les multidegrés) entre les monoïdes $\tilde{\mathcal{M}}_A\tilde{R}$ et le quotient de A^* par la congruence $\equiv$ telle que :

$$a'b'a'' \equiv b'a'a'' \quad ; \quad b'b''a' \equiv b'a'b''$$

pour tout $a', a'', b', b'' \in A$ satisfaisant $a' \leq a'' < b' \leq b''$.

Preuve. Soit $\alpha \in \tilde{\mathcal{M}}_A$. Si $\alpha P = \varphi$ et $\alpha = \varphi\gamma$, on associe à α le mot $\sigma(\alpha) = \sigma(\varphi).\gamma \in A^*$ (où $\sigma(\varphi)$ est la permutation associée à φ) qui est obtenu en lisant ces lignes successives de haut en bas. Quand $\alpha_1, \alpha_2 \in \tilde{\mathcal{M}}_A$, le mot $\sigma(\alpha_1\alpha_2)$ associé à leur produit est le produit des mots $\sigma(\alpha_1)$ et $\sigma(\alpha_2)$ associés à chacun d'eux. Ceci établit un morphisme σ préservant les multidegrés de $\tilde{\mathcal{M}}_A$ dans A^*. De fait ce morphisme est surjectif puisque l'on peut associer à chaque mot $a = a_1a_2 \ldots a_n$ $(a_j \in A)$. Le morphisme de $\tilde{\mathcal{M}}_A$ qui est le produit des morphismes α_j dont l'image est a_j et le domaine un point unique, p_j, (ces points p_j étant disposés sur une chaîne pour l'ordre croisé). Comme R commute avec les glissements, le théorème 2.4 équivaut alors à l'assertion que σ est un isomorphisme de $\tilde{\mathcal{M}}_A\tilde{R}$ sur $A^*/\equiv$ puisque les transformations élémentaires de Knuth sont celles définissant la congrence $\equiv$.

Q. E. D.

Nous désignerons désormais par $\mathbb{Z}(X)$, pour tout ensemble X, le $\mathbb{Z}$-module de base X. Si X est un monoïde $\mathbb{Z}(X)$ est une algèbre. Dans tous les cas on fera la convention habituelle de noter par la même écriture Y une partie de X et l'élément de $\mathbb{Z}(X)$ qui est la somme des membres de Y. Par exemple $\tilde{\mathcal{M}}_A(H\backslash G)$ désignera la somme dans $\mathbb{Z}(\tilde{\mathcal{M}}_A)$ des morphismes verticalement injectifs

dont l'image est contenue dans A et dont le domaine est $H\backslash G$. Dans l'énoncé suivant, F, F', G, H, H' sont trois intervalles de la famille $\hat{J}^1$ (des intervalles principaux de point minimum (1, 1)) ; les nombres $g(F, G ; H)$ sont ceux définis dans 3.7 et l'on rappelle que $g(F, G ; H) = 0$ sauf si $G, F \subset H$ et Card H = Card F + Card G.

5.5. Soient F, G et H trois intervalles de la famille $\hat{J}^1$. On a les identités suivantes dans $\mathbb{Z}(\tilde{\mathcal{M}}_A)$.

(1) $$(\tilde{\mathcal{M}}_A(H\backslash G))R = \Sigma \{g(F', G ; H) . \tilde{\mathcal{M}}_A(F') : F' \in \hat{J}^1\}$$

(2) $$(\tilde{\mathcal{M}}_A(F)\, \tilde{\mathcal{M}}_A(G))R = \Sigma \{g(F, G ; H').\tilde{\mathcal{M}}_A(H') : H' \in \hat{J}^1\} .$$

Preuve. On peut supposer $F, G \subset H$ et Card $(H\backslash G)$ = Card F = m.

Le module $\mathbb{Z}(\mathcal{M}_A)$ (des morphismes bijectifs d'image A) est un module quotient de $\mathbb{Z}(\tilde{\mathcal{M}}_A)$ obtenu en envoyant sur zéro tous les éléments dont le multidegré n'est pas $(1, 1, \ldots 1, 0, \ldots 0)$. Comme P commute avec R, il en est de même de P^{-1} et il suffit donc pour établir (1) de vérifier l'identité

(1 bis) $$(\mathcal{M}_m(H\backslash G))R = \Sigma \{g(F', G ; H)\mathcal{M}_m(F') : F' \in \hat{J}^1\}$$

et d'appliquer P^{-1} aux deux membres. L'identité (1 bis) est elle-même une simple traduction de 3.7 ainsi que nous le montrons maintenant.

Soit Λ l'ensemble des morphismes de la forme λR où $\lambda \in \mathcal{M}_m(H\backslash G)$ et F'_{λ_1} le domaine de chaque $\lambda_1 \in \Lambda$. Rappelant la notation $V(\lambda_1 ; G ; H) = \lambda_1 R^{-1} \cap \mathcal{M}_m(H\backslash G)$, $(\lambda_1 \in \Lambda)$, le membre de gauche de (1 bis) est égal à $\Sigma \{V(\lambda_1 ; G ; H)R : \lambda_1 \in \Lambda\}$.

D'après 3.7 on sait que chaque ensemble $V(\lambda_1 ; G ; H)$ contient un nom-

bre d'éléments $g(F'_{\lambda_1}, G ; H)$ qui ne dépend que du domaine de λ_1. Puisque par définition l'image par R de chacun de ses éléments est λ_1, on voit que la somme précédente est égale à

$$\Sigma \{g(F'_{\lambda_1}, G ; H)\lambda_1 : \lambda_1 \in \Lambda\} = \Sigma \{g(F, G ; H).\pi_m(F) : F \in \hat{J}^1\}$$

puisque, de plus $g(F, G ; H)$ est nul quand F n'est pas le domaine de λ_1.

L'identité (2) se vérifie de façon analogue au moyen de l'énoncé 4.5. Soient $m = \text{Card } F$, $p = \text{Card } G$ et $n = m+p$. Puisque R et P^{-1} commutent, le membre de gauche de (2) est égal à $\Sigma \{(\varphi\psi)R P^{-1} : (\varphi, \psi) \in W\}$ où W désigne l'ensemble des paires de morphismes bijectifs (φ, ψ) domaines respectifs F et G dont l'union des images est l'intervalle $[n]$. Pour chaque paire (φ, ψ) de W il existe un intervalle principal $H' \in \hat{J}^1$ et un morphisme bijectif $\chi = (\varphi\psi)R$ de domaine H'. D'après l'énoncé 4.5 on sait que pour un tel χ l'ensemble $W(F, G;\chi)$ des paires $(\varphi, \psi) \in W$ telles que $(\varphi\psi)R = \chi$ a un nombre d'éléments noté $g(F, G;H')$ qui ne dépend que de son domaine H'. Donc le membre de gauche de (2) est égal à l'expression obtenue en appliquant P^{-1} à la somme $g(F, G;H')\pi_n(H')$ étendue à tous les intervalles $H' \in \hat{J}^1$ ayant n éléments, ce qui est précisément le membre de droite de cette identité.

Q. E. D.

Soit maintenant $\mathfrak{S}_A$ l'ensemble des termes de l'algèbre quotient $\mathbb{Z}(\tilde{\pi}_A\tilde{R})$ qui ont la forme $\tilde{\pi}_A(K)$ pour un intervalle principal $K \in \hat{J}^1$ quelconque. Il est d'usage de coder K par la suite $c(K) = c_1c_2 \dots c_r$ des longueurs de ses colonnes et d'écrire $\{c_1, c_2, \dots, c_r\}$ au lieu de $\tilde{\pi}_A(K)$ quand il n'y a pas d'ambiguïté sur A. Utilisant l'isomorphisme entre les algèbres $\mathbb{Z}(\tilde{\pi}_A\tilde{R})$ et $\mathbb{Z}(A^*/\equiv)$, on trouve, par exemple, pour $A = \{a, b\}$, $K = \begin{matrix} * & \cdot \\ * & * \end{matrix}$ que $\{2, 1\} = b\,a\,a + b\,a\,b$ puisque $a\,b\,a \equiv b\,a\,a$ et $b\,b\,a \equiv b\,a\,b$.

Quand les éléments de A^* sont des variables commutatives, les termes

de la forme $\tilde{\mathfrak{m}}_A(K')$ où K' est un intervalle quelconque sont les fonctions de Schur classiques définies par K' en prenant comme définition celle fournie par le Théorème IX du chapitre X de Littlewood ([11]).

Il résulte immédiatement de la définition des morphismes verticalement injectifs que les termes $\tilde{\mathfrak{m}}_A(K)$ de $\mathfrak{S}_A$ pour lesquels le nombre des lignes de K excède Card A sont identiquement nuls (et que tous les autres sont positifs).

Par exemple si $A = \{a, b\}$ les éléments de degré au plus trois de $\mathfrak{S}_A$ sont :

$\{1\} = a + b$; $\{2\} = b\,a$; $\{11\} = a\,a + a\,b + b\,b$; $\{21\} = b\,a\,a + b\,a\,b$ ($\equiv a\,b\,a + a\,b\,b$) et $\{1, 1, 1\} = a\,a\,a + a\,a\,b + a\,b\,b + b\,b\,b$.

Pour $A = \{a, b, c\}$ on trouve, par exemple :

$\{2, 1\} = b\,a\,a + b\,a\,b + c\,a\,a + c\,a\,c + c\,b\,b + c\,b\,c + c\,a\,b + b\,a\,c$;

et $\{3\} = c\,b\,a$.

Les énoncés qui suivent constituent l'extension banale aux variables non commutatives de résultats de A. Lascoux.

THÉORÈME 5.6 . Le sous-monoïde $\mathbb{Z}(\mathfrak{S}_A)$ de $\mathbb{Z}(\tilde{\mathfrak{m}}_A\tilde{R})$ est une algèbre commutative contenant tous les termes de la forme $\tilde{\mathfrak{m}}_A(K)$ où K est un intervalle quelconque du plan, et la transposition $K \to K^T$ induit un automorphisme de $\mathbb{Z}(\mathfrak{S}_A)$.

Preuve. Tous les morphismes apparaissant dans les membres de droite des identités (1) et (2) ci-dessus ont des domaines principaux et sont donc invariants pour R . Ceci signifie que (1) et (2) sont de fait des identités dans l'algèbre quotient $\mathbb{Z}(\tilde{\mathfrak{m}}_A\tilde{R})$ et non pas seulement dans $\mathbb{Z}(\tilde{\mathfrak{m}}_A)$.

La première exprime que tout $\tilde{m}_A(K)$ où K est un intervalle quelconque appartient au module $\mathbb{Z}(\mathfrak{S}_A)$. La seconde que ce même module contient le produit de deux termes de $\mathfrak{S}_A$. Par conséquent $\mathbb{Z}(\mathfrak{S}_A)$ est une sous-algèbre de $\mathbb{Z}(\tilde{m}_A\tilde{R})$. La première égalité de l'identité (3.7 bis) signifie qu'elle est commutative puisque ses coefficients de structure satisfont l'identité $g(F, G ; H) = g(G, F ; H)$. La deuxième égalité de (3.7 bis) montre que la transposition $H \to H^T$ induit un automorphisme.

Q. E. D.

5.7. Pour chaque chaîne A, les termes non nuls de $\mathfrak{S}_A$ forment une base (indépendante) du quotient commutatif du module $(\mathfrak{S}_A)$, donc du module $\mathbb{Z}(\mathfrak{S}_A)$ lui-même.

Preuve. Pour chaque n on ordonne les intervalles principaux ayant n points par ordre lexicographique inverse de la suite (décroissante) $(\ell_1, \ldots, \ell_q)$ des longueurs de leurs lignes. Si K est l'intervalle décrit par cette suite on a $e = \tilde{m}_A(K) \neq 0$ ssi Card $A \geq q$ et, dans ce cas, la somme e contient un monôme dont le multidegré est $(\ell_1, \ldots, \ell_q)$. Ce monôme ne peut pas apparaître dans une somme de la forme $m_A(K')$ quand K' est un intervalle précédant strictement K. Par conséquent l'image de e dans le quotient commutatif de $\mathbb{Z}(\mathfrak{S}_A)$ est linéairement indépendante des images des termes qui la précèdent, ce qui établit le résultat.

Q. E. D.

5.8. En tant qu'algèbre $\mathbb{Z}(\mathfrak{S}_A)$ est engendrée par les termes correspondant aux intervalles du plan formés d'une seule colonne.

Preuve. A chaque intervalle principal H on associe la suite décroissante $c(H) = c_1 c_2 \ldots c_n$ des longueurs de ses colonnes et, pour chaque $n \geq 0$ on ordonne les intervalles ayant ce nombre de points par ordre lexicographique opposé sur cette suite. Par conséquent, avec les notations déjà utilisées, on aura

$$\{n\} < \{n-1, 1\} < \dots < \{1, 1, \dots, 1\} ,$$

en employant le même ordre pour les termes $\mathfrak{S}$ et les intervalles qui leur correspondent.

Procédant par induction sur n puis sur l'ordre $<$, on vérifie d'abord le résultat quand Card A est au moins égal à n.

Considérons un intervalle H tel que $c(H) = c_1 c_2 \dots c_r$ $(c_1 + c_2 + \dots + c_r = n)$. D'après la formule (2) du théorème 5.5 il suffit de trouver deux intervalles F et G tel que d'une part $g(F, G ; H') \neq 0$ seulement si $H' < H$ et que d'autre part $g(F, G ; H) = 1$. Pour cela définissons F et G par la condition que $c(F) = c_1 c_2 \dots c_{r-1}$ et que G soit constitué par une seule colonne de longueur c_r.

Soient $\varphi : F \to B$ et $\psi : G \to C$ deux morphismes bijectifs tels que $\{B, C\}$ soit une partition de la chaîne $[n]$. Appliquant successivement à chacune des pièces de ψ la construction de Robinson décrite au début de la section 4, on vérifie facilement que $(\varphi\psi)R$ est un morphisme dont le domaine H' est tel que si $c(H') = c'_1 c'_2 \dots c'_r$ on a $c'_i \geq c_i$ pour $i \leq r-1$ et $c'_r \leq c_r$. En effet le domaine H' doit contenir G et le nombre de ses colonnes est au plus $(r-1)+1 = r$ car, une fois introduite la première pièce de ψ (c'est-à-dire Max C) toutes les autres pièces de C sont plus petites qu'au moins une pièce figurant dans la première ligne du morphisme considéré. Donc $g(F, G ; H')$ est non nul seulement si $H' < H$. De plus, d'après la même construction on a $H' = H$ ssi C est l'ensemble des pièces figurant dans sa dernière colonne. D'après 3.7 ceci établit que $g(F, G ; H) = 1$ est par conséquent le résultat sous l'hypothèse que $m = \text{Card } A \geq n$.

Si celle-ci n'est pas satisfaite, les seuls termes non nuls de $\mathfrak{S}_A$ sont ceux pour lesquels la longueur des colonnes n'excède pas m. Si H est un tel intervalle

l'expression de $\tilde{m}_A(H)$ obtenue dans le cas général reste vraie et le résultat est donc établi dans tous les cas.

Q. E. D.

L'existence d'un automorphisme induit par la transposition implique que les "lignes" constituent aussi une base multiplicative de l'algèbre $\mathbb{Z}(\mathfrak{S}_A)$.

COROLLAIRE 5.9 . Le quotient commutatif de $\mathbb{Z}(\mathfrak{S}_A)$ est une algèbre de fonctions symétriques des variables de A .

Preuve. Ceci résulte immédiatement de l'énoncé précédent puisque quand les éléments de A commutent entre eux, chaque terme de la forme $\tilde{m}_A(G)$ où G n'a qu'une seule colonne est manifestement une fonction symétrique des éléments de A .

Q. E. D.

RÉFÉRENCES

[1] A. C. Aitken, The monomial expansion of determinental Symmetric Functions, Proc. Royal Soc. Edinburgh A 61 (1943), 300-310.

[2] E. A. Bender and D. E. Knuth, Enumeration of plane partitions, J. Combinatorial Theory (A) 13 (1972), 40-54.

[3] W. H. Burge, Four correspondences between graphs and generalized Young tableaux, J. Combinatorial Theory (A) 17 (1974), 12-30 .

[4] H. O. Foulkes, A survey of some combinatorial aspects of symmetric functions, in Permutations, A. Lentin, édit., Paris, Gauthier-Villars, 1974.

[5] C. Green, An extension of Schensted's theorem, Advances in Math. 14 (1974), 254-265.

[6] C. Green, Some partitions associated with a partially ordered set, J. Combinatorial Theory 20 (1976), 69-79.

[7] C. Green and D. J. Kleitman, The structure of Sperner k-families, J. Combinatorial Theory 20 (1976), 41-68.

[8] D.E. Knuth, Permutation matrices and generalised Young Tableaux, Pacific J. Math. 34 (1970), 709-727.

[9] D.E. Knuth, The art of computer programming, Vol. 3, Addison Wesley, 1973.

[10] A. Lascoux, Calcul de Schur dans les extensions grassmanniennes des λ-anneaux, ce volume.

[11] D.E. Littlewood, The theory of group characters, 2nd Edition, Oxford, 1950.

[12] G. de B. Robinson, On the representations of the symmetric group, American J. Math 60 (1938), 746-760.

[13] G.C. Rota, P. Doubilet et J. Stein, On the foundations of combinatorial theory IX . St udies in Applied Math. 53 (1974), 185-218.

[14] C. Schensted, Longest increasing and decreasing subsequences, Canadian J. Math. 13 (1961), 179-191.

[15] M.-P. Schützenberger, Quelques remarques sur une construction de Schensted, Math. Scand. 12 (1963), 117-128.

[16] M.-P. Schützenberger, Sur un théorème de G. de B. Robinson, C.R. Acad. Sci. Paris 272 (1971), 420-421.

[17] R.P. Stanley, Theory and application of plane partition, Studies in Applied Math. 1 (1971), 167-188 and 259-279.

[18] G.P. Thomas, Baxter algebras and Schur functions. Ph. D. Thesis, Univ. of Wales, Swansea, 1974.

[19] G.P. Thomas, Frames, Young Tableaux, and Baxter Sequences, Advances in Math. (to appear).

[20] G. Viennot, Une forme géométrique de la correspondance de Robinson-Schensted, ce volume.

M.-P. Schützenberger
97, rue du Ranelagh
75016 Paris, France

Année 1978

Bibliographie

[1] Marcel-Paul Schützenberger. Propriétés nouvelles des tableaux de Young. In *Séminaire Delange-Pisot-Poitou, 19e année : 1977/78, Théorie des nombres, Fasc. 2*, Exp. No. 26, 6 février 1978, 14 pages. Secrétariat Math., Paris, 1978.

[2] Dominique Perrin and Marcel-Paul Schützenberger. Un problème élémentaire de la théorie de l'information. In *Information theory (Proc. Internat. CNRS Colloq., Cachan, 1977) (French)*, volume 276 of *Colloq. Internat. CNRS*, pages 249–260. CNRS, Paris, 1978.

[3] Dominique Foata and Marcel-Paul Schützenberger. Major index and inversion number of permutations. *Math. Nachr.*, 83 :143–159, 1978.

[4] Alain Lascoux and Marcel-Paul Schützenberger. Sur une conjecture de H. O. Foulkes. *C. R. Acad. Sci. Paris Sér. A-B*, 286(7) :A323–A324, 1978.

[5] François Blanchard, Dominique Perrin, and Marcel-Paul Schützenberger. Une application de la théorie ergodique au problème du codage. In *Mathématiques appliquées, 1er Colloque AFCET-SMF*, pages 209–223, Tome I. Palaiseau, 1978.

Séminaire Delange-Pisot-Poitou.
Théorie des nombres

MARCEL SCHÜTZENBERGER

Propriétés nouvelles des tableaux de Young

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 19, n° 2 (1977-1978), exp. n° 26, p. 1-14.

<http://www.numdam.org/item?id=SDPP_1977-1978__19_2_A2_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
19e année, 1977/78, n° 26, 14 p.

26-01

6 février 1978

PROPRIÉTÉS NOUVELLES DES TABLEAUX DE YOUNG

par Marcel SCHÜTZENBERGER

Résumé. - Nous explicitons, par une construction sur les tableaux de Young, les coefficients des polynômes de Foulkes, qui permettent l'expression des fonctions Q de Littlewood.

1. Introduction.

Une des bases classiques de l'algèbre des fonctions symétriques (sur un ensemble arbitraire de variables qu'il est inutile de spécifier) est constituée par les fonctions de Schur, $s(J)$. Comme on le sait celles-ci sont indexées de façon bi-univoque par les partitions J de leur degré. Une autre base remarquable a été introduite par LITTLEWOOD [4]. Ces nouvelles fonctions, $Q(J)$, dépendent d'un paramètre q , et sont aussi indexées par les partitions. Elles interviennent dans la théorie des représentations des groupes linéaires finis [2] et, pour $q = -1$, dans celle de la représentation projective des groupes symétriques. On trouvera dans [5] un exposé systématique de leurs propriétés et de leurs applications.

Il existe des polynômes $F(I , J) \in \mathbb{Z}[q]$ tels que l'on ait identiquement

$$Q(I) = \sum F(I , J)\, s(J) . \tag{1}$$

Dans cette relation, la sommation porte sur l'ensemble P_n de toutes les partitions J du même entier n que I , et les $s(J)$ sont les fonctions de Schur associées à un système de variables canoniquement attachées à celles sur lesquelles sont définies les Q .

Notre regretté collègue H. O. FOULKES, auquel la théorie des fonctions symétriques est redevable de tant de beaux résultats, avait émis la conjecture [1] que les polynômes F que nous proposons d'appeler polynômes de Foulkes ont des coefficients non négatifs. Un de ses élèves, G. THOMAS l'a d'ailleurs établi pour certaines partitions I , et il était connu de FOULKES que les $F(I , J)$ constituent des q-analogues des nombres de Kostka.

Nous donnerons ici une preuve de la conjecture de Foulkes en précisant les degrés des polynômes.

Dans tout ce travail, nous appellerons partition toute application I décroissante (au sens large) de $1 , 2 , \dots , m , \dots$ dans N . La hauteur de I sera le plus grand m tel que $mI \neq 0$. On associera à I une autre application décroissante I^{Σ} par la condition que, pour chaque $m \geqslant 1$,

$$mI^{\Sigma} = \sum_{i \geqslant m} iI . \tag{2}$$

Par conséquent, $1I^{\Sigma}$ sera le poids de I , c'est-à-dire l'entier dont I est

une partition. Il est bien connu que l'ensemble P_n des partitions de poids n est muni d'un ordre naturel $\leqslant$, défini par

(3) $J \leqslant I$ si, et seulement si, $mJ^{\Sigma} \leqslant mI^{\Sigma}$ identiquement.

Notre résultat principal est résumé dans l'énoncé suivant.

THÉORÈME. - Si $J \leqslant I$, le polynôme de Foulkes $F(I ; J)$ est monique, de degré $1I^{\Sigma\Sigma} - 1J^{\Sigma\Sigma}$; dans le cas contraire, il est nul.

La preuve repose sur l'algèbre des tableaux qui joue, de par ailleurs, un certain rôle dans l'étude des groupes classiques, et consiste à attacher à chaque tableau t une valeur $t\nu \in \underset{\sim}{N}$, sa charge, de telle sorte que $F(I , J)$ soit la somme des $q^{t\nu}$ sur tous les tableaux de multidegré I et de forme J. Les définitions et les principales propriétés des tableaux sont rappelées dans la section 2. La preuve de la conjecture est effectuée dans les sections 2 et 3 en utilisant diverses propriétés de la charge qu'il est plus commode de traiter séparément, dans les sections 4 et 5 qui sont indépendantes du reste.

Notre travail a été grandement aidé par les tables étendues que notre ami C. PRECETTI a su nous établir grâce aux moyens de calcul du LA. 248, et nous l'en remercions.

2. Généralités sur les tableaux.

Dans tout ce travail, $A = \{a < b < \ldots\}$ est un alphabet totalement ordonné, et A^* le monoïde libre qu'il engendre. Soit w un mot de A^*. Son multidegré est la fonction indiquant le nombre de fois, $|w|_x$, où y figure chaque lettre x de A ; sa longueur (ou degré) est la somme $|w|$ des degrés partiels $|w|_x$. Il est commode de considérer w comme l'application dans A de son support $\{1 < 2 < \ldots < |w|\}$ envoyant chaque j sur sa j-ième lettre jw.

Un sous-mot (resp. facteur) de w est alors le mot obtenu en restreignant cette application à une partie (resp. à un sous-intervalle) de son support.

Si, et seulement si, cette application est croissante (lato sensu), w est une ligne (ce que l'on note $w \in L$). Il est clair que tout mot admet une factorisation unique en un nombre minimum de lignes. Sa forme est alors la suite des longueurs de ces dernières. Par exemple, les lignes de $w = bbacda$ sont $w_3 = bb$; $w_2 = acd$; $w_1 = a$, et la forme de w est 231. Les lignes successives seront indexées à partir de la droite (au rebours de ce qui est fait pour les lettres).

Une ligne u est minorée par une ligne v si, et seulement si,

$$|u| \leqslant |v| \quad \text{et} \quad jv < ju \quad \text{pour} \quad j = 1 , 2 , \ldots , |u| .$$

Par exemple, $u = bbcd$ est minorée par $v = aabcd$; elle ne l'est ni par $v' = aaa$ (parce que $|v'| < |u| = 4$) ni par $v'' = aacd$ (parce que $3v'' \geqslant 3u$).

Définition 2.1. - Un mot w est un tableau si, et seulement si, chacune de ses

lignes est minorée par la précédente.

On notera T l'ensemble des tableaux, et T^J le sous-ensemble de ceux dont la forme est une partition J donnée.

Cette condition équivaut à la possibilité d'écrire les lignes successives du mot les unes au-dessous des autres de telle sorte que, d'une part, l'ensemble des points occupés soit un diagramme de Ferrer et, d'autre part, que les lettres de chaque colonne soient en ordre strictement croissant. Donc, en particulier, toutes les lignes sont des tableaux, et la forme d'un tableau est une partition dont la hauteur est la longueur de la première colonne.

Par exemple : le mot cbbcdaabb est un tableau dont l'écriture plane est

```
c
b b c d
a a b b
```

(et la forme, la partition 144). Le mot bccbbaabb n'est pas un tableau à cause de sa forme (324) et il en est de même de ccbccaabb bien que sa forme (234) soit une partition, parce que sa troisième ligne (cc) n'est pas minorée par la seconde (bcc).

C'est un résultat classique (dont nous ne ferons pas usage) que la fonction de Schur $s(J)$, sur les variables de A , est la somme des images commutatives de tous les tableaux de forme J .

Par exemple, pour $A = \{a < b < c\}$, $J = 12$, il y a 8 tableaux possibles:

$$\begin{matrix} b & c & b & c & b & c & c & c \\ a\ a & a\ a & a\ b & a\ b & a\ c & a\ c & b\ b & b\ c \end{matrix}$$

et l'on obtient donc $s(12) = 2abc + \sum x^2 y$, où la sommation est étendue à toutes les paires de lettres distinctes $x , y \in A$.

Nous aurons besoin par contre de l'énoncé suivant qui est lui aussi bien connu [7], et dont la preuve est donc omise.

THÉORÈME 2.2. - Soit $\equiv$ la congruence sur A^* , définie par les relations

$$xzy \equiv zxy \quad \text{et} \quad zty \equiv tzy$$

pour toutes les lettres $x \leqslant y < z \leqslant t$ de A .

Il existe une surjection R de A^* sur l'ensemble T des tableaux telle que, si $w \in A^*$ et $t \in T$, on ait $tR = t$; $wR \equiv w$; $wR \equiv t$ si, et seulement si, $wR = t$.

Autrement dit, T est une section de la congruence $\equiv$, et R est l'opérateur de redressement associé. On notera que R préserve les multidegrés.

Remarque 2.3. - Soient $v = v_1 v_4$, $u = u_1 u_2 u_3$, deux lignes dans lesquelles u_1 (resp. $u_1 u_2$) est le plus long facteur gauche de u minorant le facteur gau-

26-04

che de même longueur v_1 (resp. un facteur droit) de v .

Le redressé $(vu)R$ est un tableau $\bar{v}\bar{u}$ dont les lignes sont $\bar{v} = v_1 g$ et $\bar{u} = u_1 f u_3$ avec $|g| = |u_2|$, $|f| = |v_4|$, et g un sous-mot de v_4 .

Si $vu \neq \bar{v}\bar{u}$, et si $v'_1 u'$ est une autre paire de lignes telle que

$$v'u' \neq (v'u')R = \bar{v}\bar{u} ,$$

on a

$$v' = v_1 v'' \quad \text{et} \quad u' = u_1 u'' ,$$

et u_1 est le plus long facteur gauche de u' minorant un facteur gauche de même longueur de v' .

Soit par exemple $v = bbcc$, $u = abcd$. On a

$$u_1 = a \ ; \ u_2 = b \ ; \ u_3 = cd \ ; \ v_1 = b \quad \text{et} \quad vuR = \begin{matrix} b & c \\ a & b \end{matrix} \ bccd .$$

Les paires (v' , u') satisfaisant les conditions de la remarque sont $(bbccd , ab)$, $(bbccc , abd)$ et $(bbc , abcd)$.

Remarque 2.4. - Soient u une ligne, et $t = t_h t_{h-1} \dots t_2 t_1$ la factorisation en lignes d'un tableau t de hauteur h . Le tableau $s = (tu)R$ a une hauteur $h' = h$ ou $h + 1$, et ses lignes successives s_i sont définies par les équations

$$(t_i v_i)R = v_{i+1} s_i , \quad v_{i+1} \text{ est une ligne,}$$

avec $v_1 = u$.

Par exemple, si

$$t = \begin{matrix} b & c & c \\ a & b & bd \end{matrix} \quad \text{et} \quad u = ab ,$$

on trouve successivement $v_2 = bd$ et $s_1 = aabb$; $v_3 = c$ et $s_2 = bbcd$; $v_4 = 1$; $s_3 = c$. Le tableau s est donc le tableau $s_3 s_2 s_1$ donné plus haut en exemple.

Il est clair que $tu = s$ quand u minore la première ligne t_1 de t .

Nous isolons aussi la remarque suivante.

Remarque 2.5. - Si $|u| \geqslant |t_1|$, et $tu \neq (tu)R = s$, on a $|s_1| > |u|$ où s_1 est la première ligne du tableau s .

En effet, posant $t_1 = v$, et utilisant les notations de la remarque 2.3, on a

$$s_1 = u_1 f u_3 ,$$

où $|f| = |v_4| = |v| - |u_1|$ est aumoins égal à $|u_2 u_3|$ puisque $|u| \geqslant |v|$ par hypothèse, et où $|u_3| > 0$ puisque tu , donc $t_1 u$, est supposé ne pas être un tableau.

3. Formule de Pieri ; suites exactes.

Soient J une partition de poids $n - m \geqslant 0$, et $m \geqslant 0$.

Définition 3.1. - $J \otimes m$ est l'ensemble des partitions H de poids n telles

que

$$\ldots \leqslant 3H \leqslant 2J \leqslant 2H \leqslant 1J \leqslant 1H \ .$$

Par exemple si $J = 123$, et $m = 2$, cet ensemble est constitué par les 7 partitions

$$125 \ ; \ 134 \ ; \ 224 \ ; \ 233 \ ; \ 1124 \ ; \ 1133 \ ; \ 1223 \ .$$

C'est celui des formes des diagrammes de Ferrer, obtenus à partir de celui de J en ajoutant un point à m de ses colonnes. Donc, de façon équivalente, $J \otimes m$ est l'ensembles des formes des tableaux qui se déduisent d'un tableau arbitraire de forme J par l'adjonction de m occurences d'une nouvelle lettre plus grande que toutes celles qui y figurent déjà. Réciproquement, si H est la forme d'un tableau t' , dont z est la plus grande lettre, et $m = |t'|_z$, la restriction de t' à $A\backslash z$ est un tableau t dont la forme J est telle que $H \in J \otimes m$.

THÉORÈME 3.2 (Formule de Pieri). - Si t est un tableau de forme J , et u une ligne de longueur m , les formes de $(tu)R$ et $(ut)R$ appartiennent à $J \otimes m$.

Réciproquement, si t' est un tableau dont la forme est dans $J \otimes m$, il existe une, et une seule, paire (t , u) constituée d'un tableau t de forme J , et d'une ligne u telle que $(tu)R = t'$; il en est de même pour l'équation $(ut)R = t'$.

Soit $n \geqslant 0$ donné. Nous désignons par M l'ensemble des paires (H , m) , où $m \leqslant n$ est un entier naturel et H une partition de $n - m$. On distingue le sous-ensemble $\bar{M}$ des paires telles que $m + 1 = 1H$, et on note M' son complément. Ce dernier contient le sous-ensemble M^0 des paires (H , m) telles que $m \geqslant 1H$.

Définition 3.3. - La suite définie par la paire $(H , m) \in M^0$ est celle des paires $(H^d , m_d) \in M$ $(d = 0 , 1 , \ldots)$ telles que $(H^0 , m_0) = (H , m)$, et pour $d \geqslant 1$,

$$m_d = dH - d \geqslant 0$$
$$kH^d = (k - 1)H - 1 \quad \text{pour} \quad k \leqslant d \ ,$$
$$kH^d = kH \qquad\quad \text{pour} \quad k > d \ ,$$

Par exemple, la suite définie par $m = 12$; $H = (2 , 4 , 6 , 6 , 9 , 9)$ est formée de (H , m) lui-même et des quatres paires suivantes correspondant à $d = 1 , 2 , 3 , 4$. Il n'en existe pas d'autre puisque $dH - d$ est négatif pour $d \geqslant 5$

$$(2 , 4 , 6 , 6 , 9 , 13 \ ; 8)$$
$$(2 , 4 , 6 , 6 , 10 , 13 \ ; 7)$$
$$(2 , 4 , 6 , 10 , 10 , 13 \ ; 3)$$
$$(2 , 4 , 7 , 10 , 10 , 13 \ ; 2)$$

LEMME d'exactitude 3.4 (cf. [3]). - L'ensemble des suites, définies par les

26-06

(H , m) de $\underset{\sim}{M}^0$, est une partition de $\underset{\sim}{M}' = \underset{\sim}{M} \setminus \bar{\underset{\sim}{M}}$.

Pour tout (H^d , d) , où $d \geqslant 1$, on a

$$m_d < dH^{d-1} = (d + 1)H - 1 < dH^d ,$$

et chaque élément de $X_d = H^d \otimes m_d$ est contenu dans un des deux ensembles analogues X_{d-1} et X_{d+1} . L'ensemble X_0 est contenu dans X_1 .

Preuve. - Soit (K , m') dans $\underset{\sim}{M}$. On lui associe la séquence de nombres formée de $m' + n = OK'$ et des n entiers naturels $jK + n - j$ $(j = 1 , 2 , \ldots , n)$. Comme K est une partition, cette séquence est strictement décroissante à partir de son deuxième terme.

Son premier terme $m' + n$, égal à un autre si, et seulement si, (K , m') , appartient au sous-ensemble exceptionnel $\bar{M}$.

Dans le cas contraire, il existe un $d \geqslant 0$ (unique !) tel que la séquence obtenue en insérant $m' + n$ entre le d-ième et le $(d + 1)$-ième terme soit strictement décroissante. Elle devient alors la séquence déduite d'une paire (H , m) de M^0 , et on vérifie que (K , m') est le d-ième terme (H^d , m_d) de la suite définie par (H , m) .

Réciproquement, cette construction redonne bien (H , m) quand on part du d-ième terme de la suite définie par un $(H , m) \in M^0$, ce qui achève la preuve de la première partie de l'énoncé.

Les inégalités suivantes résultent des définitions puisque l'on a

$$m_d = dH - d < dH^{d-1} = dH = (d + 1)H^{d+1} - 1 < dH^d = (d - 1)H + 1 .$$

Considérons pour finir un élément J de X_d . D'après les inégalités précédentes, on a

$$(d + 1)H \leqslant dJ \leqslant (d - 1)H + 1$$

en raison de la définition même de X_d . Tenant compte de ce que la suite des valeurs de $H^{(d-1)}$ (resp. H^{d+1}) ne diffère de celle de H^d que pour d (resp. pour $d + 1$), on voit que J appartient à X_{d-1} si, et seulement si, $dJ \leqslant dH$, et à X_{d+1} si, et seulement si, au contraire $dH + 1 \leqslant dJ$.

Q. E. D.

Soient I' une partition fixe de n , et $r = 1I'$. Rappelant que a est la première lettre de l'alphabet, on associe à chacune des paires (H , m) de M , considérées ci-dessus, l'ensemble $W(H)$ des mots tu de multidegré I' tels que t soit un tableau de forme H , et u une ligne : $|u| = m$, $|u|_a = r$.

On distingue, dans l'union W des $W(H)$, le sous-ensemble $\bar{W}$ de ceux pour lesquels $m + 1 = 1H$ et son complément $W' = W \setminus \bar{W}$.

Soit $w \in W'$. D'après la première partie du lemme d'exactitude, il appartient à un (et un seul) ensemble $W(H^d)$. Si, et seulement si, $wR = w$ (ce qui ne peut se

produire que pour $d = 0$), ce mot est un tableau, et nous notons $w \in W^T$. Dans le cas contraire, la formule de Pieri indique que la forme du mot redressé wR appartient à $X_d = H^d \otimes m_d$ et, d'après la dernière partie du lemme, elle appartient aussi à exactement un des deux ensembles X_{d-1} et X_{d+1} , ce que nous dénotons respectivement par $w \in W_-$ ou $w \in W_+$. En particulier, d'après la remarque 2.5, on a $w \in W_+$ quand $d = 0$.

Au total, les quatre sous-ensembles $\bar{W}$, W^T , W_- , W_+ constituent une partition de W .

PROPRIÉTÉ 3.5. - La relation $wR = w'R$ définit une bijection θ de W_+ sur W_- .

Preuve. - Supposons que $w = tu$ appartient à $W(H^d)$ et à W_+ . D'après la formule de Pieri et le lemme d'exactitude, il existe une paire (t' , u') unique telle que $wR = (t'u')R$, t' est un tableau de forme H^{d+1} , et u' est une ligne de longueur m_{d+1} . Il suffit de montrer que a^r est un facteur gauche de u' pour prouver que $w' = t'u' = w\theta$ appartient à $W(H^{d+1})$.
Soient $t_h \cdots t_1$ et $t'_{h'} \cdots t'_1$ les factorisations en lignes de t et de t' . D'après les inégalités indiquées dans le lemme précédent, on a

$$h = h' \quad \text{et} \quad |t_j| = |t'_j| \quad \text{pour tout} \quad j \geqslant d + 1 .$$

Nous effectuons le calcul de tableau $s = (tu)R = (t'u')R$ comme dans la remarque 2.4, mais en nous arrêtant au d-ième pas.

On trouve, pour $(tu)R$, que

$$s = (\bar{t}v_{d+1})R.s_d\, s_{d-1} \cdots s_1 ,$$

où $\bar{t}$ est le tableau $t_h \cdots t_{d+1}$, et une expression analogue, avec $\bar{t}'$ et v'_{d+1} pour $s = (t'u')R$. Comme on doit avoir

$$(\bar{t}v_{d+1})R = s_{h'} \cdots s_{d+1} = (\bar{t}'v'_{d+1})R$$

et que $\bar{t}$ et $\bar{t}'$ ont la même forme, la formule de Pieri montre que, de fait, $\bar{t} = \bar{t}'$ et $v_{d+1} = v'_{d+1}$.

Observons maintenant que le plus long facteur gauche u_1 , de u qui minore un facteur gauche de même longueur de la première ligne de t , admet lui-même a^r comme facteur gauche et que par conséquent $|u_1| \geqslant r$.

Par induction sur $j = 1 , 2 , \ldots , d$ on déduit de la remarque 2.3 qu'il en est de même pour la paire de ligne (v_{d+1} , s_d) , puis par induction sur $j = d,\ldots,2,1$ que chaque ligne v'_j a le même facteur gauche de longueur $|u_1|$ que v_j . Comme $v'_1 = u'$ et $v_1 = u$, ceci établit la propriété cherchée.

Par conséquent, θ est une injection de W_+ dans W_- . Un raisonnement analogue s'applique au cas où $w \in W_-$ et montre que cet ensemble est l'image de W_+ par θ .

Q. E. D.

4. Preuve de la conjecture de Foulkes.

Quand t est un tableau, on peut sans inconvénient noter $s(t)$ la fonction de Schur $s(\|t\|)$, où $\|t\|$ est la forme de t puisque celle-ci est une partition. Cette convention s'étend à tous les mots w de A^*, mais nous n'en aurons besoin que dans le cas où $w = tv$, avec t un tableau de forme K, et v une ligne de longueur $m' = n - |t|$. Supposant que $|w| = n$ et que, par conséquent, $(K , m') \in M$, on a alors :

$$s(w) = s(K , m') = 0 \quad \text{si} \quad m' + 1 = 1K ,$$

$s(w) = s(K , m') = (-1)^d s(H')$, si (K , m'), est le d-ième terme (H^d , m_d) de la suite définie en 3.3 (à partir de (H , m)).

Soient encore I' une partition fixe de n, $r = 1I'$, et I la partition de $n - r$ telle que $iI = (i + 1)I'$ identiquement. Nous nous basons sur la formule remarquable suivante, due à A. O. MORRIS [6].

LEMME 4.1.

$$Q(I') = \sum F(I , J)\, q^{m'-r}\, s(K , m') ,$$

où la sommation est étendue à l'ensemble E des triples (K , m' , J) tels que $(K , m') \in M$, $m' \geqslant r$, et $J \in K \otimes (m' - r)$.

Dans la section suivante, on définira une application $\nu : T \longrightarrow N$ (la charge), dont les propriétés utilisées ici sont rassemblées dans la proposition (5.6).

THÉORÈME 4.2. - Pour toute partition I,

$$Q(I) = \sum q^{t\nu}\, s(t) ,$$

où la sommation est étendue à tous les tableaux t de multidegré I.

Preuve. - Procédant par induction, on peut supposer le théorème établi pour $n - r$, et le lemme de Morris devient

$$Q(I') = \sum q^{t'\nu}\, q^{m'-r}\, s(K , m') ,$$

où la sommation cette fois est sur les mêmes triples (K , m' , J) de E, et pour chacun d'eux sur tous les tableaux t' de multidegré I et de forme J.

D'après la formule de Pieri, il correspond à chaque t' exactement une paire (t , v) telle que $(vt)R = t'$, t est un tableau de forme K, et v une ligne. Réciproquement, chaque semblable paire (t , v) définit un triple $(K = \|t\| , m' = |v| , J = \|(vt)R\|)$ de E défini au lemme 4.1 et un tableau $t' = (vt)R$.

On peut supposer que tous ces tableaux sont sur l'alphabet $A\backslash a$ et on obtient enfin

$$Q(I') = \sum q^{(vt)R\nu}\, q^{|v|}\, s(ta^r v) = \sum q^{(ta^r v)\nu}\, s(ta^r v)$$

où les sommations sont cette fois sur tous les mots $w = ta^r v = tu$ de l'ensemble W défini dans la section précédente, et où la deuxième égalité résulte de l'équa-

tion

$$(vt)R\nu + |v| = (ta^r\, v)\nu \ ,$$

donnée dans la proposition.

On a partitionné W en quatre ensembles à savoir, $\bar{W}$, W_+ , W_- , et l'ensemble W^T des w qui sont des tableaux.

D'après les conventions d'indexation des fonctions de Schur, la somme relative à $\bar{W}$ est nulle ; d'après ces mêmes conventions et l'existence de la bijection $\theta : W_+ \longrightarrow W_-$, il en est de même de la somme des deux suivants puisque w et $w\theta$ ont même charge (cf. Prop. 5.6). Par conséquent, $Q(I')$ se réduit à la somme sur W^T .

Q. E. D.

5. Charge.

Soient I une partition de n , A^{*I} l'ensemble des mots de multidegré I , et $\Gamma = \{\alpha < \ldots\}$ un second alphabet ordonné.

Définition 5.1. Un ordonnancement d'un mot w de A^{*I} est un mot $\bar{w}$ de $(A \times \Gamma)^*$ de même longueur tel que

1° $\bar{w}$ est envoyé sur w par la projection de $(A \times \Gamma)^*$ sur A^* ;

2° Il existe un intervalle initial F de l'ensemble ordonné $A \times \Gamma$ tel que chaque lettre de F apparaisse exactement une fois dans $\bar{w}$.

Il est clair que F est isomorphe au diagramme de Ferrer de I . Il ne dépend donc pas du choix du mot w dans A^{*I} , ni de son ordonnancement. Le multidegré de la projection de $\bar{w}$ sur Γ^* est la partition adjointe $\tilde{I}$ de I .

Par exemple, si $I = 1223$ et $w = bdacbaabc$, un des ordonnancements possibles de w serait

$$b\beta.d\alpha.a\gamma.\overline{c\beta}.\overline{b\gamma}.a\alpha.a\beta.\overline{b\alpha}.\overline{c\alpha} \ ,$$

et F peut être représenté par

$$\begin{array}{ccc} d\alpha & & \\ c\alpha & c\beta & \\ b\alpha & b\beta & \\ a\alpha & a\beta & a\gamma \ . \end{array}$$

Nous appellerons filière ζ d'un ordonnancement $\bar{w}$ le sous-mot formé des lettres dont la deuxième composante est la lettre ζ . Par exemple, la filière β est le sous-mot bca de support $\{1 , 4 , 7\}$.

Si x est une lettre de A (ou de Γ), nous désignons par x_+ (resp. x_-) son successeur (resp. prédecesseur) dans le même alphabet.

Définition 5.2. - Soit $y\eta \in F$ une lettre d'un ordonnancement $\bar{w}$. Elle est forte si, et seulement si, elle se trouve à droite de la lettre $y_-\,\eta$, et sa charge $(y\eta)\nu$ est le nombre des lettres fortes $y'\eta$, $y' \leqslant y$, de la filière η . La

charge de $\bar{w}$ est la somme des charges des lettres. De façon équivalente, $y\eta$ est forte si, et seulement si, $\bar{w}$ a le sous-mot $y\eta.y\_\eta$.

Dans l'exemple précédent, les lettres fortes sont soulignées et la table ci-dessous (indexée par les lettres de A et de Γ) donne leur charge ; celle de $\bar{w}$ est donc 7 :

$$\begin{array}{ccccc} 2 & & & & \\ 2 & 1 & & & \\ 1 & 0 & 1 & & \\ 0 & 0 & 0 & & \end{array}$$

PROPRIÉTÉ 5.3. - Le mot $w \in A^{*I}$ possède un ordonnancement unique, son relèvement $\bar{w}$, caractérisé par les conditions suivantes, pour chaque $y \in A$ et $\theta \in \Gamma$, où $x = y\_$, $\eta = \theta\_$ et où a est la première lettre de A .

1° $\bar{w}$ n'a pas de sous-mot $a\eta.a\theta$.

2° $\bar{w}$ n'a pas de sous-mot

$$y\eta.y\theta.x\eta \ , \quad y\theta.x\eta.y\eta \ , \text{ ni } \quad x\eta.y\eta.y\theta \ .$$

Preuve. - La condition 1° signifie que le sous-mot des occurences de a dans $\bar{w}$ est

$$\ldots a\gamma.a\beta.a\alpha \ .$$

Supposons par recurrence que l'on ait existence et unicité pour un intervalle initial de F contenant $x\theta$, $y\eta$, mais non $y\theta$. La condition 2° est satisfaite si l'on prend pour $y\theta$ la première occurence d'un y à gauche de $x\theta$, qui n'est pas encore affectée à une filière, si une telle occurence existe, et sinon la première occurence d'un y non encore affectée en lisant w à partir de la droite.

Définition 5.4. - La charge $w\nu$ d'un mot w est celle de son relèvement.

Le relèvement du même mot w que ci-dessus peut être obtenu par les affectations successives suivantes :

$$b.d.a\gamma.c.b.a\beta.a\alpha.b.c \ ,$$

$$b\beta.d.a\gamma.c.b\alpha.a\beta.a\alpha.b\gamma.c \ ,$$

et enfin,

$$\bar{w} = b\beta.d\alpha.a\gamma.c\alpha.b\alpha.a\beta.a\alpha.\underline{b\gamma.c\beta} \ .$$

La fonction charge est donnée par

$$\begin{array}{ccccc} 0 & & & & \\ 0 & 1 & & & \\ 0 & 0 & 1 & & \\ 0 & 0 & 0 & & \end{array}$$

et la charge de w est donc 2 .

On remarquera que lorsque $iI \leqslant 1$ identiquement, c'est-à-dire quand w est une permutation de son alphabet, sa charge est simplement son "Indice du Major" (cf. [8]).

On peut montrer que la charge d'un mot (définie par son relèvement) n'est jamais plus grande que celle définie par un autre ordonnancement et que l'on a identiquement $(x\eta)\nu \leqslant (x\eta_+)\nu$, c'est-à-dire que la fonction charge ν , associée au relèvement, est croissante (l. s.) sur F .

Ces remarques ne seront pas utilisées ici, et les preuves omises.

PROPRIÉTÉ 5.5. - Deux mots w , w' congrus mod $\equiv$ (cf. section 2) ont même charge.

Preuve. - Il suffit d'établir le résultat quand ces mots ne diffèrent que par l'une des relations élémentaires de commutation.

Soient donc $x \leqslant y < z \leqslant t$ des lettres, et d'abord $w = uxzyv$; $w' = uzxyv$, le relèvement de $\bar{w}$ étant $\bar{u}.x\xi.z\zeta.y\eta.\bar{v}$. Il résulte immédiatement de la propriété 5.3 que celui de w' est $\bar{u}.z\zeta.x\xi.y\eta.\bar{v}$ quand $z \neq x_+$ ou quand $\zeta < \xi$, les lettres fortes étant les mêmes. Maintenant si $z = x_+$ on a $y = x$ puisque $x \leqslant y < z$. De nouveau d'après la propriété 5.3, on en conclut que $\eta < \xi$, avec $\zeta \leqslant \eta$. Donc $\zeta < \xi$, ce qui établit le résultat.

Soient maintenant $w = uztyv$, $w' = uzytv$ et $\bar{w} = \bar{u}z\zeta.t\tau.y\eta.\bar{v}$.

On vérifie que si $t \neq y_+$ ou si $\tau < \eta$, le relèvement de w' ne diffère de celui de w que par l'échange des lettres $y\eta$ et $t\tau$. Supposons donc $t = y_+$, ce qui implique $z = t$, et $\tau \geqslant \eta$. On en déduit que $\zeta \geqslant \tau = \eta$ c'est-à-dire que $\bar{w} = \bar{u}.t\zeta.t\eta.y\eta.\bar{v}$ avec $\zeta > \eta$, et on trouve $\bar{w}' = \bar{u}.t\eta.y\eta.t\zeta.\bar{v}$ avec les mêmes lettres fortes.

Q. E. D.

Autrement dit, l'application charge passe au quotient :

$$\nu : A^* \longrightarrow A^*/\equiv \longrightarrow \underset{\sim}{N} .$$

PROPRIÉTÉ 5.6. - Si $w = ta^r v \in A^{*I}$, où $r = |w|_a > 0$, on a

$$w\nu - |v| = (vta^r)\nu = (vt)\nu = (vt)R\nu .$$

Preuve. - La dernière égalité résulte du théorème précédent, et la précédente de ce que l'hypothèse $|w|_a = r \geqslant |w|_b$ entraîne que les différentes occurences des b soient les mêmes dans les relèvements de w et de vt , et qu'aucune d'elles ne soit forte. Pour établir la première relation, il suffit par induction sur $|v|$ de vérifier que

$$(xta^r v')\nu - 1 = (ta^r v'x)\nu$$

quand x est une lettre $\neq a$. Notant que la règle 2° définissant les relèvements, est invariante par permutation circulaire, on voit que les relèvements de $xta^r v'$ et $ta^r v'x$ ne diffèrent que par le passage d'une lettre $x\zeta$ de la première à la dernière place. Comme $x\zeta$ est nécessairement non forte pour $xta^r v'$ et forte pour l'autre mot, le résultat est établi.

Q. E. D.

6. Tableaux extrémaux.

On note $T(I , J)$ l'ensemble des tableaux de multidegré I, et forme J, où I et J sont deux partitions du même entier n.

Si h est la hauteur de I, et si z est la h-ième lettre de l'alphabet, on voit facilement, au moyen de l'écriture plane des tableaux, qu'à chaque tableau t de $T(I , J)$ correspond un autre tableau, noté t^-, obtenu en effaçant dans t les hI occurences de z ; ainsi qu'on l'a vu précedement, la forme H de t^- satisfait la relation $J \in H \otimes hI$. Comme les occurences de z doivent être dans des colonnes différentes, il existe un plus grand indice r pour lequel $rJ \geqslant hI$, et nous dirons que les z sont en position extrémale dans t si, et seulement si, H est la partition définie par :

$$iH = iJ \qquad \text{pour} \quad i \leqslant r - 1 ;$$

$$rH = (r + 1)J + rJ - hI ;$$

$$iH = (i + 1)J \quad \text{pour} \quad i \geqslant r + 1 ;$$

Ceci permet de définir la famille des tableaux extrémaux comme la plus petite famille E contenant le tableau vide, et chaque tableau t tel que, d'une part, ses dernières lettres sont en position extrémale et, d'autre part, le tableau t^-, obtenu en effacant celles-ci, est lui-même dans E.

Par exemple, la dernière lettre d est en position extrémale dans les deux tableaux

$$t = \begin{array}{cccccc} & & & d & & \\ b & b & c & d & \text{et} & \\ a & a & a & c & & \end{array} \qquad \begin{array}{cccc} & & & d \\ b & c & c & d \\ a & a & a & b \end{array}$$

mais seul le second de ceux-ci est dans E, car c n'est pas en position extrémale dans t^-.

On rappelle que la relation d'ordre naturel entre partitions (de même poids) est définie par

$$J \leqslant I \quad \text{si, et seulement si,} \quad iJ^{\Sigma} \leqslant iI^{\Sigma} \quad \text{pour tout} \quad i \geqslant 1 .$$

6.1. - L'ensemble $T(I , J)$ est non vide si, et seulement si, $J \leqslant I$ ou, de façon équivalente, si, et seulement si, $T(I , J)$ contient un tableau extrémal. Supposant ces conditions remplies, ce tableau t est unique et sa charge est égale à $1I^{\Sigma\Sigma} - 1J^{\Sigma\Sigma}$.

Preuve. - Elle se fait par induction sur la hauteur h de I. En ce qui concerne la première assertion, il suffit de vérifier que I, J étant donnés, la forme H, décrite plus haut, est minimale (pour l'ordre naturel) parmi les partitions H' de poids $n - hI$ telles que $J \in H' \otimes hI$.

En ce qui concerne la seconde, il est clair que chaque ensemble $T(I , J)$ non vide contient au plus un tableau extrémal t. Toujours par induction sur h, on vérifie d'abord que dans son redressement les attributions des occurences de la der-

nière lettre z aux filières $\alpha < \beta < \ldots$ sont effectuées par ordre croissant en lisant les lignes de haut en bas et chaque ligne de droite à gauche. Ensuite que la charge de chacune de celles-ci est égale à la différence entre son rang h dans l'alphabet et l'indice de la ligne où se trouve cette occurence. Il en résulte facilement que la somme des charges est égale à la somme de $iI^{\Sigma} - iJ^{\Sigma}$ sur tous les $i \geqslant 1$.

Q. E. D.

Ce calcul est illustré par le tableau extrémal suivant :

$$\begin{array}{cccc} & & & d\alpha 0 \\ & & & c\alpha 0 \\ b\beta 0 & b\alpha 0 & c\beta 1 & d\beta 2 \\ a\gamma 0 & a\beta 0 & a\alpha 0 & b\gamma 1 \end{array}$$

$$I = (2\ ,\ 2\ ,\ 3\ ,\ 3)\ ;\quad I^{\Sigma} = (2\ ,\ 4\ ,\ 7\ ,\ 10)\ ;$$

$$J = (1\ ,\ 1\ ,\ 4\ ,\ 4)\qquad J^{\Sigma} = (1\ ,\ 2\ ,\ 6\ ,\ 10)\ ;$$

$1I^{\Sigma\Sigma} - 1J^{\Sigma\Sigma} = 1 + 2 + 1 = 4$ qui est bien égal à la charge du tableau.

Nous rappelons que le polynôme de Foulkes $F(I\ ,\ J)$ est la somme de $q^{t\nu}$ sur tous les tableaux t de $T(I\ ,\ J)$. Il est donc nul sauf si $J \leqslant I$.

PROPRIÉTÉ 6.2. - Supposant $J \leqslant I$, le polynôme de Foulkes est monique de degré $1I^{\Sigma\Sigma} - 1J^{\Sigma\Sigma}$.

Preuve. - Il suffit de montrer que la charge du tableau extrémal de $T(I\ ,\ J)$ est strictement plus grande que celle de tout autre tableau de ce même ensemble. Comme précédement, nous supposons ce résultat prouvé pour les partitions de hauteur strictement inférieure à celle de I .

Le tableau extrémal t est le produit d'un tableau t_1 et de sa première ligne ; cette dernière a la forme $a^s u$, où $s = 1I$, et où u est une ligne de longueur $|u| = 1J - 1I$. Soient J_1 la forme de t_1 , et I_2 la partition de $n - s$ qui est le multidegré du tableau $t_2 \equiv ut_1$.

D'après 5.6, la charge de t_2 est égale à $t\nu - |u| = c$ et, comme on le sait, sa forme appartient à $J_1 \otimes |u|$. On voit que cet ensemble contient une partition minimale unique K définie par

$$1K = 1J_1 + |u| \quad (= 2J + |u|)$$

$$iK = iJ_1 \quad (= (i + 1)J) \quad \text{pour} \quad i \geqslant 2\ ,$$

et on calcule facilement que la différence $1I_2^{\Sigma\Sigma} - 1K^{\Sigma\Sigma}$ est précisément égale à c .

Utilisant l'hypothèse d'induction, on en conclut que t_2 est le tableau extrémal de l'ensemble $T(I_2\ ,\ K)$.

Considérons maintenant un autre tableau t' de $T(I\ ,\ J)$. On a encore $t' = t'_1 a^s u'$, où t'_1 est un tableau de forme J_1 , et u' une ligne de même longueur que u ; le multidegré du tableau $t'_2 \equiv u't'_1$ est encore I_2 , sa charge

est $t'\nu - |u|$, et sa forme K' est contenue dans $J_1 \otimes |u|$.

En raison du caractère extrémal de K , on a

$$t\nu - |u| > t'\nu - |u| \quad \text{quand} \quad K' \neq K$$

et, dans le cas contraire, la même inégalité est satisfaite en raison de l'hypothèse d'induction. Q. E. D.

RÉFÉRENCES

[1] FOULKES (H. O.). - A survey of some combinatorial aspectsof symmetric functions, "Permutations", p. 79-92. - Paris, Gauthier-Villars, 1974.

[2] GREEN (J. A.). - The characters of the finite general linear groups, Trans. Amer. math. Soc., t. 80, 1955, p. 402-447.

[3] LASCOUX (A.). - Polynômes symétriques, foncteurs de Schur et grassmanniennes, Thèse Sc. math., Paris 1977.

[4] LITTLEWOOD (D. E.). - The theory of groups characters, 2nd edition. - Oxford, Clarendon Press, 1950.

[5] MORRIS (A. O.). - A survey on Hall-Littlewood functions and their applications to representation theory, "Combinatoire et représentation du groupe symétrique [1976. Strasbourg]", p. 136-154. - Berlin, Springer-Verlag, 1977 (Lecture Notes in Mathematics, 579).

[6] MORRIS (A. O.). - The characters of the group $Gl(n , q)$, Math. Z., t. 81, 1963, p. 112-123.

[7] SCHÜTZENBERGER (M. P.). - La correspondance de Robinson, "Combinatoire et représentation du groupe symétrique [1976. Strasbourg]", p. 59-113. - Berlin, Springer-Verlag, 1977 (Lecture Notes in Mathematics, 579).

[8] THOMAS (G. P.). - Further results on Baxter sequences and generalized Schur functions, "Combinatoire et représentation du groupe symétrique [1976. Strasbourg]", p. 155-167. - Berlin, Springer-Verlag, 1977 (Lecture Notes in Mathematics, 579).

(Texte reçu le 20 février 1978)

NOTE [ajoutée en septembre 1976]. - La présentation donnée ici fait partie d'un travail plus général réalisé en collaboration avec Alain LASCOUX. Les résultats ont été annoncés dans une note aux Comptes rendus :

LASCOUX (A.) et SCHÜTZENBERGER (M.-P.). - Sur une conjecture de H. O. Foulkes, C. R. Acad. Sc. Paris, t. 286, 1978, Série A, p. 323-324.

Marcel P. SCHÜTZENBERGER
97 rue du Ranelagh
75016 PARIS

Colloques Internationaux du C.N.R.S.
N° 276. -- THEORIE DE L'INFORMATION

UN PROBLEME ELEMENTAIRE DE LA THEORIE DE L'INFORMATION

D. PERRIN et M.P. SCHÜTZENBERGER

Le problème évoqué se situe dans l'hypothèse où la source est définie par une distribution de Bernouilli π sur un alphabet B et où la transmission est effectuée par une ligne sans bruit d'alphabet A. Le codage est donc simplement un morphisme injectif α du monoïde libre B^* dans le monoïde libre A^*. Si toutes les lettres de A ont le même coût, le coût moyen de la transmission, $L(\pi, \alpha)$ est simplement la longueur moyenne (par rapport à π) des mots du code $X = B\alpha$. Les inégalités classiques permettent alors de le borner inférieurement (en fonction de l'entropie de la source) et on sait que le minimum peut être atteint à l'intérieur de la sous-famille des codes préfixes (ou encore des codes X ayant un délai borné de décodage). Nous conjecturons que cette propriété remarquable reste vraie dans le cas général où les coûts des lettres de l'alphabet de transmission A sont quelconques. Cette conjecture admet une série de reformulations en langage algébrique. Nous établissons sa validité pour la sous-famille des codes X qui jouissent de la propriété d'avoir un délai de synchronisation borné.

On an elementary problem in information theory

One considers a source of information defined by an alphabet B and a Bernouilli distribution π on the the sequences over the source alphabet B; and A is the alphabet of the noiseless channel through which a transmission is realised by an encoding (with the property of unique decipherability).

If all letters in A have the same cost, the average cost of the transmission, $L(\pi, \alpha)$ is precisely the average length (with respect to π) of the code formed of the words on the alphabet A which encode the symbols from B. The classical inequalities allow an inferior bound on $L(\pi, \alpha)$, which is the entropy of the source; and it is well known that the minimum may be reached within the class of prefix codes.

We conjecture that this remarkable property remains valid in the general case, whatever be the costs of the letters from the transmission alphabet A; there is always a prefix code which does as well as any code. This conjecture admits several formulations in algebraic terms and we establish its validity for the subfamily of codes X having bounded synchronization delay.

1. INTRODUCTION

Plaçons-nous dans une situation très simple de transmission de l'information : une source émet des symboles appartenant à un ensemble B qui sont successivement codés par des mots sur un alphabet A, c'est-à-dire que l'on dispose d'une application :

$$\alpha : B \to X$$

qui à un symbole b de B associe un mot x sur l'alphabet A pris dans un ensemble X ; on suppose que l'application α réalise un codage, ce qui signifie que tout mot sur l'alphabet A s'écrit d'au plus une façon comme un produit d'éléments de X (c'est "l'unique déchiffrage") ; on dit alors que l'ensemble X est un code.

On supposera de plus, dans un souci de simplicité, que la source n'a pas de mémoire, c'est-à-dire que les apparitions successives des symboles sont indépendantes et que leur probabilité est donnée par une distribution fixe π sur l'ensemble B :

$$\pi : B \to]0,1]$$

On sait bien que, dans cette situation, le coût de la transmission est mesuré par :

$$L(\pi, \alpha) = \sum_{b \in B} |b\alpha|\ b\pi$$

qui est la longueur moyenne des mots du code $X = B\alpha$ (on note $|\ |$ la longueur d'un mot). On sait aussi que, π étant donnée, il existe un codage α rendant $L(\pi, \alpha)$ minimal et ayant la propriété que $B\alpha$ soit un code *préfixe* ; en effet la valeur de $L(\pi, \alpha)$ ne dépend que de la suite $(x_n)_{n \in N}$ donnant la distribution du nombre de mots de X de longueur n et l'on démontre facilement que toute distribution d'un code est aussi celle d'un code préfixe.

Plaçons-nous maintenant dans une situation un peu plus générale en supposant que les symboles de A ont chacun un *coût* qui intervient dans le coût de la transmission ; on dispose donc d'une application :

$$\gamma : A \to \mathbf{R}_+$$

que l'on étend à l'ensemble A^* des mots sur l'alphabet A par additivité :

$$\gamma(a_1\, a_2 \cdots a_n) = \gamma(a_1) + \gamma(a_2) + \cdots + \gamma(a_n)\,.$$

Avec ces hypothèses, le coût de la transmission devient :

$$L(\pi, \alpha, \gamma) = \sum_{b \in B} \gamma(b\alpha)\ b\pi$$

et l'on voit que le cas précédent correspond à un coût $\gamma(a)$ égal à 1 pour tout symbole a de A.

PROBLEME – Est-il possible de rendre L *minimal en choisissant un codage* α *tel que* $X = B\alpha$ *soit un code préfixe ?*

En d'autres termes, la classe des codes préfixes est-elle encore optimale du point de vue de la longueur moyenne, parmi la classe de tous les codes.

Exemple – Soit $B = \{1,2,3,4,5\}$ et $A = \{a, b\}$; si π prend la valeur 1/5 pour chaque élément de B et si

$$\gamma(a) = 3 \qquad \gamma(b) = 1$$

la valeur minimale du coût de transmission se trouve égale à 22/5 ; elle est réalisée par chacun des trois codes suivants :

$$X_0 = \{a, ba, bba, bbba, bbbb\}$$
$$X_1 = \{a, abb, ba, babb, bbb\}$$
$$X_2 = \{aa, ab, ba, bba, bbb\}$$

Les codes X_0 et X_2 sont préfixes, et on répond donc, dans ce cas, par l'affirmative au problème posé.

On peut donner au problème précédent une forme plus générale et plus algébrique que nous exposons plus loin (§ 2) ; le but de cet article est de démontrer que l'on peut répondre de façon affirmative à ce dernier problème en se restreignant à une classe de codes particulière, définie au § 3.

2. CODES

De façon plus formelle que ci-dessus, un *code* X sur l'alphabet A est un ensemble de mots sur l'alphabet A tels que toute égalité de la forme :

$$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m \quad ; \quad x_i, y_j \in X \tag{1}$$

implique $n = m$ et $x_i = y_i$ pour $i = 1, \ldots, n$. Ainsi, par exemple, l'ensemble $\{a, ab, ba\}$ n'est pas un code sur l'alphabet $A = \{a, b\}$ puisque l'on a :

$$a(ba) = (ab)a$$

On dit qu'un code X est *maximal* si et seulement si pour tout mot $z \notin X$ l'ensemble $X \cup \{z\}$ n'est plus un code. On sait que si X est un code maximal, alors pour tout mot z, il existe des mots u, v tels que uzv soit un message :

$$uzv = x_1 x_2 \cdots x_n .$$

Réciproquement si cette propriété est vraie pour tout z, et si X est fini, alors X est maximal (cf. [3] p. 94).

Les codes *préfixes* forment une classe bien conue de codes : ce sont les X tels qu'aucun élément de X ne soit un préfixe d'un autre élément de X. Dans l'exemple que nous avons donné ci-dessus, X_0 et X_2 sont des codes préfixes, mais pas X_1 ; on peut vérifier que X_1 est un code de la manière suivante : soient

$$u = a \quad ; \quad v = ba \quad ; \quad w = bb \quad ;$$

l'ensemble $Y = \{u, v, w\}$ est un code préfixe ; et les mots de X_0 peuvent s'écrire comme produits de mots de Y :

$$X_0 = \{u, v, wu, wv, ww\}$$

Si l'on considère Y comme nouvel alphabet, X_0 est un code suffixe : c'est-à-dire que ses mots lus de droite à gauche forment un code préfixe. On voit donc que le codage réalisé par X_0 est la composition d'un codage par un code préfixe suivie d'un codage par un code suffixe(1).

De plus les trois codes X_0, X_1, X_2 sont maximaux. Pour X_0 ou X_2, cela peut se démontrer en observant que pour tout mot z il existe un mot u tel que zu ait un facteur gauche dans X_0 (ce sont des "full prefix codes").

Sur ces notions de la théorie générale des codes, on pourra se reporter à [8] ou [11], ou encore [3] chap. IV (où les codes sont nommés "bases").

Maintenant nous disons que deux mots f et g sur l'alphabet A sont *commutativement équivalents* s'ils ne diffèrent que par l'ordre de leurs lettres. Formellement, on écrira

$$f \sim g$$

si et seulement si pour chaque lettre a de A, le nombre des occurrences de a dans f et g sont égaux :

$$|f|_a = |g|_a .$$

Pour deux ensembles de mots X et Y, on dira qu'ils sont commutativement équivalents s'il existe une bijection de l'un sur l'autre qui échange des mots commutativement équivalents ; formellement, on écrira :

$$X \sim Y$$

si $$X = \{x_1, x_2, \ldots, x_i, \ldots\}$$

et $$Y = \{y_1, y_2, \ldots, y_i, \ldots\} \quad \text{avec} \quad x_i \sim y_i .$$

Si X et Y sont deux codes commutativement équivalents, ils ont les mêmes paramètres numériques ; c'est-à-dire en particulier que si :

$$\gamma : A \to \mathbf{R}_+$$

est étendue à l'ensemble des mots par additivité, on aura :

$$\sum_{x \in X} \gamma(x) = \sum_{y \in Y} \gamma(y)$$

La conjecture suivante implique donc une réponse affirmative au problème posé dans l'introduction :

CONJECTURE – Tout code est commutativement équivalent à un code préfixe.

On observera par exemple que le code X_1 de l'exemple 1 est commutativement équivalent au code X_0 qui est préfixe ; en effet la bijection suivante de X_1 sur X_0 échange des mots commutativement équivalents :

(1) Il est faux que tout code puisse être obtenu par un tel procédé de surcodage utilisant seulement des codes préfixes ou suffixes. Cela est même faux des codes maximaux, comme l'a démontré Césari [1].

X_0	*a*	*ba*	*bba*	*bbba*	*bbbb*
X_1	*a*	*ba*	*abb*	*babb*	*bbbb*

Nous développons maintenant des notations et quelques résultats relatifs à l'équivalence de commutativité qui nous seront utiles dans la suite.

Notons L une partie de A*, c'est-à-dire un ensemble de mots sur l'alphabet A. Pour tout mot f de A*, on notera :

$$\lambda_L(f) = \text{Card}\ \{\ell \in L \mid f \in \ell\, A^*\}$$

qui est donc le nombre de facteurs gauches de f qui sont dans L. Pour un ensemble C de mots on écrira encore :

$$\lambda_L(C) = \sum_{f \in C} \lambda_L(f)$$

On voit que L est un code préfixe si et seulement si la fonction λ_L ne prend sur A* que les valeurs 0 ou 1.

PROPOSITION 2.1 — Une condition nécessaire et suffisante pour que L *soit commutativement équivalent à un code préfixe est que la moyenne arithmétique des valeurs de* λ_L *sur une quelconque classe* C *de l'équivalence de commutativité soit au plus égale à* 1.

Démonstration — Tout d'abord, si L est commutativement équivalent à un code préfixe X :

$$L \sim X$$

alors toute classe de commutativité contient autant de mots de L que de X. Or :

$$\lambda_L(C) = \sum_{DE \subset C} \text{Card}\,(L \cap D)\ \text{Card}\,(E)$$

où la sommation porte sur toutes les paires de classes de commutativité D, E telles que $DE \subset C$, c'est-à-dire encore sur toutes les classes D, E de mots d, e tels que :

$$de \in C\,.$$

On en déduit que

$$\lambda_L(C) = \lambda_X(C)$$

d'où la propriété.

Réciproquement, si l'inégalité

$$\lambda_L(C) \leqslant \text{Card}\,(C)$$

est vérifiée pour toute classe de commutativité C, établissons que L est commutativement équivalent à un code préfixe X. Il nous suffit de définir X par son intersection X_C avec chaque classe C ; pour la classe $C = \{1\}$ qui est

réduite au mot au vide, on prendra $X_{\{1\}} = \emptyset$ à moins que $1 \in L$ (ce qui signifie que $L = \{1\}$ puisque $\lambda_{\{1\}}(C) = \mathrm{Card}(C)$). Si l'on suppose maintenant par récurrence que les X_C sont définis pour toute classe C de mots de longueur au plus $n-1$ et que leur union est un code préfixe, on choisit une classe C de mots de longueur n et on écrit :

$$\lambda_L(C) = \sum_{DE \subset C}{}' \mathrm{Card}(L \cap D)\,\mathrm{Card}(E) + \mathrm{Card}(L \cap C)$$

où la somme Σ' porte sur tous les D, E tels que $DE \subset C$ et $C \neq D$. D'après l'hypothèse, $\lambda_L(C) \leqslant \mathrm{Card}(C)$ et donc :

$$\mathrm{Card}(L \cap C) \leqslant \mathrm{Card}(C) - \Sigma' \mathrm{Card}(X_D)\,\mathrm{Card}(E)\,.$$

On choisit alors dans C un ensemble de $\mathrm{Card}(L \cap C)$ mots pris hors de l'union des $X_D E$, que l'on définit comme X_C. On obtient ainsi un ensemble de mots de longueur au plus n qui est un code préfixe équivalent commutativement à l'ensemble des mots de L de longueur au plus n ; ceci démontre la propriété par récurrence sur n ■

REMARQUE 2.2 — On observera que la condition sur la valeur moyenne de λ_L sur une classe C peut être modifiée de façon à apparaître comme une forme plus précise de l'inégalité attribuée à Kraft et Mac Millan.

En effet, nous avons vu que :

$$\lambda_L(C) = \sum_{DE \subset C} \mathrm{Card}(L \cap D)\,\mathrm{Card}(E)\,.$$

Et l'inégalité $\lambda_L(C) \leqslant \mathrm{Card}(C)$ s'écrit donc encore :

$$\sum_{DE \subset C} \mathrm{Card}(L \cap D)\,\mathrm{Card}(E) \leqslant \mathrm{Card}(C) \tag{1}$$

Si l'on additionne membre à membre ces inégalité pour toutes les classes C de mots de longueur n, on obtient, avec $k = \mathrm{Card}(A)$:

$$\sum_{|C|=n} \sum_{DE \subset C} \mathrm{Card}(L \cap D)\,\mathrm{Card}(E) \leqslant k^n$$

d'où

$$\sum_{|D| \leqslant n} \mathrm{Card}(L \cap D)\, k^{n-|D|} \leqslant k^n$$

ou encore

$$\sum_{i=0}^{n} \mathrm{Card}(L \cap A^i)\, k^{-i} \leqslant 1 \tag{2}$$

Cette dernière inégalité est en fait un cas particulier d'une autre relation selon laquelle, si π est un morphisme multiplicatif de A^* dans l'intervalle $]0,1]$ des nombres réels, de somme 1 sur A :

$$\pi(A) = 1$$

alors, pour tout code X, on a l'inégalité :

$$\pi(X) \leqslant 1 \tag{3}$$

on démontre de plus que, pour un code X qui est fini, $\pi(X) = 1$ si et seulement si X est maximal (cf. [3], p. 231).

L'inégalité (2) correspond au cas où π prend la même valeur $1/k$ sur toutes les lettres de A. Nous ignorons s'il existe une formulation unique qui donnerait (1) et (3) comme cas particuliers.

Exemple 2.3 – Considérons un ensemble fini L de mots sur un alphabet $A = \{a, b\}$ ayant deux symboles. On suppose que tout mot dans L contient exactement une occurrence de la lettre a :

$$L \subset b^* a b^*$$

La proposition 2.1 dit, dans ce cas particulier, que L est commutativement équivalent à un code préfixe si et seulement si pour tout entier k,

$$\text{Card}\,\{b^i a b^j \in L \mid i + j \leqslant k - 1\} \leqslant k$$

cette dernière inégalité est en effet l'application de la formule (1) ci-dessus au cas où C est la classe du mot ab^{k-1}.

Ainsi la conjecture que nous avons énoncé implique en particulier qu'un tel ensemble L ne soit plus un code dès qu'il a $d + 1$ mots ou plus, où :

$$d = \max\{|\ell| \mid \ell \in L\}$$

Signalons que l'on peut montrer par une méthode d'énumération (cf. [10], théorème 3) que si $\text{Card}(L) \geqslant d + 1$, alors $L \cup \{b^d\}$ n'est pas un code.

3. SYNCHRONISATION

L'étude des algorithmes de décodage amène à poser la définition suivante : soit X un code sur l'alphabet A, on dit qu'un paire (f, g) de mots de A^* est *synchronisante* si pour tous mots p, q, la relation :

$$pfgq = x_1 x_2 \ldots x_n \quad \text{avec} \quad x_i \in X$$

implique l'existence d'un indice j, $1 \leqslant j \leqslant n$, tel que :

$$\begin{cases} pf = x_1 \ldots x_j \\ gq = x_{j+1} \ldots x_n \end{cases}$$

Intuitivement, l'apparition de la paire (f, g) au milieu d'un message permet de le couper en deux messages, indépendamment de la partie du message antérieure à f ou postérieure à g.

Exemple 3.1 – Avec le code X_2 de l'exemple du §1, la paire (ab, ab) n'est pas synchronisante ; en effet si $p = b$, $q = a$, alors

$$pfgq = (ba)(ba)(ba)$$

qui est dans X_2^* bien que ni pf, ni gq ne soient dans X_2^*. Par contre, pour tout mot g, la paire $(abba, g)$ est synchronisante car on peut vérifier que l'on a l'inclusion

$$A^* abba \subset X_2^*$$

Sur l'existence des paires synchronisantes, on pourra consulter [9]. On démontre en [15] que tout code a la même distribution de longueurs qu'un code ayant des paires synchronisantes (et on peut même choisir ce dernier préfixe).

Maintenant on dira qu'un code X a un *délai de synchronisation borné* $\leqslant s$ s'il existe un entier s tel que toute paire f, g de mots de la forme :

$$\begin{cases} f = x_1 \dots x_s \\ g = x_{s+1} \dots x_{2s}, \quad x_i \in \mathrm{X} \end{cases}$$

est une paire synchronisante.

Les codes à délai de synchronisation borné ont été étudiés en [2], [4] et [14] comme une généralisation de la notion de code "comma-free". Plus récemment, ils ont été réintroduits en [7] sous le nom de "locally parsable codes" en liaison avec la théorie des langages apériodiques ; on pourra consulter à ce sujet [13] et [5].

Enfin ces codes interviennent dans la théorie des factorisations du monoïde libre (cf. [16], [17]) qui trouve des applications à la construction des bases des algèbres de Lie libres.

Exemple 3.2 – Considérons maintenant le code X_1 de l'exemple du §1 ; il n'est pas à délai de synchronisationborné car la paire (b^{4n}, b^{4n}) n'est synchronisante pour aucun entier n. Mais le code :

$$\mathrm{Y}_1 = \mathrm{X}_1 \setminus \{b^4\} = \{a, abb, ba, babb\}$$

a un délai de synchronisation égal à 1. En effet, si (f, g) sont deux mots de Y_1, posons :

$$\begin{cases} f = b^i a b^j \\ g = b^k a b^\ell \end{cases}$$

on a alors $0 \leqslant j + k \leqslant 3$ et on peut vérifier que la valeur de $j + k$ détermine j et k suivant le tableau :

$j + k$	0	1	2	3
j	0	0	2	2
k	0	1	0	1

Cela implique que si $u f g v$ est dans X^*, alors uf et gv aussi. Restivo a démontré [12] que cette situation se produit dès que l'on a un code maximal fini $\mathrm{Y} \subset \{a, b\}^*$ et que chaque mot comporte au plus une occurrence de la lettre a.

4. RESULTAT PRINCIPAL

Nous établissons maintenant le résultat suivant :

THEOREME 4.1 – Un code ayant un délai de synchronisation borné est commutativement équivalent à un code préfixe.

Démonstration : La démonstration utilise un comptage et nécessite l'usage des séries formelles en variables non-commutatives que nous avons évité jusqu'ici. Etant donnée une partie L de A*, on notera $\underline{L}$ la série formelle à coefficients entiers :

$$\underline{L} = \sum_{f \in L} f$$

en d'autres termes $\underline{L}$ est la fonction caractéristique de L. On notera $\mathbf{Z} \ll A \gg$ l'anneau des séries à coefficients entiers dont les variables (non commutatives) sont les éléments de A ; étant donnée $S \in \mathbf{Z} \ll A \gg$, on note

$$\langle S, f \rangle$$

le coefficient du mot $f \in A^*$; c'est un élément de Z. On écrira donc :

$$S = \sum_{f \in A^*} \langle S, f \rangle f$$

Maintenant, si S est une série dont le terme constant est nul, on pose :

$$\mathrm{Log}(1 - S) = S + S^2/2 + S^3/3 + \cdots + S^n/n + \cdots$$

Soit alors X un code dont le délai de synchronisation est borné et posons :

$$T = \underline{A}^* - \underline{X}\,\underline{A}^* = (1 - \underline{X})\,\underline{A}^*$$

On aura pour tout mot $f \in A^*$: $\langle T, f \rangle = 1 - \lambda_X(f)$ où $\lambda_X(f)$ est le nombre de facteurs gauches de f dans X (cf. §2).

Ainsi, si C est une classe de commutativité, on aura :

$$\sum_{f \in C} \langle T, f \rangle = \mathrm{Card}(C) - \lambda_X(C)$$

et il nous faut donc prouver que pour toute classe C le coefficient

$$\langle T, C \rangle = \sum_{f \in C} \langle T, f \rangle$$

est positif. Calculons pour cela le logarithme de T :

$$\mathrm{Log}\, T = \mathrm{Log}\,[(1 - X)\,\underline{A}^*] ;$$

et pour toute classe de commutativité, on a (1) :

$$\langle \mathrm{Log}\, T, C \rangle = \langle \mathrm{Log}(1 - X), C \rangle + \langle \mathrm{Log}\, \underline{A}^*, C \rangle .$$

Rappelons maintenant que l'on dit que deux mots f, g de A* sont conjugués s'il existe u, v dans A* tels que :

$$f = uv ; \quad g = vu$$

cette relation est une relation d'équivalence plus fine que l'équivalence de commutativité ; considérons une classe D de conjugués comprise dans C et notons p son

(1) Quand on l'évalue sur toute une classe de commutativité, le logarithme d'un produit est la somme des logarithmes. Il suffit pour s'en convaincre de remplacer les symboles de A par des variables réelles.

exposant, c'est-à-dire l'entier p tel que tout mot de D s'écrive :

$$f = u^p$$

avec u un mot primitif c'est-à-dire qui n'est pas puissance d'un autre mot v (cf. [6] sur toutes ces questions). On sait que la classe D a exactement n/p éléments. De plus, on peut écrire :

$$\mathrm{Log}\, \underline{A}^* = -\mathrm{Log}(1 - \underline{A})$$

et on a donc :

$$\langle \mathrm{Log}\, \underline{A}^*, D \rangle = -\langle \mathrm{Log}(1 - \underline{A}), D \rangle = -\sum_{f \in D} \langle -\frac{1}{n} f, f \rangle = \frac{1}{p} .$$

Maintenant, soit X^* ne rencontre pas la classe de conjugaison D et donc :

$$\langle \mathrm{Log}(1 - \underline{X}), D \rangle + \langle \mathrm{Log}\, \underline{A}^*, D \rangle = \frac{1}{p} .$$

Soit X^* rencontre D ; posons $E = D \cap X^*$ et montrons que E est une classe de X-conjugaison, c'est-à-dire que si $f, g \in E$, il existe $u, v \in X^*$ tels que $f = uv, g = vu$. Mais si $f, g \in D$, il existe $u, v \in A^*$ tels que $f = uv$, $g = vu$ et si l'on n'avait pas $u, v \in X^*$, aucune des paires $((u, v)^n, (vu)^n)$ ne serait synchronisante. On en déduit que tous les mots de E ont même longueur m sur l'alphabet X et que E a précisément m/p éléments, d'où :

$$\langle \mathrm{Log}(1 - \underline{X}), D \rangle + \langle \mathrm{Log}\, \underline{A}^*, D \rangle = 0$$

et enfin :

$$\langle \mathrm{Log}\, T, C \rangle = \sum_{D \subset C} (\langle \mathrm{Log}(1 - \underline{X}), D \rangle + \langle \mathrm{Log}\, \underline{A}^*, D \rangle) \geqslant 0$$

Cela implique que $\langle T, C \rangle$ soit lui aussi non négatif car $T = \exp \mathrm{Log}\, T$ et que l'exponentielle n'a que des coefficients positifs ; ceci achève la preuve ■

Exemple 4.2 – Soit $A = \{a, b\}$ un alphabet à deux lettres et $X \subset A^*$ un code maximal fini tel que chaque mot comporte au plus une occurence de la lettre a :

$$X \subset b^* \cup b^* a b^* .$$

Nous avons cité (cf. exemple 3.2) le résultat de Restivo suivant lequel si n est l'entier tel que $b^n \in X$ il existe deux parties P, Q de l'ensemble $\{0, 1, \ldots, n-1\}$ telles que :

i) $X = \{b^n\} \cup \{b^p a b^q \mid p \in P, q \in Q\}$

ii) tout entier $i \in \{0, 1, \ldots, n-1\}$ s'écrit d'une façon et d'une seule comme :

$$i = p + q \quad \text{avec} \quad p \in P, q \in Q .$$

Césari(1) a donné une preuve très élégante de ce résultat qui utilise les séries formelles : soient :

$$P = \{p \in N \mid b^p a \in X\}$$
$$Q = \{q \in N \mid a b^q \in X\}$$

(1) Communication personnelle.

et notons b^{P} la série :

$$b^{\mathrm{P}} = \sum_{p \in \mathrm{P}} b^p$$

on établit alors l'égalité entre séries suivante :

$$\underline{\mathrm{A}}^* = b^{\mathrm{Q}}\, \underline{\mathrm{X}}^*\, b^{\mathrm{P}} \tag{1}$$

en effet pour tout mot $f \in \mathrm{A}^*$, il existe u et v dans A^* tels que

$$uaafaav \in \mathrm{X}^* \tag{2}$$

puisque X est un code maximal (cf. § 2). On en déduit que $f = b^q x b^p$, avec $p \in \mathrm{P}$, $x \in \mathrm{X}$ et $q \in \mathrm{Q}$; et cette écriture est unique sans quoi (2) aurait plusieurs factorisations en mots de X. Prenons maintenant les inverses des deux membres de (1) et multiplions-les ensuite par b^{P} à gauche et par b^{Q} à droite :

$$1 - \underline{\mathrm{X}} = b^{\mathrm{P}}(1 - \underline{\mathrm{A}})\, b^{\mathrm{Q}}$$

si l'on ne considère que les mots de b^*, on obtient donc :

$$1 - b^n = b^{\mathrm{P}}(1 - b)\, b^{\mathrm{Q}}$$
$$1 + \cdots + b^{n-1} = b^{\mathrm{P}}\, b^{\mathrm{Q}}$$

ce qui est équivalent à la condition (ii) ci-dessus. On en déduit alors :

$$\underline{\mathrm{X}} = b^n + b^{\mathrm{P}}\, ab^{\mathrm{Q}}$$

ce qui est la condition (i).

Il est intéressant de remarquer que si X est un tel code, alors

$$\mathrm{Y} = \mathrm{X} \cap b^* a b^*$$

est à délai de synchronisation 1, d'après le théorème de Restivo ; et qu'il est d'autre part (évidemment) équivalent commutativement au code préfixe :

$$\mathrm{Z} = \{b^i a \mid 0 \leqslant i \leqslant n - 1\}$$

qui a lui aussi un délai de synchronisation égal à 1. Nous ne savons pas s'il est toujours possible de trouver un code préfixe commutativement équivalent à un code à délai de synchronisation borné qui ait lui aussi un délai borné. Signalons seulement que cela est vrai en ce qui concerne la distribution des longueurs (cf. [14]) : pour tout code à délai de synchronisation borné, il existe un code préfixe ayant la même propriété qui a même distribution de longueurs.

REFERENCES

[1] Y. CESARI – Sur l'application du théorème de Suschkevitch à l'étude des codes rationnels complets, in *Automata, Languages and Programming*, (J. Loeckx ed.). Lecture Notes in Computer Science, Springer Verlag (1974), 342-350.

[2] W.L. EASTMAN – On the construction of comma-free codes, *IEEE Trans. on Inf. Th.*, IT-11, 2 (1965), 263-367.

[3] S. EILENBERG – *Automata, Languages and Machines*, Vol. A, Academic Press (1974).

[4] S.W. GOLOMB and B. GORDON – Codes with bounded synchronization delay, *Information and Control, 8* (1965), 355-372.

[5] K. HASHIGUCHI and N. HONDA – Properties of code events and homomorphisms over regular events, *J. Computer Syst. Sci. 12* (1976), 352-367.

[6] A. LENTIN – *Equations dans les Monoïdes Libres,* Gauthier-Villars, Paris (1972).

[7] R. Mc NAUGHTON and S. PAPERT – *Counter Free Automata,* MIT Press, Cambridge, Mass. (1971).

[8] M. NIVAT – Elements de la théorie générale des codes, in *Automata Theory* (E.R. Caianiella ed.) Academic Press (1966), 278-294.

[9] D. PERRIN – Codes asynchrones, *Bull, Soc. Math. de France,* 105, 1977, p. 385-404.

[10] D. PERRIN et M.P. SCHUTZENBERGER – Codes et sous-monoïdes possédant des mots neutres, in *Theoretical Computer Science* (H. Walter ed.) Lecture Notes in Comput. Sci. *48,* Springer Verlag (1977), 270-281.

[11] J.F. PERROT – La théorie des codes à longueur variable, in *Theoretical Computer Science,* Lecture Notes in Comput. Sci. *48,* Springer Verlag, 27-44.

[12] A. RESTIVO – On a family of codes, in *Automata, Languages and Programming* (S. Michaelson ed.) Edinburth University Press (1976), 38-44.

[13] A. RESTIVO – A combinatorial property of codes having finite synchronisation delay, *Theoretical Comput. Sci. 1* (1975), 95-101.

[14] M.P. SCHUTZENBERGER – Sur une question concernant certains sous-monoïdes libres, *C.R. Acad. Sci. Paris, 261* (1965), 2419-2420.

[15] M.P. SCHUTZENBERGER – On synchronizing prefix codes, *Information and Control 11* (1967), 396-401.

[16] M.P. SCHUTZENBERGER – On a factorization of free monoïds, *Proc. Amer. Math. Soc. 16* (1965), 21-24.

[17] G. VIENNOT – *Algèbres de Lie libres et monoïdes libres,* Thèse, Paris (1974).

Math. Nachr. 83, 143–159 (1978)

Major Index and Inversion Number of Permutations

By Dominique Foata in Strasbourg
and Marcel-Paul Schützenberger in Paris

(Eingegangen am 14. 1. 1976)

1. Introduction

Consider the fixed finite chain $[n]=\{1<2<\ldots<n\}$. With each mapping s of $[n]$ into itself one associates its *inversion number* INV s defined as the number of pairs (i,j) such that $1\leqq i<j\leqq n$ and $s(i)>s(j)$. One also defines the *down set* of s by

$$\text{DOWN } s=\{i\colon 1\leqq i\leqq n-1,\quad s(i)>s(i+1)\}\,,$$

and the *major index* MAJ s of s as the sum (possibly zero) of the elements in DOWN s.

When S is the set of all mappings s such that the sequence card $s^{-1}(j)$ $(1\leqq j\leqq n)$ has a fixed value, the generating function for the inversion number over S has a remarkably simple form (see [13] chap. 4 and [6] p. 108). Major MacMahon to whom we owe the consideration of the major index ([11] § 104) found that it has the same generating function ([10], [12]). A combinatorial proof of this theorem was obtained in [7]. Further results on these parameters are due to Carlitz ([1], [4]) and Stanley [18].

The case where S is the set of all the $n!$ permutations of $[n]$, enjoys special properties. In the present paper we restrict our attention to that case. We can then speak of the *idown set* of s, denoted by IDOWN s, and defined by

$$\text{IDOWN } s=\text{DOWN } s^{-1},$$

with s^{-1} the inverse of s in the group S. The notions of down and idown sets are classical. Carlitz [3] referred to "*patterns*" and Foulkes [8] to "*up-down*" and "*inversion sequences*". The pattern or updown sequence of s is a sequence of $(n-1)$ plus or minus signs whose i-th term is $+$ or $-$ according as $s(i)$ is greater than $s(i+1)$ or not. Our down set is simply the set of ali indices i for which the i-th term of the pattern (or up-down sequence) is a plus. Clearly, the integer i of $[n]$ belongs to IDOWN s if and only if there exists a pair (j,k) such that $1\leqq\leqq j<k\leqq n$, $s(j)=i+1$ and $s(k)=i$, that is to say, if $i+1$ is to the left of i.

For instance, with

$$s=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\7&4&9&2&6&1&5&8&3\end{pmatrix},$$

one gets the pattern $+-+-+--+$, the down set $\{1, 3, 5, 8\}$, and the idown set $\{1, 3, 5, 6, 8\}$.

Our first result is the following theorem.

Theorem 1. *There exists a bijection* $\varphi: S \to S$ *preserving* IDOWN *and exchanging* INV *and* MAJ. *In other words, one has identically*

$$\text{IDOWN } \varphi(s) = \text{IDOWN } s \quad \textit{and} \quad \text{INV } \varphi(s) = \text{MAJ } s\,.$$

Theorem 1 has two corollaries which are easily stated. For each s in S let IMAJ s be the sum of the elements in IDOWN s, just as MAJ s was the sum of the elements in DOWN s.

Corollary 1. *The three pairs of parameters* (MAJ, INV), (IMAJ, INV) *and* (IMAJ, MAJ) *have the same bivariate distribution over the* $n!$ *elements of* S.

As the distribution of the pair (IMAJ, MAJ) is symmetric by definition, the same holds for (MAJ, INV). Professor Chung C. Wang, of the University of Kentucky, has published [19] tables of the distribution of (MAJ, INV) up to $n=7$ and so observed the symmetry. A sharper form of this property is expressed in the next corollary.

Corollary 2. *There exists an involution* ψ *on* S *with the property that* $\text{INV } \psi(s) = \text{MAJ } s$ *and* $\text{MAJ } \psi(s) = \text{INV } s$ *hold identically.*

It may be pointed out that this symmetry is not be observed in general for other sets S of mappings covered by MacMahon's theorem, which only asserts that the marginal distributions of (MAJ, INV) are equal.

Let us now state our second result.

Theorem 2. *There exists an involution* $\boldsymbol{j}$ *of* S *preserving* IDOWN *and exchanging* DOWN *with its complement to* n. *In other words one has identically*

$$\text{IDOWN } \boldsymbol{j}s = \text{IDOWN } s$$

and

$$\text{DOWN } \boldsymbol{j}s = \{n - x : x \in \text{DOWN } s\}\,.$$

The two bijections φ and $\boldsymbol{j}$ involved in theorems 1 and 2 were introduced in earlier papers ([7] and [17]). Hereafter their properties will be systematically explored. The construction of $\boldsymbol{j}$ given here involves the Robinson correspondence between permutations and ordered pairs of standard Young tableaux. It would be interesting to find a proof of theorem 2 that could avoid the use of that correspondence. The constructions of φ and φ^{-1} appear in section 2. Theorem 1 and its two corollaries are proved in section 3 that also contains the construction of the involution ψ. The proof of theorem 2 will be completed in section 6.

For each s in S let us define the numerical parameters

$$\text{DES } s = \text{card DOWN } s \quad \text{and} \quad \text{IDES } s = \text{card IDOWN } s\,.$$

Of course, DES s is the number of *descents* of s. Its generating function over S is the classical Eulerian polynomial (see [3] or [14] pp. 213–216). The joint

distribution of (DES, MAJ) is its q-generalization, as was shown by Carlitz [4]. Finally, the joint distribution of (DES, IDES) was studied by Carlitz et al. [5] who obtained explicit formulas in connection with Simon Newcomb's problem. This motivates the second part of our paper in which we examine the symmetries of the joint distribution of all those statistics.

For each s in S let $V(s)$ be the 4-vector (DES s, IDES s, MAJ s, IMAJ s) and for each 4-vector v let $N(v)$ denote the number of s in S for which $V(s)=v$. We suggest that the reader has a look at tables 2 where this function is displayed for $n=3$, 4, 5 and 6, since our theorem 3 is nothing but the proof that the regularities observed there still hold for arbitrary n. The display shows sublocks corresponding to fixed values (a, b) of (DES, IDES). There are symmetries within the whole table, symmetries within each subblock, and symmetries between subblocks. More precisely notice the following facts.

(i) The symmetry along the main diagonal. It results trivially from the definition of (IDES s, IMAJ s) as (DES s^{-1}, MAJ s^{-1}), where $s \to s^{-1}$ is an involution of S. This leads to the identity

$$N(a, b, x, y)=N(b, a, y, x)\ .$$

(ii) Consider the subblock corresponding to the value (a, b) of (DES, IDES). It has one horizontal (resp. vertical) axis of symmetry, with ordinate (resp. abscissa) MAJ $=na/2$ (resp. IMAJ $=nb/2$). This suggests introducing the notation

$$N'(a, b, x', y') \quad \text{for} \quad N(a, b, x'+(na)/2, y'+(nb)/2)\ ,$$

that is to say, replacing x and y by their distances $x'=x-(na)/2$, $y'=y-(nb)/2$ to the appropriate "central values" $(na)/2$ and $(nb)/2$. One then obtains that $N'(a, b, x', y')$ depends only on the absolute values of x' and y', i.e.

$$N(a, b, x, y)=N'(a, b, \pm x', \pm y')\ .$$

(iii) The subblocks corresponding to DES $=a$, IDES $=b$, and to DES $=n-1-a$, IDES $=n-1-b$ are equal. By using the same notations in terms of the "centralized" variables this gives

$$N'(a, b, x', y')=N'(n-1-a, n-1-b, x', y')\ .$$

These remarks are summarized in the next theorem.

Theorem 3. *The following identities hold*

(i) $N(a, b, x, y)=N(b, a, y, x)$;
(ii) $N(a, b, x, y)=N'(a, b, \pm x', \pm y')$;
(iii) $N'(a, b, x', y')=N'(n-1-a, n-1-b, x', y')$.

By combining these identities one finds that each $v=(a, b, x, y)$ belongs to a set of sixteen $(=2\times 4\times 2)$ vectors for which N takes the same value. The underlying group G is the direct product of the dihedral group D_4 of order 8 by a group of two elements. In section 4 we describe a version for the dihedral group D_4. Section 5 contains the construction of the group G by means of the Robinson correspondence. Finally, the proofs of theorems 2 and 3 are completed in section 6.

2. Construction of the bijection φ

For the construction of φ it will be convenient to regard each permutation s of $[n]$ as an associative monomial or word $w=s(1)\ s(2)\ldots s(n)$ in the n distinct letters $s(1), s(2), \ldots, s(n)$. In the same manner, let $1 \leqq m \leqq n$ and $v=s(1)\ s(2)\ldots s(m)$ be a word with m distinct letters taken out of $[n]$. Denote by $\{t(1)<t(2)<\ldots<t(m)\}$ the increasing chain made of the m elements of the set $\{s(1), s(2), \ldots, s(m)\}$. Then the word v will be regarded as the permutation

$$v: t(i)\to s(i) \quad (i=1, 2, \ldots, m)$$

of the set $\{t(1), t(2), \ldots, t(m)\}$. Let $p \geqq 1$ and $w_1, w_2, \ldots, w_p$ be p non-empty words. If w is the concatenation product of $w_1, w_2, \ldots, w_p$, in this order, i.e., if $w=w_1w_2\ldots w_p$, it is said that

$$(w_1, w_2, \ldots, w_p) \text{ is a } \textit{factorization} \text{ of } w.$$

Let x be an integer and v a non-empty word. If the last letter of v is greater (resp. smaller) than x, the word v admits a unique factorization

$$(v_1y_1, v_2y_2, \ldots, v_py_p)\ ,$$

called its *x-factorization* having the following properties

(i) y_i is a letter satisfying $y_i>x$ (resp. $y_i<x$) for each $i=1, 2, \ldots, p$;

(ii) w_i is a word which is either empty, or has all its letters smaller (resp. greater) than x $(1 \leqq i \leqq p)$.

Put

$$\gamma_x(v)=y_1v_1y_2v_2\ldots y_pv_p\ .$$

(Note that $v=v_1y_1v_2y_2\ldots v_py_p$.) The bijection φ will be defined by induction on the length of the words. If w has length one, let

$$\varphi(w)=w\ .$$

If w has length at least two, write $w=vx$ with x its last letter and put

$$\varphi(vx)=\gamma_x(\varphi(v))\ x\ .$$

In other words, define $\varphi(v)$ by induction, apply γ_x to the word $\varphi(v)$ and put the letter x at the end of the transformed word $\gamma_x(\varphi(v))$.

It was proved in [7] that φ was bijective. It seems convenient for further reference to describe the effective algorithms for both φ and its inverse φ^{-1}.

Algorithm for φ. Let $w=s(1)\ s(2)\ldots s(n)$ be a permutation.

(i) Define $w_1=s(1)$; assume that w_k has been defined for some k with $1 \leqq k<n$, then

(ii) if the last letter of w_k is greater (resp. smaller) than $s\ (k+1)$, split w_k *after* each letter greater (resp. smaller) than $s\ (k+1)$; then

(iii) in each compartment of w_k determined by the splits move the last letter to the beginning; for obtaining w_{k+1} put $s(k+1)$ at the end of the transformed word; replace k by $k+1$;
(iv) if $k=n$, then $\varphi(w)=w_k$; if not, return to (ii).

For instance, the image under φ of the word $w=7\ 4\ 9\ 2\ 6\ 1\ 5\ 8\ 3$ is obtained as follows

$$\begin{aligned}
w_1&=7\ |\\
w_2&=7\ |\ 4\ |\\
w_3&=7\ |\ 4\ |\ 9\ |\\
w_4&=7\ \ 4\ |\ 9\ \ 2\ |\\
w_5&=4\ |\ 7\ |\ 2\ |\ 9\ |\ 6\ |\\
w_6&=4\ |\ 7\ \ 2\ |\ 9\ \ 6\ \ 1\ |\\
w_7&=4\ |\ 2\ |\ 7\ |\ 1\ |\ 9\ \ 6\ |\ 5\ |\\
w_8&=4\ |\ 2\ \ 7\ |\ 1\ \ 6\ |\ 9\ |\ 5\ |\ 8\ |\\
\varphi(w)=w_9&=4\ \ 7\ \ 2\ \ 6\ \ 1\ \ 9\ \ 5\ \ 8\ \ 3
\end{aligned}$$

Algorithm for φ^{-1}. Let $v=t(1)\ t(2)\ldots t(n)$; for getting $w=s(1)\ s(2)\ldots s(n)=\varphi^{-1}(v)$ apply the following procedure to v;
(i) put $v_{n-1}=t(1)\ t(2)\ldots t\,(n-1)$ and $s(n)=t(n)$; assume that the word v_k and the integers $s\,(k+1)$, $s\,(k+2),\ldots,s(n)$ have been defined for some k with $1\leqq k<n$;
(ii) if the first letter of v_k is greater (resp. smaller) than $s\,(k+1)$, split v_k *before* each letter greater (resp. smaller) than $s\,(k+1)$;
(iii) in each compartment of v_k determined by the splits move the first letter to the end; for obtaining v_{k-1} delete the last letter of the transformed word; furthermore, put $s(k)$ equal to that deleted letter;
(iv) if $k=1$ then $\varphi^{-1}(v)=s(1)\ s(2)\ldots s(n)$; if not, replace k by $k-1$ and return to instruction (ii).

For instance the image of $v=6\ 4\ 9\ 7\ 2\ 5\ 8\ 1\ 3$ under φ^{-1} is

$$\begin{aligned}
v_8&=6\ |\ 4\ |\ 9\ |\ 7\ \ 2\ |\ 5\ |\ 8\ \ 1\ .\ 3&&=s(9)\\
v_7&=6\ |\ 4\ \ 9\ |\ 2\ |\ 7\ |\ 5\ |\ 1\ .\ 8&&=s(8)\\
v_6&=6\ |\ 9\ |\ 4\ |\ 2\ |\ 7\ |\ 5\ .\ 1&&=s(7)\\
v_5&=6\ |\ 9\ \ 4\ \ 2\ |\ 7\ .\ 5&&=s(6)\\
v_4&=6\ |\ 4\ |\ 2\ \ 9\ .\ 7&&=s(5)\\
v_3&=6\ |\ 4\ |\ 9\ .\ 2&&=s(4)\\
v_2&=6\ \ 4\ .\ 9&&=s(3)\\
v_1&=6\ .\ 4&&=s(2)\\
&\ \ 6&&=s(1)\\
w=\varphi^{-1}(v)&=6\ \ 4\ \ 9\ \ 2\ \ 7\ \ 5\ \ 1\ \ 8\ \ 3
\end{aligned}$$

3. Symmetry of the distribution of the major index and inversion number

In [7] it was proved that φ was bijective and satisfied the identity

$$\text{INV } \varphi(s) = \text{MAJ } s$$

under very general conditions. Thus we only have to verify the further identity

$$\text{IDOWN } \varphi(s) = \text{IDOWN } s\ ,$$

that holds only for permutations. Let us first establish the following lemma.

Lemma 3.1. *Let $m \geqq 1$ and $w = s(1)\ s(2) \ldots s(m+1)$ be a word with $(m+1)$ distinct letters. Put $v = s(1)\ s(2) \ldots s(m)$ and $x = s(m+1)$. Then*

(i) $\text{IDOWN } vx = \text{IDOWN } v$ *if* $x = \max\{s(1), s(2), \ldots, s(m+1)\}$
$= \text{IDOWN } v \cup \{x\}$ *otherwise*;

(ii) $\text{IDOWN } \gamma_x(v) = \text{IDOWN } v$.

Proof. Assertion (i) is straightforward, for x belongs to IDOWN vx if and only if $x+1$ occurs in v, i.e. if x is not the maximum letter of vx.

Let $t = t(1)\ t(2) \ldots t(m+1)$ be the increasing rearrangement of the word $w = vx$. There so exists a unique integer l with $1 \leqq l \leqq m+1$ and $t(l) = x$. If $l = 1$, i.e. $x = \min\{s(1), s(2), \ldots, s(m+1)\}$ (resp. $l = m+1$, i.e. $x = \max\{s(1), s(2), \ldots, s(m+1)\}$), the x-factorization of v is simply $(s(1), s(2), \ldots, s(m))$. With the notations of the preceding section the v_i's are empty, $p = m$ and $y_i = s(i)$ for $i = 1, 2, \ldots, p$. Hence

$$\gamma_x(v) = v\ ,$$

and

$$\text{IDOWN } \gamma_x(v) = \text{IDOWN } v\ .$$

Assume $2 \leqq l \leqq m$. The integer $t(i)$ $(1 \leqq i \leqq m;\ i \neq l)$ belongs to IDOWN v if and only if $t(i+1)$ is to the left of $t(i)$ in v. Note that $t(l-1)$ is in neither IDOWN v, nor IDOWN $\gamma_x(v)$. Assume that $1 \leqq i \leqq m$ and $i \neq l-1, l$. If $t(i)$ and $t(i+1)$ are letters of two different factors of the x-factorization $(v_1y_1, v_2y_2, \ldots, v_py_p)$ of v, say v_jy_j and v_ky_k, they are also letters of y_jv_j and y_kv_k. Hence $t(i)$ is in IDOWN $\gamma_x(v)$ if and only if $t(i)$ belongs to IDOWN v. If $t(i)$ and $t(i+1)$ are letters of the same factor, say v_jy_j, of the x-factorization of v, neither one can be the letter y_j, for either $1 \leqq t(i) < t(i+1) < x$, or $x < t(i) < t(i+1) \leqq m+1$ must hold. Thus the mutual order of $t(i)$ and $t(i+1)$ remains the same in both v and $\gamma_x(v)$,

q. e. d.

The proof of theorem 1 is completed as follows. Let $w = vx$ be a word with final letter x. Then

$$\begin{aligned}\text{IDOWN } \varphi(w) &= \text{IDOWN } \varphi(vx) = \text{IDOWN } \gamma_x(\varphi(v))\ x \text{ (by definition of } \varphi)\\ &= \text{IDOWN } \gamma_x(\varphi(v)) \text{ or IDOWN } \gamma_x(\varphi(v)) \cup \{x\} \text{ (by lemma1 } (i))\\ &= \text{IDOWN } \varphi(v) \text{ or IDOWN } \varphi(v) \cup \{x\} \text{ (by lemma 1(ii))}\\ &= \text{IDOWN } v \text{ or IDOWN } v \cup \{x\} \text{ (by induction),}\end{aligned}$$

according as x is the maximum letter of vx or not.

Thus

$$\begin{aligned}\text{IDOWN } \varphi(w) &= \text{IDOWN } vx \text{ (by lemma 1}(i)\text{)}\\ &= \text{IDOWN } w,\end{aligned}$$

q. e. d.

Let us turn our attention to the two corollaries of theorem 1. Denote by $\boldsymbol{i}$ the involution of S that maps each s in S onto its inverse $s^{-1}=\boldsymbol{i}s$. By the very definition of INV one has

(1) $$\text{INV } \boldsymbol{i}s = \text{INV } s\ .$$

On the other hand, as IMAJ $s=$ card IDOWN s, theorem 1 implies that

(2) $$\text{IMAJ } \varphi(s) = \text{IMAJ } s\ .$$

Consider the sequence

(3) $$s \xrightarrow{\boldsymbol{i}} s_1 \xrightarrow{\varphi^{-1}} s_2 \xrightarrow{\boldsymbol{i}} s_3 \xrightarrow{\varphi} s_4 \xrightarrow{\boldsymbol{i}} s_5\ .$$

From theorem 1, (1) and (2) it follows that

$$\text{MAJ } s = \text{IMAJ } s_1 = \text{IMAJ } s_2 = \text{MAJ } s_3 = \text{INV } s_4 = \text{INV } s_5$$

$$\text{INV } s = \text{INV } s_1 = \text{MAJ } s_2 = \text{IMAJ } s_3 = \text{IMAJ } s_4 = \text{MAJ } s_5\ .$$

As every mapping occurring in (3) is bijective, the pairs (MAJ, INV), (IMAJ, INV) and (IMAJ, MAJ) are identically distributed. This proves corollary 1.

Next form the composition product $\psi=\boldsymbol{i}\varphi\boldsymbol{i}\varphi^{-1}\boldsymbol{i}$ that maps s onto s_5, as shown in (3). Direct computation shows that $\psi\psi$ is the identity map. Thus ψ is an involution of S. Furthermore

$$\text{MAJ } s = \text{INV } s_5 = \text{INV } \psi(s)\ .$$

$$\text{INV } s = \text{MAJ } s_5 = \text{MAJ } \psi(s)\ .$$

This establishes corollary 2.

4. The dihedral group $\boldsymbol{D_4}$

Denote by $\sum$ the group of all the permutations of S. Three elements of $\sum$ are now defined. First $\boldsymbol{i}$ is the *inverse* operation already introduced

$$\boldsymbol{i}\colon s \to s^{-1}\ .$$

Second $\boldsymbol{c}$ is the *complement* to $(n+1)$. If $s=s(1)\,s(2)\ldots s(n)$, then

$$\boldsymbol{c}s = (n+1-s(1))\,(n+1-s(2))\ldots(n+1-s(n))\ .$$

Finally, $\boldsymbol{r}$ sends each $s=s(1)\,s(2)\ldots s(n)$ onto its *reversal* $\boldsymbol{r}s=s(n)\ldots s(2)\,s(1)$. Direct computation shows that $\boldsymbol{r}=\boldsymbol{ici}$. The next property is stated for the sake of completeness.

Property 4.1. *The subgroup of* $\sum$ *generated by* $\{\boldsymbol{i}, \boldsymbol{c}\}$ *is isomorphic to the dihedral group* D_4 *of order* 8.

Proof. Consider the product $[n]\times[n]$, regarded as a square with the four vertices $(1,1)$, $(1,n)$, (n,n), $(n,1)$. Let Γ be the graph of a permutation s. It consists of a set of n points $(1, s(1)), (2, s(2)), \ldots, (n, s(n))$ contained in the square. When the reflection about the horizontal axis of ordinate $(n+1)/2$ (resp. about the major diagonal) is performed, the graph Γ is transformed into the graph of the permutation $\boldsymbol{c}s$ (resp. $\boldsymbol{i}s$). As those two reflections generate all the symmetries of the square and the correspondence between graphs and mappings is one-to-one, the proof of the lemma is completed, q. e. d.

Note that the following relations hold $\boldsymbol{rc}=\boldsymbol{cr}$, $\boldsymbol{ir}=\boldsymbol{ci}$, $\boldsymbol{irc}=\boldsymbol{rci}$.

Property 4.2. *For each s in S one has*

$$\text{DOWN } \boldsymbol{c}s=[n-1]\backslash\text{DOWN } s;$$

$$\text{DOWN } \boldsymbol{rc}s=n-\text{DOWN } s=\{n-i: i\in\text{DOWN } s\}\,.$$

Proof. Let $s=s(1)\,s(2)\ldots s(n)$, $\boldsymbol{c}s=s'(1)\,s'(2)\ldots s'(n)$ and $\boldsymbol{rc}s=s''(1)\,s''(2)\ldots s''(n)$, where by definition $s'(j)=n+1-s(j)$ and $s''(j)=n+1-s\,(n+1-j)$. Suppose j in DOWN s. This is equivalent with $j\in[n-1]$ and $s(j)>s\,(j+1)$, hence with $s'(j)<s'\,(j+1)$ and with $s''(j'')<s''\,(j''+1)$ where $j''=n+1-j-1$. It follows immediately that j belongs to DOWN s if and only if j belongs to $[n-1]$ and, in equivalent fashion, $j\notin$DOWN $\boldsymbol{r}s$ or $n-j\in$DOWN $\boldsymbol{rc}s$,

q. e. d.

5. The Robinson correspondence

In what follows we have to rely upon the Robinson correspondence, that establishes a bijection between our set S and a new set, say $\mathfrak{T}^{(2)}$, of the pairs of standard Young tableaux of the same shape. The reader is referred to the excellent exposition of the relevant material given in ([9], pp. 48–72) by Donald E. Knuth, of Stanford University. However our treatment will be axiomatic in the sense that nothing will be used that is not stated in the following theorem.

Theorem 4. *There exists a surjection* ROB: $S\to\mathfrak{T}$ *onto a set* $\mathfrak{T}$ *having the following properties*

(i) $s\to(\text{ROB } s, \text{ROB } \boldsymbol{i}s)$ *is injective*;
(ii) *if* $s, s'\in S$ *and* ROB $s=$ROB s',
then ROB $\boldsymbol{r}s=$ROB $\boldsymbol{r}s'$ *and* ROB $\boldsymbol{c}s=$ROB $\boldsymbol{c}s'$;
(iii) *if* $s, s'\in S$ *and* ROB $\boldsymbol{i}s=$ROB $\boldsymbol{i}s'$, *then* DOWN $s=$DOWN s';
(iv) *for each s in S there exists an element s' of S satisfying*

$$(\text{ROB } s', \text{ROB } \boldsymbol{i}s')=(\text{ROB } \boldsymbol{r}s, \text{ROB } \boldsymbol{ri}s)\,.$$

Of course, theorem 4 does not say the full truth: $\mathfrak{T}$ is indeed the set of all standard Young tableaux of order n. On $\mathfrak{T}$ there is the equivalence "to have the same shape", which is such that the mapping $s\to(\text{ROB } s, \text{ROB } \boldsymbol{i}s)$ is bijective

upon the pairs of equivalent tableaux. Furthermore, the operation $P \to P^T$ below is the *transposition*. The algorithm called "S" by KNUTH ([9], pp. 57–59) transforms each standard YOUNG tableau P into a tableau P'. Replacing each integer i in P' by $n+1-i$ yields a new tableau denoted by P^J. The transposed tableau of P^J is precisely P^F that is further introduced. The fundamental discovery that there exists a surjection ROB: $S \to \mathfrak{T}$ having property (ii) was made by ROBINSON [15]. SCHENSTED [16] proved the part of the above property concerning T, namely the first part of (ii). The remaining proofs were given in [17]. A numerical example is given at the end of section 6.

As ROB is surjective, each element of $\mathfrak{T}$ can be written as ROB s with s in S. From (ii) it follows that we may define the two mappings $P \to P^T$ and $P \to P^F$ of $\mathfrak{T}$ into itself by

$$(\text{ROB } s)^T = \text{ROB } \boldsymbol{r}s \quad \text{and} \quad (\text{ROB } s)^F = \text{ROB } \boldsymbol{c}s\ .$$

Property 5.1. *The operations T and F are involutions of $\mathfrak{T}$ that commute with each other, i.e.*

$$T^2 = F^2 = 1 \quad \textit{and} \quad TF = FT\ .$$

Proof. From $\boldsymbol{r}^2 = 1$ we deduce that

$$\text{ROB } s = \text{ROB } \boldsymbol{r}^2 s = (\text{ROB } \boldsymbol{r}s)^T = (\text{ROB } s)^{T^2}.$$

Thus $T^2 = 1$. In the same manner

$$\text{ROB } s = \text{ROB } \boldsymbol{c}^2 s = (\text{ROB } \boldsymbol{c}s)^F = (\text{ROB } s)^{F^2},$$

showing that $F^2 = 1$. Finally, from $\boldsymbol{cr} = \boldsymbol{rc}$ we get

$$\begin{aligned}(\text{ROB } s)^{TF} &= ((\text{ROB } s)^T)^F = (\text{ROB } \boldsymbol{r}s)^F = \text{ROB } \boldsymbol{cr}s \\ &= \text{ROB } \boldsymbol{rc}s = (\text{ROB } \boldsymbol{c}s)^T = ((\text{ROB } s)^F)^T = (\text{ROB } s)^{FT}\ .\end{aligned}$$

Thus $TF = FT$, q.e.d.

Next put $J = FT$. Clearly J is involutive and commutes with T. Let $\mathfrak{T}^{(2)}$ be the set of all ordered pairs (ROB s, ROB $\boldsymbol{i}s$) where s runs over all of S.

Property 5.2. *If (P, Q) belongs to $\mathfrak{T}^{(2)}$ then the following three pairs*

$$(Q, P), \quad (P, Q^J), \quad (P^T, Q^T)$$

also belong to $\mathfrak{T}^{(2)}$.

Proof. Let s be the element of S with $= (P, Q) = (\text{ROB } s,\ \text{ROB } \boldsymbol{i}s)$. Then $(Q, P) = (\text{ROB } \boldsymbol{i}s,\ \text{ROB } \boldsymbol{ii}s)$ also belongs to $\mathfrak{T}^{(2)}$ according to theorem 4 (i). Next consider the pair $(\text{ROB } s,\ (\text{ROB } \boldsymbol{i}s)^J)$. As $\boldsymbol{rci} = \boldsymbol{rir}$, we get

$$(\text{ROB } \boldsymbol{i}s)^J = (\text{ROB } \boldsymbol{i}s)^{FT} = \text{ROB } \boldsymbol{rci}s = \text{ROB } \boldsymbol{rir}s\ .$$

Hence $(\text{ROB } s,\ (\text{ROB } \boldsymbol{i}s)^J) = (\text{ROB } \boldsymbol{rr}s,\ \text{ROB } \boldsymbol{rir}s)$. From theorem 4 (iv) there exists an element s' of S with the property that

$$(\text{ROB } \boldsymbol{rr}s,\ \text{ROB } \boldsymbol{rir}s) = (\text{ROB } s',\ \text{ROB } \boldsymbol{i}s')\ ,$$

that is, $(\text{ROB } s,\ (\text{ROB } \boldsymbol{i}s)^J)$ belongs to $\mathfrak{T}^{(2)}$. Finally $(P^T, Q^T) = (\text{ROB } \boldsymbol{r}s,\ \text{ROB } \boldsymbol{ri}s)$ is also in $\mathfrak{T}^{(2)}$ according to theorem 4 (iv), q.e.d.

We can then define the following operations on $\mathfrak{T}^{(2)}$

$$\boldsymbol{i}'(P,Q)=(Q,P);\quad \boldsymbol{j}'(P,Q)=(P,Q^J);\quad \boldsymbol{t}'(P,Q)=(P^T,Q^T)\,.$$

Let G' be the subgroup of the permutation group acting on $\mathfrak{T}^{(2)}$ that is generated by $\{\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{t}'\}$. The relations

$$\boldsymbol{i}'^2=\boldsymbol{j}'^2=\boldsymbol{t}'^2=(\boldsymbol{i}'\boldsymbol{j}')^4=1,\quad \boldsymbol{i}'\boldsymbol{t}'=\boldsymbol{t}'\boldsymbol{i}',\quad \boldsymbol{j}'\boldsymbol{t}'=\boldsymbol{t}'\boldsymbol{j}'$$

follow immediately from the above definition for $\boldsymbol{i}',\boldsymbol{j}',\boldsymbol{t}'$ and property 5.1. The CAYLEY diagram of the group G' is shown in figure 1.

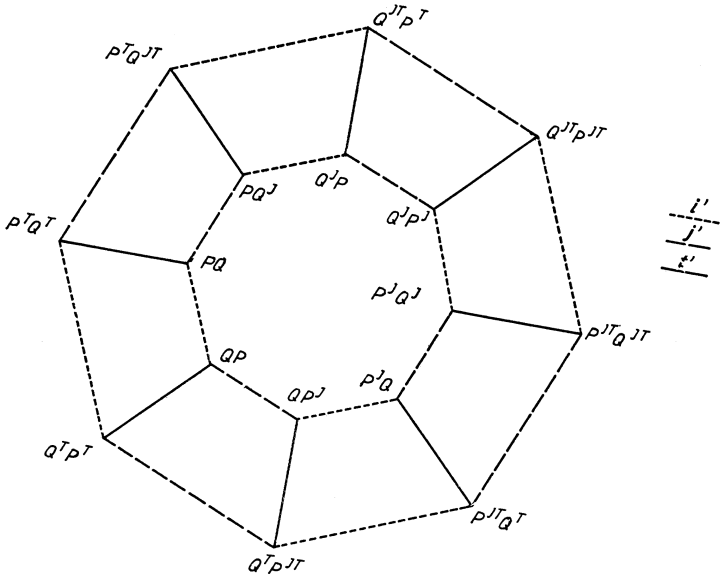


fig. 1

Clearly G' is the direct product of the dihedral group D_4 (generated by $\{\boldsymbol{i}',\boldsymbol{j}'\}$) by the group of two elements $\{1,\boldsymbol{t}'\}$.

From theorem 4 (iii) it also follows that we may define a mapping $\triangle$ of $\mathfrak{T}$ into $2^{[n-1]}$ by

$$\Delta(\mathrm{ROB}\ \boldsymbol{i}s)=\mathrm{DOWN}\ s\,.$$

Hence, we get

$$\Delta(\mathrm{ROB}\ s)=\mathrm{IDOWN}\ s\,.$$

Property 5.3. *For each Q in $\mathfrak{T}$ one has*

$$\Delta(Q^J)=n-\Delta(Q)$$
$$\Delta(Q^T)=[n-1]\backslash\Delta(Q)\,.$$

Proof. Let s be such that ROB $\boldsymbol{is}=Q$. Then $(\text{ROB } \boldsymbol{is})^J=(\text{ROB } \boldsymbol{is})^{FT}=$ $=\text{ROB } \boldsymbol{rcis}=\text{ROB } \boldsymbol{ircs}$. Hence $\Delta(Q^J)=\text{DOWN } \boldsymbol{rcs}=n-\text{DOWN } s$ according to property 4.2. Thus $\Delta(Q^J)=n-\Delta(Q)$.

In the same manner

$$(\text{ROB } \boldsymbol{is})^T=\text{ROB } \boldsymbol{ris}=\text{ROB } \boldsymbol{ics}\ .$$

Again, from property 4.2

$$\Delta(Q^T)=\Delta(\text{ROB } \boldsymbol{ics})=\text{DOWN } \boldsymbol{cs}=[n-1]\backslash\text{DOWN } s$$
$$=[n-1]\backslash\Delta(Q)\ , \qquad \text{q.e.d.}$$

6. Proofs of theorems 2 and 3

From theorem (i) and the very definition of $\mathfrak{T}^{(2)}$ the mapping

$$\varrho\colon s\to(\text{ROB } s, \text{ROB } \boldsymbol{is})$$

is a bijection of S onto $\mathfrak{T}^{(2)}$. Let

$$\boldsymbol{j}=\varrho^{-1}\boldsymbol{j}'\varrho \quad \text{and} \quad \boldsymbol{t}=\varrho^{-1}\boldsymbol{t}'\varrho\ .$$

As $\boldsymbol{i}=\varrho^{-1}\boldsymbol{i}'\varrho$, we see that the subgroup G of Σ generated by $\{\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{t}\}$ is isomorphic to G'. In particular, the following relations hold

$$\boldsymbol{i}^2=\boldsymbol{j}^2=\boldsymbol{t}^2=(\boldsymbol{ij})^4=1, \quad \boldsymbol{it}=\boldsymbol{ti}, \quad \boldsymbol{jt}=\boldsymbol{tj}\ .$$

Also the group G contains the dihedral group D_4 generated by $\{\boldsymbol{i}, \boldsymbol{c}\}$, since we can easily verify the following relations

$$\boldsymbol{r}=\boldsymbol{tj}=\boldsymbol{jt} \quad \text{and} \quad \boldsymbol{c}=\boldsymbol{ijti}\ .$$

In fact, if $\varrho(s)=(P, Q)$, we have the relations

$$\varrho(\boldsymbol{r}s)=(P^T, Q^{JT}) \quad \text{and} \quad \varrho(\boldsymbol{c}s)=(P^{JT}, Q^T)\ .$$

Let us now complete the proof of theorem 2. With s in S we get

$$\varrho(\boldsymbol{j}s)=(\text{ROB } s, (\text{ROB } \boldsymbol{is})^J)\ .$$

Hence

$$\text{IDOWN } \boldsymbol{j}s=\Delta(\text{ROB } \boldsymbol{j}s)=\Delta(\text{ROB } s)=\text{IDOWN } s\ .$$

Thus the involution $\boldsymbol{j}$ preserves IDOWN. Furthermore

$$\text{DOWN } \boldsymbol{j}s=\Delta(\text{ROB } \boldsymbol{ij}s)=\Delta((\text{ROB } \boldsymbol{is})^J)\ .$$

From property 5.3 it then follows that

$$\text{DOWN } \boldsymbol{j}s=n-\Delta(\text{ROB } \boldsymbol{is})=n-\text{DOWN } s\ .$$

This completes the proof of theorem 2.

Property 6.1. *For each s in S the following identities hold*

$$\text{DOWN } \boldsymbol{t}s=[n-1]\backslash\text{DOWN } s$$
$$\text{IDOWN } \boldsymbol{t}s=[n-1]\backslash\text{IDOWN } s\ .$$

Proof. Again property 5.3 implies that

$$\text{DOWN } \boldsymbol{t}s = \Delta(\text{ROB } \boldsymbol{it}s) = \Delta((\text{ROB } \boldsymbol{i}s)^T = [n-1]\backslash\Delta(\text{ROB } \boldsymbol{i}s)$$
$$= [n-1]\backslash\text{DOWN } s\ .$$

Also $\text{IDOWN } \boldsymbol{t}s = \text{DOWN } \boldsymbol{it}s = \text{DOWN } \boldsymbol{ti}s = [n-1]\backslash\text{DOWN } \boldsymbol{i}s = [n-1]\backslash\text{IDOWN } s$ q.e.d

We are now ready to prove theorem 3. Recall that $N(a, b, x, y)$ is the set of all s in S with $\text{DES } s = a$, $\text{IDES } s = b$, $\text{MAJ } s = x$, $\text{IMAJ } s = y$. Clearly the involution $\boldsymbol{i}: s \to s^{-1}$ of S maps in a one-to-one manner each set

$$\{s \in S: \text{DES } s = a, \text{IDES } s = b, \text{MAJ } s = x, \text{IMAJ } s = y\}$$

onto the set

$$\{s \in S: \text{DES } s = b, \text{IDES } s = a, \text{MAJ } s = y, \text{IMAJ } s = x\}\ .$$

This proves the first identity $N(a, b, x, y) = N(b, a, y, x)$.

Now remember that $\text{DES } s$ (resp. $\text{IDES } s$) is the number of elements in $\text{DOWN } s$, while $\text{MAJ } s$ (resp. $\text{IMAJ } s$) is the sum of the elements in $\text{DOWN } s$ (resp. $\text{IDOWN } s$). It then follows from theorem 2 that

$$\text{IDES } \boldsymbol{j}s = \text{IDES } s \quad \text{and} \quad \text{IMAJ } \boldsymbol{j}s = \text{IMAJ } s\ .$$

Also

$$\text{DES } \boldsymbol{j}s = \text{DES } s$$

and

$$\text{MAJ } \boldsymbol{j}s = \Sigma\{n - x: x \in \text{DOWN } s\} = n\ \text{DES } s - \text{MAJ } s\ .$$

Thus the involution $\boldsymbol{j}$ maps each set

$$\{s \in S: \text{DES } s = a, \text{IDES } s = b, \text{MAJ } s = x, \text{IMAJ } s = y\}$$

onto

$$\{s \in S: \text{DES } s = a, \text{IDES } s = b, \text{MAJ } s = na - x, \text{IMAJ } s = y\}\ ,$$

which establishes the identity

$$N(a, b, x, y) = N(a, b, na - x, y).$$

Hence

$$N'(a, b, x', y') = N'(a, b, -x', y').$$

Combining with the first identity of theorem 3 gives

$$N'(a, b, x', y') = N'(a, b, \pm x', \pm y').$$

The last identity of theorem 3 is a consequence of property 6.2. We have

$$\text{DES } \boldsymbol{t}s = n - 1 - \text{DES } s; \quad \text{IDES } \boldsymbol{t}s = n - 1 - \text{IDES } s\ .$$

Also, as the sum of the elements in $[n-1]$ is $n\,(n-1)/2$ we deduce

$$\text{MAJ } \boldsymbol{t}s = n\,(n-1)/2 - \text{MAJ } s \quad \text{and} \quad \text{IMAJ } \boldsymbol{t}s = n\,(n-1)/2 - \text{IMAJ } s\ .$$

Thus the identity

$$N(a, b, x, y) = N(n-1-a,\ n-1-b,\ n\,(n-1)/2-x,\ n\,(n-1)/2-y)$$

holds, as well as the identities

$$N'(a, b, x', y') = N'(n-1-a,\ n-1-b,\ -x',\ -y')$$

and

$$N'(a, b, x', y') = N'(n-1-a,\ n-1-b,\ x',\ y')$$

because of theorem 3 (ii).

Example 6.2, Consider the two standard YOUNG tableaux of order 5

$$P = \begin{array}{|c|c|c|c|c|}\hline 3 & 4 \\ \hline 1 & 2 & 5 \\ \hline \end{array} \qquad Q = \begin{array}{|c|c|c|c|c|}\hline 2 & 4 \\ \hline 1 & 3 & 5 \\ \hline \end{array}$$

As mentioned in the beginning of section 5 the two tableaux P^J and Q^J are obtained by first applying algorithm "S" (as described in [9], pp. 57 – 59) to P and Q, then replacing each integer i by $6-i$:

$$P^J = \begin{array}{|c|c|c|c|c|}\hline 4 & 5 \\ \hline 1 & 2 & 3 \\ \hline \end{array} \qquad Q^J = \begin{array}{|c|c|c|c|c|}\hline 3 & 5 \\ \hline 1 & 2 & 4 \\ \hline \end{array}$$

Hence

$$P^T = \begin{array}{|c|c|c|}\hline 5 \\ \hline 2 & 4 \\ \hline 1 & 3 \\ \hline \end{array} \qquad Q^T = \begin{array}{|c|c|c|}\hline 5 \\ \hline 3 & 4 \\ \hline 1 & 2 \\ \hline \end{array} \qquad P^{JT} = \begin{array}{|c|c|c|}\hline 3 \\ \hline 2 & 5 \\ \hline 1 & 4 \\ \hline \end{array} \qquad Q^{JT} = \begin{array}{|c|c|c|}\hline 4 \\ \hline 2 & 5 \\ \hline 1 & 3 \\ \hline \end{array}$$

When the group G' acts on the above pair (P, Q) we get the sixteen pairs of tableaux of figure 1. Each of these pairs is associated under the inverse ϱ^{-1} of the Robinson correspondence (see [9], p. 52) with a permutation of $\{1, 2, 3, 4, 5\}$, as shown in the next table.

Table 1.

tableaux	permutations	tableaux	permutations
$PQ = \varrho(s)$	$s = 3\ 1\ 4\ 2\ 5$	P^TQ^T	$ts = 2\ 5\ 1\ 4\ 3$
PQ^J	$js = 3\ 4\ 1\ 5\ 2$	P^TQ^{JT}	$rs = 5\ 2\ 4\ 1\ 3$
P^JQ	$4\ 1\ 5\ 2\ 3$	$P^{JT}Q^T$	$cs = 3\ 5\ 2\ 4\ 1$
P^JQ^J	$1\ 4\ 2\ 5\ 3$	$P^{JT}Q^{JT}$	$3\ 2\ 5\ 1\ 4$
QP	$is = 2\ 4\ 1\ 3\ 5$	Q^TP^T	$3\ 1\ 5\ 4\ 2$
Q^JP	$3\ 5\ 1\ 2\ 4$	$Q^{JT}P^T$	$4\ 2\ 5\ 3\ 1$
QP^J	$2\ 4\ 5\ 1\ 3$	Q^TP^{JT}	$5\ 3\ 1\ 4\ 2$
Q^JP^J	$1\ 3\ 5\ 2\ 4$	$Q^{JT}P^{JT}$	$4\ 2\ 1\ 5\ 3$

Note that DOWN $s = \{1, 3\}$

$$\text{DOWN } js = \{2, 4\} = 5 - \{1, 3\}$$

and

$$\text{IDOWN } s = \text{IDOWN } js = \{2\}\ .$$

Tables 2 show the distribution of the vector $V = (\mathrm{DES}, \mathrm{MAJ}, \mathrm{IDES}, \mathrm{IMAJ})$ over the $n!$ permutations of $[n]$ for $n = 3, 4, 5, 6$.

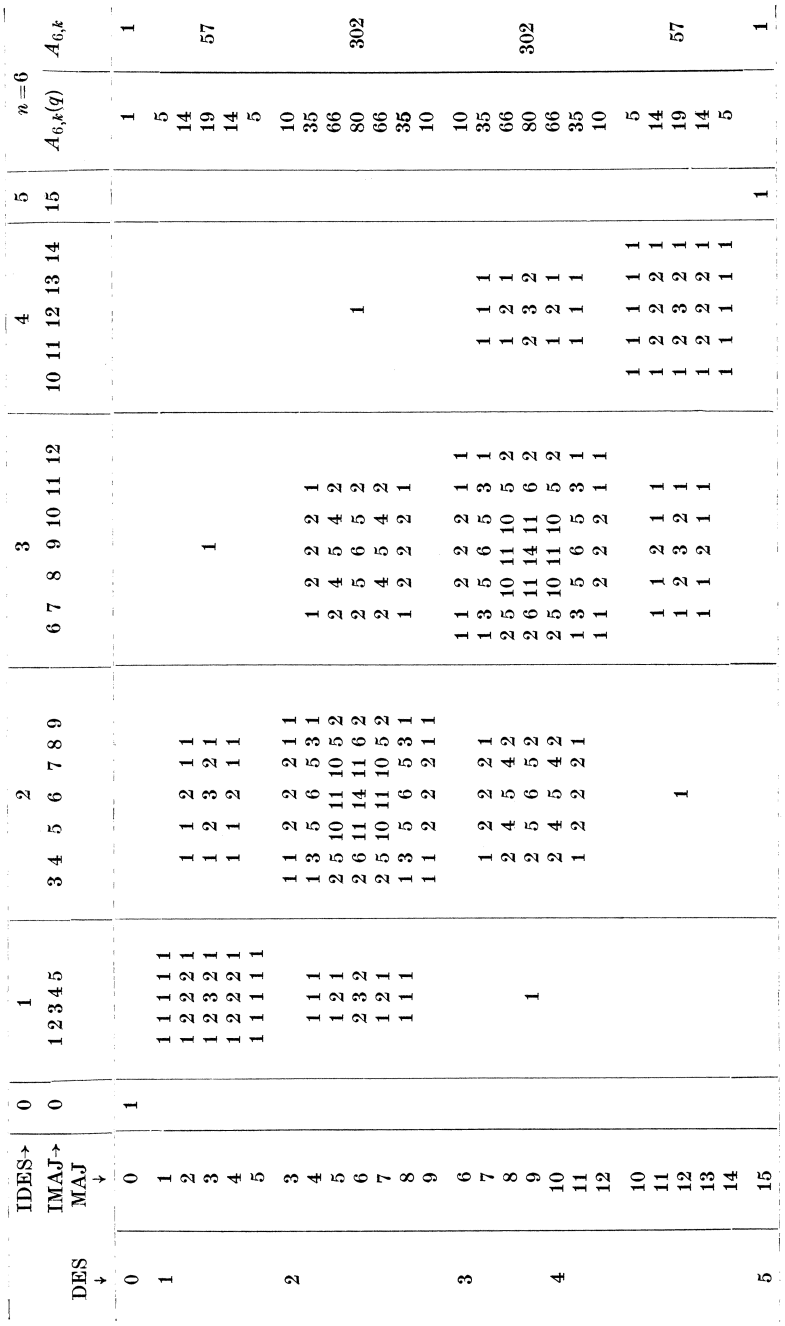
Note that the last two columns show the q-EULERian numbers $A_{n,k}(q)$ (see [1] p. 336) and the EULERian numbers $A_{n,k}$.

Tables 2.

	IDES→	0	1	2	$n=3$	
DES ↓	IMAJ→ MAJ ↓	0	12	3	$A_{3,k}(q)$	$A_{3,k}$
0	0	1			1	1
1	1		11		2	
	2		11		2	4
2				1	1	1

	IDES→	0	1	2	3	$n=4$	
DES ↓	IMAJ→ MAJ ↓	0	123	345	6	$A_{4,k}(q)$	$A_{4,k}$
0	0	1				1	1
1	1		111			3	
	2		121	1		5	11
	3		111			3	
2	3			111		3	
	4		1	121		5	11
	5			111		3	
3	6				1	1	1

	IDES→	0	1	2	3	4	$n=5$	
DES ↓	IMAJ→ MAJ ↓	0	1234	34567	6789	10	$A_{5,k}(q)$	$A_{5,k}$
0	0	1					1	1
1	1		1111				4	
	2		1221	111			9	26
	3		1221	111			9	
	4		1111				4	
2	3			11211			6	
	4		11	13431	11		16	
	5		11	24642	11		22	66
	6		11	13431	11		16	
	7			11211			6	
3	6				1111		4	
	7			111	1221		9	
	8			111	1221		9	26
	9				1111		4	
4	10					1	1	1


n=6
$A_{6,k}$
$A_{6,k}(q)$
IDES→
IMAJ→
MAJ →
DES →

References

[1] L. Carlitz, q-Bernoulli and Eulerian numbers, Trans. Amer. Math. Soc. **76**, 332–350 (1954).
[2] –, Eulerian numbers and polynomials, Math. Magazine **33**, 247–260 (1959).
[3] –, Permutations with a prescribed pattern, Math. Nachr. **58**, 31–53 (1973).
[4] –, A combinatorial property of q-Eulerian numbers, Amer. Math. Monthly **82**, 51–54 (1975).
[5] L. Carlitz, D. P. Roselle and R. A. Scoville, Permutations and sequences with repetitions by number of increases, J. Combinatorial Theory **1**, 350–374 (1966).
[6] L. Comtet, Analyse Combinatoire, vol. 2, Presses Universitaires de France, Paris 1970.
[7] D. Foata, On the Netto inversion number of a sequence, Proc. Amer. Math. Soc. **19**, 236–240 (1968).
[8] H. O. Foulkes, Enumeration of permutations with prescribed up-down and inversion sequences, Discrete Math. **15**, 235–252 (1976).
[9] D. E. Knuth, The art of Computer Programming, Vol. 3 Sorting and Searching, 1973.
[10] P. A. MacMahon, The indices of permutations and the derivation therefrom of functions of a single variable associated with the permutations of any assemblage of objects, Amer. J. Math. **35**, 314–321 (1913).
[11] –, Combinatory Analysis, Vol. 1, Cambridge Univ. Press, Cambridge 1915. (Reimpressed New-York 1955.)
[12] –, Two applications of general theorems in combinatory analysis, Proc. London Math. Soc. **15**, 314–321 (1916).
[13] E. Netto, Lehrbuch der Combinatorik, B. G. Teubner Leipzig 1901.
[14] J. Riordan, An Introduction to Combinatorial Analysis, J. Wiley New York 1958.
[15] G. de B. Robinson, On the representations of the symmetric group, Amer. J. Math. **60**, 745–760 (1938).
[16] C. Schensted, Longest increasing and decreasing sequences, Canad. J. Math. **13**, 179–192 (1961).
[17] M.-P. Schützenberger, Quelques remarques sur une construction de Schensted, Math. Scand. **12**, 117–128 (1963).
[18] R. Stanley, Ordered structures and partitions, Memoirs Amer. Math. Soc. no. **119**, Providence 1972.
[19] R. Alter, T. B. Curtz and C. C. Wang, Permutations with fixed index and number of inversions, Proc. 5th. S.-E. Conf. Combinatorics, Graph Theory, and Computing [Boca Raton, Florida, Feb. 25–March 1, 1974], Florida Atlantic Univ., 1974, 209–228.

Note added in proof. Since the paper has been submitted for publication, several results related to the distribution of the five-vector (DES, IDES, MAJ, IMAJ, INV) have been published. Stanley [20] found the bivariate generating function for the pair (DES, INV), that appears to be a second q-analog for the Eulerian numbers, the first one being the generating function for (DES, MAJ) obtained by Carlitz ([1], [4]). Then, Gessel [21] developed an original combinatorial theory of q-series, that enabled him to get the three-variate distribution for (DES, MAJ, INV). On the other hand, by extending the results of the present paper Foata [22] showed that the ten marginal bivariate distributions of the above five-vector were known and reduced to four different analytical expressions. Finally, Garsia [23] has investigated the relations between the two q-analogs of the Eulerian numbers and obtained new formulas for those two q-extensions.

Supplementary bibliography

[20] R. P. Stanley, Binomial posets, Möbius inversion, and permutation enumeration, J. Combinatorial Theory Ser. A **20**, 336–356 (1976).
[21] I. M. Gessel, Generating functions and enumeration of sequences, Ph. D. thesis, Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Mass., 111 p., 1977.

[22] D. Foata, Distributions Eulériennes et Mahonniennes sur le groupe des permutations, Higher Combinatorics, Proc. NATO Adv. Study Inst. [Berlin, Sept. 1–10, 1976], M. Aigner, ed., D. Reidel Publ. Co., 1977, 27–49.
[23] A. M. Garsia, On the "maj" and "inv" q-analogues of Eulerian Polynomials, Department of Mathematics, University of California, San Diego, La Jolla, Calif., 1978.

Département de Mathématique
Université de Strasbourg
7, rue René Descartes
67084 Strasbourg, France

Département de Mathématique
Université de Paris VII
2, Place Jussieu
75005 Paris, France

C. R. Acad. Sc. Paris, t. 286 (20 février 1978) **Série A — 323**

THÉORIE DES GROUPES. — *Sur une conjecture de* H. O. Foulkes. Note (*) de **Alain Lascoux** et **Marcel-Paul Schützenberger,** présentée par M. André Lichnerowicz.

On annonce la preuve d'une conjecture de H. O. Foulkes sur certains polynômes intervenant dans les fonctions symétriques associées aux représentations projectives du groupe symétrique et des groupes linéaires sur les corps finis.

One sketches a proof of Foulkes' conjecture on the polynomials defining Littlewood Q*-functions in terms of Schur functions.*

On note Z^N l'ensemble des applications I de N dans Z telles que $n\,I=0$ pour tout n assez grand ce qui permet de définir $I^\Sigma \in Z^N$ par $n\,I^\Sigma = \sum_{m \geqq n} m\,I$; le *poids* de I est donc $0\,I^\Sigma$. Les partitions d'un entier n sont les $I \in Z^N$ de poids n telles que $0\,I \geqq 1\,I \geqq 2\,I \geqq \ldots$

Littlewood (1) a défini une famille basique de fonctions symétriques (en les variables d'un ensemble arbitraire qu'il est inutile d'expliciter) indexées par les partitions, $\{Q(I)\}$ au moyen d'une identité

$$Q(I) = \sum s'(J)\,F(I;J), \tag{1}$$

dans laquelle les $s'(J)$ sont les fonctions de Schur (modifiées), la sommation est étendue à toutes les partitions J de même poids que I et les $F(I;J)$ sont des polynômes à coefficients entiers en une nouvelle variable q. Nous proposons d'appeler ces derniers *polynômes de Foulkes* en mémoire du regretté H. O. Foulkes auquel sont dus tant de beaux résultats sur les fonctions symétriques et qui a émis (2) la conjecture que tous leurs coefficients sont dans N. Nous faisons remarquer que ces polynômes sont les caractéristiques (polynomiales) d'Euler-Poincaré des modules inversibles de variétés drapeaux.

Nous annonçons le :

THÉORÈME I. — $F(I;J)$ *est un polynôme monique à coefficients non négatifs qui est nul si l'une des différences* $n\,I^\Sigma - n\,J^\Sigma$ $(n \in N)$ *est négative et dont le degré est égal à leur somme dans le cas contraire.*

La preuve utilise les tableaux de Young. Soient A^* le monoïde libre engendré par un alphabet totalement ordonné A et $\equiv$ la plus petite congruence satisfaisant $xzy \equiv zxy$ et $zty \equiv tzy$ pour toutes les lettres x, y, z, t de A telles que $x \leqq y < z \leqq t$.

Il existe une section $A^*/\equiv \to A^*$; on dit que son image T est l'ensemble des tableaux de Young. Le composé $A^* \to A^*/\equiv \to T$ est le *redressement*. T contient le sous-ensemble L des *lignes*, c'est-à-dire des mots $xyz\ldots$ tels que $x \leqq y \leqq z \leqq \ldots$ et chaque tableau $t \in T$ est un produit $u_k u_{k-1} \ldots u_0$ de lignes dont la suite des degrés $|u_0| \geqq |u_1| \geqq \ldots \geqq |u_k|$ constitue une partition $\|t\|$ (dite *forme* de t).

Soit aussi $A^*\uparrow = \bigcup A^{*I}$ le sous-monoïde des mots w de A dont le multidegré est une partition I (de leur degré $|w|$). Nous introduisons une application $\nu : A^*\uparrow \to N$ (la *charge*) satisfaisant les deux conditions :

1. $f, g \in A^*\uparrow, f \equiv g \Rightarrow f\nu = g\nu$;

2. $f, g \in A^*$, $fg \in A^*\uparrow$, le degré $|g|_a$ de g en a (première lettre de A) est nul $\Rightarrow (fg)\nu = (gf)\nu + |g|$.

324 — Série A **C. R. Acad. Sc. Paris, t. 286 (20 février 1978)**

Sa définition complète fait intervenir une autre condition d'extrémalité trop lourde pour être donnée ici. Si I, J sont deux partitions de même poids, on sait que l'ensemble $T^J \cap A^{*I}$ des tableaux de forme J et de multidegré I est vide sauf si les différences $n\,I^\Sigma - n\,J^\Sigma$ sont toutes non négatives, et on montre que la charge $t\,\nu$ est au plus égale à $O(I^\Sigma - J^\Sigma)^\Sigma$, l'égalité étant atteinte par un tableau unique.

Par conséquent, le théorème I résulte du :

THÉORÈME I'. — *Soient* I *et* J *deux partitions de même poids. Le polynôme de Foulkes* F (I; J) *est égal à* $\sum q^{t\nu}$, *somme sur tous les tableaux* $t \in T^J \cap A^{*I}$.

Cet énoncé contient les résultats antérieurs de Macdonald [*cf.* (3)], et d'un élève de Foulkes, Thomas (4).

Grâce à un lemme d'induction dû à Morris (5), et à la formule dite de Pieri de multiplication d'un tableau par une ligne, on réduit l'expression (1) de Q (I) :

$$Q(I) = \sum \{ s'(\| tu \|)\, q^{|u| - 0I}\, q^{(ut)\nu} / u \in L,\ t \in T,\ |t|_a = 0,\ ut \in A^{*I} \}. \tag{2}$$

Dans cette équation $\| tu \|$ désigne l'élément J de Z^N tel que

$$0\,J = |u|; \qquad 1\,J = 0\,\| t \|, \qquad \ldots, \qquad n\,J = (n-1)\,\| t \|, \qquad \ldots$$

D'après les conventions classiques, $s'(J) = \operatorname{sgn}(J).\, s'(J^\Lambda)$ où $\operatorname{sgn} J \in \{-1, 0, 1\}$ et où, quand $\operatorname{sgn} J \neq 0$, J^Λ est une certaine partition de même poids que J.

La charge ayant la propriété que $(|u| - 0\,I) + (ut)\nu = (tu)\nu$, il suffit alors pour établir le théorème I' de vérifier la nullité de la restriction de la somme (2) à l'ensemble X des paires (t, u) telles que $tu \notin T$ et $\operatorname{sgn}(\| tu \|) \neq 0$. Ceci est la partie substantielle de la preuve, et repose sur la suite exacte introduite dans (6) (p. O.64). On montre qu'il existe une partie X_- de X et une bijection ζ de X_- sur $X \setminus X_-$, telle que si $(t, u)\zeta = (t', u')$ on a $tu \equiv t'u'$, donc $(tu)\nu = (t'u')\nu$, et $s'(\| tu \|) + s'(\| t'u' \|) = 0$. Les détails seront publiés ultérieurement.

(*) Séance du 9 janvier 1978.

(1) D. E. LITTLEWOOD, *Proc. London Math. Soc.*, (B), II, 1961, p. 485-498.

(2) H. O. FOULKES, *A Survey of Some Combinatorial Aspects of Symmetric Functions*, in *Permutations*, Gauthier-Villars, Paris, 1974.

(3) A. O. MORRIS, *A Survey of Hall-Littlewood Functions and Their Applications to Representation Theory*, in *Combinatoire et representation du groupe symétrique*, D. FOATA, éd. (*Springer Lecture Notes*, n° 579, 1977, p. 136-154).

(4) G. THOMAS, *Further Results on Baxter Sequences and Generalised Schur Functions* (ibid., p. 155-167).

(5) A. O. MORRIS, *Math. Zeit*, 81, 1963, p. 112-123.

(6) A. LASCOUX, *Thèse*, Paris, 1977.

Laboratoire d'Informatique théorique et Programmation, L. A. 248,
Université Paris-VII, Tour 55-56, 2, *Place Jussieu*, 75005 *Paris*.

1er COLLOQUE AFCET–SMF DE MATHÉMATIQUES APPLIQUÉES

FIRST MEETING AFCET–SMF ON APPLIED MATHEMATICS

4-8 Septembre 1978

Ecole Polytechnique
PALAISEAU (FRANCE)

Tome I

CONFERENCES - INVITED PAPERS
COMMUNICATIONS THEMES I, II

AFCET : Association Française pour la Cybernétique Économique et Technique
156, boulevard Péreire
B.P. 571
75826 Paris Cédex 17

SMF : Société Mathématique de France
11, rue Pierre et Marie Curie
75231 Paris Cédex 05

UNE APPLICATION DE LA THEORIE ERGODIQUE AU PROBLEME DU CODAGE

F. BLANCHARD
Université Paris VI

D. PERRIN
Université de Rouen

M.P. SCHÜTZENBERGER
Université Paris VII

1. INTRODUCTION

On étudie ici les problèmes soulevés par le codage sur des mots (doublement) infinis et on emploie pour cela des notions et des résultats empruntés à la théorie ergodique.

On se donne un codage (i.e. un morphisme injectif)

$$\alpha : B \longrightarrow X \subset A^*$$

que l'on étend de façon naturelle aux suites infinies de $B^{\mathbb{Z}}$. Il n'est alors en général plus injectif puisque si, par exemple, $B = \{u,v\}$ $A = \{a,b\}$ et :

$$\alpha : \quad u \longmapsto ab, \quad v \longmapsto ba ,$$

le mot $(ab)^{\mathbb{Z}}$ admet deux décodages : $u^{\mathbb{Z}}$ ou $v^{\mathbb{Z}}$.

Ce phénomène correspond à un problème bien connu en théorie des automates : c'est l'étude des sous-groupes du monoïde syntaxique d'un langage et, en particulier, le problème de la synchronisation des codes .

Nous l'abordons ici sous l'aspect des probabilités : on se donne une mesure P sur $B^{\mathbb{Z}}$ qui induit par α une mesure

$$Q = P^{\alpha}$$

sur $A^{\mathbb{Z}}$ ayant les mêmes propriétés d'invariance ou d'ergodicité (cf. § 2). Il peut sembler intuitif que, même si un ensemble de mots de $A^{\mathbb{Z}}$ admet plusieurs décodages en sous ensembles de $B^{\mathbb{Z}}$, l'un de ceux-ci soit plus probable que les autres. Le résultat principal de cet article établit que ceci est, en un sens, exact dans le cas où l'équation en P :

$$P^{\alpha} = Q$$

admet le nombre maximum de solutions . On peut faire apparaître ce résultat comme une sorte de relation d'incertitude reliant l'inambiguité (stochastique) du décodage à la possibilité d'identifier la source (i.e. de déterminer P à partir de Q).

Nous remercions F. Ledrappier de nous avoir aidé à simplifier la démonstration de la prop. 10.

2. NOTATIONS

On note A^* le monoïde libre sur A et $A^+ = A^* \setminus 1$ le semigroupe libre sur A. On considère un morphisme

$$\alpha : B^* \to A^*.$$

On dira que c'est un codage s'il est injectif de B^* dans A^*. La partie $X = B\alpha$ de A^* est alors, par définition, un code. On suppose ici que B, A et donc X sont des ensembles finis.

On notera $R = X(A^+)^{-1} = \{ p \in A^* \mid pA^+ \cap X \neq \emptyset \}$ l'ensemble des préfixes de X et

$$S = (A^+)^{-1} X = \{ q \in A^* \mid A^+ q \cap X \neq \emptyset \}$$ l'ensemble de ses suffixes.

Etant donné un morphisme $\alpha : B^* \to A^*$, une interprétation d'un mot $w \in A^*$ est un triplet $y = (q, b, p)$ de $S \times B^* \times R$ tel que $w = q.b\alpha.p$.

Maintenant si on dispose d'une application,

$$P : B^* \to \mathbb{R}$$

on définit une nouvelle application :

$$P^\alpha : A^* \to \mathbb{R}$$

que l'on dira induite par α, de la façon suivante :

$$P^\alpha(w) = \sum P(b_1 b b_2)$$

où la somme porte sur les triplets (b_1, b, b_2) tels que w admet une interprétation (q, b, p) et $b_1 = 1$ (resp. $b_2 = 1$) si $q = 1$ (resp. $p = 1$), $b_1 \in B$, $b_1\alpha \in A^*q$ sinon (resp. $b_2 \in B$, $b_2\alpha \in pA^*$).

Supposons maintenant que l'on utilise P pour définir sur l'espace $B^{\mathbb{Z}}$ une mesure. Elle induit une mesure P^α sur $A^{\mathbb{Z}}$ et l'on a :

Proposition 1 : *Si* P *définit une mesure invariante ou ergodique, il en est de même de* P^{α}, *pour tout morphisme* α *de* B^* *dans* A^*.

Pour établir ce résultat, il suffit de montrer que la construction de P^{α} coïncide avec la construction habituelle d'une tour au dessus de $B^{\mathbb{Z}}$.

Il est commode de définir pour cela une partie Ω de $B^{\mathbb{Z}} \times \mathbb{N}$:

$$\Omega = \{ (b, i) \in B^{\mathbb{Z}} \times \mathbb{N} \mid 0 \leq i < f(b) - 1 \}$$

ou $b = (b_j)_{j \in \mathbb{Z}}$ et $f(b) = |b_0\alpha|$ est la longueur du mot $b_0\alpha \in A^*$.

On étend l'application α en une application

$$\varphi : \Omega \longrightarrow A^{\mathbb{Z}}$$

définie ainsi : pour $b \in B^{\mathbb{Z}}$ et $i \in \mathbb{N}$ on pose

$$\begin{cases} b_0\alpha \cdot b_1\alpha \cdot b_2\alpha \ldots = a_{-i}\, a_{-i+1}\, a_{-i+2} \ldots\ldots \\ \ldots\, b_{-2}\alpha\, b_{-1}\alpha = \ldots\, a_{-i-2}\, a_{-i-1} \cdot \end{cases}$$

Un automorphisme $\bar{\sigma}$ est défini sur Ω par extension du shift sur $B^{\mathbb{Z}}$:

$$\bar{\sigma}(b, i) = (b, i+1) \quad \text{si} \quad i < f(b) - 1$$
$$= (\sigma b, 0) \quad \text{si} \quad i = f(b) - 1 .$$

Cela donne un diagramme commutatif utilisant le shift τ de $A^{\mathbb{Z}}$:

$$\begin{array}{ccc} \Omega & \xrightarrow{\varphi} & A^{\mathbb{Z}} \\ \bar{\sigma} \downarrow & & \downarrow \tau \\ \Omega & \xrightarrow{\varphi} & A^{\mathbb{Z}} \end{array}$$

Cette construction n'est autre que celle de la tour de hauteur f au dessus de l'espace $B^{\mathbb{Z}}$; la mesure P^{α} définie précédemment coïncide avec la mesure induite par φ sur $A^{\mathbb{Z}}$ à partir de la restriction à Ω de la mesure produit sur $B^{\mathbb{Z}} \times \mathbb{N}$. Il est classique (et facile à vérifier) que cette mesure possède relativement au shift $\bar{\sigma}$ les propriétés indiquées dans la proposition 1. L'hypothèse que α est injective sur B^*, c'est-à-dire que α est un codage, n'est pas nécessaire pour obtenir ce résultat.

Si P est une mesure de probabilité, alors

$$\frac{1}{E_\ell(\alpha)}\ P^\alpha$$

est une mesure de probabilité sur $A^{\mathbb{Z}}$, où $E_\ell(\alpha) = \sum_{b \in B} |b\alpha|\ \ell(b)$ est la longueur moyenne de X.

3. INTERPRETATIONS

Pour une suite infinie $a \in A^{\mathbb{Z}}$ nous définissons une interprétation de a (relative à un morphisme α) comme un ensemble $I \subset \mathbb{Z}$ tel que pour deux éléments consécutifs $n,m \in I$, on a :

$$a_n\, a_{n+1} \cdots a_{m-1} \in X = B\alpha\ .$$

On remarquera que cette définition est cohérente avec celle des interpretations d'un mot $w \in A^*$.

L'ensemble des suites qui ont au moins une interprétation est l'image par φ de Ω ; la proposition suivante montre que l'appartenance d'une suite à cet ensemble ne dépend que de ses facteurs finis :

Proposition 2 : *Une suite* $a \in A^{\mathbb{Z}}$ *est dans* $\Omega\varphi$ *ssi tous ses facteurs* $w \in A^*$ *sont dans l'ensemble :*

$$W(X^*) = (A^*)^{-1}\, X^*\, (A^*)^{-1} = \left\{ w \in A^* \mid A^* w A^* \cap X^* \neq \emptyset \right\}.$$

Démonstration : La condition est certainement nécessaire ; elle est suffisante puisqu'à toute suite $a \in A^{\mathbb{Z}}$ ayant tous ses facteurs dans l'ensemble $W(X^*)$ on peut faire correspondre une suite $(b^{(n)})_{n \in \mathbb{N}}$ d'éléments de $B^{\mathbb{Z}}$ telle que : $a_{-n}\, a_{-n+1} \cdots a_{n-1}\, a_n$ soit facteur de $b^{(n)}\alpha$. Comme B est fini, on peut extraire de cette suite une sous-suite convergente ; sa limite est un élément de $a\varphi^{-1}$ □

Ce résultat montre que l'ensemble $\Omega\varphi$ (qui contient le support de P^α) est un "sofic system" au sens de B Weiss. En effet, il est bien connu que si X est fini, il existe un morphisme

$$\delta : A^* \longrightarrow M$$

sur un monoïde fini M tel que $\delta^{-1}\delta X = X$. On peut, par exemple, prendre pour M le monoïde des relations sur l'ensemble (fini) R des préfixes de X et définir l'image par δ d'une lettre $a \in A$ comme la relation constituée des couples (p, pa) pour tout $p \in R$ tel que $pa \in R$ et des $(p, 1)$ pour tout $p \in R$ tel que $pa \in X$. Une telle construction est possible plus généralement quand X est reconnaissable (cf. [5] par exemple).

Nous donnons maintenant deux énoncés portant sur l'ensemble des interprétations d'une suite $a \in A^{\mathbb{Z}}$. Nous supposons pour cela dorénavant que α est un codage.

Le nombre d'interprétations (q, b, p) d'un mot $w \in A^*$ est borné puisque le couple $(q, p) \in S \times R$ détermine $b \in B^*$:

$$q.b\alpha.p = q.b'\alpha.p \Rightarrow b\alpha = b'\alpha \Rightarrow b = b'.$$

La proposition suivante montre que le nombre d'interprétations d'une suite infinie $a \in A^{\mathbb{Z}}$ est fini :

Proposition 3 : *Le nombre d'interprétations de* $a \in A^{\mathbb{Z}}$ *est la limite inférieure du nombre d'interprétations de ses facteurs de la forme :*

$$w_n = a_{-n}\, a_{-n+1} \cdots a_{n-1}\, a_n .$$

Démonstration : Si $d(a)$ (resp. $d(w)$) est le nombre d'interprétations de $a \in A^{\mathbb{Z}}$ (resp. de $w \in A^*$), on a certainement

$$d(a) \leqslant d(w_n)$$

pour tout entier $n \geqslant n_o$, où n_o est le plus grand élément des $I \cap J$ pour tout couple I,J d'interprétations distinctes de a. Et si k est un point d'accumulation de la suite $d(w_n)_{n \in \mathbb{N}}$, on montre, comme dans la preuve de la proposition 2, que la suite a k interprétations distinctes □

Le nombre d'interprétations disjointes d'une suite apériodique est borné par le cardinal de B (i.e. le nombre d'éléments de X) ; on pourra à ce sujet consulter les importants résultats de J.P. Duval [4].

La propriété suivante montre en particulier que (pour une mesure invariante) deux interprétations distinctes d'une même suite sont presque sûrement disjointes. On verra au paragraphe suivant une preuve directe de ce fait.

On dira qu'une suite $a \in A^{\mathbb{Z}}$ est *formellement récurrente* si tout facteur

$$w = a_i\, a_{i+1} \cdots a_{i+j}\ ,\ i \in \mathbb{Z}\ ,\ j \in \mathbb{N}\ ,$$

peut être trouvé une infinité de fois pour $i \geqslant 0$ et pour $i \leqslant 0$.

Proposition 4 : *Deux interprétations distinctes d'une suite formellement récurrente sont disjointes.*

Démontration : Nous établissons tout d'abord l'énoncé suivant :

Lemme 1 : *Soit* γ *un morphisme de* A^* *sur un monoïde fini* M ; *si* a *est formellement récurrente, il existe une partie* I *de* $\mathbb{Z}$ *et un idempotent* u *de* M *tels que pour deux éléments consécutifs* i,j *de* I , *on ait :*

$$(a_i\, a_{i+1} \cdots a_j)\gamma = u\,.$$

Démonstration : Soit K le plus petit idéal de M qui contient l'image par φ d'au moins un facteur de a , et n un entier tel que :

$$g = a_{-n} \cdots a_{-2}\, a_{-1}\,,\quad g\gamma \in K\,.$$

Maintenant il existe au moins un intervalle positif qui est le support du même mot et donc un entier m tel que :

$$g' = a_o\, a_1 \cdots a_m\,,\quad g'\gamma \in K\,.$$

Soit alors $(H_t)_{t \in \mathbb{Z}}$ une suite d'intervalles disjoints qui sont le support du mot $h = gg'$; si on note U_t l'intervalle de $\mathbb{Z}$ qui sépare H_t de H_{t+1} et u_t le mot dont il est le support, on a alors :

$$a_o\, a_1\, a_2 \cdots = g'\, u_1\, gg'\, u_2\, gg'\, u_3\, gg' \cdots$$

de sorte que $\mathbb{Z}$ est partitionné en une suite d'intervalles disjoints de la forme $(H''_t \cup U_t \cup H'_{t+1})$ où $H_t = H'_t \cup H''_t$, et H'_t (resp. H''_t) est le support de g (resp. g'). D'autre part, d'après le lemme de Green (cf. [3]), les mots $v_t = g'u_t g$ ont une image par γ équivalente par la relation $\mathcal{H}$ à celle de g'g :

$$v_t\gamma\, \mathcal{H}\, (g'g)\gamma\,.$$

Notons $v = (v_t)_{t \in \mathbb{Z}}$ et considérons la fonction ν définie sur lès facteurs de v par :

$$\nu(v_i\, v_{i+1} \cdots v_{i+j}) = \mathrm{Card}\left\{ (v_{i+k} \cdots v_{i+j})\gamma \mid 0 \leqslant k \leqslant j \right\}.$$

On choisit un facteur

$$h = v_i\, v_{i+1} \cdots v_{i+j}$$

de v tel que $\nu(h)$ soit maximal. Comme a est formellement récurrent, on peut écrire :

$$a = \cdots h r_{-1} h r_o h r_1 h r_2 h \cdots\cdots \quad \text{ou } r_i \text{ est}$$

facteur de v . Maintenant, pour tout entier k , $0 \leqslant k \leqslant j$ et tout $t \in \mathbb{Z}$, il existe un entier k' tel que : $(v_{i+k} \cdots v_{i+j}\, r_t\, h)\gamma = (v_{i+k'} \cdots v_{i+j})\gamma$.

Cela implique que $v_{i+k} \cdots v_{i+j}\, r_t\, v_i \cdots v_{i+k'-1}$ ait une image par γ égale à l'idempotent contenu dans la $\mathcal{H}$-classe de g'g et établit le lemme □

Considérons maintenant le morphisme γ de A^* dans le monoïde des relations sur l'ensemble $R = X(A^+)^{-1}$ des préfixes de X défini ci-dessus. On a l'équivalence suivante, pour tout mot $w \in A^*$:

$$(p, p') \in w\gamma \iff pw \in X^* p' .$$

Nous démontrons l'énoncé suivant qui est établi en [2] dans un cadre plus général :

Lemme 2 : *Si $w\gamma$ est idempotent, et si $(p, p') \in w\gamma$, il existe un unique $u \in P$ tel que*

$$(p, u), (u, p') \in w\gamma ;$$

on a de plus $(u, u) \in w\gamma$.

Démonstration : Puisque $w\gamma = w^2\gamma$, il existe au moins un $u \in R$ tel que :

$$(p, u), (u, p') \in w\gamma ;$$

et s'il en existait un autre, soit u', on obtiendrait deux interprétations du mot pw^2 qui sont $(1, (xy)\alpha^{-1}, p')$ et $(1, (x'y')\alpha^{-1}, p')$ avec :

$$pw = xu, \quad uw = yp', \quad pw = x'u', \quad u'w = y'p'.$$

Du fait que ces interprétations sont égales, on obtient $u = u'$.

Enfin, comme $w^2\gamma = w^3\gamma$, il existe un $u' \in P$ tel que :

$$(p, u), (u, u'), (u', p') \in w\gamma .$$

Mais on obtient alors aussi $(p, u') \in w\gamma$, et l'unicité de u implique $u = u'$ □

Nous terminons maintenant la preuve de la proposition 4 : soit a une suite formellement récurrente et J, K deux interprétations de a qui possèdent en commun le point $i \in J \cap K$. On peut alors trouver une partie I de $\mathbb{Z}$ contenant le point i satisfaisant les hypothèses du lemme 1 ; d'après le lemme 2, l'ensemble I est contenu tout entier dans $J \cap K$, ce qui montre que $J = K$ et démontre le résultat.

4. CONSTRUCTIONS D'ESPACES MESURABLES

Nous avons vu qu'une mesure de probabilité P ergodique sur $B^{\mathbb{Z}}$ se transporte en une mesure ergodique P^{α} sur $A^{\mathbb{Z}}$. Avant d'attaquer le problème inverse, introduisons un certain nombre d'espaces isomorphes à Ω.

A) Soit Σ l'ensemble des parties de $\mathbb{Z}$ de bornes $-\infty$ et $+\infty$. Il est muni de la tribu $\mathcal{C}$ rendant mesurable le nombre de points de la partie I dans tout intervalle de $\mathbb{Z}$; si I_o est le premier point de I d'abscisse négative, les autres étant numérotés à partir de celui-ci dans l'ordre croissant, $\mathcal{C}$ est aussi la plus petite tribu rendant mesurables les applications

$$I \longrightarrow I_k \quad , \quad k \in \mathbb{Z} \ .$$

Σ est muni de la translation

$$I \longrightarrow I\text{-}1 \quad ,$$ qui est une bijection bimesurable.

Définitions : On dira que $I \in \Sigma$ et $y \in A^{\mathbb{Z}}$ sont compatibles si I est une interprétation de y. Si $t \in I$, t est une scansion de y ou de (y,I).

L'ensemble Ω' des couples compatibles est une partie mesurable de $(A^{\mathbb{Z}} \times \Sigma, \mathcal{A} \otimes \mathcal{C})$.

Munissons donc Ω' de la restriction $\mathcal{F}'$ de $\mathcal{A} \otimes \mathcal{C}$. Ω' est muni en outre de l'application bijective bimesurable ν :

$$\nu(y,I) = (\tau y, I\text{-}1) \ .$$

Ainsi défini, $(\Omega', \mathcal{F}', \nu)$ est isomorphe à $(\Omega, \mathcal{F}, \overline{\sigma})$ à une condition près :

Proposition 5 : *Si $\alpha_{|B}$ est une injection, il existe une bijection bimesurable $\psi_1 : \Omega \to \Omega'$ telle que*

$$\nu \circ \psi_1 = \psi_1 \circ \overline{\sigma} \ .$$

Démonstration : Posons

$$\psi_1(x,i) = (\phi(x,i) , \{f_k(x)-i , k \in Z\}) .$$

ψ_1 est mesurable. L'application qui à (y,I) fait corespondre a) le point de $B^{\mathbb{Z}}$ de coordonnées $x_k = \alpha^{-1}(y_{I_k} \dots y_{I_{k+1}-1})$, où x_k est bien défini grâce à notre hypothèse, et b) l'entier $-I_o$, est inverse de ψ_1 et mesurable. La dernière relation se vérifie à la main ∎

Nous savons qu'il peut y avoir plusieurs relèvements d'un point y de $A^{\mathbb{Z}}$ dans Ω' : appelons Ω'_y l'ensemble de ces relèvements (qui est fini et même borné dès que α est un codage) .

Proposition 6 : *Soit α un codage de B^* dans A^* . 1) L'application d' : $A^{\mathbb{Z}} \to \mathbb{N}$*

$d'(y) = card\ (\Omega'_y)$

est mesurable.

2) L'ensemble des points de $A^{\mathbb{Z}}$ ayant au moins deux interprétations (y,I) et (y,I') telles que $I \cap I' \neq \emptyset$ est mesurable.

Démonstration :

1) résulte immédiatement de la proposition 3 .

2) entrainé par un argument analogue ∎

B) Nous nous intéressons maintenant à l'ensemble $E(d',\alpha) = E_{d'}$ des mots infinis de $A^{\mathbb{Z}}$ ayant exactement d'interprétations deux à deux disjointes. D'après la proposition, les mots formellement récurrents sont dans $E_{d'}$. Nous venons de démontrer que $E_{d'}$ est mesurable dans $(A^{\mathbb{Z}}, \mathcal{A})$. Posons

$$\Omega_{d'} = \phi^{-1}(E_{d'}) , \text{ et}$$
$$\overline{d'} = \{o,1, \dots d'-1\} \text{ pour } d' \in \mathbb{N} .$$

Proposition 7 : *Soit α un codage, d'un entier strictement positif tel que $E_{d'} \neq \emptyset$. Il existe alors une bijection bimesurable*

$$\psi : \Omega_{d'} \longrightarrow \Omega''_{d'} = E_{d'} \times \overline{d'} ,$$

et une bijection bimesurable $\tilde{\tau}$ de $E_{d'} \times \overline{d'} = \Omega''_{d'}$,

$$\tilde{\tau} = \psi_o \bar{\sigma}_o \psi^{-1} \text{ , telle que}$$

1) l'application coordonnée de ψ dans $E_{d'}$, coïncide avec ϕ .

2) $\tilde{\tau}(y,i) = (\tau y, p(y,i))$ où $p(y,\cdot)$ est une permutation sur $\bar{d}'$.

Démonstration :

1) Il nous suffit d'exhiber une bijection convenable de $\Omega'_{d'} = \psi_1(\Omega_{d'})$ dans $E_{d'} \times \bar{d}' = \Omega''_{d'}$, pour obtenir

$$\psi = \psi_2 \circ \psi_1 \text{ .}$$

L'application coordonnée de ψ_2 dans $E_{d'}$ est l'identité. Considérons $y \in E_{d'}$, et ses d' interprétations distinctes, qui n'ont pas de scansion commune ; soit comme plus haut

$$I_o = \sup \{t \in I : t<o\} \text{ .}$$

Rangeons les d' interprétations dans l'ordre décroissant de leurs I_o respectifs, ce qui est possible puisqu'elles n'ont pas de scansions communes : ceci définit une application de Ω'_y dans $\{y\} \times \bar{d}'$, qui est bijective, et appelons ψ_2 l'application correspondante de Ω' dans $\Omega''_{d'}$. La mesurabilité de ψ_2 et ψ_2^{-1} s'obtient de façon simple. La première coordonnée de ψ est ϕ .

2) Par conséquent $\tilde{\tau}(y,i) = (\tau y,j)$. Pour identifier la seconde coordonnée, deux cas sont à distinguer :

a) sur $\{(y,j) : 1 \notin \bigcup_{I : (y,I) \in \Omega'} I\}$, on a

$$\tilde{\tau}(y,j) = (\tau\, y,j) \text{ .}$$

L'action de ν ne modifie pas l'ordre des interprétations.

b) sur $\{(y,j) : \exists_k \in \bar{d}' : 1 \in I_k\}$, l'ordre des interprétations est modifié par ν de la façon suivante :

$$p(y,j) = \begin{cases} j+1 & \text{pour } o \leq j<i \\ 0 & \text{pour } j = i \\ j & \text{pour } j > i \end{cases}$$

La mesurabilité des deux ensembles considérés, et celle de la variable partielle i définie ci-dessus, découlent immédiatement de la définition des tribus utilisées ∎

5. DEGRE DU CANAL.

Supposons qu'étant donnée une mesure ergodique Q sur A^Z, nous connaissions déjà une mesure R sur Ω''_d, dont elle soit l'image sur la première coordonnée. Nous allons voir d'abord que l'application ψ^{-1} permet de ramener R sur Ω, après quoi on lui associe une mesure ergodique P unique sur B^Z. Toutes les mesures considérées seront des probabilités.

Proposition 8 : *Soit α un codage de B^* dans A^*, Q une mesure invariante sur A^Z, ne chargeant que $\phi(\Omega)$.*

1) Alors, pour presque tout point de A^Z, deux interprétations distinctes sont disjointes.

2) Si de plus Q est ergodique, le nombre d'interprétations distinctes est presque surement constant.

Démonstration :

1) Il suffit de remarquer que, grâce à la stationnarité, presque tous les mots sont formellement récurrents, et d'appliquer la proposition 4. On peut aussi le démontrer sans utiliser la propriété de récurrence formelle.

2) Le nombre d'interprétations distinctes est mesurable (proposition 6) et invariant par τ, donc presque surement constant si Q est ergodique ∎

Cette proposition signifie que l'application ϕ est presque partout définie et ne fait intervenir qu'un ensemble Ω''_d. Appelons degré du canal l'entier $d' = d'(\alpha,Q)$ associé par la proposition précédente à la mesure Q.

6. DECODAGE ET IDENTIFICATION DE LA SOURCE.

Le problème qu'il nous reste à résoudre consiste, étant donnée une mesure ergodique Q sur $A^{\mathbb{Z}}$, à la remonter en une mesure ergodique sur $\Omega''_{d'}(\alpha,Q)$.

Appelons η l'application coordonnée de $\Omega''_{d'}$ dans $E_{d'}$, et $\tilde{Q}$ la mesure sur $\Omega''_{d'}$:

$$\tilde{Q} = \frac{1}{d'} Q \otimes \left(\sum_{i \in \bar{d}'} \delta_i \right).$$

Proposition 9 : *La mesure $\tilde{Q}$ est invariante par τ ; la tribu de ses invariants $\mathcal{J}$ est atomique et compte au plus d' atomes.*

Démonstration : $\tilde{\tau}$ est le produit de la transformation τ, qui conserve Q, par des permutations de $\bar{d}'$. Elle laisse donc $\tilde{Q}$ invariante.

Supposons qu'il existe un ensemble invariant E mesurable dans $\Omega''_{d'}$, tel que

$$0 < \tilde{Q}(E) < \frac{1}{d'} .$$

On peut trouver j dans $\bar{d}'$, tel que

$$\tilde{Q}\{(y,j) : (y,j) \in E\} \neq 0 .$$

Alors le sous-ensemble $\eta(E)$ de $E_{d'}$, de mesure $Q(\eta(E)) \leq d' \cdot \tilde{Q}(E) < 1$, est invariant par τ, ce qui contredit l'ergodicité de la mesure Q pour τ.

Remarque : On voit facilement qu'à chaque y, pour un ensemble invariant E, est associé un entier positif $d'' = \mathrm{card}\{(y,i) : (y,i) \in E\}$, qui est presque surement constant.

Voici maintenant le résultat principal de cet article. Il est énoncé sous sa forme la plus abstraite, nous expliquerons ensuite ce qu'il signifie.

Proposition 10 : *Soit α un codage, Q une mesure ergodique finie sur $A^{\mathbb{Z}}$, ne chargeant que l'ensemble $E_{d'}$. Les mesures ergodiques R sur $(\Omega''_{d'}, \tilde{\tau})$ de marginale Q sont, à un coefficient près, les restrictions de $\tilde{Q}$ aux atomes de sa tribu invariante. Les entiers $d''(\alpha,R)$ associés à*

chacune d'entre elles d'après la remarque précédente vérifient

$$(2) \qquad \sum_{\{R:R\nu^{-1}=Q\}} d''(\alpha,R) = d'(\alpha,Q) \quad .$$

Cette proposition répond aux deux questions que nous nous sommes posées :

1) Celle de l'identification de la source a au moins 1 et au plus $d'(\alpha,Q)$ solutions, suivant la structure de $\underset{\sim}{Q}$.

2) Celle de l'ambiguïté du décodage : presque tout mot y de $A^{\mathbb{Z}}$ a d'' interprétations "probables", et d'' est compris entre 1 et d' .

Si on suppose que la mesure R provient d'une mesure P sur $B^{\mathbb{Z}}$, nous appellerons $d'' = d''(\alpha,P)$ degré de la source P .

3) Enfin, globalement, le décodage est d'autant moins ambigu que le nombre de solutions de l'équation $P^{\alpha} = Q$ est plus proche de d', donc l'identification de la source plus difficile.

On peut donner de la réponse à la question du décodage une interprétation finitiste. Soit $y \in E_{d'}$, et $\{A_n\}$ la suite décroissante d'événements mesurables

$$A_n = \{z \in E_{d'} : z_n = y_{-n}, z_{-n+1} = y_{-n+1} \cdots z_n = y_n\} \quad .$$

Soit P une mesure ergodique sur $B^{\mathbb{Z}}$, $R = P_o\psi^{-1}$, $Q = P^{\alpha}$. Le théorème des martingales affirme que la suite

$$d' \frac{R(A_n \times \{i\})}{Q(A_n)} = \frac{R(A \times \{i\})}{\underset{\sim}{Q}(A_n \times \{i\})} \quad , \quad n \in \mathbb{N}$$

tend pour presque tout y quand $n \to +\infty$ vers $\frac{dR}{d\underset{\sim}{Q}}(y,i)$, c'est-à-dire vers $\frac{d'}{d''}$ ou 0, suivant que (y,i) fait ou non partie du support de R .
C'est-à-dire que connaissant un segment fini mais suffisamment long du mot y, on pourra distinguer les interprétations "probables" au sens de P de celles qui ne le sont pas.

Démonstration de la proposition 10 :

1) a) Soit R telle que $R\sigma\eta^{-1} = Q$.

Ceci implique que R est absolument continue par rapport à $\tilde{Q}$: donc la dérivée $\frac{dR}{d\tilde{Q}}$ existe, et c'est une fonction presque surement invariante par $\tilde{\tau}$. Elle est donc constante sur chacun des atomes de la tribu $\mathfrak{I}$ des invariants de $\tilde{\tau}$ pour $\tilde{Q}$. Comme R est ergodique, elle est nulle partout sauf sur l'un des ces atomes E, ce qui signifie que R est absolument continue par rapport à la restriction $\tilde{Q}_{|E}$. Deux mesures ergodiques distinctes ne peuvent avoir même support, donc à un coefficient près $R = \tilde{Q}_{|E}$.

b) Réciproquement la marginale $\tilde{Q}_{|E}o\eta^{-1}$ a son support contenu dans celui de Q, et comme il s'agit de deux mesures ergodiques, elles coïncident. $\tilde{Q}_{|E}$ est donc une solution de l'équation considérée.

2) La relation (2) résulte de la définition de d''.

BIBLIOGRAPHIE

(1) BILLINGSLEY : "Ergodic Theory and Information". Wiley.

(2) BOË J.M. : "Représentations des monoïdes". Thèse de 3ème Cycle (1976).

(3) CLIFFORD A.H. and G.B. PRESTON : "The Algebraic Theory of Semigroups". Vol. 1 Amer. Math. Soc. (1961).

(4) DUVAL J.P. : "Périodes et répétitions des mots du monoïde libre". A paraître dans Theoretical Computer Science .

(5) EILENBERG S. : "Automata, Languages and Machines". Vol A, Academic Press (1974).

(6) WEISS B. : "Subshifts of finite type and sofic systems". Monatshefte für Math., 77 (1973) 462-474.

Table des matières

Tome IX

Marcel-Paul Schützenberger

ŒUVRES COMPLÈTES

éditées par Jean Berstel, Alain Lascoux et Dominique Perrin

Les treize tomes de cette édition contiennent l'ensemble des œuvres de Marcel-Paul Schützenberger qui ont fait l'objet d'une publication dans une revue scientifique ou un livre. Ses travaux couvrent une période de plus de 50 ans, depuis sa première note aux Comptes Rendus en 1943 jusqu'à son dernier article, paru en 1997.
Les publications sont présentées dans l'ordre chronologique. Chaque tome est précédé d'une courte introduction qui essaie d'éclairer certains des travaux, tant pour leur intérêt scientifique intrinsèque que pour l'écho qu'ils ont rencontré et les développements qu'ils ont suscités.

Tome 9 : 1976 – 1978

Les recherches réunies dans ce tome portent sur les variétés de monoïdes et les transductions rationnelles, poursuivant les travaux précédents. Il contient aussi des travaux fondamentaux de combinatoire.
L'article « Sur le produit de concaténation non ambigu » porte sur la variété des semigroupes finis dont toute $\mathcal{D}$-classe régulière est un semigroupe. Bien qu'il soit moins connu que celui sur les langages sans étoile de 1965, cet article a eu lui aussi une influence considérable sur les développements ultérieurs.
Les articles « Sur les relations rationnelles entre monoïdes libres », puis « Sur une caractérisation des parties reconnaissables d'un monoïde libre » et « Une caractérisation des parties reconnaissables » traitent de propriétés des relations rationnelles.
L'article sur « La correspondance de Robinson » est un texte fondamental, quoique de lecture quelque peu ardue. Il présente la théorie des tableaux de Young par l'intermédiaire de glissements planaires (essentiellement le jeu de taquin). Ceci permet de réinterpréter les constructions de Robinson, Schensted, Knuth, les tableaux apparaissant comme représentants canoniques de chaque classe de congruence. Par cette construction, l'algèbre des polynômes symétriques est plongée dans l'algèbre plaxique, et on obtient ainsi des versions non commutatives d'énoncés sur les polynômes.