Marcel-Paul Schützenberger

# ŒUVRES COMPLÈTES

éditées par
Jean Berstel, Alain Lascoux et Dominique Perrin

*

## Tome 10 : 1979–1982

Institut Gaspard-Monge, Université Paris-Est
2009

# Introduction
# Tome X : 1979–1982

De nombreux écrits de Marcel-Paul Schützenberger de ces années portent sur la combinatoire algébrique. La plupart des travaux mathématiques de Schützenberger, à partir de cette période, seront consacrés à ce sujet.

Les polynômes de Kostka-Foulkes sont définis comme la somme $\sum q^{c(t)}$, $t$ parcourant l'ensemble des tableaux de forme et d'évaluations données, $c(t)$ étant la charge. La note [1979-4] montre la croissance de ces polynômes relativement à l'ordre dit naturel sur le treillis des évaluations. Cette propiété fut par la suite généralisée en décomposant l'ensemble des tableaux en *atomes*, les polynômes de Kostka-Foulkes s'obtenant par sommation à partir des atomes, voir [5].

L'article [1980-3] montre que la charge, en tant que fonction à valeurs entières sur les mots, vérifie une propriété de minimalité.

L'article [1981-1] tenait spécialement à coeur à M.-P. Schützenberger. Il reprend la théorie des *tableaux de Young*, dans un style différent de [1977-4], cette fois-ci en mettant l'accent sur l'aspect monoïde. L'*algèbre plaxique* est définie comme quotient de l'algèbre libre sur un alphabet totalement ordonné, par une congruence sur les facteurs de longueur 3 due à Knuth. Cette algèbre contient comme sous-algèbre commutative l'anneau des polynômes symétriques, ce qui permet de donner une version non-commutative de différentes propriétés des fonctions de Schur. Deux opérations fondamentales, qui connaîtront de nombreux développements, sont introduites :

- un relèvement à l'algèbre libre de l'action du groupe symétrique sur les polynômes,
- le *cyclage*, c'est-à-dire l'opération induite sur les tableaux par les permutations circulaires sur les mots.

L'algèbre de Hecke du groupe symétrique est une déformation de l'algèbre usuelle du groupe symétrique. Kazhdan et Lusztig en ont défini une nouvelle base linéaire, dont les coefficients de décomposition dans la base usuelle sont les *polynômes de Kazhdan-Lusztig*. L'article [1981-2] obtient ces polynômes dans le cas correspondant aux variétés de Grassmann. Leur description utilise les étiquetages croissants des arbres correspondants aux permutations ayant une seule descente. Cette construction a été généralisée aux permutations vexillaires dans [4].

La note [1982-1] fonde la théorie des *polynômes de Schubert*. Ces polynômes sont une base linéaire de l'anneau des polynômes en $x_1, x_2, \ldots$. Ils sont définis à l'aide des *différences divisées* de Newton :

$$f(x,y) \to \big(f(x,y) - f(y,x)\big)(x-y)^{-1}\,.$$

Les polynômes qui correspondent aux permutations *vexillaires* possèdent nombre des propriétés des fonctions de Schur, qui en sont une sous-famille. Plus généralement, la combinatoire des polynômes de Schubert est associée à une combinatoire des permutations qui étend la combinatoire des partitions en oeuvre dans la théorie des fonctions symétriques.

Une méthode d'étude des fonctions symétriques est de les filtrer suivant la première variable $x_1$, ce qui révèle la structure d'*algèbre de Hopf* de l'anneau des polynômes symétriques. La note [1982-2] met en oeuvre cette approche pour les polynômes de Schubert et les polynômes de Grothendieck. Un corollaire en est l'énumération des décompositions réduites de toute permutation, qui peut aussi s'obtenir à l'aide d'un monoïde apparenté au monoïde plaxique, le *monoïde nilplaxique*. Ce dernier objet a été étudié en détail par Edelman et Greene [3].

Le texte *A propos du livre « On system analysis » de D. Berlinski* [1979-5], suivi de *Sur l'analyse des systèmes* [1980-6] fait référence à la publication du livre de David Berlinski [1]. Le texte est une charge contre la théorie générale de systèmes en tant que conception holistique du savoir et fourmille de formules mordantes. Il offre un amusant contrepoint au style très mesuré et d'une prudence toute anglo-saxonne de Berlinski (qui poursuit toutefois exactement le même but).

L'article sur l'analyse des systèmes fera le bonheur de deux auteurs en guerre contre l'introduction maladroite de l'informatique dans l'enseignement scolaire [2]. Ceux-ci relèvent de nombreuses formules frappantes, ainsi celle qui définit l'imposture comme « cette référence au théorème des forces vives dans un discours célèbrant ou dénigrant l'énergie des grands chefs militaires et civils ». Ils notent toutefois (p. 196) : « le seul dommage est qu'il ait donné à sa demonstration un tour si cocasse et si allusif qu'elle demeure presque impénétrable à des initiés même ».

Comme le précédent, *Mathématiques et linguistique* [1979-6] est le texte d'une conférence. Elle est l'une des rares occasions où M.-P. Schützenberger expose son point de vue sur la possibilité de la formalisation mathématique de la linguistique. La conclusion est plutôt pessimiste mais, dit-il « Les mathématiciens non plus ne doivent pas pleurer. Si leur but est, comme il se doit, de faire progresser la connaissance des objets mathématiques (et non d'enrichir ou de raffiner une nouvelle rhétorique) ils ont acquis toute une série d'intuitions nouvelles sur des objets classiques et sur des objets nouveaux qui ne semblent pas déraisonnables ».

L'article *On prétend que..* [1980-4] suivi de *Compléments sur le traitement automatique des langues naturelles* [1980-5], tous deux avec Maurice Gross, est une charge contre la prédiction de la généralisation de l'usage de l'informatique et son impact culturel. Même si les critiques contre la surestimation de l'intelligence des ordinateurs ont gardé toute leur pertinence, la généralisation de l'usage d'Internet leur a en partie donné tort.

La note *A conjecture on sets of differences of integer pairs* [1981-3] avec Dominique Perrin propose une conjecture issue de la conjecture de l'équivalence commutative des codes (voir l'introduction du tome 9). Un contre exemple à cette conjecture a été trouvé par Shor [6]. C'est le premier exemple d'un code fini qui n'est pas commutativement préfixe. Il a conduit à formuler la conjecture sous la forme suivante : *Tout code maximal fini est commutativement préfixe.*

[1] David Berlinski. *On System Analysis.* MIT Press, 1976.

[2] Jean-Pierre Despins and Marie-Claude Bartholy. *Arsenic et jeunes cervelles.* Union Générale d'Editions, 1987.

[3] Paul Edelman and Curtis Greene. Balanced tableaux. *Adv. in Math.*, 63(1) :42–99, 1987.

[4] Alain Lascoux. Polynômes de Kazhdan-Lusztig pour les variétés de Schubert vexillaires. *C. R. Acad. Sci. Paris Sér. I Math.*, 321(6) :667–670, 1995.

[5] Alain Lascoux, Bernard Leclerc, and Jean-Yves Thibon. The Plactic Monoid. In M. Lothaire, editor, *Combinatorics on Words.* Cambridge University Press, 2001.

[6] P. W. Shor. A counterexample to the triangle conjecture. *J. Combin. Theory Ser. A*, 38(1) :110–112, 1985.

# Année 1979

## Bibliographie


[1979-1] Marcel-Paul Schützenberger. A property of finitely generated submonoids of free monoids. In *Algebraic theory of semigroups (Proc. Sixth Algebraic Conf., Szeged, 1976)*, volume 20 of *Colloq. Math. Soc. János Bolyai*, pages 545–576. North-Holland, Amsterdam, 1979.

[1979-2] Marcel-Paul Schützenberger. Sur les sous groupes de rang fini d'un groupe libre. In G. Pirillo, editor, *Atti del Convegno su "Codage et Transductions"*, pages 1–29. Istituto di Analisi Globale del C.N.R., Firenze, 1979. 15-17 octobre.

[1979-3] François Blanchard, Dominique Perrin et Marcel-Paul Schützenberger. On an application of ergodic theory to some problems on coding. In *Transactions Eigth Prague Conference on Information Theory*, pages 47–53. Czechoslovak Academy of Sciences, 1979.

[1979-4] Alain Lascoux et Marcel-Paul Schützenberger. Croissance des polynômes de Foulkes-Green. *C. R. Acad. Sci. Paris Sér. A-B*, 288(2) :A95–A98, 1979.

[1979-5] Marcel-Paul Schützenberger. À propos du livre "On system analysis" de D. Berlinski. Technical Report 79-80, LITP, 1979.

[1979-6] Marcel-Paul Schützenberger. Mathématiques et linguistique. In *Séminaire sur les fondements des sciences*, number 92, pages 23–34. Université Louis Pasteur, Strasbourg, 1979.

COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
20. ALGEBRAIC THEORY OF SEMIGROUPS, SZEGED (HUNGARY), 1976.

# A PROPERTY OF FINITELY GENERATED SUBMONOIDS OF FREE MONOIDS

M.P. SCHÜTZENBERGER

*To the memory of C. and A. Rényi*

## 1. INTRODUCTION

Various problems in algebra lead to the study of the ways in which the words of a free monoid $A^*$ (generated by the alphabet $A$) can be factorized as products of the words from a given subset $X$ of $A^*$. It suffices to make reference to the works of Al.A. Markov [1], Y.I. Khmelevski [2], S.I. Adjan [3], to the recent thesis of J.C. Spehner [4], and, especially, to the book of A. Lentin on the equations in free monoids [5]. One technique to approach this question uses the syntactic monoid $S = \mathrm{Synt}(X^*)$ of the submonoid $X^*$ generated by $X$. According to S. Eilenberg's theory [6], $S$ is the least quotient of $A^*$ such that the natural morphism $\sigma$ of $A^*$ on $S$ *recognises* $X^*$ (in the sense that $X^* = X^*\sigma\sigma^{-1}$). In equivalent fashion, let the $X^*$*-context* of a word $w$ be the set of all pairs of words $(v, v')$ such that $vwv'$ is in $X^*$; then $S$ is the quotient of $A^*$ by the congruence which is defined by the equality of contextes [7]. Here we shall be mainly concerned with the case of a finite $X$. Its interest, apart from the applications, is demonstrated by the researches of J.F. Perrot [8], [9] and Perrin [10] who have shown that this hypothesis implies severe conditions on $S$.

It is well known that the finiteness of $S = \mathrm{Synt}(X^*)$ for finite $X$ is a trivial special case of Kleene's theorem (cf. [6], Chap. VII). It entails a bound on $S$ as a function of the sum $L$ of the lengths of the words in $X$. To see it directly, recall the standard notation $A^+$ for the free semigroup $A^* \setminus 1$ generated by the same alphabet $A$ as $A^*$ and assume without loss of generality that $X$ is the minimum generating set of $X^*$, i.e., that $X$ is equal to $X^+ \setminus X^+ \cdot X^+$ (where, of course, $X^+ = X^* \setminus 1$). As usual, the *prefixes* (resp. *suffixes*) of $X$ are the proper left (resp. right) factors of its words. By definition, their set is

$$P = X(A^+)^{-1} = \{a \in A^*:\ aA^+ \cap X \neq \phi\}$$

and

$$Q = (A^+)^{-1}X = \{a \in A^*:\ A^+a \cap X \neq \phi\}.$$

Their number is at most $L$ and it is clear that any two words have the same context when their contextes have the same restriction to $P \times Q$. Accordingly, the number of classes of the syntactic congruence is not more than $2^{L^2}$.

Before examining some examples we recall that in any semigroup $M$ the *conjugacy* relation is the least equivalence on $M$ such that $mm'$ and $m'm$ belong to the same class for any two elements $m$ and $m'$ of $M$. It follows that two groups in $M$ generate the same ideal iff their idempotents are conjugate. Classical theorems by Clifford and Miller [11] show that two such maximal groups are isomorphic. One says then that thay are *conjugate*. Also, an element $m$ is *primitive* iff the submonoid $m^*$ contains every element $m'$ such that $m$ is included in $m'^*$. When $M$ is a group, the conjugacy relation is the usual one (since $m' = g^{-1}mg$ is equivalent with $m' = (g^{-1})(mg)$ and $m = (mg)(g^{-1})$) and $m$ is primitive iff it generates a maximal cyclic subgroup.

These notions are of special significance also when $M$ is a free monoid because, (as it is well known) every word $w \neq 1$ is in a unique manner a power $w = h^r$ of a primitive word $h$ (often noted $\sqrt{w}$) and its conjugacy class consists of the $|h|$ words $(h'h'')^r$ where $|h|$ is the length of $h$ and $h'$ and $h''$ satisfy $h = h''h'$. Thus, here, primitive elements correspond to maximal commutative subsemigroups because, in a free monoid, two words commute iff they are both powers of the same word (cf. [5]).

We let $X$ have $k$ elements and we say for short that a parameter of $S = \text{Synt}\,(X^*)$ is *absolutely finite* if it can be bounded as a function of $k$ only. Suppose first $k = 1$ and $X = \{h^P\}$ where $h$ is a primitive word of length $|h|$ and $p$ a positive integer. Then $S$ contains $|h|$ conjugate cyclic groups of order $p$. Therefore neither the number of elements or groups in $S$ nor the order of these groups is absolutely finite. The same is true for the number of principal ideals in $S$ as it is shown by the example of $X = \{h^P, a\}$ with $h^P$ as above and $a \neq h$ any letter in $A$, where $S$ has certainly more than $|h|$ such ideals. More generally, if $X = \{h_1^P, h_2^P, \ldots, h_k^P\}$ where $p \geqslant 2$ and where the $h_i$'s are non conjugate words, $S$ contains $k$ classes of conjugate cyclic groups of order $p$, and the number of its principal quasi ideals (12) not meeting the images of these cyclic groups grows linearly as a function of $p$ for each fixed $k \geqslant 2$.

Our main result, to be proved in Section 4, is that nonetheless some of the parameters of $S$ are absolutely finite. It can be summarized by the following assertions:

(1) The number of conjugate classes of groups in $S$, i.e. the number of principal idempotent ideals, is absolutely finite.

(2) Apart from at most $k$ conjugate classes of special cyclic groups of arbitrary orders, any group in $S$ is (isomorphic to) a subgroup of the symmetric group of order $(2k)!$.

(3) The inverse images of $A^*$ of the special groups are themselves cyclic subsemigroups of $A^*$.

(4) Each bi-ideal $uSv$ where $u$ and $v$ are non special idempotents is absolutely finite.

The proof is an application of the theory developed by Fine and Wilf in [13]. The corollaries required for the present study are established in Section 2. To make the connection with syntactic monoids we introduce in Section 3 a somewhat larger monoid $M$, the *monoid of interpretations* of $X^*$.

The bound $(2k)!$ in (2) seems quite extravagant since the largest value known is $(k-1)!$ corresponding to $X$ made up of the words:

$$a^{k-1}; a^{k-2}ba; a^{k-3}b; a^{k-4-j}ba^{2+j} \qquad (0 \leqslant j \leqslant k-4)$$

for any $k \geqslant 4$. One computes that the syntactic images of the words $ba^{k-1}$ and $ba^{k-2}$ (for instance) are a cyclic permutation and a transposition generating a symmetric group of the desired order, respectively (cf. [10]).

This result (or more accurately, the bound $k!$) would be achieved if one was able to obtain the "first periodicity lemma" of the Fine – Wilf theory under a weaker hypothesis of "twice covering".*

To end this introduction let us briefly indicate how similar observations can be applied to a special family of equidivisible monoids in the sense of McKnight and Storey [14]. Let $F'$ be the family of all the functions $f$ from the reals into themselves whose domain is a finite semi-open initial interval which is noted $]0, |f|]$ for each function $f$. The product of $f$ with another function $g$ is obtained by concatenating $g$ with a translate of $g$. Explicitely, it is the function $h$ of domain $]0, |h|]$ where $|h| = |f| + |g|$ and the value of $h$ at any point $r$ of its domain is defined as follows:

$$h(r) = \begin{cases} f(r) & \text{if} \quad r \leqslant |f|; \\ f(|f|) + g(r - |f|) & \text{otherwise.} \end{cases}$$

Thus, $h$ is continuous when $f$ and $g$ are so. It has been demonstrated by Fine and Wilf (in a slightly different language) that their theory holds for submonoids of $F'$ containing all "smooth" enough functions. In this

*Note (added in proof): This property has been proved since by Y. Césari (C.R. Acad. Sci. Paris, t. 286, 1175-1177) and further important results have been obtained by J-P. Duval (Theoretical Computer Science, to appear).

case, a maximal commutative subsemigroup of $F'$ consists of all functions which are the restrictions to finite initial intervals of a given (ordinary) linear function.

The two "periodicity lemmas" require more stringent restrictions and one is led to consider the submonoid $F$ of $F'$ that is generated by all monotonic (increasing or decreasing) functions. In fact $F$ is almost a free monoid and there is no difficulty in defining the monoid of interpretations (and the syntactic monoid) of an arbitrary submonoid $X^*$ of $F$. Assuming now that $X^*$ is finitely generated, one can apply the same proof techniques with the obvious modifications imposed by the nature of the maximal commutative subsemigroups, and one verifies that the assertions (1)-(4) above remain true in this more general set-up. This explains our introduction of the notion of "absolute finiteness" since in this case the number of principal ideals (for instance) of the syntactic monoid of $X^*$ is in general not even enumerable.

## 2. THE THEORY OF FINE AND WILF

In all this section we consider a fixed word $w$ in $A^+$ of positive length $m = |w|$. In order to deal with the various occurrences of the same word as a factor of $w$ and with their mutual relationships, we shall view $w$ as a sequence of letters and, more accurately, as a map into the alphabet $A$ of a basic sequence $C$ of $m$ consecutive indices. For convenience we shall always take for $C$ the basic chain (i.e. totally ordered set) $C = (1, 2, \ldots, m)$. If $I = (i, i+1, \ldots, i+k)$ is a subinterval of positive length $k+1$ of $C$, we let $Iw$ be the word $(i)w \cdot (i+1)w \cdot \ldots \ldots \cdot (i+k)w$ obtained when restricting $w$ to $I$. The pair $(I, w)$ is a *segment* of $w$; $I$ is its *support* and $Iw$ is a factor of $w$. Of course, $Cw = w$ and, in the opposite direction, $Iw$ is the neutral element of the monoid $A^*$ iff $I$ is the empty interval.

Suppose that, for instance $w$ is the word *baabaabababaab* of length 12 where $a$ and $b$ are two letters. The word $f = baaba$ occurs twice as a factor of $w$ in the segments $(I', f)$ and $(I'', f)$ with $I' = (1, 5)$ and $I'' = (4, 8)$; in the same manner the word *aba* occurs three times, the corresponding supports being respectively $(3, 5), (6, 8)$ and $(8, 10)$.

The reader will notice that the intervals $I'$ and $I''$ overlap and that their union $I = (1, 8)$ is the support of the word $Iw = baabaaba$ which exhibits an obvious periodicity. The theorem of Fine and Wilf gives a complete (and optimal) analysis of this phenomenon.

The theory is based upon the notions of *translation* and of *periodicity*. We say that a subinterval $I$ of $C$ admits the translation $p$ iff $p$ is a positive integer strictly less than the length $|I|$ of $I$ and if one has $iw = (i + p)w$ for the indices $i$ in $I$ such that $i + p$ is also in $I$.

This condition is equivalent with $I'w = I''w$ where $I'$ (resp. $I''$) is the initial (resp. final) interval of length $|I| - p$ of $I$. Therefore it is equivalent to the existence of words $f, g, g'$ such that $Iw = fg = g'f$ where $g$ and $g'$ both have length $p$.

Returning to the same example as above, we see that $I = (1, 8)$ admits the translation 3 and that the word $f = I'w = I''w$ satisfies the equation $fg = g'f$ with $g = (6, 8)w = aba$ and $g' = (1, 3)w = baa$; it also admits the translation 6. In similar fashion the interval $(8, 12)$ which is the support of the word $abaab$ admits exactly one translation, viz. 3, and the interval $(7, 11)$ admits no translation whatsoever.

It is clear that when $I$ admits the translation $p$ it also admits any translation $kp \leqslant |I|$ for $k$ a positive integer. We shall call *step of* $I$ the least translation which it admits and denote it by $\|I\|$ (with the convention that the step is infinite when $I$ admits no translation). Algebraic reasons lead to reserve the term "period" to the ratio $|I| : \|I\|$ when it is an integer.

All these notions would easily carry over to the case of the monoids of functions presented at the end of the introduction. Then the basic structure would be a fixed real valued function $w$ of a fixed interval $C = ]0, |w|]$, the only difference being that the indices would vary continuously in $C$ instead of being the successive integers $1, 2, \ldots, m$ and that the translations could be any positive real. We refer once more to (13) for this deeper case which will not be touched here.

Since the word $w$ and the basic interval $C$ are fixed it is understood in what follows that any interval mentioned is a subinterval of $C$. We begin by a remark.

**2.1.** *Let $K$ be an interval of length $n$ admitting the translations $p$ and $q$ where $q < p < n$. Its initial (or final) interval of length $n-q$ admits the translation $p-q$.*

**Proof.** Let $K=(k,k')$ where $k'=k+n-1$. If $i$ belongs to the initial interval $K'$ of length $n-p$ of $K$, one has $i+p \in K$. Thus $iw = (i+p)w$ since $K$ admits the translation $p$. Because of $p>q$, one has $i+p-q>i$, hence $i+p-q \in K$ and $(i+p-q)w=(i+p)w$ since $K$ admits the translation $q$. Therefore $(i+p-q)w$ is equal to $iw$ for each $i$ in $K'$ which shows that the initial interval of length $n-q=|K'|+p-q$ admits the translation $p-q$ The same argument applies to the final interval of $K$. Q.E.D.

**2.2. Theorem** (Fine and Wilf). *Let $I$ and $J$ be two intervals admitting the translations $p$ and $q$, respectively, and having an intersection $K$ of length at least $p+q-r$ where $r$ is the greatest common divisor of $p$ and $q$. Their union $L$ admits the translation $r$.*

**Proof.** We may assume $p \geqslant q$, hence $|K| \geqslant p$ with equality iff $q=r$, i.e. iff $p$ is a multiple of $q$.

The hypothesis that $I$ admits the translation $p$ implies that we can take in $K$ an interval $K'$ of length $p$ such that for any index $i$ in $I$ there is an index $i'$ in $K'$ differing of $i$ by an integral multiple of $p$. Thus $iw=i'w$. Accordingly, if $p$ is a multiple of $q\ (=r)$ and if $x,y \in L$ differ by a multiple of $r$, we can find $x',y'$ in $K'$ such that $xw=x'w$ and $yw=y'w$ by using the hypothesis that $J$ admits the translation $q$ when any of these indices is in $J$. Since $K'$ is included in $J$, the same hypothesis shows that $x'w=y'w$ from which we conclude that $xw=yw$ in this case. This proves the result when $q$ is equal to $r$ and we can assume hence forth that $q$ is strictly greater than $r$.

We proceed by induction on the integer $(p+q){:}\ r$, the case when it is equal to $2$ being already covered. From 2.1 we know that $K$ contains an interval $K'$ of length at least $(p+q-r)-q=p-r$ that admits the translation $p' = p - q$. One has $p' \geqslant r$. If $p' = r$, $q$ is a multiple of $r$ and the same reasoning as above shows successively that $J$, hence $K$, hence $I$, hence $L$ admits the translation $r$. If $p' \neq r$, $K'$ admits the translations $p'$ and $q$. Since $r$ is again the greatest common divisor of $p'$ and $q$ and since the length of $K'$ is at least $p' + q - r = $ $= p - r$, the induction hypothesis shows that $K'$ admits the translation $r$. It follows as above that $J, K, I$ and $L$ have the same property. Q.E.D.

**2.3. Corollary.** *If the interval* $I$ *has step* $q$, *each translation* $p \leqslant$ $\leqslant \frac{1}{2} |I|$ *of* $I$ *is a multiple of* $q$.

**Proof.** Suppose indeed that $I$ admits the translation $p$ where $2q \leqslant 2p \leqslant |I|$. By the theorem above, $I$ admits the translation $r$ where $r$ is the greatest common divisor of $p$ and $q$, since its length is at least $p + q$. Since $q$ is the step, one must have $q \leqslant r$, hence $q = r$ showing that $p$ is a multiple of $q$. Q.E.D.

We spell out a (well known, cf. [15]) equivalent formulation in terms of words.

**2.3 bis.** *Assume that the word* $a \neq 1$ *satisfies an equation* $ba = ab'$ *where* $b \neq 1$ *and* $|a| \geqslant 2|b| - 1$. *There is a unique primitive word* $h$ *such that* $a = h^r h'$ *with* $h'$ *a prefixe of* $h$ *and either* $r \geqslant 2$ *or* $r = 1$ *and* $|h'| = |h| - 1$. *Then* $b$ *is a power of* $h$.

**Proof.** Let $a = Iw$ and apply 2.3. Q.E.D.

There is no confusion in writing $h = \sqrt{a}$ with the convention that $\sqrt{a} = a$ when the hypothesis of 2.3 bis are not satisfied. In the rest of this paper we shall say that an interval $I$ is *periodic* iff, in equivalent fashion, $a \neq \sqrt{a}$ where $a = Iw$, or iff $|I| \geqslant 2\|I\| - 1$. It will be said to be *r-periodic* iff it satisfies the stronger condition $|I| \geqslant r\|I\| + 1$ and *long* iff it is 4-periodic. The same terminology will be applied to the words and, accordingly, $a$ is a long periodic word iff $a = h^r h'$ with $r = 4$ and $h' \neq 1$ a prefix of $h$ or $a = h^r$ with $r \geqslant 5$.

Let $I = (i, i')$ be a long periodic interval and $p$ its step. Its *"internal* *zone"* is the interval $(i+p-1, i'-p+1) = I°$. Within it we distinguish the *"body"* $(i+2p, i'-2p)$, the *"left margin"* $I^g = (i+p, i+2p-1)$ and the *"right margin"* $I^d = (i'-2p+1, i'-p)$.

These notions are motivated by the next statements which allow to relate the geometry of the intervals with the study of syntactic monoids. For short we say that an index $n$ is *covered three times by the word* $y$ iff $n$ is contained in three *distinct* intervals $I, J$ and $K$ such that $y = Iw = Jw = Kw$.

**2.4.** *A necessary and sufficient condition that an index $t$ belongs to the body of some long interval $L$ is that it be covered three times by a word $y$. If this condition is satisfied, $y$ is 3-periodic and its step is the same as that of $L$.*

**Proof.** Assume that $L = (i, k')$ is a long interval whose body contains $t$. There exist a primitive word $h$ of length $P = \| L \|$, a prefix $h'$ of $h$ and an integer $k \geqslant 4$ such that $Lw = h^k h'$. One verifies immediately that the conditions are satisfied by the intervals $I = (i, k'-2p)$, $J = (i+p, k'-p)$, $K = (i+2p, k')$ since their intersection is the body $(i+2p, k'-2p)$ of $L$ and since the words $Iw, Jw$ and $Kw$ are all equal to $h^{k-2}h'$.

In the opposite direction assume that $t$ is covered three times by $y$, the corresponding supports being $I = (i, i')$, $J = (j, j')$, $K = (k, k')$. We can assume that $i < j < k$ and we have then $k \leqslant t \leqslant i'$ since $t$ must be contained in the intersection $(k, i')$ of the three intervals. By construction $J$ is contained in the union of $I$ and $K$. Thus, by reason of symmetry, we can suppose that its intersection with $I$ is at least as long as that with $K$, i.e. that the difference $q = j - i$ is at most equal to half the common length $|y|$ of $I, J$ and $K$.

Let $L' = (i, j')$ be the union of $I$ and $J$. The hypothesis $Iw = Jw$ entails that $L'$ admits the translation $q$, which is strictly less than half the length of $L'$. Applying the theorem of Fine and Wilf and its corollary we conclude that $L'$ is periodic and that its step $p$ divides $q$. Since $2q$ is at most equal to $|y|$, the same is true of $p$ and we have proved that $y$, hence $I, J$ and $K$, are periodic with step $p$.

The intersection $(k,j')$ of $K$ with $L'$ contains $(i',j')$ since $k \leqslant t \leqslant i'$ and this last mentioned interval has length $q \geqslant p$. Using again the same theorem, we see that the union $L$ of $L'$ and $K$ admits the translation $p$. In fact $p$ is its step because $p$ is the step of $J$. The relation $Jw = Kw$ implies that $p$ divides the difference $k' - j'$, hence that $p \geqslant k' - j'$. This last inequality entails that the length of $L$ is at least $4p$, i.e. that $L$ is long and one checks easily that $t$ is contained in the body of $L$. Q.E.D.

We introduce the term "complete" to express that a periodic interval $I = (i,i')$ is maximal among the sub-intervals of $C$ containing it and having the same step $p$. This is equivalent to the hypothesis that $(i-1)w \neq (i-1+p)w$ and $(i'+1)w \neq (i'+1-p)w$. It is clear that any periodic interval $I$ is contained in a complete interval $I'$ (having the same step) and that $I'$ contains any interval having the properties to admit a translation $p' \leqslant p$ and to contain $I$. $I'$ is the *completion* of $I$; its body contains the body of $I$ when $I$ is long.

**2.5.** *Let $I$ and $J \neq I$ be two complete long periodic intervals such that $\|J\| (= q) \leqslant \|I\| (= p)$ and that the body $J^\circ$ of $J$ meets one of the margins $I^\times$ of $I$. Then $3q < p$ and $I^\times$ contains one of the margins of $J$.*

**Proof.** Let $K$ be the intersection of $I$ and $J$. Its length is at most $p + q - 2$. Indeed, otherwise, the union $L$ of $I$ and $J$ would admit the translation $r \leqslant p,q$ by the theorem of Fine and Wilf, where $r = p$ and $r = q$ according to the definitions of $q$ and $p$ as the steps of $J$ and of $I$. Therefore, one would have $p = q$, hence $L = I = J$ since $I$ and $J$ are supposed to be complete, in contradiction with our initial hypothesis that $I \neq J$.

This remark shows that $I$ is not contained in $J$, since, otherwise, one would have $K = I$ where $I$ has length at least $4p + 1$ (because it is long) giving the inequality $1 + 4p \leqslant p + q - 2$ which contradicts the hypothesis $q \leqslant p$. In similar fashion, one verifies that if $J$ is contained in $I$ one has $1 + 4q \leqslant p + q - 2$, hence $3q < p$.

Assume now that for instance the body $J^\circ = (j + 2q, j' - 2q)$ of

$J$ meets the left margin $I^g = (i+p, i+2p-1)$ of $I$. Suppose also that the left margin $J^g = (j+q, j+2q-1)$ is not included in $I^g$. We have the inequalities $j+q \leqslant i+p \leqslant j+2q-1$ where $j+2q-1 \leqslant \leqslant i+2p-1$ in view of $q \leqslant p$. It follows that the intersection $K$ contains the interval $(j+2q, j+3q-1)$ which has length $q$. Also $i<j$ since, otherwise, $K$ would contain the interval $(i, i+p-1)$ disjoint from the previous one, in contradiction to $|K| \leqslant p+q-2$. Accordingly, $K$ contains the initial interval of length $q$, $(j, j+q-1)$ of $J$. Since $j+q < i+p$, the same inequality on the length of $K$ entails that $J$ does not contain the left margin $I^g$, i.e. that $J' < i+2p-1$ and this shows that $I^g$ contains the right margin of $J$. Q.E.D.

Recall that the internal zone of a long interval is the union of its body with the two margins.

**2.6. Periodicity lemma.** *Let $L'$ $(\neq \phi)$ be an interval such that any of its indices is covered three times by a word and assume that $L'$ is maximal among the intervals having the same property. There exists a long periodic interval $L$ whose body is contained in $L'$ and whose internal zone strictly contains $L'$. The step of $L$ is equal to the maximum of the steps of the intervals used to cover $L'$.*

**Proof.** According to 2.4, any index $t$ of $L'$ is contained in the body of a long interval $L_t$ having step $p_t$. Choose $t$ such that $p_t$ be maximum and let $L$ be the completion of $L_t$. By the same remark all the indices of $L^\circ$ are covered three times. Thus $L^\circ$ is contained in $L'$ in view of the extremal character of $L'$. To conclude the proof it suffices to show that at least one index belonging to a margin of $L$ is not in $L'$. We do this by showing that the opposite hypothesis on (say) $L^g$ leads to the construction of an infinite nested family of periodic intervals, which is impossible.

Let $t'$ be an index of $L^g$ which belongs to $L'$. It can be choosen so that the corresponding step $p' = p_{t'}$ is maximum. By our initial hypothesis $p'$ is not greater than $p_t$ and the long interval $L_{t'}$ has a body meeting the margin $L^g$. The same is true of its completion $L_1$ and we have $L_1 \neq L$ since $L$ is complete. Thus, by 2.5, one of the margins of

$L_1$ is contained in $L^g$ and $p'$ is strictly smaller than $P_t$. Again, if this margin of $L_1$ was to contain an index belonging to $L'$, we could repeat the same construction obtaining a new long complete interval $L_2$ of step $p'' < p'$ which would have a margin contained in that of $L_1$, etc. Q.E.D.

The reader will notice that in the case of the monoid of functions alluded to in the introduction, the above proof does not go through without some supplementary assumption of "smoothness" forcing the conclusion at the end of the argument. The same remark applies to the second periodicity lemma.

In the next statements we say that an index $n$ of the basic interval $C = (1, m)$ is *covered three times by the suffixes* of a word iff there exist three intervals $K = (1, k)$, $J = (j', j)$, $I = (i', i)$ such that $1 \leqslant j' \leqslant i' \leqslant \leqslant n \leqslant k < j < i$ and that on the one hand the word $Kw$ is a suffix of the word $Iw$ and, on the other hand, either $Jw = Iw$ (in which case, of course, $i' - j' = i - j$) or $Jw$ is a suffix of $Iw$ and then $j' = 1$.

In similar fashion, we shall use the phrase "*covered three times by the prefixes*" to express the symmetric notion obtained when exchanging the indices 1 and $m$, the direction of the inequalities and the terms prefix and suffix.

2.7. *Let $n$ be an index of $C$ which is covered three times by the suffixes of a word. Then*

(1) *The initial interval $(1, i)$ admits the translation $d = i - j$.*

(2) *If there is a long periodic interval $H = (h', h)$ with $j \leqslant h$ such that its left margin contains $n$, the completion of $H$ is an initial interval of $C$.*

**Proof.** The hypothesis that $Jw$ is equal to $Iw$ or to one of its suffixes implies that the interval $(j', i)$ admits the translation $d\ (= i - j)$. Thus, (1) is proved when $j' = 1$. If it is not so, we must have $Jw = Iw$ hence $i' - j' = d$. Since $Kw$ is a suffix of $Jw$, the interval $(1, j)$ admits the translation $d' = j - k$. The length of its intersection with $J$ is at least $d + d'$ (because $i' \leqslant n < i$). According to the Fine – Wilf theorem, $J$, hence the union $(1, i)$ of $K, J$ and $I$ are periodic with a step $p$ dividing $d$ and $d'$. This concludes the proof of (1).

Assume now that the hypothesis of (2) are fulfilled. We have just seen that $(1, j)$ admits the translation $d'$. The length of its intersection with $H$ is at least $d + r$ where $r$ is the step of $H$. Accordingly, as above, $(1, h)$ is periodic with a step $r'$ dividing $r$ and $d'$. Since $r$ is the step of $H$, we must have $r \leqslant r'$. Thus $r = r'$, concluding the proof. Q.E.D.

**2.8. Second periodicity lemma.** *The basic interval* $C = (1, m)$ *is* 3-*periodic iff each of its indices is covered three times by a word or by the suffixes or by the prefixes of a word.*

**Proof.** The proof that this condition is sufficient proceeds in the same manner as above and it can be omitted.

Reciprocally, assume that the covering condition is fulfilled.

There is a largest index $k \geqslant 1$ that is covered three times by the suffixes of a word, the corresponding intervals being $K, J, I$ as above. Symmetrically, there is a least index $f$ that is covered three times by the prefixes of a word the corresponding intervals being $F = (f, m)$, $G = (g, g')$, $Q = (q, q')$ with $q < g < f \leqslant q' \leqslant g' \leqslant m$ (= the last index of $C$).

Suppose first that $g \leqslant j$. The intersection $(q, i)$ of $(1, i)$ and $(q, m)$ has length greater or equal $d + e$ where $d = i - j$ and $e = g - q$. Using the last result and the Fine – Wilf theorem, one concludes that their union (which is $C$) is periodic with a step $r$ dividing $d$ and $e$ and one checks easily that in fact $C$ is 3-periodic.

We can therefore suppose that $j < q$, an assumption which entails that no index in the non-empty interval $(k, f)$ is covered three times by the prefixes or the suffixes of a word. Since each of them must be covered three times anyway, we can use the first periodicity lemma to establish the existence of a long periodic interval $H$ whose internal zone strictly contains $(k, f)$. If $r$ is its step, this quantity is also the length of its margins. It follows that $H$ has an intersection of length at least $r + d$

(resp. $r+e$) with the interval $(1,i)$ (resp. with $(q,m)$) and the desired conclusion is obtained as above. Q.E.D.

Taking a 5 letters alphabet $A=\{a,b,c,d,e\}$ and letting $x=abc$; $u=xdxdx$; $v=dxexd$, the example of the word $w=c(vu)^3va\ (=Cw)$ shows that the hypothesis of the lemma do not imply that $w$ is long.

Various other applications of the theory of Fine and Wilf can be found in the literature (cf. [13], [15] and [5]). We record here two simple observations for later reference.

**2.9.** *Let $T$ be a non-empty subsemigroup of $A^+$. Each of the following conditions implies that it is contained in a cyclic subsemigroup $h^+$ of $A^*$.*

(i) *For some $\epsilon>0$, any word $w$ in $T$ has a periodic factor $w'$ of length $|w'|\geqslant \epsilon|w|$.*

(ii) *There are words $f,f'$ such that $ft^+t'^+f'$ contains a non-primitive word for any $t,t'$ in $T$.*

*In* (ii) *there are $h',h''$ satisfying $h'h''=h$ or $=1$ such that $f$ is in $h''\cdot h^*$ and $f'$ in $h^*\cdot h'$.*

**Proof.** Take in $T$ a fixed $t$ which can be assumed to be a power $t=h^r$ of a primitive word $h$.

For (i) let $u$ be any word in $T$ and consider the word

$$w=t^2u^2t^3u^3\ldots t^ku^k\ldots t^nu^n$$

where $n$ is large enough for $t^n$ and $u^n$ to have both a length less than $\frac{1}{8}\epsilon|w|$. Then any periodic factor $w'$ of $w$ of length $\geqslant\epsilon|w|$ has the form $gt^ku^k\ldots t^{k'}u^{k'}g'$ with $k'\geqslant k+2$. The hypothesis that it is periodic implies that $t^ku^k$ is (equal to) a factor of $t^{k''}u^{k''}t^{k''+1}u^{k''+1}$ where $k\leqslant k''\leqslant k'-1$. Replacing $t$ by $h^r$ and using the hypothesis that $h$ is primitive shows that $u$ must also be a power of $h$ and it establishes the result.

For (ii) we can assume that $t$ is longer than $f$ and $f'$. Take now any power $t'$ of an arbitrary word of $T$ and choose it so that its length satisfies the same condition as that of $t$. The existence of a non-primitive word $w = ft^k t'^{k'} f'$ implies as above that $w$ is a power of a word conjugate with $h$ and the result follows by identifying the initial and final factors $f$ and $f'$.

## 3. THE MONOID OF INTERPRETATION

In this section and in the next one we consider a fixed non-empty subset $X$ of the free semigroup $A^+ = A^* \setminus 1$ and we assume that it is the minimal generating set of $X^+$, i.e. that its intersection with $X^+X^+$ is empty. The set $X(A^+)^{-1}$ (resp. $(A^+)^{-1}X$) of its prefixes (resp. suffixes) will be denoted by $P$ (resp. by $Q$). We also consider another alphabet $B$ and a bijection $\alpha$ of $B$ into $X$ which is extended to a morphism into $A^*$ of the free monoid $B^*$.

An *interpretation* of a word $a$ in $A^*$ is a triple $y = (q, b, p)$ in $Q \times B^* \times P$ such that $a = q \cdot b\alpha \cdot p$ $(= y\alpha)$ and $a\beta$ will be the set of the interpretations of $a$. Thus, $(1, 1, 1)$ is the only interpretation of the neutral element $1$ of $A^*$ and no other word admits it as an interpretation.

In the following definitions, $a$ (resp. $b, p, q$) denotes an arbitrary element of $A^*$ (resp. of $B^*, P, Q$); $c$ is either a letter of $B$ or the neutral element $1$.

$[p, a] = pa$ if $pa$ is in $P$ and $= \phi$ otherwise;

$[a, q] = aq$ if $aq$ is in $Q$ and $= \phi$ otherwise;

$[p, q] = c$ if either $p = q = 1$ or $p, q \neq 1$;
$pq = c\alpha$; and $[p, q] = \phi$ otherwise.

Also we use the following Boolean matrices:

$C$ = the $P \times Q$ matrix such that its $(p, q)$ entry is $1$ iff $[p, q] \neq \phi$;

$a\pi =$ the $P \times P$ matrix such that its $(p, p')$ entry is $1$ iff $pa = p'$;

$a\chi =$ the $Q \times Q$ matrix such that its $(q', q)$ entry is 1 iff $aq = q'$;

$a\gamma =$ the $Q \times P$ matrix such that its $(q, p)$ entry is 1 iff $a$ admits an interpretation of the form $(q, b, p)$ for at least one word $b$.

$a\mu = C \cdot a\gamma + a\pi.$

The only reason for using Boolean matrices instead of (binary) relations is typographic convenience.

A simple remark allows connecting the product on $A^*$ with one on the set of interpretations.

**3.1.** *For any two words* $a$ *and* $a'$ *the set of interpretations of* $aa'$ *is the union over all the interpretations* $y = (q, b, p)$ *of* $a$ *and* $y' = (q', b', p')$ *of* $a'$ *of their product*

$$yy' = (q, b, [p, a']) + (q, b \cdot [p, q'] \cdot b', q') + ([a, p], b', p').$$

**Proof.** It follows immediately from the definitions that each term written is an interpretation of $aa'$ or $\phi$.

Reciprocally, consider an interpretation $y'' = (q'', b'', p'')$ of $aa'$. When $a' = 1$, it is also an interpretation of $a$ and it appears in the product since $y'' = (q'', b'', [p'', a'])$. A symmetric remark applies when $a = 1$ and we assume henceforth that $a, a' = 1$.

If the word $a$ has a length $|a|$ greater of equal that of $q'' \cdot b''\alpha$, there is a prefix $p$ such that $y = (q'', p'', p)$ is an interpretation of $a$. One has $[p'', a'] = p''$ showing that $y'' = (q'', b'', [p, a']$ is in the product. The same holds if $|a| \leqslant |q''|$ because this inequality is equivalent to $|b''\alpha \cdot p''| \leqslant |a'|$. In the remaining case there is a factorization $b'' = bcb'$ with $[p, q'] = c$ such that $a = q'' \cdot b\alpha \cdot p$. Then $y = (q'', b, p)$ and $y' = (q', b', p'')$, are interpretations of $a$ and of $a'$ whose product contains $y''$. Q.E.D.

We recall that the *residual* of a subset $K$ of any monoid $T$ is the set of all $t$ in $T$ such that $K$ does not meet the ideal $TtT$. Therefore it is always an ideal (possibly empty). It is clear that when $T$ is the free monoid $A^*$ and when $X$ is finite the residual of $X$ contains all the words longer than its longest element. We summarize the properties of $\mu$ which will be needed later.

3.2. *The mapping* $\mu$ *is a morphism. It recognizes* $X^*$. *Further:*

– *for any word* $a$ *the* $(p,p)$ *entry of the matrix* $a\mu$ *is* $1$ *iff* $a$ *has an interpretation of the form* $(q,b,p)$ *for some suffix* $q$ *such that* $[p,q] \neq \phi$;

– *if one of the words* $a$ *and* $a'$ *is in the residual of* $X$, *one has* $(aa')\mu = a\mu \cdot a'\mu$;

– *the residual of* $X^*$ *is the inverse image of the zero* $P \times P$ *matrix.*

**Proof.** It is clear that $\pi$ and $\chi$ are two morphisms and that they reduce to $0$ on the residual of $X$. They satisfy the intertwinning identity $a\pi \cdot C = C \cdot a\chi$ because $C(pa,q) = C(p,aq)$ for any $a,p,q$.

The formula given for the product of interpretations translates into the identity

$$(aa')\gamma = a\gamma \cdot a'\pi + a\gamma \cdot C \cdot a'\gamma + a\chi \cdot a'\gamma.$$

Multiply it on the left by $C$ and add $(aa')\pi = a\pi \cdot a'\pi$ to both members. Since $C \cdot a\gamma \cdot a'\gamma = a\pi \cdot C \cdot a'\gamma$, one can regroup terms and one obtains the identity $(aa')\mu = a\mu \cdot a'\mu$ which establishes that $\mu$ is a morphism.

It is clear that $1\pi = 1\mu$ is the unit $P \times P$ matrix and that every diagonal entry of $a\pi$ is $0$ when $a \neq 1$. Thus, for $a$ in $A^+$, the $(p,p)$ entry of $a\mu$ is $1$ iff there is a $q$ such that $C(p,q) = a\gamma(q,p) = 1$, which is the result stated because of the definition of $C$ and of $\gamma$. Also $(aa')\mu = C \cdot a\gamma \cdot C \cdot a'\gamma = a\mu \cdot a'\mu$ when $a$ or $a'$ is in the residual of $X$ since then the matrix $a\pi$ or $a'\pi$ is $0$.

Consider now the entry $(1,1)$ of $a\mu$. It is $1$ when $a = 1$. When $a \neq 1$ it is $1$ iff there is a suffix $q$ such that $[1,q] = 1$ and that $a$ has an interpretation of the form $(q,b,1)$. The first condition implies that

$q = 1$ and then, the second is equivalent with $a \in X^*$. Thus $\mu$ recognizes $X^*$.

Suppose that the $(p, p')$ entry of $a\mu$ is 1. There is a suffix $q'$ such that $p'q'$ is in $X$, if $p' = 1$ and that $p'q' = 1$ otherwise. In both cases $paq'$ is in $X^*$ as we have just seen and, consequently, $a$ is not in the residual of $X^*$. In the opposite direction, if $a\mu$ is 0, no matrix $(a'aa'')\mu$ can have its $(1, 1)$ entry equal to 1 and $a$ is in this residual. Q.E.D.

It may be mentioned that $X^*$ is also recognized by $\gamma$ since the $(1, 1)$ entry of $a\gamma$ is 1 iff $a$ has an interpretation of the form $(1, b, 1)$, i.e. iff it is in $X^*$. The formula given in the preceding proof shows that the restriction of $\gamma$ to the residual of $X$ is a morphism with respect to the "sandwich" multiplication $(aa')\gamma = a\gamma \cdot C \cdot a'\gamma$. For the whole of $A^*$, the mapping $(\pi, \gamma, \chi)$ is a morphism (with the indicated product for $\gamma$).

We call $M = A^*\mu$ *the monoid of interpretations* of $X^*$. The syntactic monoid $S$ of $X^*$ is a quotient of $M$ in view of the minimal character of $S$ and of the fact that $\mu$ recognizes $X^*$. The reader will notice the relationship between $M$ and the left to right non deterministic automaton realizing the relation from $B^*$ to $A^*$ which is the inverse of the morphism $\alpha$.

When $X$ is finite the same is true of $P$, hence of $M$. It is a known fact that under this hypothesis every group in $S$ is a quotient of a group in $M$. The same holds when $X$ is a recognizable set in the sense of S. Eilenberg but we shall not make use of this generalization.

These notions are illustrated by the following example which shows that except in a very special case the morphism $\mu$ also recognizes $\{1\}$, hence the semigroup $X^+$.

**Example.** A necessary and sufficient condition that $w\mu = 1\mu$ for some $w_1 = w \neq 1$ is the existence of $d \geqslant 1$ and a letter $a$ such that $X$ consists of $a^d$ and of words of the form $a^{d'}a'$ with $d' \leqslant d - 1$ and $a'$ a letter different from $a$.

Reciprocally, if $X$ has this form, $M$ has a subgroup of order $d$ whose inverse image is $a^*$ and $w_1$ is a power of $a^d$.

**Proof.** Assume first that $X$ has the form indicated. The set of the prefixes $P$ consists of the words $a^{d'}$ with $d' \leqslant d-1$. The matrix $a\pi$ has a 1-entry for the pairs $(a^{d'}, a^{d'+1})$ where $d'+1 \leqslant d-1$. One has $C(p,p') = 1$ iff $p = p' = 1$ or if $p, p' \neq 1$ and $pp' = a^d$. Since the only interpretations of $a$ are $(a, 1, 1)$ and $(1, 1, a)$ one sees that $a\mu$ is the cyclic matrix $m$ obtained when adding the 1-entry $(a^{d-1}, 1)$ to $a\pi$. For any other letter $a'$ and prefix $p$, the line $p$ of $a'$ is zero if $pa'$ is not in $X$ and it has a single 1-entry in the column 1 otherwise. This shows that the condition is sufficient and that the *subgroup* of $M$ (i.e. the maximal group in $M$ whose idempotent is 1) has the properties stated.

In the opposite direction, assume $w \neq 1$ and that the matrix $w\mu$ contains $1\mu$, i.e. that all its diagonal entries are 1. As we have seen it, this implies that $w$ is in $X^*$ and that it has an interpretation $(q, b, p)$ for each prefix $p$ in $P$. Thus, if $a$ is the last letter of $w$, it is also the last letter of any prefix $p$ and since $P$ contains every left factor of its members we see that it consists of the powers $a^k$ of $a$ for $k \leqslant d-1$ where $d$ is the length of the longest word in $X$.

Consider the prefix $p = a^{d-1}$. Since $w(p,p) = 1$ there is a suffix $q$ such that $[p,q] \neq \phi$ and $w = qxp$ for some $x$ in $X^*$. The first relation implies $q \neq 1$ and the maximal character of $d$ that $q$ is the first letter of $w$. Since $w$ is in $X$, this letter is a prefix in $P$, hence it is $a$, proving that $X$ contains the word $a^d$. It follows, as above, that $a\mu$ contains the cyclic matrix $m$.

Assume now that $w\mu = 1\mu$. It is in the subgroup of the monoid of the $P \times P$ Boolean matrices. Thus $a'\mu$ is a permutation matrix for any letter $a'$ which is a factor of $w$, hence in particular for $a$ (since $a$ is the first letter of $w$). It follows that $a^d$ is the only power of $a$ which is in $X$ because $a^k$ in $X$ implies that the $(a^{k-1}, 1)$ entry of $a\mu$ be 1. This shows that $X$ has the form indicated and computing $a'\mu$ for a letter $a' \neq a$ establishes that it is not a permutation matrix. Thus, $w$ is a power of $a^d$. Q.E.D.

We recall that a $P \times P$ matrix $m$ has finite *rank* $\leqslant r$ iff there is a subset $K$ of at most $r$ elements of $P$ such that $m$ admits a factorization $m = m'hm''$ where $m'$ (resp. $m''$) is a $P \times K$ (resp. $K \times P$) matrix and $h$ a $K \times K$ matrix. If it is so, all the matrices in the ideal $MmM$ have the same property and, more accurately, it is isomorphic to a semigroup of $K \times K$ matrices. These notions apply as well to the case of the Boolean matrices with which we are concerned here.

**3.3.** *A necessary and sufficient condition for the monoid of interpretations $M$ to have a 0-minimal ideal completely 0-simple and a finite Suschkewitsch group $G$ is that $X$ and $X^*$ have different residuals.*

**Proof.** Since $X$ is contained in $X^*$, its residual contains the residual of $X$. Thus, if these two residuals are not equal we can find a word $w$ in $X^*$ which belongs to the residual of $X$. Suppose it is so and consider an interpretation $(q, b, p)$ of $w$. One has $b \neq 1$ or $p, q \neq 1$ and the matrix $w\pi$ is $0$. It follows instantly that the matrix $a\mu = C \cdot w\gamma + w\pi$ has a rank at most equal to the length of $w$. Thus $M \cdot w\mu \cdot M$ is an ideal not reduced to $0$ in which all the matrices have a finite rank. This shows that $M$ has a completely 0-simple 0-minimal ideal. Taking $w$ such that $w\mu$ has a minimal rank, the bi-ideal $wMw$ is finite and it is isomorphic to the group $G$. This proves that the condition stated is sufficient. Since the syntactic monoid of $X^*$ is a quotient of $M$ we see that it also enjoys the same property.

Reciprocally, suppose that $M$ has a 0-minimal completely 0-simple ideal $D' + 0$ and that the group $G'$ is finite. This is also true of the syntactic monoid $S$ and we denote the corresponding objects by $D$ and $G$. We can assume that $G$ meets the image of $X^*$ in $S$. Since $G$ is finite and $X^*$ is a semigroup, the idempotent $u$ of $G$ belongs to the image of $X^*$. Since $D$ is 0-simple, there is a subgroup $H$ of $G$, a union $R$ of $\mathscr{R}$-classes of $D$ and a union $L$ of $\mathscr{L}$-classes of $D$ such that the intersection $E$ of $D$ with the image of $X^*$ is the set of all the elements $d$ belonging to $R$ and $L$ which satisfy $udu \in H$.

We now construct a finite sequence $(g_0 = u, g_1, \ldots, g_n)$ of elements of $G$ having the property that for any $g$ in $G$ one has $u = gg_0g_1 \dots g_i$ for at least one index $i$. This is possible since $G$ is a finite group.

Also, for each $g_i$, we take a word $a_i \neq 1$ in its inverse image. Having selected $g_n$ so that $g_0g_i \dots g_n = u$, the product $w = a_0a_1 \dots a_n$ is in $X^2X$ and we have only to verify that it belongs to the residual of $X$.

Suppose to the contrary that $awa'$ is in $X$ for some pair of words $a$ and $a'$, and let, for an arbitrary $i$, $d$ and $d'$ be the images of the words $aa_0 \dots a_i$ and $a_{i+1} \dots a_na'$. Since $D$ is 0-simple, $d$ and $d'$ belong to the intersection of $R$ and of $L$ and the same is true of $udu$ and $ud'u$. Further $udd'u = uduud'u$ is in the subgroup $H$. Choose $i$ in such a way that $udu = u$. We have also $ud'u$ in $H$ and, accordingly, $d$ and $d'$ both belong to the image $E$ of $X^*$ in $D$. This shows that $aa_1 \dots a_i$ and $a_{i+1} \dots a_n$ belong to $X$, and, in fact, to $X^+$. Thus $awa'$ is in $X^+X^+$, in contradiction with our initial hypothesis that $X$ is disjoint from this set (because we assumed that $X$ was a minimal generating set). Q.E.D.

From now on we shall let $W$ denote the set of the words which belong to the residual of $X$ and not to that of $X^*$. It is clear that if $X$ is finite, $W$ contains every long enough word which is not in the residual $0\mu^{-1}$ of $X^*$.

**3.6.** *Every element $g$ in $M$ such that the intersection $W_g$ of its inverse image with the residual $W$ is not empty, has a finite order (i.e. it has a positive power which is idempotent).*

**Proof.** Take a word $w$ in $W_g$ and let $P'$ (resp. $Q'$) be the set of the prefixes (resp. suffixes) which can appear as the prefix (suffix) component of one of its interpretations. It is a finite set since the lengths of its elements is bounded by the length of $w$. Further, $P'$ and $Q'$ contain the corresponding sets for any positive power $w^n$ because $w$ is in $W$. Therefore any non zero entry of the matrix $w^n\gamma$ is in its $Q' \times P'$-part. It follows that the number of different matrices $w^n\gamma$ is bounded in function of the number of elements of $P'$ and $Q'$; the same applies to the matrices $w^n\mu = C \cdot w^n\gamma$ etc. The rest of the argument is a classical one. Q.E.D.

If $u$ is an idempotent, we let $G_u$ denote the (necessarily unique) maximal group containing it. We say that $u$ (or $G_u$) is *strongly cyclic* iff its inverse image does not reduces to $\{1\}$ (i.e. if it meets $A^+$) and it is contained in a cyclic submonoid of $A^*$, that is, in a submonoid generated by a single word.

**3.5.** *Assume that $u$ is a strongly cyclic idempotent. Then:*

– *there is a unique primitive word $h$ called the root of $G_u$, such that the inverse image of $G_u$ is contained in $h^*$;*

– *$G_u$ is a finite cyclic group and $MuM$ is a maximal principal idempotent ideal or $M$ itself depending upon whether $u \neq 1$ or not;*

– *the conjugacy class of $G_u$ consists of groups having the same properties; the corresponding roots are the words conjugate with $h$;*

– *there is at most* Card $(X)$ *conjugacy classes of such groups such that their root $h$ has the following further property: there is a word $x$ in $X$ of length $|x| = 2|h| - 1$ or $= |h|$ which is a factor of a word in $h$.*

**Proof.** Since the inverse image of $u$ is an infinite semigroup, we can apply 2.9 to conclude to the existence of a unique primitive word $h$ such that it is contained in $h^*$. The fact that the inverse image of $G_u$ is contained in the same cyclic submonoid follows from the observation that the inverse image of $u$ meets $a^n A^*$ for any $n$ and any word $a$ in the inverse image of $G_u$. It is then a classical exercise to show that $G_u$ is a finite cyclic group. The last assertion of 2.9 shows that $MuM$ is contained in $MvM$ where $v = v^2 \neq 1$ iff the inverse image of $v$ is contained in the cyclic submonoid generated by a word conjugate with $h$. Thus $MuM$ is maximal (as a proper principal idempotent ideal of $M$) unless $u = 1$.

Suppose now that the root $h$ and the word $x$ satisfy the supplementary conditions stated. There is a unique word $h'$ conjugate with $h$

which is a prefix of $x$. Returning to the notions developped as the beginning of Section 2, we see that in fact one has $h' = x$ since $h'$ is primitive, and since either $h' = x$ of $h''h''$ with the inequality on the lengths stated. This provides an injection into $X$ of the corresponding classes. Q.E.D.

For later reference we call *special* the strongly cyclic idempotents (or their maximal groups) satisfying the supplementary condition at the end of 3.5.

Let us recall that if $u$ is an idempotent $P \times P$ (Boolean) matrix there exists a maximal partial equivalence relation, noted $\hat{u}$, on $P$ whose support is contained in $u$ (i.e. which is such that the $(p, p')$ entry of $u$ is 1 for every pair $(p, p')$ in $\hat{u}$). Its proper domain will be noted $P_u$. One knows that a group in $M$ having $u$ as its idempotent is a permutation group on the $\hat{u}$-classes of $P_u$. Therefore its degree, $\deg(u)$, is the number of these classes. It is zero iff $u = 0$.

To do this we consider an interpretation $y = (q, b, p)$ of a word $w$ and we say that it is *repeatable* iff $[q, p] \neq \phi$, this implies that any positive power of $w$ has an interpretation having the same suffix and prefix components, $q$ and $p$, as $y$. Another interpretation $y_2 = (q_2, b_2, p_2)$ of $w$ is *linked* with $y$ iff there are factorizations $b = b'b''$ and $b_2 = b'_2 b''_2$ such that the words $q \cdot b'\alpha$ and $q_2 \cdot b'_2\alpha$ have the same length; otherwise, $y$ and $y_2$ are *separated.*

The following observations supply the connection between the Fine – Wilf theory and its applications in the next section.

**3.6.** *Assume that the maximal group* $G = G_u$ *has an element* $g$ *whose inverse image has a non empty intersection* $W_g$ *with the residual* $W$. *Then, if* $G$ *is not strongly cyclic, every* $W_g$ *contains an infinity of primitive words. In any case:*

– *every word in* $W_u$ *is conjugate with a word in* $X^*$*;*

– *any word* $w$ *in* $W_u$ *admits a system of* $d = \deg(u)$ *pairwise separated repeatable interpretations; further, for any two of them, say*

*$y_1$ and $y_2$, there is no chain $(y_1, y_2, \ldots, y_n)$ of interpretations of $w$ such that each $y_i$ is linked with $y_{i+1}$.*

**Proof.** Assume $w'$ in $W_g$. The ideal $A^*w'A^*$ meets $W_u$ since $g$ has an inverse. Thus $W_u$ is a non empty semigroup. Assuming for a moment that $u$ is not strongly cyclic the assertions concerning the primitive words follow from 2.9.

Consider a word $w$ in $W_u$ and a prefix $p$ such that the $(p, p)$ entry of the matrix $u$ is $1$. Since $w$ is in the residual of $X$ we know that this is equivalent with the existence of an interpretation $y = (q, b, p)$ of $w$ such that $[p, q] \neq \phi$. The word $b\alpha \cdot pq$ is conjugate with $w$ and it is in $X^*$ by construction, proving the second assertion.

Let $y_2 = (q_2, b_2, p_2)$ be another interpretation of $w$ and suppose that it is linked with $y$. Using the same notations as above we see that $w$ admits the interpretations $(q, b'b_2'', p_2)$ and $(q_2, b_2'b'', p)$. Therefore the entries $(p, p_2)$ and $(p_2, p)$ of $u$ are $1$ and the same is true of the entry $(p_2, p_2)$ since $u$ is idempotent. We conclude that the class of the prefix $p$ in the equivalence $\hat{u}$ contains any prefix which is linked with it in this manner and the truth of the last assertion follows. Q.E.D.

## 4. APPLICATIONS

We come to the proof of the main results stated in the introduction. To simplify we make the standing assumption that the generating set $X$ of $X^*$ has a finite number $k \geqslant 2$ of words and that it has not the very special from displayed in the example of the last section. Letting $L$ denote the maximum of the lengths of the words of $X$, we have that the inverse image $u\mu^{-1}$ of any idempotent $u$ in the monoid of interpretations $M$ has an intersection $W_u$ with the residual $W$ of $X$ that is an infinite semigroup and that $W$ contains $A^L A^+$.

We recall the notion of a *special group* in $M$ introduced in 3.5 and that the number of their conjugacy classes is at most $k$. By 3.6 and the finiteness of the complement of $W$ every conjugate class of groups in $M$ has a member such that its idempotent is in the image of $X^*$.

**4.1.** *Any idempotent* $u \neq 1$ *of degree* $2k+1$ *or more is special.*

**Proof.** Let $u = u^2 \neq 1$ have degree $d \geqslant 2k+1$ and take any primitive word $h$ having a power $h^r$ in its inverse image. We can choose $r$ large enough for the length $m$ of $w = h^r$ to satisfy the inequality $m \geqslant 2L + 4|h|$.

As explained in the beginning of Section 2 we consider $w$ as a mapping in $A$ of the basic interval $C = (1, m)$. Let $j$ be any index in the sub-interval $L' = (L+1, m-L)$. By 3.4 we know that $w$ has a system $Y$ of $d$ pairwise separated repeatable interpretations. If $y = (q, b, p)$ is any one of them, our choice of $j$ implies a factorization $b = b'cb''$ where the support $I_y$ of $c$ contains $j$, i.e. where $c\alpha$ is a word $x_y$ of $X$ and where $|q \cdot b'\alpha| < j \leqslant |q \cdot (b'c)\alpha|$. Since $d \geqslant 2k+1$ there are three interpretation for which the word $x$ is the same. Therefore our hypotheses imply that every index in $(L+1, m-L)$ is covered three times. Applying the First Periodicity Lemma of the Fine – Wilf theory, we conclude that it is a long periodic interval. By the same lemma its step $p$ is the step of one of the covering words $x$ in $X$. Further, $L'$ admits the translation $|h|$ because of our choice of the exponent $r$. Applying once more the Fine – Wilf theory we conclude that the length of $h$ is exactly $p$ since it is a primitive word. The conclusion follows from 2.9 since it applies to any word $h$ having a power in $u\mu^{-1}$. Q.E.D.

**Observation.** For each word $x$ in $X$ let $r(x)$ be $0$ if $x$ is not a factor of a word of $h^*$. In the opposite case, let $r(x) = 2$ if $|x| \leqslant 2|h|$ and $r(x) = p$ if $p \geqslant 3$ is the least integer such that $|x| \leqslant p|h|$. Since every index $j$ can be covered three times by a word $x$ only if $r(x) \geqslant 3$, one sees that the degree $d$ is at most equal to the sum of the numbers $r(x)$.

**4.2. Corollary.** *Apart from at most* $k$ *conjugate classes of maximum cyclic groups that generate maximal idempotent principal ideals, every group in the monoid of interpretations or in the syntactic monoid of* $X^*$ *divides the symmetric group of order* $(2k)!$.

**Proof.** This is just a reformulation of the previously established result since every group in $S$ is a quotient of a group in $M$. Q.E.D.

From now on, we let $U$ denote the set of the idempotents $u \neq 0, 1$ which are not special, and we proceed with the proof of other absolute finiteness properties concerning the ideal $MUM$. If $R$ is a subset of $P$, let $e_R$ denote the idempotent diagonal $P \times P$ matrix such that its entry $(p, p')$ is 1 iff $p = p'$ is an element of $R$. A pair $(F, F')$ of subsets of $A^+$ will be said to be a *R-factorization* of the subset $K$ of $M$ iff:

(i) $F = A^*F$, $F' = F'A^*$ and $K$ is contained in the image of $FF'$ by $\mu$;

(ii) For any $f$ in $F$ and $f'$ in $F'$, one has $(ff')\mu = f\mu \cdot e_R \cdot f'\mu$.

To motivate this notion we apply it in the following remark.

**4.3.** *Assume that* $(F, F')$ *is a* $R$*-factorization of an ideal* $K$*. The number of idempotent principal ideals in* $K$ *is at most* $2^n$ *where* $n = (\mathrm{Card}\, R)^2$.

**Proof.** Consider an idempotent $u$ in $K$ and a $R$-factorization $(f, f')$ of $u$. Since $u = u^3$, one has $u = (ff'ff'ff')\mu$. The matrix $m_u = (f'ff'f)\mu$ generates the same ideal as $u$ since it is contained in $MuM$ and since $u$ is in $Mm_uM$.

Because of condition (ii) and of the fact that $F$ is a left ideal and $F'$ a right one, we have also $u = f\mu \cdot m'_u \cdot f'\mu$ where $m'_u = e_R \cdot M_u \cdot e_R$.

Let now $v$ be another idempotent in $K$ and $m_v$ and $m'_v$ the corresponding matrices. Suppose further that $m'_u = m'_v$. Again by (ii) we have $u = f\mu \cdot m'_u \cdot f'\mu = f\mu \cdot m'_v \cdot f'\mu = f\mu \cdot m_v \cdot f'\mu$ showing that $u$ is in $MvM$ since $m_v$ is in $MvM$. By symmetry, $Mum = MvM$. The result follows since the number of classes for the equivalence defined by $m'_u = m'_v$ is certainly less than the number of Boolean $R \times R$ matrices. Q.E.D.

For each word $x$ in $X$ let $U(x)$ denote the set of the idempotents $u$ in $U$ which have the property that $x$ has a maximum length among the words $x'$ in $X$ such that $MuM$ is contained in the image of $Ax'A$, i.e. among the $x'$ which are a factor of at least one word in the inverse image of $u$. It is clear that we can find a minimal subset $X_0$ of $X$ such that $U$ is the union of the sets $U(x)$ over all $x$ in $X_0$.

Let now $x$ be any fixed element of $X_0$. We construct a subset $R = R(x)$ of $P$ and a $R$-factorization of $MU(x)M$. Since this is slightly complicated by the possibility that $x$ can be a 3-periodic word (in the sense given to this expression in Section 2), we break it into several steps before proving that it has the desired properties.

**Construction.**

(1) If $x$ is not 3-periodic we consider it as a mapping in $A$ of its basic interval $(1, m)$ where $m$ is its length. In view of the Second Periodicity Lemma we can select an index $j$ in $(1, m)$ which is not covered three times (understood, by a word, or by the suffixes or by the prefixes of a word).

In the opposite case, $x = h^r h_1$ where $r \geqslant 3$, $h = \sqrt{x}$ is a primitive word of length $n$ equal to the step of $x$ and $h_1$ is a prefix of $h$. Consider first $w = h^2$ as a mapping of its basic interval $(1, 2n)$. The word $w$ is periodic but since $h$ is primitive it is not 3-preiodic. Thus, as above, we can choose an index $j'$ in $(1, 2n)$ which is not covered three times. Returning to $x$ and to its basic interval $(1, m)$, we let $j = j'$ or $= j' + n$ depending upon whether $j' \geqslant n$ or not. Thus, in both cases $n < j \leqslant 2n$.

(2) An interpretation $(q, b, p)$ of $x$ is *acceptable* iff $p$ is a prefix of at least one word in the subset $X'$ of the words of $X$ which are not strictly longer than $x$ and the symmetric conditions hold for $q$. When $x$ is 3-preiodic we impose the further restriction that $q$ is a suffix of at least one word from the subset $X''$ of the words $x''$ of $X'$ which have the form $x'' = p'q$ with $|p'| < n \; (= |h|)$ or $p' = p''h''$ where $h''$ is any word of length $n$ different from $h$.

(3) Let $y = (q, b, p)$ be an acceptable interpretation of $x$. It can be of three types depending upon the position of $j$ with respect of the supports of $p$ and of $q$. In each case we select a subset $P_y$ of $P$.

*Type X.* $|q| < j \leqslant |q \cdot b\alpha|$. There are factorizations $b = b'cb''$ and $c\alpha = p_y q_y = x_y$ such that $x_y$ is a word of $X$ and $j = |q \cdot b\alpha \cdot p_y|$. if $q_y \neq 1$ we let $p_y^X = \{p_y\}$; otherwise, $p_y = x_y$ and we let $p_y^X = \{1\}$.

*Type P.* $|q \cdot b\alpha| < j$. Then $P_y^p = \{p_y\}$ where this word is the left factor of $p$ such that $|q \cdot b\alpha \cdot p_y| = j$.

*Type Q.* $j < |q|$. Let $q = aq_y$ where $a$ has length $j$. Then $P_y^Q$ is the set of all prefixes $p'$ of the form $p' = p''a$ which are such that $p'q_y = x_y$ is a word of $X''$ or of $X'$ depending upon $x$ whether it is or not 3-periodic.

For $T = X$, $P$ or $Q$ we let $P^T$ denote the union of the sets $P_y^T$ over all the acceptable interpretations of $x$ and $R = R(x)$ be the union of the $P^T$'s.

(4) Let $x = zz'$ where $z$ has length $j$. We let $F' = F'(x)$ be the right ideal $z'A^L A^+$ where, we recall, $L$ is the maximum of the length of the words in $X$. If $x$ is not 3-periodic, $F = F(x) = A^+A^L z$. If it is, we replace in the definition of $F$ the set $A^L$ of all words of length $L$ by $A^L \setminus A^*h$, i.e. by the set of the words of the same length such that their suffix of length $n$ is not the word $h$ defined in (1) above.

This concludes the construction.

**4.4.** *The pair* $(F, F')$ *is a* $R$*-factorization of* $MU(x)M$.

**Proof.** Let $u$ be any idempotent in $U(x)$. There are arbitrary long words $g, g'$ such that $w = gxg'$ is in its inverse image. Thus we can take $z'g'$ in $F'$ and, when $x$ is not 3-periodic, $gz$ in $F$. In the opposite case let $W''$ be the set of all $g''$ such that $g''xg'$ is in the inverse image of $u$. It contains a suitable $g$ unless all its members have the form $g_1 h'^s$ with $s \geqslant 0$, $h' = \sqrt{x}$ and $|g_1| < |h| = |h'|$. However, in view of $u = u^2$, the set $W''$ contains $wW''$. Therefore such a possibility could arise cnly if there were a factorization $h' = h''h'''$ for which $xg'$ were in $h'h''$ and $W'$ a subset of $h'''h'^*$. This is excluded by the initial hypothesis that $u$ is not special. Thus we can always take $gz$ in $F$.

Let $y_1 = (q, b_1, p)$ be an interpretation of $gxg'$. Because of the hypothesis upon the lengths of the words in $X$ involved, one sees that there are interpretations $y = (q, b, p')$ of $gz$ and $y' = (q', b', p)$ of $z'g'$ such that $y_1 = yy'$, i.e. $b_1 = b \cdot [p', q'] \cdot b'$ and one checks readily that $p'$ is in $R$.

It follows that all the $P \setminus R$ columns of the matrix $(gz)u$ are identically zero, i.e. that $(gz)u = (gz)\mu \cdot e_R$.

The same holds for any matrix $m$ in $MuM$ since it has the form $m'um''$ for suitable $m', m''$. Q.E.D.

**4.5.** *The set $R$ has less than $6k^2$ elements.*

**Proof.** Consider first the case when $x$ is not 3-periodic.

Since the index $j$ is not covered three times by a word, each $x'$ in $X'$ can appear at most twice as the word $x_y$ in an interpretation $y$ of $z$ of type $X$. Each times it supplies one prefix to $P^X$ and, consequently, this set has at most $2k$ elements. In the same manner, since $j$ is not covered three times by the prefix of a word, each $x'$ can have at most two different prefixes which appear as the prefix term of an interpretation of type $P$. Thus, Card $(P^P) \leqslant 2k$.

If $q$ is the suffix term of an interpretation $y$ of type $Q$ the corresponding set $P_y^Q$ has at most $k$ elements since for any two of them, $p'$ and $p''$, the words $p'q$ and $p''q$ are different. Because $j$ is not covered three times by the suffixes, the number of interpretations of type $Q$ is $\leqslant 2k$.

Consequently, $6k^2$ is a generous bound for $R$.

Assume now that $x = h^r h_1$ is 3-periodic.

Since $j$ is not covered three times as a member of the interval $(1, 2n)$, we see as above that the total contribution to $R$ of the $k'$ words of $X$ of length less than $2n$ is inferior to $6k^2$. Consider now a word $x'$ of $X'$ of length $2n$ or more. There are three mutually exclusive possibilities:

– $x' = h'^s h'_1$ where $h'$ is conjugate with $h$, $h'_1$ is a prefix of $h'$ and $s \geqslant 2$;

– $x' = h'^s t$ with $h'$ as before, $s \geqslant 0$ and $t \neq 1$ not a prefix of $h'$;

– symmetrically, $x' = th'^s$ with $t \neq 1$ not a prefix of $h'$.

The last two cannot participate in interpretations of type $X$. In the first one, the fact that $h'$ is conjugate with $h = \sqrt{x}$ entails the existence of fixed words $a, a'$ such that any factorization of $x$ involving $x'$ has the form $x = h^{s'} ax'a'h^{s''} h_1$ $(s', s'' \geqslant 0)$. Because of $n < j \leqslant 2n$ we see that $x'$ can be a word $x_y$ in a type $X$ interpretation only if $s' = 0$ or $1$. Thus, the corresponding contribution to $P^X$ of these words $x'$ is at most twice their number $k'$.

A similar argument applies for the interpretations of type $P$ and, again, the only words involved belong to one of the first two categories. For the type $Q$, the word $x'$ must belong to the first or third category. Because of our restriction to acceptable interpretations, it can supply at most one suffix term. Thus its contribution to $P^Q$ is at most $k - k'$ by the same observation as in the initial non periodic case and we conclude that $R$ has less than $6k'^2 + 6(k - k')^2$ elements when $x$ is 3-periodic. Q.E.D.

**4.6.** *The number of conjugacy classes of maximal groups in $M$ (or in $S$) is absolutely finite.*

**Proof.** There is at most $k$ special classes and, for the other ones, the result follows from the last three Remarks 4.3, 4.4 and 4.5, since $MuM$ is the union of the $k'' \leqslant k$ ideals $MU(x)M$.

**4.7.** *For any two elements $m, m'$ of $MUM$ the bi-ideal $mMm'$ is absolutely finite.*

**Proof.** We have $m$ in $MU(x)M$ and $m'$ in $MU(x')M$ for words $x, x'$ of $X$. Therefore, by the preceding remarks, there are subsets $R$ and $R'$ of $P$ having less than $6k^2$ elements and matrices $m_i$ such that $m = m_1 e_R m_2$ and $m' = m_3 e_R m_4$. Each element of the bi-ideal has the form $mm''m'$, hence $m_1 m_5 m_4$ where $m_5 = e_R m_2 m'' m_3 e_R$, has all its non zero entries in $R \times R'$ and, accordingly, it belongs to an absolutely finite set. Q.E.D.

* * * * * * * * *

Let us thank A. Lentin, pioneer of this subject, whose friendly vigilance has preserved me from many mistakes.

REFERENCES


[1] Al.A. Markov, On finitely generated subsemigroups of a free semigroup, *Semigroup Forum*, 3 (1971), 251-258.

[2] Y.I. Khmelevski, *Equations in free semigroups,* Proc. Steklov Inst., 107 (1971) (in Russian).

[3] S.I. Adjan, *Definition relations and algorithmic problems for groups and semigroups,* Proc. Steklov Inst., 85 (1966) (in Russian).

[4] A. Spehner, Quelques problèmes d'extension de conjugaison et de présentation des sous-monoïdes d'un monoïde libre, Thèse Paris (1976).

[5] A. Lentin, *Equations dans les monoïdes libres,* Gauthier-Villars, Paris (1972).

[6] S. Eilenberg, *Automata languages and machines,* Vol. A, Academic Press, N.Y. (1975).

[7] R. Croisot, Equivalences principales bilatères définies dans un demigroupe, *J. Math. Pures Appl.,* (9) 36 (1957), 373-417.

[8] J-F. Perrot, Contribution à l'étude des monoïdes syntaxiques et de certains groupes associés aux automates finis, Thèse, Paris (1972).

[9] J-F. Perrot, Groupes de permutations associés aux codes préfixes finis, in *Permutations,* Gauthier-Villars, Paris (1972), 201-235.

[10] D. Perrin, La transitivité du groupe d'un code bipréfixe fini, *Math. Zeitschrift,* 153 (1977), 283-287.

[11] D.D. Miller – A.H. Clifford, Regular *D*-classes in semigroups, *Trans. Amer. Math. Soc.,* 82 (1956), 270-280.

[12] O. Steinfeld, Über die quasi-ideale von Halbgruppen, *Publ. Debrecen,* 4 (1956), 262-275.

[13] N.J. Fine – M.S. Wilf, Uniqueness theorem for periodic functions, *Proc. Amer. Math. Soc.,* 16 (1965), 109-114.

[14] J.D. McKnight – J.A. Storey, Equidivisible semigroups, *J. Algebra,* 12 (1969), 24-48.

[15] A. Lentin, Sur l'équation $a^m = b^n c^b d^q$ dans un monoïde libre, *C.R. Acad. Sci. Paris.,* 260 (1965), 3242-3244.

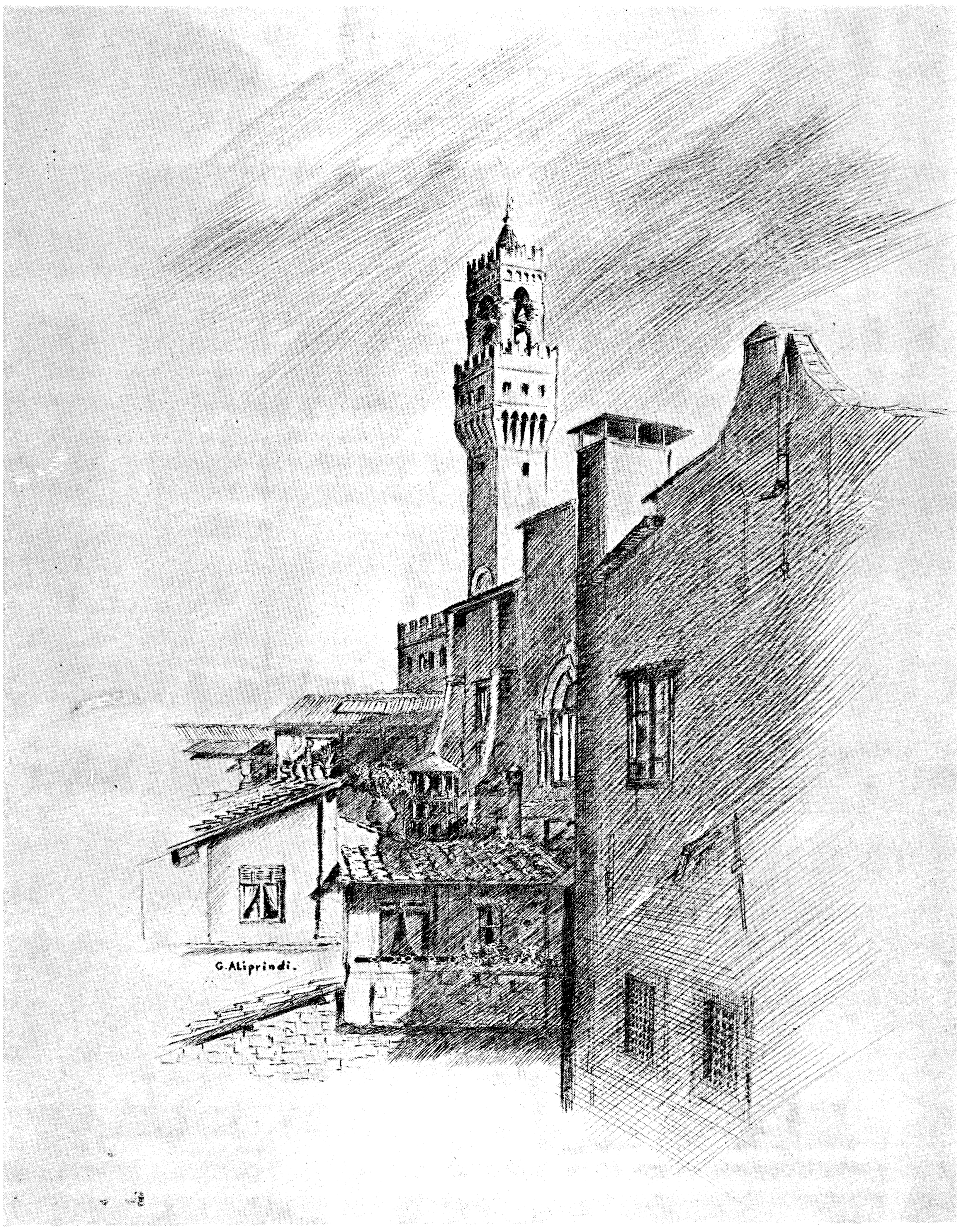
M.P. Schützenberger

Laboratoire d'Informatique Théorique et Programmation, LA 248, Université Paris VII, 2, Place Jussieu 75221 Paris Cedex 05, France.

CONSIGLIO NAZIONALE DELLE RICERCHE
ISTITUTO DI ANALISI GLOBALE

ATTI DEL CONVEGNO SU

# CODAGES et TRANSDUCTIONS




a cura di giuseppe pirillo

firenze, 15-17 ottobre 1979

*MARCO SCHÜTZENBERGER*

*Université de Paris 7*

*Laboratoire d'Informatique Théorique et Programmation du CNRS, Paris*

*SUR LES SOUS GROUPES DE RANG FINI D'UN GROUPE LIBRE*

*Résumé: On associe à chaque sous-groupe H de rang r d'un groupe libre F des sous-groupes de F, dits annexes de H, qui sont de groupes de permutations sur les classes latérales de F. On montre que le degré d'un groupe annexe (i.e. le nombre de points sur lequels il opère) est borné en fontion du rang r de H (par le nombre 3r-1) excepté quand le groupe annexe est cyclique (et le nombre de classes de conjugaison de groupes annexes cycliques est borné par r).*

*Abstract: We prove that certain permutation groups, associated with a subgroup of finite rank r of a free group, have rank one (i.e. are cyclic) when their degree exceds 3r-1.*

*Riassunto: Sia H un sottogruppo a r generatori di un gruppo libero. Noi proviamo che alcuni gruppi di permutazioni associati ad H sono ciclici quando il numero di punti sui quali essi operano supera 3r-1.*

# SUR LES SOUS GROUPES DE RANG FINI D'UN GROUPE LIBRE

Le résultat principal est la Proposition 1; il est la seule motivation des énoncés précédant sa preuve donnée dans la section 3, sauf les remarques de l'Introduction O qui n'ont d'autre prétention que d'éclairer la définition 1. La section 1 est surtout un exposé des notations nécéssaires pour passer du Théorème de Nielsen sous sa forme classique empruntée au traité [5] de Lyndon et Schupp aux monoïdes libres.

Celles-ci sont encore plus détaillées dans la section 3. La section 4 est un exercice de traduction de la méthode des transversales de Schreier en termes de représentations de semi-groupes finis et donne un algorithme de construction des classes de groupes annexes. Il aurait dû venir avant la section 2, si nous n'avions voulu manifester des prévenances pour un eventuel lecteur plus familier, o combien!, avec les groupes libres qu'avec les concepts et les techniques exposées dans les ouvrages de S. Eilenberg [3] ou de G. Lallement [4].

Ce travail a été écrit au Centre d'Analyse Globale à Florence dont le Directeur, le Professeur Gherardelli nous a fait l'honneur de nous inviter sous les auspices du C.N.R. Que lui même et le Professeur Pucci veuillent accepter cet essai en hommage d'amicale reconnaissance.

## 0. Introduction

Dans tout ce qui suit $F$ est un groupe libre et $H$ un sous groupe de rang ( = nombre de générateurs) fini $r$ de $F$. On s'intéresse à l'action de $F$ et de certains de ses sous groupes $G$ sur les classes latérales $Hf$ ($f \in F$). Un sous ensemble de ces dernières sera désigné par une notation telle que $HF_1$ en convenant que $F_1 \subset F$ est une transversale c'est-à-dire que $Hf \neq Hf'$ pour deux quelconques de ses éléments $f$ et $f' \neq f$.

Définition 1. Un sous groupe $G$ de $F$ est un groupe annexe (de la paire $(H,F)$) ssi il est le stabilisateur, $G = \{f \in F : HF_1 f = HF_1\}$ d'une union finie $HF_1$ de classes latérales telles que $HfG$ contienne une infinité de classes pour chaque $f \notin HF_1$. Son degré est le nombre des classes latérales dans $HF_1$ ; son degré d'intransitivité est le nombre maximum d'éléments dans une tranversale $F'_1 \subset F_1$ telle que $f'' \notin Hf'G$ pour toute paire d'éléments $f'$ et $f'' \neq f'$ de $F'_1$.

Par conséquent $F$ lui-même est le seul groupe annexe quand il n'y a qu'un nombre fini de classes latérales et pourvu que le rang $r$ de $H$ soit $\geqslant 2$, son degré est fourni par la formule de Schreier ([5]), $d = (r-1)/(r'-1)$ où $r'$ reste le rang de $F$. Quand $H$ est engendré par un seul élément $h$, tous les groupes annexes sont conjugués du groupe $G$, engendré par l'élément $g = \sqrt{h}$ tel que $h = g^p$ $(p \geqslant 1)$ avec $p$ maximum et le degré de $G$ est $p$.

Dans le cas général, le théorème de Nielsen [5] montre facilement (section 1) que le degré des groupes annexes est au plus égal au double de la somme $k$ des longueurs des mots d'une base de $H$ et que le nombre de leurs classes (sous entendu, de conjugaison) n'excéde pas $4^k$

3

Proposition 1. Tous les groupes annexes ont un degré d'intransitivité $\leqslant 3r-1$ et le nombre de leurs classes est inférieur à $1/2\ (3^{3r-1}-1)$; ceux dont le degré est $\geqslant 3r-1$ sont de rang un et le nombre de leurs classes est $\leqslant 3r-2$.

Pour discuter commodément ces notions, on dira que deux transversales $F_1$ et $F_1'$ sont équivalentes ssi $HF_1 = HF_1'$ et que $F_1$ est une transversale du groupe annexe $G$ ssi c'est une transversale finie maximale dont $G$ est le stabilisateur. Toutes les transversales de $G$ sont donc équivalentes et les transversales des groupes $f^{-1}\ G\ f$ $(f \in F)$ de la classe de $G$ sont leurs translatés $F_1\ f$.

Comme d'usage, 1 est l'élément neutre de tout monoïde et on pose $\sqrt{H} = \{\sqrt{h} : h \in H\}$ où, comme ci-dessus, $\sqrt{h}$ désigne le générateur du plus grand semi-groupe de rang un contenant $h$.

0.1 Si $\sqrt{H} \subset H$ chaque groupe annexe $G$ est le fixateur $(HfG = Hf)$ des éléments de ses transversales. Réciproquement $H$ est contenu dans l'union des groupes annexes; tout élément de ces derniers est conjugué d'une puissance d'un élément de $\sqrt{H}$ et si $p$ est le plus petit entier tel que pour un $g^p \in H$, tout groupe annexe contenant $g$ a un degré $\geqslant p$.

Preuve. Supposons au contraire qu'un groupe annexe $G$ contienne un $g$ tel que $H\ f\ g \neq H\ f$ pour un élément $f$ d'une transversale $F_1$ de $G$. Quitte à remplacer $F_1$ par $F_1 f^{-1}$ et $G$ et $g$ par leurs conjugués $f\ G\ f^{-1}$ et $f\ g\ f^{-1}$ on peut supposer $f = 1$. Donc $Hg \neq H$, c'est-à-dire $g \notin H$.

Comme $d = \mathrm{Card}\ (F_1)$ est fini, par hypothèse chaque $d!$-ième puissance d'un élément de $G$ est dans le fixateur de $F_1$, donc en particulier dans $H$ qui est le fixateur de $1$. Par conséquent $g$ a une plus petite puissance $p \geqslant 2$ telle que $g^p = h \in H$ et,comme il est lui-même la q-ième puissance $(q \geqslant 1)$ de $x = \sqrt{h} = \sqrt{g}$, on en conclut que $H$ ne contient pas $\sqrt{H}$. De plus $\{1, g, \ldots, g^{p-1}\}$ forme une transversale équivalente à une partie de $F_1$ et par conséquent $d \geqslant p$.

Considérons maintenant $x = \sqrt{h} = \sqrt{g}$ et le sous groupe $X$ qu'il engendre. Pour chaque $f \in F_1$, $H f X$ est l'union d'au plus $q$ classes latérales. Donc $X$ est dans le stabilisateur de l'union <u>finie</u> $HF_1X$ de classes latérales. Anticipant sur la section suivante, nous faisons appel au Théorème de Nielsen qui donne une borne supérieur $k < \infty$ , ne dépendant que de $H$, à toute transversale <u>finie</u> qui est stabilisée par un sous groupe $(\neq \{1\})$ de $F$. Ce fait implique que $F_1X$ soit contenu (mod $H$) dans une plus petite transversale $F_2$, stabilisée par $X$ et telle que $H f X$ contienne une infinité de classes latérales quand $f \notin H F_2$ . Son stabilisateur $G'$ est un groupe annexe contenant $X$, donc $g$, donc $h$ (mais non nécessairement $G$) ,ce qui achève d'établir la remarque.

Q.E.D.

0.2 Si $H \cap f^{-1} H f = \{1\}$ pour chaque $f \notin H$, tous les groupes annexes sont conjugués de $H$ et ont degré $1$. Réciproquement, chaque sous groupe $\neq \{1\}$ de la forme $H \cap f^{-1} H f$ $(f \notin H)$ est contenu dans un groupe annexe $\neq H$.

<u>Preuve</u>. Soit $F_1$ une trasversale d'un groupe annexe $G$; le degré local de $G$ en $f \in F_1$ est le nombre des classes latérales dans $H f G$ et on peut supposer $G$ choisi parmi ses conjugués de telle sorte que le degré local soit maximal pour $f = 1$. Supposons que $H$ ait une intersection

triviale avec tous ces conjugués. Ceci implique que $\sqrt{H} \subset H$, puisque $\sqrt{h}$ commute avec h. Donc le degré local de G en 1 est un, ce qui signifie que G est un sous groupe de H. Par construction le degré local est aussi 1 en tout autre $f \in F_1 \setminus \{1\}$, s'il en existe. Supposons-le. On a $Hfg = Hf$, c'est-à-dire $fgf^{-1} \in H$ où $g \in G \subset H$ en contradiction avec l'hypothèse initiale. Donc le degré de G est 1, c'est-à-dire que $G = H$.

Réciproquement tout $h \neq 1$ contenu dans l'intersection H' de H avec $f^{-1} H f$ satisfait $f h = h' f$ pour un $h' \in H$, donc $Hfh = Hf$. Supposant $f \notin H$, le même argument que dans 0.1 montre que l'ensemble des $f' \in F$ tels que H' soit de degré local fini en Hf' est contenu dans une union $HF_1$ d'au plus k classes latérales dont le stabilisateur est un groupe annexe contenant H'.

0.3 Le nombre des classes de H-conjugaison qui peuvent être contenues dans une classe de conjugaison de F est au plus égal au maximum des degrés des groupes annexes de rang $\geqslant 2$ et des degrés d'intransitivité des groupes annexes de rang 1.

<u>Preuve</u>. Soient $h = h_1 \in H_1$, $f_1 = 1$ et $\{h_i = f_i\ h\ f_1^{-1} : 1 \leqslant i \leqslant d\}$ un système maximal d'éléments $h_i$ de H qui ne sont pas H-conjugués c'est-à-dire qui sont tels que $h_i = h'\ h_j\ h^{i-1}$ pour un $h' \in H$ seulement si $i = j$.

Comme précédement on voit que $\{f_i : 1 \leqslant i \leqslant d\}$ est une partie d'une transversale $F_1$ dont le stabilisateur G est un groupe annexe de degré $\geqslant d$ qui contient h. Supposons que G soit le groupe de rang 1 engendré par un élément g de F. On a $g = \sqrt{h}$ et l'hypothèse que les $h_i$ ne sont pas H conjugués implique qu'aucun $f_j$ ne soit tel que

6

$Hf_j = Hf_i\, g^m$ pour un $m \geqslant 1$ et $f_i \neq f_j$ car sinon on aurait $h_j = f_j\, h\, f_j^{-1} = f_i\, g^m\, h\, g^{-m}\, f_i^{-1} = h_i$.

Donc $d$ est borné à la fois par le degré des groupes annexes et par le degré d'intransitivité de ceux qui sont de rang un.

Q.E.D.

Le groupe de permutation fini $[G]$ quotient du groupe annexe $G$ par restriction à une de ses transversales de son action sur les classes latérales peut être arbitrairement compliqué: il suffit de prendre pour $H$ le groupe engendré par une partie de la base d'un sous groupe d'index fini, ainsi que me l'a fait observer D. Perrin dont les avis et les suggestions sont à l'origine de ces recherches.

Les valeurs numériques indiquées dans la Proposition sont manifestement ridicules. Non pas parce que divers calcus subsidiaires permettant de les réduire de quelques unités ont été omis, mais parceque je n'ai pas trouvé le moyen d'utiliser les structure de $E$ et du morphisme $\beta: B^* \longrightarrow A^*$ de la section 2, ni, vraisemblablement,de voir des propriétés moins superficielles des groupes annexes que celles présentées dans l'Introduction. Certains lecteurs informaticiens auront d'ailleurs reconnu dans la section 3 l'application brutale d'une technique pour borner les groupes dans le monoïde syntaxique d'une partie rationnelle $K = V^*\varphi \subset A$ en fonction du rang d'une partie locale $E$ dont $K$ est l'image. Les seules propriétés spécifiques de $E$ qui soient mises en oeuvre sont celles qui découlent de l'existence d'inversions formelles c'est-à-dire de mots réduits; elles diminuent le rang par un facteur deux. Le théorème de Cesari et Duval donnant des bornes optimales du point de vue des techniques employées,d'autres idées seraient donc nécessaires. En effet on a toute raison de penser qu'il existe $r$ éléments de

$\Gamma$ tels que, d'une part, chaque groupe annexe de degré $\geqslant r+1$ (ou peut-être $\geqslant r$) est conjugué du sous groupe engendré par l'un d'eux et que, d'autre part, une base de H est constituée d'un système de leurs puissances. Je n'ai pas pu dépasser le cas de $r = 2$ qui de toutes façons, comme on le sait, présente pour ce type de problèmes des particularités qui ne se rencontrent pas pour les rangs plus élevés.

## 1. Première application du théorème de Nielsen

Une $\pm$ base d'un groupe est l'union d'une base (= ensemble générateur minimal) et des inverses de ses éléments. On suppose qu'une $\pm$ base A de F a été choisie une fois pour toute ce qui fait qu'il existe un morphisme surjectif $\alpha$ sur F du monoïde libre $A^*$ engendré par A. On note $A^+$ le semigroupe libre $A^+ = A^* \backslash \{1\}$ engendré par A. Pour chaque lettre a de A on écrit indifférement $a^{-1}$ ou $\bar{a}$ et l'inverse formel d'un mot $w = a_1 a_2 \ldots a_n$ $(n \geqslant 0,\ a_i \in A)$ est $\bar{w} = \bar{a}_n \ldots \bar{a}_2 \bar{a}_1$ donc $\bar{\bar{w}} = w$ et $\bar{w}\alpha = (w\alpha)^{-1}$. Si X est une partie de $A^*$, on écrit $\bar{X} = \{\bar{x} : x \in X\}$ et on dit que X est symétrique ssi $X = \bar{X}$.

L'ensemble des mots réduits est $L^1 = \{1\} \cup L$ où

$L = A^+ \backslash \{A^* a \bar{a} A^* : a \in A\}$.

On sait que c'est une section de F en ce sens qu'il existe une bisection $\varphi$ de F sur $L^1$ telle que $w = w\alpha\varphi$ ssi $w \in L^1$. L'expérience montre qu'il n'y a pas d'inconvénient à écrire w au lieu de $w\alpha$ pour désigner un élément de F, donc à définir $w\varphi$ pour chaque mot w comme l'unique mot réduit représentant l'élément w de F. Ce mot réduit est obtenu en effaçant dans w tous les facteurs de la forme $a\bar{a}$ et en continuant l'opération tant que le mot résultant n'est pas réduit; le mot final w ne dépend pas de la manière dont les effacements (= cancellations) sont effectués, comme le savent tous les lecteurs du beau livre de J. Berstel sur les langages algèbriques.

Pour préciser les calculs on désigne par $w \wedge w'$ le plus long facteur gauche commun de deux mots $w, w'$; leur plus long facteur droit commun est donc l'inverse formel de $\bar{w} \wedge \bar{w}'$.

Soient $w, w' \in L$, $u = \bar{w} \wedge \bar{w}'$ $w = v\bar{u}$, $w' = u\, v'$ $(v, v' \in A)$. On a $w\, w' = v\, v' \in L^1$ ce qui est la réalisation dans $A^*$ du produit dans F. Considérons le cas particulier de $w' = w$. On montre facilement que l'hypothèse $w \in L$ implique $2|u|<|w|$, c.-à-d. que $w = u\, v''\, \bar{u}$ où $v'' \in A^+$ ; le mot $v''$ est le <u>facteur circulaire</u> de $w$ et $(w^p)\varphi = u(v'')^p\, \bar{u}$ : $(p \leqslant 1)$.

Le mot réduit $w = a_1 \ldots a_n$ $(n \geqslant 1,\ a_i \in A)$ est <u>circulairement réduit</u> ssi $w = v''$, c'est-à-dire, de façon équivalente, ssi il est réduit et $\bar{a}_1 \neq a_n$ ou si son carré $w^2$ est réduit. On rappelle que les <u>conjugués</u> dans le monoïde libre $A^*$ de $w$ sont les mots $a_i \ldots a_n\, a_1 \ldots a_{i-1}$.

Un calcul bien connu montre que la classe de conjugaison $\{f\, w\, f^{-1} : f \in F\}$ de $w$ dans le groupe F est formée des mots dont le facteur circulaire est conjugué dans $A^*$ de celui de $w$.

Soient maintenant H le sous groupe donné de F et $V = \{v_i\ ,\ \bar{v}_i : 1 \leqslant i \leqslant r\} \subset L$ une $\pm$ base de H; il sera commode de désigner $\bar{v}_i$ par $v_{-i}$ $(1 \leqslant i \leqslant r)$. H est représenté par l'ensemble de mots réduits $V^*\varphi$ (V = le sous monoïde engendré par V). Comme H est (isomorphe à) un groupe libre, chacun de ses éléments est égal de façon unique à un produit $v_{i_1} \ldots v_{i_n}$ $(v_{i_j} \in V)$ qui est V-<u>réduit</u> en ce sens que $V_{-i_j} \neq V_{i_{j+1}}$ $(1 \leqslant j \leqslant n-1)$.

Le théorème suivant est la base du reste du travail. Il est prouvé dans [5] p. 7 . L'enoncé est alourdi par les précisions de notations nécessaires pour la suite.

<u>Théorème de Nielsen</u>. Le groupe H a un $\pm$ base $V \subset L$ telle que chaque $v_i \in V$ ait une factorisation distinguée $v_i = y_i\, x_i\, \bar{y}_{-i}$ ayant les trois propriétés suivantes:

(1) $x_i \in A^+$ et $y_{-i}\, \bar{x}_i\, \bar{y}_i$ est la factorisation distinguée de $v_{-i} = \bar{v}_i$;

(2) $y_i$ est le plus long facteur de $v_i$ de la forme $v_i \wedge v_j$ $(v_j \in V \setminus v_i)$;

(3) $|y_i| \leqslant |x_i\, \bar{y}_{-i}|$ ;

Par conséquent si $-i \neq k$ on a $(v_i\, v_k)\varphi = y_i\, x_i\, \bar{y}'_{-i}\, y'_k\, x_k\, y''_k$ où $y'_{-1}$ (resp. $y'_h$) est un facteur gauche de $\bar{y}_{-i}$ (resp. droit de $y_h$ ). Plus généralement, soit $h \in H \setminus 1$; il est de façon unique un produit V-réduit $v_1 \ldots v_n$ $(v_i \in V)$ et le mot réduit $h\varphi$ qui le représente a une factorisation $v''_1\, v'_2 \ldots v''_n$ dont nous soulignons les propriétés:

$v''_1$ (resp. $v''_n$ ) est un facteur gauche (resp. droit) du $v \in V$ de même indice;

chaque $v'_i$ est un facteur du $v_i \in V$ correspondant admettant lui-même comme facteur la partie ineffaçable $x_i$ .

Nous appellerons cette factorisation la <u>factorisation de Nielsen</u> de h et n sera la <u>V-longueur</u> de h. On notera que la factorisation de Nielsen de $v_2 \ldots v_n$ est $v''_2 \ldots v''_n$ où $v''_2$ admet $v'_2$ comme facteur droit et que si h est <u>circulairement</u> V-<u>réduit</u> en ce sens que $\bar{v}_1 \neq v_n$ , le facteur circulaire de $h\varphi$ est $v'_1 \ldots v'_n$ avec $v'_1$ , $v'_n$ comme ci-dessus.

La base de Nielsen V sera désormais supposée être choisie et on notera P l'ensemble des mots $\neq 1$ qui sont des facteurs gauches de ses éléments. Donc $V \subset P \subset L$ .

Remarque 1.1 Soient $u \neq 1$ circulairement réduit et $f$ tels que $H\,f\,u = H\,f$. Il y a un $p \in P$ tel que $H\,f = H\,p = H\,p\,u$ avec $pu \in L$.

Preuve L'équation $H\,f\,u = H\,f$ signifie que $(f\,u\,\bar{f})\varphi = h \in H$. Si l'on remplace $f$ par $(f\,u^n)\varphi$ pour $n$ assez grand on obtient un mot $f'$ de la même classe latérale que $f$ qui satisfait $f'$, $f'u \in L$. On peut donc supposer que $f$ lui-même a été choisi dans sa classe latérale de façon à satisfaire cette condition et à minimiser la longueur de $(f\,u\,\bar{f})\varphi$. Ceci entraine que le plus long facteur droit commun $u'$ de $f$ et de $u$ soit de longueur $|u'| < |u|$. Il existe donc $y \in A^*$ et $u'' \neq 1$ tels que $f = y\,u'$ ; $u = u''u'$ et enfin $(f\,u\,\bar{f})\varphi = y\,u'u''\bar{y}$.

Soit $v''_1 \ldots v''_n$ la factorisation de Nielsen de ce mot. Il existe un indice $j$, un mot $t \neq 1$ et un mot $t'$ tels que $f = v''_1 \ldots v'_{j-1}\,t$ , $v'_j = t\,t'$.

Soient $h' = (v_1 \ldots v_{j-1})\varphi \in H$ et $v''_j \ldots v''_n$ la factorisation de Nielsen de $(\bar{h}'\,h)\varphi = (v_j \ldots v_n)\varphi \in H$.

On a vu que $v'_j$ est un facteur droit de $v''_j$ et que ce dernier mot est un facteur gauche de $v_j \in V$. Il y a donc un $p' \in A^*$ tel que $v''_j = p'\,v'_j = p'\,t\,t'$ , ce qui fait que $p = p'\,t$ est un facteur gauche d'un mot $v_j$ de $V$ et qu'il appartient à $P$ puisque $|p| \geqslant |y| \geqslant |0|$ par construction. D'après le choix de l'indice $j$ on a $(\bar{h}'\,f)\,\varphi = p'\,y = p$, ce qui montre que $H\,p = H\,f$ et la relation $p\,u \in L$ découle de ce que $y\,u'' \in L$ où $u'' \neq 1$ est un facteur gauche de $u$.

Q.E.D.

Remarque 1.2 Soient $G \neq \{1\}$ un sous groupe de $F$ et $F_1$ une transversale telle que $H\,f\,G$ soit une union finie de classes pour chaque $f \in F_1$. On a Card $(F_1) \leqslant$ Card $(P)$ et le stabilisateur de $H\,F_1$ est un groupe annexe

11

contenant $G$ .

<u>Preuve</u> On prend un élément arbitraire $x u \bar{x}$ ( $x \in A^*$, $u$ circulairement réduit) dans $G \setminus 1$. Quitte à remplacer $G$ par $x^{-1} G x$ et $F_1$ par $F_1 x$ on peut supposer $x = 1$.

Pour chaque $f \in F_1$ il existe un plus petit $p$ positif fini tel que $H f u^p = H f$. La même relation vaut pour chaque $f u^j$ $(0 \leqslant j \leqslant p - 1)$. D'après la remarque précédente cet ensemble d'éléments forme une transversale équivalente à une partie $P_{1i}$ de $P$, et la conclusion en découle puisque $P$ est fini.

Q.E.D.

On rappelle qu'un mot $s$ est dit <u>primitif</u> ssi $s = \sqrt{s}$ et que $s^+$ désigne le semigroupe engendré par $s$.

<u>Lemme 1.3</u> Il existe un ensemble $S$ de mots primitifs circulairement réduits en bijection avec les classes $C$ de groupes annexes, et pour chaque classe $C$ un groupe $G \in C$ contenant $s = s\,(C) \in S$, et une transversale $P_s \subset P$ de $G$ tels que $P_s\, s^+ \subset L$ et qu'en outre :

(i) Si $G$ n'est pas de rang un, la longueur de $s$ excède celle des mots de $V$;

(ii) Si $C' \neq C$ est une autre classe, $s\,(C')$ n'est conjugué d'aucune puissance de $s$ ni de $\bar{s}$ .

<u>Preuve</u> Soit $q = (\text{Card } P)\,!$ On peut choisir $G \in C$ contenant au moins un mot circulairement réduit $u \neq 1$. Comme l'ensemble des $f \in F$ pour lesquels $H f u^+$ est une union finie de classes est le même que pour $\sqrt{u}$, on peut supposer $u = \sqrt{u}$, donc $u$ primitif. Appliquant la construction de la remarque 1.1 à $u^q$ , on obtient une transversale $P_1 \subset P$ de $G$ avec $P_1 u \in L$

12

et on peut trouver pour chaque $p \in P_1$ un $p''$ satisfaisant la condition indiquée pour $s$.

Nous montrons maintenant que l'on peut choisir $u$ au départ de façon à satisfaire (i) et (ii).

Si $G$ a rang $\geqslant 2$ il existe un $g \in G$ qui n'est pas une puissance de $s$. La même chose vaut pour les mots $(u^n g u^n)\varphi = g'$ et il suffit de vérifier que pour tout $n$ assez grand $u^n g'^n$ est un mot primitif circulairement réduit aussi long qu'on le veut.

En raison des rapports entre la conjugaison des groupes et la translation des transversales et du fait que chaque groupe annexe est défini comme le stabilisateur de sa transversale, il suffit pour établir (ii), de montrer que l'on peut choisir $u$ de telle sorte que $H f u^q \neq H f$ pour tout $f \in H P_1$. Supposons que cela ne soit pas le cas pour $p \notin H P_1$. Il existe un $y \in G$ tel que $H p g^m \cap H P_1 \neq \emptyset$ pour tout $m$ assez grand; on peut trouver un $n$ tel que $(u^{nq} g^m u^{nq})$ soit circulairement réduit quelque soit $m$. Remplaçant $u$ par ce nouvel élément, diminue d'au moins une unité le nombre des classes $Hp$ $(p \in P_1)$.

## 2. Un corollaire du théorème de Nielsen

On se propose de construire un nouvel alphabet $B = B_1 \cup B_2 \cup \bar{B}_2$ et un morphisme $\beta : B^* \longrightarrow A^*$ de façon à satisfaire les conditions énoncées dans le Lemme 2.1 ci-dessous.

Comme la Proposition 1 ne dépend pas du choix du groupe $H$ dans sa classe de conjugaison, on fera désormais l'hypothèse que $H$ est réduit en ce sens que 1 est le plus long facteur gauche commun des mots de la base de Nielsen V. On peut toujours se ramener à ce cas. En effet, soit

13

$f = \wedge\{v : v \varepsilon V\}$. Comme $V$ est symétrique $(V = \overline{V} = \{\overline{v} : v \varepsilon V\})$ chaque $v_i \varepsilon V$ a la forme $f\, v_1'\, \overline{f}$ et d'après la définition même, de sa factorisation distinguée, $y_i\, x_i\, \overline{y}_{-i}$, $f$ (resp. $\overline{f}$) est un facteur gauche (resp. droit) de $y_i$ (resp. $\overline{y}_{-i}$). Donc $V' = (\overline{f}\; V\; f)\varphi$ est une base de Nielsen du sous groupe conjugué $f^{-1}\, H\, f$ et $1$ est le seul facteur gauche commun de ses mots.

Pour obtenir $B$, on commence par définir la famille $T$ des parties $V' \neq \emptyset$ de $V$ telles que le mot $w(V') = \wedge\{v' \varepsilon V'\}$ soit $\neq 1$ et ne soit facteur gauche d'aucun mot de $V \setminus V'$; le sous ensemble $T_1$ des éléments minimaux de $T$ est donc constitué par les $2r$ singolets $\{v_i\}$ $(v_i \varepsilon V)$.

Pour chaque $V' \varepsilon T$ le mot $y' = w\,(V')$ a un plus long facteur gauche $y'' \neq y'$ qui est $1$ ou de la forme $y'' = w\,(V'')$ avec $V'' \varepsilon T$ ; dans le premier cas on pose $V'\vartheta = V$; dans le second $V'\vartheta = V''$.

Si $V'$ n'est pas un singolet on lui attache une lettre de $B$ que l'on note $b\,(V'\vartheta, V')$ et dont l'image par $B$ est le mot $z$ tel que $y''z = y'$; l'inverse formel de cette lettre sera la lettre $b\,(\overline{V}', \overline{V'\vartheta})$ d'image $\overline{z}$ par $B$. L'ensemble de ces lettres forme le sous alphabet $B_2 \cup \overline{B}_2$ de $B$; on a $B_2 \cap \overline{B}_2 = \emptyset$ puisque l'indice gauche $V'\vartheta$ contient strictement l'indice droit $V'$ pour les lettres de $B_2$ alors que c'est le contraire qui se produit pour l'ensemble $\overline{B}_2$ de leurs inverses formels.

Dans le cas opposé où $V'$ est un singolet $\{v_i\}$ on définit une lettre $b \varepsilon B_1$ dont l'indice gauche est $\{v_i\}\vartheta$, l'indice droit $\overline{\{v_{-i}\}\vartheta}$ et qui a un indice intermédiaire $v_i$. Son inverse formel est la lettre du même sous alphabet $B_1$ qui est définie par le singolet $\{v_{-i}\}$ et son image par $\beta$ est le facteur ineffaçable $x_i$ de $v_i$. Par conséquent $B = B_1 \cup B_2 \cup \overline{B}_2$ est muni d'une inversion formelle et le morphisme

$\beta: B^* \to A^*$ qui prolonge $\beta$ commute avec celle-ci. Le lecteur pourra noter que la construction est invariante pour l'échange de la gauche et de la droite. En effet, en raison de $V = \bar{V}$ et de la symétrie des factorisations distinguées $y_i\ x_i\ \bar{y}_{-i}$ des mots de Nielsen, cet échange remplacerait l'opération $\wedge$ par l'opération correspondante sur les facteurs communs droits.

On désignera par les mêmes symboles $\alpha$ et $\varphi$ que pour $A^*$ le morphisme naturel $(\bar{b}\alpha = (b\alpha)^{-1})$ envoyant $B^*$ sur le groupe libre de $\pm$ base B et l'opération de réduction envoyant chaque mot sur l'unique mot réduit qui représente le même élément de $B^*\alpha$.

Nous construisons maintenant un ensemble $W \subset B^+$ qui constitue une base de Nielsen d'un sous groupe $H'$ de $B^*\alpha$ de rang 2 tel que B envoie $W^*\varphi$ sur $V^*\varphi$.

Reprenant la construction de B, on voit que W est l'ensemble des mots w de $B^+$ qui satisfont les cinq conditions suivantes dont les quatre premières portent sur tous leurs facteurs de la forme b ou bb' $(b, b' \in B)$ :

(1) w est réduit, c'est-à-dire $b' \neq \bar{b}$ ;

(2) Si $b \in B_2$ alors $b' \notin \bar{B}_2$ ;

(3) L'indice droit de b est égal à l'indice gauche de b';

(4) L'indice gauche de la première lettre est V et il en est de même de l'indice droit de la dernière;

(5) w a exactement une occurence d'une lettre de $B_1$ ;

Il suffit d'examiner le réduction de $w\,w' \to (w\,w')\varphi$ $(w, w' \in W)$ pour constater que $W^+\varphi$ est formé des mots qui satisfont les quatre premières conditions.

Puisque les groupes H et H' sont isomorphes (en tant que groupes libres de même rang) la restriction de $\beta$ à $W^*\varphi$ est une bijection sur $V^*\varphi$.

De plus en raison du théorème de Nielsen l'image de $B^*$ par $\beta$ dans $A^*$ (qui peut d'ailleurs se trouver être égale à $A^*$) est par construction le plus petit sous monoïde de $A^*$ qui contienne le plus long facteur gauche commun de deux mots de $V^*\varphi = H$ ce qui a pour conséquence que cette image ne dépend que de H et non de la base de Nielsen V qui a été choisie.

Pour disposer plus tard de toutes les notations, nous supposons donné un ordre total $\leqslant$ sur B tel que chaque lettre b soit contiguë de son inverse formel et que l'on ait $b' < b$ toutes les fois que $b'\beta < b\beta$.
A chaque lettre b on associe l'ensemble $S(b)$ des mots $s \in S$ pour lesquels b (c'est-à-dire $b\alpha$) est un facteur de $s^+$ (c'est-à-dire d'un mot de $s^+$) et pour lesquels ceci n'est vrai d'aucun $b' > b, \bar{b}$. Si l'on avait un $s \in S(b) \setminus S(\bar{b})$ et un $s' \in S(\bar{b}) \setminus S(b)$ on pourrait remplacer s' par $\bar{s}$ dans la construction du Lemme 1.3. On peut donc supposer donnée une moitié $B_+$ de B (c'est-à-dire B = l'union disjointe de $B_+$ et $\bar{B}_+$ ) telle que les blocs $S(b)$ $(b \in B_+)$ constituent une partition de l'ensemble S de tous les mots s du lemme 1.3

Corollaire du Théorème de Nielsen 2.1 Il existe un monoïde libre $(B_+ \cup \bar{B}_+)^*$ un morphisme $\beta : B^* \longrightarrow A^*$ commutant avec l'inversion formelle et une partie E de $B^*$ contenant les facteurs gauches de ses mots tels que pour tout $s = s\ (C)$ on ait :

(i) $\mathrm{Card}\ (B_+) \leqslant 3r - 2$ ;

(ii) $P_s\, s^+$ est contenu dans l'ensemble des facteurs gauches des mots de $E\beta$ ;

(iii) Si $f' \neq 1$ est un facteur gauche de s, $m \geqslant 0$, et $p_1 \neq p_2$ deux éléments de $P_s$, il n'existe pas de lettre $b \in B$ telle que

16

$p_1 s^m f'$ et $p_2 s^m f'$ soient contenus dans $(E \cap B^* b)$

Preuve (i). Le sous alphabet $B_1 = \bar{B}_1$ a 2r lettres, et les lettres de $B_2$ sont en bisection avec les membres de $T$ qui ne sont pas des singolets. Comme $T \cup \{V\}$ est engendré à partir de ces derniers par itération de l'application strictement croissante $\vartheta$, le nombre des membres de $T \cup \{V\}$ est au plus égal au nombre des singolets moins un.

Donc $\text{Card}\ (B_2) \leqslant 2r - 2$ et

$\text{Card}\ (B) \leqslant 2r + 2\ (2r - 2) = 2\ (3r - 2)$ ;

(ii) est la conséquence immédiate de ce que les mots de $P_s s^+$ sont des facteurs gauches de ceux de $V^*\varphi$ et de ce que $V^*\varphi \subset W^*\varphi \subset E$

(iii) Le caractère local des conditions définissant $W^*\varphi$ implique que si $w \in E$ l'ensemble des $w'' \in B^*$ tels que $w\, w'' \in W^*\varphi$ ne dépend que de la dernière lettre de $w$. Par conséquent chaque $(E \cap B\ b)\beta$ est contenu dans une classe latérale de $H$ ne dépendant que de $b$ $(b \in B)$ et le résultat en découle puisque $P_s$ est une transversale, c'est-à-dire puisque par hypothèse $p_1$ et $p_2$ appartiennent à des classes latérales distinctes.

Q.E.D.

Question. Existe-t'il des propriétés de la paire de groupes $(H, F)$ que l'on puisse attacher à la structure $(T, \vartheta)$ ?

3. Preuve de la Proposition

On aura besoin de distinguer les diverses occurrences d'un même mot comme facteur d'un mot donné $w = a_1 \ldots a_n$ $(a_i \in A)$ de longueur positive n. Pour cela on considérera $w$ comme une application dans $A$ de l'intervalle de base $[1, n]$, et on dira qu'un sous intervalle $I = [i, j]$ est

17

un support du mot $f$ ssi $f = a_i \ldots a_j$ que l'on notera $f = I\, w$. Ceci justifie que l'on dise que $I$ (ou le mot $Iw$) a la périodicité $p$ ssi $1 \leqslant p \leqslant j + 1 - i$ et $a_k = a_{k+p}$ pour $i \leqslant k \leqslant k + p \leqslant j$; $p$ sera une période (de $I$ ou de $Iw$) ssi de plus $I$ n'a pas une périodicité $p'$ où $p' \neq p$ est un diviseur de $p$.

Il est clair qu'un mot $f$ a une période egale à sa longueur ssi il est primitif $(f = \sqrt{}f)$. On dit qu'il est périodique ssi il a une période $p$ telle que $2\,p \leqslant |f|$ et on sait qu'il a au plus une telle période. Une racine de $f$ est un facteur gauche de longueur égale à une période. Donc les conjugués des racines de $f$ sont tous les mots primitifs $g$ tels que $|g| \leqslant |f|$ et que $f$ soient un facteur d'une de leurs puissances.

L'énoncé qui suit (connu de tous, sous une forme ou une autre) résume les propriétés élémentaires de ces notions.

Lemme de conjugaison. Les propriétés suivantes d'un mot $w$ de longueur positive $n$ sont équivalentes;

(1) $w$ a une périodicité $m' < n$;

(2) Il existe un mot $g$ de longueur $n - m'$ qui est à la fois facteur gauche et facteur droit de $w$ $(w \in g\,A^* \cap A^* g)$;

(3) $w$ a une racine dont la longueur $m$ divise $m'$;

(4) $w = (uv)^p u$ où $p \geqslant 1$, $u \in A^+, v \in A^*$ $uv$ est primitif de longueur $m$ et $p\, m = m'$.

Preuve. (1) implique que $a_i = a_{i+m'}$ pour $1 \leqslant i < i + m' \leqslant n$, donc (2) avec $g = [1, n-m']\ w = [1+m', n]\ w$. Réciproquement si $w = g\,f' = f\,g$ $(f, f' \in A^*)$ on a $a_i = a_{i+q}$ pour $1 \leqslant i \leqslant i + q \leqslant n$ où $q = |f| = |f'| = n - |g|$ donc (1).

Soit maintenant $m$ le plus petit diviseur de $m'$ tel que $w$ ait

18

périodicité $m$; on pose $n = m\,p + q$ où $1 \leqslant q \leqslant p$ et on considère le mot $[1, m]\ w = u\,v$ où $u = [1, q]\ w$ est le facteur gauche de $f$ de longueur $q$. L'hypothèse que $w$ a périodicité $m$ équivaut à $w = (u\,v)^p\,u$. Si $uv$ n'était pas primitif, c'est-à-dire si on avait $u\,v = s^r$ avec $s \in A^+$, $r \geqslant 2$ on aurait $w = s^{rp+p'} s_1$ avec $s_1$ un facteur gauche de $s$ et par conséquent $w$ aurait une périodicité $|s| < m$ divisant $m'$ en contradiction avec le caractère minimal de $m$. Donc $f = u\,v$ est primitif et, comme $w\,v = f^{p+1}$, c'est une racine de $w$. Par construction tous les mots $g' = (u\,v)^{p'}u$ $(0 \leqslant p' \leqslant p)$ sont à la fois des facteurs gauches et des facteurs droits de $w$, ce qui conclut la preuve.

Q.E.D.

Une notion moins immédiate est la suivante. La <u>période locale</u> de $w$ en $j$ $(1 \leqslant j \leqslant n)$ est le minimum $p$ de la longueur des mots $z$ tels que l'on puisse trouver $g', g'' \in A^*$ pour lesquels $z$ est facteur gauche de $g'a_1 \ldots a_j$ et facteur droit de $a_{j+1} \ldots a_n\, g''$.

On vérifie sans difficulté qu'il existe un $z$ de longueur minimale $p$ et que $p \leqslant n$, et, plus précisément $p \leqslant \pi(w)$, en notant $\pi(w)$ la période minima de $w$. L'indice $j$ est dit <u>critique</u> ssi $p = \pi(w)$. La réciproque est l'objet d'un théorème découvert par Césari ([1]) dont la version optimale a été obtenue par Duval ([2]) auquel nous faisons référence pour la preuve et que nous utiliserons sous la forme suivante dans laquelle on suppose évidemment que la période $p$ est $\geqslant 2$ c'est-à-dire que $w$ n'est pas une puissance d'une lettre.

<u>Théorème de Cesari et Duval</u>. Tout mot $w$ a un indice critique $k < p$ où $p = \pi(w)$ est la période minima de $w$.

On procède maintenant à une série de calculs qui sont loin d'être nouveaux mais auxquels l'emploi de l'indice critique apporte une clarté qu'apprécieront les rares amateurs. On note $h$ la racine minima $a_1 \ldots. a_p$ de $w$, et $k \leqslant p$ un indice critique de $w$.

3.1 Si $w$ admet des périodes $\neq n$ autres que $p$, on a $k \geqslant n- p'$ où $p'$ est la plus petite de ces dernières.

<u>Preuve</u>. Soit $p < p' < n$. Comme $w$ est facteur gauche de puissances de ses racines, on a $w = h\, h_1$ où $q \geqslant 1$ et $h_1$ un facteur gauche propre (c'est-à-dire $\neq h$) de $h$. De même $w = h'^{q'}\, h'_1$. Si $w$ n'est pas périodique, $q = 1$ c'est-à-dire $h = h_1\, h_2$; $w = h\, h_1$, et aussi $w = h'_1\, h'_2\, h'_1$. Si $w$ est périodique, $q \geqslant 2$ et $q' = 1$ puisqu'un mot n'a qu'une seule racine de longueur inférieure ou égale à la moitié de sa longueur. Donc $w = (h_1\, h_2)^q\, h_1 = h'_1\, h'_2\, h'_1$ avec dans tous les cas $h_1$ et $h'_1$ des facteurs gauches de $h$ et le plus court de ces deux mots, disons $g$, un facteur droit de l'autre. Cette relation, comme on sait, implique l'existence d'un $m \geqslant 0$ et de mots $x \in A^+$, $y \in A^*$ tels que $g = (x\, y)^m x$, $g' = g\, y\, x$.

Soit $d = |x\, y|$. Si $j \leqslant |g|$, le mot $a_{j+1} \ldots a_{j+d}$ est facteur droit de $a_1 \ldots a_j$ ou il a ce mot comme facteur droit. Donc la période en $j$ de $w$ est $\leqslant d$ où $d < p$ ce qui achève la preuve puisque dans les deux cas $|g| \leqslant n - p'$.

Q.E.D.

3.2 Supposant $n \geqslant k + p$, $p$ est la période minima de tout facteur $g$ de $w$ dont le support contient les indices $k$ et $k + p$.

<u>Preuve</u>. Supposons au contraire que $g$ a une période $p' \leqslant p$. La même chose est vraie de son facteur $g'$ dont le support est $[k, p+k]$. On peut donc

20

supposer $g = g'$. En raison de la périodicité $p$ on a $x = a_k = a_{p+k} \varepsilon A$. Le calcul précédent montre que $g = x\,z\,x\,y\,x\,z\,x$. De nouveau à cause de la périodicité $p$ de $w$, $z\,x$ est facteur droit d'un mot de $A^* a_1 \ldots a_k$. La période locale de $w$ en $k$ est donc $\leqslant |z\,x|$ où $|z\,x| < p$. Contradiction.

Q.E.D.

3.3 Soient $h'$ et $h''$ deux facteurs gauches de $h$ tels que $k \leqslant |h'| \leqslant |h''|$. Alors $h'$ n'est pas facteur droit de $h''$.

Preuve. Sinon on aurait $h' = (x\,y)^q\,x$, $h'' = (x\,y)^r\,x$ avec $x \varepsilon A^+$, $r > q$ et $w$ aurait donc période locale $\leqslant |x\,y| < p$ en tout $j \leqslant |h_1|$.

Q.E.D.

Afin d'appliquer le Théorème de Césari et Duval, on dira qu'un mot $f$ rencontre $w$ selon l'intervalle $I = [i, j]$ de $[1, n]$ $(n = |w|)$ ssi $k \varepsilon I$ et si posant $f' = I\,w$ l'une des trois éventualités mutuellement exclusives suivantes se produit:

(1) $f = f'$ ;

(2) $j = n$ et $f = f'g'$ avec $y' \varepsilon A^+$ ;

(3) $i = 1$ et $f = g\,f'$ avec $g \varepsilon A^+$ ;

Pour alléger le discours on parlera de rencontre interne, droite ou gauche selon ces trois cas et une rencontre sera propre si c'est une rencontre interne ou droite ou si c'est une rencontre gauche telle que $h\,f'$ n'est pas un facteur droit de $f$.

On conviendra que si $f$ rencontre $w$ selon les intervalles $I_1 = [i_1, j_1]$, $I_2 = [i_2, j_2]$ ... etc., l'indexage de ceux-ci est tel que $i_1 \leqslant i_2$ ... et $j_1 \leqslant j_2 \leqslant \ldots$.

21

3.4 Soit $f$ de longueur $\leqslant n$ rencontrant $w$ en $I_1$ et $I_2 \neq I_1$. Alors:

(1) La rencontre $I_1$ est une rencontre gauche;

(2) Si $I_2$ est une rencontre droite, on a $2|f| > n$ ;

Dans le cas contraire:

(3) La différence $d = j_2 - j_1$ est un multiple de $p$;

(4) La rencontre $I_1$ est impropre quand $I_2$ est une rencontre gauche ou quand $d > p$ ;

(5) Quand $I_2$ est une rencontre interne, $p$ est la période minima de $f$ et sinon c'est celle de son facteur droit $f_2 = I_2\, w$.

Preuve. Par hypothèse on a $i_1 \leqslant i_2 \leqslant h \leqslant j_1 \leqslant j_2$ avec $i_1 = i_2$ ssi la valeur commune des deux indices est $1$ et symétriquement pour $j_1 = j_2$.

Montrons d'abord que l'hypothèse que $I_1$ n'est pas une rencontre gauche contredit l'hypothèse que $k < P$ est un indice critique. En effet elle implique que $f_1 = I_1\, w$ et $f_2 = I_2\, w$ soient deux facteurs gauches de $f$ et par conséquent que $d' = i_2 - i_1 > 0$ soit une périodicité de l'intervalle $[i_1, j_2]$. Comme dans les calculs précédents, on vérifie que ceci entraine que la période locale en $k$ soit $\leqslant d'$, ce qui est impossible puisque $i_1 < i_2 = i_1 + d' \leqslant k \leqslant p$ et par conséquent $d' \leqslant p$.

On suppose donc désormais que $I_1$ est une rencontre gauche. Quand $I_2$ est une rencontre droite on a $2\,|f| \geqslant |f_1| + |f_2| = j_1 + n+1 - j_2 > n$. Donc (1) et (2) sont établis. Désormais $I_2$ n'est pas une rencontre droite. Donc $f_1$ et $f_2$ sont deux facteurs droits de $f$ et on a une équation $f_2 = g\, f_1$ où $|g| \geqslant d = j_2 - j_1$. On note $f_2''$ le mot de support $[1, j_2]$.

Comme $w$ est facteur gauche d'une puissance de sa racine $h$, ce dernier mot a des facteurs gauches $h_1$, $h_2 \neq h$ tels que $f_1 = h^r h$, $f_2 = h^{r'} h_2$. Puisque $f_1$ est facteur droit de $f_2$ qui est lui-même facteur droit

22

$f'_2$ , on a $h_1 = h_2$ d'après 3.3 ce qui établit (3).

Quand $I_2$ est une rencontre gauche on a $f_2 = f'_2$ donc $f_2 = h^q f_1$ avec $q > 1$. Il en est de même quand $d > p$ puisque d'après (3) on a alors $d = m\,p$ avec $m \geqslant 2$. Quand tel n'est pas le cas, on a $f = f_2$ et (5) résulte de 3.2 puisque $i_2 \leqslant k$ par hypothèse et que

$$k \leqslant j_i < k + p \leqslant j_2 = j_1 + d$$

en raison de $d \geqslant p$ .

Q.E.D.

On pourrait préciser un peu ce qui se produit dans le cas (2) mais je n'ai pas vu comment utiliser cette information supplémentaire pour diminuer substantiellement les valeurs numériques données dans la Proposition.

Nous supposons maintenant que $w$ est un mot réduit.

3.5 Le mot $w$ a au plus deux rencontres propres avec $f$ et son inverse formel $\bar{f}$.

Preuve. Si $f$ a plusieurs rencontres avec $I$ les points (1) et (2) de la remarque précédente montrent qu'au plus une d'entre elles peut être une rencontre droite et que toutes les autres sont des rencontres gauches. Donc d'après le point (4) au plus une de ces dernières est une rencontre propre.

Supposons maintemant que $\bar{f}$ rencontre $w$ selon l'intervalle $J$ et $f$ selon $I$ et $I'$. Daprès (1) de 3.4 on peut supposer que $I$ est une rencontre gauche. Donc $f = g\,f'$ où $f' = I'w$, $g \in A^+$. On a $\bar{f} = \bar{f}'\bar{g}$. Comme les intervalles $I$ et $J$ contiennent tous les deux $k$ et comme l'hypothèse que $w$ est réduit fait qu'aucun de ses intervalles ne peut être support d'un mot et de son inverse formel, on voit que $Jw$ doit être un facteur de $\bar{g}$, ce qui implique que $J$ soit aussi une rencontre gauche.

Appliquant le même raisonnement à $I'$, à partir de $J$, montre que $I'$ est aussi une rencontre gauche, donc qu'au plus une des rencontres $I$ et $I'$ peut être propre.

Q.E.D.

Nous en venons maintenant à la preuve proprement dite de la Proposition et nous considérons un $b \in B_+$ donné, les conventions étant celles introduites à la fin de la Section 2.

Soient $w \in A^+$ de longueur $n \geqslant |b\beta|$ et $s \in S(b)$. On suppose $g\,w\,g' = s^q$ où $g, g' \in A^*$ sont de longueur strictement inférieure à $s$. Comme dans les remarques précédentes $k < p$ est un indice critique de $w$ et on suppose toujours que $m$ est un entier assez grand pour que $s^m$ soit plus long que $b$ (c'est-à-dire que $b\beta$).

Si $p \in P_s$ le corollaire 2.1 du théorème de Nielsen implique l'existence d'une lettre $b' = b'(p)$ et de mots $e, e'$ tels que $e\,b'e' \in E$, $p\,s^{m+q}$ est facteur gauche de $e\,b'e'$ et $|e'\beta| < |p\,s^m\,g| + k \leqslant |e'\beta| + |b'\beta|$.

On a évidement $b' \leqslant b$ et ces relations définissent une rencontre de $b'$ (c'est-à-dire de $f = b'\beta$) avec $w$ selon un certain intervalle $I_p$. L'ensemble des paires $(b'(p), I_p)$ pour $p$ parcourant $P_s$ a les deux propriétés essentielles suivantes:

(1) Au plus un membre de chaque paire $(b', \bar{b}')$ peut y figurer;

(2) Si $p \neq p'$ et $b'(p) = b'(p')$ on a $I_p \neq I_{p'}$.

Compte tenu de l'identité $\bar{b}'\beta = \overline{b'\beta}$, la première est la conséquence immédiate de ce que $j^{m+q}$ est un mot réduit puisque les intervalles de rencontre ont une intersection non vide (contenant $k$). La seconde résulte tout aussi immédiatement du corollaire 2.1.

24

Ce sera d'ailleurs notre seule référence à celui-ci hormis l'inégalité Card $(B_+) = r' \leqslant 3r - 2$.

## 4. Construction des groupes annexes

On revient aux notations de la section 1. En particulier $V$ est une base de Nielsen et $P$ est l'ensemble des facteurs gauches $\neq 1$ des mots de $V$. On suppose toujours $H$ réduit c'est-à-dire que $1$ est le seul facteur gauche commun des mots $V$.

Soit $Q$ l'ensemble des paires $(Hp, a)$ où $a$ est une lettre et $Hp$ une classe latérale contenant au moins un $p \in P$ qui se termine par $a$. On définit un morphisme $\mu$ de $A^*$ dans le monoïde des fonctions $Q \longrightarrow Q$ en posant pour chaque $b \in B$ et $q = (Hp, a)$

$$q.b\mu = (Hp', b) \in Q \quad \text{si } \bar{a} \neq b \text{ et si la classe latérale } Hpb \text{ contient un } p' \in P \cap A^* b\ ;$$
$$= \emptyset \quad \text{sinon.}$$

Soit désormais, $K = V^*\varphi$ l'ensemble des mots réduits représentant les éléments de $H$.

3.1 Le morphisme $\mu$ est un morphisme syntaxique de $K$.

Preuve. On considère l'ensemble $Q'$ formé des paires $(p, a)$ où $a \in A$ et $p \in P \cap A^* a$ et pour chaque $q' = (p, a) \notin Q'$ et $b \in A$ on pose

$$q'.b\mu' \begin{cases} = (p', b) & \text{si } pb = p' \in P; \\ = (b, b) & \text{si } \bar{a} \neq b,\ p \in V \text{ et } b \in P; \\ = \emptyset & \text{sinon.} \end{cases}$$

L'hypothèse que H est réduit implique que pour chaque $b \in P \cap A$ il existe une lettre $a \neq \bar{b}$ telle $V \cap A^{*}a \neq \emptyset$. Il en résulte immédiatement que K est l'image inverse par $\mu'$ des mots f tels que $Q'_1 . f \mu' \cap Q'_1 \neq \emptyset$ où $Q'_1 = Q' \cap (V \times A)$. Il suffit maintenant de vérifier que l'équivalence $(p, a) \sim (p', b)$ ssi $a = b$ et $H p = H p'$ est compatible avec la multiplication pour voir que $Q = Q'/\sim$ et $\mu = \mu'/\sim$ reconnaissent K.

Il n'existe pas de congruence $\approx$ sur Q qui soit compatible avec la reconnaissance de K et pour laquel on ait $(p, a) \approx (p', a')$ avec $H p \neq H p'$. Il faut encore vérifier que quand $H p = H p'$ et $a \neq a'$,il existe au moins une lettre b telle que un et un seul de $(p, a) . b \mu$ et $(p', a'), b \mu$ est $\neq \emptyset$. Supposons qu'il n'en soit pas ainsi c'est-à-dire que ces deux produits soient des états. Comme $H p = H p'$, ils seraient le même état $(H p'', b) = q$ et l'on pourrait trouver un mot x tel que $q. x \mu \in Q \times (H \times A)$. Considérant $(p\, b\, x\, \bar{x}\, \bar{b}\, p')\varphi$ , on voit que ce mot a le facteur $a \bar{a}'$. Comme il appartient à K, on en conclut que $(p. a) . \bar{a}' \mu \neq \emptyset$ alors que $(p', a') . \bar{a}' \mu = \emptyset$.

Q.E.D.

On montre sans difficulté que l'action $\mu : Q \times A^{*} \longrightarrow Q$ est transitive, quelle reconnait 1 et que $0 \mu^{-1}$ est le complément dans $A^{*}$ des facteurs des mots de K. Il est claire qu'elle est le produit en couronne d'un monoïde de constantes dans un groupe de permutations. Le cas où H n'a qu'un nombre fini de classes latérales correspond à celui où ce produit est un produit direct, le groupe étant alors le quotient [F] de l'action de F sur les classes latérales et étant le seul groupe maximal $\neq \{0\}$ dans le semigroupe $A^{+}\mu$ .

Dans le cas général soit $M = A^{*} \mu$. Nous rappelons que chaque groupe

26

maximal $S'$ est défini par une partie monoïde $Q_S$ de $Q$ telle que $Q\,M = Q_S\,M = Q_S$ et qu'il est conjugué de $S'$ ssi il existe $m, m' \varepsilon M$ tels que $Q_S.m = Q_{S'}$ ; $Q_{S'} = Q_S.m'$. Il est clair qu'une partie $Q_S$ est définie par une transversale $P_S \subset P_1$ et une lettre $a$, c'est-à-dire que $Q_S = \{(H\,p,\,a) : p \,\varepsilon\, S\}$. On dira qu'un autre groupe $S'$ est <u>F-conjugué</u> de $S$ ssi il existe un $f \,\varepsilon\, F$ tel que $P_{S'} = (P_S\, f)\varphi$. On peut montrer que si $S'$ n'était pas conjugué de $S$ (au sens usuel), $S$ et $S'$ se-raient cycliques ($= S\mu^{-1}$ engendré par un seul mot et $S$ transitif sur $Q_S$) et qu'il existerait $S''$ conjugué de $S'$ tel que le générateur de $S''\mu^{-1}$ soit l'inverse formel de celui de $S\mu^{-1}$. Cette observation n'est pas nécessaire pour la vérification de la propriété suivante qui est une simple reformulation des définitions.

<u>Propriété 2</u>. Il existe une bijection naturelle entre les classes de F-conjugaisons de groupes maximaux dans $(Q, A^+\mu)$ et les classes de groupes annexes. Si la classe de $(Q_S, S)$ correspond à celle de $G$, le groupe $(Q_S, S)$ est isomorphe (en tant que groupe de permutations) au groupe quotient $\boxed{G}$ de $G$.

Naturellement cette bijection est celle qui est induite par $\mu$. On notera qu'elle <u>inverse</u> l'inclusion: si les groupes maximaux $S$ et $S'$ ne sont pas conjugués et si $S'$ est contenu dans l'idéal (de $A^*\mu$) engendré par $S$, il existe un groupe annexe $G'$ correspondant à $S'$ qui admet comme sous groupe un groupe annexe $G$ correspondant à $S$ et réciproquement; les groupes annexes de rang un correspondent donc à des idéaux maximaux .

Avec un peu plus de travail on pourrait montrer qu'il existe un alphabet $C$ (de cardinalité <u>finie</u> bornée en fonction du seul rang $r$), un morphisme $\gamma: C^* \to A^*$ et une partie locale $E' \subset C^*$ telle que $E'\gamma$ soit le plus petit sous monoïde $X^+$ de $A^*$ qui contienne $\sqrt{K}$ . Il résulte de ce

27

que l'on vient de voir que le sous groupe $H'$ de $F$ engendré par $X^* \mu^{-1}$ contient $H$ et au moins un membre de chaque classe des groupes annexes.

Pour conclure, considérons maintenant les sous groupes $G$ du groupe libre $F$ définis par la condition d'être le stabilisateur d'une transversale $F_1$ telle qu'au moins un $y \in G$ a la propriété que pour tout $f \in F$ on a $H f g = H f$ ssi $f \in H F_1$. Dans le cas où $[F]$ est infini, ces groupes sont évidemment les groupes annexes. Il n'en est pas de même quand $[F]$ est fini. Leurs propriétés se rattachent de façon assez évidentes aux rapports entre la H-conjugaison et la conjugaison dans $F$.

Question. Est-il possible d'associer à $(H, F)$ un monoïde fini de façon à ce qu'une Propriété analogue à 2 soit vraie pour cette famille de sous groupes?

## R E F E R E N C E S

(1) Y. CESARI et M. VINCENT, Une caractérisation des mots périodiques. Comptes Rendus Acad. Sci., Paris, 286 (1978) pp.1175-77.

(2) J.P. DUVAL, Périodes et répétitions. Theoretical Computer Science 9 (1979), pp. 17-26.

(3) S. EILENBERG, Automata, Languages and Machines. Academic Press, New York, 1974.

(4) G. LALLEMENT, Semigroups and Combinatorial Applications, J. Wiley and Sons, New York, 1979.

(5) R.C. LYNDON et P.E. SCHUPP, Combinatorial Group Theory, Springer Verlag, Berlin, 1977.

# TRANSACTIONS

*of the*

# EIGHTH PRAGUE CONFERENCE

*on*

## INFORMATION THEORY, STATISTICAL DECISION FUNCTIONS, RANDOM PROCESSES

held at

Prague, from August 28 to September 1, 1978

VOLUME C

ACADEMIA

PUBLISHING HOUSE
OF THE
CZECHOSLOVAK ACADEMY OF SCIENCES

*PRAGUE 1979*

# ON AN APPLICATION OF ERGODIC THEORY TO SOME PROBLEMS IN CODING

F. BLANCHARD, D. PERRIN, M.P. SCHÜTZENBERGER

## 1. INTRODUCTION

Consider a source with alphabet $B$ which is encoded over a channel with alphabet $A$ by means of a mapping

$$\alpha : B \to X$$

of $B$ into a set $X$ of finite strings over the alphabet $A$.

Moroever a probability $\mu$ is defined on the space $B^{\mathbb{Z}}$ of (doubly) infinite strings over $B$.

This probability induces in a natural way (cf. §3) a probability $\nu$ on $A^{\mathbb{Z}}$ and two questions arise :

1. does $\nu$ allow to compute $\mu$ (source identification problem) ?

2. for which $\mu$ is it possible to achieve a stochastic decoding (choosing among the various decodings of a given infinite string in $A^{\mathbb{Z}}$) ?

The question 2 is relevant even if the mapping $\alpha$ is one to one on the set $B^*$ of finite strings over $B$. In fact, even in this case an infinite string of $A^{\mathbb{Z}}$ may admit various decodings in $B^{\mathbb{Z}}$ and this phenomenon in related to a property of codes called synchronization.

We will show how one may use methods of ergodic theory to answer questions 1 and 2 by assuming convenient hypotheses on the measures $\mu,\nu$ : this is the transfer theorem of §5.

The terminology and properties of ergodic theory used here may be found in [1]. Proofs will appear elsewhere.

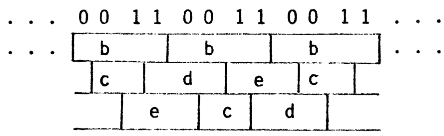
## 2. EXAMPLE

Let $B = \{a,b,c,d,e\}$ , $A = \{0,1\}$ and $\alpha$ be the mapping :

$$\alpha(a) = 0\,0\,0,\quad \alpha(b) = 0\,0\,1\,1,\quad \alpha(c) = 0\,1,\ \alpha(d) = 1\,0\,0,\quad \alpha(e) = 1\,1\,0.$$

It may be verified that no element of $X = \alpha(B)$ is a left or right factor of another and that $\alpha$ is consequently one to one from $B^*$ into $A^*$.

Let $G = \{a,b\}^{\mathbb{Z}}$ and $H$ the subset of $B^{\mathbb{Z}}$ of all infinite words that may be written as an infinite product of finite strings taken out of the set $a^*c\,d\,a^*e$. After using the substitution $\alpha$ one obtains the same subset $Z \subset A^{\mathbb{Z}}$ for $G$ and $H$ ; any infinite word in $Z$ can be read in one way as an image of an element of $G$ and in two different ways as the image of an element of $H$. For instance :




Let $\nu$ be a finite ergodic measure on $Z$ distinct of the Dirac measure on the point $0^{\mathbb{Z}}$. Any ergodic measure $\mu$ on $B^{\mathbb{Z}}$ such that $\mu^\alpha=\nu$ will have a support included either in $G$ or in $H$. In fact there is exactly one such measure with $\mu(G) = 1$ and there may be either one or two such measures with $\mu(H) = 1$.

For instance, if $\mu_1$ is such that for almost every element of $H$, the number of symbols a following an $e$ is odd whereas it is even after a d. Then the equation $\mu^\alpha = \mu_1^\alpha$ has a solution $\mu_2$ which has the reverse property since

$$\alpha(de) = 0\,\alpha(h)0$$

and the parity is inverted between the two intepretations in $H$.

In this case it is not possible to compute $\mu$ knowing $\nu$ (i.e. the source may not be idendified) but it is possible to distinguish the two interpretations in H of a given sequence in Z.

## 3. DEFINITIONS

Let $A^*$ denote the set of finite strings over $A$ ; $A^*$ is the free monoid over the set $A$.

An encoding

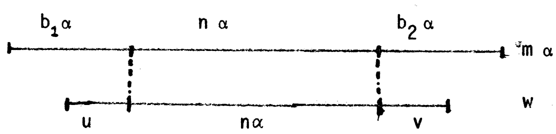
$$\alpha : B \to X \subset A^*$$

is a mapping from $B$ into $A^*$ which can be extended to an injective morphism from $B^*$ into $A^*$. We suppose $A, B$ and thus $X$ to be finite.

We shall say that a string $m \in B^*$ is a covering of $w \in A^*$ if :

$m = b_1\, n\, b_2$ ; $b_1, b_2 \in B$

$$f = u(n\alpha)v \ ; \ b_1\alpha \in A^*u \ ; \ b_2\alpha \in vA^*$$




Let $C(w)$ be the set of coverings of $w$.

Now for any $\mu : B^* \to \mathbb{R}$,

we define $\mu^\alpha : A^* \to \mathbb{R}$

by :

$$\mu^\alpha(w) = \frac{1}{E_\mu(\alpha)} \sum_{m \in C(w)} \mu(m),$$

where $E_\mu(\alpha) = \sum_{b \in B} |b\alpha|\, \mu(b)$ is the average length of $X = B\alpha$.

The following fact is easy to check :

Proposition 1.- If $\mu$ defines an invariant or ergodic measure on the space $B^{\mathbb{Z}}$, so does $\mu^\alpha$.

It is convenient to define a subset $\Omega$ of $B^{\mathbb{Z}} \times \mathbb{N}$ as follows :

$$\Omega = \{(b,i) \in B^{\mathbb{Z}} \times \mathbb{N} \mid 0 \leq i < f(b)\}$$

where $b = (b_j)_{j \in \mathbb{Z}}$ and $f(b) = |\alpha(b_0)|$ denotes the length of the string $\alpha(b_0) \in A^*$.

The mapping $\alpha : B \to X \subset A^*$ may be extended in a unique way to $\phi : \Omega \to A^{\mathbb{Z}}$ by stipulating that (cf. fig. 1) :

$$\phi(b,i) = \dots a_{-1}\, a_0\, a_1 \dots$$

and

$$\begin{cases} \dots a_{-i-2}\, a_{i-1} = \dots \alpha(b_{-2})\, \alpha(b_{-1}), \\ a_{-i}\, a_{-i+1} \dots = \alpha(b_0)\, \alpha(b_1) \dots \end{cases}$$

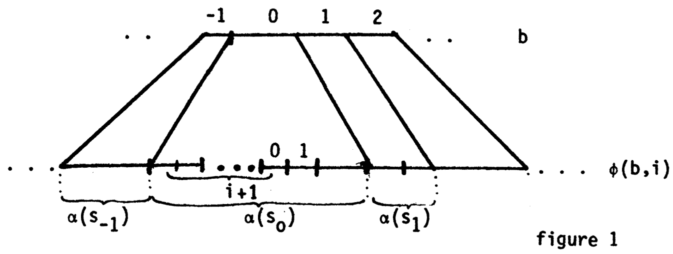



figure 1

An automorphism (i.e. an invertible bimeasurable function) is defined on the set $\Omega$ by extension of the natural shift $S$ on $B^{\mathbb{Z}}$ :

$$\begin{aligned} \bar{S}(b,i) &= (b,i+1) \quad \text{if } i < f(b) - 1 \\ &= (Sb,0) \quad \text{if } i = f(b) - 1. \end{aligned}$$

In this way, we have a commutative diagram using the shift $T$ on $A^{\mathbb{Z}}$ :

$$\begin{array}{ccc} \Omega & \xrightarrow{\phi} & A^{\mathbb{Z}} \\ \downarrow{\scriptstyle \bar{S}} & & \downarrow{\scriptstyle T} \\ \Omega & \xrightarrow{\phi} & A^{\mathbb{Z}} \end{array}$$

This construction is just that of the standard <u>tower</u> of height $f$ over the space $B^{\mathbb{Z}}$ ; and the measure $\mu^\alpha$ defined above is nothing else than the measure induced by $\phi$ on $A^{\mathbb{Z}}$ from the restriction to $\Omega$ of the product measure on $B^{\mathbb{Z}} \times \mathbb{N}$.

One may also note that the image of $\Omega$ in $A^{\mathbb{Z}}$ by $\phi$ is a sofic system, as defined by B. Weiss [4] ; in fact, it is classical that if $X$ is a finite set, there exists a finite monoid $M$ and a morphism

$$\sigma : A^* \to M$$

such that $\sigma^{-1} \sigma X^* = X^*$ (cf. [3], for instance).

## 4. INTERPRETATIONS

Given an $a \in A^{\mathbb{Z}}$, we say that $I \subset \mathbb{Z}$ is an <u>interpretation</u> of $a$ if for any consecutive elements $n,m$ in $I$, one has :

$$a_n \, a_{n+1} \cdots a_{m-1} \in X.$$

Thus, for example, for any $(b,i) \in \Omega$, the element $\phi(b,i)$ admits an interpretation containing the point $-i$.

<u>Proposition 2</u>.- Let $\nu$ be a shift invariant measure on $A^{\mathbb{Z}}$ whose support is included in $\phi(\Omega)$ ; for almost any point in $A^{\mathbb{Z}}$, two distinct interpretations have an empty intersection.

If $\nu$ is ergodic, the number of interpretation is almost surely constant.

It is worthwhile to mention that both statements of this proposition have an algebraic counterpart. The second one is related to the Suschkevitch theorem in finite monoids (cf. [2]) and the first one may be restated as follows :

Say that $a$ $A^{\mathbb{Z}}$ is <u>formally recurrent</u> if any finite factor

$$w = a_i \, a_{i+1} \cdots a_{i+j}$$

occurring in $a$ may be found infinitely many times for $i \geq 0$ and for $i \leq 0$.

<u>Proposition 3</u>.- Two distinct interpretations of a formally recurrent sequence are disjoint.

Let us now suppose that $\nu$ is an ergodic measure on $A^{\mathbb{Z}}$ ; we call <u>degree of the channel</u> the integer $d = d(\alpha,\nu)$ which is the number of interpretations of almost every point in $A^{\mathbb{Z}}$ ; $E$ is the set of these points.

The set $E \times \bar{d} = E \times \{1,2,\ldots,d\}$ is equipped with a bimeasurable bijection $\tilde{T}$ making the following diagram commute :

$$\begin{tikzcd} \Omega \arrow[r, "\eta"] \arrow[d, "\bar{S}"'] & E \times \bar{d} \arrow[d, "\tilde{T}"] \\ \Omega \arrow[r, "\eta"] & E \times \bar{d} \end{tikzcd}$$

where $\eta(b,i) = (\phi(b,i),j)$, with $j$ determinated by an arbitrary ordering of the set of interpretations of $a = \phi(b,i)$.

In this way, $\tilde{T}(a,j) = (Ta, p_a(j))$

where $p_a$ is a permutation.

If we are given an ergodic measure $\mu$ on $B^{\mathbb{Z}}$ such that $\mu^{\alpha} = \nu$, we may define the degree of the source using the following statement :

Proposition 3.- There exists an event $P \subset \Omega$ with measure 1 such that for any $a$ in $E$, the cardinality of the set

$$\{j \in \bar{d} \mid (a,j) \in \eta\, P\}$$

is almost surely constant.

We denote by $d' = d'(\alpha,\mu)$ this integer, which is by definition the degree of the source ; it is obviously the number of interpretations of an element of $A^{\mathbb{Z}}$, coherent with the measure $\mu$. These interpretations may be asymptotically discriminated from the others, considering only finite strings of $A^*$.

## 5. TRANSFER THEOREM

Denote by $\tilde{\nu}$ the measure on $E \times \bar{d}$ which is the product of the ergodic measure $\nu$ by the measure giving weight $1/d$ to each point of $\bar{d}$.

Proposition 4.- The measure $\tilde{\nu}$ is invariant by $\tilde{T}$

We can now state the main result of this paper which may be considered as a transfer theorem from the ergodic measures on $A^{\mathbb{Z}}$ to that on $B^{\mathbb{Z}}$ by means of the encoding :

Theorem. - The ergodic measures $\mu$ on $B^{\mathbb{Z}}$ solution of

$$\mu^{\alpha} = \nu$$

are elements of the set $M$ of ergodic decomposition of $\tilde{\nu}$. Moroever :

$$\sum_{\mu \in M} d'(\alpha,\mu) = d.$$

In other words if $\mu$ is an ergodic measure inducing by $\alpha$ the measure $\mu = \nu^{\alpha}$, an element of $A^{\mathbb{Z}}$ admits $d' = d'(\alpha,\mu)$ indistinguishable interpretations.

Thus the source identification problem is easiest when $d'=d$ whereas stochastic decoding is of maximal complexity. Conversely, when $d'=1$, the number of possible sources is $d$ but for a given source stochastic decoding may be achieved unambiguously.

REFERENCES

[1] BILLINGSLEY, P. : Ergodic Theory and Information
Wiley, 1965.

[2] CLIFFORD, A.H. et C.B. PRESTON : The Algebraic Theory of Semigroups
Vol. 1 , Amer. Math. Soc. (1961).

[3] EILENBERG, S. : Automata, Languages and Machines, Vol. A
Academic Press, (1974).

[4] WEISS, B. : Subshifts of finite type and sofic systems,
Monatshefte für Math., 77 (1973) 462-474.

F. BLANCHARD
UNIVERSITE PARIS VI
LABORATOIRE DE PROBABILITES
Tour 56
4 Place Jussieu

75230 PARIS CEDEX 05

D. PERRIN
UNIVERSITE DE ROUEN
et LABORATOIRE C N R S
Informatique théorique et
Programmation

M.P. SCHÜTZENBERGER
UNIVERSITE PARIS VII
et L I T P

C. R. Acad. Sc. Paris, t. 288 (15 janvier 1979) Série A — 95

THÉORIE DES GROUPES. — *Croissance des polynômes de Foulkes-Green*. Note (*)
de **Alain Lascoux** et **Marcel Paul Schützenberger,** Correspondant de l'Académie.

On énonce un théorème d'isomorphie entre les classes de conjugaison d'un certain monoïde et on en déduit des inégalités entre polynômes de Green des groupes linéaires finis.

*An isomorphism theorem within the plactic monoïd is given. Applications are made relating Green polynomials for finite linear groups to the structure of the lattice of partitions.*

Soit $A^*$ le monoïde libre engendré par l'ensemble fini totalement ordonné $\{A, \leqq\}$. On note $\#$ l'antiautomorphisme naturel (défini par sa restriction à A : $c\# < b\#$ ssi $b < c$).

Tout intervalle B de A définit un morphisme de restriction de $A^* \to B^*$ envoyant chaque mot $w$ sur son plus long sous-mot $w \cap B^*$ contenu dans $B^*$.

On prouve :

Il existe dans $A^*$ une congruence minimale (unique) notée $\equiv$ telle que :

— d'une part dans l'algèbre $\mathbf{Z}(A^*/\equiv)$ les éléments $\sum\{x : x \in A\}$ et $\sum\{yx : x, y \in A, y > x\}$ commutent;

— d'autre part, pour tout intervalle B, $w \equiv w'$ implique

$$w \cap B^* \equiv w' \cap B^*.$$

Le monoïde quotient $A^*/\equiv$ est dit *monoïde plaxique;* nous en avons donné une *présentation* légèrement différente dans [1].

Rappelons quelques propriétés élémentaires :

(1) les classes dans $Z(A^*/\equiv)$ des éléments

$$S_k = \sum\{x_1 \ldots x_k : x_i \in A, x_1 \leqq \ldots \leqq x_k\}$$

engendrent une sous-algèbre commutative;

(2) $w \equiv w' \Rightarrow w\# \equiv w'\#$;

(3) Il existe une section remarquable $A^*/\equiv \to A^*$ dont l'image est l'ensemble T des *tableaux* (*cf.* [1]). La composition $A^* \to A^*/\equiv \to T$ est dit *redressement* et notée R.

(4) Il existe une application $t - \overline{t}|$ des tableaux sur l'ensemble des partitions ($\overline{t}|$ est le *diagramme* ou la *forme* de $t$), ainsi qu'une bijection

$$w \to (w\,R, w\,\mathscr{C})$$

de $A^*$ sur l'ensemble des paires de tableaux

$$t = w\,R, \qquad t' = w\,\mathscr{C} : \quad \overline{t}| = \overline{t'}|, \qquad t' \in A^!$$

(i. e. $t'$ est une permutation des premières lettres de A).

De fait, si $w \in A^!$, $t' = w^{-1}\,R$, où $w^{-1}$ est la permutation inverse de $w$.

Soit $N^A$ le monoïde *commutatif* libre sur A. Son groupe Aut ($N^A$) se relève de façon unique en un groupe Bij$(A^*)$ de bijections : $A^* \to A^*$ [ce n'est pas le relèvement élémentaire $x_1\,x_2 \ldots \to (x_1)\sigma(x_2)\sigma \ldots$] :

$$\sigma \in \text{Aut} \to \sigma \in \text{Bij}$$

en imposant les deux conditions :

pour tout $w \in A^*$, $\sigma \in \text{Aut}$, et tout intervalle B de A, on a :

(1) $$\{B\sigma\} = \{B\} \quad \Rightarrow \quad (w \cap B^*)\sigma = w\sigma \cap B^*,$$

(2) $$w\mathscr{C} = w\sigma\mathscr{C}.$$

On a alors :

Proposition 1 :

(1) $w\sigma \# = w \# \sigma^{\#}$ [avec $\sigma^{\#}$ : $\forall b \in A$, $b\sigma^{\#} = (b\sigma)\#$];

(2) $w R\sigma = w\sigma R$;

(3) si $a$ est la première lettre de A et si $a\sigma = a$, alors

$$(aw)\sigma = a(w\sigma).$$

Théorème 2 (théorème de conjugaison). — *Pour chaque factorisation $w = w_1 w_2$ d'un mot $w$, pour chaque $\sigma \in \text{Bij}(A^*)$, on a*

$$(w_1 w_2)\sigma = w_1' w_2', \qquad |w_1| = |w_1'| \quad \Rightarrow \quad (w_2 w_1)\sigma = w_2' w_1'.$$

(*$|w|$ est la longueur de $w$*).

On peut remarquer que les éléments de Bij (A*) préservent les puissances

$$(w^n)\sigma = (w\sigma)^n.$$

Soit I une partition, $I \in \mathbf{N}^A$ (i. e. $\ldots \leqq cI \leqq bI \leqq aI$). Appelons *cyclage* d'un tableau $t$ d'évaluation commutative I toute opération

$$t \to t' \in T: \quad \exists t'', \qquad x \in \{A \setminus a\}, \qquad t \equiv xt'', \qquad t' \equiv t''x$$

Il est aisé de voir que tout tableau peut être transformé en le tableau *ligne* de même évaluation $\underbrace{a\ldots a}_{aI}\underbrace{b\ldots b}_{bI}\ldots$ *par une suite de cyclages.*

Soit T (I) l'ensemble {tableaux d'évaluation I, cyclages}. Le théorème 2 permet de transporter la structure de cyclage aux tableaux d'évaluation quelconque H. Soit en effet I la partition

$$\exists \sigma \in \text{Aut}(\mathbf{N}^A), \qquad H\sigma = I.$$

Par définition, $t \to t'$ est un *cyclage* de tableaux d'évaluation H si et seulement si $t\sigma \to t'\sigma$ l'est, et l'on définit T (H) comme l'image de T (I) par $\sigma$.

Lemme 3. — *Il existe une fonction $\upsilon : T \to \mathbf{N}$ dite* cocharge *telle que :*

(1) *$t\upsilon = 0$ ssi $t$ est un tableau ligne;*

(2) *si $t \to t'$ est un cyclage, alors*

$$t\upsilon = t'\upsilon + 1.$$

*Remarque.* — Nous avons défini dans [1] la charge $\nu$ d'un tableau d'évaluation une partition I; la cocharge est de fait égale à

$$bI + 2(cI) + 3(dI) + \ldots - \nu.$$

Soit H, $H' \in N^A$, $aH' = aH + 1$, $bH' = bH - 1$, $xH' = xH \, \forall x \neq a, b$. Il est clair que l'opération « changer $a$ le plus à droite en $b$ » est une injection de l'ensemble des tableaux d'évaluation H′ dans l'ensemble des tableaux d'évaluation H. On a plus :

Proposition 4. — *L'opération ci-dessus une injection de* T(H′) *dans* T(H) *conservant la cocharge et la forme.*

Corollaire 5. — *Soit* I *et* J *deux partitions de poids n, et soit* G(I, J) *le polynôme de Green du groupe linéaire fini* $\mathrm{Gl}(n, F_q)$ *associé à ces deux partitions. Alors pour toute partition* $I' \leqq I$ :

$$G(I', J) \leqq G(I, J).$$

*Démonstration.* — Le polynôme de Green est, à une puissance de $q$ près, et en échangeant $q$ en $1/q$, égal au polynôme de Foulkes F(I, J) (*cf.* [2]); plus précisément, d'après [3] :

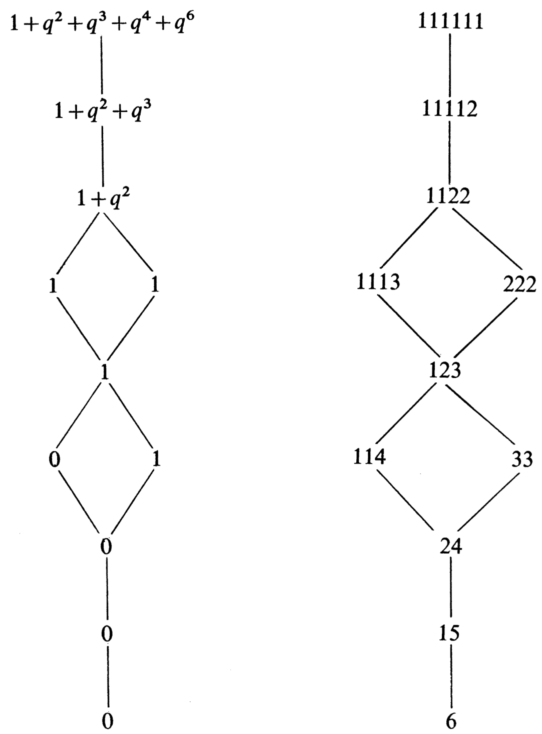
$$G(I, J) = \sum \{ q^{\upsilon(t)} : t \in T(I), \overline{t}| = J \}.$$

Il suffit de se placer dans le cas où les partitions I et I′ sont consécutives dans le treillis des partitions; il est clair (*cf.* [3]) qu'il existe σ tel que H = I σ, H′ = I′ σ vérifient les hypothèses de la proposition 4, et donc

$$T(I') \simeq T(I'\sigma) \subsetneq T(I\sigma) \simeq T(I)$$

entraîne le corollaire.

Exemple. — Pour le poids 6 et J = 000033, nous avons figuré côte à côte le treillis des partitions et les polynômes de Green correspondants :



La même technique permet d'obtenir un système d'inégalités plus complexes. Par exemple si $I_1$, $I'_1$, $I_2$, $I'_2$ sont quatre partitions de même poids telles que

$$c\,I_1 = c\,I'_1 = c\,I_2 - 1 = c\,I'_2 - 1 < b\,I_1 = b\,I'_1 + 1 = b\,I_2 - 1 = b\,I'_2 < a\,I_1 = a\,I'_1 - 1 = a\,I_2 = a\,I'_2 - 1,$$

avec égalité pour les autres lettres, on a pour toute partition J :

$$(F(I_1, J) - q\,F(I'_1, J)) - q\,(F(I_2, J) - q\,F(I'_2, J)) \geqq 0.$$

(*) Séance du 8 janvier 1979.

[1] A. Lascoux et M. P. Schützenberger, *Comptes rendus*, 286, série A, 1978, p. 323.
[2] I. G. Macdonald, *Symmetric Functions and Hall Polynomials* (à paraître).
[3] H. Kraft et C. Procesi, *Closures of Conjugacy Classes of Matrices Are Normal*, preprint 1978.

*Laboratoire d'Informatique théorique et Programmation, L. A.* 248,
*Université Paris-VII*, Tour 55-56, 2, *place Jussieu*, 75005 *Paris*.

A propos du livre "On system Analysis" de D. Berlinski

M. P. Schützenberger

## 1 - Introduction

Les remarques que je développerai plus loin sur la Théorie Générale des Systèmes soulèveront de nombreuses objections. Beaucoup d'entre elles seront tellement irréfutables que je n'entreprendrai pas d'y répondre : ce sont celles qui sont armées d'arguments d'une portée si universelle qu'elles vaudraient avec la même force pour (ou contre) la plupart des théories qu'elles soient vraies, absurdes, certaines fausses ou vides.

Le premier argument, version démocratique du principe d'autorité, oppose à tout examen d'un système le fait réel ou allégué de son acceptation comme idéologie d'une pratique sociale plus ou moins populaire. Il rend futile devant certains la discussion de l'astrologie, de la radiesthésie, de l'existence des antipodes, de la psychanalyse, des prévisions météorologiques, de la théorie élémentaire des ensembles, etc, etc.

Notez ici, je vous prie, que l'urgence de la nécessité motivant cette pratique sociale (mettons l'astragalomancie computeurizée de vos amours, du prix des épices ou de ma mort) ne diminue en rien l'ineptitude (éventuelle) de la théorie qui la sous-tend.

Après vient le recours à la défense élastique vantant la théorie non point pour ce qu'elle dit, concédé être faux ou vain, mais au nom des travaux qu'elle aurait provoqués ou, plus souvent, des progrès admirables qui découleront sans doute des recherches qu'elle

./

ne manquera pas de susciter. Nous voici donc renvoyés au cabinet des horreurs de l'histoire des techniques ou à la Science des Futurs. Mais si vous acceptez cet argument il vous faut encore acclamer l'astrologie mère de l'astronomie, tout autant que l'erreur de Cassini à laquelle nous dûmes deux laponnes.

Ainsi que les autres, l'argument suivant est ontologiquement imparable : c'est celui de la valeur explicative. Pour ceux d'entre nous dont je respecte les convictions marxistes (resp. darwiniennes, resp. bretonnes, resp. freudiennes) le matérialisme dialectique (resp. la sélection naturelle, resp. la lune, resp. l'inconscient) expliquent, et fort bien, tout (resp. les marées, resp. n'importe quoi). Pour d'autres, absolument pas. Quant à moi, je tiens la primatité du nombre 127, expliquée à la perfection par le double fait qu'il divise $-2+(1.416.317.954)^2$ et par celui que Dieu est beau. Position ferme et irrévocable contre laquelle vous ne prévaudrez pas. En réciprocité, je ne tente pas d'altérer votre opinion personnelle (peut être donnez-vous des priorités inverses aux deux raisons ci-dessus) car une explication ne vaut que pour qui s'en sent illuminé.

Pourquoi donc croire à l'effet de la lune sur les marées ? Certainement pas seulement parceque de nombreux témoins graves ont dans de longs écrits déclaré avoir vu celles-ci (et aussi la lune) sans que l'on puisse soupçonner leurs observations d'être viciées par des intérêts personnels (même abyssaux) ou par l'effet d'un entraînement collectif.

Non plus parce que des calculs par machine prétendant se baser sur les mouvements de notre satellite permettent une prévision efficace, socialement louable et numériquement précise des niveaux de la mer (ils incorporent tant de données locales ...). Mais il me semble parce que la théorie de l'Attraction Universelle (disons) et de son action sur l'hydrosphère rend compte sans (trop de) failles ni glissements de sens sournois d'une mutitude de phénomènes. Certains qualitatifs non triviaux (pourquoi donc cette coïncidence entre les

./

hautes eaux et les équinoxes ?) d'autres quantitatifs et ceux-ci très fidèlement, au moyen de paramètres empiriques dont elles donnent avec franchise la liste à priori ainsi que la prescription à suivre pour les déterminer.

Bien plus encore, comme vous l'instaurâtes, Sir Karl, notre Maître, parce que ce tissu immense de raisonnements tomberait en charpie si l'on y changeait le moindre point ou si se rencontrait quelque désaccord avec ce qui se peut observer (bien que maint pêcheur du Maîne ait été étonné quand le goût des vacances l'a conduit au Tonkin).

Ceci achève la recopie du cours de logique à vous transmis depuis la classe du Philo du Collège Agricole d'Ouzouer-le-Marché où il me fût dicté bien avant que l'informatique ait changé tout cela.

Et pour conclure, et faire transition, l'argument d'obsolescence ou d'incompétence, souverain dans les domaines (tels Parapsychologie, Intelligence Artificielle, structure de la mode, diététique, etc. etc.) où l'espoir de flux monétaires intenses induit un progrès rotatif rapide et incessant. La multiplication concomittante des chapelles vibrionniques ne laisse au commentateur que le choix de l'aveu : il n'a pas encore lu le prochain livre à paraître qui, enfin, sera le bon, ou, plus dangeureusement, il a cru entendre le dernier séminaire rival. Donc, sans aucun doute, le commentateur est un ignorant et un vilain jaloux. Un cuistre.

- Le but et les méthodes

La théorie générale des sytèmes (GST) est un mouvement d'idées aux origines multiples et aux visées immenses qui s'est assez largement développé aux Etats-Unis dans les années 60 et dont la popularité est devenue mondiale avec le "rapport de Rome" auquel s'est attaché le nom de J.W. Forrester un des plus influents protagonistes de la GST. (World Dynamics 1971). A tel point que même les instances les plus élevées de l'administration scientifique française ont été au courant de ce phénomène (Cf. le projet de 1977 du CNRS sur la G.S.T.).

Quelles en sont les sources, les buts, les méthodes ?

J'ai déjà dit que les origines de la G.S.T. étaient diverses : parmi celles que citent le plus volontier les auteurs figurent l'oeuvre d'un biométricien mineur (en tant que biologiste) mais respectable, von Bertalanffy (General System Theory 1968), d'un psychiatre anglais Ross Ashby (An introduction to Cybernetics 1956), et les livres biographiques ou de vulgarisation scientifique d'un grand mathématicien, Norbert Wiener (Cybernétique, etc. 1955).

De fait, d'autres auteurs non moins graves semblent se réclamer de toutes autres sources puisqu'aucun de ces trois noms ne figure dans l'exposé d'ensemble de la G.S.T. destiné au grand public (Compton Conferences, MIT 1968) par le mieux reconnu des théoriciens des systèmes, Herbert A. Simon. Il en est de même d'ailleur du nom de A. Rapoport, bien que ce dernier comme les autres déjà cités doive être considéré comme l'un des cinq auteurs les plus influents d'après l'étude "systématique" publiée en 1977 par R. Cavallo (in Klir, Applied General Systems Research).

Pour ce qui est des thèmes, la boule de feu première paraît être indubitablement le grand bouillonnement d'idées nouvelles qui s'étaient exprimées dans les années 50 à la cafétéria du MIT (en particulier) et (de façon plus incontrôlée) dans les symposiums de la Josiah Macy Foundation : ce sont ces projets, et ces espoirs qui constituent la substance de la partie non autobiographique du livre de N. Wiener et il me paraît digne d'y associer la mémoire d'un autre de mes Maîtres, Warren Mc Culloch, psychiatre et homme de culture dont l'intelligence et la bonté rayonnante encourageaient les pires audaces intellectuelles. Quelques années plus tard, sous l'influence de Warren, le même mouvement s'implantera dans les plaines de l'Ohio, sous le nom de Bionics, avec un infléchissement très marqué vers la biologie ingénieresque et von Bertalanffy finira par être inscrit parmi les précurseurs.

./.

Quand au courant strictement cybernétique (qui n'avait jamais été pris au sérieux aux Etats-Unis) il va fleurir en URSS, dans certains pays de l'Est, en Italie, à Namur.

Ceci pour l'anecdote et l'on pourrait sans peine retracer les filiations effectives qui d'un centre à un autre ont permis le développement de ces idées et l'attribution des crédits.

Intellectuellement, les motivations sont doubles : La plus immédiate est la poursuite de l'ambition scientifique de <u>tout</u> réduire à la mathématique : les succès admirables de von Neuman et de Shannon dans la formalisation des jeux et des communications faisaient espérer que la même entreprise devrait réussir ailleurs : en sociologie au delà de Lewin et de Moreno, en psychologie, plus profondément que par la psychométrie, en physiologie cérébrale, etc. etc.

Bien sûr, cet effort est dans la tradition scientifique la plus classique. Notons cependant qu'elle a pour outil essentiel les modèles dont le succès ou l'échec ne peut être discuté qu'en fonction de leur adéquation empirique et que cet empirisme s'évanouira chez les systémistes plus récents.

La deuxième, tout au contraire, est une réaction contre l'ambiance intellectuelle atomiste et réductionniste des pays de culture anglo-saxonne. Reprenant de vieux thèmes continentaux sur la prééminence du tout sur la partie et le primat de la relation par rapport à l'objet, elle a d'autant plus de succès qu'elle apparaît dans l'Ohio puis en Californie comme une nouveauté révolutionnaire fulgurante. (Tout comme, bien entendu, les échos appauvris de l'associationisme, soulèveront l'enthousiasme romantique des lecteurs européens formés à la rhétorique sonore de la Sorbonne Lettres).

Et entrent en scène pour tout réconcilier les mathématiques formelles dont la connaissance commence à pénétrer les chaumières. D'autant que par chance, les ordinateurs permettent de sauter par le biais de la simulation toute difficulté de raisonnement mathématique qui ferait apparaître les failles du discours.

./

Les voici donc prêts à résoudre les problèmes fondamentaux qui confrontent le monde moderne :

Attendu que toute chose (la plante, la ville, la famille, le cerveau, la prison, l'oecumène) est un système ; attendu que tout système est une entité complexe, hiérarchisée dans laquelle les interactions entre les parties et le tout constituent l'essentiel.
attendu qu'il est impérieux de contrôler l'évolution ce ces systèmes sous peine de périr (de pollution, de manque ou d'excès de communication, de vivisection, ou de trop de calories ... etc etc.)
attendu que les techniques classiques n'y peuvent rien ;
il faut au plus vite élaborer une théorie générale permettant la compréhension des dits systèmes, et du même mouvement la possibilité de guider leur cours (s'il en est encore temps !).

Voici pour les buts.

Quand aux méthodes, elles feront largement appel aux mathématiques les plus modernes (catégories, récursivité) aux chapitres les plus récents (théorie de l'information, des jeux, des automates) et aussi à la modélisation sur ordinateur la plus impitoyable qu'on ait vue depuis le règne de Procuste.

Je ne crois pas que cette insistance sur l'aspect <u>mathématique</u> de la G.S.T. soit une interprétation personnelle. Certes des auteurs importants (par exemple le doux Laszlo) ne se préoccupent que de l'aspect philosophique, (curieusement toutefois, le seul linguiste qu'il cite est aussi le seul ayant effectivement tenté de mathématiser sa discipline) ; certes aussi H. Simon évite prudemment les raisonnements formalisés et préfère la force de vérité foudroyante d'assertion telle que la suivante qu'un psychiatre aurait dû se retenir de citer :

"L'homme considéré comme un système animé est relativement simple. L'apparente complexité de son comportement est, pour une large part, le reflet de la complexité de l'environnement dans lequel il vit". (loc. cit. trad. française p. 69).

./

En ce qui concerne la philosophie ou la psychologie à ce niveau je n'ai rien à dire, non plus qu'en ce qui concerne l'usage poétique que peut jouer la G.S.T. dans l'expression de la pensée de certains de mes amis. Mais je le répète, la partie mathématique est l'ingrédient essentiel de la G.S.T. Le même livre de H. Simon abonde en références corroboratives aux travaux de M. Minsky (Prof. aux Dpts de Mathématiques et d'Informatique du MIT) ; le livre fondamental de Mesarovic (Theory of hierarchical multilevel Systems) a toutes les apparences typographiques d'un ouvrage normal de la série dans lequel il est paru (Mathematics in Science and Engineering) ; de même celui de Zeigler. Bref, je ne pense offenser personne en affirmant que les trois quarts ou plus des communications présentées à la Conference Internationale de G.S.T. à New York en 1977 sont incompréhensibles à tout lecteur de bonne volonté dont la culture mathématique ne dépasserait pas très nettement celle du bac. C.

C'est donc à ce titre que le cordonnier que je suis peut se permettre une observation sur une doctrine qui a valu un prix Nobel à un de ses meilleurs Pères.

Cette observation est que la partie mathématique de la G.S.T. est une imposture absolue.

Je dois avoir l'honnêteté d'ajouter que la même observation avait déjà été faite par D. Berlinski (sur une base bien différente, comme on pense).

## 3 - Des mathématiques comme instrument d'imposture

Il faut maintenant que je justifie mon observation, et je tourne la plume sans parvenir à me décider sur le choix d'une stratégie. Vous vous souvenez du personnage de Huxley qui demande (avant guerre, bien sûr) qu'on lui prouve que la face postérieure de la lune n'est pas habitée par une race spéciale d'éléphants verts ? je suis ici son interlocuteur. Seriez-vous prêts à ce que je démontre à coup d'équations les erreurs grossières de Rosen, la fausseté du théorème principal d'Ashby, le

./

8.

caractère absurde des simulations de Forrester (voir cependant à ce propos ce qu'est amené à en dire Berlinski), que je développe la noire série d'arguments techniques qui permet de prévoir l'échec du "General Problem Solver" de H. Simon ainsi que d'autres il y a 10 ans avaient permis la même prédiction en ce qui concernait le perceptron ou la traduction automatique ? Les outils conceptuels et les théorèmes seront là depuis Kleene et on peut maintenant s'appuyer sur la rigueur du Traité de S. Eilenberg (Automata, Formal Languages and Machines, 1974-1976) pour fixer les bornes de ce que ne peut pas atteindre un certain type d'approche. Mais il est bien douteux que vous ayez l'indulgente bonté de me suivre pendant trente pages de raisonnement mathématique.

Cependant, ce sont ces énoncés faux ou ces assertions absurdes qui étayent le discours de la GST.

Donc je renonce ici à l'argument de la rigueur absolue et je me borne à affirmer répétitivement :

La litterature de la G.S.T. abonde en énoncés mathématiques faux, irrémédiablement faux

Du même coup, sans plus guère d'espoir de convaincre les Autorités Supérieures Administratives qui s'évertuent à diriger notre Recherche, j'affirme : (en m'appuyant très particulièrement sur Mesarovic)

La quasi totalité de ce qui n'est pas faux est inexorablement trivial

Pour les non-spécialistes l'argument de trivialité ne pèse pas, voire ne signifie rien, je le sais. J'espère donc n'offenser aucun de ceux qui ont appris les rudiments de l'algèbre universelle dans les oeuvres de mon ami Rapoport ou la topologie générale dans les travaux d'Arbib (qui ont d'ailleurs fait mieux en d'autres lieux) et un peu de théorie de la mesure grâce aux ensembles pileux.

./

Plus facile peut-être parce que moins technique serait de confronter le contenu des chapitres de la mathématique que l'on invoque avec ce que l'on leur fait dire. Sur deux d'entre eux, Berlinski se tait pudiquement et je les examinerai ici.

Permettez que je prenne d'abord la théorie de l'information de Shannon puisquelle est l'un des thèmes les plus inlassablement paraphrasés dans les publications de la G.S.T. Que contient-elle qui puisse se dire en mots sans employer de formules mathématiques :

"Si un émetteur produit des messages selon une loi de probabilité connue il est possible d'attacher à cette loi une certaine quantité de telle sorte que la correspondance entre l'émetteur et le récepteur (qui constitue la transmission) puisse selon cette mesure être réalisée de façon arbitrairement précise par complexification du codage quand on considère une transmission arbitrairement longue".

Exemple : en parlant au téléphone on parvient à se faire entendre en répétant chaque phrase autant de fois qu'il le faut.

L'exemple est ridicule car la beauté merveilleuse du Théorème de Shannon n'est pas dans cette platitude mais d'abord dans le fait que quand les lois de probabilité sont connues, la vitesse d'approximation à la transmission correcte est calculable. Ensuite, dans ce que cette expression formalise de façon essentielle la notion d'information transmisé dans les cas où un schéma probabiliste connu s'applique à l'émetteur. Surtout dans la preuve qui est si profonde que nous n'avons pas fini d'en exploiter les filons.

Mais l'exemple n'est pas que ridicule. Si les lois de probabilité sont inconnues, il n'y a pas de théorie de Shannon, Qu'importe alors que la soi-disant "quantité d'information" soit le logarithme du maximum d'une probabilité quand cette dernière n'existe pas, ce qui est évidemment toujours le cas en dehors de certains domaines techniques précis des Télécommunications ? A quoi bon imiter Lévi-Strauss ou McLuhan et faire doctement référence dans un contexte qui lui est étranger à une théorie qui par son essence même ne dit rien hors le cadre conceptuel précis dans leque- elle a été créée ?

(Remarque : j'ai oublié de préciser que pour abréger, j'appelle imposture toute référence au Théorème des Forces Vives dans un discours célébrant ou dénigrant l'énergie des Grands Chefs Militaires et Civils). Pourquoi par exemple ne pas parler de Fisher qui a introduit (en 1930) une autre mesure de l'information qui s'enseigne depuis dans tous les cours de statistique avancée ? Elle serait (peut-être !) parfois moins irrelevante, mais surement aussi moins prestigieuse.

Seconde farce, la théorie des automates que l'on trouve mentionnée si fréquement dans l'ouvrage de Klir déjà cité.

Tout d'abord mettons à part un opuscule tardif de von Neuman (qui est resté sans postérité intellectuelle) essayant de discuter le nombre minimum d'éléments d'une machine de Turing dans un système axiomatique un peu différent. Si je vous dis que ce minimum est 18 êtes vous plus éclairé ? Et votre vision du monde serait-elle changée si c'était plutôt 242 ? Ou 79 ? Vous sentez bien que tout est dans le choix des définitions.

Depuis, grâce au théorème de Kleen qui l'a fondée la théorie des automates s'occupe de tout autre chose : essentiellement d'étudier en profondeur la nature des calculs qui n'exigent pour être faits que des moyens si rudimentaires que c'est presque scandale que de les appeler calcul. Ainsi la théorie des automates n'a rien à dire (et ne dit rien) sur la multiplication des entiers (il y a là cependant des choses profondes, mais c'est une toute autre théorie, ignorée de la G.S.T. qui étudie les algorithmes utilisant la multiplication). Sujet misérable donc direz-vous. J'y consens. Mais ayant sa vertu, la rigueur. De fait, son impulsion originelle (Kleene) provient du désir de fixer de façon rigoureuse les limites d'une thèse avancée par Wo Mc.Culloch et Pitts et, comme vous le savez maintenant, ces limites sont très étroites : un système fini d'objets discrets, opérant en temps discret ne peut que très, très mal simuler tout autre chose que lui-même ; en particulier, un processus pourtant aussi élémentaire que la compilation (= analyse grammaticale) d'un programme d'ordinateur.

Et voici expliqué pourquoi on ne parle plus désormais de l'application du General Problem Solver de H. Simon à cette tache pourtant bien humble et bien utile.

Naturellement les automates ont aussi leurs illuminés dont le zèle finit par s'éteindre dans le moëlleux des chaires. On ne chante plus cette mesure de toute les complexités du monde qui était basée sur la déoomposition en groupe simple (combinés par produit en couronne) bien qu'elle fit florès il y a dix ans. N'est ce pas, Arbib ?

Mais le théorème de Rhodes survit au reflux de la mode. Il y avait une tentative d'imposture, mais dont le fondement n'était pas le vide absolu car nous étions dans le domaine des mathématiques.

De nouveau je demande pourquoi la G.S.T. fait tant référence à mon ami McNaughton dont le théorème (superbe) concerne exclusivement certains problèmes posés et résolubles dans un cadre délimité avec une rigueur si efficace que tout affaiblissement des hypothèses le réduit à néant ?

Peut-être par métaphore ? Voyons un peu. Qu'elle idée a suscité chez ceux d'entre vous qui ne connaîtraient point la théorie des automates, le terme charmant de produit en couronne ? Erreur, vous êtes sur une fausse piste. La seule allusion valable était aux sous-groupes de Sylow du groupe symétrique. Peut-être comprenez-vous mieux maintenant ce que j'entends par le mot imposture.

On pourrait continuer et vérifier que pour chacun des chapitres des mathématiques l'emploi fait par celui-ci en G.S.T. ne relève que de la rhétorique des commissions de budgets. Ceci bien sûr

pour les chapitres qui existent, puisqu'il faut préciser que rien en mathématiques n'est désigné par des noms ronflants tels que cybernétique ou théorie des hiérarchies. Et comme cet essai est une critique du livre de D. Berlinski, j'y fait référence pour des exemples hilarants que cet auteur fournit sans efforts à propos de la logique, de la théorie de la stabilité, de l'algèbre linéaire, etc., etc.

./

4 - Conclusions provisoires

Tristes. (Que de jeunes talents ou pire d'enthousiasmes dans les Instituts de Recherches ...). A chaque ligne, je me suis retenu de citer un ami ou un autre dont je partage les espoirs de voir un jour la mathématique informer de nouveaux domaines et contribuer selon son mode propre à les mettre aux services des hommes. L'auteur du livre que nous commentons ici mérite qu'on le respecte.

Mais la connaissance ne se nourrit pas de la fumée des bonnes intentions et l'affirmation judicieuse que le tout contient les parties ne mérite de place à ses auteurs qu'au Panthéon de la Sagesse des Nations dont la clef fût en Chine. Bref, il faut tenter d'établir un bilan provisoire des faits ou théorèmes que nous devons à la G.S.T. Et on ne prendra pas en compte la diffusion (fût-elle crue utile) dans le vocabulàire des billets de Paris de termes courants dans les laboratoires (feed-back, optimisation, homéostat, decision process, etc., etc.).

Pas plus que l'habitude touchante (et bien commode dans la pédagogie audiovisuelle) d'orner toute conférence de trois ou quatre boites noires se poursuivant au tableau de même couleur.

En psychologie ou en sociologie, je n'ai rien sû voir dans les ouvrages que j'ai consultés : pris jusqu'au vertige de ce qui fût une mode en mathématique, les systémistes préfèrent la théorie à l'observation et la généralité à la preuve. Il y a plus de cinquante ans le Colonel Rimaillot notait qu'un homme ne peut guère en commander directement que quatre et discutait sous cet angle diverses structures sociales. La G.S.T. théorise les hiérarchies et les inter-relations mais je n'y trouve rien qui enrichisse ou précise ces premiers pas d'une science de l'organisation des micro-sociétés. En psychologie, la Gestalt Theorie avait été vite éteinte dans les laboratoires. La G.S.T. reprend le flambeau, mais hormi quelques études bien molles sur la psychologie des joueurs d'échecs, elle a élaboré des "modèles cognitifs" et des "paradigmes heuristiques" à l'aide de catégories ou de fonction non récursives, sans que les psychologues que nous fûmes y trouvent grand chose à ajouter à ce qui s'enseignait déjà il y a cinquante ans (qui eussent sans doute ailleurs trouvé la joie de la recherche ...)

./

En biologie, la cybernétique a fait faillite sans avoir même commencé. Les manuels tchèques ou italiens ressassent toujours les mêmes expériences douteuses qui faisaient la joie du MIT dans les années cinquante et que l'on sait depuis avoir été encore plus mal interprétées que faites.

Peut-être, j'espère, je me trompe, et on saura me montrer toutes les découvertes admirables que j'ignore ou méconnais dans les sciences de l'homme ou dans celles de la vie. Peut-être aussi suis-je injuste et peut-être que les mathématiques de la psychanalyse Lacaniennes procèdent directement de la G.S.T.; certes et j'y joins, en couronne, celles du structuralisme parisien et de la sémiotique générale.

Mais je le répète, ceci paraît peu vraisemblable et la lecture des publications les plus récentes de la G S T ne semble pas indiquer quelle ait accumulé quoique ce soit dans le domaine des connaissances empiriques car il n'y est jamais question que des mêmes fadaises péri ou para-mathématiques sous-tendues ou non par de pieuses vaticinations écologiques ou ilytchiennes. Des idées, des projets, des formules, mais point de fait.

Et nous voici revenu au même pôle. Il faut juger la G.S.T. comme une philosophie ou une discipline mathématique. Une ou des philosophies ? car il est bien difficile de tirer au clair qui l'exprime : Laszlo, Simon, Mesarovic, Bertalanffy ? car pour l'essentiel ils s'ignorent les uns les autres et prêchent chacun pour son église sans discuter ni utiliser ce que dit son collègue ?

De toute façon, il est vain de prétendre juger un philosophe et je ne m'y aventurerai donc pas. Reste la mathématique. Je la tiens pour fausse ou triviale. De toute façon irrelevante aux buts déclarés. (... pour le confort des programmes furent envoyés labourer la glace ...).

De nouveau j'espère que je me trompe et je supplie, que l'on me sorte du cauchemard dantesque de ce vol de chercheurs cantando lor lei et alignant depuis vingt ans un tourbillon de calculs imbéciles. Nous attendons donc avec impatience le rapport final que publieront les responsables du CNRS sur les résultats de l'Action Thématique en G.S.T. qu'ils animent, (... et ne reviendront que meurtris). Et pour prendre patience relisons Berlinski. (On system Analysis ; MIT Press 1976).

*cahiers*
**FUNDAMENTA SCIENTIAE**

SEMINAIRE SUR LES FONDEMENTS DES SCIENCES

N° 92

**PROBLEMES LINGUISTIQUE ET SEMIOLOGIQUES**

L'ANALYSE SEMIOLOGIQUE

*Jeanne MARTINET*

MATHEMATIQUES ET LINGUISTIQUE

*M.P. SCHUTZENBERGER*

* *

*

1979

**UNIVERSITE LOUIS PASTEUR**

**STRASBOURG**

# MATHEMATIQUES ET LINGUISTIQUE

par

M.P. Schutzenberger *

* Monsieur M.P. SCHUTZENBERGER
Département de mathématiques
Université Paris VII
2 place Jussieu
75230 PARIS CEDEX 05

Quel titre imposant ai-je accepté dans un mouvement d'enthousiasme, pour les quelques remarques précaires que je suis seulement capable de soumettre à votre discussion ! Et d'ailleurs, que pourrais-je faire d'autre puisque pour traiter le sujet il faudrait être un mathématicien linguiste, si une telle créature peut exister, ou du moins un mathématicien et un linguiste ce qui n'est doublement pas mon cas.

Permettez que nous procédions d'abord à une série de négations visant à exclure ce dont on ne pourrait parler avec profit dans le temps d'une conférence, d'autant qu'il faudra bien raconter la Belle Histoire des langages context-free de Chomsky pour qu'une partie de l'audience ne soit pas trop frustrée dans ses pieuses attentes.

Tout d'abord, statistique et linguistique : je ne crois pas être le seul ici à croire que la statistique est l'une des plus belles applications du Calcul des Probabilités et que ce dernier lui-même est un admirable chapitre de la Physique traitant d'un certain phénomène physique (je répète), à savoir le hasard. Par conséquent, la statistique a une place prééminente partout où l'observation est rendue difficile par des facteurs parasites aléatoires, impossibles à contrôler. Elle a dominé la génétique et joue un rôle grandissant en astronomie. Il ne me semble n'y avoir aucun doute sur sa valeur dans toutes les branches de la linguistique, de la phonétique à la philologie, et sur le fait que nous sommes encore très très loin d'avoir essayé de l'employer partout où cela semble raisonnablement prometteur, comme par exemple en grammaire.

Rappelons pour mémoire quelle dette a contracté le Calcul des Probabilités vis-à-vis des sciences du langage et de la communication. Nous leur devons aussi bien les chaînes de Markov que le théorème du codage de Shannon, donc pour les plus élégants, la classification des shifts bernouilliens. Ici encore, nous proposons que le sujet mérite un séminaire et nous en tirons la conclusion qui s'impose.

A l'autre extrême s'étendent la logique élémentaire et les notations de la théorie des ensembles qui ont donné prétexte à de nombreux ouvrages dont les titres alléchants ont fourvoyé plus d'un étudiant. Précédées ou non d'un cours de probabilités du niveau du brevet de gymnastique, on y voit de longues chaînes de théorèmes aboutissant au résultat majeur que l'ensemble des mots de douze lettres qui commencent par un k est l'intersection de celui des mots dont douze est la cardinalité du nombre des lettres par le complément de celui des mots qui commencent par une autre lettre que k. J'ai, bien sûr, modifié l'exemple auquel je pense pour n'offenser personne, mais quiconque a fréquenté les mathématiques des sciences humaines aura la tentation d'en soumettre de plus drôles. Passons vite, non sans regretter pour les forêts scandinaves que Hjemslev n'aît pas connu Boole. Et souscrivons à l'opinion du prochain conférencier que les "math. modernes" présentent quelques mérites pour ce qui est de l'enrichissement du vocabulaire des marmots. Autre sujet de séminaire !

Nous avons du même coup annoncé que nous ne parlerions que des modèles de langage : mise à part la phonétique pure qui emploie avec succès l'acoustique, refermé les brèves parenthèses de la glottochronologie de Swadesh et du calcul de Lambek et annoncé avec déférence la Théorie sémantique et grammaticale de Thom, l'élaboration de ces modèles est, à ma connaissance, la seule branche de la linguistique où interviennent des mathématiques autres que la théorie statistique ou le vocabulaire des ensembles, ou enfin, mais ceci ne nous concerne pas ici, la logique mathématique.

Excusez-moi d'avoir été aussi expéditif mais je préfère consacrer le temps à plus de réflexion préliminaire sur ce que signifie le fait même d'appliquer les mathématiques à une discipline, comme on disait autrefois ou des mathématiser celle-ci comme on le dit plus volontiers aujourd'hui. Pour aborder ce point il est commode de s'interroger en toute généralité sur les principes qui peuvent permettre de juger que la mathématisation (totale ou partielle)d'une discipline a été ou non réussie. C'est une question qui ne rencontre guère d'échos chez les mathématiciens bien que les plus sages semblent avoir pour critère le nombre des postes d'enseignants et de chercheurs qu'elle permet de faire créer.

De fait le succès prodigieux (succès "au delà de toute raison" dit Wigner) de la mathématisation de la physique ne laisse place chez la plupart des mathématiciens à aucun doute sur la validité ni même la possibilité de l'extension de cette réussite à toutes les autres disciplines. Il est cependant nécessaire de serrer la question de plus près quand ce ne serait que pour marquer les progrès accomplis et dans ce but je propose (sans originalité) que les deux objectifs majeurs sont l'explication la prévision. J'entends par là que la théorie mathématique d'un phénomène peut réaliser (et souvent simultanément) deux buts : donner à ceux qui la connaissent le sentiment d'avoir mieux compris ce phénomène, c'est l'explication – et de sa valeur, seuls peuvent être juges ceux qui éprouvent ce sentiment d'intime illumination–; ou bien, prévoir des conséquences observables, non triviales, qualitatives ou quantitatives.

La physique newtonienne atteint indiscutablement ces deux buts (et aussi un autre bien plus fondamental concernant l'activité de définition qui exigerait à elle seule une longue discussion). Il en est de même,de façon bien plus modeste,de la mécanique de l'hérédité mendélienne. Par contre la génétique des populations peut-être considérée comme purement explicative (avec sans doute quelque exagération dans un sens qu'il est inutile de préciser). Le moindre modèle doit recéler tant de paramètres et chaque observation est tellement perturbée par des facteurs transients ou séculaires que l'accord entre les chiffres (ou les faits) calculés et observés ne peut qu'être la conclusion d'une étude particulière sans permettre de prédiction pour un autre cas. Par contraste, la physique possède en plus de ses théories générales une foule de lois semi-empiriques qui n'expliquent, ni ne prétendent expliquer, rien mais qui conduisent à des prédictions précises et efficaces.

Peut-être pourrait-on soumettre toute mathématisation à l'épreuve suivante inspirée par la méthode de falsification de Popper. Utilise-t-elle un théorème dont les observations permettraient de conjecturer sérieusement la vérité si il se trouvait que la preuve mathématique en fût encore inconnue ?

Un très bel exemple est celui du théorème de Poisson sur l'annulation du potentiel à l'intérieur d'une sphère chargée. Un autre me semble être celui du théorème de Nash (sur la convergence vers le point-selle) qui pourrait être vérifié expérimentalement en faisant disputer des milliers de parties à des joueurs professionnels. Naturellement, il s'agit ici d'une expérience rêvée mais dont le caractère utopique n'a rien à voir avec l'essence du processus étudié.

Un contre-exemple intéressant est l'équation différentielle de Volterra (sur les oscillations des systèmes de populations) qui a fait la joie de tant d'enseignants du PCB à court d'exemples biologiques. Elle ne paraît pas pouvoir passer avec succès notre épreuve.

La question mathématique étant de savoir si les solutions de tel type d'équation différentielle possèdent ou non tel caractère oscillatoire, aucune observation de population ne peut y apporter de réponse. En effet il faut toute la fraîcheur d'âme d'un mathématicien pour croire que le modèle particulier proposé a un rapport plus singulier avec les processus effectifs que mille autres possibles qui en seraient radicalement différents du point de vue mathématique, et, par conséquent, l'observation dans la nature d'oscillations plus ou moins analogues ne dit rien sur l'équation en cause (sinon qu'elle n'est pas trop grossièrement contredite par les faits).

Autrement dit la dynamique des populations offre une illustration du comportement d'un être mathématique et il semble bien vraisemblable que c'est ainsi que l'avait vue l'illustre géomètre. Dans le même ordre d'idée je rappelle à votre attention l'immense littérature médiévale sur les nombres parfaits et le caractère si contemporain de ce mode de discours.

Je suis sûr que nos collègues qui pratiquent l'économie mathématique pourraient singulièrement enrichir de beaux exemples toute cette discussion et après ces préliminaires (trop longs, trop sommaires et trop partiaux) nous en venons à la question impliquée par le titre de la conférence : Existe-t-il des théorèmes conduisant à prévoir des phénomènes linguistiques de façon non triviale ?

J'avance que la réponse est positive et voici pourquoi. Comme on sait, la mode était il y a vingt ans de considérer que pour l'essentiel les phénomènes langagiers étaient de nature markoviens, les états de la chaîne étant les dernières syllabes ou mots prononcés et la matrice de transition étant par définition la langue considérée. Modèle excellent pour les fins qui l'avaient suggéré (la transmission du signal) mais peut être un peu sommaire pour le reste. Comme la théorie des chaînes de Markov à une infinité d'états était aussi fort à la mode, le remède du passage à la limite (par augmentation du nombre des états) était sous la main, et dans les Collèges les plus illustres on entendit déjà quelques années plus tard promettre des explications savantes du langage fondées sur cette approche.

Au tournant de cette époque était apparue une autre théorie. Abandonnant toute tentative de production séquentielle de la chaîne du discours, N. Chomsky proposait d'engendrer l'ensemble des phrases grammaticalement acceptables par un algorithme différent reposant sur des substitutions itérées. La chose est trop connue pour que nous nous attardions à plus de détails.

Pour un raisonnement mathématique il en déduisait plusieurs conséquences. La première est que si son modèle était correct toute tentative d'approximer les phrases grammaticalement acceptables par un système markovien devait buter irrémédiablement sur l'obstacle d'une croissance trop rapide (de type exponentiel) du nombre des états requis avec la longueur des phrases à analyser. Une seconde (à vrai dire plutôt indiquée qu'imposée par le modèle) était l'abondance d'ambiguïtés <u>inhérentes</u> dans l'analyse grammaticale.

L'une et l'autre ont été amplement confirmées par les expériences qui de Leningrad à Washington ont consacré des dizaines de millions à vérifier l'impossibilité de la traduction automatique. Pour les besoins de cet exposé je préfère les considérer comme une possibilité de "vérifier empiriquement" un théorème trop technique pour être énoncé ici et dont on doit la substance à Kleene et à Chomsky.

Une troisième conséquence observable et mathématiquement dérivable du modèle de Chomsky concerne la géométrie des relations de dépendance grammaticale : à un certain niveau d'approximation elles sont représentables par des graphes <u>planaires</u>. Phénomène remarquable que Tesnières avait vu il y a une quarantaine d'années dans des travaux anticipant ce qui se fait aujourd'hui. De nouveau, je vous invite à voir dans le fait que quasiment toutes les langues naturelles examinées présentent ce caractère de planarité, une confirmation empirique de la preuve d'un énoncé mathématique non trivial.

Tout ceci date d'il y a vingt ans. Depuis, la théorie mathématique de ce que l'on appelle maintenant les "langages" (=parties d'un monoïde libre) "algébriques" (= solutions formelles d'équations polynomiales en variables non commutatives) s'est épanouie et la brillante école que M. Nivat a réussi à former autour de lui est connue pour tenir le premier rang parmi les nombreux chercheurs qui cultivent ce sujet dans le monde.

Un facteur essentiel de ce développement est que la structure générative proposée par Chomsky comme modèle de grammaticalité pour les langues naturelles est à peu près parfaitement réalisée dans les langages de programmation tels que le Fortran ou l'Algol. Les questions mathématiques que posent les "langages" algébriques sont donc liées de façon très intime aux problèmes dits "de compilation". De plus, une technique informatique importante en analyse non numérique (la "gestion de pile") se trouve être en correspondance avec l'un des algorithmes de base de la théorie algébrique. Le livre de J. Berstel (sous presse chez Teubner) fait à merveille le point des résultats acquis.

Sur un autre versant les rapports entretenus avec les mathématiques les plus classiques sont assez profonds. Par exemple c'est avec joie que nous avons vu R. Lyndon (qui ne s'est jamais, je crois, soucié des langages algébriques) faire intervenir avec succès des considérations de planarité (cf. plus haut) dans la théorie dite combinatoire des groupes libres (par exemple dans la preuve du lemme de Greendlinger). Ici encore je dois me borner à être abusivement allusif en jalonnant des noms de Lentin, Tutte et Cori les très larges routes qui relient ces résultats.

Nous ne sommes pas tout à fait sorti du sujet puisqu'il s'agissait de langages pour communiquer avec les ordinateurs mais il vaut mieux revenir à la linguistique stricto sensu, et la deuxième question qui me paraît se poser maintenant est celle de la continuation de contacts non triviaux entre celle-ci et ses modèles mathématiques.

Autrement dit, mises à part les applications du calcul des probabilités et de la statistique, existe-t-il une discipline que l'on puisse sérieusement appeler linguistique mathématique ?

Bien sûr, je ne parle pas d'un enseignement portant ce nom puisque tout ce que j'ai déjà exposé (et quelques autres sujets non négligeables que j'ai laissés dans l'ombre) justifient amplement l'existence d'une propédeutique à contenu mathématique (et informatique) contribuant à la formation de linguistes.

Bien sûr aussi, je ne parle pas de ce qui peut ou pourrait être demain. Très concrètement je parle de recherches actuelles actives et sérieuses dans lesquelles la solution d'un problème mathématique donnerait la réponse à une question linguistique, ou en poserait une nouvelle, comme cela se passe quotidiennement en physique.

La réponse me paraît (aujourd'hui) être non et ceci pour la base de deux faits. Le premier est le développement de l'Ecole de Chomsky. Ainsi que j'ai essayé de le montrer plus haut les premiers résultats mathématiques de cet auteur avaient une signification linguistique certaine et immédiate.

Depuis, malgré une audience mondiale, des imitateurs nombreux et l'atmosphère vigoureusement pro-mathématique et interdisciplinaire de l'époque, et spécialement de M.I.T., rien de nouveau ne semble devoir être ajouté à ce qui se trouve déjà dans les chapitres qu'il avait écrit en 1963 avec G. Miller dans le Manuel de Psychologie Mathématique. Les travaux de l'école chomskienne ont porté sur l'usage du modèle génératif dans la discussion subtile de phénomène langagiers.

Pour ce qui est des techniques mathématiques employées, les arbres de Tesnière y suffiraient largement. D'ailleurs, développant une autre méthode proposée par Zellig Harris, ce modèle trop étroit a vite été remplacé par un modèle transformationnel dont les propriétés mathématiques sont nulles. Ceci ne signifie évidemment pas qu'il soit vide ou inintéressant mais simplement qu'il ne possède pas une structure abstraite assez précise et assez riche pour bénéficier de raisonnements mathématiques excédant ceux des "Math. Modernes". D'autres recherches de la même école se sont constamment appuyées sur la logique mathématique, mais ceci n'est en rien le propre de la linguistique puisqu'une interaction de cette nature est un trait général de la philosophie anglo-saxonne. A titre de confirmation, je vous renvoie aux ouvrages les plus récents des exposants autorisés français de la linguistique générative et transformationnelle, et je précise qu'il en est de même en ce qui concerne les écoles dissidentes (schismatiques ou hérétiques).

Tel me paraît être le constat relatif au courant le plus porté à la mathématisation et un deuxième ordre de faits me conduit à croire que ceci a des causes internes propres au langage lui-même.

Je veux parler ici des travaux de mon ami M. Gross. Parti il y a quinze ans du désir d'appliquer les méthodes dont nous venons de parler il a inventorié exhaustivement les phénomènes qu'il voulait étudier. Principe habituel dans les sciences de la nature mais idée extrêmement neuve et féconde dans une discipline où (comme dans bien d'autres!) le raisonnement coutumier procède par voie d'exemples et contre-exemples sans le moindre souci de leur extensionnalité. Or, à sa surprise, les faits rassemblés sont apparus très différents de ceux qu'aurait prescrit la théorie initiale : utilisant les mêmes critères ou des critères analogues à ceux employés dans la casuistique des exemples, les huit mille verbes de français se révèlent à peu près tous être chacun unique quand aux propriétés grammaticales. Sautant à la conclusion, nous retrouvons à un autre niveau la même contradiction qui avait conduit à écarter les modèles markoviens. Même à un niveau d'approximation sommaire, la réalité linguistique se révèle trop complexe pour être utilement modélisée par les grammaires génératives ou transformationnelles. L'étude fine des propriétés mathématiques ou logiques de ces dernières est donc aussi inadéquate au but poursuivi que le serait la théorie de l'approximation des nombres algébriques de Baker à la théorie des gaz nonobstant la loi de Mariotte et la définition des logarithmes.

Depuis, l'école de M. Gross a retrouvé dans d'autres langues que le français, les mêmes phénomènes et l'on sait que cette richesse de complexité s'est traduite par un renouvellement de la problématique et la solution de nombreuses questions linguistiques selon des méthodes originales qui (malheureusement dira-t-on) n'ont rien de mathématique.

Résultat inattendu ? peut-être moins, si l'on avait mieux compris les indications de Zellig Harris (dont et Chomsky et Gross sont les élèves). En tous cas je tire de ces deux ordres de faits la conclusion que pour ce qui est du passé et du présent, la linguistique et les mathématiques ont eu un point de tangence - peut être même d'osculation. Je ne sais ce que réserve le futur.

Veuillez ne voir dans ces propos, ni pessimisme ni regret. L'osculation (comme toute la géométrie différentielle) est une très belle chose et de voir les recherches linguistiques lancées dans une direction nouvelle ne peut que susciter l'enthousiasme.

Les mathématiciens non plus ne doivent pas pleurer. Si leur but est,comme il se doit,de faire progresser la connaissance des objets mathématiques (et non d'enrichir ou de raffiner une nouvelle rhétorique) ils ont acquis toute une série d'intuitions nouvelles sur des objets classiques et quelques objets nouveaux qui ne semblent pas déraisonnables. Vous pourrez juger sur pièces quand sera paru le volume C du traité de Eilenberg,si les travaux publiés jusqu'ici vous semblent n'avoir pas encore atteint ce niveau de perfection abstraite qu'exigent les canons de l'époque.

*

* *

# Année 1980

## Bibliographie


[1980-1] Dominique Foata et Marcel-Paul Schützenberger. H. O. Foulkes (1907–1977). *Discrete Math.*, 30(1) :1 (1 plate), 1980.

[1980-2] Marcel-Paul Schützenberger. Sur les sous-groupes de rang fini d'un groupe libre. *C. R. Acad. Sci. Paris Sér. A-B*, 290(5) :A207–A208, 1980.

[1980-3] Alain Lascoux et Marcel-Paul Schützenberger. A new statistics on words. *Ann. Discrete Math.*, 6 :251–255, 1980. Combinatorial mathematics, optimal designs and their applications (Proc. Sympos. Combin. Math. and Optimal Design, Colorado State Univ., Fort Collins, Colo., 1978).

[1980-4] Maurice Gross et Marcel-Paul Schützenberger. On prétend que .... In Lemoine et Gallouedec-Genuys, editors, *Les enjeux culturel de l'information*, volume 9 of *Informatisation et société*, pages 127–128. La Documentation Française, 1980.

[1980-5] Maurice Gross et Marcel-Paul Schützenberger. Compléments sur le traitement automatique des langues naturelles. In Lemoine et Gallouedec-Genuys, editors, *Les enjeux culturel de l'information*, volume 9 of *Informatisation et société*, pages 135–142. La Documentation Française, 1980.

[1980-6] Marcel-Paul Schützenberger. Sur l'analyse des systèmes. In Lemoine et Gallouedec-Genuys, editors, *Les enjeux culturel de l'information*, volume 9 of *Informatisation et société*, pages 205–215. La Documentation Française, 1980.

Discrete Mathematics 30 (1980) 1
© North-Holland Publishing Company

## H.O. FOULKES (1907–1977)

The present issue of Discrete Mathematics is devoted to the publication of the last paper ever written by the late Professor Foulkes. The editors of the Journal, were kind enough to respond very favorably to our suggestion of having a special issue dedicated to his memory.

During the last five years of his life Professor Foulkes had written several papers on the relations between Enumeration and Symmetric Group Representation (essentially, Foulkes [9–13] as they are referred to in the subsequent bibliography and, of course, the following paper itself). Until the very end "his mind was teeming with new ideas" so that on several occasions he told his devoted wife, Mrs. Beryl Foulkes, that "his head was sprouting with fascinating ideas, which isn't fair on an old man". It is unfortunate that we shall miss those ideas of his for ever. At least, he could find the time to complete the paper "Eulerian numbers, Newcomb's problem and representations of the symmetric groups", we are now very pleased and honored to present to the mathematical community.

On the occasion of the Table Ronde on Combinatorics and Representation of the Symmetric Group held in Strasbourg in 1976 we had the privilege of hearing him talk on the essential parts of this paper. Everybody was impressed and charmed by the clarity of his lecture. One of the problems he mentioned on a surprising refinement of the Eulerian Numbers was elegantly solved by the young E. Gansner [14].

Combinatorial properties on Classical Numbers, such as Eulerian, Euler, Tangent, Genocchi Numbers have recently been discovered. Professor Foulkes quickly realized that those properties could also be reinterpreted in the classical set-up of Symmetric Functions (Littlewood–Richardson Coefficients, Kostka Numbers, Irreducible Characters of the Symmetric Group). The present paper belongs to this vein. There is an unexpected connection between Eulerian Numbers and Symmetric Function coefficients, that gives rise to numerous identities involving the two families of numbers. Several numerical tables are also included in the paper.

A detailed obituary of Professor Foulkes has recently appeared (Bull. London Math. Soc. 11 (1979) 208–214). It provides a very interesting account of his career and mathematical work.

D. Foata and M.-P. Schützenberger

C. R. Acad. Sc. Paris, t. 290 (4 février 1980) Série A — 207

THÉORIE DES GROUPES. — *Sur les sous-groupes de rang fini d'un groupe libre*. Note (*) de **Marcel Paul Schützenberger,** Correspondant de l'Académie.

On indique des bornes ne dépendant que de $r$ pour le degré de certains groupes de permutations finis associés à un groupe donné H de rang fini $r$ d'un groupe libre.

*It is announced that certain groups associated with a subgroup of finite rank r of a free group have rank one when their degree exceeds* $3r-1$.

Soient F un groupe libre et H un sous-groupe donné de F de rang fini $r$; il est plus commode de supposer d'emblée $r \geqq 2$ et que H n'est pas d'indice fini. On appelle ici *groupe annexe* [de la paire (H, F)] tout sous-groupe G de F qui est le stabilisateur (relativement à l'action à droite de F) d'un ensemble noté $HF_1$, d'un nombre *fini d* de classes latérales de H telles que $HfG$ contienne une infinité de classes quand $f$ est un élément de F qui n'est pas dans $HF_1$; le *degré* de G est $d$ et on note [G] le groupe de permutations de même degré induit par la restriction de l'action de G aux classes latérales dans $HF_1$.

Si H était d'indice fini, le seul groupe annexe serait F et $d$ serait donné par la formule de Schreier ([1], p. 16); si H avait rang 1, tout groupe annexe serait conjugué du plus grand sous-groupe de rang 1 contenant H. Dans le cas général, le théorème de Nielsen ([1], prop. 2.3, p. 7) montre facilement que le degré des groupes annexes est borné par le double de la somme $m$ des longueurs des mots de base de H et qu'ils se répartissent en moins de $4^m$ classes de conjugaison. On en déduit que l'union des groupes annexes contient tous les éléments de F ayant une puissance positive finie dans H et, de même, que chaque intersection infinie de H avec un de ses conjugués $fHf^{-1}$ ($f \notin H$) est incluse dans un groupe annexe différent de H; enfin le nombre maximal de classes de H-conjugaisons d'éléments de H que peut contenir une classe de conjugaison de F est borné à la fois par le degré des groupes annexes de rang $\geqq 2$ et par le degré d'intransitivité (c'est-à-dire le nombre de classes de transitivité) des groupes quotients [G] où G est un groupe annexe de rang 1. Dans la direction opposée tous les groupes annexes sont conjugués de H (ou, de façon équivalente, ont degré 1) si et seulement si toutes les intersections de H avec ses conjugués sont triviales.

Supposons choisie une base $A_+$ de F; la méthode des transversales de Schreier formulée en termes d'automates ([2] ou [3]) permet de trouver une relation rationnelle fonctionnelle multiplicative de F sur un semi-groupe fini (Q, S) d'applications partielles dans lui-même d'un ensemble Q ayant au plus $2m$ éléments qui a les propriétés suivantes :

(1) $\alpha$ est compatible avec l'anti-isomorphisme naturel induit par l'inversion $f \to f^{-1}$ de F;

(2) $\alpha$ induit une bijection entre les classes de conjugaison de groupes annexes et les classes de conjugaison (de semi-groupe avec anti-isomorphismes) de groupes maximaux dans (Q, S);

(3) cette bijection établit des isomorphismes de groupes de permutations entre les groupes quotients [G] et les dits groupes maximaux dans (Q, S).

Le semi-groupe (Q, S) joue donc ici un rôle analogue à celui joué par le groupe quotient [F] dans le cas où H est d'indice fini.

La relation $\alpha$ associe aux classes de conjugaisons des groupes annexes de rang 1, certains idéaux principaux idempotents maximaux particuliers de S.

Ces observations sont l'application directe des techniques de construction du semi-groupe syntaxique d'une partie rationnelle d'un monoïde libre ([2], [3]), qui est ici l'ensemble K des mots réduits représentant les éléments de H dans le monoïde libre $(A_+ \cup \overline{A}_+)^*$ dont F est le quotient (*cf.* [4]). Elles impliquent, grâce à un théorème d'Anissimov et Seifert que tous les groupes annexes sont de rang fini ([5], p. 58).

On choisit maintenant une base de Nielsen de H. Une autre technique usuelle combinée avec un corollaire assez pesant du théorème de Nielsen montre que K est l'image par un morphisme (de monoïde libre) d'une partie *locale* ([2], [3]) d'un autre monoïde libre de rang $\leqq 2(3r-2)$. Faisant appel à des résultats plus spéciaux, c'est-à-dire essentiellement aux théorèmes d'indice critique pour les mots périodiques ([6], [7]), on peut obtenir quelques précisions supplémentaires qui constituent l'énoncé principal de ce travail.

Proposition. — *Tous les groupes annexes ont un degré d'intransitivité au plus égal à* $3r-1$ *et le nombre de leurs classes de conjugaison est inférieur à* $O(3^{3r})$; *ceux dont le degré est* $\geqq 3r-1$ *sont de rang* 1 *et le nombre de leurs classes est au plus* $r$.

Ces valeurs numériques sont assurément ridicules et il semble que l'on puisse toujours trouver $r$ sous-groupes de rang 1 de F tels que, d'une part chaque groupe annexe de degré $\geqq r$ (peut être même $\geqq r-1$) soit conjugué de l'un d'eux, et que d'autre part, leur union contienne une base de H.

On peut aussi borner en fonction du seul rang $r$ la longueur de certaines sous-chaînes spéciales d'idéaux principaux dans le semi-groupe fini S.

De nouveaux les preuves ne sont pas difficiles mais la lourdeur des notations requises pour passer des groupes libres aux monoïdes (libres ou finis) et pour relier ceux-ci aux propriétés plus géométriques des mots, empêche que l'on soit plus explicite; les détails sont donnés dans les actes du *Convegno d'Analisi Globale* (Florence, octobre 1979).

(*) Remise le 4 février 1980.

[1] R. C. Lyndon et P. E. Schupp, *Combinatorial Group Theory*, Springer, 1977.
[2] S. Eilenberg, *Automata, formal Languages and Machines*, Academic Press, 1976.
[3] G. Lallement, *Semigroups and Combinatorial Applications*, Wiley, 1979.
[4] M. Benois, *Comptes rendus*, 269, série A, 1969, p. 1188.
[5] J. Berstel, *Transductions and Context-Free Languages*, Teubner, 1979.
[6] Y. Cesari et M. Vincent, *Comptes rendus*, 286, série A, 1978, p. 1175.
[7] J. P. Duval, *Comptes rendus*, 289, série A, 1979, p. 185.

*Laboratoire d'Informatique*, Tour 55-56, 2, *place Jussieu*, 75230 *Paris Cedex* 05.

Annals of Discrete Mathematics 6 (1980) 251–255
© North-Holland Publishing Company

# A NEW STATISTICS ON WORDS

A. LASCOUX and M.P. SCHÜTZENBERGER

*Départment de Mathématiques, Paris VII, Tour 55, 2 Place Jussieu, 75005 Paris (France)*

The study of various statistics on words is a chapter of combinatorics and it has been recently surveyed by Foata [1]. One ot these statistics is the so-called "Major Index" of a word. It plays a role in the theory of representations of the symmetric group. We present here a generalization, the "load", which we used to prove Foulkes' conjecture, i.e. to supply a $q$-analogue of Kostka numbers [2].

It turns out that the load can be defined in terms of a minimization problem. We develop this approach here without entering into the algebraïc background or applications. A special feature of the problem is that a solution is given by the most simple minded algorithm, a not too frequent occurrence. Therefore, we suspect that it is a very degenerate special case of a more general question already encountered in operations research. Since we have not been able to trace it in the literature, we apologize to those authors, whose articles may have been unwillingly overlooked.

## 1. The minimization problem

Throughout this paper consider two finite totally ordered alphabets,

$$A=\{a<b<c<\cdots\} \quad \text{and} \quad \Gamma=\{\alpha<\beta<\cdots\}.$$

As usual the number of occurrences of a letter $x$ in a word $w$ is denoted by $|w|_x$, and one says that a word is *standard* iff no letter occurs more than once in it.

We also consider a fixed word $v$ in the free monoid $A^*$, and we make the basic assumption that its multidegree is non-increasing, i.e. that $|v|_a \geq |v|_b \geq \cdots$.

A *lifting* of $v$ is a standard word $w$ in the free monoid $(A\times\Gamma)^*$ such that, on the one hand, $v$ is its projection on $A^*$ and, on the other hand, its minimal alphabet, $B$, is an initial interval of $A\times\Gamma$, i.e. $c\gamma\in B$ only if $c'\gamma'\in B$ for any $c'\leq c$ and $\gamma'\leq\gamma$. Our basic assumption on the multidegree of $v$ insures that $v$ has at least one lifting (and, in fact it has only one iff $v$ is standard). Note that $B$ is the union over all greek letters $\gamma$ of sets $A_\gamma\times\{\gamma\}$ where $A_\gamma$ is an initial intervalle of $A$.

Let $w$ be a lifting of $v$. For each $c\gamma\in B$ we say that the letter $c\gamma$ is *marked* iff it is on the *right* of the letter $c_-\gamma$ where $c_-$ denotes the (immediate) predecessor of $c$

in $A$. Thus, $a$ being always the first letter of $A$, we have that no letter $a\gamma$ is marked. We deduce by two summations the *delay function* $\mu = \mu_w$ and the *integrated delay function* $\bar{\mu}$ of the lifting $w$. The first one has domain $B$ and $(c\gamma)\mu$ is defined as the number of marked $c'\gamma$ with $c' \leqslant c$. The second one has domain $A \times \Gamma$ and $(c\gamma)\bar{\mu}$ is the sum of $(c'\gamma')\mu$ over all $c' \leqslant c$ and $\gamma' \leqslant \gamma$.

The problem is to choose a lifting so as to minimise the maximum of the integrated delay function, i.e. the sum of the values of the delay function itself. This minimax quantity is the *load* of the word $v$.

**Example.** Let $v = a\,b\,d\,a\,b\,c\,b\,a\,c\,d$, of length $|v| = 10$. The partition of 10 expressing the multidegree is $K = (2\,2\,3\,3)$. One of the $2!\,2!\,3!\,3!$ possible liftings is:

$$a\gamma,\ b\beta,\ d\alpha,\ a\alpha,\ \underline{b}\gamma,\ c\alpha,\ a\beta,\ b\alpha,\ \underline{c}\beta,\ \underline{d}\beta.$$

Marked letters are underlined. The delay and integrated delay functions are:

$$\begin{array}{c|ccc} d & 1 & 2 & \\ c & 1 & 1 & \\ b & 1 & 0 & 1 \\ a & 0 & 0 & 0 \\ \hline & \alpha & \beta & \gamma \end{array} \qquad \begin{array}{c|ccc} d & 3 & 6 & 7 \\ c & 2 & 3 & 4 \\ b & 1 & 1 & 2 \\ a & 0 & 0 & 0 \\ \hline & \alpha & \beta & \gamma \end{array}$$

The natural lifting (discussed below) and corresponding functions are:

$$a\gamma,\ b\beta,\ d\alpha,\ a\beta,\ b\alpha,\ \underline{c\beta},\ a\alpha,\ \underline{b\gamma},\ \underline{c\alpha},\ \underline{d\beta}.$$

$$\begin{array}{c|ccc} d & 1 & 2 & \\ c & 1 & 1 & \\ b & 0 & 0 & 1 \\ a & 0 & 0 & 0 \\ \hline & \alpha & \beta & \gamma \end{array} \qquad \begin{array}{c|ccc} d & 2 & 5 & 6 \\ c & 1 & 2 & 3 \\ b & 0 & 0 & 1 \\ a & 0 & 0 & 0 \\ \hline & \alpha & \beta & \gamma \end{array}$$

We shall prove that 6 is indeed the load of $v$.

A case of special interest is when $v$ is a standard word. Then the lifting and subsequent marking and functions are unique. We consider $v$ as a permutation on the set of its letters and look at the inverse permutation $v^{-1}$ on the places. For instance if $v = d\,a\,\underline{e}\,c\,\underline{f}\,\underline{b}$, one has $v^{-1} = 2\,\underline{6}\,4\,1\,\underline{3}\,\underline{5}$. Marked letters correspond to numbers greater than their left neighbour. The load of $v$ is by definition $0+1+1+1+2+3=8$. Up to reversal, this is the major index $5+2+1$ of $v^{-1}$, i.e. the sum of the lengths of the right segments of $v^{-1}$ determined by the underlined numbers. No such connection between the major index and the load exists for non-standard words.

## 2. The main result

For any lifting $w$ and $\gamma \in \Gamma$, we denote by $w^\gamma$ the subword of $w$ whose alphabet is $A_\gamma \times \{\gamma\}$. A straightforward attempt at a solution of our minimax problem consists in constructing successively these subwords for $\gamma=\alpha,\beta,\ldots$ by the following algorithm in which $w$ is understood to be read from right to left.

Suppose that the subwords $w^\beta$ have already been determined for $\beta<\gamma$. Then $a\gamma$ is the first occurrence of $a$ (which has not yet been used) and, supposing that $c_-\gamma$ has been chosen, one takes for $c\gamma$ the first (non-used) occurrence of a $c$, on the left of $c_-\gamma$, if there is one. If none exists $c\gamma$ is the first occurrence of a (non used) $c$ in $w$. This second possibility is the one which induces a marking of $c\gamma$.

The resulting lifting, marking and functions will be called *natural*. Our main result is the

**Property 1.** *The number of marked letters is minimal for the natural lifting; further, if $\bar{\nu}$ is the natural integrated delay function, one has $\bar{\nu}\leqslant\bar{\mu}$ for the integrated delay function $\bar{\mu}$ relative to any other lifting of $v$.*

Thus the load of $v$ is given by the above algorithm.

## 3. A conjugacy lemma

We suppose here that $v=cv'$, where $c$ is a letter which is not the first one of $A$ and one of its liftings $w=c\gamma\cdot w'$. Let $v_1=v'c$. It is clear that $w_1=w'\cdot c\gamma$ is a lifting of $v_1$. The number of marked letters and delay function of $w$ (resp. $w_1$) will be $r$ and $\nu$ (resp. $r_1$ and $\nu_1$).

**Lemma 1.** *The lifting $w_1$ is natural iff $w$ is so. Further: $r_1=r+1$ or $=r$, depending upon whether $c$ is or is not the last letter of $A_\gamma$; the delay functions $\nu$ and $\nu_1$ are equal except for $(c\gamma)\nu=(c\gamma)\nu_1+1$.*

**Proof.** The truth of the first assertion follows immediately from the definitions. To check the other ones, note that the markings of $w$ and $w_1$ are the same except, possibly for $c\gamma$ and $c_+\gamma$ ($c_+=$ the successor of $c$). In fact, because of $c\neq a$, the letter $c\gamma$ is marked in $w_1$ but not in $w$ and if $c_+\in A_\gamma$, i.e. if $c$ is not the last letter of $A_\gamma$, the contrary is true of $c_+\gamma$.

**Corollary 2.** *Assume $v=v'a^m$ where $m=|v|_a$ and that Property 1 holds for $v'$. Then it holds for any word $v_1=u''a^mu'$, where $u'u''=v'$.*

**Proof.** The definitions apply to the word $v'$ since it has a non-increasing multidegree on the alphabet $A\backslash a$.

The natural lifting of $v$ is deduced from that of $v'$ by left multiplication by the word $\cdots a\beta\cdot a\alpha$. Since this does not change the marking, Property 1 also holds for $v$. Thus, by induction on the length of $u'$, it suffices to check the result when $u'$ is a single letter. But this follows from the lemma since $u'\neq a$ by hypothesis.

## 4. Proof of the main result

We recall that the *plactic monoid* is the quotient of the free monoid $A^*$ by the least congruence $\equiv$ such that for any letters $b, c, d$, one has:

$$\text{if} \quad b<c<d, \quad \text{then} \quad cbd \equiv cdb \quad \text{and} \quad bdc \equiv dbc;$$
$$\text{if} \quad b<c, \quad \text{then} \quad cbb \equiv bcb \quad \text{and} \quad ccb \equiv cbc.$$

It has been studied by G. de B. Robinson, C. Schensted, D.E. Knuth and Curtis Greene (Cf. [3]). We shall only require the fact that all the words in a congruence class have the same multidegree and that one of them has the form $u''a^m u'$ with $a$ not occurring in $u''$ or $u'$.

**Lemma 3.** *If $v$ and $v_1$ are congruent there corresponds to any lifting of $v$ a lifting of $v_1$ having the same marked letters.*

**Proof.** Consider first the case when $v = v'bdv''$ and $v_1 = v'dbv''$ where $b < d \neq b_+$. It is clear that $w' \cdot b\gamma \cdot d\gamma' \cdot w''$ is a lifting of $v$ iff $w' \cdot d\gamma' \cdot b\gamma \cdot w''$ is a lifting of $v_1$ and that they have the same marked letters. This case covers the first elementary congruence defining $\equiv$. Suppose now that $v = v'cbbv''$ and $v_1 = v' = v'bcbv''$ where $c = b_+$. Let $w = w' \cdot c\gamma \cdot b\gamma' \cdot b\gamma'' \cdot w''$ be a lifting of $v$, where $\gamma$, $\gamma'$ and $\gamma''$ are any three greek letters. If $\gamma \neq \gamma'$ it is clear that $w' \cdot b\gamma' \cdot c\gamma \cdot b\gamma'' \cdot w''$ is a lifting of $v_1$ having the same marked letters. If $\gamma = \gamma'$ we have $\gamma \neq \gamma''$ and we can begin by replacing $w_1$ by the lifting $w_1' = w' \cdot c\gamma \cdot b\gamma'' \cdot b\gamma \cdot w''$ of $v$ without changing the marking. A similar argument applies to the other cases needed to cover the second elementary defining congruences, and the result is proved.

To conclude the proof of Property 1 we proceed by induction on the number of letters of the alphabet, the initial case being trivial.

Take any word $v_1 = u''a^m u'$ with $|u''u'|_a = 0$ in the congruence class of $v$. By the induction hypothesis the property holds for the word $u'u''$ which is on the smaller alphabet $A \setminus a$. Thus, by Corollary 3, it holds for $v_1$, i.e. one has the inequality $\bar{\nu}_1 \leq \bar{\mu}_1$ between any integrated delay function $\bar{\mu}_1$ and the natural one $\bar{\nu}_1$. Applying Lemma 3 gives the result, and a similar argument shows that the natural lifting has a minimal number of marked letters.

## 5. A further property of the natural delay function

We consider the natural lifting $w$ of the word $v$, and two consecutive greek letters $\beta$ and $\gamma = \beta_+$. We let $M$ be the set of marked letters.

**Lemma 4.** *Assume that $d\beta \in M$ and $d\gamma \notin M$. There exists a letter $b < d$ such that $b\beta \notin M$ and $b\gamma \in M$ and that $c\beta, c\gamma \notin M$ for any intermediate $c$, i.e. $b < c < d$.*

**Proof.** Because of the algorithm defining the natural lifting we can assume for simplicity, that $\beta$ is the first letter of the greek alphabet. The hypothesis $d\beta \in M$ implies that all the letters $d$ are to the right of $d_{-}\beta$ and $d\beta$ is the first of them. Thus $w$ has the subword $d_{-}\beta \cdot d\gamma \cdot d\beta$. Now if $d\gamma$ is not marked, $d_{-}\gamma$ must be to the right of $d\gamma$, and we have shown that $w$ contains the subword $d_{-}\beta \cdot d_{-}\gamma$.

To conclude the proof we need only to verify, by induction on the number of intermediate letters, that if $c\beta \cdot c\gamma$ is a subword of $w$, then $c\beta$ is not marked and, either $c\gamma$ is marked or $c_{-}\beta \cdot c_{-}\gamma$ is again a subword of $w$. Indeed the hypothesis that $c\beta$ is to the left of $c\gamma$ prevents that it be marked, i.e. that $c_{-}\beta$ be to its left. Thus $w$ contains the subword $c\beta \cdot c_{-}\beta \cdot c\gamma$. Suppose further that $c\gamma$ is not marked. Then $c_{-}\gamma$ must be on its right and the argument is concluded.

**Corollary 5.** *The natural delay function $\nu$ is non-decreasing in each of its two arguments.*

**Proof.** By definition, one has $(b\beta)\nu \leqslant (c\beta)\nu$ for $b < c$ and any $\beta$, and the inequality $(c\beta)\nu \leqslant (c\gamma)\nu$ follows from the above lemma by induction in the alphabet, since $(a\beta)\nu = 0$ identically.

## References

[1] D. Foata, Distributions eulériennes et mahonniennes, in: Proc. Advanced School on Higher Combinatorics. (M. Aigner Editor, Berlin, 1978).

[2] A. Lascoux and M.P. Schützenberger, Sur une conjecture de H.O. Foulkes, C.R. Acad. Sci. Paris 286 (1978) 323–324.

[3] G.P. Thomas, On Schensted's construction and the multiplication of Schur functions, Adv. in Math. 30 (1978) 8–32.

# les enjeux culturels de l'informatisation

ouvrage collectif sous la direction de
Françoise GALLOUEDEC-GENUYS et Philippe LEMOINE

préface de Bernard TRICOT

informatisation et société 9

LA DOCUMENTATION FRANÇAISE

# *On prétend que ...*

***MAURICE GROSS***
***MARCEL-PAUL SCHUTZENBERGER***

On prétend qu'une vague informatique va déferler sur tous les aspects de la vie quotidienne, donc sur la culture. La plupart des objets informatiques imaginés pour le public vont simuler des comportements humains quotidiens. Or les comportements d'intelligence sont actuellement hors d'atteinte de la compréhension scientifique. Les simulateurs proposés sur le marché seront donc tous décevants, et l'on peut prédire un reflux important de la panoplie des objets proposés :

– l'analyse des systèmes ne nous semble pas apporter de moyens de simuler des structures économiques ou sociales en dimensions réalistes ;

– ni les langages artificiels, ni l'analyse formelle des langues naturelles ne seront avant longtemps (au moins vingt ans) en mesure de rendre commode, donc courante, l'utilisation des ordinateurs ;

– nous avons fait des essais de dictionnaires de poche électroniques ; mis à part leur pauvreté qui est susceptible d'être améliorée, ils apparaissent comme pénibles d'emploi : le nombre des touches dont il faut mémoriser la fonction, la frappe de mots sur un clavier inadapté sont des facteurs qui limiteront longtemps la performance par rapport au dictionnaire ordinaire ;

— la traduction et la documentation automatiques vont se développer mais comme des versions dégradées de ce que l'on appelle communément traduction ou recherche de documentation. D'autres « services » du même type, tels le système de réservation de places à la S.N.C.F., vont se répandre. On peut prévoir qu'il faudra des années nombreuses avant que des remises en question les constituent en progrès.

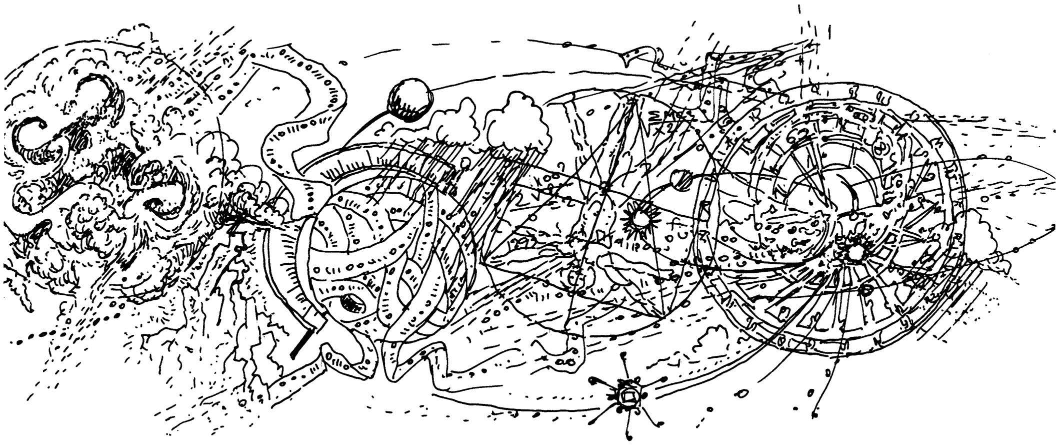
Nous avons surtout présenté les aspects négatifs des principaux projets informatiques qui devraient affecter le quotidien. Il ne subsistera guère de ce raz de marée que les jeux électroniques couplés à des écrans de télévision. Ces jeux comprendront les « quiz » qualifiés d'éducatifs et probablement rebaptisés aides informatiques à l'enseignement ou enseignement assisté par ordinateur. Les clubs d'amateurs auront un effet limité. Les amateurs ne résoudront pas les problèmes de logiciel auxquels se consacrent les grandes équipes de recherche.

# Compléments sur le traitement automatique des langues naturelles

*MAURICE GROSS*
*MARCEL-PAUL SCHUTZENBERGER*

## *La documentation automatique et les banques de données*

La popularité des banques de données tient certainement au fait qu'après avoir traité les problèmes de paye des entreprises, les facturations et redevances aux grandes compagnies et administrations, les fichiers publicitaires d'adresses et les fichiers de titres de documents, on a envisagé l'accumulation en machine de grandes quantités d'information de nature et d'origine quelconque. Mais alors, les problèmes se posant sont purement économiques ; dans quelle mesure les investissements initiaux toujours lourds peuvent-ils être justifiés par un nombre suffisant de consultations ? Les caractéristiques techniques se trouvent donc déjà dans les systèmes documentaires existants.



La terminologie ne doit pas tromper : banque de données ne signifie rien d'autre que grand fichier. Quand on qualifie une banque de données de relationnelle, cela signifie que des renvois, plus ou moins systématiques, ont été placés entre les divers éléments d'information. Les constructeurs de fichiers n'ont pas attendu la diffusion de ces termes nouveaux pour établir de telles relations. La nouveauté, si elle existe, ne peut guère être que commerciale, elle sera recherchée du côté des logiciels que les fabriquants proposent avec leurs machines.

Les méthodes (maintenant traditionnelles) d'analyse du discours ou de documentation automatique reposent sans exception, sur l'utilisation de mots-clés ; il s'y superpose parfois des raffinements statistiques ou structurels (lexiques de synonymes, lexiques organisés au moyen de relations entre les éléments). La méthode des mots-clés est acceptée et probablement acceptable dans des domaines techniques bien délimités. Par contre, dans ses applications aux sciences humaines, économiques et juridiques, où le vocabulaire n'est pas très technique, il est fréquent que des termes importants soient ambigus : l'utilisation des mots-clés est alors peut efficace. Il en va de même lorsque le système documentaire porte simultanément sur plusieurs domaines scientifiques différents. Un même terme peut alors avoir plusieurs définitions qui dépendent de chacun des domaines scientifiques (ainsi le terme perturbation a des sens différents en astronomie ou en mathématiques, et en météorologie).

De nombreuses méthodes, plus puissantes ont été proposées pour remédier à ces difficultés. Elles consistent à répertorier les associations syntactico-sémantiques de mots, dans le but de lever les ambiguïtés pour un domaine technique déterminé. Des algorithmes de calcul, qui ont pour point de départ les marques formelles (syntaxiques) du texte, établissent un réseau de relation devant être filtré par les associations sémantiques entre mots.

Toutes ces méthodes mettent en jeu un langage documentaire particulier, c'est-à-dire un système formalisé dans lequel il est nécessaire de traduire textes et questions. La traduction du langage naturel en langage documentaire n'est jamais entièrement automatisable, car les relations sémantiques ne suffisent pas à éliminer les ambiguïtés dues au calcul syntaxique. Il est donc nécessaire d'avoir recours à une traduction partiellement manuelle donc coûteuse, surtout si de grandes quantités de textes sont en jeu. Tous ces systèmes n'existent donc qu'associés à des échantillons de documents qui ne peuvent être qu'anecdotiques. Il n'existe aucune garantie qu'ils peuvent fonctionner en vraie grandeur.

De nombreux chercheurs ont considéré que l'amélioration de cette situation passait par une analyse poussée des textes traités et, en particulier par des raffinements de l'analyse syntaxique automatique. Ces raffinements nécessitent des progrès importants dans la connaissance fondamentale des langues naturelles.

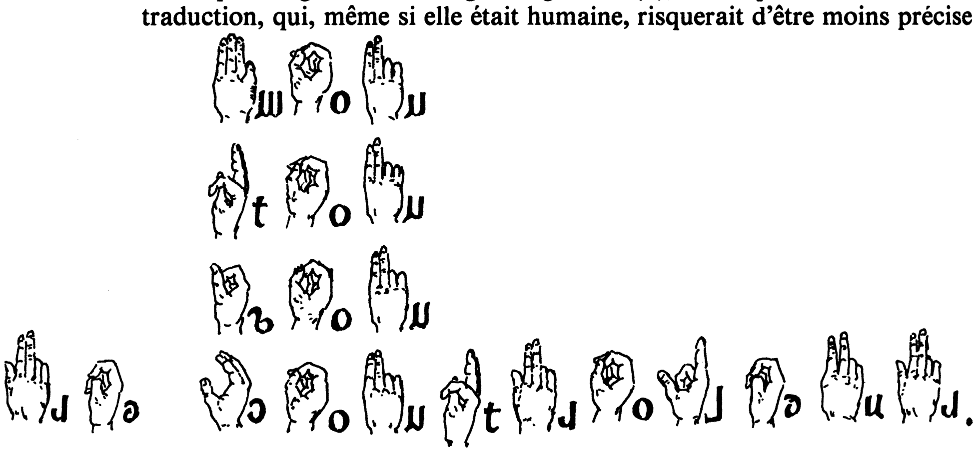
Les propositions les plus évoluées de la documentation automatique sont les systèmes d'interrogation en langue naturelle. Une banque contient des données, un utilisateur quelconque n'ayant pas appris de langage d'interrogation spécial doit pouvoir poser des questions quelconques. Celles-ci sont confrontées avec les données de la banque, et une réponse doit être fournie en langue naturelle après d'éventuelles transformations, de préférence syntaxiques et sémantiques (règles de déduction, d'inférence logique). Si la banque contient des données constituées de textes, il est clair que de nombreux problèmes d'analyse linguistique vont se poser au niveau de la constitution et de la mise à jour de la banque, ainsi qu'à celui de sa consultation.

Les problèmes purement linguistiques sont encore mal connus et probablement mal posés. Par contre, du fait de leur parenté avec les langages logiques, les langages formels de représentation ont déjà fait l'objet de nombreuses publications.

## *La traduction automatique (T.A.)*

Il est toujours possible de construire des modèles rudimentaires de traducteurs mécaniques. Considérons l'exemple d'un programme qui traduit mot à mot n'importe quel texte de n'importe quelle langue dans une autre langue. Il ne comportera que quelques dizaines d'instructions. Il est difficile d'arguer que les résultats obtenus de cette façon ne sont pas des traductions. De plus, si par exemple l'ordre des mots n'est pas le même dans les deux langues, un programme opérant à la suite de la traduction mot à mot replacera dans l'ordre correct certains des mots de la langue cible. Par rapport au mode de traduction mot à mot, nous aurons là une traduction améliorée. C'est précisément cette démarche qui a permis à certains auteurs de programmes de T.A. de prétendre qu'un processus de convergence était amorcé. De nombreuses tentatives infructueuses, ainsi qu'une analyse poussée de cette activité ont montré de façon convaincante qu'elle était sans issue. Mais il a paru alors possible de parler de pourcentage de succès, terme particulièrement sensible dans les activités appliquées. Or en aucun cas, on ne peut évaluer des pourcentages offrant le moindre intérêt. Dans le cas de la traduction, on peut compter les pourcentages de mots traduits, mais cela n'a guère de sens puisqu'en principe on peut augmenter à volonté la taille des lexiques et remédier ainsi aux absences. Si l'on désire effectuer des décomptes sur les fautes de syntaxe, on se heurte alors au problème des statistiques sur les formes syntaxiques des textes, problème qui est loin d'être résolu.

Nous considérons donc que dans l'état actuel des connaissances il n'est pas possible de mettre au point des applications à caractère quelque peu économique. Mais des circonstances spéciales peuvent rendre utilisables des procédures automatiques qui simulent la traduction. Considérons la situation suivante. Dans un pays P, il existe une langue dominante L(P), dans laquelle sont effectuées toutes les publications scientifiques, techniques, administratives, ... Dans ce pays, il existe une minorité quasi-bilingue dont la langue, réprimée, est L(M), et dont les revendications linguistiques ont été acceptées : tous les documents produits dans L(P) seront traduit dans L(M). Le problème est évidemment politique. Mais du point de vue linguistique, on peut se demander dans quelle mesure la minorité (bilingue) a besoin des traductions : est-ce pour se documenter ou pour s'affirmer comme réalité politique ? Supposons qu'un ingénieur activiste, mais bilingue, de la minorité ait à modifier un appareil nucléo-électronique extrêmement important, donc coûteux. Il aura intérêt à utiliser la notice technique rédigée dans la langue originale L(P), et non pas à recourir à une traduction, qui, même si elle était humaine, risquerait d'être moins précise



que le texte original. Cette situation risque d'être des plus générales, au point que le seul fait qu'une traduction soit produite en un lieu quelconque, et quelle que soit sa qualité, puisse suffire à satisfaire les aspirations de la minorité. Dans de telles conditions, il est clair que des traductions même rudimentaires seront des plus « utiles ». Et puis, si cette minorité considérait que les traductions de mauvaise qualité ne résolvaient pas ses problèmes linguistiques, il deviendrait alors nécessaire que les deux parties s'entendent sur une définition de la notion de traduction acceptable. Le problème serait alors placé entre les mains de commissions paritaires dont on ne voit pas quel accord simple elles pourraient espérer atteindre, d'où le renvoi du problème en sous-commission, où les mêmes algorithmes de discussion seront utilisés (une telle boucle semble difficile à rompre).

Il n'est donc pas exclu que des produits destinés à des fins nouvelles puissent être construits (par exemple, au sens des organisations internationales où les besoins en traduction sont énormes). Il est difficile de juger de la qualité de tels travaux en s'appuyant sur l'état présent des deux domaines de base : informatique et linguistique. Les seuls évaluations qui pourront être faites n'auront lieu qu'à posteriori. Il n'y a que le résultat pratique éventuellement obtenu qui justifiera cette activité et donc décidera de sa prospérité.

En général donc, l'amélioration des procédures de traduction automatique nécessitera l'acquisition de connaissances nouvelles en linguistique, sans que le succès économique soit garanti. L'accumulation de ces connaissances risque de perdre du temps. Ainsi, la construction du lexique-grammaire du L.A.D.L. a pris plus de dix ans ; elle n'est pas terminée. Il n'en existe pas pour d'autres langues que le français. Il ne fait pas de doute que des descriptions analogues de langues différentes pourraient s'accélérer maintenant que des méthodes ont été développées. Mais il sera également nécessaire de mettre au point des règles de transfert d'un lexique-grammaire à un autre. Dans ce domaine, tout est à faire. La syntaxe comparée formalisée constitue un domaine de recherche très limité, à l'heure actuelle. Les problèmes y semblent nombreux et complexes, des exemples comme le suivant nous en donnent un aperçu. Considérons les phrases anglaises :

**Max knows Guy**
**Max knows Russian**
**Max knows that your sister left**

Les traductions les plus simples sont respectivement

**Max connaît Guy**
**Max (connaît + sait) le russe**
**Max sait que (ta + votre) sœur est partie**

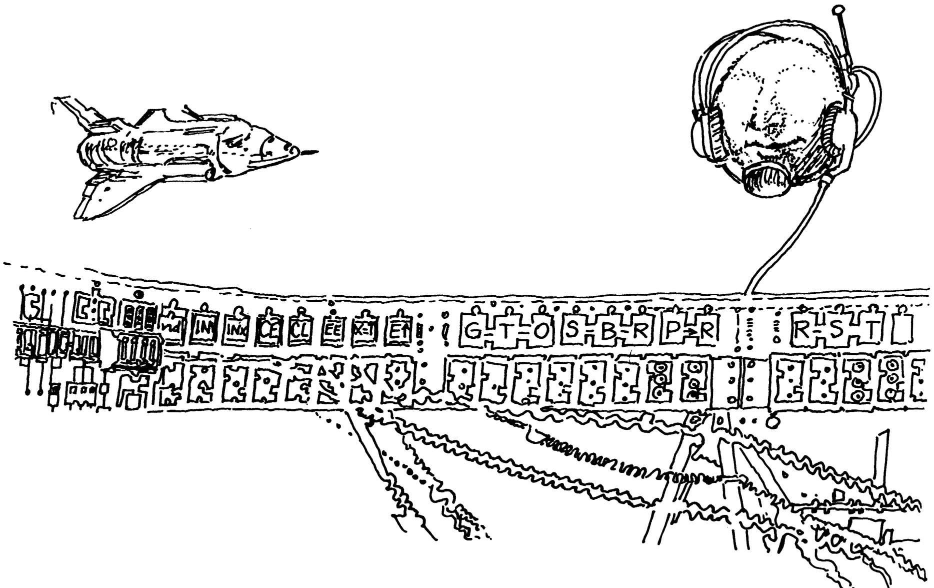
Le verbe **to know** se traduit tantôt par **connaître,** tantôt par **savoir,** mais les conditions sont complexes, puisque l'on a les interdictions

*** Max sait Guy**
*** Max connaît que ta sœur est partie**

Notons de plus que la complétive n'est pas toujours interdite avec **connaître** puisque l'on accepte

**Que ta sœur est partie est connu de tous**
**Il est bien connu que ta sœur est partie**

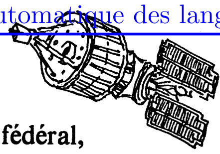
Il est clair que si des études détaillées et systématiques étaient effectuées sur de telles questions, non seulement une certaine mécanisation de la traduction pourrait intervenir, mais les retombées sur la connaissance des langues, et donc leur enseignement et leur traitement, seraient immenses.



Il est intéressant d'observer que parallèlement aux études stériles de T.A., il n'y a pas eu d'études plus modestes, mais dont les résultats auraient été garantis et probablement utiles. Ainsi, aucun dictionnaire multilingue n'a été construit en traduction automatique, alors que les auteurs de projets ne pouvaient pas ignorer qu'un tel composant était nécessaire quelque soit le système de traduction adopté ! Il n'est donc resté aucun sous-produit utilisable des études de T.A., pas même un dictionnaire qui aurait pu être l'amorce d'un dispositif d'aide mécanique à la traduction humaine.

Ce n'est que depuis quelques années que l'on reparle de dictionnaires informatisés et les réalisations les plus ambitieuses sont :

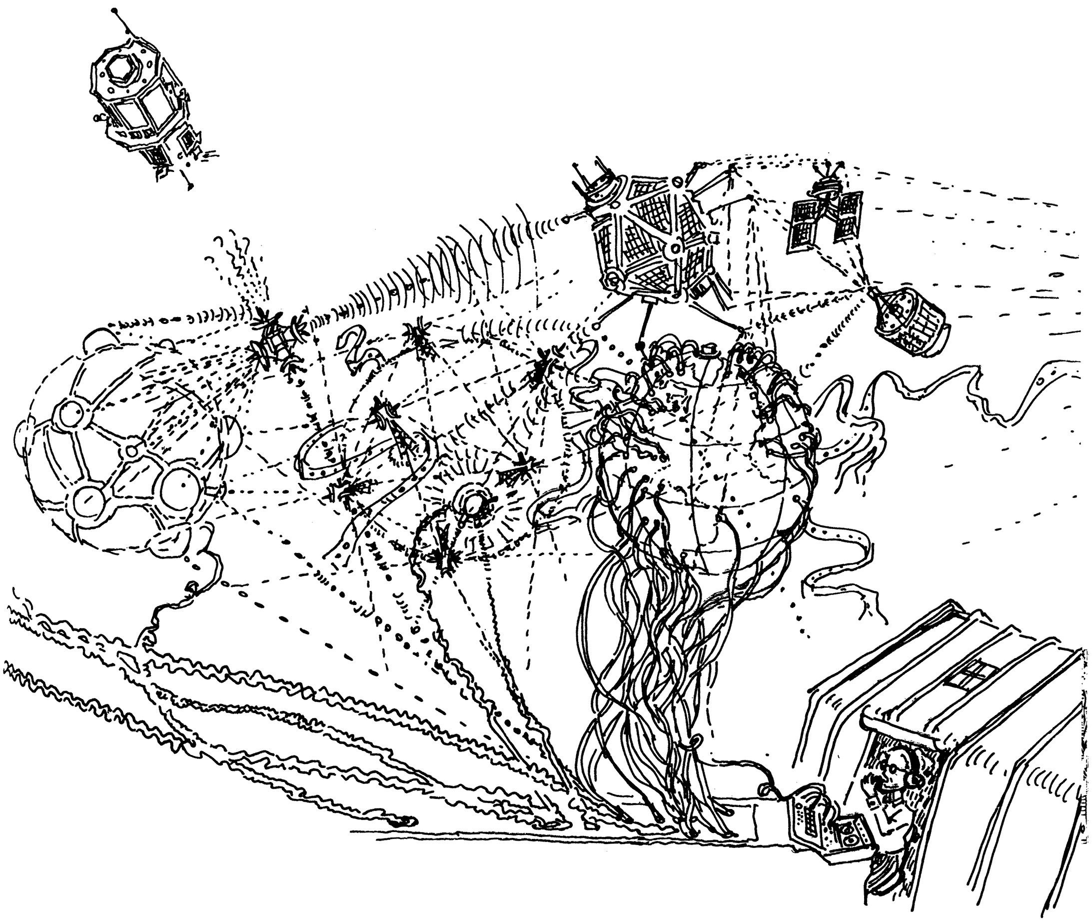
— celles du Canada, elles sont destinées à aider à la résolution des problèmes linguistiques du Québec. Deux banques de données terminologiques



viennent en aide aux traducteurs : à Ottawa, celle du gouvernement fédéral, à Québec celle du gouvernement québécois ;

– celles d'organisations internationales, surtout en Europe (C.E.E.).

Toutefois, les motivations de l'emploi de ces dictionnaires étant peu claires ou peu avouables, l'évaluation de leur efficacité et de leur avenir n'est pas chose facile. Par contre, nous avons eu l'occasion de voir fonctionner un dictionnaire dans des conditions économiques connues, celui de la compagnie Siemens à Münich. Ce dictionnaire est destiné à faciliter les travaux de traduction des notices techniques des appareils produits par la compagnie et vendus à l'étranger. Le nombre des traducteurs intéressés par ce système est de l'ordre de 1 500. Ils peuvent consulter le dictionnaire par terminal, ou bien disposer de dictionnaires de forme classique (livre en papier) mais produits de façon entièrement automatique (y compris la photocomposition). Il est apparu qu'un tel système avait une utilité réelle, mais nous insistons encore une fois sur l'existence de conditions économiques



favorables, du point de vue de la constitution (coûteuse) du fonds initial. De plus, dans ce dispositif, la mise à jour du dictionnaire est faite de façon continue, à partir des problèmes quotidiens posés par les traducteurs, ce qui dispense de constituer des équipes de fonctionnaires chargées à temps plein de l'entretien du système.

Les dictionnaires miniaturisés toucheront sans nul doute un public beaucoup plus nombreux. Notons que les deux types de réalisations : grands systèmes de dictionnaires et dictionnaires électroniques de poche ne sont pas des activités indépendantes. Les mémoires des dictionnaires de poche seront obtenues automatiquement en vidant tout ou partie d'une mémoire de grand ordinateur dans la pastille constituant la mémoire de l'appareil de poche. En attendant, les exemples disponibles dans le commerce sont des gadgets qui ne peuvent en aucun cas entrer en compétition avec des dictionnaires sous forme de livre.

Nous avons ici un exemple des deux principales voies qui s'ouvrent à l'introduction de moyens informatiques dans le grand public : terminaux connectés à de grands systèmes (par téléphone ordinaire ou spécial) ou micro-ordinateurs individuels. Si nous prenons le cas de l'utilisation de dictionnaires (ou d'encyclopédies) à l'école, les deux solutions apparaissent comme toutes deux envisageables, et d'ailleurs pas forcément incompatibles.

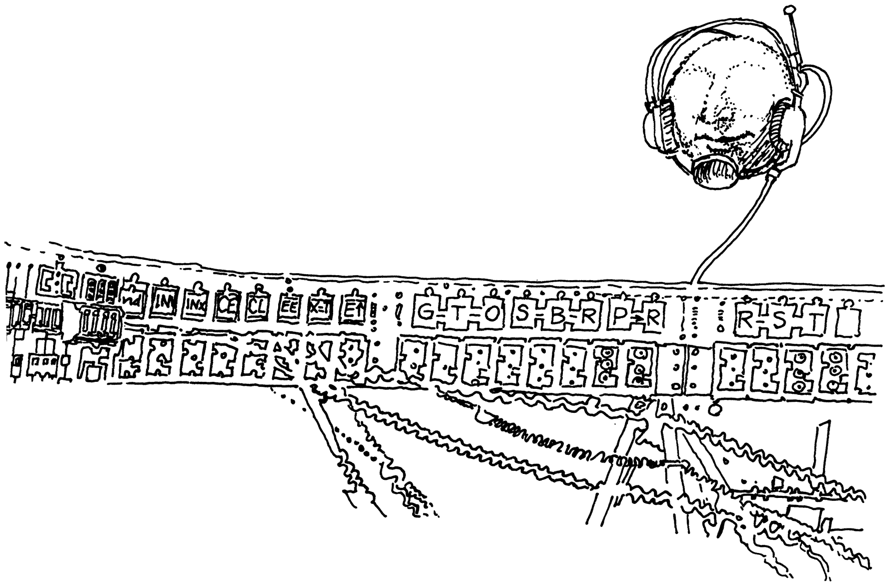
# *Sur l'analyse des systèmes*

*MARCEL-PAUL SCHUTZENBERGER*

Les remarques que je développerai plus loin sur la théorie générale des systèmes soulèveront de nombreuses objections. Beaucoup d'entre elles seront tellement irréfutables que je n'entreprendrai pas d'y répondre : ce sont celles qui sont armées d'arguments d'une portée si universelle qu'elles touchaient avec la même force pour (ou contre) la plupart des théories qu'elles soient vraies, absurdes, certaines fausses ou vides.

Le premier argument, version démocratique du principe d'autorité, oppose à tout examen d'un système le fait réel ou allégué de son acceptation comme idéologie d'une pratique sociale plus ou moins populaire. Il rend futile devant certains la discussion de l'astrologie, de la radiesthésie, de l'existence des antipodes, de la psychanalyse, des prévisions météorologiques, de la théorie élémentaire des ensembles,...

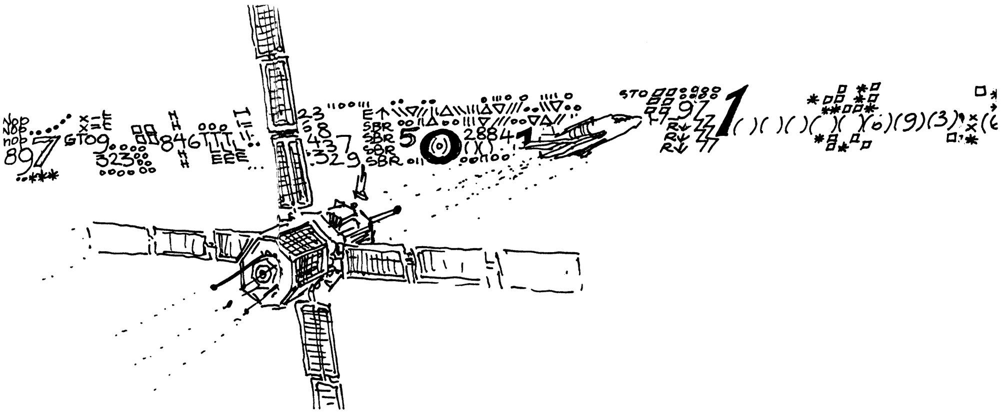
Notez ici, je vous prie, que l'urgence de la nécessité motivant cette pratique sociale (mettons l'astragalomancie computeurizée de vos amours, du prix des épices ou de ma mort) ne diminue en rien l'inaptitude (éventuelle) de la théorie qui la sous-tend.



Après vient le recours à la défense élastique vantant la théorie non point pour ce quelle dit, concédé être faux ou vain, mais au nom des travaux qu'elle aurait provoqués ou plus souvent des progrès admirables qui découleront sans doute des recherches qu'elle ne manquera pas de susciter. Nous voici donc renvoyés au cabinet des horreurs de l'histoire des techniques ou à la science des futurs. Mais si vous acceptez cet argument, il vous faut encore acclamer l'astrologie, mère de l'astronomie, tout autant que l'erreur de Cassini à laquelle nous dûmes deux Laponnes.

Ainsi que les autres, l'argument suivant est ontologiquement imparable : c'est celui de la **valeur explicative.** Pour ceux d'entre nous dont je respecte les convictions marxistes (resp. darwiniennes, resp. bretonnes, resp. freudiennes), le matérialisme dialectique (resp. la sélection naturelle, **resp. la lune, resp. l'inconscient) explique, et fort bien, l'histoire** (resp. l'évolution, resp. les marées, resp. tout). Pour d'autres, absolument pas. Quant à moi, je tiens la primarité du nombre 127, expliquée **à la perfection** par le fait qu'il divise $-2+(1.416.317.954)^2$ et par celui que Dieu est beau. Position ferme et irrévocable contre laquelle vous ne prévaudrez pas. En réciprocité, je ne tente pas d'altérer votre opinion personnelle (peut-être donnez-vous des priorités inverses aux deux raisons ci-dessus) car une explication ne vaut que pour qui s'en sent illuminé.

Pourquoi donc croire à l'effet de la lune sur les marées. Certainement pas seulement parce que de nombreux témoins **graves** ont dans de longs écrits déclaré avoir vu celles-ci (et aussi la lune) sans que l'on puisse soupçonner leurs observations d'être viciées par des intérêts personnels (même abyssaux) ou par l'effet d'un entraînement collectif.

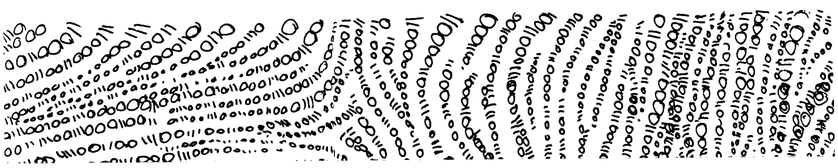


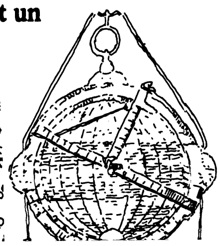
Non plus parce que des calculs par machine prétendant se baser sur les mouvements de notre satellite permettent une prévision efficace, socialement louable et numériquement précise des niveaux de la mer (ils incorporent tant de données locales...). Mais il me semble parce que la théorie de l'attraction universelle (disons) et de son action sur l'hydrosphère rend compte sans (trop de) failles ni glissements de sens sournois d'une multitude de phénomènes. Certains qualitatifs non triviaux (pourquoi donc cette coïncidence entre les hautes eaux et les équinoxes ?) d'autres quantitatifs et ceux-ci très fidèlement, au moyen de paramètres empiriques dont elles donnent avec franchise la liste à priori ainsi que la prescription à suivre pour les déterminer.

Bien plus encore, comme vous l'instaurâtes, Sir Karl, mon bon Maître, parce que ce tissu immense de raisonnements tomberait en charpie si l'on y changeait le moindre point ou si se rencontrait quelque désaccord avec ce qui se peut observer (bien que maint pêcheur du Maine a été étonné quand le goût des vacances l'a conduit au Tonkin).

Ceci achève la recopie du cours de logique à vous transmis depuis la classe de philo du Collège agricole d'Ouzouer-le-Marché où il me fut dicté bien avant que l'informatique ait changé tout cela.

Et pour conclure, et faire transition, l'argument d'obsolescence ou d'incompétence souverain dans les domaines (tels para-psychologie, intelligence artificielle, structure de la mode, diététique, ...) où l'espoir de flux monétaires intenses induit un progrès rotatif rapide et incessant. La multiplication concomittante des chapelles vibrionniques ne laisse au commentateur que le choix de l'aveu : il n'a pas encore lu le prochain livre à paraître qui, enfin, sera le bon, ou, plus dangeureusement, il a cru entendre le dernier séminaire rival. **Donc, sans aucun doute, le commentateur est un ignorant et un vilain jaloux. Un cuistre.**





# *Le but et les méthodes*

La théorie générale des systèmes (G.S.T.) est un mouvement d'idées aux origines multiples et aux visées immenses qui s'est assez largement développé aux États-Unis dans les années 60 et dont la popularité est devenue mondiale avec le « rapport de Rome » auquel s'est attaché le nom de J.W. Forrester, un des plus influents protagonistes de la G.S.T. (*World Dynamics,* 1971). A tel point que même les instances les plus élevées de l'administration scientifique française ont été au courant de ce phénomène (Cf. le projet de 1977 du CNRS sur la G.S.T.).

Quelles en sont les sources, les buts, les méthodes ?

J'ai déjà dit que les origines de la G.S.T. étaient diverses : parmi celles que citent le plus volontiers les auteurs, figurent l'œuvre d'un biométricien mineur (en tant que biologiste) mais respectable, von Bertalanffy *(General System Theory,* 1968), d'un psychiatre anglais Ross Ashby *(An introduction to Cybernetics,* 1956), et les livres biographiques ou de vulgarisation scientifique d'un grand mathématicien, mon bon Maître Norbert Wiener *(Cybernétique,* etc., 1955).

De fait, d'autres auteurs non moins graves semblent se réclamer de toutes autres sources puisqu'aucun de ces trois noms ne figure dans l'exposé d'ensemble de la G.S.T. destiné au grand public *(Compton Conferences,* MIT, 1968) par le mieux reconnu des théoriciens des systèmes, Herbert A. Simon. La même remarque vaut d'ailleurs aussi pour A. Rapoport, qui, comme les autres déjà cités, doit être considéré comme l'un des cinq auteurs les plus influents d'après l'étude « systématique » publiée en 1977 par R. Cavallo (in Klir, *Applied General Systems Research).*

Pour ce qui est des thèmes, la boule de feu première paraît être indubitablement le grand bouillonnement d'idées nouvelles qui s'étaient exprimées dans les années 50 à la cafétéria du MIT (en particulier) et (de façon plus incontrôlée) dans les symposiums de la Josiah Macy Foundation : ce sont ces projets, ces ambitions, ces espoirs qui constituent la substance de la partie non autobiographique du livre de N. Wiener et il me paraît digne d'y associer la mémoire d'un autre de mes Maîtres Warren Mc Culloch, psychiatre et homme de culture dont l'intelligence et la bonté rayonnante encourageaient les pires audaces intellectuelles. Quelques années plus tard, sous l'influence de Warren, le même mouvement s'implantera dans les plaines de l'Ohio, sous le nom de Bionics, avec un infléchissement très marqué vers la biologie ingénieresque et von Bertalanffy finira par être inscrit parmi les précurseurs.

Quand au courant strictement cybernétique (qui n'avait jamais été pris au sérieux aux États-Unis) il va fleurir en URSS, dans certains pays de l'Est, en Italie, à Namur.

Ceci pour l'anecdote et l'on pourrait sans peine retracer les filiations effectives qui d'un centre à un autre ont permis le développement de ces idées et l'attribution des crédits.

Intellectuellement, les motivations sont doubles. La plus immédiate est la poursuite de l'ambition scientifique de **tout** réduire à la mathématique. Les succès admirables de von Neuman et de Shannon dans la formalisation des jeux et des communications faisaient espérer que la même entreprise devrait réussir ailleurs : en sociologie, au-delà de Lewin et de Moreno, en psychologie, plus profondément que par la psychométrie, en physiologie cérébrale, ...

Bien sûr, cet effort est dans la tradition scientifique la plus classique. Notons cependant qu'elle a pour outil essentiel les modèles dont le succès n'est guère discutable qu'en termes d'adéquation empirique et que cet empirisme s'évanouira chez les systémistes plus récents.

La deuxième, tout au contraire, est une réaction contre l'ambiance intellectuelle atomiste et réductionniste des pays de culture anglo-saxonne. Reprenant de vieux thèmes continentaux sur la prééminence du tout sur la partie, sur le primat de la relation par rapport à l'objet, elle a d'autant plus de succès qu'elle apparaît dans l'Ohio puis en Californie comme une nouveauté révolutionnaire fulgurante. (Tout comme, bien entendu, les échos appauvris de l'associationisme, soulèveront l'enthousiasme romantique des lecteurs européens formés à la rhétorique sonore de la Sorbonne Lettres).

Et entrent en scène pour tout réconcilier les mathématiques formelles dont la connaissance commence à pénétrer les chaumières.

D'autant que par chance, les ordinateurs permettent de sauter par le biais de la simulation toute difficulté de raisonnement mathématique qui ferait apparaître les failles du discours.

Les voici donc prêts à résoudre les problèmes fondamentaux qui confrontent le monde moderne :

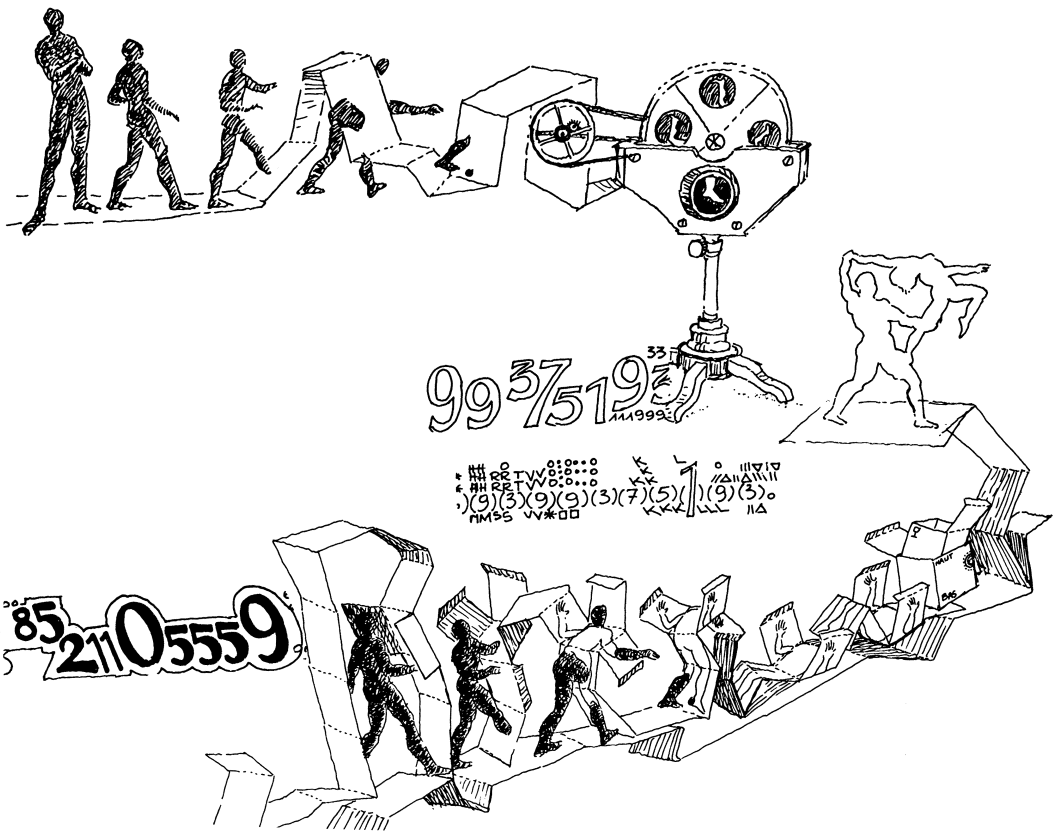
Attendu que toute chose (la plante, la ville, la famille, le cerveau, la prison, l'œcumène) est un système ;
attendu que tout système est une entité complexe, hiérarchisée dans laquelle les interactions entre les parties et le tout constituent l'essentiel ;
attendu qu'il est impérieux de contrôler l'évolution de ces systèmes sous peine de périr (de pollution, de manque de communication, de mal d'estomac, ...) ;
attendu que les techniques classiques n'y peuvent rien ;
il faut au plus vite élaborer une théorie générale permettant la compréhen-

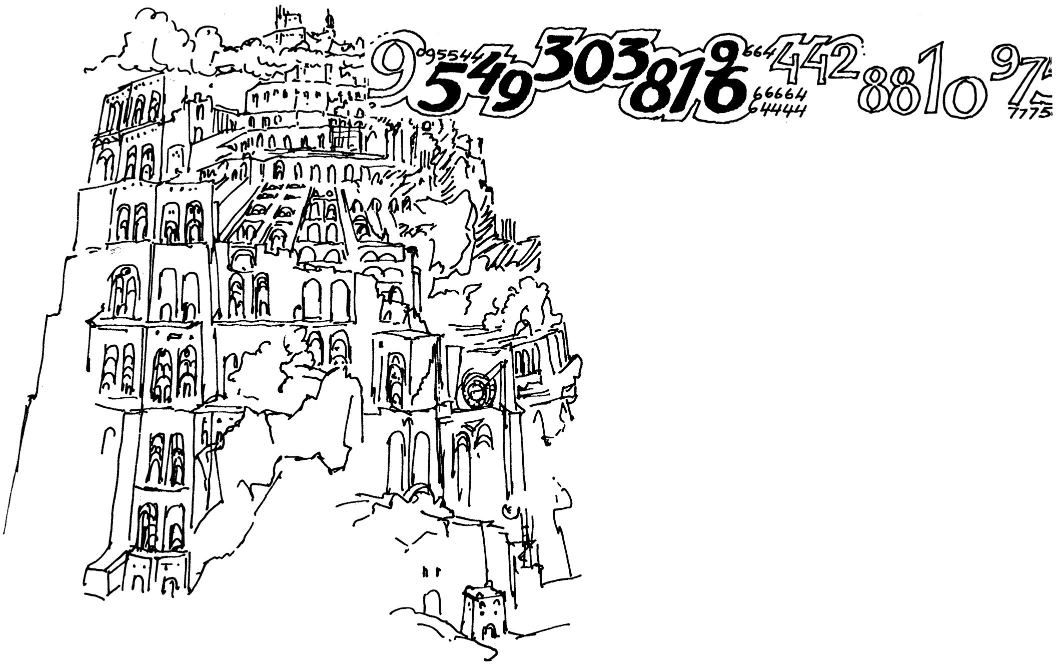
sion des dits systèmes, et du même mouvement la possibilité de guider leur cours (s'il en est encore temps !).

Voici pour les buts.

Quant aux méthodes, elles feront largement appel aux mathématiques les plus modernes (catégories, récursivité), aux chapitres les plus récents (théorie de l'information, des jeux, des automates) et aussi à la modélisation sur ordinateur la plus impitoyable depuis le règne de Procuste.

Je ne crois pas que cette insistance sur l'aspect **mathématique** de la G.S.T. soit une interprétation personnelle. Certes des auteurs importants (par exemple le doux Laszlo) ne se préoccupent que de l'aspect philosophique, (curieusement toutefois, le seul linguiste qu'il cite est aussi le seul ayant effectivement tenté de mathématiser sa discipline) ; certes aussi H. Simon évite prudemment les raisonnements formalisés et préfère la force de vérité foudroyante d'assertion telle que la suivante qu'un psychiatre aurait dû se retenir de citer :





« L'homme considéré comme un système animé est relativement simple. L'apparente complexité de son comportement est, pour une large part, le reflet de la complexité de l'environnement dans lequel il vit ». (Loc. cit. trad. française, p. 69).

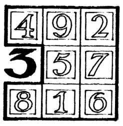
En ce qui concerne la philosophie ou la psychologie je n'ai rien à dire, non plus qu'en ce qui concerne l'usage poétique que peut jouer la G.S.T. dans l'expression de la pensée de certains de mes amis. Mais je le répète, la partie mathématique est l'ingrédient essentiel de la G.S.T. Le même livre de H. Simon abonde en références corroboratives aux travaux de M. Minsky (Prof. aux Dpts de Mathématiques et d'Informatique du MIT) ; le livre fondamental de Mesarovic *(Theory of hierarchical multilevel Systems)* a toutes les apparences typographiques d'un ouvrage normal de la série dans lequel il est paru (Mathematics in Science and Engineering) ; de même celui de Zeigler. Bref, je ne pense offenser personne en affirmant que les trois quarts ou plus des communications présentées à la Conference Internationale de G.S.T. à New York en 1977 sont incompréhensibles à tout lecteur de bonne volonté dont la culture mathématique ne dépasserait pas très nettement celle du bac. C.

C'est donc à ce titre que le cordonnier que je suis peut se permettre une observation sur une œuvre qui a valu un prix Nobel à un de ses meilleurs Pères.

Cette observation est que la partie mathématique de la G.S.T. est une imposture absolue.

Je dois avoir l'honnêteté d'ajouter que la même observation avait déjà été faite par D. Berlinski (sur une base bien différente, comme on pense).

# *Des mathématiques comme instrument d'imposture*



Il faut maintenant que je justifie mon observation, et je tourne la plume sans parvenir à me décider sur le choix d'une stratégie. Vous vous souvenez du personnage de Huxley qui demande (avant guerre, bien sûr) qu'on lui prouve que la face postérieure de la lune n'est pas habitée par une race spéciale d'éléphants verts ? Je suis ici son interlocuteur. Seriez-vous prêts à ce que je démontre à coup d'équations les erreurs grossières de Rosen, la fausseté du théorème principal d'Ashby, le caractère absurde des simulations de Forrester (voir cependant à ce propos ce qu'est forcé d'en dire Berlinski), que je développe la noire série d'arguments techniques qui permet de prévoir l'échec du « General Problem Solver » de H. Simon ainsi que d'autres il y a 10 ans avaient permis la même prédiction en ce qui concernait le perceptron ou la traduction automatique ? Les outils conceptuels et les théorèmes seront là depuis Kleene et on peut maintenant s'appuyer sur la rigueur du Traité de S. Eilenberg *(Automata, Formal Languages and Machines,* 1974-1976) pour fixer les bornes de ce que ne peut pas faire un certain type d'approche. Mais il est bien douteux que vous ayez l'indulgente bonté de me suivre pendant trente pages de raisonnement mathématique.

Cependant, ce sont ces énoncés faux ou ces assertions absurdes qui étayent le discours de la G.S.T.

Donc je renonce ici à l'argument de la rigueur absolue et je me borne à affirmer répétitivement :

**la littérature de la G.S.T. abonde en énoncés mathématiques faux, irrémédiablement faux.**

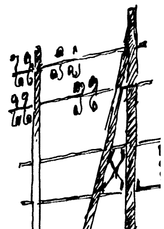
Du même coup, sans plus guère d'espoir de convaincre les Autorités Supérieures Administratives qui s'évertuent à diriger notre Recherche, j'affirme (en m'appuyant très particulièrement sur Mesarovic) :

**la quasi totalité de ce qui n'est pas faux est inexorablement trivial.**

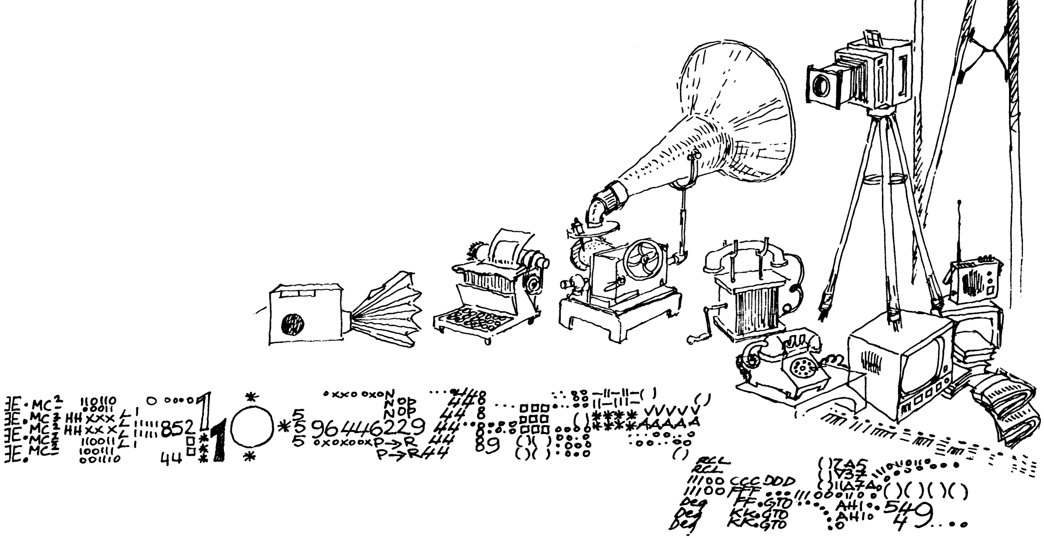
Pour les non-spécialistes cet argument ne pèse pas, voire ne signifie rien, je le sais. J'espère donc n'offenser aucun de ceux qui ont appris les rudiments de l'algèbre universelle dans les œuvres de mon ami Rapoport ou la topologie générale dans les travaux d'Arbib (qui ont d'ailleurs fait mieux en d'autres lieux) et un peu de théorie de la mesure grâce aux ensembles pileux.

210

Plus facile peut-être parce que moins technique serait de confronter le contenu des chapitres de la mathématique que l'on invoque avec ce que l'on leur fait dire. Sur deux d'entre eux, Berlinski se tait pudiquement et je les examinerai ici.



Permettez que je prenne d'abord la théorie de l'information de Shannon puisqu'elle est l'un des thèmes les plus inlassablement paraphrasés dans les publications de la G.S.T. Que contient-elle qui puisse se dire en **mots** sans employer de formules mathématiques :



« Si un émetteur produit des messages selon une loi de probabilité **connue** il est possible d'attacher à cette loi une certaine quantité de telle sorte que la correspondance entre l'émetteur et le récepteur (qui constitue la transmission) puisse selon cette mesure être réalisée de façon arbitrairement précise par complexification du codage quand on considère une transmission arbitrairement longue ».

Exemple : en parlant au téléphone on parvient à se faire entendre en répétant chaque phrase autant de fois qu'il le faut.

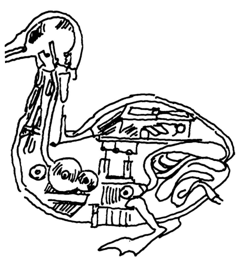
L'exemple est ridicule car la beauté merveilleuse du théorème de Shannon n'est pas dans cette platitude mais d'abord dans le fait que quand les lois de probabilité sont connues, la vitesse d'approximation à la transmission correcte est calculable. Ensuite, dans ce que cette expression formalise de façon essentielle la notion d'information transmise dans les cas où un schéma probabiliste connu s'applique à l'émetteur. Surtout dans la preuve qui est si profonde que nous n'avons pas fini d'en exploiter les filons.

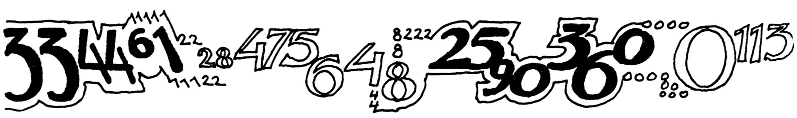
Mais l'exemple n'est pas que ridicule. Si les lois de probabilité sont inconnues, il n'y a **pas** de théorie de Shannon. Qu'importe alors que la « soi-disant » quantité d'information » soit le logarithme du maximum d'une probabilité quand celle-ci **n'existe pas,** ce qui est évidemment toujours le cas en dehors de certains domaines techniques précis des télécommunications ? A quoi bon imiter Lévi-Strauss ou McLuhan et faire doctement référence dans un contexte qui lui est étranger à une théorie qui par son essence même, ne dit **rien** hors le cadre conceptuel précis dans lequel elle a été créée ? (Remarque : j'ai oublié de préciser que pour abréger, j'appelle **imposture** toute référence au théorème des Forces Vives dans un discours célébrant ou dénigrant l'énergie des Grands Chefs Militaires et Civils). Pourquoi par exemple ne pas parler de Fisher qui a introduit (en 1930) une autre mesure de l'information qui s'enseigne depuis dans tous les cours de statistique avancée ? Elle serait (peut-être !) parfois moins irrelevante, mais sûrement aussi moins prestigieuse.

Seconde farce, la théorie des automates que l'on trouve mentionnée si fréquemment dans l'ouvrage de Klir déjà cité.

Tout d'abord mettons à part un opuscule tardif de von Neuman (qui est resté sans postérité intellectuelle) essayant de discuter le nombre minimum d'éléments d'une machine de Turing dans un cadre conceptuel un peu différent. Si je vous dis que ce minimum est 18 êtes vous plus éclairé ? Et votre vision du monde serait-elle changée si c'était plutôt 242 ? Ou 79 ? Vous sentez bien que tout est dans le choix des définitions.

**Depuis, grâce au théorème de Kleen qui l'a fondée,** la théorie des automates s'occupe de tout autre chose : essentiellement d'étudier **en profondeur** la nature des calculs qui n'exigent pour être faits que des moyens si rudimentaires que c'est presque scandale que de les appeler calcul. Ainsi la théorie des automates n'a rien à dire (et ne dit rien) sur la multiplication des entiers (il y a là cependant des choses profondes, mais c'est une toute autre théorie, ignorée de la G.S.T. qui étudie les algorithmes utilisant la multiplication). Sujet misérable donc, direz-vous. J'y consens. Mais ayant **sa vertu, la rigueur. De fait, son impulsion originelle (Kleen)** provient du désir de fixer de façon rigoureuse les limites d'une thèse avancée par McCulloch et Pitts et, comme vous le savez maintenant, ces limites sont très étroites : un système fini d'objets discrets, opérant en temps discret ne peut que très, très mal simuler tout autre chose que lui-même ; en particulier, un processus pourtant aussi élémentaire que la compilation (= analyse grammaticale) d'un programme d'ordinateur.





Et voici expliqué pourquoi on ne parle plus désormais de l'application du General Problem Solver de H. Simon à cette tâche pourtant bien humble et bien utile.

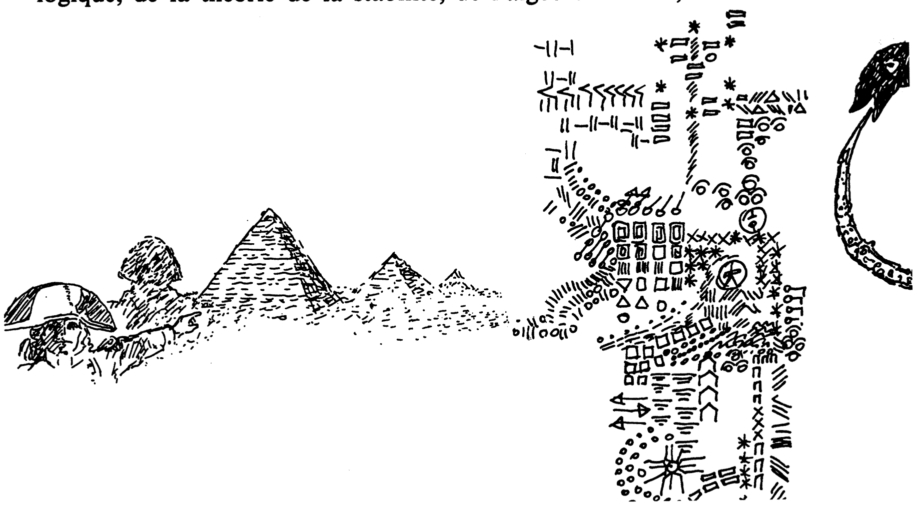
Naturellement les automates ont aussi leurs illuminés dont le zèle finit par s'éteindre dans le moëlleux des chaires. On ne chante plus cette mesure de toute les complexités du monde qui était basée sur la décomposition en groupe simple (combinés par produit en couronne) bien qu'elle fit florès il y a dix ans. N'est-ce pas, Arbib ?

Mais le théorème de Rhodes survit au reflux de la mode. Il y avait une tentative d'imposture, mais dont le fondement n'était pas le vide absolu car nous étions dans le domaine des mathématiques.

De nouveau je demande pourquoi la G.S.T. fait tant référence à mon ami McNaughton dont le théorème (superbe) ne concerne que des problèmes posés et résolubles dans un cadre délimité avec une rigueur si efficace que tout affaiblissement des hypothèses le réduit à néant ?

Peut-être par métaphore ? Voyons un peu. Qu'elle idée a suscité chez ceux d'entre vous qui ne connaîtraient point la théorie des automates, le terme charmant de **produit en couronne** ? Erreur, vous êtes sur une fausse piste. La seule allusion valable était aux sous-groupes de Sylow du groupe symétrique. Peut-être comprenez-vous mieux maintenant ce que j'entends par le mot imposture.

On pourrait continuer et vérifier que pour chacun des chapitres des mathématiques, l'emploi fait par celui-ci en G.S.T. ne relève que de la rhétorique des commissions de budgets. Ceci bien sûr pour les chapitres qui existent, puisqu'il faut préciser que **rien** en mathématiques n'est désigné par des noms ronflants tels que cybernétique ou théorie des hiérarchies. Et comme cet essai est une critique du livre de D. Berlinski, j'y fais référence par des exemples hilarants que cet auteur fournit sans effort à propos de la logique, de la théorie de la stabilité, de l'algèbre linéaire, etc.



# *Conclusions provisoires*

Tristes. (Que de jeunes talents ou pire d'enthousiasmes dans les Instituts de recherches...). A chaque ligne, je me suis retenu de citer un ami ou un autre dont je partage les espoirs de voir un jour la mathématique informer de nouveaux domaines et contribuer selon son mode propre à les mettre aux services des hommes. L'auteur du livre que nous commentons ici mérite qu'on le respecte.

Mais la connaissance ne se nourrit pas de la fumée des bonnes intentions et l'affirmation judicieuse que le tout contient les parties ne mérite de place à ses auteurs qu'au Panthéon de la Sagesse des Nations dont la clef fût en Chine. Bref, il faut tenter d'établir un bilan provisoire des faits ou théorèmes que nous devons à la G.S.T. Et on ne prendra pas en compte la diffusion (fût-elle crue utile) dans le vocabulaire des billets de Paris de termes courants dans les laboratoires (feed-back, optimisation, homéostat, decision process).

Pas plus que l'habitude touchante (et bien commode dans la pédagogie audiovisuelle) d'orner toute conférence de trois ou quatre boîtes noires se poursuivant au tableau de même couleur.

En psychologie ou en sociologie, je n'ai rien su voir dans les ouvrages que j'ai consultés : pris jusqu'au vertige de ce qui fût une mode en mathématique, les systémistes préfèrent la théorie à l'observation et la généralité à la preuve. Il y a plus de cinquante ans le Colonel Rimaillot notait qu'un homme ne peut guère en commander directement que quatre et discutait sous cet angle diverses structures sociales. La G.S.T. théorise les hiérarchies et les inter-relations mais je n'y trouve rien qui enrichisse ou précise ces premiers pas d'une science de l'organisation des micro-sociétés. En psychologie, la Gestalt Theorie avait été vite éteinte dans les laboratoires. La G.S.T. reprend le flambeau, mais hormis quelques études bien molles sur la psychologie des joueurs d'échecs, elle a élaboré des « modèles cognitifs » et des « paradigmes heuristiques » à l'aide de catégories ou de fonction non récursives, sans que les psychologues que nous fûmes y trouvent grand chose à ajouter à ce qui s'enseignait déjà il y a cinquante ans.

En biologie, la cybernétique a fait faillite sans avoir même commencé. Les manuels tchèques ou italiens ressassent toujours les mêmes expériences douteuses qui faisaient la joie du MIT dans les années cinquante et que l'on sait depuis avoir été encore plus mal interprétées que faites.

Peut-être, j'espère, je me trompe, et on saura me montrer toutes les découvertes admirables que j'ignore ou méconnais dans les sciences de l'homme ou dans celles de la vie. Peut-être aussi suis-je injuste et peut-être que les mathématiques de la psychanalyse Lacanienne procèdent directement de la G.S.T. ; certes et j'y joins en couronne celles du structuralisme parisien et de la sémiotique générale.

Mais je le répète, ceci paraît peu vraisemblable et la lecture des publications les plus récentes de la G.S.T. ne semble pas indiquer quelle ait accumulé quoique ce soit dans le domaine des connaissances empiriques car il n'y est jamais question que des mêmes fadaises péri ou paramathématiques sous-tendues ou non par les pieuses vaticinations écologiques ou illytchiennes. Des idées, des projets, des formules, mais point de fait.

Et nous voici revenus au même pôle. Il faut juger la G.S.T. comme une philosophie ou une discipline mathématique. Une ou des philosophies ? car il est bien difficile de tirer au clair qui l'exprime : Laszlo, Simon, Mesarovic, Bertalanffy ? qui pour l'essentiel s'ignorent les uns les autres et prêchent chacun pour son église sans discuter ni utiliser ce que dit son collègue ?

De toute façon, il est très mal vu depuis Athènes de vouloir juger un philosophe et je ne m'y aventurerai donc pas. Reste la mathématique. Je la tiens pour fausse ou triviale. De toute façon irrelevante aux buts déclarés. (... pour le confort des programmes furent envoyés labourer la glace...).

De nouveau j'espère que je me trompe et je supplie, que l'on me sorte du cauchemar dantesque de ce vol de chercheurs cantando lor lei et alignant depuis vingt ans un tourbillon de calculs imbéciles. Nous attendons donc avec impatience le rapport final que publieront les responsables du CNRS sur les résultats de l'action thématique en G.S.T. qu'il animent, (... et ne reviendront que meurtris). Et pour prendre patience relisons Berlinski. ***(On system Analysis ;*** MIT Press 1976).

# Année 1981

## Bibliographie

[1981-1] Alain Lascoux et Marcel-Paul Schützenberger. Le monoïde plaxique. In *Noncommutative structures in algebra and geometric combinatorics (Naples, 1978)*, volume 109 of *Quad. "Ricerca Sci."*, pages 129–156. CNR, Rome, 1981.

[1981-2] Alain Lascoux et Marcel-Paul Schützenberger. Polynômes de Kazhdan & Lusztig pour les grassmanniennes. In *Young tableaux and Schur functors in algebra and geometry (Toruń, 1980)*, volume 87-88 of *Astérisque*, pages 249–266. Soc. Math. France, Paris, 1981.

[1981-3] Dominique Perrin et Marcel-Paul Schützenberger. A conjecture on sets of differences of integer pairs. *J. Combin. Theory Ser. B*, 30(1) :91–93, 1981.

CONSIGLIO NAZIONALE DELLE RICERCHE

ALAIN LASCOUX & MARCEL P. SCHÜTZENBERGER

# Le monoïde plaxique

Estratto dalla collana
**Quaderni de 'La ricerca scientifica', n. 109**
*Non–commutative structures in Algebra and Geometric Combinatorics*
ROMA, CNR, 1981

# Le monoïde plaxique

**ALAIN LASCOUX & MARCEL P. SCHÜTZENBERGER**
**Laboratoire d'Informatique Théorique et Programmation, Université – Paris (France)**

**Riassunto** – *Monoide 'a placche'.*

**La descrizione combinatoria delle rappresentazioni dei gruppi simmetrico e lineare si basa sulle tavole di Young. Un progresso decisivo è stato quello di munire l'insieme delle tavole di una moltiplicazione. Noi sviluppiamo questo punto di vista e diamo le principali proprietà del monoide 'a placche', che hanno molteplici e varie applicazioni (rappresentazione dei gruppi lineari finiti, algebre di Hecke, coomologia delle varietà 'a bandiere').**

## 1 – Préface.

L'étude du monoïde plaxique se situe dans la lignée de plusieurs théories mathématiques développées plus ou moins indépendamment en algèbre et en géometrie.

On peut remonter à un texte de Jacobi (*De Alternantibus*...) ainsi qu'à un exercice destiné aux élèves de l'Ecole Polytechnique dû à Cauchy, où sont introduites les fonctions symétriques fondamentales comme des quotients de fonctions antisymétriques par la plus simple de ces dernières, le déterminant de Vandermonde. Le sujet est alors traité comme branche des 'alternants' à l'intérieur de la vaste famille des 'déterminants'. Kostka calcule en 1880 les premières tables de décomposition des fonctions symétriques, indiquant ainsi les problèmes numératifs attachés à ces fonctions.

Partant d'une toute autre source, Pieri en 1873, et Schubert, quelque quinze ans plus tard, suivis d'autres géomètres énumératifs, se lancent dans l'étude de ce qui sera appelé de nos jours l'anneau de cohomologie des grassmanniennes. De grands progrès sont dûs à Giambelli qui met clairement à jour le lien entre les problèmes d'énumération 'degli spazi secanti' et les fonctions symétriques.

Troisième apport, celui de Schur dont les travaux sur la représentation des groupes linéaires en 1901, prolongeant l'oeuvre de Frobenius, montrent que les représentations irréductibes sont en bijection avec la base fondamentale des fonctions symétriques, celle–là même introduite par Jacobi, à laquelle on attachera désormais son nom : pour chaque matrice, la trace de son image dans une représentation irréductible est la fonction symétrique correspondante de ses valeurs propres. L'indexation de ces objets est assurée par les partitions dont quelques propriétés combinatoires connues depuis Euler commencent à prendre une signification mathématique.

A cette époque, les problèmes de la théorie des représentations sont souvent traités dans le langage spécialisé des invariants, ce qui signifie que l'on étudie l'action conjointe des groupes linéaires et symétriques sur les produits tensoriels d'espaces vectoriels. C'est le point de départ de Young qui introduit les fameux objets combinatoires, les *tableaux*, pour coder de façon merveilleusement efficace les idempotents des algèbres du groupe symétrique et des représentations. Premier enrichissement, et combien décisif de la notion de partition, qui devient dès lors la *forme* des tableaux de Young.

Le livre classique de Littlewood marque une étape nouvelle. Il intègre une foule de travaux partiels en ramenant systématiquement l'étude des représentations des groupes classiques à celle des fonctions symétriques associées. Il montre de plus très explicitement comment les fonctions de Schur des puissances d'une variable $q$ peuvent fonder ce calcul des '$q$–analogues' ; cette méthode ne sera comprise que beaucoup plus tard.

Le calcul des fonctions symétriques se formule aujourd'hui de façon adéquate dans le cadre de la théorie des $\lambda$–anneaux qui permettent d'y réintégrer la cohomologie des grassmanniennes.

Un rôle singulier est joué par la célèbre règle de Littlewood–Richardson (1934) qui illustre une nouvelle extension des tableaux de Young et suggère qu'ils se rattachent à des structures algébriques plus riches. Indépendamment, Specht (1935) et Hodge (1942) montrent que les tableaux peuvent être considérés comme une base, pour le premier, d'un module de représentation du groupe symétrique, pour le second, de l'espace des 'formes polynomiales' sur une variété de Schubert. Ceci conduira aux 'bitableaux' développés avec succès par Rota, De Concini et Procesi.

Enfin, dernière source : les études purement combinatoires sur les tableaux. La construction de Robinson (1938), redécouverte indépendamment et considérablement développée par Schensted (1961), met à jour une profusion de propriétés surprenantes dont les preuves sont souvent malaisées. Certaines, et c'est l'apport décisif de Schensted et de Knuth, rendent possible de munir l'ensemble des tableaux d'une structure de monoïde (non commutatif). D'autres font jouer des propriétés profondes des ensembles ordonnés finis : c'est le théorème de Greene. Dans les deux cas, le point de départ est le monoïde libre sur un alphabet totalement ordonné dont on considère un quotient remarquable, le monoïde plaxique, et l'agèbre engendrée par ce dernier, dans laquelle on définit des fonctions de Schur non commutatives.

On se propose de réintroduire des opérations 'naturelles' qui compensent la perte de l'invariance des méthodes classiques de l'algèbre linéaire en relevant les opérations classiques sur les fonctions symétriques. Il en résulte un calcul plus compliqué, mais plus riche, puisque les variables satisfont des lois de commutativité extrêmement spéciales.

On trouvera dans les pages suivantes les principales propriétés du monoïde plaxique telles que nous les connaissons aujourd'hui et telles que nous y ont mené une série de recherches sur les polynômes de Foulkes/Green et les produits de Kronecker des représentations. Nous avons laissé de côté nombre de propriétés qui sont encore sans applications.

Il nous a paru inutile de reécrire la partie proprement combinatoire qui est traitée en détail et dans un autre esprit dans l'exposé [L&S 1], où le lecteur pourra trouver une bibliographie complète, et des références à divers travaux intéressants dans des domaines liés. Pour ce qui est des deux auteurs, on se réfèrera dans ce qui suit à

[L&S 1] Schützenberger, M. P. : « La Correspondance de Robinson », in *Combinatoire et représentation du groupe symétrique*, *Springer Lect. Not.*, n° 579, (Strasbourg, 1976).

[L&S 2] Lascoux, A. : « Calcul de Schur et extensions grassmanniennes des $\lambda$–anneaux », même volume que [L&S 1].

[L&S 3] Schützenberger, P. M. : *Propriétés nouvelles des tableaux de Young*, *Séminaire Pisot 1978* (Paris, 1978).

[L&S 4] Lascoux, A. & Schützenberger, M. P. : « Croissance des polynômes de Foulkes–Green », *C.R. Acad. Sci. Paris*, **288**, 95–98 (1979).

[L&S 5] Lascoux, A. & Schützenberger, M. P. : « A new statistics on words », in *Proceedings de Fort Collins 1978* (à paraître).

[L&S 6] Lascoux, A. : « Produit de Kronecker des représentations du groupe symétrique », in *Séminaire Dubreuil–Malliavin 1978–1979*, *Springer Lect. Not.* (à paraître).

A la bibliographie de [L&S 1] il faut ajouter

Garsia, A. & Gessel, I. : « Permutations statistics and partitions », *Adv. Math.*, **31**, 288–305 (1979).

Thomas, G. : « On Schensted's construction and the multiplication of Schur functions », *Adv. Math.*, **30**, 8–30 (1978).

White, D. E. : « Some connections between the Littlewood–Richardson rule and the construction of Schensted », preprint 1979.

Il faudrait enfin mentionner la théorie des groupes linéaires finis, des algèbres de Hecke, de la cohomologie des variétés drapeaux sur les corps finis, mais malheureusement, la plupart de ces travaux sont écrits dans un langage trop spécialisé pour être facilement accessible. Le livre de Macdonald, cité en fin de texte, qui reprend le point de vue de Littlewood et le langage élémentaire des fonctions symétriques, remplira en grande partie cette fonction (quoique le monoïde plaxique n'y figure point !).

## 2 – L'équivalence plaxique.

Dans tout ce mémoire, $(A, \leqslant)$ est un alphabet fini totalement ordonné et $A^*$ le monoïde libre qu'il engendre. L'évaluation d'un mot est l'image de ce mot par le morphisme naturel de $A^*$ sur le monoïde commutatif libre de même base, noté $\mathbb{N}^A$.

Le *monoïde plaxique* est le quotient de $A^*$ par une certaine congruence $\equiv$ faisant que deux lettres commutent quand elles sont suivies ou précédées d'une troisième qui se trouve entre elles pour l'ordre de l'aphabet. De façon plus précise, la *congruence plaxique* est définie par les conditions suivantes qui sont dûes à Knuth [3] :

**2.1** – Si $x < y < z$ sont trois lettres, alors :

$$z\,x\,y \equiv x\,z\,y \quad \text{et} \quad y\,z\,x \equiv y\,x\,z$$

Si $x < y$ sont deux lettres, alors :

$$y\,x\,x \equiv x\,y\,x \quad \text{et} \quad y\,y\,x \equiv y\,x\,y$$

Il est clair que deux mots congrus pour $\equiv$ ont même évaluation. On voit aussi que les deux dernières relations sont les images des premières par les morphismes $\varphi : A^* \to A^*$ tels que, respectivement, $x\,\varphi = y\,\varphi$ et $y\,\varphi = z\,\varphi$. Par conséquent, le morphisme naturel de $A^*$ sur $A^*/\equiv$ commute avec l'évaluation et avec tout morphisme injectif $\varphi : A^* \to B^*$ envoyant $A$ dans la base $B$ de $B^*$ et respectant l'ordre. Un tel morphisme sera dit *alphabétique*.

Deux autres propriétés utiles découlent immédiatement de la définition.

**2.2** – Soit $B$ un intervalle de $A$. Il définit un morphisme $w \to w \cap B^*$ envoyant chaque mot $w$ sur son plus long sous–mot dans $B^*$ ('effacement' des lettres de $A \setminus B$). Un tel morphisme est dit *morphisme de restriction*, et l'on voit aisément que les relations (2.1) commutent avec les morphismes de restriction aux intervalles.

**2.3** – Soit d'autre part $w \to \tilde{w}$ l'antiautomorphisme $A^* \to A^*$ envoyant chaque mot $w = x_1\,x_2 \dots x_n$ sur son *retourné* $\tilde{w} = x_n \dots x_2\,x_1$ $(x_i \in A)$ et $\#$ l'involution $A \to A$ telle que $x \leqslant y$ ssi $y^{\#} \leqslant x^{\#}$ pour toutes les paires de lettres $x$, $y$ de $A$. On étend ce dernier à un antiisomorphisme $\# : A^* \to A^*$ en posant $w\,\# = x_n{}^{\#} \dots x_1{}^{\#}$.

On voit immédiatement que les congruences (2.1) sont échangées par $\#$. Donc $w \equiv w'$ équivaut à $w\,\# \equiv w'\,\#$ identiquement. Il n'en est pas de même pour le retournement $\sim$, puisque par exemple, si $x < y$, on a $y\widetilde{xx} = xxy$ mais $y\widetilde{xy} = xyx \not\equiv xxy$. Par contre, si par exemple $x < y < z$, on a bien $z\widetilde{xy} = yxz \equiv yzx = x\widetilde{zy}$. Rappelant qu'un mot *standard* est un mot dans lequel chaque lettre apparait une fois au plus, on a donc que le retournement commute avec la congruence plaxique pour les mots standards.

**2.4** – Ceci conduit à introduire une opération dite de *standardisation* associant un mot standard à tout mot $w$ de $A$. Pour cela, on indexe les diverses occurence de chaque lettre dans $w$ par un indice $i = 1, 2, \dots$ de gauche à droit. Le mot résultant, Stand$(w)$, est un mot standard sur l'alphabet $A \times N$ ordonné lexicographiquement.

Par exemple, si $w = b\,a\,a\,c\,b$ on a Stand$(w) = b1\ a1\ a2\ c1\ b2$. Il est immédiat que si deux mots $w$ et $w'$ ne différent que par l'une des congruences élémentaires plaxiques (2.1), on a encore Stand$(w) \equiv$ Stand$(w')$.

Les diverses propriétés que nous venons de décrire sont rassemblées dans l'énoncé suivant :

2.5 – **Proposition :**

La congruence plaxique commute à l'évaluation, à l'involution $\#$, aux morphismes de restriction aux intervalles et à la standardisation.

2.6. – L'intérêt du monoïde plaxique est lié au fait qu'il possède une section remarquable ; l'image de cette section est l'*ensemble des tableaux* $T$ que nous décrivons ci–après. On appelle *redressement* et on note $R$ l'application $A^* \to T$ envoyant chaque mot $w$ sur l'unique tableau $wR \in T$ auquel il est congru. En d'autres termes, $tR = t$ si le mot $t$ est un tableau, et $w \equiv w'$ ssi $wR = w'R$.

2.7 – Il est commode d'appeler *ligne* (resp. *colonne*) tout mot $v = x_1 x_2 \dots x_k$ dont les lettres $x_i$ vont en croissant, c'est–à–dire satisfont $x_1 \leqslant x_2 \leqslant \dots x_k$ (resp. $x_1 > > x_2 > \dots x_k$).

Soit une lettre $x$ et une ligne $v$ ; si $vx$ n'est pas une ligne, alors $v = v' \, y \, v''$ avec $v' = x_1 \dots x_i$, $x_i \leqslant x$ et $y > x$.

On vérifie facilement que les relations plaxiques (2.1) entrainent

$$v\,x \equiv y\,v'\,x\,v''.$$

Par exemple, $(bcdde)\,c \equiv d\,(bccde)$.
De même, si $u$ est une colonne :

ou bien $x\,u$ est une colonne,
ou bien l'on a $u = u'\,y\,u''$, $u'x$ colonne, $y \leqslant x$

et alors,

$$x\,u \equiv u'\,x\,u''\,y$$

En particulier $x\,u \equiv u\,x$ lorsque $x$ est une lettre de $u$.

Ces règles de 'multiplication' ont été découvertes par Schensted [7] auquel on doit les premiers résultats importants de toute cette théorie. Le cas de commutation d'une lettre et d'une colonne se généralise en

2.8 – *Remarque :* Deux colonnes commutent si et seulement si l'une est un sous–mot de l'autre.

2.9 – Appelons *forme* d'un mot $w$ la suite $\overline{w}|$ des longueurs de ses lignes (i.e. des facteurs maximaux qui sont des lignes). Par exemple, la forme de $t = debccdaabc$ est 2 4 4, puisque les lignes de $t$ sont $de$, $bccd$ et $aabc$. Ceci posé, un mot $t$ est un *tableau* ssi d'une part sa forme est une suite croissante au sens large (i.e. une partition), d'autre part, pour chaque $i$, le sous mot formé des $i$–ièmes lettres de chaque ligne de $t$ est une colonne. Par exemple, le mot $t$ ci–dessus est un tableau dont les sous–mots–colonnes sont $dba$, $eca$, $cb$ et $dc$.

Ceci se voit plus facilement quand on emploit l'écriture plane d'un tableau obtenue en disposant ses lignes les unes au dessus des autres, en commençant sur la même colonne :

$$t =: \begin{matrix} d\ e & & & \\ b\ c\ c\ d \\ a\ a\ b\ c \end{matrix}$$

Le diagramme des points occupés par les lettres de $t$ est classiquement dit *diagramme de Ferrers* de la partition $\overline{t\,|}$ de la longueur $|\,t\,|$ de $t$ ; l'écriture planaire d'un tableau fournit l'objet combinatoire classique dit *tableau de Young*. Les règles de Schensted (2.7) donnent un moyen commode de trouver le tableau équivalent au produit d'un tableau par une lettre, donc par induction, de redresser (au sens 2.6) tout mot.

Par exemple, pour le tableau ci–dessus,
$t\,b =: de\ bccd\ aabc\ b \equiv de\ bccd\ c\ aabb \equiv de\ d\ bccc\ aabb \equiv e\ dd\ bccc\ aabb =: (tb)\,\boldsymbol{R}$, ce dernier tableau ayant l'écriture plane

$$\begin{matrix} e & & & \\ d\ d \\ b\ c\ c\ c \\ a\ a\ b\ b \end{matrix}$$

On notera que les règles de Schensted impliquent qu'un tableau soit congru au produit de ses sous–mots–colonnes (pour l'exemple, $t \equiv dba\ eca\ cb\ dc$), et c'est à partir de cette écriture d'un tableau qu'on peut facilement le multiplier sur la gauche par une lettre.

Nous renvoyons au Colloque de Strasbourg [L&S 1] pour plus de détails sur les propriétés classiques des tableaux, et nous nous bornons ici à énoncer

**2.10** – Théorème de la section :

L'ensemble des tableaux est une section de la congruence plaxique, c'est–à–dire, dans chaque classe d'équivalence, il y a un tableau et un seul.

**2.11** – Les relations entre la forme d'un tableau et celle de son produit par une ligne ou une colonne sont contenues dans le Théorème de Pieri. En voici tout d'abord le cas le plus simple

Théorème de Pieri pour une lettre :

Si $t$ est un tableau et $x$ une lettre, la forme de $(tx)\,\boldsymbol{R}$ et la forme de $(xt)\,\boldsymbol{R}$ sont obtenues en ajoutant un point au diagramme de $t$. Réciproquement, si $\boldsymbol{I'}$ est le diagramme d'une partition obtenu enlevant un point à $\overline{t\,|}$, il existe des factorisations uniques $t \equiv t'\,x'$ et $t \equiv x''\,t''$ telles que $x'$, $x''$ soient des lettres et $t'$, $t''$ des tableaux de forme $\boldsymbol{I'}$.

Par exemple, si $\overline{t\,|} =: (\mathbf{2, 4, 4})$ comme ci–dessus, $\boldsymbol{I'}$ ne peut être que $(\mathbf{1, 4, 4})$ ou que $(\mathbf{2, 3, 4})$ et pour chacune de ces formes, on trouve les factorisations (uniques !) de $t =: debcc\,aab\cancel{d}$ :
d c

$$t \equiv (d\,bcce\,aabd)\,c \equiv d\,(e\,bccd\,aabc)$$

et

$$t \equiv (de\,bcc\,aabd)\,\cancel{d}_{c} \equiv b\,(de\,ccd\,aabc).$$

Si $t \equiv x\,t'$, avec $x \in A$, on posera $(x, t') =: t\,\gamma^h$ où $h$ est l'indice de la ligne de $t$ qui est plus courte que celle de $t'$ (en convenant que $t\,\gamma^h =: \varnothing$ si l'opération n'est pas possible, c'est-à-dire si la ligne d'indice $h+1$ de $t$ n'est pas strictement plus courte que celle d'indice $h$). Plus généralement, on écrira

$$(x_1\,x_2 \dots x_n,\, t'') =: t\,\gamma^{h_1\,h_2 \dots h_n}$$

où $\gamma^{h_1 \dots h_n}$ désigne le produit des opérateurs $\gamma^h$.

**2.12 – Théorème de Pieri :**

Soit $(x_1 \dots x_n,\, s) =: t\,\gamma^{h_1 \dots h_n}$. Alors le mot $x_1 \dots x_n$ est une ligne si et seulement si $h_1 \leqslant h_2 \leqslant \dots h_n$ et une colonne si et seulement si $h_1 > h_2 \dots > h_n$.

Inversement, si $w =: x_1 \dots x_n$ est une ligne (resp. colonne) et $s$ un tableau, il existe suite (unique) d'entiers $h_1, .., h_n$ telle que

$$t\,\gamma^{h_1 \dots h_n} =: (w,\, s),$$

où $t =: (w\,s)\,R$.

Il n'y a pas que la factorisation par une ligne ou une colonne que l'on sache décrire :

**2.13 – Lemme de la petite équerre :**

Soient des entiers $h_1 > h_2$ et un tableau $t$ tel que $t\,\gamma^{h_1} =: (y,\, s)$ et $t\,\gamma^{h_2} =: (y',\, s')$. Alors on a $y \geqslant y'$ et il existe $h_3$ satisfaisant $h_1 > h_3 \geqslant h_2$ pour lequel $t\,\gamma^{h_1\,h_2\,h_3} \neq \varnothing$ ; pour de tels $h_3$ : Si $y =: y'$, on a $t\,\gamma^{h_1\,h_2\,h_3} =: (y\,x\,z,\ s'')$ et $t\,\gamma^{h_2\,h_1\,h_3} =: (y\,z\,x,\ s'')$ où $x < y \leqslant z$ (et donc $y\,x\,z \equiv y\,z\,x$), sinon $t\,\gamma^{h_1\,h_2\,h_3} =: (y\,y'\,x,\ s'')$ et $t\,\gamma^{h_2\,h_1\,h_3} =: (y'\,y\,x,\ s'')$ où $y \geqslant x > y'$ (et donc $y\,y'\,x \equiv y'\,y\,x$).

**2.14** – Notons $L^{(k)}$ l'ensemble des mots qui envisagés comme suite de lettres sont union disjointe de $k$ lignes. $L^{(1)}$ est simplement l'ensemble $L$ des lignes et $L^{(k)}$ le *produit de schuffle* de $k$ fois $L$. Ainsi $c\,b\,e\,a\,d\,c\,c$ appartient à $L^{(3)}$ puisqu'il est produit de schuffle des trois lignes *ce*, *bd* et *acc* (et aussi bien, de *ce*, *bcc* et *ad*, etc...).

La *forme immanente* d'un mot $w$ est la suite $(m_k, \dots, m_2, m_1)$ telle que $m_i + \dots + m_2 + m_1$ soit la longueur maximale des sous-mots de $w$ qui appartiennent à $L^{(i)}$. La forme immanente d'une ligne (resp. colonne) de longueur $n$ est donc $(n)$ (resp. $(1, 1, \dots 1)$). Plus généralement, la forme immanente d'un tableau est simplement sa forme (cfr. 2.9).

On vérifierait que, par exemple, la forme immanente de *dbaedabc* est $(2, 2, 4)$ en raison des sous-mots $aabc \in L^{(1)}$ et $badabc \in L^{(2)}$. Une conséquence assez surprenante du théorème de Greene [2] est que $m_1 \geqslant m_2 \geqslant \dots$

**2.15 – Théorème :**

La congruence plaxique est la plus grande congruence $\equiv$ sur $A^*$ telle que pour chaque paire de mots $w$, $w'$ on ait $w \equiv w'$ si et seulement si pour tout $u$, $v \in A^*$ les mots $u\,w\,v$ et $u\,w'\,v$ ont même forme immanente.

Nous donnons enfin une troisième caractérisation de la congruence plaxique qui fait percevoir ses liens avec la théorie des fonctions symétriques. Soit $Z(A^*)$ l'algèbre libre engendrée par $A$. A chaque entier $n \geqslant 0$, on associe la somme $S(1^n)$ de toutes les colonnes $x_n\,x_{n-1} \ldots x_1$ $(x_n > x_{n-1} > \ldots x_1)$ de longueur $n$. Son image dans l'algèbre commutative libre est la fonction de Schur l'indice $1^n$. On sait que dans l'algèbre $Z(A^*/\equiv)$ du monoïde plaxique, on a identiquement

$$S(1^n)\,S(1^m) \equiv S(1^m)\,S(1^n) \qquad (m, n \geqslant 0).$$

**2.16 – Théorème :**

La congruence plaxique est la plus petite congruence sur $\equiv$ $A^*$ commutant à l'évaluation, aux morphismes injectifs d'alphabets ordonnés et aux morphismes de restriction aux intervalles, et telle que les $S(1^m)$ engendrent une sous-algèbre commutative de $Z(A^*/\equiv)$.

*Remarque :* on dit, en théorie des monoïdes d'alphabets totalement ordonnés, qu'une relation d'équivalence est *naturelle* si elle est préservée par tout morphisme d'alphabet injectif et croissant $A \to B$ ; on a donc que la congruence plaxique est naturelle.

*Démonstration du théorème :*

Nous vérifierons seulement que les conditions figurant dans l'énoncé du théorème suffisent à déterminer la congruence plaxique.

Soient trois lettres $x<y<z$. L'équation

$$S(1)\,S(11) \equiv S(11)\,S(1)$$

se décompose suivant l'évaluation, et après élimination des termes identiques, les équations de plus bas degré que l'on obtient sont :

(1) $$x\,y\,x \equiv y\,x\,x$$

(2) $$y\,y\,x \equiv y\,x\,y$$

(3) $$x\,z\,y + y\,z\,x \equiv z\,x\,y + y\,x\,z$$

Cette dernière congruence implique :

ou bien

(3′) $$x\,z\,y \equiv z\,x\,y \quad \text{et} \quad y\,z\,x \equiv y\,x\,z$$

ou bien

(3″) $$x\,z\,y \equiv y\,x\,z \quad \text{et} \quad y\,z\,x \equiv z\,x\,y$$

Le premier cas [relations (1), (2) et (3′)] constitue bien l'ensemble des relations plaxiques (2.1). On élimine le second cas, c'est–à–dire la relation (3″), par la condition de restriction aux intervalles, puisque en prenant le plus petit intervalle contenant $x$ et $y$ (c'est–à–dire en effaçant $z$), on devrait avoir $x\,y \equiv y\,z$.

Il est remarquable que le deuxième système de congruences [(1), (2) et (3″)] implique aussi que les $S(1^m)$ engendrent une sous–algèbre commutative. La vérification repose sur la remarque que deux mots standards sont congrus si et seulement si d'une part, ils ont le même nombre d'inversion, et d'autre part, le sous–mot des deux lettres extrèmes (pour l'ordre sur $A$) est le même. Par exemple, la classe de $a\,d\,b\,c$ pour la congruence (3″) est composée de, outre *adbc*, *acdb*, *badc*, *bcad*, *cabd*.

**2.17** – Nous donnons maintenant une propriété importante de l'ensemble des mots dont le redressé est un tableau donné.

L'opération de standardisation a été définie en (2.4). A un changement d'alphabet près, on peut considérer le standardisé d'un mot comme une permutation de l'ensemble 1,..., $n$. Notons que le standardisé d'un tableau est un tableau ; inversement, pour chaque tableau standard donné, il existe au plus un tableau d'évaluation donnée dont il est le standardisé. Par exemple, le tableau 24 135 peut être le standardisé des tableaux *bd ace*, *bd acd*, *bc abd*, *bc abc* (ou des tableaux qui s'en déduisent par changement d'alphabet) puisqu'en passant de 1 à 2 et de 3 à 4, on doit passer d'une lettre à une lettre ultèrieure.

L'ensemble des mots dont un tableau standard est le redressé est beaucoup plus complexe, mais il a une structure remarquable. Pour le décrire, notons d'abord qu'un mot standard $w$ peut être considéré comme une permutation de son alphabet, et qu'on peut donc lui associer un mot standard $w^{-1}$ (sur le meme ensemble de lettres).

Le *Ia–symbole*, $w\mathfrak{R}$, d'un mot $w$ est le tableau standard obtenu en redressant l'inverse du standardisé de $w$.

**2.18** – Théorème (Cauchy, G. de B. Robinson – cfr. [L&S 1], p. 88)

L'application $w \to (w\,R,\ w\,\mathfrak{R})$ est une bijection de l'ensemble des mots sur les paires de tableaux de même forme, le deuxième étant standard (d'évaluation 1 2 ... $|w|$).

Par exemple, il y a cinq mots standards dont le redressé est
$$\begin{matrix} 2\,4 & \\ 1\,3\,5 \end{matrix}\ .$$

Ce sont :

**24513** , **14253** , **24135** , **21453** , **21435** ,

dont les *Ia–symboles* respectifs sont

$$\begin{matrix}4\,5\\1\,2\,3\end{matrix}\ ,\quad \begin{matrix}3\,5\\1\,2\,4\end{matrix}\ ,\quad \begin{matrix}3\,4\\1\,2\,5\end{matrix}\ ,\quad \begin{matrix}2\,5\\1\,3\,4\end{matrix}\ ,\quad \begin{matrix}2\,4\\1\,3\,5\end{matrix}$$

et ces derniers tableaux constituent bien l'ensemble des tableaux standards de forme (2,3).

**2.19 – Propriété :**

Soix $w\,x$ $(x \in A)$ un mot de longueur $n$. Le *Ia–symbole* de $w$ est la restriction à $\{1,\ldots, n-1\}$ de celui de $w\,x$.

Comme les formes de $w\,x\,\text{Я}$ et $w\,\text{Я}$ sont respectivement égales à celle de $w\,x\,\boldsymbol{R}$ et $w\,\boldsymbol{R}$, ceci montre que $(wx)\,\text{Я}$ est obtenu en ajoutant le chiffre $n$ au point du diagramme de $(wx)\boldsymbol{R}$ qui n'est pas dans $w\boldsymbol{R}$.

**2.20 – Propriété :**

Deux mots ayant meme Я–symbole ont même forme.

*Preuve :*

Une file d'un mot est un sous–mot maximum croissant dont l'alphabet est un intervalle de $A$. On vérifie que la forme $(m_1, m_2, \ldots\, m_k)$ d'un mot est égale à la suite des longueurs des files de son Я–symbole, celles–ci étant ordonnées par ordre croisant de leur première lettre. □

Par exemple, le mot $b\;a\;a\;c\;a\;d\;c$ a la forme $1\;3\;2\;1$. Son Я–symbole est $\begin{array}{l} 2\;5\;7 \\ 1\;3\;4\;6 \end{array}$ dont les files successives sont (1), (234), (56), (7).

**2.21 – Propriété :**

Si $w$ est un mot standard, le redressé du retourné $\tilde{w}$ de $w$ est le tableau transposé du tableau $w\,\boldsymbol{R}$ (c'est–à–dire le tableau obtenu en échangeant les lignes et les colonnes).

Par exemple, si $w = 2\;4\;5\;1\;3$, son redressé est $\begin{array}{l} 2\;4 \\ 1\;3\;5 \end{array}$ et celui de $\tilde{w}$ est $\begin{array}{l} 5 \\ 3\;4 \\ 1\;2 \end{array}$.

La propriété la plus anciennement connue de monoïde plaxique apparait dans la 'Règle de Littlewood–Richardson' dont nous donnons ici une version améliorée. Le produit extèrieur des représentations des groupes symétriques induit une multiplication sur les sommes de partition ; les coefficients de structure sont des entiers non négatifs, dits aussi *coefficients de multiplication des fonctions de Schur*, que nous relions à l'opération de schuffle.

**2.22 – Théorème** (Littlewood–Richardson, cfr. [L&S 6]) :

Soit $t'$, $t''$ deux tableaux tels que $x' < x''$ pour toute paire de lettres figurant respectivement dans $t'$, $t''$, et soit $I = \overline{t'}\,|$, $J = \overline{t''}\,|$. Alors il existe un ensemble fini de tableaux $T_{I,J}$ tels que

$$\{t'\,\boldsymbol{R}^{-1} \sqcup\!\sqcup\, t''\,\boldsymbol{R}^{-1}\} = \{t\,\boldsymbol{R}^{-1} : t \in T_{I,J}\}.$$

Le nombre des tableaux de forme $K$ dans $T_{I,J}$ est la constante de structure d'indice $K$ dans le produit des fonctions de Schur d'indices respectifs $I$ et $J$.

COROLLAIRE :

Cette constante est donc le nombre de tableaux de forme $K$ dans l'ensemble de mots $\{t' \boldsymbol{R}^{-1} \sqcup\!\sqcup\, t'' \boldsymbol{R}^{-1}\}$.

(On note $\sqcup\!\sqcup$ l'opération de schuffle, shuffle en anglais, qui a été introduite en (2.14).

En combinant le théorème de Cauchy (2.18) avec la deuxième définition de la congruence plaxique (2.15), on obtient la

**2.23** – PROPRIÉTÉ :

Soit $(m_k,\dots, m_1)$ la forme immanente d'un mot $w$. Pour chaque permutation $(m'_k,\dots, m'_1)$ de celle–ci, il existe un et un seul mot $w'$ congru à $w$ dont la forme est $(m'_k,\dots, m'_1)$.

Par exemple, la forme ($=$ 2,4, 4)) de $w =$ *de bccd aabc* est égale à sa forme immanente, puisque $w$ est un tableau. On trouve que $w$ est congru à *bcde cd aabc* et *bcde aacd bc*, ces deux mots ayant pour formes respectives (4,2,4) et (4,4,2).

Il resulte en particulier de cette propriété que chaque tableau $t$ de forme $(m_k,\dots, m_2, m_1)$ est le redressé d'un (et d'un seul) mot $s$ de forme $(m_1, m_2,\dots, m_k)$. On montre que pour tout $i$ le sous–mot de $s$ formé des $i$–èmes lettres de chaque ligne (comptées à partir de la droite) est une colonne, ceci permet une écriture plane que l'on appelera un *antitableau.*

L'exemple ci–dessus montre que l'antitableau associé au tableau de *bccd aabc* est *bcde aacd bc* que l'on peut écrire planairement :

$$\begin{array}{llll} b & c & d & e \\ a & a & c & d \\ & b & c. & \end{array}$$

Soit un mot $w$, $B$ l'ensemble des lettres figurant dans $w$, et $\#_B$ l'antiisimorphisme de $B$ (cfr. 2.3). Il clair que $w$ est un tableau si et seulement si $w\#_B$ est un antitableau.

On note $t \to t \not\#$ l'involution sur l'ensemble des tableaux qui consiste à prendre l'image par $\#_B$ de l'antitableau associé ($B$ dépend du tableau considéré). Par construction, $t \not\#$ a même forme que $t$ lui–même.

**2.24** – PROPOSITION (cfr. [L&S 1], p. 94) :

Pour tout mot $w$, on a

$$(w\#)\,\boldsymbol{R} = (w\,\boldsymbol{R})\,\not\#$$

et

$$(w\#)\,Я = (w\,Я)\,\not\#$$

Ainsi, pour $w = bdaacaa$, on trouve

$$w\boldsymbol{R} = \begin{array}{llll} d & & & \\ b & c & & \\ a & a & a & a \end{array} \quad ; \quad w\,Я = \begin{array}{llll} 6 & & & \\ 3 & 4 & & \\ 1 & 2 & 5 & 7 \end{array} \quad ; \quad w\# = d\,d\,b\,d\,d\,a\,c \quad ;$$

$$(w\#)\,\boldsymbol{R} = \begin{array}{llll} d & & & \\ b & d & & \\ a & c & d & d \end{array} \quad ; \quad w\#\,Я = \begin{array}{llll} 6 & & & \\ 3 & 7 & & \\ 1 & 2 & 4 & 5 \end{array}$$

## 3 – Quelques propriétés algébriques du monoïde plaxique.

**3.1** – Une *partition* $I$ est une suite décroissante d'entiers $\geqslant 0$. On lui associe canoniquement l'élément du monoïde commutatif $N^A$ dans lequel le degré de la $j$–ième lettre de $A$ (pour l'ordre sur $A$) est $jI$ identiquement. Un tel élément, ainsi que les mots de $A^*$ dont il est l'évaluation seront dits *partitionnels*. Ainsi, à la partition 0 0 0 1 2 3 (lue de droite à gauche) est associé l'élément suivant de $N^A$, noté $a^3\, b^2\, c^1$: $a \to 3$, $b \to 2$, $c \to 1$, $x \to 0 \;\forall\; x > c$, qui est l'évaluation des mots de $A^*$ : *aaabbc*, *aababc*, *abaabc*,... Un mot est *homogène* sì et seulement si il a le même degré en toutes les lettres qui y figurent.

Le plus grand mot colonne homogène de degré 1 sera noté (ou $e_A$). Comme une lettre $x$ commute avec une colonne si et seulement si elle y figure, ainsi qu'on l'a vu en (2.8), on a la

**3.2** – Propriété :

Le centre de $A^*/\equiv$ est le sous–monoïde $e^*$.

Le quotient du monoïde plaxique par son centre sera désigné par $T/e^*$. Dans le cas où $A$ n'a que deux lettres, c'est un objet classique appelé *monoïde bicyclique* (cfr. [1] et [4]).

**3.3** – Si $g$ est une colonne, nous notons $\widehat{g}$ la colonne complémentaire formée des lettres n'apparaissant pas dans $g$. Ainsi, pour $A = \{1, 2, ..., 5\}$, la colonne complémentaire de $g = 4\,2$ est $\widehat{g} = 5\,3\,1$. La colonne complémentaire de $e = e_A$ est la colonne vide $\widehat{e} = e^0$ qui est l'élément neutre du monoïde libre $A^*$.

Plus généralement, soit $t$ un tableau. Ainsi qu'il a été dit en (2.9), il est congru au produit $g_1\, g_2 \dots g_r$ de ses mots–colonnes (lues de gauche à droite). Nous définissons le *complément* $\widehat{t}$ de $t$ comme le redressé du produit $\widehat{g}_r \dots \widehat{g}_2\, \widehat{g}_1$. En fait on vérifie facilement que $\widehat{g}_r, ..., \widehat{g}_1$ sont les colonnes successives de $\widehat{t}$. Par exemple, si

$$t = \begin{matrix} 5 & & & \\ 2 & 4 & & \\ 1 & 1 & 3 & 4 \end{matrix} \quad , \qquad \widehat{g}_4\, \widehat{g}_3\, \widehat{g}_2\, \widehat{g}_1 = 5321\;\; 5421\;\; 532\;\; 43$$

ce qui est bien le produit des colonnes de

$$\widehat{t} = \begin{matrix} 5 & 5 & & \\ 3 & 4 & 5 & \\ 2 & 2 & 3 & 4 \\ 1 & 1 & 2 & 3 \end{matrix} \quad .$$

Il est clair que $\widehat{t_1} = \widehat{t_2}$ quand $t_1$ et $t_2$ ne diffèrent que par le nombre de leurs colonnes complètes. Par conséquent, la complémentation $t \to \widehat{t}$ est une involution sur lui–même du quotient par son centre du monoïde plaxique.

**3.4 – Propriété :**

La complémentation est un antiisomorphisme de $T\,/\,e^*$ sur lui-même.

*Preuve :*

Soit $x$ une lettre. On vérifie que si $x'$ est une autre lettre, on a $x'\,\widehat{x} \equiv \widehat{x}\,x'$ si $x \neq x'$ et $x\,\widehat{x} = \widehat{x}_+\,x_+$ sinon (où $x_+$ est le successeur de $x$ dans $A$). Il s'en déduit que si les trois lettres $x$, $y$ et $z$ sont telles que $x \leqslant y < z$ on a $\widehat{y}\,\widehat{x}\,\widehat{z} \equiv \widehat{y}\,\widehat{z}\,\widehat{x}$ ; on vérifie pareillement les autres congruences plaxiques (2.1). Donc l'antiisomorphisme de $A$ sur lui-même envoyant chaque mot $w = x_1\,x_2 \dots x_n$ (avec $x_i \in A$) sur $\widehat{x}_n \dots \widehat{x}_2\,\widehat{x}_1$ préserve la congruence plaxique. Comme, par ailleurs, il est clair que si $w$ est une colonne, alors $\widehat{x}_n \dots \widehat{x}_1 \equiv e^{n-1}\,\widehat{w}$, ceci conclut le preuve.

On vérifie tout aussi aisément la

**3.5 – Propriété :**

L'involution $t \to \widehat{t}$ commute avec l'involution $t \to t\#$

**3.6** – Un *mot de Yamanouchi* est un mot dont tous les facteurs droits sont partitionnels. Un *tableau de Yamanouchi* est un mot de Yamanouchi qui est un tableau. On note $Y$ leur ensemble.

**3.7 – Propriété :**

(i) Pour chaque partition $I$, il existe un et un seul tableau $t = y_I$ de forme $I$ qui satisfasse l'une des cinq conditions équivalentes suivantes :

(1) les colonnes de $t$ sont des intervalles initiaux de $A$
(2) $t$ est partitionnel et chaque lettre ne figure que dans une seule ligne
(3) $t$ est partitionnel et ses colonnes commutent deux à deux
(4) $t$ a une évaluation égale à sa forme $I$
(5) $t$ est une tableau de Yamanouchi

(ii) l'application $I \to y_I$ est un isomorphisme du monoïde des partitions (considéré comme sous-monoïde de $N^A$) sur le monoïde $Y$, i.e. on a

$$y_{I+J} = (y_I\,y_J)\,R$$

où $I + J$ est la partition : $x\,(I + J) = xI + xJ$ pour tout $x \in A$

(iii) $(\widehat{t}\,t)\,R \in e^*$ si $t \in Y$

(iv) $Y$ est l'ensemble des tableaux $t$ tels que

$$(T\,t)\,R \cap e^* \neq \varnothing$$

(v) $Y\,R^{-1}$ est l'ensemble des mots de Yamanouchi.

*Preuve :*

Pour ce qui est de (i), l'équivalence de (1), (2), (3) et (4) est immédiate, de même que l'implication (2) ⇒ (5). Réciproquement, soit $v_h\, v_{h-1} \dots v_1$ la factorisation en lignes d'un tableau de Yamanouchi. Comme chaque ligne est un produit de lettres dans l'ordre croissant, la condition d'être un mot de Yamanouchi entraine que $v_1$ n'est composée que de $a$, puis $v_2$ que de $b$,..., ce qui montre que (5) implique (2) et achève la preuve de (i).

Celle de (ii) est un simple calcul dans le monoïde plaxique en raison de (3) et (1), et il en est de même de (iii).

Supposons maintenant que $(t'\, t)\, R = t'' \in e^*$ pour un certain tableau $t'$. Lre première ligne de $t''$ contient celle de $t$ qui doit donc être de la forme $a^m$. De même on voit que la deuxième ligne de $t$ est $b^n$, etc..., établissant ainsi (iv).

Pour finir, soit $x\, w$ $(x \in A)$ un mot de Yamanouchi ; à fortiori, $w$ est un mot de Yamanouchi, et par induction, on peut supposer que $w\, R \in Y$. En raison de (2), il en est de même pour $(x\, w)\, R$ puisque par hypothèse, le degré $|x\, w|_x$ de $x$ dans $x\, w$ est au plus égal au degré $|x\, w|_{x_-}$ de la lettre $x_-$ précédant $x$ (dans A). Réciproquement, soit $x\, w : (x\, w)\, R \in Y$ ; cette condition entraine que $w\, R \in Y$ et que $|x\, w|_x \leqslant$ $\leqslant |x\, w|_{x_-}$, et donc par induction, que $w$, $x\, w$ et tous les facteurs droits de $w$ soient partitionnels. □

**3.8** – Corollaire :

Le monoïde $T/e^*$ est simple, c'est–à–dire que pour tout $w \in A^*$, il existe $w'$, $w'' \in A^*$ tels que $(w'\, w\, w'') \in e^*$.

*Preuve :*

D'après (iii), il suffit de vérifier que pour chaque mot $w$ on peut choisir un élément $J$ de $N^A$ tel que $w\, d^{dJ} \dots b^{bJ}\, a^{aJ}$ soit partitionnel.

Nous mentionnons sans preuve la propreté suivante dans laquelle la condition donnée sur $t$ est facilement levée au moyen d'un morphisme injectif $A^* \to B^*$.

**3.9** – Propriété :

Soient $k + 1 =$ card $A$ et $t$ un tableau dans lequel chaque lettre de $A$ figure une fois au moins. Les propriétés suivantes sont équivalentes :

(1) $t \equiv t^2$ (mod $e^*$),

(2) $t \equiv s^k$ où $s$ est un tableau homogène qui contient toutes les lettres ; on a alors de plus $t \equiv s^{k+n}$ pour tout $n \geqslant 0$,

(3) $t \equiv s\, s'$, où $s$ et $s'$ sont deux tableaux tels que $s'\, s \equiv 1$ mod $e^*$ (et donc, $s$ est un tableau de Yamanouchi et $s'$ son unique inverse mod $e^*$),

(4) $t \equiv \Pi\, g_i\, \Pi\, \widehat{g}_i$, où $g_i$ est une colonne qui est un intervalle commençant (par la première lettre de $A$) et $\widehat{g}_i$ la colonne complémentaire, l'ordre des facteurs $g_i$ (resp. $\widehat{g}_i$) étant arbitraire.

D'après le point (4), en regroupant les colonnes égales, on voit donc que les idempotents (modulo le centre) sont en bijection avec $N^k$, et que deux idempotents commutent lorsque l'un est supérieur à l'autre (pour l'ordre de $N^k$).

Les propriétés algébriques du monoïde plaxique s'étendent sans difficulté à diverses généralisations de ce dernier. La plus simple consiste, pour un alphabet ayant un nombre *fini* $k$ de lettres, à prendre come 'tableau généralisé' les $k(k-1)/2$–tuples de réels non négatifs $(t_{ij})$ appartenant au polytope convexe $T$ défini par les inégalités :

$$0 \leqslant \Sigma\,\{t_{i+1,j} : 1 \leqslant j \leqslant j'\} \leqslant \Sigma\,\{t_{i,j} : 1 \leqslant j \leqslant j'\} \qquad (i =: 1, 2 \dots k{-}1\,;\ j' =: 1, \dots i).$$

La multiplication est alors une application continue $T \times T \to T$ linéaire par morceaux qui se réduit à l'opération $(t, t') \to (t\,t')\,R$ quand les $t_{ij}$ sont entiers.

## 4 – Automorphisme de conjugaison.

4.1 – On rappelle que dans tout semi–groupe $S$ la relation de *conjugaison* est la plus petite équivalence $\sim$ telle que $s'\,s'' \sim s''\,s'$ pour tout couple d'éléments de $S$. Cette relation est la relation habituelle quand $S$ est un groupe et elle n'est triviale que si $S$ est un semi–groupe commutatif. Nous vérifierons dans la section suivante qu'en ce qui concerne le monoïde plaxique les classes de conjugaison ont une structure remarquable et qu'elles sont les images inverses (par $Ev^{-1}$) des éléments du monoïde commutatif libre. Dans cette section, nous établissons un résultat préliminaire permettant de passer d'une classe à une autre.

Soit $\gamma_A$ le groupe symétrique sur $A$. Il a une représentation naturelle sur le groupe Aut $(N^A)$ des automorphismes du monoïde commutatif libre $N^A$ :

$$\text{si} \qquad \gamma_A \ni \sigma : A \to A \quad \text{et} \quad N^A \ni I : A \to N,$$

alors

$$\sigma I \quad \text{est le composé} \quad A \xrightarrow{\sigma} A \xrightarrow{I} N.$$

On obtient un relèvement naïf de cette représentation en une représentation de $\gamma_A$ dans le groupe des bijections de $A^*$, noté $Bij(A^*)$, en posant :

$$\text{si} \quad w =: x_1 \dots x_n \in A^*, \quad \sigma \in \gamma_A, \quad \text{alors} \quad w\,\bar{\sigma} =: (x_1\,\sigma) \dots (x_n\,\sigma).$$

Ce relèvement ne possède pas de bonnes propriétés vis–à–vis de la congruence plaxique. Nous en définissons un autre que nous appelons *relèvement plaxique*, et l'image de $\gamma_A$ par ce relèvement dans $Bij(A^*)$ est dit *groupe des automorphismes de conjugaison* de $A^*$, et noté Aut $(A^*)$. L'image de $\sigma \in \gamma_A$ dans Aut $(A^*)$ sera notée par la même lettre.

Nous devons procéder par étape en définissant d'abord le relèvement pour les transpositions de lettres consécutives.

4.2 – Soient $c$, $d =: c_+$ deux lettres consécutives, $B =: \{c, d\}$ et $\tau$ la transposition de ces deux lettres. On définit $w\,\tau$, pour $w \in B^*$ par

(1) $w\,\tau\,\text{ꓤ} = w\,\text{ꓤ}$

(2) le relèvement de $\tau$ est une bijection de $B^*$ telle que

$$\begin{array}{ccc} B^* & \xrightarrow{\ \tau\ } & B^* \\ {\scriptstyle \mathrm{ev}}\downarrow & & \downarrow{\scriptstyle \mathrm{ev}} \\ N^B & \xrightarrow{\ \tau\ } & N^B \end{array}$$

soit un diagramme commutatif.

La condition (2) signifie que si $|w|_c = m$, $|w|_d = n$, alors $|w\,\tau|_c = n$ et $|w\,\tau|_d = m$ ; il est clair que les deux conditions déterminent $w\,\tau$ et que $w = w\,\tau$ si et seulement si $w$ a même degré en $c$ et $d$.

4.3 – On étend $\tau$ en une bijection de $A^*$ dans $A^*$ par

(3) $\tau\text{ꓤ} = \text{ꓤ}$

(4) pour tout intervalle $B$ de $A$ tel que $\{B\,\tau\} = \{B\}$, alors

$$(w \cap B^*)\,\tau = (w\,\tau) \cap B^*$$

c'est–à–dire, $\tau$ commute aux morphismes de restriction aux intervalles globalement invariants.

*Preuve :*

On raisonne par récurrence sur le nombre de lettres de $A$ et l'on voit que si $w = x_1 \dots x_n$ et $w\,\tau = x'_1 \dots x'_{n'}$, alors $n = n'$, $x_i \neq c, d \Rightarrow x'_i = x_i$ et le sous–mot $w\tau \cap \{c, d\}^*$ est égal au mot $(w \cap \{c, d\}^*)\,\tau$ construit plus haut. □

Plus explicitement, on construit $w\,\tau$ comme suit :

si $w = x_1 \dots x_m\, d\, w_1\, c\, x_{m+1} \dots$, avec $w_1 \cap \{c, d\}^* = \varnothing$, alors

$$w\,\tau = x'_1 \dots x'_m\, d\, w_1\, c\, x'_{m+1} \dots$$

si et seulement si

$$(x_1 \dots x_m\, x_{m+1} \dots)\,\tau = (x'_1 \dots x'_m\, x'_{m+1} \dots).$$

La méthode consiste donc à isoler successivement des facteurs $d\,w_i\,c$ tels que $w_i \cap \{c, d\}^* = \varnothing$, qui sont invariants par $\tau$, en terminant par

$$(c^m\, d^n)\,\tau = c^n\, d^m.$$

On constate que l'image d'un tableau est un tableau.

**4.4 – Lemme :**

Soit $\tau'$ une autre transposition de lettres consécutives ne commutant pas avec $\tau$. Soit $B$ l'intervalle (à trois lettres) qui est l'union des orbites de $\tau$ et $\tau'$. Soit $t$ un tableau appartenant à $B^*$. Alors

$$((t\,\tau)\,\tau')\,\tau = ((t\,\tau')\,\tau)\,\tau'.$$

Un exemple remplacera la vérification de ce Lemme :

Lorsque $t = e\,dd\,ccc$, on a

$$t = \begin{array}{l} e \\ d\,d \\ c\,c\,c \end{array}$$

$$t\,\tau = \begin{array}{l} e \\ d\,d \\ c\,c\,d \end{array} \qquad\qquad \begin{array}{l} e \\ d\,e \\ c\,c\,c \end{array} = t\,\tau'$$

$$t\,\tau\,\tau' = \begin{array}{l} e \\ d\,e \\ c\,c\,e \end{array} \qquad\qquad \begin{array}{l} e \\ d\,e \\ c\,d\,d \end{array} = t\,\tau'\,\tau$$

$$t\,\tau\,\tau'\,\tau \quad = \quad \begin{array}{l} e \\ d\,e \\ c\,d\,e \end{array} = t\,\tau'\,\tau\,\tau'$$

Nous sommes maintenant en position de donner la définition du relèvement plaxique, en même temps que certaines de ses propriétés, qui le caractérisent.

**4.5 – Proposition :**

(1) l'application $\tau \in \gamma_A \to \tau \in Bij(A^*)$ définie en (4.3) s'étend en une représentation de $\gamma_A$, dont l'image est dite $\mathrm{Aut}(A^*)$.

(2) pour tout $\sigma \in \gamma_A$, le diagramme suivant est commutatif

$$\begin{tikzcd} A^* \arrow[r, dashed, "\sigma"] \arrow[d, "\mathrm{cv}"'] & A^* \arrow[d, "\mathrm{ev}"] \\ N^A \arrow[r, dashed, "\sigma"] & N^A \end{tikzcd}$$

(3) pour tout $\sigma \in \mathrm{Aut}(A^*)$, $\sigma\,\text{Я} = \text{Я}$

(4) pour tout mot $w$ de $A^*$, pour tout intervalle $B : \{B\,\sigma\} = B$, alors

$$w\,\sigma \cap B^* = (w \cap B^*)\,\sigma$$

(5) tout élément de $\mathrm{Aut}(A^*)$ commute au redressement.

***Démonstration :***

Soit $\sigma$ un élément de $\gamma_A$. On peut le factoriser en un produit de transpositions de lettres consécutives et relever ce produit de transpositions d'après la construction (4.3). Il est clair que ce relèvement vérifie les propriétés (2), (3), (4), (5) puisqu'il les vérifie pour les transpositions de lettres consécutives, comme il a été vu plus haut. Il nous reste donc à montrer que le relèvement de $\sigma$ ne dépend pas de sa factorisation en produit de transpositions, c'est–à–dire, d'après les relations de Coxeter :

— si $\tau$ et $\tau'$ commutent dans $\gamma_A$, alors $\tau\,\tau' = \tau'\,\tau$ dans $Bij(A^*)$

— si $\tau$, $\tau'$ ne commutent pas (ce qui implique que $\tau'\,\tau\,\tau' = \tau\,\tau'\,\tau$), alors $\tau'\,\tau\,\tau' = \tau\,\tau'\,\tau$ en tant qu'éléments de $Bij(A)$.

Le premier cas est évident, puisque $\tau$ et $\tau'$ ont des orbites disjointes et que leur relèvement n'agit que sur les lettres dans ces orbites respectives.

Soient donc, dans le deuxième cas, trois lettres consécutives $c$, $d$, $e$, $B$ l'intervalle $\{c, d, e\}$ et $\tau$ la transposition de $c$ et $d$, $\tau'$ la transposition de $d$ et $e$. Soit $\theta \in Bij(A^*)$ le produit des relèvements $\tau\,\tau'\,\tau$ et $\theta'$ le produit $\tau'\,\tau\,\tau'$.

Soit $w \in A^*$ ; par construction, $w\,\theta$ et $w\,\theta'$ ne peuvent différer que pour les lettres appartenant à $B$. D'après la Propriété (4) de (4.3),

$$w\,\theta \cap B^* = (w \cap B^*)\theta \quad (\text{resp. } w\,\theta' \cap B^* = (w \cap B^*)\theta').$$

Les mots $(w \cap B^*)\theta$ et $(w \cap B^*)\theta'$ ont même $\text{Я}$–symbole d'après (4.3 (3)), et finalement, d'après la vérification (4.4), comme $\theta$ et $\theta'$ commutent au redressement, les mots $(w \cap B^*)\theta$ et $(w \cap B^*)\theta'$ ont aussi même redressé. Cela assure, d'après le théorème de Cauchy–Robinson (2.18) qu'ils sont identiques, et donc que $w\,\theta$ et $w\,\theta'$ le sont.

Il nous reste à justifier le nom de *groupe des automorphismes de conjugaison*, pour l'image de $\gamma_A$ dans $Bij(A^*)$. C'est le but du théorème suivant.

### 4.6 – Théorème de conjugaison :

Soit $\sigma \in \mathrm{Aut}(A^*)$ et $w_i$, $w_i'$ $(i = 1, 2)$ quatre mots : $|w_i| = |w_i'|$, tels que $(w_1\,w_2)\sigma = w_1'\,w_2'$. Alors

(1) $w_i\,\text{Я} = w_i'\,\text{Я} \quad (i = 1, 2)$

(2) pour tout entier $n \geqslant 0$, $\quad (w_2\,w_1)^n\,\sigma = (w_2'\,w_1')^n$.

Il suffit de vérifier l'énoncé dans le cas où $\sigma$ est la transposition de deux lettres consécutives, ce qui se fait sans difficulté.

### 4.7 – Théorème :

La restriction de tout automorphisme de conjugaison à un sousmonoïde commutatif de $A^*/\equiv$ est un isomorphisme (de monoïde).

Suivant la remarque déjà amplement utilisée, il nous suffit de considérer le cas d'une transposition $\tau$ de lettres consécutive $c$, $d$. Il nous faut prouver que si deux mots $w$, $w'$ commutent dans $A^*/\equiv$, alors $w\,\tau$, $w'\,\tau$ commutent de même. D'après la construction du relèvement, on peut supposer que $w, w' \in \{c, d\}^*$.

Soit donc $w \equiv (d\,c)^p\, c^n\, d^m$, $w' \equiv (d\,c)^{p'}\, c^{n'}\, d^{m'}$, avec par exemple $n \leqslant n', p'$. La condition $w\,w' \equiv w'\,w$ équivaut à l'une des deux suivantes :

$$m = n \leqslant n',\ m' \quad \text{ou} \quad n' = n \leqslant m,\ m' \ ;$$

on vérifie alors directement que

$$(w\,w')\,\tau = w\,\tau \cdot w'\,\tau \equiv w'\,\tau \cdot w\,\tau = (w'\,w)\,\tau \qquad \square$$

Soit $J : A \to N$ une évaluation. Il existe une et une seule partition $I$ telle que $J\,\sigma = I$ pour au moins une permutation $\sigma$ de $A$ et on peut choisir cette dernière de telle sorte que $x\,\sigma \leqslant y\,\sigma$ quand $x\,J = y\,J$ et $x \leqslant y$ ; cette permutation (et l'automorphisme de conjugaison associé par le relèvement plaxique) est la *rectification* de $J$. Si donc $w$ a pour évaluation $J$ et $\sigma$ est la rectification de $J$, alors $w\,\sigma$ est un mot partitionnel qui est dit le *rectifié* de $w$.

4.8 – La construction suivante facilite le calcul du rectifié d'un mot :

Soit $w \in A^*$, $J$ l'évaluation de $w$. Soit $B$ un intervalle initial $= [a \ldots d]$ de $A$, et soit $b \in B$ tel que $x\,J \geqslant b\,J\ \forall\ x \in B$. Soit $\sigma$ la permutation circulaire sur les lettres $[b \ldots d]$ : $\sigma : a \ldots b_-\, b\, b_+ \ldots d\, d_+ \ldots \to a \ldots b_-\, b_+ \ldots d\, b\, d_+ \ldots$

Alors $w\,\sigma$ s'obtient par constructions de 'filières' successives : par lettre *voisine* d'une lettre $x_i = x$ dans un mot, on entend la première lettre $x_+$ à gauche de $x_i$ dans la *lecture circulaire* de ce mot (c'est-à-dire, on repart de l'extrémité droite du mot si l'on ne trouve pas de $x_+$ à gauche de $x_i$). On prend alors une lettre $b$, puis les voisins successifs des lettres atteintes, jusqu'à la lettre $d$ incluse. On élimine le mot standard ainsi obtenu et l'on recommence l'opération à partir de n'importe quelle autre lettre $b$. Finalement, on isole ainsi un sous-mot homogène $w'$ de $w$, d'évaluation $(b \ldots d)^{bJ}$. Le mot $w\,\sigma$ s'obtient alors par l'opération : $x_i = x \to x_-$ si $x \in [b_+ \ldots d]$ et $x_i \notin w'$, et $x_i$ inchangé sinon.

Exemple :

$$\begin{array}{ll}
w = e\,a\,e\,b\,c\,d\,a\,e\,b\,d\,a\,c\,c\,e\,d\,d & \\
\longrightarrow e\,a\,e\,b\,\underline{c}\,d\,a\,e\,\underline{b}\,d\,a\,c\,c\,e\,d\,\underline{d} & \text{(construction de la première filière)} \\
\longrightarrow e\,a\,e\,\underline{\underline{b}}\,\underline{c}\,d\,a\,e\,\underline{b}\,\underline{\underline{d}}\,a\,c\,\underline{\underline{c}}\,e\,d\,\underline{d} & \text{(deuxième filière)} \\
\longrightarrow e\,a\,e\,b\,c\,c\,a\,e\,b\,d\,a\,b\,c\,e\,c\,d & = x\,\sigma
\end{array}$$

Une lettre $x$ sera dite *en place* dans un tableau $t$ si et seulement si ses $|\,t\,|_x$ occurences se trouvent dans les premières (à partir de la gauche) colonnes de $t$. Moyennant cette définition, on alors :

4.9 – Remarque :

Les conditions suivantes sur un tableau $t$ sont équivalentes :

— ses mots colonnes commutent deux-à-deux
— sa forme et son évaluation rectifiée sont la même partittion
— son rectifié est un tableau de Yamanouchi
— toutes ses lettres sont en place.

*Preuve :*

L'équivalence des trois premières caractérisations résulte immédiatement de (4.7) et (3.7) puisque les automorphismes de conjugaison préservent la propriété d'un mot d'être une colonne. Celle de la dernière avec la première est immédiate en raison des règles de commutation entre colonnes (2.8). □

## 5 – Cyclage.

L'étude des polynômes de Foulkes/Green repose sur celle des classes de conjugaison dans le monoïde plaxique, ces dernières étant munies d'une structure d'ordre obtenue en restreignant la conjugaison à une relation spéciale dite de *cyclage.*

Soient $J : A \to N$ une évaluation et $W^J$ (resp. $T^J$) l'ensemble des mots (resp. tableaux) ayant cette évaluation. On vient de voir qu'il existe un automorphisme de conjugaison unique $\sigma = \sigma_J$ envoyant bijectivement $W^J$ (resp. $T^J$) sur l'ensemble $W^I$ (resp. $T^I$), où $I = J\,\sigma$ est la partition obtenue en réordonnant $J$. L'ensemble $T^J$ contient un tableau ligne unique $v_J$ dont l'image par $\sigma$ est l'unique tableau ligne $v_I \in T^I$ (puisque $\sigma$ conserve la forme).

Nous rappelons un résultat connu [L&S 3 et L&S 4) :

### 5.1 – Propriété :

Il existe une et une seule application $v : W^I \to N$, la *cocharge*, satisfaisant identiquement les conditions suivantes :

(1) $w\,v = (w\,R)\,v$
(2) $v_I\,v = 0$
(3) Si $w = x\,w'$ $(x \in A)$, alors $(w'\,x)\,v \geqslant w\,v$ quand $x = a$
et $(w'\,x)\,v = w\,v - 1$ quand $x > a$.

De fait, quand $w$ est un mot standard (c'est–à–dire quand $I = (1,\ldots,1)$) la cocharge de $w$ est l'index du Major de la permutation $w^{-1}\,\#$ (cfr. [5]) et c'est Thomas [8] qui a montré le lien entre cette statistique classique et les polynômes de Foulkes–Green. Pour les partitions plus générales, la cocharge de $w$ est la somme des cocharges sur un système de sous–mots standards de $w$ déterminés par un algorithme qui rend cette somme extrémale.

Grâce au théorème de conjugaison (4.6), nous pouvons définir la cocharge d'un mot $w$ de $W^J$ comme étant égale à celle du mot $w\,\sigma_J$.

Rappelons maintenant que si $t$ est un tableau dont la $h$–ième ligne est strictement plus courte que la $(h+1)$–ième, la Théorème de Pieri (2.11) permet de définir une paire unique $(x, s) = t\,\gamma^h$ telle que $(x\,s)\,R = t$, $x \in A$ et $s$ est un tableau dont la forme ne diffère de celle de $t$ que par suppression d'un point à la $h$–ième ligne. Le tableau $(s\,x)\,R$ est conjugué de $t$ (par $x$) dans le monoïde plaxique. Nous dirons que c'est le *$h$–cyclage de $t$ par $x$* si et seulement si sa cocharge est strictement inférieure à celle de $t$. Par conséquent, d'après la Proposition (5.1), quand l'évaluation de $t$ est une partition, cette condition est remplie si et seulement si $x \neq a$. Dans le cas contraire où $t \in T^J$, le théorème de conjugaison (4.6) montre que $(s\, x)\, \boldsymbol{R}\, \sigma_J = (s'\, x')\, \boldsymbol{R}$, où la paire $(x', s')$ est égale à $(t\, \sigma_J)\, \gamma^h$, et $(s\, x)\, \boldsymbol{R}$ est alors un cyclage si et seulement si $x' \neq a$.

Il est important de noter que d'après la Proposition (5.1), l'opération de cyclage réduit la cocharge d'exactement une unité. On observera aussi que si $t\, \gamma^h = (x, s)$, le tableau $(s\, x)\, \boldsymbol{R}$ est toujours un cyclage quand $h \geqslant 2$. Quand $h = 1$, c'est aussi un cyclage si et seulement si $x \neq a$ lorsque le degré de $a$ dans $t$ est maximal (i.e. $a\, \boldsymbol{J} \geqslant y\, \boldsymbol{J}$ pour tout $y \in A$). Nous ne connaissons pas de condition nécessaire et suffisante simple permettant de vérifier directement si $t \to (s\, x)\, \boldsymbol{R}$ est ou non un cyclage, sans passer par le calcul de $t\, \sigma_J$.

Soit par exemple

$$t = \begin{array}{l} c\ d \\ b\ b\ c \\ a\ a\ a\ d\ e \end{array} \quad ;$$

il admet trois factorisations $(x_h, s_h)$ correspondant à $h = 1, 2, 3$ respectivement :

$$t \equiv (b) \begin{array}{l} c\ d \\ b\ c\ d \\ a\ a\ a\ e \end{array} \quad , \quad t \equiv (b) \begin{array}{l} c\ d \\ b\ c \\ a\ a\ a\ d\ e \end{array} \quad , \quad t \equiv (c) \begin{array}{l} d \\ b\ b\ c \\ a\ a\ a\ d\ e \end{array} \quad ,$$

les tableaux $t_h = (s_h\, x_h)\, \boldsymbol{R}$ étant :

$$t_1 = \begin{array}{l} c\ d \\ b\ b\ d\ e \\ a\ a\ a\ b \end{array} \quad , \quad t_2 = \begin{array}{l} c\ d \\ b\ c\ d \\ a\ a\ a\ b\ e \end{array} \quad , \quad t_3 = \begin{array}{l} d \\ b\ b\ c\ d \\ a\ a\ a\ c\ e \end{array}$$

Ces trois tableaux sont des cyclages, puisque l'évaluation de $t$ est une partition et que $x_h \neq a$.

Considérons par contre le tableau $t' = t\, f^n$ ; on a

$$t'\, \gamma^h = (x_h\, s_h\, f^n) \quad \text{et} \quad (s_h\, f^n\, x_h)\, \boldsymbol{R} = t_h\, f^n.$$

Pour $h = 2$ ou $3$, ce sont encore des cyclages de $t'$. Par contre, pour $h = 1$ lorsque $n = 4 + m$, $m \geqslant 0$, $t_1 f^n$ n'est pas un cyclage de $t'$ : en effet, $t' \sigma_J$ est égal à

$$\begin{array}{l} c\ d \\ b\ b\ b \\ a\ a\ a\ a \ldots a\ c\ d\ e\ e\ f \end{array} = t'' \quad \text{et} \quad t''\, \gamma^1 = (a, s'').$$

5. 2 – Propriété :

Soit $T^J$ l'ensemble des tableaux d'évaluation $J$. Le cyclage est la relation de consécutivité d'un ordre partiel sur $T^J$ dont l'élément minimum unique est le tableau ligne $v_J$, et qui admet la cocharge comme fonction de hauteur. Les éléments maximaux de cette relation sont les tableaux dont la longueur de la première ligne est le maximum des degrés des lettres ; parmi ceux–ci l'élément de hauteur maximum est l'unique tableau $t \in T^J$ dont la forme est la partition $I = J\,\sigma_J$.

*Preuve :*

Puisque la structure de cyclage de $T^J$ est l'image de celle de $T^J$ par l'automorphisme $\sigma_J{}^{-1} : T^I \to T^J$, il suffit de vérifier l'énoncé dans le cas d'une partition ; la description des éléments maximaux résulte alors de (4.9) et le reste de la proposition de (5.1).

Certaines proposition s'énoncent plus facilement en utilisant la *charge* $w\,\nu$ (cfr. [L&S 3]) que nous définissons ici comme la différence $w_0\,v - w\,v$, où $w_0$ est le mot de Yamanouchi dont l'évaluation est la rectifiée de celle de $w$. On a alors :

**5.3 – Propriété :**

La charge d'un tableau $t$ est égale à :

(i) celle d'une quelconque de ses puissances
(ii) celle de tout mot $w'\,z\,x\,w''$ si $t \equiv w'\,x\,z\,w''$ et $x, z$ sont deux lettres non consécutives dans $A$
(iii) celle du tableau complémentaire de $t$ défini en (3.3).

*Preuve :*

On peut supposer $t$ partitionnel. Nous ne reproduisons pas les preuves de (i) et (ii) qui découlent immédiatement de l'algorithme de calcul des charges exposé ailleurs (cfr. [L&S 5]). La preuve de (iii) résulte de l'égalité $t\,\nu = \widehat{t}\,\nu$ $(= 0)$ pour les tableaux de Yamanouchi et du lemme qui suit

**5.4 – Lemme :**

Soient $w$ un mot, et $\widehat{y}$ la colonne complémentaire d'une lettre $y \neq a$. On a $(w\,\widehat{y})\,v = 1 + (\widehat{y}\,w)\,v$, où $v$ désigne la cocharge.

*Preuve :*

On peut, au moyen d'un automorphisme de conjugaison, se ramener au cas où l'évaluation de $w\,\widehat{y}$ est une partition. Le résultat se vérifie directement quand $w$ est une ligne et on procède par induction sur la cocharge de $w\,y$.

Si donc $w$ n'est pas une ligne, il existe une lettre $x \neq a$ telle que $w \equiv x\,w'$.

Supposons d'abord $x \neq y$. On a alors $\widehat{y}\,x \equiv x\,\widehat{y}$, et donc le diagramme commutatif suivant, où l'on a figuré la variation de la cocharge

$$\begin{tikzcd}
x\,\widehat{y}\,w' \equiv \widehat{y}\,x\,w' \equiv \widehat{y}\,w \arrow[rr, dashed, "?"] \arrow[d, "-1"] & & w\,\widehat{y} \equiv x\,w'\,\widehat{y} \arrow[d, "-1"'] \\
\widehat{y}\,w'\,x \arrow[rr, dashed, "+1"] & & w'\,x\,\widehat{y} \equiv w'\,\widehat{y}\,x
\end{tikzcd}$$

Les deux flèches verticales sont des cyclages, et donc d'après (5.1), la cocharge baisse de 1 ; par ailleurs, la cocharge augmente de 1 pour la flèche du bas, d'après l'hypothèse d'induction ; il en est donc de même pour la flèche du haut, comme annoncé.

On traite le cas où $x =: y$ pareillement, en remplaçant la relation de commutation $\widehat{y}\, x \equiv x\, \widehat{y}$ par $\widehat{y}\, y \equiv y_-\, \widehat{y}_-$ dans le cas où $y \neq: b =: a_+$, et l'on vérifie directement le lemme pour $x =: y =: b$.

Les deux propriétés qui suivent servent à prouver certaines inégalités entre les polynômes de Foulkes/Green que nous avons publiées ailleurs [L&S 4].

**5.5 – Propriété :**

Soient $I$ et $J$ deux évaluations telles que $aJ =: 1 + aI$ et $xJ =: xI$ pour les autres lettres. L'application $t \to (a\,t)\,R$ est une bijection de $T^I$ sur le sous–ensemble $T'$ des tableaux de $T^J$ n'admettant pas de 1–cyclage et ayant leur seconde ligne strictement plus courte que la première. L'application inverse est un morphisme de cyclage.

*Preuve :*

Soit $t' \in T^J$. Une condition nécessaire et suffisante pour que $t' \equiv a\,t$ est que sa deuxième ligne $v'_2$ soit strictement plus courte que sa première ligne $v'_1$ et que la $i$–ème lettre de $v'_2$ soit strictement supérieure à la $i{+}1$–ième lettre de $v'_1$ pour $i =: 1, 2, \ldots, |v'_2|$. Ceci montre immédiatement que $T' = \{(a\,t)\,R : t \in T^I\}$, puisqu'un tableau $t' \in T^J$ n'admet un 1–cyclage que si $|v'_1| > |v'_2|$ et si la $i$–ème lettre de $v'_2$ est inférieure ou égale à la $i{+}1$–ième de $v'_1$ pour un certain $i$.

Supposons maintenant que $t' =: (a\,t)\,R$, où $t \in T^I$, admette un $h$–cyclage par une lettre $x$ ($\neq:$ a par définition du cyclage). On a donc $h \geqslant 2$ et si $t' \equiv x\,s'$ on voit que les deux premières lignes du tableau $s'$ satisfont les mêmes conditions que celles de $t'$. Donc $s' =: a\,s$, où $(x\,s)\,R =: t$ et où $t \to (s\,x)\,R$ est un $h$–cyclage. □

Notons $\delta$ l'opération consistant à changer en un $b$ le dernier $a$ de la première ligne d'un tableau $t$. Par exemple, si

$$t =: \begin{matrix} b\,c \\ a\,a\,b\,d \end{matrix} \qquad \text{on a} \qquad t\delta =: \begin{matrix} b\,c \\ a\,b\,b\,d \end{matrix}\,.$$

Si $I$ est l'évaluation de $t$, on note $I\,\delta =: J$ celle de $t\,\delta$.

**5.6 – Propriété :**

Soit $I$ une évaluation telle que $a\,I > b\,I$. L'opération $\delta$ est une bijection de $T^I$ sur l'ensemble $T'$ des tableaux de $T^J$ qui ont au moins un $b$ sur la première ligne. C'est un morphisme de cyclage.

*Preuve :*

Le fait que $\delta : T^I \to T'$ est bijectif est immédiat, car si $t' \in T'$, l'hypothèse $a\,I > b\,I$ implique que le mot obtenu en changeant en un $a$ le premier $b$ de sa première ligne est encore un tableau.

Soit maintenant $t \equiv x\,s \to (s\,x)\,R$ un $h$–cyclage de $t \in T^I$ par la lettre $x$. En considérant la première ligne de $t$ on voit que $t\,\delta \equiv x\,(s\,\delta) \to (s\,\delta\,x)\,R$ est aussi un $h$–cyclage de $t\,\delta$. □

Soient $v$ une ligne et $t$ un tableau de même évaluation que $v$. Si $p$ est la cocharge de $t$ il existe au moins une suite de cyclages par les lettres $x_1,\dots, x_p$ menant de $t$ à $v$. Le mot $w = x_1\,x_2 \dots x_p$ est appelé un *mot de cyclage* de $t$. Il satisfait l'équation $t\,w \equiv w\,v$ et nous conjecturons que toute solution de cette équation qui n'est pas un mot de cyclage de $t$ a une longueur strictement supérieure à $p$.

Quand $t$ est partitionnel, l'algorithme de calcul des charges montre directement que tous les mots de cyclage de $t$ ont la même évaluation. Un résultat plus fort est obtenu au moyen de l'opération $K$ décrite à la fin de la section.

Soit $r + 1$ le nombre de lettres de l'alphabet du tableau $t$.

### 5.7 – Théorème :

Tout mot de cyclage de $t$ est congru au produit $t_1\,t \dots t_r$, où $t_j$ est le tableau obtenu en supprimant la première ligne dans le tableau $t\,K^{j-1}$ ($j = 1,\dots, r$).

La preuve du théorème repose sur deux lemmes d'intérêt indépendant.

### 5.8 – Lemme de l'hexagone :

Soit $t$ un tableau admettant un $h_1$–cyclage $t \to t_1$ par une lettre $y$ et un $h_2$–cyclage $t \to t'_1$ par $y'$, où $h_1 > h_2$ et $h_1 \neq 2$. Il existe des lettres $y_2, y_3, y'_2, y'_3$ et un tableau $t_3$ tels que $y\,y_2\,y_3 \equiv y'\,y'_2\,y'_3$ et que $t_3$ soit à la fois un cyclage de $t_1$ par le mot $y_2\,y_3$ et de $t'_1$ par $y'_2\,y'_3$.

*Preuve :*

On applique le lemme de l'équerre (2.13) en prenant $h_3 = h_1 - 1$. Les lettres cherchées sont définies par

$$t\,\gamma^{h_1 h_2 h_3} = (y\,y_2\,y_3,\, s'') \quad ; \quad t'\,\gamma^{h_2 h_1 h_3} = (y'\,y'_2\,y'_3,\, s'')$$

et le tableau $t_3$ est $(s''\,y\,y_2\,y_3)\,R = (s''\,y'\,y'_2\,y'_3)\,R$.

Il suffit de vérifier que toutes les opérations sont bien des cyclages, ce qui est clair lorsque $h_2 \geqslant 2$ ou quand $y \neq y'$. Quand $h_2 = 1$ et $y = y'$, on a $y_2 = y'_3$, avec $y'_3 \neq a$ puisque $h_3 = h_1 - 1 \geqslant 2$ par hypothèse, montrant que l'opération $(s\,y)\,R = y_2\,s' \to (s'\,y_2)\,R$ est bien un cyclage. □

### 5.9 – Exemple :

Soit $$t = \begin{array}{llll} c & & & \\ b & d & & \\ a & b & e & f \end{array} \quad \text{et} \quad h_1 = 3, \quad h_2 = 1.$$

On a l'hexagone

$$
\begin{tikzcd}[column sep=small]
 & \begin{smallmatrix} c & & & \\ b & d & & \\ a & b & e & f \end{smallmatrix} \arrow[dl, dash, "{(3,\,c)}"'] \arrow[dr, dash, "{(1,\,c)}"] & \\
\begin{smallmatrix} b & d & e & \\ a & b & c & f \end{smallmatrix} = \left(\left(\begin{smallmatrix} b & d & & \\ a & b & e & f \end{smallmatrix}\right) c\right) \boldsymbol{R} \arrow[d, dash, "{(1,\,b)}"'] & & \begin{smallmatrix} d & & \\ b & e & f \\ a & b & c \end{smallmatrix} = \left(\left(\begin{smallmatrix} d & & \\ b & e & \\ a & b & f \end{smallmatrix}\right) c\right) \boldsymbol{R} \arrow[d, dash, "{(3,\,d)}"] \\
\begin{smallmatrix} d & & \\ c & e & f \\ a & b & b \end{smallmatrix} = \left(\left(\begin{smallmatrix} d & e & f \\ a & b & c \end{smallmatrix}\right) b\right) \boldsymbol{R} \arrow[dr, dash, "{(2,\,d)}"'] & & \begin{smallmatrix} b & e & f & \\ a & b & c & d \end{smallmatrix} \arrow[dl, dash, "{(2,\,b)}"] \\
 & \begin{smallmatrix} e & & & \\ c & f & & \\ a & b & b & d \end{smallmatrix} &
\end{tikzcd}
$$

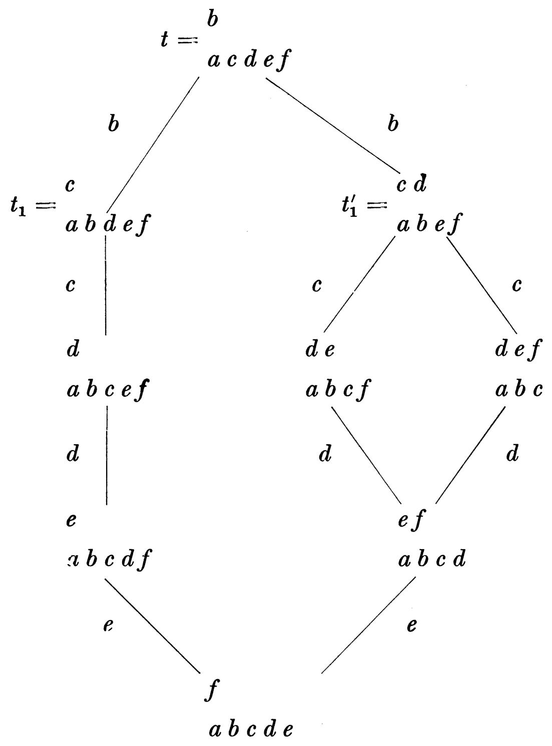
$(n, x)$ désignant le $n$–cyclage par la lettre $x$.

Ce lemme suffit pour montrer par induction sur la cocharge que deux mots de cyclage sont congrus quand aucune des deux chaines correspondantes ne contient de 1–cyclage. Pour compléter la preuve, un second lemme est nécessaire. Les seuls démonstrations que nous en connaissions font appel à une série de calcul trop spéciaux pour que nous les reproduisions ici et nous nous bornerons à en donner l'énoncé. Dans celui–ci, nous appelons *cyclage restreint* tout cyclage qui n'est pas un 1–cyclage d'un tableau qui a au moins trois lignes (il n'y a donc pas de restriction sur les cyclages des tableaux à deux lignes) ; la *structure de cyclage restreint* de $t_1$ est le plus petit ensemble contenant $t_1$ et tout tableau obtenu à partir d'un tableau de l'ensemble par cyclage restreint. Enfin, un morphisme de cyclage est *complet* si et seulement si il conserve les lettres de cyclage.

**5.10 – Lemme :**

Soit $t$ un tableau admettant un 2–cyclage $t \to t_1$ et un 1–cyclage $t \to t_1'$ par la même lettre. Il existe alors un morphisme de cyclage complet de la structure de cyclage restreint de $t_1$ dans celle de $t_1'$.

**5.11** – Exemple : (illustrant en même temps la nécessité de la condition $h_1 \neq 2$ dans le lemme de l'hexagone et le fait que le morphisme du Lemme (5.10) n'est pas bijectif)




Dans le cas particulier d'un tableau à deux lignes, s'il existe deux cyclages, ils sont nécessairement par la même lettre. En utilisant le lemme de l'hexagone (5.8), le lemme précédent achève de prouver que deux mots de cyclage d'un tableau sont congrus. Le fait qu'ils soient congrus au mot décrit dans le théorème résulte alors d'une simple induction sur la cocharge en considérant le cyclage de $t$ par sa première lettre (en tant que mot).

**5.12** – Soit $t$ un tableau d'évaluation $J$, et $b$ la première lettre (pour l'ordre de $A$) telle que $xJ \neq 0$. On suppose que $bJ \geqslant xJ \; \forall \; x$ ; on note dans ce cas par $tK$ le tableau $(v\,t')\,R$, où $t = t'\,b^p\,v$, $p = |\,t\,|_b$. L'opération $K$ permet une récurrence sur le nombre de lettres de l'alphabet d'un tableau dans plusieurs démonstrations ; l'énoncé suivant (qui a des applications à la multiplication des fonctions de Hall–Littlewood) illustre cette technique.

5.13 – PROPOSITION :

Soit $B$ un intervalle initial de $A$ et $J$ une évaluation telle que l'image de $B$ par la rectification $\sigma$ de $J$ soit un intervalle $C$. Pour chaque tableau $t$ d'évaluation $J$, les deux conditions suivantes sont équivalentes :

(i) toutes les lettres de $B$ sont en place dans $t$
(ii) les lettres de $C$ sont en place dans $(t\,\sigma)\,K^r$, où $r$ est le nombre de lettres précédant $C$ dans $A$.

*Démonstration :*

Tout d'abord, la condition que l'image de $B$ par la rectification de $J$ soit un intervalle équivaut à :

$$\forall\ x \notin B \quad , \quad \text{ou bien} \quad x\,J > \max_{y\in J} y\,J, \quad \text{ou bien} \quad x\,J \leqslant \inf_{y\in J} y\,J.$$

On peut supposer que le maximum de $J$ n'est pas atteint sur $B$, sinon les assertions (i) et (ii) sont identiques.

Par ailleurs, si un tableau $t'$ a une évaluation $J'$ telle que a $J' \geqslant x\,J'\ \forall\ x$, alors pour tout autmorphisme $\sigma'$ tel que $a\,\sigma' = a$, on a $(t\,K)\,\sigma' = (t\,\sigma')\,K$ d'après le théorème de conjugaison (4.6).

Grâce à cette remarque et au moyen d'un automorphisme de conjugaison laissant $B = [a, b,..., c, d]$ invariant, lequel permet de supposer que $e\,J = \max x\,J$ (avec $e = d_+$, successeur de $d$), on est ramené par récurrence à montrer l'équivalence de (i) et

(iii) Soit $\sigma'$ l'automorphisme $a, b,..., d, e,... \to e, a, b,..., d,...$ laissant fixes les lettres plus grandes que $e$ ; alors dans $(t\,\sigma')\,K$, les lettres $b,..., d, e$ sont en place.

La démonstration de la proposition repose alors sur le fait (4.9) que pour les lettres d'un intervalle $D$ et un tableau $t$, l'assertion : « les lettres de $D$ sont en place dans $t$» est équivalent à : « $\forall\ \sigma : \{D\,\sigma\} = \{D\}$, les lettres de $D$ sont en place dans $t\,\sigma$ ».

Pour ne pas avoir à surcharger l'exposé par la notation des automorphismes de conjugaison nécessaires, nous désignerons par $t\,(a^{aH}\,b^{bH}...)$ l'image de $t$ par l'automorphisme tel que $H = J_\sigma$, en n'écrivant pas les lettres pour les quelles $x\,H = x\,J$.

(iii) $\Rightarrow$ (i) La condition que $b,..., c, d, e$ soient en place dans $t' = t(a^{eJ}\,b^{aJ}...\,d^{cJ}\,e^{dJ})\,K$ implique que les lettres $b,..., c, d$ soient en place dans $t\,(a^{eJ}\,b^{aJ}...\,d^{cJ}\,e^{dJ})$ : on ne peut en effet pas extraire (au sens 2.12) de lettres $b,..., d$ par la gauche dans $t'$. Comme $a$ est nécessairement en place, après un automorphisme de conjugaison sur $a,..., d$ on voit que les lettres $a,..., d$ sont en place dans $t\,(a^{aJ}...\,c^{cJ}\,d^{eJ}\,e^{dJ})$. Il n'est pas difficile de vérifier que, après transposition de $d$ et $e$, les lettres $a,..., d$ sont encore en place.

(i) $\Rightarrow$ (iii) Soit $\tau$ la transposition de $d$ et $e$ ; comme $d$ est en place dans $t$ et que $d\,J \geqslant x\,J\ \forall\ x \leqslant d$, l'automorphisme $\tau$ n'opère que sur la première ligne de $t$. Les lettres $a,..., d$ sont donc en place dans $t\,(a^{aJ}\,...\,c^{cJ}\,d^{eJ}\,e^{dJ})$ tout autant que dans $t\,(a^{eJ}\,b^{aJ}\,...\,d^{cJ}\,e^{dJ})$. Dans ce dernier tableau, étant donné qu'il y a strictement plus de lettres $a$ que de $b,..., d$ respectivement, il n'y a pas de $b,..., d$ en première ligne ; ces lettres sont en place et le restent dans $t\,(a^{eJ}\,b^{aJ}\ldots e^{dJ})\,K$ ; en outre, comme le nombre de $e$ n'est pas inférieur au maximum du nombre de $b,\ldots, d$, la lettre $e$ se trouve en place apres l'opération $K$. □

**5.14** – **Exemple :**

$$t\,(=t\,(a^2\,b^3\,c^1\,d^4\,e^5)) = \begin{array}{l} d\,e \\ c\,d\,e \\ b\,b\,d \\ a\,a\,b\,d\,e\,e\,e \end{array} \quad ;$$

$$t\,(a^2\,b^3\,c^1\,d^5\,e^4) = \begin{array}{l} d\,e \\ c\,d\,e \\ b\,b\,d \\ a\,a\,b\,d\,d\,e\,e \end{array} \quad ; \quad t\,(a^5\,b^2\,c^3\,d^1\,e^4) = \begin{array}{l} d\,e \\ c\,c\,e \\ b\,b\,c \\ a\,a\,a\,a\,a\,e\,e \end{array} \quad ;$$

$$t\,(a^5\,b^2\,c^3\,d^1\,e^4)\,K = \Bigl(e\,e\cdot \begin{array}{l} d\,e \\ c\,c\,e \\ b\,b\,c \end{array}\Bigr)\,R = \begin{array}{l} e \\ d\,e \\ c\,c\,e \\ b\,b\,c\,e \end{array}$$

## REFERENCES

Outre les références désignées par [L&S $n$] qui sont détaillées dans la préface, on renvoie à :


[1] Clifford, A. H. & Preston, G. B. : « Theory of Semigroups », *Providence, Amer. Math. Soc.* (1961), Math. Surveys, n. 7.

[2] Greene, C. : « An extension of Schensted's theorem », *Adv. Math.*, 14, 254–265 (1974).

[3] Knuth, D. E. : « Permutation matrices and generalised Young tableaux », *Pac. J. Math.*, 34, 709–727 (1970).

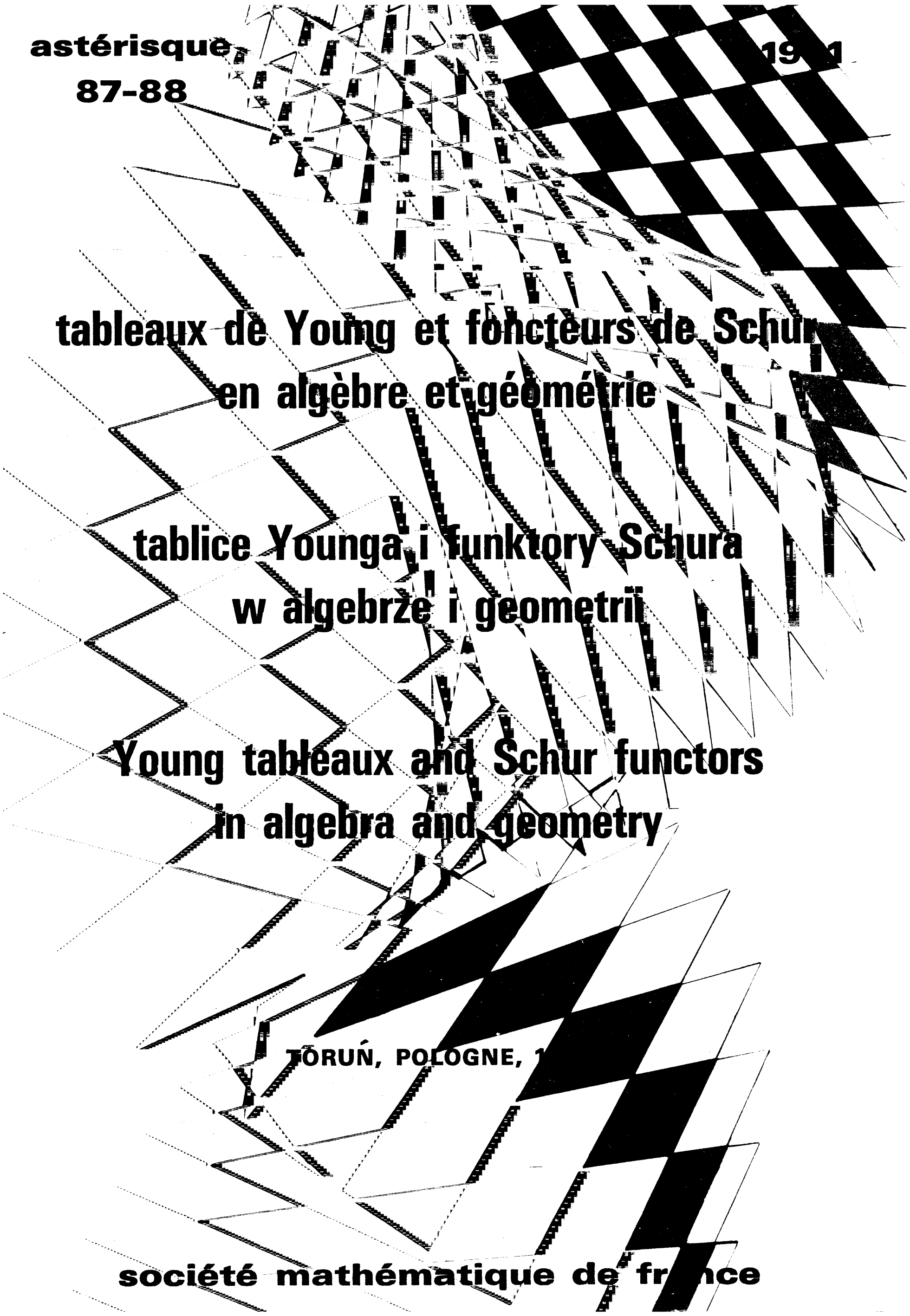
[4] Lallement, G. : *Semigroups and Combinatorial Applications* (New York, Wiley, 1979).

[5] Macdonald, I. G. : *Symmetric functions and Hall polynomials* (à paraître).

[6] Robinson, G. de B. : « On the representations of the symmetric group », *Am. J. Math.*, 60, 746–760 (1938).

[7] Schensted, C. : « Longest increasing and decreasing sequences », *Can. J. Math.*, 13, 179–191 (1961).

[8] Thomas, G. P. : « Further results on Baxter sequences and generalized Schur functions », *Combinatoire et représentation du groupe symétrique* (Strasbourg, 1976), Springer Lect. Notes, n. 579.


astérisque
87-88
tableaux de Young et foncteurs de Schur
en algèbre et géométrie
tablice Younga i funktory Schura
w algebrze i geometrii
Young tableaux and Schur functors
in algebra and geometry
TORUŃ, POLOGNE,
société mathématique de

# POLYNÔMES DE KAZHDAN & LUSZTIG POUR LES GRASSMANNIENNES

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

Alain Lascoux et Marcel-Paul Schützenberger

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆

## 1. Introduction.

Kazhdan et Lusztig ont défini, pour tout groupe de Coxeter fini, des polynômes $P_v^w(q)$ indexés par les paires d'éléments $(v,w)$ du groupe. Ces polynômes, que nous appelerons Polynômes de K&L sont fondamentaux et trouvent maintes applications :

- leur terme dominant détermine un graphe qui fournit la représentation régulière du groupe (cf. [K&L 1])

- les valeurs pour $q = 1$ de ces polynômes sont les multiplicités des modules de Verma (cf.[Brylinski])

- dans le cas du groupe symétrique, les coefficients des polynômes de K&L sont les dimensions des espaces de cohomologie singulière des variétés de Schubert : c'est la première description numérique des singularités de ces variétés (cf.[K&L2])

- plus généralement, on définit de même des polynômes de K&L pour les groupes de Weyl affines (cf. [Lusztig]). Parmi ceux-ci, on trouve les polynômes de Foulkes-Green que nous avons étudiés par ailleurs (cf. [Macdonald],[Schützenberger]) ; ils sont associés aux représentations complexes des groupes linéaires finis ; ce sont aussi les multiplicités des représentations du groupe symétrique sur la cohomologie de certaines sous-variétés de la variété drapeau (cf[De Concini&Procesi], résolvant la conjecture de[Kraft]), ainsi que les caractéristiques d'Euler-Poincaré des modules inversibles sur les variétés drapeaux (cf [Lascoux 2]) .

Ayant prouvé l'existence des polynômes dans [K&L1] , Kazhdan et Lusztig montrent par une voie détournée la non-négativité de leurs coefficients pour le groupe symétrique dans [K&L2]. Ce n'est pas la seule propriété remarquable de ces polynomes qui forment une famille très spéciale. Par exemple, en degré 0 et 1, les seuls polynômes possibles sont $0$, $1$, $1+q$, $1+2q$ , les seuls polynômes de liaison (cf. plus bas ; ce sont ceux de degré maximum, qui donnent les représentations du groupe symétrique) sont en degré 2 , les polynômes $1+q^2$, $1+q+q^2$, $1+2q+q^2$, $1+3q+q^2$, $1+4q+q^2$ . Nous conjecturons d'ailleurs que, pour un degré $d$ quelconque, ces polynômes de liaison sont bornés supérieurement par le polynôme eulérien de degré $d$ , et qu'il n'y a qu'un nombre fini de polynômes de K&L de degré donné (pour le groupe symétrique).

*A. LASCOUX, M. P. SCHÜTZENBERGER*

Le présent travail est consacré au cas grassmannien, pour lequel nous donnons une formulation explicite des polynômes de K&L reposant sur des objets combinatoires qui livrent du même coup les représentations associées. Le cas grassmannien présente certaines particularités notables qui ne se retrouvent pas dans le cas général, sur lequel nous reviendrons dans un autre article.

Au §2, à la suite de K&L, nous rappelons comment un graphe peut coder une représentation du groupe symétrique.

Aux §3,4,5 , nous examinons un sous-graphe du graphe complet, et montrons dans ce cas, indépendamment des polynômes de K&L, que le monoïde cycliste fournit l'existence des représentations.

Au §6, nous définissons des polynômes d'emboîtement de manière purement combinatoire.

Au §7, nous vérifions que les polynômes d'emboîtement sont bien les polynômes de K&L.

Aux §8,9,10 , nous donnons quelques propriétés de ces polynômes qui ne découlent de façon immédiate ni de leur définition dans [K&L1] , ni de leur interprétation cohomologique dans [K&L2] .

Le §11 précise les implications géométriques pour les grassmanniennes des résultats précédents.

## 2. Représentation associée à un graphe.

Chacune des représentations précédemment connues du groupe symétrique présente des inconvénients : la représentation "régulière" (i.e. l'algèbre du groupe) contient toutes les représentations complexes, mais avec multiplicité et les idempotents dans cette algèbre sont des sommes de permutations qu'il devient vîte impossible de développer, sans ou avec ordinateur. On peut facilement décomposer ou multiplier les "modules de Specht", mais l'action du groupe symétrique sur ces espaces n'a pas d' expression matricielles simple : il faut faire appel à la "straightening formula" de Garnir, qui malgrè les développements du Professeur Rota, reste d'un maniement malaisé. Dans la représentation semi-normale de Young, les matrices des générateurs du groupe symétrique sont au contraire très simples (la construction est de fait réduite à $S_2$ ), s'étendent à l'algèbre de Hecke ("q-analogue"), mais ne sont pas à coefficients entiers, et le pourquoi du succès de cette construction n'est en rien justifié par la théorie.

La représentation de Kazhdan et Lusztig offre (presque) tous les avantages, une fois rendue explicite :

les matrices représentant les générateurs du groupe symétrique sont très simples, ne comportant que des 0, 1 et −1, et codées simultanément par un seul graphe ; la restriction aux sous-groupes de Schur est triviale, de même que l'extension à l'algèbre de Hecke.

*POLYNÔMES DE KAZHDAN ET LUSZTIG*

Décrivons rapidement la représentation de K&L, et montrons tout d'abord comment un graphe peut coder des matrices.

Soit $n$ un entier. Soit $W$ une famille de permutations appartenant à $S_n$ et $\mu$ une application symétrique : $\mu : W \times W \to Z$. On étiquette chaque $w \in W$ par l'ensemble des lettres $i$ telles que $(i+1\ i)$ soit un sous-mot de $w$, c'est-à-dire telles que $i+1$ soit à gauche de $i$ dans $w$.

C'est la donnée d'une telle famille étiquetée que K&L appellent "graphe", $\mu(v,w)$ étant la multiplicité de l'arête $(v,w)$.

A un graphe de K&L sont associés $n-1$ opérateurs $T_i$ comme suit : soit $E$ le Z-module libre de base $e_w$, $w \in W$. Alors pour $i$ : $1 \leq i \leq n-1$, on définit $T_i \in \mathrm{End}(E)$ par

$$\begin{cases} T_i(e_w) = -e_w & \text{si } w \text{ a l'étiquette } i \\ T_i(e_w) = e_w + \Sigma\, \mu(v,w)\, e_v & \text{si } w \text{ n'a pas l'étiquette } i \\ & \text{somme sur tous les } v \text{ qui ont l'étiquette } i \end{cases}$$

Définition. Le graphe représente le groupe symétrique si $\tau_i \to T_i$ est une représentation (où les $\tau_i$, $1 \leq i \leq n-1$, sont les générateurs de Coxeter du groupe symétrique).

En d'autres termes, il suffit de vérifier les relations de commutation de Coxeter pour les $T_i$ : $T_i T_{i+1} T_i = T_{i+1} T_i T_{i+1}$ et $T_i T_j = T_j T_i$ si $i, j$ ne sont pas consécutifs (les relations $T_i T_i$ = identité découlent de la construction).

Théorème( K&L1 ). Il existe des polynômes $P_w^v(q)$ indexés par toutes les paires d'éléments de $S_n$, tels que le graphe ayant pour sommets les éléments de $S_n$, pour multiplicité d'arête $\mu(v,w)$, $v \leq w$, le coefficient du terme $q^{(\lg w - \lg v - 1)/2}$ dans $P_w^v(q)$, représente le groupe symétrique $S_n$ ; de plus toute représentation irréductible (en caractéristique 0) peut s'obtenir par restriction à un sous-ensemble de sommets.

Il a été conjecturé par K&L que la multiplicité $\mu$ est 0 ou 1 (c'est-à-dire que la construction est purement ensembliste).

Cette propriété découle dans le cas grassmannien de l'interprétation combinatoire donnée au §6.

Dans le cas général, il est d'ailleurs possible de construire directement un graphe de représentation (ensembliste) à partir du monoïde plaxique, indépendamment du calcul des polynômes de K&L ; ces derniers n'interviennent alors que pour vérifier l'identité de cet objet avec le graphe de K&L.

Dans tout ce qui suit, nous ne traitons plus que du cas grassmannien, qu'il nous reste à définir.

*A. LASCOUX, M. P. SCHÜTZENBERGER*

## 3. Graphe grassmannien.

Soit $n = n'+n''$ des entiers, $W_{n',n''}$ l'ensemble des mots de degrés respectifs $n'$ et $n''$ en $\alpha$ et $\beta$ .

On étiquette les mots de $W_{n',n''}$ par :

★ $w$ a l'étiquette $i$ ssi $w$ a pour facteur $\alpha\beta$ aux places $i,i+1$ .

A toute paire de mots $(v,w)$ de même degré, on associe une paire réduite $(v^{red},w^{red})$ en effaçant successivement les facteurs $\alpha\beta$ qui sont à la même place dans les deux mots. Par exemple, $\begin{matrix}\beta\ \alpha\ \alpha\ \beta\ \beta\ \alpha\\ \alpha\ \alpha\ \alpha\ \beta\ \beta\ \beta\end{matrix}$ donne par réduction $\begin{matrix}\beta\ \alpha\ .\ .\ \beta\ \alpha\\ \alpha\ \alpha\ .\ .\ \beta\ \beta\end{matrix}$ et finalement $\begin{matrix}\beta\ .\ .\ .\ .\ \alpha\\ \alpha\ .\ .\ .\ .\ \beta\end{matrix}$ .

On pose alors $\mu(v,w) = \mu(w,v) = 1$ et l'on dit que $v$ et $w$ sont liés si et seulement si $w^{red} = w'\ \beta\alpha\ w''$ , $v^{red} = w'\ \alpha\beta\ w''$ , c'est-à-dire si et seulement si $w^{red}$ et $v^{red}$ diffèrent par le changement d'un facteur $\alpha\beta$ en $\beta\alpha$ . On pose en outre $\mu(v,w) = 0$ dans les autres cas.

Pour montrer que le graphe ainsi défini représente le groupe symétrique, nous avons besoin de quelques généralités sur le monoïde plaxique à deux lettres.

Remarquons, pour faire le lien avec le §2, que tout mot de $W_{n',n''}$ peut être considéré comme une permutation (que nous dirons grassmannienne), en numérotant les $\alpha$ de droite à gauche par $1, 2, \dots, n'$, puis les $\beta$ par $n'+1, \dots, n'+n''$ . L'étiquetage que nous choisissons ici est l'inverse de celui du §2.

## 4. Monoïde cycliste

On sait depuis longtemps munir $N\times N$ d'une structure de monoïde (monoïde des parenthèses de Łukasiewicz) : c'est le cas particulier du monoïde plaxique (cf.[Lascoux-Schützenberger]) lorsque l'alphabet est réduit à deux lettres.

Définition. Le monoïde cycliste est le quotient du monoïde libre $\{\alpha,\beta\}^{\star}$ par les relations $\alpha\ \alpha\ \beta \sim \alpha\ \beta\ \alpha$ et $\beta\ \alpha\ \beta \sim \alpha\ \beta\ \beta$ .

Sur l'interprétation graphique donnée ci-après, on voit aisément :

Lemme. Le centre (i.e. l'ensemble des mots $v$ tels que $\forall\ w \in \{\alpha,\beta\}^{\star}$ ,alors $vw \sim wv$) est l'ensemble des mots équivalents à une puissance de $\alpha\beta$ . C'est le plus petit sous-monoïde qui, contenant $w$ , contient aussi $\alpha\ w\ \beta$ .

Il n'est guère difficile de vérifier la

Proposition. Soient $v,w \in \{\alpha,\beta\}^{\star}$ deux mots de mêmes degrés respectifs en $\alpha,\beta$ . Alors $v$ et $w$ sont liés (au sens du §3) si et seulement si il existe un mot $e$ du centre tel que $w = w_1\ \alpha\ e\ \beta\ w_2$ et $v = w_1\ \beta\ e\ \alpha\ w_2$ .

Interprétation graphique. Si l'on représente un mot par un chemin dans $Z\times Z$ , $\alpha$ étant le segment $(m,n) \to (m+1,n-1)$ et $\beta$ le segment $(m,n) \to (m+1,n+1)$ , alors un mot est dans le centre si et seulement si les points terminaux sont sur la même horizontale et si le chemin ne traverse pas cette dernière.

## 5. Le graphe grassmannien représente le groupe symétrique.

Comme nous l'avons déjà dit au §2, il suffit de vérifier les relations de Coxeter pour les opérateurs $T_i$ , c'est-à-dire :

5.1 $T_i^2 =$ identité

5.2 $T_i\,T_j = T_j\,T_i$ pour des orbites disjointes

5.3 $T_i\,T_{i+1}\,T_i = T_{i+1}\,T_i\,T_{i+1}$

La propriété 5.1 est automatique pour des opérateurs associés à un graphe ; il en est de même de la relation 5.3 pour le cas grassmannien auquel nous nous limitons ici.

En raison du fait qu'une liaison est une transposition de deux lettres, et donc que l'on n'a qu'un nombre fini de cas à considérer pour la composition de deux liaisons, on peut montrer une propriété plus forte que 5.2 :

Disons qu'un triple (ordonné) de mots : $(w_1, w_2, w_3)$ est un <u>(i,j)-triple</u> si et seulement si $(w_1, w_2)$ et $(w_2, w_3)$ sont des arêtes du graphe grassmannien, et si

$$\begin{cases} w_1 \text{ a les étiquettes } i \text{ et } j \\ w_2 \text{ a l'étiquette } i \text{ et pas } j \\ w_3 \text{ n'a ni } i \text{ ni } j \text{ .} \end{cases}$$

Alors, on a la proposition suivante :

<u>Proposition.</u> <u>Soit</u> $(w_1,w_2,w_3)$ <u>un</u> (i,j)-<u>triple. Alors il n'existe pas de mot</u> $w$ <u>tel que</u> $(w_1,w,w_3)$ <u>soit un autre</u> (i,j)-<u>triple, et il existe un seul</u> $w$ <u>tel que</u> $(w_1,w,w_3)$ <u>soit un</u> (j,i)-triple.

La proposition est en fait équivalente à la relation 5.2, plus le fait que la matrice représentant $T_i\,T_j$ ne comporte que des 0, 1 ou −1 .

## 6. Polynômes d'emboîtement

6.1 Le graphe du §3 traduit une certaines propriété des paires de permutations grassmanniennes ; des propriétés plus fines se lisent sur un nouvel objet combinatoire que l'on construit comme suit.

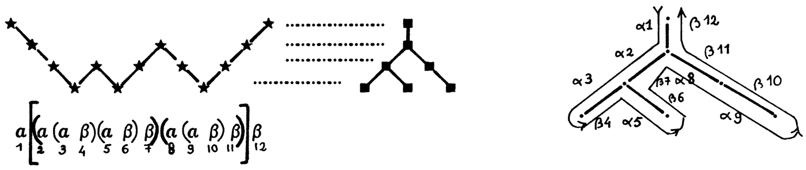
Soit $w$ une permutation grassmannienne que nous considèrerons comme un mot en $\alpha$ , $\beta$ et représenterons par un chemin, ainsi qu'il est indiqué au §4. On lui associe un <u>schéma d'emboîtement</u> $A(w)$ qui décrit ses factorisation successives en éléments du centre : chaque paire $\alpha \ldots \beta$ <u>en regard</u>, c'est-à-dire telle que $w = w'\alpha e\beta w''$ , $e$ appartenant au centre, correspond à un <u>segment</u> ; un <u>facteur</u> $\alpha\beta$ (dit <u>creux</u> du chemin $w$ ) correspond à un <u>segment terminal</u> ; on définit par récurrence l'attachement des segments par :

i) $A(\beta\ldots\beta\alpha\ldots\alpha)$ est le schéma vide

ii) A( w' $\underline{\alpha}\alpha\beta\underline{\beta}$ w") est le schéma obtenu en attachant un segment au segment terminal de A( w' $\underline{\alpha\beta}$ w") correspondant au facteur $\underline{\alpha\beta}$ souligné

iii) A(w'w") est le "produit" des schémas A(w') et A(w") (i.e. les deux schémas sont réunis par leur sommet) si w' ou w" appartient au centre.

6.2 Exemple

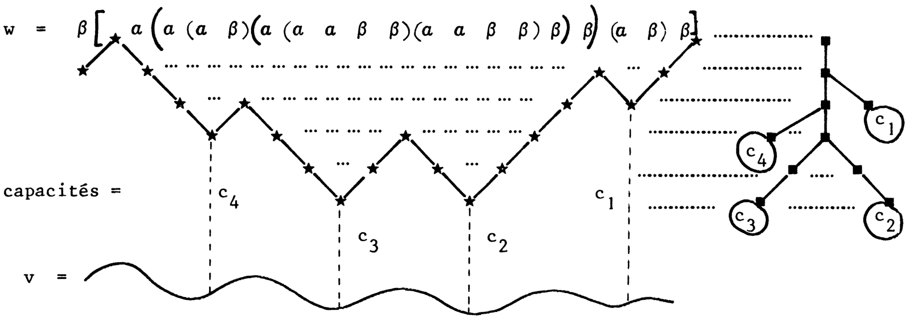



mot schéma parcours du schéma

On notera qu'en fait, si w appartient au centre, ce qui est le cas de l'exemple, on retrouve le mot w en parcourant le schéma comme on le fait en recherche systématique des données, $\alpha$ marquant un déplacement vers le bas et $\beta$ vers le haut, et que dans le cas général, le mot ainsi obtenu en parcourant A(w) est le plus grand sous-mot de w appartenant au centre.

6.3 Etant donnée une paire de mots (v,w) de mêmes degrés respectifs en $\alpha$ , $\beta$ , tels que $v \leqslant w$ pour l'ordre de Bruhat (c'est-à-dire tels que le chemin v soit en dessous du chemin w), étant donné un creux $\alpha\beta$ de w , on appelle <u>capacité</u> en ce creux la distance verticale de ce creux à v , i.e. si w = w' $\alpha\beta$ w" et v = v' v" , avec $|v'| = |w'\alpha|$ , alors la distance est $|v'|_\alpha - |w'\alpha|_\alpha = |v''|_\beta - |\beta w''|_\beta$ , où $|v|_\beta$ désigne le degré en $\beta$ . <u>La capacité de</u> w <u>par rapport à</u> v est la collection des capacités des creux de w ; il est commode de faire figurer celles-ci sur des disques accrochés aux segments terminaux de A(w) et de noter par A(w/v) le schéma muni de ses disques.

Si v n'est pas en dessous de w , on pose : capacité de w/v = $\emptyset$ (ne pas confondre avec la capacité nulle).



6.5 Un remplissage $\nu$ du schéma $A(w/v)$ est un remplissage de chaque segment par un entier $\geqslant 0$, de telle sorte que le remplissage soit décroissant (au sens large) de bas en haut, et que le remplissage de tout segment terminal n'excède pas sa capacité.

Le poids $|\nu|$ d'un remplissage est la somme des remplissages des segments.

La fonction génératrice des poids des remplissages, dite polynôme d'emboîtement du schéma $A(w/v)$ et notée $Q_w^v(q)$ est par définition $\Sigma_\nu\ q^{|\nu|}$, somme sur tous les remplissages de $A(w/v)$.

6.6 Lemme. $Q_{w'\alpha\beta w''}^{v'\alpha\beta v''} = Q_{w'\alpha\beta w''}^{v'\beta\alpha v''} + q^c\, Q_{w'w''}^{v'v''}$, où $c = |v'|_\alpha - |w'|_\alpha$ est la capacité du creux distingué.

En effet, étant donné un segment terminal $\alpha\beta$, l'ensemble des remplissages se décompose en deux familles, suivant que l'on remplit ce segment par un entier $\leqslant c-1$ ou par $c$ ; le premier ensemble a pour fonction génératrice des poids $Q_{w'\alpha\beta w''}^{v'\beta\alpha v''}$ et le second $q^c\, Q_{w'w''}^{v'v''}$.

## 7. Polynômes de K&L

7.1 Pour toute paire de permutations $(v,w)$, K&L ont défini un polynôme $P_w^v(q)$ en une variable $q$, de degré inférieur à $(\lg w - \lg v - 1)/2$, et posé

$$P_w^v(q) = \mu(v,w)\, q^{(\lg w - \lg v - 1)/2} + \text{termes de degré inférieur}.$$

D'après K&L 1, ces polynômes sont déterminés par les propriétés suivantes, que nous écrivons pour des mots grassmanniens $\in\{\alpha,\beta\}^*$, avec l'ordre sur les lettres: $\alpha<\beta$.

7.2.1 $P_w^v(q) = 0$ si $v \nleq w$

7.2.2 Simplification à droite et à gauche : $P_{w'ww''}^{w'vw''} = P_w^v$ et $P_\emptyset^\emptyset(q) = 1$

7.2.3 Normalisation.
$$P_{w'w_1w_2w''}^{v'v_1v_2v''} = P_{w'w_1w_2w''}^{v'v_2v_1v''} \quad \text{avec } v_1,v_2,w_1,w_2 \in \{\alpha,\beta\},\ w_1 \geqslant w_2$$

7.2.4 Récurrence sur la longueur de $w$

i) $P_{w'\beta\alpha\beta w''}^{v'zxyv''} = P_{w'\alpha\beta\beta w''}^{v'xzyv''} + qP_{w'\alpha\beta\beta w''}^{v'zxyv''} - \Sigma_u\ \mu(u,w)\ q^{(\lg w - \lg u + 1)/2}\ P_{u'u_1u_2u_3u''}^{v'z\,x\,y\,v''}$

avec $x,y,z,u_1,u_2,u_3 \in \{\alpha,\beta\}$, $z \geqslant x$, $|v'| = |w'| = |u'|$, somme sur tous les mots $u$ tels que $u_1 \geqslant u_2 \geqslant u_3$.

ii) formule analogue pour $P_{w'\alpha\beta\alpha w''}^{v'yzxv''} = P_{w'\alpha\alpha\beta w''}^{v'yxzv''} + \ldots$

7.3 La règle 7.2.3 entraine l'invariance des polynômes $P_w^v(q)$ par l'action sur $v$ d'un sous-groupe de Schur (dépendant de $w$) : au dessus d'une suite décroissante de lettres de $w$, on a le droit de permuter arbitrairement les lettres de $v$

sans changer le polynôme, i.e., si $w_1 \geqslant w_2 \geqslant \ldots \geqslant w_n$ , alors

$$P^{v'v_1\ldots v_n v''}_{w'w_1\ldots w_n w''} = P^{v'u_1\ldots u_n v''}_{w'w_1\ldots w_n w''}$$

$(u_1,\ldots,u_n)$ étant une permutation quelconque de $(v_1,\ldots,v_n)$.

Etant donné $w$ , on choisit dans l'orbite de $v$ sous l'action de ce groupe l'élément $\overline{v}$ de plus grande longueur, c'est-à-dire tel que tout facteur de $\overline{v}$ au dessus d'un facteur décroissant de $w$ soit décroissant ; $\overline{v}$ est dit le normalisé (par rapport à $w$ ) de $v$ .

Il est clair que si l'on considère les creux $\alpha\beta$ plutôt que les suites décroissantes, on a la caractérisation suivante :

7.4 Lemme. $v$ est normalisé par rapport à $w$ si et seulement si tout facteur $\alpha\beta$ de $v$ est au dessus d'un facteur $\alpha\beta$ de $w$.

Soit deux mots tels que $\begin{cases} v = v'\ x\alpha\beta\ v'' \\ w = w'\ \beta\alpha\beta\ w'' \end{cases}$ . En appliquant la récurrence 7.2.4 aux mots $v'\ x\alpha\beta\ v''$ et $v'\ x\beta\alpha\ v''$ , et en soustrayant, on obtient le lemme fondamental suivant qui permet le calcul effectif des polynômes de K&L :

7.5 Lemme. $P^{v'x\alpha\beta v''}_{w'\beta\alpha\beta w''} - P^{v'x\beta\alpha v''}_{w'\beta\alpha\beta w''} = q^{\delta}( P^{v'\alpha\beta x v''}_{w'\alpha\beta\beta w''} - P^{v'\beta\alpha x v''}_{w'\alpha\beta\beta w''} )$

avec $\delta = \chi(x{=}\alpha)$ , i.e. $\delta = 1$ si $x = \alpha$ , $= 0$ si $x \neq \alpha$ .

En effet, d'après la règle de normalisation 7.2.3, les termes en $u$ s'éliminent:

$$\Sigma_u\, \mu(u,w)\, q^{lg}\, P^{v'x\,\alpha\,\beta\,v''}_{u'u_1u_2u_3u''} = \Sigma_u\, \mu(u,w)\, q^{lg}\, P^{v'x\,\beta\,\alpha\,v''}_{u'u_1u_2u_3u''} \quad \text{puisque} \quad u_1 \geqslant u_2 \geqslant u_3 \ .$$

Si $x = \beta$ , on en tire, en n'écrivant que le triple de lettres permutées :

$P^{\beta\alpha\beta}_{\beta\alpha\beta} - P^{\beta\beta\alpha}_{\beta\alpha\beta} = P^{\alpha\beta\beta}_{\alpha\beta\beta} - P^{\beta\beta\alpha}_{\alpha\beta\beta} + q( P^{\beta\alpha\beta}_{\alpha\beta\beta} - P^{\beta\beta\alpha}_{\alpha\beta\beta} ) = P^{\alpha\beta\beta}_{\alpha\beta\beta} - P^{\beta\alpha\beta}_{\alpha\beta\beta}$ d'après la règle 7.2.3 .

Si au contraire $x = \alpha$ , on obtient $P^{\alpha\alpha\beta}_{\beta\alpha\beta} - P^{\alpha\beta\alpha}_{\beta\alpha\beta} = q( P^{\alpha\beta\alpha}_{\alpha\beta\beta} - P^{\beta\alpha\alpha}_{\alpha\beta\beta} )$ , et le lemme n'est autre qu'une écriture condensée de ces deux cas .

Symétriquement, on a :

7.6 Lemme. $P^{v'\alpha\beta x v''}_{w'\alpha\beta\alpha w''} - P^{v'\beta\alpha x v''}_{w'\alpha\beta\alpha w''} = q^{1-\delta}\, (P^{v'x\alpha\beta v''}_{w'\alpha\alpha\beta w''} - P^{v'x\beta\alpha v''}_{w'\alpha\alpha\beta w''} )$

avec $1-\delta = \chi(\ x = \beta) = 1 - \chi(\ x = \alpha)$ .

7.7 Au paragraphe 3, nous avons donné le terme de degré maximum du polynôme $P^{v}_{w}(q)$ en affirmant que la fonction $\mu$ ne prenait que les valeurs $0$ ou $1$ , et en caractérisant les paires telles que $\mu(v,w) = 1$ . Ces propriétés découlent du théorème suivant, qui établit que les polynômes de K&L pour les grassmanniennes ne sont autres que les polynômes d'emboîtement du §6 .

7.8 Théorème. Soit deux permutations grassmanniennes $v, w$. Le polynôme de K&L $P_w^v(q)$ est la fonction génératrice des poids des remplissages du schéma d'emboîtement $A(w/v)$, c'est-à-dire, on a, avec les définitions du §6

$$P_w^v(q) = Q_w^v(q) = \Sigma_\nu\, q^{|\nu|}$$

somme sur tous les remplissages de $A(w/v)$

Démonstration. On peut supposer que $v$ est normalisé par rapport à $w$. Choisissant un facteur $\alpha\beta$ dans $v$ (qui est donc au dessus d'un facteur $\alpha\beta$ dans $w$), on peut le porter par application successive des lemmes 7.4 et 7.5 en début des mots $v$ et $w$ : partant de $\begin{cases} v = v'\alpha\beta v'' \\ w = w'\alpha\beta w'' \end{cases}$, on obtient :

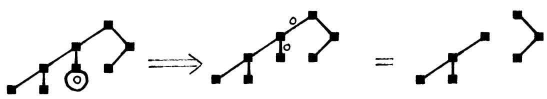
$P_w^v - P_{w'\alpha\beta w''}^{v'\beta\alpha v''} = q^c\,(P_{\alpha\beta w'w''}^{\alpha\beta v'v''} - P_{\alpha\beta w'w''}^{\beta\alpha v'v''}) = q^c\, P_{\alpha\beta w'w''}^{\alpha\beta v'v''} = q^c\, P_{w'w''}^{v'v''}$ avec $c$ = capacité du creux considéré $= |v'|_a - |w'|_a$ (le terme $P_{\alpha\beta w'w''}^{\beta\alpha v'v''}$ est nul puisque $\beta\alpha v'v'' \not\leq \alpha\beta w'w''$)

Les polynômes d'emboîtement vérifient la même formule (Lemme 6.6). Comme $lg(w'\alpha\beta w'') - lg(v'\beta\alpha v'')$ et $lg(w'w'') - lg(v'v'')$ sont strictement inférieures à $lg(w) - lg(v)$, le déplacement ci-dessus du facteur $\alpha\beta$ prouve par récurrence sur $lg(w) - lg(v)$ l'identité $P_w^v(q) = Q_w^v(q)$ Q.E.D.

## 8. Polynôme d'un ruban.

8.1 On dit que $w/v$ est un ruban lorsque toutes les capacités de $w$ par rapport à $v$ sont égales à 0 ou 1, et que $v$ est normalisé par rapport à $w$.

Si $\begin{cases} v = v'\alpha\beta v'' \\ w = w'\alpha\beta w'' \end{cases}$ et si la capacité en le creux $\alpha\beta$ distingué est 0, il est alors clair que $Q_w^v(q) = Q_{w'}^{v'}(q) \cdot Q_{w''}^{v''}(q)$, la capacité 0 partageant le schéma $A(w/v)$ en deux parties :



On peut donc supposer que le ruban est connexe, c'est-à-dire que toutes les capacités sont égales à 1. On écrira alors $P_w(q)$ pour $P_w^v(q)$.

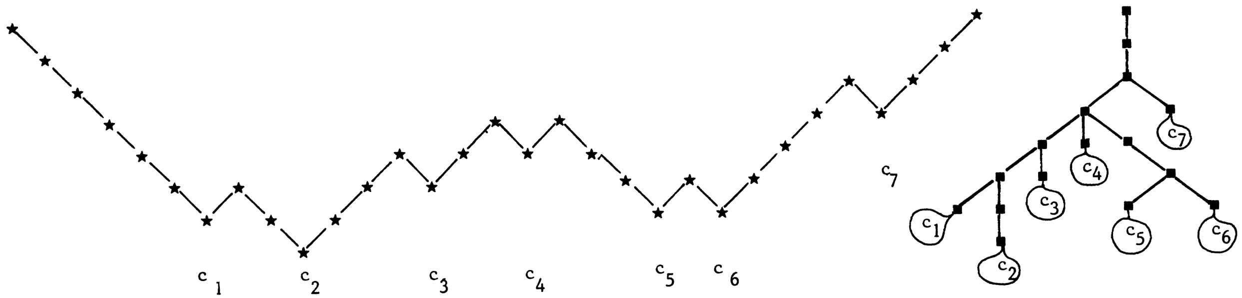
Les $P_w(q)$ se calculent directement sur le parenthésage de $w$ en éléments du centre ; il est clair en effet que les fonctions génératrices des poids des remplissages vérifient dans ce cas les règles suivantes qui les déterminent :

8.2.1 $P_{w'w''} = P_{w'} \cdot P_{w''}$ si $w'$ ou $w''$ appartient au centre

8.2.2 $P_{\beta\ldots\beta\alpha w\beta\alpha\ldots\alpha} = P_w + q^{p+1}$, avec $p$ = degré $(P_w)$

257

CALCUL D'UN POLYNÔME




$$a\ a\left[a\left(a\left(a\ (a\ \beta)(a\ a\ \beta\ \beta)\ \beta\right)(a\ \beta)\ \beta\right)\left(a\ \beta\right)\left(a\ a\ (a\ \beta)(a\ \beta)\ \beta\ \beta\right)\beta\right](a\ \beta)\ \beta\ \beta$$

Polynôme dans le cas de la liaison $(c_1 = \ldots = c_7 \neq 1)$ :

$$\left[\left(\left((1+q)(1+q+q^2) + q^4\right)(1+q) + q^6\right)(1+q)\left(q^4 + q^3 + (1+q)(1+q)\right) + q^{12}\right](1+q) + q^{14} + q^{15}$$

$$= 1 + 7q + 22\,q^2 + 42\,q^3 + 57\,q^4 + 62\,q^5 + 58\,q^6 + 47\,q^7 + 32\,q^8 + 18\,q^9 + 9\,q^{10} + 4\,q^{11} + 2\,q^{12} + q^{13} + q^{14} + q^{15}$$

<u>Exemple 8.3</u>

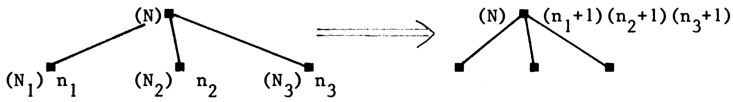
*POLYNÔMES DE KAZHDAN ET LUSZTIG*

8.4 On en déduit la règle de calcul suivante pour les valeurs $P_w(1)$ qui interviennent dans la théorie des modules de Verma (cf.[Brylinski]) :

l'algorithme consiste à numéroter de bas en haut, par étage horizontal, les noeuds du schéma $A(w)$ , et non plus les segments :

i) on porte 1 sur tous les noeuds terminaux du bas

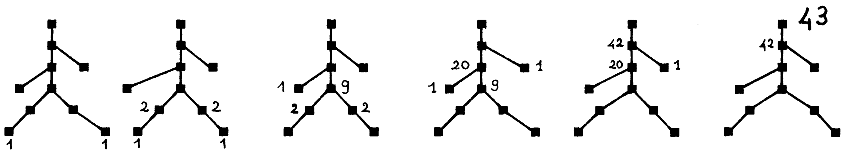
ii) En un noeud $N$ , on porte $\Pi(n_i+1)$ , où les $n_i$ sont les nombres portés par les noeuds $N_i$ de l'étage inférieur, tels que $N\,N_i$ soit un segment de $A(w)$,

par exemple 


Il est clair que cet algorithme est équivalent aux relations 7.2 lorsque l'on y pose $q = 1$ , et donc on a le

Lemme. $P_w(1)$ est le nombre porté par le noeud supérieur du schéma $A(w)$ .

Dans le cas de l'exemple 6.4 , on trouve




8.5 Du même algorithme, on tire que

Lemme. $P_w(-1) \begin{cases} = 0 & \text{si } P_w(1) \text{ est pair} \\ = 1 & \text{sinon} \end{cases}$

8.6 Interprétation des coefficients de $P_w(q)$

$P_w(q)$ est la fonction génératrice des poids des remplissages par les entiers 0 ou 1 du schéma $A(w)$ . Chaque remplissage consiste à choisir des sous-schémas terminaux de $A(w)$ et à les remplir par 1 . Ceci entraine que les coefficients de $P_w(q)$ peuvent être interprétés comme dénombrant les sous-mots de $w$ appartenant au centre :

Si l'on pose $P_w(q) = 1 + a_1\, q + a_2\, q^2 + \dots$ , alors $a_1$ est le nombre de facteurs $\alpha\beta$ dans $w$ , $a_2$ est le nombre de facteurs $\alpha\alpha\beta\beta$ + le nombre de paires de facteurs $\alpha\beta$ , etc...

## 9. Capacités infinies

9.1 Un autre cas où l'écriture des $P^v_w(q)$ est immédiate est lorsque les capacités tendent vers l'infini, c'est-à-dire, on remarque que $\lim_{n\to\infty} P^{\alpha^n v \beta^n}_{\beta^n w \alpha^n}$

existe en tant que série formelle et ne dépend pas de $v$ (c'est la fonction génératrice des poids des remplissages de $A(w)$ par des entiers $\geqslant 0$ ).

On peut noter cette limite

$$P_w^{-\infty}(q)$$

et les règles 8.2 sont remplacées par

9.2.1 $P_{w'w''}^{-\infty} = P_{w'}^{-\infty} \cdot P_{w''}^{-\infty}$ si $w'$ ou $w''$ appartient au centre

9.2.2 $P_{\alpha w\beta}^{-\infty} = P_w^{-\infty} \cdot 1/(1-q^{p+1})$ où $p$ est le nombre de segments de $A(w)$

9.2.3 $P_{\beta\ldots\beta w\alpha\ldots\alpha}^{-\infty} = P_w^{-\infty}$

9.3 De ces règles, on déduit l'algorithme suivant, qui consiste à numéroter les segments de $A(w)$ de bas en haut :

Soit un segment $B$ et soit $p(B)$ le nombre de segments du schéma en dessous, segment $B$ compris . Alors

Lemme. $P_w^{-\infty}(q) = \prod_B 1/(1-q^{p(B)})$ , produit sur tous les segments $B$ de $A(w)$.

Ceci est analogue au calcul des dimensions des représentations du groupe symétrique, ou du groupe linéaire $GL(n)$ , pour $n \to \infty$ ( les $p(B)$ sont alors dits "longueurs des équerres" ou "hook-lengths" ).

9.4 Un mot $\alpha^p \beta^p$ donne $P_{\alpha^p\beta^p}^{-\infty}(q) = 1 / (1-q)\ldots(1-q^p)$ , et donc, si $p$ est le nombre de segments de $A(w)$, alors

$$P_w^{-\infty}(q) \;/\; P_{\alpha^p\beta^p}^{-\infty}(q) = (1-q)\ldots(1-q^p) \;/\; \prod_B (1-q^{p(B)}) \;.$$

Le rapport de ces deux séries est en fait un polynôme qui intervient dans la belle théorie des $P\omega$-partitions de R.Stanley, dont nous ne dirons rien ici, et pour laquelle nous renvoyons au livre d'[Andrews] et aux exercices de [Knuth] .

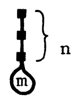
## 10. Quelques propriétés des polynômes de K&L

Dans la famille des polynômes de K&L, on trouve les polynômes fondamentaux que sont les <u>polynômes de Gauss</u> :

<u>10.1 Lemme.</u> $P_{\beta^m\alpha^n\beta^n\alpha^m}^{\alpha^m\alpha^n\beta^n\beta^m} = (1-q^{m+n})\ldots(1-q^{m+1}) \;/\; (1-q)\ldots(1-q^n)$

polynôme dit <u>polynôme de Gauss</u> et noté $\binom{m+n}{n}_q$

En effet, le schéma $A(w/v)$ est dans ce cas




dont il est bien connu que les remplissages décroissants au sens large par des entiers $\in \{1,2,\ldots,m\}$ ont pour fonction génératrice $\binom{m+n}{n}_q$ (cf. [Andrews]).

*POLYNÔMES DE KAZHDAN ET LUSZTIG*

10.2 D'après la définition qu'en donnent K&L, le polynôme $P_w^v(q)$ a un degré $\leqslant (\lg w - \lg v - 1)/2$ si $v < w$ ; ce nombre est dit degré maximum pour le couple $(v,w)$. Il est commode de considérer que $P_w^w(q)$ $(=1)$ n'est pas de degré maximum. Le lemme suivant montre qu'il est facile de caractériser les polynômes de liaison, i.e. correspondant aux couples de degré maximum.

10.3 Lemme. $P_w^v(q)$ est de degré maximum si et seulement si $w$ est lié à $v$ (au sens du §3), c'est-à-dire si et seulement si $\begin{cases} v = w'\,\alpha\, e\, \beta\, w'' \\ w = w'\,\beta\, e\, \alpha\, w'' \end{cases}$ avec $e$ appartenant au centre.

Démonstration. Tout d'abord, d'après 7.2.3, $v$ doit être normalisé dans le cas du degré maximum, c'est-à-dire tout facteur $\alpha\beta$ de $v$ doit être au dessus d'un facteur $\alpha\beta$ de $w$ si $\lg w - \lg v > 1$. Soit donc un facteur $\alpha\beta$ commun : $\begin{cases} v = v'\,\alpha\beta\, v'' \\ w = w'\,\alpha\beta\, w'' \end{cases}$ et soit $c$ la capacité de $w/v$ en le creux associé au facteur considéré. D'après le lemme 6.6 ,

$$\text{degré } P_w^v(q) = c + \text{degré } P_{w'w''}^{v'v''}(q) \quad .$$

Or, notant $v = v_1 \dots v_n$ et $w = w_1 \dots w_n$ , $v_i, w_i \in \{\alpha,\beta\}$ , alors si $v \leqslant w$ , $\lg w - \lg v = \Sigma_{i=1}^{i=n} |v_1 \dots v_i|_\alpha - |w_1 \dots w_i|_\alpha$ (c'est l'aire entre les chemins $v$ et $w$) et donc

$$\lg w - \lg v = \lg(w'w'') - \lg(v'v'') + 2c \quad .$$

Il s'ensuit que pour que le polynôme $P_w^v(q)$ soit de degré maximum, il faut et il suffit que $P_{w'w''}^{v'v''}(q)$ le soit ; en particulier, il est nécessaire que $v'v''$ soit normalisé par rapport à $w'w''$. Eliminant tous les facteurs successifs $\alpha\beta$ de $v$ , on obtient donc le couple $(v^{red}, w^{red})$ et l'on a :

- ou bien $v^{red}$ est à distance 1 de $w^{red}$, et alors $v$ et $w$ sont liés et $P_w^v(q)$ est de degré maximum puisque $P_{w^{red}}^{v^{red}}(q) = 1$ est de degré maximum ;
- ou bien $v^{red}$ n'a plus de facteur $\alpha\beta$ , i.e. $v^{red} = \beta \dots \beta\alpha \dots \alpha$ , et dans ce cas, $w^{red} = v^{red}$ (puisque $w \geqslant v \Rightarrow w^{red} \geqslant v^{red}$), ce qui implique que $w = v$ , cas exclu. Q.E.D.

On notera que les polynômes d'emboîtement sont tous unitaires, ce qui n'est pas vrai pour les polynômes de K&L généraux (pour le groupe symétrique), mais seulement pour les polynômes de liaison . Le lemme 10.3 assure que le graphe grassmannien *du §3 est bien le graphe de K&L .*

## 11. Grassmanniennes.

11.1 Il est bien connu que de nombreuses propriétés du groupe symétrique ont leur contrepartie géométrique dans la théorie des variétés drapeaux sous le groupe linéaire, dont les grassmanniennes sont un cas particulier. De cette théorie, nous n'aurons besoin ici que de considérations élémentaires.

*A. LASCOUX, M. P. SCHÜTZENBERGER*

Soit $E$ un espace vectoriel de dimension $m+n$ sur $\mathbf{C}$. L'ensemble des sous-espaces vectoriels $V$ de $E$ de dimension $n$ est de manière naturelle une variété algébrique dite grassmannienne d'ordre $n$ et notée $G_n(E)$.

Toute suite croissante $\mathbb{A} = 0 \subseteq A_1 \subsetneq A_2 \subsetneq \dots \subsetneq A_n$ de sous-espaces vectoriels de $E$ (dite drapeau) définit une sous-variété de $G_n(E)$, appelée variété de Schubert $\Omega(\mathbb{A})$ : en tant qu'ensemble,

$$\Omega(\mathbb{A}) = \{V \mid \forall i,\ \dim(V \cap A_i) \geqslant i\}$$

Il est clair qu'étant donné deux drapeaux $\mathbb{A}$ et $\mathbb{B}$ de mêmes dimensions respectives, il existe au moins un élément de $GL(E)$ qui envoit $\mathbb{A}$ sur $\mathbb{B}$, et donc, à isomorphisme près, que $\Omega(\mathbb{A})$ ne dépend que des dimensions des $A_i$.

On pose

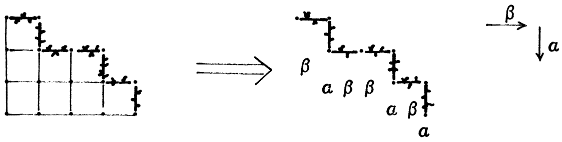
$$I = (i_1, \dots, i_n) = (\dim A_1 - 1, \dots, \dim A_n - n)$$

( $I$ est une partition, i.e. une suite croissante au sens large), et l'on note $\Omega_I$ la variété de Schubert $\Omega(\mathbb{A})$ à isomorphisme près. Ainsi $\Omega_{o\dots o}$ est un point et $\Omega_{m..m}$ est la grassmannienne $G_n(E)$ ; si $\dim A_1 = 0$, on pose $\Omega_{-1\dots} = \emptyset$.

La dimension de $\Omega_I$ est le poids $|I| = i_1 + \dots + i_n$ de la partition $I$.

11.2 On représente usuellement une partition par un diagramme, qui, hors le Royaume Uni et ses dépendances, consiste en un empilement de $i_1, \dots, i_n$ boîtes rectifié à gauche, e.g.

( 1, 3, 4 ) =




La frontière nord-est du diagramme donne un mot $w(I) \in \{\alpha, \beta\}^*$, lorsque l'on convient de coder un pas horizontal par $\beta$ et par $\alpha$ un pas vertical ; au §4, nous avons représenté ce mot par un chemin, qui, de fait, est obtenu à partir de la frontière du diagramme par une rotation d'angle $\pi/4$.

On dit qu'une partition $J$ est contenue dans une autre $I$ $(J \subset I)$ si et seulement si cela est vrai de leurs diagrammes respectifs, lorsque l'on juxtapose leurs origines $\Longleftrightarrow$ le chemin $w(J)$ est en dessous de $w(I)$

$\Longleftrightarrow$ $w(J) \leqslant w(I)$ pour l'ordre de Bruhat

$\Longleftrightarrow$ $\mathring{\Omega}_J$ est une cellule dans la décomposition cellulaire naturelle de $\Omega_I$.

11.3 Ecrivant $P_I^J(q)$ au lieu de $P_{w(I)}^{w(J)}(q)$, et en utilisanc la cohomologie de Deligne-Goreski-MacPherson, on a alors :

Théorème ( [K&L1] ).

$$P_I^J(q) = \Sigma_i \; q^i \dim \mathcal{H}^{2i}_{\Omega_J}(\Omega_I)$$

Nous donnons en annexe ces polynômes pour les grassmanniennes $G_n(m+n)$ , avec $m, n \leqslant 4$ . Certaines des propriétés des polynômes de K&L apparaissent clairement comme liées aux singularités des variétés de Schubert, sans qu'il soit nécessaire de rien savoir de la théorie cohomologique qui justifie ce rapport :

11.4 $P_I^J(q) = 0$ si et seulement si $\Omega_J \not\subset \Omega_I$ .

11.5 $P_I^J(q) \neq 0, 1$ si et seulement si $\Omega_J$ est contenu dans le lieu singulier de $\Omega_I$ .

En effet, le lieu singulier, en tant qu'ensemble, est la réunion des $\Omega_J$ tels qu'il existe au moins un creux du chemin $w(I)$ qui soit à distance $\geqslant 1$ du chemin $w(J)$ (cf. [Svanes] ou [Lascoux1] ).

$\Longleftrightarrow$ $w(J)$ est en dessous de $w(I)$ et au moins une des capacités de $w(I)$ par rapport à $w(J)$ est $\geqslant 1$ .

$\Longleftrightarrow$ il existe au moins un remplissage de $A(\,w(I)/w(J)\,)$ de poids $> 0$ .

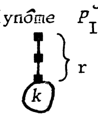
11.6 Plus généralement, il est clair sur les schémas d'emboîtement que si $H \subset J \subset I$ , alors $P_I^J(q) \leqslant P_I^H(q)$ , et ces polynômes sont différents si au moins une des capacités de $w(I)/w(J)$ est différente de la capacité correspondante de $w(I)/w(H)$ .

11.7 Soit $I = \underbrace{p\ldots p}_{r}\underbrace{p+r\ldots p+r}_{p}$ .

Alors $\Omega_I$ est une variété de Schubert dite <u>spéciale</u> (ou encore <u>variété déterminantale</u>), qui peut être définie par un drapeau ayant un seul élément : soit $A$ un espace vectoriel de dimension $p+r = n$ dans $E$ de dimension $2n$ ; alors

$$\Omega_I = \{ V \,|\, \dim(\,V \cap A\,) \geqslant r \} \hookrightarrow G_n(E) \;.$$

Il est facile de voir que le lieu singulier de $\Omega_I$ est stratifié en la suite emboîtée $\Omega_I \hookleftarrow \Omega_{J_1} \hookleftarrow \Omega_{J_2} \hookleftarrow \cdots$ des variétés $\Omega_{J_k} = \{ V \,|\, \dim(\,V \cap A) \geqslant r+k \}$ avec $J_k = \underbrace{p-k\ldots p-k}_{r+k}\underbrace{n\ldots n}_{p-k}$ .

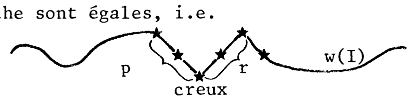
En fait (cf. Kleiman ), il existe une désingularisation de $\Omega_I$ telle que la fibre au dessus d'un point de $\Omega_{J_k} - \Omega_{J_{k+1}}$ soit *isomorphe à la grassmannienne* $G_k(r+k)$. Il est classique que le polynôme d'Euler-Poincaré de cette dernière variété est le polynôme de Gauss $\binom{r+k}{k}_q$ . Or c'est aussi *le polynôme* $P_I^{J_k}(q)$ , *puisque* le schéma d'emboîtement $A(\,w(I)/w(J_k)\,)$ est dans ce cas  .

263

Les $P_I^{J_k}(q)$ mesurent donc dans ce cas la désingularisation de Kleiman de $\Omega_I$ (cette désingularisation est "minimale" en un sens que nous ne préciserons pas).

11.8 Les composantes irréductibles du lieu singulier de $\Omega_I$ sont les $\Omega_J$ :

J est toute partition telle que $\begin{cases} w(I) = w' \,\beta\, \alpha^p\, \beta^r\, \alpha\, w'' \\ w(J) = w' \,\alpha\, \alpha^p\, \beta^r\, \beta\, w'' \end{cases}$ ( on choisit un creux de $w(I)$ et on l'abaisse d'une distance 1 ) . Or la variété $\Omega_I$ est de Gorenstein (cf. [Svanes] ) si et seulement si pour tout creux de $w(I)$ , les longueurs des versants droit et gauche sont égales, i.e.

$p = r$ avec 


(dans ce cas les syzygies canoniques de $\Omega_I$ sont symétriques, cf. [Lascoux1] ).

En d'autres termes, d'après le §9, on a la caractérisation suivante :

<u>11.9 Proposition.</u> <u>La variété de Schubert $\Omega_I$ est de Gorenstein si et seulement si pour toute composante irréductible du lieu singulier, le polynôme $P_I^J(q)$ est de degré maximum (et dans ce cas, il est symétrique).</u>

RÉFÉRENCES.

Andrews G. The theory of partitions, Encyclopedia of Maths, Vol.2 .

Brylinski J-L.& Kashiwara M. Démonstration de la conjecture de K&L sur les modules de Verma. C.R.Acad.Sc.Paris <u>291</u>(1980) 373-376 .

DeConcini C.& Procesi C. Symmetric functions, conjugacy classes and the flag variety. Invent. <u>64</u>(1981) 203-220 .

Kazhdan D.& Lusztig G.1 Representations of Coxeter groups. Invent. <u>53</u> (1979)165-184.

Kazhdan D.& Lusztig G.2 Schubert varieties and Poincaré Duality Proc. Symp. Pure Maths A.M.S. 1980.

Knuth Donald Irving. The Art of Computer Programming, vol.3, Addison-Wesley .

Kraft H. Conjugacy classes and Weyl Group Representations, ce volume .

Lascoux A.1 . Polynômes symétriques, Foncteurs de Schur et Grassmanniennes, Thèse Université Paris 7 (1977).

Lascoux A.2 . Finite linear groups, Tagung über Invariantentheorie, Bonn 1978.

Lascoux A.& Schützenberger M.P. Le Monoïde Plaxique, Napoli 1978 (à paraître dans les Quaderni della Ricerca Scientifica).

Lusztig G. Green polynomials and Singularity of unipotent classes Adv.in Math <u>42</u> (1981) 169-178 .

Macdonald I.G. Symmetric functions and Hall polynomials, Oxford Math.Monographs 1979.

Svanes T. Coherent cohomology on Schubert subschemes of flag schemes Adv. in Math. <u>14</u> (1974) 369-453 .

Schützenberger M.P. Tableaux de Young, Sém.Th.Nombres Pisot, Paris 1977/78 .

*POLYNÔMES DE KAZDHAN ET LUSZTIG*

POLYNÔMES DANS LE CAS GRASSMANNIEN

Nous donnons tous les polynômes $P_w^v(q)$ pour $w$ correspondant à une partition $I(w) = (i_1,\ldots,i_4)$ : $0 \leqslant i_1 \leqslant \cdots \leqslant i_4$ (Grassmanniennes $G_n(m+n)$, $m,n \leqslant 4$ ). On n'a écrit les polynômes que pour certains $v \in V(w)$, car l'on a pour les autres

$$P_w^u(q) = P_w^{v(u)}(q) \qquad \text{avec} \quad v(u) = \inf\left\{ v \in V(w) \ , \ u \leqslant v \right\}$$

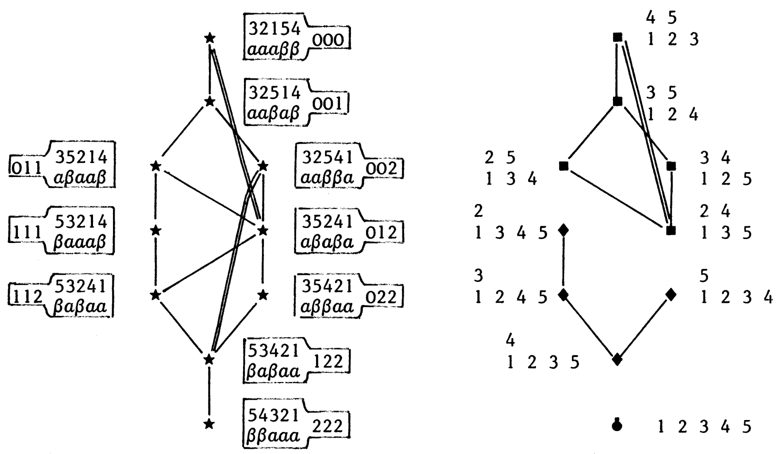
En d'autres termes, étant donnée une partition $u$ , on cherche dans la table pour $w$ fixé, la plus petite de celles qui la contiennent.

Si $w$ est un rectangle (i.e. $I(w) = 0,\ldots,0,n,\ldots,n$ ), alors $P_w^v(q) = 1$ si $v \leqslant w$ et $= 0$ sinon ; de plus, si $w = w_1\, w'\, w_2$ et $v = w_1\, v'\, w_2$ , alors $P_w^v(q) = P_{w'}^{v'}(q)$ . Moyennant ces deux remarques, la table est complète.

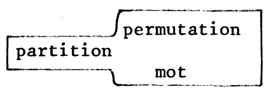
| I(w) | |
|---|---|
| 3444 | 2244 : $1+q$   1114 : $1+q+q^2$   0000 : $1+q+q^2+q^3$ |
| 3344 | 2224 : $1+q$   1111 : $1+q+q^2$ |
| 2444 | 1144 : $1+q$   0004 : $1+q+q^2$ |
| 2344 | 1144 : $1+q$   2224 : $1+q$   1124 : $(1+q)^2$   0004 : $(1+q)(1+q+q^2)$ : 1111 |
| 3334 | 2222 : $1+q$   0001 : $(1+q+q^2)^2$ |
| 1444 | 0044 : $1+q$ |
| 2244 | 1114 : $1+q+q^2$   0000 : $(1+q^2)(1+q+q^2)$ |
| 2334 | 1134 : $1+q$   2222 : $1+q$   1122 : $(1+q)^2$   0004 : $1+q+q^2$   0002 : $(1+q)(1+q+q^2)$ |
| 1344 | 0044 : $1+q$   1224 : $1+q$   0024 : $(1+q)^2$   1111 : $1+q+q^2$   0011 : $(1+q)(1+q+q^2)$ |
| 1334 | 0034 : $1+q$   1222 : $1+q$   0022 : $(1+q)^2$ |
| 1244 | 0044 : $1+q$   1144 : $1+q$   0014 : $(1+q)^2$   0000 : $(1+q)(1+q+q^2)$ |
| 2234 | 2222 : $1+q$   1114 : $1+q$   1112 : $(1+q)^2$   0000 : $(1+q)(1+q+q^2)$ |
| 1234 | 0034 : $1+q$   1114 : $1+q$   1222 : $1+q$   0014 : $(1+q)^2$   1112 : $(1+q)^2$ <br> 0022 : $(1+q)^2$   0012 : $(1+q)^3$   0000 : $(1+q)^2(1+q+q^2)$ |
| 2224 | 1111 : $1+q+q^2$ |
| 1144 | 0004 : $1+q+q^2$ |
| 1224 | 1111 : $1+q+q^2$   0024 : $1+q$   0011 : $(1+q)(1+q+q^2)$ |
| 1134 | 0004 : $1+q+q^2$   1122 : $1+q$   0002 : $(1+q)(1+q+q^2)$ |
| 1124 | 0004 : $1+q$   1111 : $1+q$   0001 : $1+2q+q^2+q^3$ |
| 1114 | 0000 : $1+q+q^2+q^3$ |

*A. LASCOUX, M. P. SCHÜTZENBERGER*

REPRÉSENTATION SUR UN ENSEMBLE DE MOTS




légende :

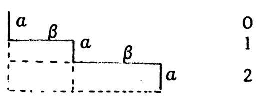



sous-graphes irréductibles

On a construit le graphe comme indiqué au §3 ; les deux liaisons non triviales sont obtenues par déplacement de $\alpha\beta$ :

$$\underbrace{\begin{matrix}\alpha\beta & \alpha\alpha\beta\\ \alpha\beta & \alpha\beta\alpha\end{matrix} \longrightarrow}_{\text{triviale}} \underbrace{\begin{matrix}\alpha & \alpha\beta & \alpha\beta\\ \alpha & \alpha\beta & \beta\alpha\end{matrix} \longrightarrow \begin{matrix}\alpha\alpha & \alpha\beta & \beta\\ \alpha\beta & \alpha\beta & \alpha\end{matrix}}_{\text{non triviales}}$$

En remplaçant $..\alpha..\alpha..\alpha..$ par $..3..2..1..$ et $..\beta..\beta..$ par $..5..4..$, on associe à chaque mot une permutation, et une partition en lisant le mot comme un chemin dans Z x Z :




= partition (0,1,2) ,

ou bien encore, en prenant les places de $\alpha$ dans le mot et en leur soustrayant respectivement 1,2,3 : $\alpha\beta\alpha\beta\alpha \longrightarrow$ places $(1,3,5) \longrightarrow$ partition $(0,1,2)$ .

La représentation figurée ci-dessus est la somme des représentations irréductibles de $S_5$ indexées par les partitions (2,3) , (1,4) et (0,5) de dimensions respectives 5, 4, 1 ; ces représentations correspondent aux trois sous-graphes dont les sommets sont les tableaux de Young standard de formes respectives (2,3), (1,4) et (0,5), les dits tableaux étant dérivés des mots par les techniques appropriées du monoïde plaxique.

Reprinted from JOURNAL OF COMBINATORIAL THEORY, Series B Vol. 30, No. 1, February 1981
All Rights Reserved by Academic Press, New York and London *Printed in Belgium*

## Note

# A Conjecture on Sets of Differences of Integer Pairs

D. PERRIN

*Departement de Mathématiques, Université de Rouen, Rouen, France*

AND

M. P. SCHÜTZENBERGER

*Université Paris VII, U.E.R. de Mathématiques, 75221 Paris, Cedex 05, France*

*Communicated by the Editors*

Received June 8, 1978

We propose a conjecture on the set of differences of integer pairs taken out of a sufficiently dense subset of the plane.

Consider a finite set $X$ of pairs of positive integers $(i, j)$, with $i, j \geqslant 1$, and let $d = \max\{i+j \mid (i, j) \in X\}$.

Associate to $X$ the vertex set $V = \{0, 1,..., d-2\}$ and construct on $V$ a directed graph $G$ having a directed edge from $v$ to $w$ whenever there exist two distinct pairs $(i, j)$ and $(i', j')$ in $X$ such that

$$v = |i - i'|, \qquad w = |j - j'|.$$

The following conjecture is suggested by a problem in coding theory:

CONJECTURE. *If* $\operatorname{Card}(X) \geqslant d$, *the graph* $G$ *has a circuit from* 0 *to* 0.

The bound $d$ is certainly the best one since, for $X = \{(i, d-i) \mid 1 \leqslant i \leqslant d-1\}$, the graph $G$ is reduced to the loops $(x, x)$, for $x = 1, 2,..., d-2$.

The following result conforts the conjecture:

91

0095-8956/81/010091-03\$02.00/0

Copyright © 1981 by Academic Press, Inc.
All rights of reproduction in any form reserved.

PROPOSITION 1. *Let $H$ be the graph obtained by adding to $G$ the edges*

$$(i, d-i-1)$$

*for all $i$ in $V\backslash\{0\}$.*

*If* $\mathrm{Card}(X) \geqslant d$, *then $H$ has a cycle from $O$ to $O$.*

*Proof.* Consider the set $X^r$ of all sequences of $r$ elements of $X$; if $c=\mathrm{Card}(X)$, then $\mathrm{Card}(X^r)=c^r$.

Now, to each $y=(y_1,..., y_r)$ in $X^r$, we associate the sequence $s(y)$ of residuals mod $(d-1)$ of the numbers

$$j_k+i_{k+1}, \qquad k=0, 1,..., r,$$

for $y_k=(i_k, j_k)$ and $j_0=i_{r+1}=0$.

Let us suppose that $c \geqslant d$; then for all large enough $r$, one has

$$c^r > (d-1)^{r+1}.$$

One may then find at least two elements $y, z \in X^r$ such that

$$s(y)=s(z).$$

This provides a circuit from 0 to 0 using successively the edges

$$e_k=(v_k, w_k), \qquad k=1, 2,..., r,$$

where

$$v_k=i_k-m_k, \qquad w_k=j_k-n_k$$

and

$$y_k=(i_k, j_k), \qquad z_k=(m_k, n_k).$$

In fact, either $j_k+i_{k+1}=n_k+m_{k+1}$ and $w_k=v_{k+1}$, or

$$j_k+i_{k+1}=n_k+m_{k+1} \pm (d-1)$$

and $w_k$ may be connected to $v_{k+1}$ using one of the edges added to $G$. ∎

We also prove the following result which is closely related to the conjecture:

PROPOSITION 2. *Suppose that the projections of the set $X$ on the two components are both equal to the set $\{1, 2,..., e\}$ then the graph $G$ has a circuit from* 0 *to* 0 *whenever* $\mathrm{Card}(X) \geqslant e+1$.

*Proof.* If $X$ satisfies the hypothesis and $\mathrm{Card}(X) \geqslant e+1$, we may find a permutation $\sigma$ of the set $\{1, 2,..., e\}$ such that $X$ contains all the elements

$$(i, i\sigma), \qquad i = 1, 2,..., e$$

and an extra element $(m, n)$ with $n \neq m\sigma$.

If $r$ is the order of the permutation $\tau$ defined by

$$i\tau = e - i\sigma + 1, \qquad i = 1, 2,..., e,$$

then the two sequences of elements of $X$

$$y_k = (m\tau^k, m\tau^k\sigma), \qquad k = 0,..., r-1; \quad y_r = (m, n),$$
$$z_k = (n\sigma^{-1}\tau^k, n\sigma^{-1}\tau^k\sigma), \qquad k = 1,..., r; \quad z_0 = (m, n)$$

provide a circuit from 0 to 0 by taking their differences, since for $k = 1, 2,..., r-1$, one has

$$m\tau^k\sigma + m\tau^{K+1} = n\sigma^{-1}\tau^k\sigma + n\sigma^{-1}\tau^{k+1} = e + 1. \quad \blacksquare$$

In the last proposition, it is not possible to suppose only that the projection of $X$ on the first component is equal to $\{1, 2,..., e\}$ and the projection on the second one is included in it. In fact, for

$$X = \{(1, 1), (2, 1), (2, 3), (3, 3)\}$$

the graph $G$ reduces to $G = \{(0, 2), (1, 2), (1, 0)\}$, which has no circuit from 0 to 0.

## NOTE

G. Hansel (private communication) showed that the number of distinct sequences $s'(y)$ taken as in the proof of Proposition 1, but in $\mathbb{N}$ instead of $\mathbb{Z}/(d-1)$, is a polynomial of degree $r+1$ in $d$ whose leading term is

$$[(d-1)/2^{1/2}]^{r+1}.$$

This entails the validity of the conjecture under the stronger hypothesis $\mathrm{Card}(X) \geqslant (2^{1/2}/2)d$.

Other partial results towards the conjecture have been obtained by Imre Simon (São Paulo), J. E. Pin (Paris) and J. P. Duval (Rouen).

Printed by the St. Catherine Press Ltd., Tempelhof 41, Bruges, Belgium

# Année 1982

## Bibliographie


[1982-1] Alain Lascoux et Marcel-Paul Schützenberger. Polynômes de Schubert. *C. R. Acad. Sci. Paris Sér. I Math.*, 294(13) :447–450, 1982.

[1982-2] Alain Lascoux et Marcel-Paul Schützenberger. Structure de Hopf de l'anneau de cohomologie et de l'anneau de Grothendieck d'une variété de drapeaux. *C. R. Acad. Sci. Paris Sér. I Math.*, 295(11) :629–633, 1982.

**C. R. Acad. Sc. Paris, t. 294 (29 mars 1982)** **Série I – 447**

GÉOMÉTRIE ALGÉBRIQUE. — *Polynômes de Schubert*. Note (*) de **Alain Lascoux** et **Marcel-Paul Schützenberger,** Correspondant de l'Académie.

Nous définissons une famille de polynômes généralisant les fonctions symétriques de Schur, qui grâce à l'introduction d'une forme quadratique, permettent des calculs effectifs dans l'anneau de cohomologie des variétés de drapeaux.

*ALGEBRAIC GEOMETRY.* — Schubert Polynomials.

*We define a family of polynomials generalizing Schur symmetrical functions. We examine a subfamily and give explicit relations hips in the cohomology ring of the flag manifold.*

1. On considère l'anneau $\mathbb{Z}[A]$ des polynômes en les variables de $A=A_{n+1}=\{a_1, \ldots, a_{n+1}\}$ et le groupe $W=W_{n+1}$ des permutations de A; W est engendré par les transpositions $\sigma_i$ échangeant $a_i$ et $a_{i+1}$; chaque $w \in W$ est étendu à un isomorphisme $f \to f^w$ de $\mathbb{Z}[A]$ et on utilise l'abréviation $f^{1+w}=f+f^w$; les annexes I et II précisent les autres notations.

Soient $r', r'' \in \mathbb{Z}$ fixes; on associe à chaque $\sigma_i$ l'opérateur linéaire $D_{\sigma_i}(r', r'')$, noté $D_\sigma$ lorsqu'aucune confusion n'est possible, envoyant chaque $f \in \mathbb{Z}[A]$ sur le polynôme :

$$(1.1) \qquad f\,D_\sigma=[f(r'+r''\,a_i)/(a_i-a_{i+1})]^{1+\sigma_i} \in \mathbb{Z}[A].$$

On vérifie que $D_\sigma D_\sigma = r'' D_\sigma$ et que pour tout autre transposition $\tau$ :

$$(1.2) \qquad D_\sigma D_\tau = D_\tau D_\sigma \quad \text{ou} \quad D_\sigma D_\tau D_\sigma = D_\tau D_\sigma D_\tau,$$

selon que $\sigma$ et $\tau$ commutent ou non.

Donc, d'après la proposition 5 de [14], l'opérateur $D_w=D_\sigma D_{\sigma'} \ldots D_{\sigma''}$, où $\sigma\sigma' \ldots \sigma''$ est une décomposition réduite de $w$, est bien défini pour chaque $w \in W$. On pose désormais $\partial_w = D_w(1, 0)$ et $\pi_w = D_w(0, 1)$ (*cf.* [1] et [3], [4] pour $\partial$, et indépendamment [5] pour $\pi$), et l'on désigne par $\omega$ l'élément de longueur maximale de W.

(1.3) Définition. — Pour chaque permutation $w \in W$, le *polynôme de Schubert* d'indice $w$ est $X_w = a^E \partial_{\omega w}$ où $a^E = a_1^n a_2^{n-1} \ldots a_n$ (*cf.* annexe).

Par construction, $X_w$ est symétrique en $a_i$ et $a_{i+1}$ si et seulement si $1(w) < 1(w\sigma_i)$.

On reconnaît dans :

$$(1.4) \qquad f\,\pi_\omega = \Pi_{i<j}(a_i-a_j)^{-1}\,\Sigma_w[(-1)^{l(w)}\,a^E f]^w,$$

l'expression du symétriseur de Bott, et celle du symétriseur de Jacobi $\partial_w$ serait obtenue en remplaçant $a^E$ par 1 dans (1.4). Les fonctions de Hall-Littlewood [11] de paramètre $q$ sont données par la formule :

$$(1.5) \qquad Q_I = (\Pi_{i<j}(1-q\,a_j/a_i)\,a^{I\dagger})\,\pi_\omega,$$

pour toute suite non décroissante I d'entiers positifs.

Comme (1.1) et (1.2) restent valables dans l'algèbre du groupe commutatif engendré par les éléments de A, on peut prendre pour $f$ un monôme $a^I$ où $I \in \mathbb{Z}^{n+1}$. Utilisant les définitions de l'annexe et la factorisation de $\pi_\omega$ en produit de $\pi_w$, on obtient la forme combinatoire du théorème classique de Bott :

(1.6) Théorème (Bott). — *Si* $I \geqq -E$, *alors* $a^I \pi_\omega = S_{I\dagger}(A)$.

2. La formule de Pieri. — Soit $X_w$ un polynôme de Schubert et I le code de $w$. Il résulte immédiatement de la définition (1.3) que $X_w$ est un polynôme de degré $l(w)=|I|$ en les variables de $A_m=\{a_1, \ldots, a_m\}$, où $m$ est la longueur de I.

Un calcul facile montre que $X_w=X_{w'}$ quand $w'$ est la permutation de $W_{n'+1}$, $n' \geqq n$, ayant même code I que $w$.

Si I est une suite non décroissante, $X_w$ est la fonction de Schur $S_K(A_m)$ dont l'indice K est l'évaluation de I; les polynômes de ce type correspondent aux sous-variétés de Schubert des grassmanniennes, variétés dites « spéciales » lorsque $X_w=S_p(A_m)$ ou $=\Lambda_p(A_m)$, $1 \leqq p, m \leqq n$. La formule 2.2 ci-dessous pour $p=1$ (c'est-à-dire pour $X=S_1(A_m)=\Lambda_1(A_m)=a_1+\ldots+a_m$) est due à Monk [12]; Hiller [8] a montré que cette dernière entraînait les résultats classiques pour les grassmanniennes.

(2.1) Définition. — Soient $w \in W$ et $p, m \geqq 1$. Un *m-soulèvement gauche* (resp. *droit*) *de degré p de w* est une permutation $\zeta$ telle que, $\zeta=\zeta_1 \zeta_2 \ldots \zeta_k$ étant sa décomposition en cycles, on ait :

(2.1.1) $$p=l(w\zeta)-l(w)=\Sigma\, l(\zeta_i);$$

(2.1.2) pour chaque cycle $\zeta_i$, posant $w_i=w\zeta_i$, d'une part $jw>jw_i$ (resp. $jw<jw_i$) pour exactement un $j$, $1 \leqq j \leqq n+1$, et d'autre part $j'w \neq j'w_i$ pour exactement un $j'>m$ (resp. $j'<m$).

(2.2) Formule. — *Soient $w \in W$ et $X=\Lambda_p(A_m)$ (resp. $=S_p(A_m)$). Si $n \geqq m+p$, on a :*

$$XX_w=\Sigma\, X_{w\zeta},$$

*où la somme est étendue à tous les m-soulèvements gauches (resp. droits) de degré p de w.*

Par exemple, si $X=\Lambda_2(A_5)$ (i. e. $=\Sigma_{1 \leqq i<j \leqq 5}\, a_i a_j$) et $w=351\,974\,286$, on trouve $XX_w=X_{473\,981\,256}+X_{472\,983\,156}+X_{463\,981\,275}+X_{462\,983\,175}$.

La preuve se fait par double récurrence sur $p$ et $m$ au moyen de l'identité $\Lambda_p(A_{m+1})=\Lambda_p(A_m)+a_{m+1}\,\Lambda_{p-1}(A_m)$ (resp. de l'identité correspondante pour $S_p$).

Soit $\mathscr{T}$ l'ensemble des paires $(w, w') \in W \times W$ telles que l'on puisse trouver $a \in A$ et $v, w_1, \ldots, w_k \in W$ satisfaisant $X_w-X_{w'}-a\,X_v=\Sigma\, X_{w_i}$; $\mathscr{T}$ est la relation de consécutivité d'une relation d'ordre. Soit d'autre part $\succ$ la fermeture de transivité de l'union de $\mathscr{T}$ et des paires $(w, w')$ et $(w', w)$ telles que $X^{\zeta}_{w'}=X_x|_{a_1=0}$ où $\zeta$ désigne la permutation circulaire envoyant chaque $a_i$ sur $a_{i+1}$. Le préordre $\succ$ est invariant pour $w \to w^{-1}$ et l'équivalence associée $\approx$ est invariante pour $w \to \omega w \omega$; quand $w \approx w'$, les codes de $w$ et de $w'$ ont même évaluation.

Ces remarques se déduisent du cas $p=1$ de la formule 2.2; elles permettent de montrer que les $X_w$ sont des polynômes à coefficients non négatifs et que $X_w=(a_1+\ldots+a_m)(a_1+\ldots+a_{m'})\ldots(a_1+\ldots+a_{m''})$, où $m, m', \ldots, m''$ forme une suite croissante d'entiers dont les différences sont au moins égales à 2, quand $w$ est maximal pour $\succ$.

3. Une famille particulière. — Soit $S_I(\mathbb{B})$ une fonction de Schur drapeau. On dit que la suite $I=(i_1, \ldots, i_m)$ *encadre* $\mathbb{B}$ si card $(B_{m'} \setminus B_k) \leqq m'-k+i_{m'}-i_k$ pour tout $m' \leqq m$ et tout $k<m'$. tel que $i_{k-1} \neq i_k$. Lorsque I est une partition et que I encadre $\mathbb{B}$, il existe une suite $\mathbb{C}$ non décroissante de parties de A et une partition J' telles que $S_I(\mathbb{B})=\Lambda_{J'}(\mathbb{C})$; cette propriété de dualité admet une réciproque moyennant quelques définitions supplémentaires (*cf.* [9]).

C. R. Acad. Sc. Paris, t. 294 (29 mars 1982) Série I — 449

(3.1) THÉORÈME. — *Une fonction de Schur drapeau* $S_I(\mathbb{B})$ *est un polynôme de Schubert si et seulement si* I *est une partition et encadre* $\mathbb{B}$. *et dans ce cas* I *est l'évaluation du code de la permutation indiçant le polynôme de Schubert.*

*Réciproquement, soit* $w \in W$. *Les conditions suivantes sont équivalentes :*

(i) $X_w$ *est une fonction de Schur drapeau;*

(ii) $w$ *appartient à une classe minimale de* $\succ$;

(iii) *l'évaluation du code de* $w^{-1}$ *est l'adjointe de l'évaluation du code de* $w$;

(iv) $w \approx w'$ où $X_{w'}$ *est une fonction de Schur propre;*

(v) $w \approx w'$ où $X_{w'}$ *est un monôme.*

La preuve se fait par induction sur la longueur de $w$. Elle repose sur un diagramme montré à l'un de nous par J. Riguet il y a maintes années qui joue vis-à-vis des fonctions de Schubert un rôle analogue à celui du diagramme de Ferrers [11] pour les fonctions de Schur [13]. Cette construction n'a pu être développée ici.

4. UNE FORME QUADRATIQUE. — Soient $\mathscr{I}$ l'idéal de $\mathbb{Z}[A]$ engendré par les polynômes symétriques en toutes les variables et $\mathscr{H} = \mathbb{Z}[A]/\mathscr{I}$. Il est bien connu [2] que $\mathscr{H}$ peut s'interpréter comme l'anneau de cohomologie entière de la variété des drapeaux complets de sous-espaces vectoriels de $\mathbb{C}^{n+1}$; une $\mathbb{Z}$-base de $\mathscr{H}$ est formée des classes dans $\mathscr{H}$ des $X_w$, que nous noterons encore par la même lettre.

Une autre base de $\mathscr{H}$ est $\mathscr{E} = \{ a^I : I \in \mathbb{N}^{n+1} : I \leqq E\dagger \}$.

Soient $a^I$, $a^J \in \mathscr{E}$. On pose :

$$\langle a^I, a^J \rangle = a^{I - J\dagger} \pi_\omega. \tag{4.1}$$

La différence $I' = I - J\dagger$ satisfait $-E \leqq I' \leqq E\dagger$. Donc d'après le théorème 1.6 et les remarques de la fin de l'annexe II, on a $\langle a^I, a^J \rangle = \langle a^J, a^I \rangle \in \{-1, 0, 1\}$, avec de plus $\langle a^I, a^J \rangle = 0$ quand I et J n'ont pas le même poids. On étend par linéarité $\langle\ ,\ \rangle$ à une forme quadratique $\mathscr{H} \times \mathscr{H} \to \mathbb{Z}$.

(4.2) THÉORÈME. — *La base adjointe de* $\mathscr{E}$ *par rapport à* $\langle\ ,\ \rangle$ *est formée des polynômes* $P_I = \Pi_{0 \leqq m \leqq n+1} \Lambda_{i_m} (A \diagdown A_{n-m+1})$ *pour* $I \in \mathbb{N}^{n+1}$ *et* $I \leqq E\dagger$.

(4.3) THÉORÈME. — *Pour tout* $w, w' \in W$, $\langle X_w, X_{w'} \rangle \equiv (-1)^{l(w)}$ *ou* 0 *selon que* $w' = \omega w \omega$ *ou non.*

Ce dernier résultat est obtenu en étendant aux polynômes de Schubert un énoncé déjà connu pour les fonctions de Schur [10] et en utilisant le fait que si $l(w) + l(w') = l(\omega)$, on a $X_w X_{w'} \equiv a^E$ ou 0 selon que $w' = \omega w$ ou non (*cf.* Ehresmann [6], et Chevalley pour une extension aux groupes de Coxeter finis).

Si $Y \in \mathscr{H}$ est un polynôme homogène de degré $p$, la formule de redressement de Bott-Rota (Bott-Rota's straightening) :

$$(-1)^p Y \equiv \Sigma \langle Y, P_I \rangle a^I \equiv \Sigma \langle Y, a^I \rangle P_I \ (\text{mod. } \mathscr{I}),$$

où la sommation porte sur toutes les suites $I : 0 \leqq I \leqq E\dagger$ de poids $p$, est un corollaire immédiat du théorème 4.2.; on notera qu'elle permet un calcul effectif dans $\mathscr{H}$.

ANNEXE I. — Le *poids* d'une suite $I = (i_1, \ldots, i_m) \in \mathbb{Z}^m$ est la somme $|I|$ des $i_j$; on utilise les abréviations $a^I = a_1^{i_1} \ldots a_m^{i_m}$ et $I\dagger = (i_m, \ldots, i_1)$, et on réserve la notation E pour la suite $(n, n-1, \ldots, 1, 0)$; si tous les $i_j$ sont $\geqq 0$, l'*évaluation* de I est la partition de $|I|$ obtenue en réordonnant en ordre non décroissant les $i_j$ strictement positifs.

C. R. Acad. Sc. Paris, t. 295 (29 novembre 1982) Série I — 629

GÉOMÉTRIE ALGÉBRIQUE. — *Structure de Hopf de l'anneau de cohomologie et de l'anneau de Grothendieck d'une variété de drapeaux*. Note (*) de **Alain Lascoux** et **Marcel-Paul Schützenberger,** Correspondant de l'Académie.

On donne des formules de développement des polynômes de Schubert et de Grothendieck traduisant les structures d'algèbre de Hopf respectives des anneaux de cohomologie et de Grothendieck des variétés de drapeaux. On obtient comme corollaire des propriétés nouvelles des décompositions réduites des éléments du groupe symétrique.

*ALGEBRAIC GEOMETRY*. — Hopf Algebra Structures of the Cohomology Ring and Grothendieck Ring of a Flag Manifold.

*Hopf algebra structures of the cohomology ring and of the Grothendieck ring of flag manifolds provide new formulas for the associated polynomials; hence independent proofs of results on the reduced decompositions in the symmetric group that were obtained otherwise from consideration of the nilplactic monoid.*

1. Polynômes de Schubert. — On sait (*cf.* [2], [4], [10]) que l'algèbre des représentations du groupe symétrique est une algèbre de Hopf, la preuve reposant pour l'essentiel sur l'expression d'une fonction de Schur $S_I(A)$ en les variables de l'ensemble A comme une somme de produits $S_J(A-B)\, S_K(B)$, où B est une partie donnée de A, c'est-à-dire sur la structure de pré-λ-anneau de A. Nous étendons ici ces formules aux généralisations des fonctions de Schur que sont les polynômes de Schubert et de Grothendieck. Les notations sont celles de [5]. En particulier $A(=A_n)$ est l'ensemble totalement ordonné (alphabet) $\{a_1<\ldots<a_n\}$ et $W(=W_n)$ le groupe symétrique agissant sur A; ses éléments sont désignés par la permutation correspondante de 1, 2, ..., $n$ ou, sans qu'il puisse y avoir ambiguïté, d'un alphabet quelconque, ce qui permet d'interpréter tout sous-mot de longueur $m$ de $w=w_1\ldots w_n\in W_n$ comme un élément de $W_m$. Réciproquement, pour $m$ positif, on désignera par $m\nearrow$ l'injection de $W_n$ dans $W_{n+m}$ envoyant chaque $w_1\ldots w_n$ sur $1\,2\ldots m\, w_1+m\ldots w_n+m$. On réservera la notation $\omega(=\omega(n))$ pour l'élément $n\, n-1\ldots 2\,1$ de longueur maximale de $W_n$.

Les *polynômes de Schubert* $X_w(A)$ (notés $X_w$ s'il est inutile de spécifier l'ensemble de variables) sont définis par la formule :

1.1 $$X_w=X_\omega\,\partial_{\omega w}\quad\text{avec}\quad X_\omega=a_1^{n-1}\ldots a_{n-2}^2\,a_{n-1},$$

où $\partial$ est l'opérateur de symétrisation décrit dans [5] à la suite de Demazure [3], Bernstein, J. M. Gelfand et S. Gelfand [1]. Les classes des polynômes de Schubert (les *cycles de Schubert*) dans l'anneau de cohomologie de la variété de drapeaux sont une $\mathbb{Z}$-base de cet anneau. Posant $\partial_i=\partial_{\sigma_i}$ pour chaque générateur $\sigma_i$ de W (échangeant $a_i$ et $a_{i+1}$), on a en particulier :

1.2 $$X_w\,\partial_i=X_{w\sigma_i}\ \text{ou}\ 0,\quad \text{selon que}\ l(w\,\sigma_i)<l(w)\ \text{ou non}.$$

Nous définissons un autre endomorphisme $\delta_i$ du $\mathbb{Z}$-module de base $\{X_w\}$ par les relations :

1.3 $$X_w\,\delta_i=X_{\sigma_i w}\ \text{ou}\ 0,\quad \text{selon que}\ l(\sigma_i\,w)<l(w)\ \text{ou non}.$$

On a identiquement :

1.4 $$\delta_i\,\partial_j=\partial_j\,\delta_i\qquad (1\leqq i,j\leqq n).$$

Soit maintenant $m\leqq n$ donné. On pose $B_m=A-A_m=\{a_{m+1}<\ldots<a_n\}$ et on se propose de trouver des entiers $d_w^m(u,v)$ (de fait non négatifs) tels que :

1.5 $$X_w(A)=\Sigma\,\{d_w^m(u,v)\,X_v(A_m)\,X_u(B_m) : u\in W_m,\ v\in W_{n-m}\}.$$

Dans le cas particulier où $m=1$ et où $w=1\,n\,n-1\ldots 2=1\nearrow\omega'$ avec $\omega'=\omega(n-1)$, $X_w$ est une *fonction de Schur drapeau* que l'on sait développer selon les puissances de $a=a_1$ (*cf.* Macdonald [8]); le résultat peut s'écrire :

1.6 $$X_{1\nearrow\omega'}(A)=X_{\omega'}(B)(1+a\delta_{n-2})\ldots(1+a\delta_1),$$

avec $B=A-\{a\}=\{a_2<\ldots<a_n\}$. Comme les opérateurs $\delta$ et $\partial$ commutent, on en déduit :

PROPOSITION 1.7. — *Soit* $w=i\,w_2\ldots w_n\in W_n$, $w'=w_2\ldots w_n\in W_{n-1}$. *Alors*

$$X_w(A)=X_{w'}(B)\,a^{i-1}(1+a\delta_{n-2})\ldots(1+a\delta_i).$$

Par exemple :

1.8 $$X_{263154}=X_{52143}\,a(1+a\delta_4)(1+a\delta_3)(1+a\delta_2)$$
$$=a\,X_{52143}+a^2(X_{42153}+X_{52134})+a^3\,X_{32154}+a^4\,X_{23154}.$$

Le développement de $X_w$ selon les puissances de $a$ est l'opération duale de la multiplication par $\Sigma_{0\leq k}\,a^k=(1-a)^{-1}$ que la formule de Pieri permet de calculer explicitement en termes de soulèvements (*cf.* [5]). En effet, quand $u=1\nearrow\omega'$ avec $\omega=\omega(n-1)$, on a :

1.9 $$X_u(1-a)^{-1}=\Sigma\{X_v : v\in V\},$$

où V est l'intervalle entre $1\nearrow\omega'$ et $\omega$ selon l'ordre de Bruhat, ce qui s'écrit aussi :

1.10 $$X_u(1-a)^{-1}=X_\omega(A)(1+\delta_{n-1})\ldots(1+\delta_1).$$

Utilisant l'expression de $X_u$ fournie par 1.6, on en déduit :

PROPOSITION 1.11. — $X_{1\nearrow w}(A)=\Sigma\,a^{l(w)-l(v)}X_v(B)$ *où la somme est étendue à tous les* $v\in W_{n-1}$ *tels que nv apparaisse dans le produit* $X_{1\nearrow w}(A)(1-a)^{-1}$.

Par application successive de la proposition 1.7, on déduit le cas de $m$ quelconque; on traite d'abord le cas $w_1>w_2>\ldots>w_m$.

PROPOSITION 1.12. — *Soit* $m\leqq n$, $w\in W_n$ *tel que* $w_1>w_2>\ldots>w_m$, $w'=w_{m+1}\ldots w_n\in W_{n-m}$, $a^{w,m}$ *le monôme* $a_1^{w_1-1}a_2^{w_2-1}\ldots a_m^{w_m-1}$, B *l'alphabet* $\{a_{m+1}<\ldots<a_n\}$, $\Delta_{w,m}$ *l'opérateur*

$$(1+a_1\,\delta_{n-m-1})\ldots(1+a_1\,\delta_{w_1-m+1})\ldots(1+a_m\delta_{n-m-1})\ldots(1+a_m\delta_{w_m}).$$

*Alors :*

$$X_w(A)=a^{w,m}X_{w'}(B)\,\Delta_{w,m}.$$

On sait par ailleurs décomposer les monômes $a^I$ dans la base des polynômes de Schubert (*cf.* [6]) : soit C un nouvel alphabet infini, $A'_m$ l'alphabet $\{a_1<\ldots<a_m<c_1<c_2\ldots\}$, $\partial'_i$ *et* $\partial'_w$ les opérateurs correspondant à $A'_m$; soit $\varepsilon$ l'augmentation $\mathbb{Z}[A'_m]\to\mathbb{Z}$ envoyant chaque polynôme P sur son terme constant $P\,\varepsilon$. Alors (*cf.* [6], *cf.* [3] pour les cycles de Schubert) on a :

1.13 $$\forall\,P\in\mathbb{Z}[A_m],\qquad P=\Sigma_w\,P\,\partial'_{w^{-1}}\varepsilon.X_w(A'_m).$$

En fait, l'alphabet C n'est qu'un intermédiaire de calcul qui ne figure pas dans le développement 1.13; par exemple :

$$a_1^2\,a_2^4=X_{361245}(A'_2)-X_{451236}(A'_2)-X_{531246}(A'_2),$$

C. R. Acad. Sc. Paris, t. 295 (29 novembre 1982) Série I — 631

puisque :

$$X_{361245}(A'_2)=a_1^4a_2^2+a_1^3a_2^3+a_1^2a_2^4, \qquad X_{451236}(A'_2)=a_1^3a_2^3,$$
$$X_{531246}(A'_2)=a_1^4a_2^2.$$

Combinant 1.12, 1.13 et 1.4, on obtient :

THÉORÈME 1.14. — *Soit* $m\leqq n$, *soit* $w, \zeta\in W_n$, $\zeta_{m+1}=m+1, \ldots, \zeta_n=n$ *tels que* $w\zeta$ *soit l'élément de plus grande longueur de* $w\,W_m$, *soit* $w'=w_{m+1}\ldots w_n$. *Alors, reprenant les notations de* 1.12, *on a l'identité :*

$$X_w(A)=\Sigma_v\, a^{w\zeta, m}\, X_{w'}(B)\, \Delta_{w\zeta, m}\, \partial'_{v^{-1}}\, \varepsilon . X_{v\zeta^{-1}}(A'_m)$$

*somme sur tous les* $v$ *tels que* $l(v\zeta^{-1})=l(v)-l(\zeta)$.

Par exemple :

$$X_{316\,542}(A)=a_1^2\, X_{4321}(B)(1+a_1\,\delta_3)(1+a_1\,\delta_2)(1+a_2\,\delta_3)(1+a_2\,\delta_2)(1+a_2\,\delta_1).$$

et le coefficient de $X_{351246}(A'_2)$, polynôme égal à $a_1^3a_2^2+a_1^2a_2^3$, est :

$$X_{316542}(A)\,\partial'_2\,\partial'_3\,\partial'_4\,\partial'_1\,\partial'_2\,\varepsilon=X_{4321}(B)\,\delta_3\,\delta_2\,\delta_1=X_{1432}(B)$$

puisque :

$$(1+a_2\,\delta_3)(1+a_2\,\delta_2)(1+a_2\,\delta_1)\,\partial'_2\,\partial'_3\,\partial'_4=\delta_3\,\delta_2\,\delta_1$$

et :

$$a_1^2(1+a_1\,\delta_3)(1+a_1\,\delta_2)\,\partial'_1\,\partial'_2\,\varepsilon=a_1^2\,\partial'_1\,\partial'_2=1.$$

Nous terminons le paragraphe sur un cas particulier du théorème lié aux propriétés des décompositions réduites dans le groupe symétrique.

Soit $w\in W_{n-m}$; $X_{m\nearrow w}(A)$ est un polynôme symétrique en $a_1, \ldots, a_m$ et cette propriété est respectée par la décomposition 1.14. En particulier, le terme obtenu en annulant B est une fonction symétrique en $a_1, \ldots, a_m$ qui est une somme à coefficients entiers non négatifs de fonctions de Schur $S_I(A_m)$ (les fonctions de Schur sont les polynômes de Schubert symétriques; on les indexe par les partitions, plutôt que par les permutations correspondantes). On a donc :

1.15 $$X_{m\nearrow w}(A)\,|_{B=0}=\Sigma_I\, d_w(I)\, S_I(A_m),$$

où les $d_w(I)$ sont des entiers non négatifs qui ne dépendent pas de $m$ et où la somme s'étend aux partitions de poids $l(w)$; toutefois, comme $S_I(A_m)=0$ si la longueur de I est supérieure à $m$, les $d_w(I)$ qui apparaissent effectivement dans 1.15 ne dépendent pas de $m$ quand ce paramètre excède $l(w)$.

L'application £ : $w\to\Sigma\, d_w(I)\, I$ du groupe symétrique dans l'ensemble des sommes de partitions généralise les tableaux de Young standards (qui peuvent être considérés comme les chaînes complètes dans le treillis des partitions). En particulier, le nombre des décompositions réduites de $w$ est égal à $\Sigma\, d_w(I)\, n_I$, où $n_I$ est la dimension de la représentation irréductible du groupe symétrique $W_{l(w)}$. L'existence d'une telle application avait été conjecturée par Stanley. On remarque que $\Sigma_I\, d_w(I)=1$ si et seulement si $w$ est une permutation caractérisée au paragraphe 3 de [5] et dite *vexillaire* (dans les notations présentes, $w_1\ldots w_n$ est vexillaire si et seulement si il ne contient pas de sous-mot $w_h\,w_i\,w_j\,w_k$ avec $w_i<w_h<w_k<w_j$).

Les $d_w(\mathrm{I})$ se calculent facilement par les relations de [5], § 2, dont les propriétés d'invariance impliquent que $d_{w^{-1}}(\mathrm{I})=d_w(\mathrm{I}^{\sim})$. Un résultat plus précis repose sur le *monoïde nilplaxique*, mentionné dans l'appendice. Par exemple :

$$£\,(3251746)=(1,1,1,4)+(1,1,2,3)+(2,2,3)+2(1,2,4)+(1,3,3)+(3,4).$$

2. Polynômes de Grothendieck. — La variété de drapeaux est munie de fibrés inversibles $\mathrm{L}_1, \ldots, \mathrm{L}_n$ dont les classes de Chern respectives sont $1+a_1, \ldots, 1+a_n$. On pose $x_i=1-\mathrm{L}_i^{-1}$; l'anneau de Grothendieck $\mathscr{K}$ de la variété de drapeaux est le quotient de l'anneau de polynômes $\mathbb{Z}[x_1, \ldots, x_n]$ par l'idéal engendré par les fonctions symétriques en les $x_i$. Les $\mathrm{X}_w$, en l'alphabet $\{x_1, \ldots, x_n\}$, sont une $\mathbb{Z}$-base de $\mathscr{K}$, tout comme les $\mathrm{X}_w(\mathrm{A})$ sont une base de l'anneau de cohomologie, mais il est plus intéressant de prendre comme base les classes des faisceaux structuraux des variétés de Schubert.

On pose $\pi_i=\mathrm{L}_i\,\partial_i$ (où $\partial_i$ est l'opérateur correspondant à l'alphabet $\{\mathrm{L}_1<\ldots<\mathrm{L}_n\}$) et l'on définit les opérateurs $\pi_w$ comme produits des $\pi_i$ (*cf.* [6]), et les polynômes de Grothendieck par :

2.1 $$\mathrm{G}_w=\mathrm{G}_\omega\,\pi_{\omega w} \qquad \text{avec} \quad \mathrm{G}_\omega=x_1^{n-1}\,x_2^{n-2}\ldots x_{n-1}.$$

La classe de $\mathrm{G}_w$ dans $\mathscr{K}$ est la classe du faisceau structural de la variété de Schubert d'indice $w$; $\mathrm{G}_w$ est un polynôme non homogène en l'alphabet $\{x_1, \ldots, x_n\}$ dont la partie de plus bas degré est $\mathrm{X}_w$, et donc les $\mathrm{G}_w$ sont linéairement indépendants.

La définition 2.1, jointe à $\pi_i^2=\pi_i$ pour tout $i$, implique :

2.2 $$\mathrm{G}_w\,\pi_i=\mathrm{G}_{w\,\sigma_i} \text{ ou } \mathrm{G}_w \text{ suivant que } l(w\,\sigma_i)<l(w) \text{ ou non,}$$

ou bien encore :

2.3 $$\mathrm{G}_w(\pi_i-1)=\mathrm{G}_{w\sigma_i}-\mathrm{G}_w \text{ ou } 0 \text{ suivant que } l(w\sigma_i)<l(w) \text{ ou non.}$$

On définit symétriquement les opérateurs $\varphi_i$ sur le $\mathbb{Z}$-module de base $\{\mathrm{G}_w\}$ par

2.4 $$\mathrm{G}_w.\varphi_i=\mathrm{G}_{\sigma_i w}-\mathrm{G}_w \text{ ou } 0 \text{ suivant que } l(\sigma_i\,w)<l(w) \text{ ou non.}$$

Les opérateurs $\varphi_i$ et $\pi_j$ commutent et toutes les formules du premier paragraphe se transcrivent *mutatis mutandis*.

Par exemple, l'analogue de la proposition 1.7 se présente ainsi :

Théorème 2.5. — *Soit :*

$$w\in \mathrm{W}_n, \qquad w_1=i, \qquad w'=w_2\ldots w_n, \qquad x_1=x, \qquad \mathscr{Y}=\{x_2<\ldots<x_n\}.$$

*Alors :*

$$\mathrm{G}_w=\mathrm{X}_{w'}(\mathscr{Y})\,x^{i-1}(1+x\,\varphi_{n-2})\ldots(1+x\,\varphi_i).$$

Par exemple, la permutation considérée en 1.8 donne :

2.6 $$\mathrm{G}_{263154}=x(1-x)^2\,\mathrm{G}_{52143}(\mathscr{Y})+x^2(1-x)(\mathrm{G}_{42153}(\mathscr{Y})+\mathrm{G}_{52134}(\mathscr{Y})) + x^3(1-x)\,\mathrm{G}_{32154}(\mathscr{Y})+x^4\,\mathrm{G}_{23154}(\mathscr{Y}).$$

La décomposition d'un polynôme de Grothendieck suivant les puissances de la première lettre $x$ est l'opération duale de la multiplication par les polynômes *spéciaux*, c'est-à-dire de la *formule de Pieri* dans l'anneau de Grothendieck, que nous expliciterons ailleurs.

Appendice. — Soit $\mathrm{T}=\{\tau_1<\tau_2\ldots<\tau_{n-1}\}$ un alphabet; le *monoïde nilplaxique* NP est le quotient du monoïde libre T par la congruence définie par :

$$\forall j, \quad \forall\, i\leqq j\leqq k \qquad \text{tels que} \quad i+2\leqq k,$$

C. R. Acad. Sc. Paris, t. 295 (29 novembre 1982) Série I — 633

on a :

$$\tau_j\tau_i\tau_k \equiv \tau_j\tau_k\tau_i; \qquad \tau_i\tau_k\tau_j \equiv \tau_k\tau_i\tau_j,$$

$$\tau_j\tau_j \equiv 0; \qquad \tau_j\tau_{j+1}\tau_j \equiv \tau_{j+1}\tau_j\tau_{j+1}.$$

Il est clair que l'application $\tau_j \to \partial_j$ s'étend à un morphisme de NP sur le monoïde engendré par $\{\partial_j : 1 \leqq j \leqq n-1\}$, l'image inverse de 0 étant 0. Le calcul dans NP se ramène au calcul dans le monoïde plaxique moyennant les automorphismes de conjugaison introduits dans [7].

En particulier NP-$\{0\}$ a une section remarquable dans T* qui est formée des tableaux $t$ non congrus à 0, et la classe nilplaxique de chacun d'eux (c'est-à-dire l'ensemble des $v \in \mathrm{T}^*$ tels que $v \equiv t$) est en bijection avec les tableaux standards ayant même forme que $t$.

Dans l'algèbre $\mathbb{Z}(\mathrm{NP})$ la *fonction de Schur* $\mathrm{S_I}$ est, pour chaque partition I, la somme des tableaux de forme I; l'ensemble des $\mathrm{S_I}$ est la $\mathbb{Z}$-base d'une sous-algèbre commutative de $\mathbb{Z}(\mathrm{NP})$ (comme dans l'algèbre plaxique) qui est d'ailleurs isomorphe au quotient de l'algèbre des fonctions de Schur obtenu en annulant toutes les $\mathrm{S_J}$ telles que J n'est pas contenue dans la partition $(1, 2, \ldots, n-1)$.

Soit maintenant $t_\omega$ le seul tableau $\not\equiv 0$ de forme $(1, 2, \ldots, n-1)$. Pour chaque permutation $w \in \mathrm{W}_n$, on prend une décomposition réduite $s = \sigma_{i_1}\sigma_{i_2}\ldots\sigma_{i_k}$ de $w^{-1}\omega$ et on associe à $w$ l'ensemble des tableaux $t$ tels que $t\tau_{i_1}\tau_{i_2}\ldots\tau_{i_k} \equiv t_\omega$. L'union des classes nilplaxiques de ces tableaux est en bijection naturelle (par $\tau_i \to \sigma_i$) avec l'ensemble des décompositions réduites de $w$; elle est indépendante du choix de $s$; les formes de ces tableaux ont été calculées plus haut.

Par exemple, les $11 = 5 + 6$ décompositions réduites de $w = 25143$ correspondent aux éléments des classes nilplaxiques des deux tableaux :

$$\tau_4\tau_3\tau_1\tau_4\tau_2 \qquad \text{et} \qquad \tau_4\tau_3\tau_1\tau_2\tau_4.$$

D'autres propriétés des décompositions réduites se déduisent du remplissage standard d'un diagramme attaché à $w$ (*cf.* [5], p. 449) auquel il ne nous est possible ici que de faire une allusion.

(*) Remise le 22 novembre 1982.

[1] I. N. Bernstein, I. M. Gelfand et S. Gelfand, *Russian Math. Sur.*, 28, 1973, p. 1-26.
[2] P. Cartier, *Séminaire Bourbaki*, n° 597, 1982.
[3] M. Demazure, *Ann. Sc. E.N.S.*, 7, 1974, p. 53-88.
[4] L. Geissinger, in *Combinatoire et représentation du groupe symétrique*, D. Foata, éd., Springer L.N. n° 579, p. 168-181.
[5] A. Lascoux et M. P. Schutzenberger, *Comptes rendus*, 294, série I, 1982, p. 447.
[6] A. Lascoux et M. P. Schutzenberger, *Reports Math. Stockholm*, n° 32, 1982.
[7] A. Lascoux et M. P. Schutzenberger, *Colloque de Naples*, 1978, Quaderni de la Ricerca Scientifica n° 109.
[8] I. G. MacDonald, *Symmetric and Hall Polynomials* (*Oxford Math. Mono.*, 1979).
[9] R. Q. Stanley, Conjecture communiquée par A. Björner, 1982.
[10] A. Zelevinsky, *Representations of Finite Classical Groups*, Springer L.N. n° 869.

*Laboratoire d'Informatique théorique et Programmation,*
*L.A. n° 248, Université Paris-VII, 2, place Jussieu, 75005 Paris.*

# Table des matières

# Tome X

## 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 10 : 1979 – 1982

*À partir de 1978, la majeure partie des travaux mathématiques de Schützenberger sont consacrés à la combinatoire algébrique.*
*L'article « Le monoïde plaxique » lui tenait spécialement à cœur. Ce travail reprend la théorie des tableaux de Young, cette fois-ci en mettant l'accent sur l'aspect monoïde. L'algèbre plaxique est définie comme quotient de l'algèbre libre sur un alphabet totalement ordonné, par une congruence sur les facteurs de longueur 3 due à Knuth. Cette algèbre contient comme sous-algèbre commutative l'anneau des polynômes symétriques, ce qui permet de donner une version non commutative de différentes propriétés des fonctions de Schur.*
*La note « Polynômes de Schubert » fonde la théorie de ces polynômes. Ceux-ci forment une base linéaire de l'espace des polynômes en un ensemble fini de variables, et trouvent de nombreuses applications en géométrie algébrique (variétés de Schubert) ou en interpolation (extension à plusieurs variables de l'interpolation de Newton). Ils contiennent comme sous-famille les fonctions de Schur, la combinatoire des permutations remplaçant alors la combinatoire des partitions.*