Marcel-Paul Schützenberger

ŒUVRES COMPLÈTES

éditées par
Jean Berstel, Alain Lascoux et Dominique Perrin

*

Tome 12 : 1990–

Institut Gaspard-Monge, Université Paris-Est
2009

Introduction
Tome XII : 1990–

Les *polynômes clefs* (caractères de Demazure pour le type A), sont des généralisations non-symétriques des fonctions de Schur. En remontant les constructions au niveau de l'algèbre libre, l'article *Keys & standard bases* [1990-1] donne une interprétation en terme de tableaux, ou de mots satisfaisant des conditions de drapeaux, de ces polynômes. Cette interpétation recoupe la théorie des *bases standard* de Lakshmibai-Seshadri, relative aux variétés de drapeaux pour les groupes classiques.

L'*algèbre des différences divisées* est par définition l'algèbre des combinaisons linéaires de différences divisées, dont les coefficients sont des fonctions rationnelles en les variables sur lesquelles agissent les différences divisées. Elle contient en particulier comme sous-algèbre différentes copies de l'algèbre de Hecke. L'article *Décompositions dans l'algèbre des différences divisées* [1992-2] développe [1987-1] et explicite différents changements de base.

L'article fondamental *Treillis et bases des groupes de Coxeter* [1996-1] part d'un problème qui rejoint les premiers travaux de M.-P. Schützenberger sur le *clivage* des treillis. La question examinée est : comment décomposer le groupe symétrique en deux intervalles complémentaires (relativement à l'ordre d'Ehresmann–Bruhat) ? La réponse exhibe un sous-ensemble minimal de permutations qui code toute l'information sur l'ordre. Ce sous-ensemble engendre un treillis distributif, qui contient comme sous-ensemble ordonné le groupe symétrique, et dont les éléments s'identifient aux *matrices à signe alternant*. On trouvera dans le livre de D. Bressoud [1] de nombreuses propriétés de ces derniers objets, apparus tout récemment en combinatoire. Geck et Kim [2] étendent à tous les groupes de Coxeter finis le plongement dans un treillis.

L'article *Pour le monoïde plaxique* [1997-3], sous forme d'une lettre à ses amis André Lentin et Gian-Carlo Rota, est un plaidoyer de M.-P. Schützenberger pour justifier pourquoi il a consacré autant de ses efforts, dans les vingt dernières années, aux beautés du monoïde plaxique.

Les dernières considérations mathématiques de M.-P. Schützenberger concernent la combinatoire de l'*équation de Yang-Baxter*, et sont exposées dans [3].

---

[1] David M. Bressoud. *Proofs and confirmations.* MAA Spectrum. Mathematical Association of America, 1999. The story of the alternating sign matrix conjecture.

[2] Meinolf Geck and Sungsoon Kim. Bases for the Bruhat-Chevalley order on all finite Coxeter groups. *J. Algebra*, 197(1) :278–310, 1997.

[3] Alain Lascoux. Potentiel Yin sur le groupe symétrique. *Sém. Lothar. Combin.*, 38 :Art. B38a, 12 pp. (electronic), 1996.

Année 1990

Bibliographie

[1990-1] Alain Lascoux et Marcel-Paul Schützenberger. Keys & standard bases. In D. Stanton, editor, *Invariant theory and tableaux (Minneapolis, MN, 1988)*, volume 19 of *IMA Vol. Math. Appl.*, pages 125–144. Springer, 1990.

[1990-2] Marcel-Paul Schützenberger. Sur les modèles mathématiques. Propos d'un mathématicien philomate. In *La Société philomatique de Paris et deux siècles de science en France : Colloque du bicentenaire de la Société philomatique de Paris*, pages 83–88. Presses Universitaires de France, 1990.

[1990-3] Marcel-Paul Schützenberger. Sens et évolution. In Jacques Arsac et Philippe Sentis, editors, *Science et sens*, pages 97–98. Vrin, 1990. Publications de l'Institut Interdisciplinaire d'Études Épistémologiques, Actes du colloque organisé dans le cadre de l'Académie Meudonaise.

THE IMA VOLUMES
IN MATHEMATICS
AND ITS APPLICATIONS VOLUME 19

Dennis Stanton
Editor

Invariant Theory and Tableaux

Springer-Verlag

KEYS & STANDARD BASES

ALAIN LASCOUX AND MARCEL-PAUL SCHÜTZENBERGER*

1. Introduction. The irreducible characters of the linear group on **C** {*Schur Functions*} are combinatorially interpreted as sums of *Young tableaux*.

Demazure **[D1]** **[D2]** has given a "Formule des caractères" which interpolates between a dominant weight, corresponding to a partition I, and the Schur function of index I. For every permutation μ, he obtains a "partial" character which can be interpreted as the class of the space of section $\mathcal{V}_{I,\mu}$ of the line bundle associated to I over the Schubert variety of index μ, in an appropriate Grothendieck ring; identifying this ring with the ring of polynomials, we can view $\mathcal{V}_{I,\mu}$ as a polynomial $\mathcal{D}(\mu, I)$.

An independent study of the same spaces $\mathcal{V}_{I,\mu}$, and more precisely, of their "standard bases", is due to Lakshmibai-Musili-Seshadri **[L-M-S]**. Extending the work of Hodge, they interpret Young tableaux as products of *Plücker coordinates* of the flag variety and associate to them *chains* of permutations to describe the different bases (see also **[L-W]**).

The link between the two constructions is not immediate. Moreover, none of these two point of view furnishes the multiplicative structure of sections which is needed in geometry to describe the *postulation* of Schubert varieties. Indeed, the product $\mathcal{V}_{I,\mu} \otimes \cdots \otimes \mathcal{V}_{I,\mu}$ contains more than the sections corresponding to a multiple of the weight I and thus the products of standard bases are not standard bases.

The answer comes from working in the free algebra rather than the Grothendieck ring or the ring of coordinates. Young tableaux (2.1) are now *words* which are representatives of certain congruence classes (th.2.4). More general words (*frank words*, 2.7) obtained from tableaux by permutation allow to associate to each congruence class two special tableaux *right* and *left keys* (2.9). The set of keys (2.12) is in fact the image of the embedding of the symmetric group in the set of tableaux (embedding originally defined by Ehresmann **[E]** to describe how cells attach in a cellular decomposition of the flag variety).

Now, a standard basis is a set (or a sum) of tableaux having the same right key (th.3.6). To generate it, one uses *symmetrizing operators* (3.5) on the free algebra which lift the operators on the ring of polynomial used by Demazure and Bernstein-Gelfand-Gelfand. Thus, the polynomial $\mathcal{D}(I, \mu)$ is just the commutative image of a sum of standard bases (th.3.8).

For what concerns the multiplicative structure of sections, the answer is also given by keys: the product of two tableaux t, t' belongs to a standard basis iff the right key of t is less than the left key of t' (2.11 and 4.2) . This allows us in section 4 to give a combinatorial interpretation of the Hilbert function associated to a weight

*L.I.T.P., Université Paris 7, 2 Place Jussieu, 75251 PARIS Ced 05, France, supported by the P.R.C. Mathématiques-Informatique

as an enumeration of chains of tableaux (th.4.3 and 4.4). See **[L-S6]** for the related order on the symmetric group and its Eulerianity properties. The link between keys, reduced decompositions of permutations and the Schubert cycles (i.e. the classes of the Schubert varieties in the cohomology ring of the flag manifold) is given in **[L-S4]**.

In section 5, we explicit some different ways of describing the standard bases.

In appendix 6, we have isolated a property of actions of the symmetric group which is of independent interest.

Caution. As usual, operators operate *on their left.*

2. Frank words and keys. Let A^* be the free monoid generated by the alphabet $\mathsf{A} = \{a_1 < a_2 < ...\}$. A word $v = x_1...x_r (x_i \in \mathsf{A})$ is called a *column* iff $x_1 > ... > x_r$ and a *row* iff $x_1 \leq x_2 \leq \cdots \leq x_r$. Let V denote the set of all columns. Every word $w \in \mathsf{A}^*$ admits a unique factorisation as a product of a minimal number of columns : $w = v_1 v_2 \cdots v_k (v_i \in \mathsf{V})$. We shall call it the *column factorisation* of w and denote it occasionally by $w = v_1 \cdot v_2 \cdot \ldots \cdot v_k$, v_1 being the *left column* $w\mathcal{L}$ of w and v_k the *right column* $w\$$ of w . The *shape* of w is the sequence $\|w\| = (|v_1|, ..., |v_r|)$ of the degrees (or lengths) of the column factors of w.

To use a traditional term (see [Mc]), $\|w\|$ is a *composition* of the integer $|w|$ and the $|v_i|$ are the parts of $\|w\|$. On the set of compositions, one has the following preorder: $I \geq J$ iff for every k, the sum of the k biggest parts of I is bigger than the sum of the k biggest parts of J. It is clear that if $I \geq J$ and $J \geq I$, then I is a permutation of J , and that if H is any composition, $IH \geq JH \Leftrightarrow I \geq J$. One can imbed the set of compositions into the set of words : $I = (1I, 2I, ..., rI) \rightarrow (1I \cdots 1)\big((1I+2I)\cdots(1I+1)\big)\cdots\big((1I+2I+\cdots+rI)\cdots(1I+2I+\cdots+(r-1)I)\big)$. We note this word $I\mathbf{M}$ and call it a *composition word*. It can be looked as the maximal element (as a permutation) of the Young group $\mathcal{S}_I \hookrightarrow \mathcal{S}_{1I+\cdots+rI}$. For instance, the composition word $(2,4,1)\mathbf{M}$ is $(21)(6543)(7)$, which is the maximal element of the subgroup $\mathcal{S}_2 \times \mathcal{S}_4 \times \mathcal{S}_1$ of $\mathcal{S}_7$.

Taking the underlying set of a column defines a bijection $v \rightarrow \{v\}$ between the set V of the columns and the family 2^{A} of the subsets of A ; one extends to V the order $\leq$ on A by letting $u \leq v$ iff there is an increasing injection of $\{u\}$ into $\{v\}$. Thus $u \leq v$ is the least order on V that contains both the inclusion order $\{u\} \subset \{v\}$ and the term to term order between equipotent subsets of A.

DEFINITION 2.1. A *contretableau* is a word which is an increasing product of columns.

For instance, if $\mathsf{A} = \{1 < 2 < 3 < \cdots\}$, the word 2 3 41 421 is a contretableau because of $2 \leq 3 \leq 41 \leq 421$.

It is convenient to define another order $\triangleright$ on V by letting $u \triangleright v$ iff there is a decreasing injection of $\{v\}$ into $\{u\}$ and to call a *tableau* any product $u_1 u_2 \cdots u_k$ where the columns u_i are decreasing for $\triangleright$, i.e. $u_1 \triangleright u_2 \triangleright \cdots \triangleright u_k$. For instance, 321 31 2 4 is a tableau because $321 \triangleright 31 \triangleright 2 \triangleright 4$.

The two orders $\leq$ and $\triangleright$ are linked by the fact that $u \triangleright v$ iff $v' \leq u'$ where $v \to v'$ is the bijection on $\mathbf{V}$ induced by the "reversal" of the alphabet $\mathbf{A}$ assumed to be finite (i.e. by the morphism $a_i \to a_{n+1-i}$, n being the cardinal of $\mathbf{A}$).

It follows from the definitions that the shape of any tableau t is a partition of its degree. This suggests writing the letters of t into the boxes of the Ferrers diagram of $\|t\|$. For instance, 321 31 2 4 can be represented by $\begin{smallmatrix} & & 3 \\ & 23 & \\ 1124 & & \end{smallmatrix}$. A similar remark holds for contretableaux and we can represent 2 3 41 421 by $\begin{smallmatrix} & & 2344 \\ & 12 & \\ 1 & & \end{smallmatrix}$. It is a direct consequence of the definition of the orders $\leq$ and $\triangleright$ that each row of the planar writings of tableaux or contretableaux is a weakly increasing sequence of letters.

There is essentially one natural congruence $\equiv$ on $\mathbf{A}^*$ that admits as a section the set of contretableaux, where *natural* means that it commutes with the order preserving injections of alphabets. It is called the *plactic congruence*. As shown by D. Knuth, it can be defined by the following identities where a, b, c are any three letters of $\mathbf{A}$ such that $a < b < c$:

$$baa \equiv aba \; ; \; bba \equiv bab \; ; \; cab \equiv acb \; ; \; bca \equiv bac \tag{2.2}$$

As it has been observed by [**K-L**], these generating congruences are exactly all the pairs of words of degree 3 that are not a column nor a line and that differ by the transposition of two adjacent letters. Thus one member of each pair is a tableau (e.g. $\begin{smallmatrix} b & \\ ac & \end{smallmatrix}$ or $\begin{smallmatrix} b & \\ aa & \end{smallmatrix}$) and the other one, a contretableau (e.g. $\begin{smallmatrix} b\,c & \\ a & \end{smallmatrix}$ or $\begin{smallmatrix} a\,b & \\ a & \end{smallmatrix}$) .

It turns out that the set of all tableaux is also a section of the plactic congruence and the defining relations (2.2) are simply the expression of this fact for the words of degree 3.

Another remarkable property of the plactic congruence is that every tableau (or contretableau) is congruent to the word obtained when reading by rows (from top to bottom) its planar representation. For instance, 321 31 2 4 $\equiv$ 3 23 1124 or 2 3 41 421 $\equiv$ 2344 12 1.

This phenomenon is closely tied with another definition of the plactic congruence $\equiv$ as one of the least congruences on $\mathbf{A}^*$ such that the subalgebra of $\mathbf{Z}(\mathbf{A}^*/\equiv)$ generated by the (non commutative) symmetric sums

$$\Lambda_p = \sum\{v : v \in V \; , |v| = p\} \; , \; p = 1, 2,$$

is a commutative algebra isomorphic to the usual algebra of symmetric polynomials in the letters of $\mathbf{A}$.

To obtain the complete characterisation of the plactic congruence, one needs to add a further condition which follows immediately from 2.2 and which will be used later.

PROPOSITION 2.3. *The plactic congruence $\equiv$ is the least congruence on $\mathbf{A}^*$ for which $\Lambda_1\Lambda_2 \equiv \Lambda_2\Lambda_1$, and which moreover satisfies for any interval $\mathbf{B}$ of $\mathbf{A}$ the relation*

$$w \equiv w' \Rightarrow w \cap \mathbf{B}^* \equiv w' \cap \mathbf{B}^*$$

($w \cap \mathbf{B}^*$ *denotes the word obtained by erasing the letters not in* $\mathbf{B}$).

Taking $\mathbf{B}$ equal to a single letter, 2.3 implies that the plactic congruence commutes with the natural morphism $w \to \underline{w}$ of $\mathbf{A}^*$ onto the free commutative monoid; this can also be directly checked on relations 2.2.

The plactic congruence is no other than the algebraic formalization of Schensted's construction, whose main result can be summarized in the following theorem ([**Sche**], [**L-S1**]).

THEOREM 2.4. 1) *Each plactic class contains a unique tableau* t *and a unique contretableau.*

2) *The elements of the class of* t *are in bijection with the set of permutation tableaux (called insertion tableaux) of the same shape as* t .

By a permutation tableau, we mean, of course, a permutation (of any alphabet) which is at the same time a tableau. Given any word w, we denote $w\mathbf{R}$ the tableau congruent to it and $w@$ its insertion tableau. It is well known (see [**Schu**]) that the involution $w \to w^{-1}$ on permutation words corresponds to the exchange of $w\mathbf{R}$ and $w@$; we shall not use this fact.

More explicitely, the insertion tableau (which is the Q-symbol of Schensted) of a word $w = x_1x_2...$ describes the increasing sequence of the shapes of the tableaux $x_1\mathbf{R}$, $x_1x_2\mathbf{R}$, $x_1x_2x_3\mathbf{R}$,... . The particular choice of the alphabet being irrelevant, $\begin{smallmatrix}2\\13\end{smallmatrix}$, $\begin{smallmatrix}6\\28\end{smallmatrix}$ and $\begin{smallmatrix}\beta\\\alpha\gamma\end{smallmatrix}$, with $\alpha < \beta < \gamma$, must be considered as the same insertion tableau representing the sequence of shapes $\varnothing \to \diamond \to \begin{smallmatrix}\diamond\\\diamond\end{smallmatrix} \to \begin{smallmatrix}\diamond\\\diamond\diamond\end{smallmatrix}$.

More generally, any word congruent to $w@$ will be called an *insertion word* for w. Insertion words are compatible with restriction of alphabets (see [**L-S1**]):

LEMMA 2.5. *Given any word* $w = x_1...x_{m-1}x_m...x_{m+r}x_{m+r+1}...$, *then the word* $w@ \cap \{m, ..., m+r\}$ *is an insertion word for the factor* $x_m \cdots x_{m+r}$.

In particular, as pointed out by Schensted, $w@$ contains the subword $m\ m+1$ iff $x_m \leq x_{m+1}$ and the subword $m+1\ m$ iff $x_m > x_{m+1}$. Call *file* of a permutation of $\{1, 2, 3 \dots\}$ any maximal subword of the type $(m+k)\cdots(m+1)m$. The shape $\|w\|$ corresponds to the files of any insertion word for w. More precisely, one has the following lemma:

LEMMA 2.6. *Let* $w = v_1 \cdot \ldots \cdot v_k$ *be a word,* μ *an insertion word for* w . *Then*

1) *The files of* μ *are the same as those of the composition word* $\|w\|\mathbf{M}$.
2) $\|w\| \leq \|w\mathbf{R}\|$; *equality happens iff* $\|w\|\mathbf{M}$ *is an insertion word for* w.
3) *For each permutation* J *of the shape* $\|w\mathbf{R}\|$, *there exists one and only one word of shape* J *congruent to* w.

Proof. Assertion *1)* is a direct corollary of 2.5: the files of μ are the same as the files of $w@$ and they encode exactly the inequalities $x_i \leq x_{i+1}$ or $x_i > x_{i+1}$ for all the pairs of adjacent letters in w . For what concerns *2)*, it is easy to check that the tableau $\mu\mathbf{R}$ has shape greater than the composition corresponding to the files

of μ ; this composition being $\|w\|$ and the shape of $\mu\mathbf{R} = w@$ being equal to that of $w\mathbf{R}$, we get the required inequality. In the case of equality, the tableau $\mu\mathbf{R}$ is determined by its files : consecutive entries in a file must be in consecutive rows of $\mu\mathbf{R}$. A mild intimacy with the jeu de taquin shows that this last condition is equivalent to requiring that $\|w\|\mathbf{M} \equiv \mu\mathbf{R}$. Finally, condition *3)* is a rewriting of the case where $\|w\|$ is a permutation of $\|w\mathbf{R}\|$; we just saw that in this case the insertion tableau $w@$ is uniquely determined, which means, thanks to the bijection 2.4.*2* that w is uniquely determined. □

For example, $w = 53 \cdot 61 \cdot 2 \cdot 4$ has shape $2211 \leq 321 = \|w\mathbf{R}\|$; the sequence of tableaux congruent to the left factors of w : $\varnothing \longrightarrow 5 \longrightarrow \begin{smallmatrix}5\\3\end{smallmatrix} \longrightarrow \begin{smallmatrix}5\\3\,6\end{smallmatrix} \longrightarrow \begin{smallmatrix}5\\3\\1\,6\end{smallmatrix} \longrightarrow \begin{smallmatrix}5\\3\,6\\1\,2\end{smallmatrix} \longrightarrow \begin{smallmatrix}5\\3\,6\\1\,2\,4\end{smallmatrix}$ shows that $w@ = \begin{smallmatrix}4\\2\,5\\1\,3\,6\end{smallmatrix}$; w admits the insertion word $\mu = 452361$, since $\mu \equiv w@$; the files of μ are 21, 43, 5, 6 and are identical to those of the composition word $\|w\|\mathbf{M} = 21\ 43\ 5\ 6$. On the other hand, in the same congruence class, we have a unique word w' of shape 213; it is determined by its insertion tableau congruent to the composition word $213\mathbf{M} = 21\ 3\ 654 \equiv \begin{smallmatrix}6\\2\,5\\1\,3\,4\end{smallmatrix}$. Indeed, $w' = 51\ 3\ 642$ as we can check from the sequence of tableaux congruent to its left factors : $\varnothing \longrightarrow 5 \longrightarrow \begin{smallmatrix}5\\1\end{smallmatrix} \longrightarrow \begin{smallmatrix}5\\1\,3\end{smallmatrix} \longrightarrow \begin{smallmatrix}5\\1\,3\,6\end{smallmatrix} \longrightarrow \begin{smallmatrix}5\,6\\1\,3\,4\end{smallmatrix} \longrightarrow \begin{smallmatrix}5\\3\,6\\1\,2\,4\end{smallmatrix}$. The words corresponding to the other permutations of 321 are given next page.

The preceding lemma has detached in the congruence class of a tableau t, the set of those words w (among which the tableau and the contretableau) for which $\|w\|$ is a permutation of $\|t\|$:

DEFINITION 2.7. A word w is *frank* iff $\|w\|$ is a permutation of $\|w\mathbf{R}\|$.

Equivalently, thanks to 2.6.*2*, a word w is frank iff it admits the composition word $\|w\|\mathbf{M}$ as an insertion word.

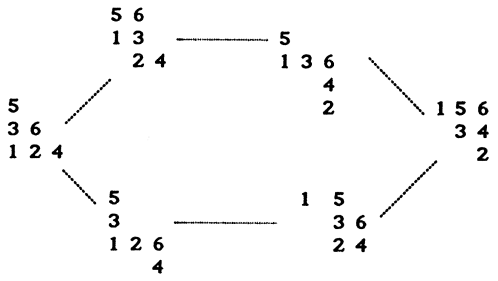
For a two-columns tableau t, finding its congruent contretableau t' can be considered as using the generator $\flat$ of the symmetric group $\mathcal{S}(2)$ to transpose the two columns of t . This is best done with the jeu de taquin ([**L-S1**]) : $\begin{smallmatrix}4\\3\\1\end{smallmatrix}\ \begin{smallmatrix}6\\2\end{smallmatrix} \Rightarrow \begin{smallmatrix}4\\1\end{smallmatrix}\ \begin{smallmatrix}6\\3\\2\end{smallmatrix}$. We shall write $t' = t^\flat$ and $t = t'^\flat$. Notice that $t\$ = 62$ is a subword of $t'\$ = 632$ and that $t'\pounds = 41$ is a subword of $t\pounds = 431$.

More generally, on the set of k-columns words, one has an action (not everywhere defined; we use the symbol $\varnothing$ when it is not defined) of the symmetric group $\mathcal{S}(k)$. First, if the factor $v_r v_{r+1}$ of $w = v_1 \cdot \ldots \cdot v_k$, $v_i \in \mathbf{V}$, is a tableau or a contretableau, then the image of w by the simple transposition σ_r , $1 \leq r < k$, is set equal to $v_1 \cdots v_{r-1}(v_r v_{r+1})^\flat v_{r+2} \cdots v_k$ if moreover this last word has still k columns. In all other cases, the image of w by σ_r is set equal to $\varnothing$. It is checked in section 6 that this extends to an action of the symmetric group for which frank words play a special rôle that we summarize in the following theorem (*1* and *2* being a rewriting of 2.6.*2* and 2.6.*3*):

THEOREM 2.8.

1) *For each word* w *, one has* $\|w\| \geq \|w\mathbf{R}\|$ *, with equality iff* w *is frank.*
2) *The set of frank words in the plactic class of a tableau* t *is in bijection with the set of permutations of the shape of* t *.*
3) *The product of two frank words* w *,* w' *is frank iff* $u\$.u'\pounds$ *is frank for any pair of frank words* u, u'*, with* $u \equiv w$ *and* $u' \equiv w'$ *.*

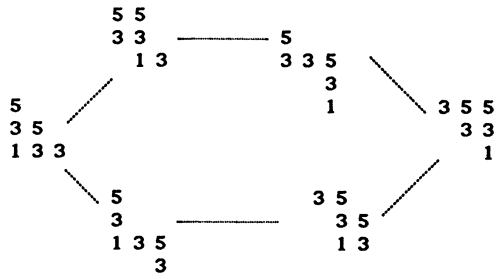
For example, the class of 531 62 4 contains the six frank words (read vertically!) which correspond to the six permutations of the shape 321 :



On the other hand, the product of the two frank words 31 42 and 4 51 is not frank: the insertion tableau of 31 42 4 51 is 721 43 5 6, which is not congruent to 21 43 5 76. Indeed, 4 51 $\equiv$ 41 5, and condition 3) is violated, because $42 \cdot 41$ is not frank.

We now come to the study of keys.

By definition, a *key* is a tableau such that its columns are pairwise comparable for the inclusion order. This condition implies that the action of the symmetric group giving the frank words is simply the permutation of the columns because this is true (and easily verified) in the special case of two-columns keys, where the operation $\flat$ reduces to just commutation. For example, 531 53 3 is a key and the frank words in its congruence class are



DEFINITION 2.9. The *right key* $t\mathbf{K}_+$ of a tableau t (or of any word congruent to t) is the tableau of the same shape as t whose columns belong to the set of columns $\{u\$\ ,\ u \equiv t$ and u frank$\}$. The *left key* $t\mathbf{K}_-$ of t is the tableau of the same shape as t whose columns belong to the set $\{u\pounds, u \equiv t$ and u frank$\}$.

In other words, the left key (resp. right key) of t is made of the left (resp. right) columns, repeated the appropriate number of times so as to fill the shape of t, of the frank words in the class of t . For instance, the above hexagon for the tableau 531 62 4 give the keys $t\mathbf{K}_- = \begin{smallmatrix} & & 5 \\ 3 & 5 & \\ 1 & 1 & 1 \end{smallmatrix}$ and $t\mathbf{K}_+ = \begin{smallmatrix} & & 6 \\ 4 & 6 & \\ 2 & 4 & 4 \end{smallmatrix}$. *Notice that a tableau is* a key iff it is equal to its right (resp. left) key. In other case, the keys of a tableau belong to different plactic classes.

Since the test that the product of two frank words w, w' is frank involves exactly the columns composing $w\mathbf{K}_+$ and $w'\mathbf{K}_-$, we can reformulate th.2.8:

THEOREM 2.10. *1) A word w is frank iff $\|w\mathbf{R}\|$ is a permutation of $\|w\|$.*
2) A product ww' of two frank words w, w' is frank iff the shape of $ww'\mathbf{R}$ is the union of the shapes $\|w\mathbf{R}\|$ and $\|w'\mathbf{R}\|$.
3) A product ww' of two frank words w, w' is frank iff $(w\mathbf{K}_+)(w'\mathbf{K}_-)$ is frank.

If a pair of columns satisfies $u \leq v$, then $u' \leq v'$ for any other pair of columns u', v' such that $\{u'\} \subseteq \{u\}, \{v'\} \supseteq \{v\}$; similarly, $u \triangleright v$ implies $u' \triangleright v'$ for any pair such that $\{u'\} \supseteq \{u\}$, $\{v'\} \subseteq \{v\}$. Thus, in the special case of two frank words w, w' having the same shape up to a reordering, condition *3)* can be restricted to the comparison of columns in $w\mathbf{K}_+$ and $w'\mathbf{K}_-$ of the same length instead of all pairs of columns (as required by 2.8.*3*). Recall that for columns of the same length, the order $\leq$ is the componentwise order on words of the same degree (that we can denote by the same symbol $\leq$). In short, one can replace in that case 2.10.*3* by:

THEOREM 2.11. *Assume that w, w' are two frank words such that $\|w\mathbf{R}\| = \|w'\mathbf{R}\|$, then ww' is frank iff $w\mathbf{K}_+ \leq w'\mathbf{K}_-$.*

For example, the product of the two tableaux $w =$ 421 41 3 and $w' =$ 432 32 4 is not frank ; condition *2)* is violated since (421 41 3)(432 32 4)$\mathbf{R}$ = 421 431 432 3 4 is a tableau of shape (= 33311) different from 332211. In fact, 421 41 3 $\cong$ 421 1 43 and 432 32 4 $\cong$ 32 432 4, but $(43\ 32)^\flat = \varnothing$, and thus condition *3)* of the theorem is violated. Condition 2.11 has the same fate, since 431 43 3 (= (421 41 3)$\mathbf{K}_+$) is not smaller than 432 32 3 (= (432 43 4)$\mathbf{K}_-$).

On the other hand, 421 31 3 432 32 4 $\mathbf{R}$ = 421 431 32 32 3 4 has shape 332211, as is insured by the inequality 431 31 3 (= (421 31 3)$\mathbf{K}_+$) $\leq$ 432 32 3 (= (432 43 4)$\mathbf{K}_-$) required by 2.11.

Definition 2.12. *Key of a permutation*: to each pair consisting of a permutation $\zeta \in \mathcal{S}(n)$, and a partition $I = (1I, 2I, \dots)$, Ehresmann [E] has associated a key, noted $\mathbf{K}(\zeta, I)$, by taking the sequence of left reordered factors of ζ (considered as a word) of successive degrees $1I, 2I, \dots$.

For example, $\zeta =$ 316452 and $I =$ 532 give the key 65431 631 31.

In case that $I = n...21$, we shall simply write $\mathbf{K}(\zeta)$ instead of $\mathbf{K}(\zeta, n...21)$; thus $\zeta \to \mathbf{K}(\zeta)$ is an embedding of $\mathcal{S}(n)$ into the set of tableaux of shape $n...21$. The reader may notice that the so-called "strong", "Bruhat order" on permutations (see **[Bj]**) is a special case of the pervading order on words (componentwise) which we have been repeatedly using, by way of the equivalence due to Ehresmann :

$$\eta \leq \zeta \quad \Leftrightarrow \quad \mathbf{K}(\eta) \leq \mathbf{K}(\zeta) \tag{2.13}$$

For example, the keys associated to $\zeta = 3241, \eta = 2143$ and $\mu = 1423$ are $\mathbf{K}(\zeta) = 4321\ 432\ 32\ 3$, $\mathbf{K}(\eta) = 4321\ 421\ 21\ 1$, $\mathbf{K}(\mu) = 4321\ 421\ 41\ 1$; thus $\zeta \geq \eta$, but ζ and μ are not comparable since the two columns 32 and 41 are not comparable.

3. Symmetrizations. The definition of tableaux is strictly dependent upon a chosen total order on A . It is remarkable that nonetheless the commutative image of the sum S_I of all tableaux of a given shape I be a symmetrical function: this is the most constructive definition of the *Schur Function* of index I. To understand this phenomenon (see nevertheless Knuth's proof **[B-K]**), one must define an action of the symmetric group on the free algebra such that the S_I are invariant under this action. Further, this action must induce the usual action of the symmetric group when projected by $w \to \underline{w}$ on the commutative algebra. By the duality $w \to w^{-1}$ for permutation words, the new action we shall define now can be specialized to give the action that we have been using in our study of frank words.

Consider first the case of a two-letters alphabet $\mathsf{A} = \{a, b\}$. It is clear that the image by the transposition $\sigma = \sigma_{ab}$ of the tableau $t = (ba)^h a^k b^m$ must be $t^\sigma = (ba)^h a^m b^k$, since t^σ is the only tableau of the same shape as t whose commutative image is the monomial $a^{m+h} b^{h+k}$.

More generally, because words w in a, b are determined by their insertion tableau $w@$ and their commutative image $\underline{w}$ (we recover $w\mathbf{R}$ from its content $\underline{w}$ and its shape, equal to that of $w@$), one defines w^σ to be the word:

$$(w^\sigma)@ = w@ \quad \& \quad (\underline{w})^\sigma = \underline{(w^\sigma)} \tag{3.1}$$

In other terms σ , as it has been defined, preserves the insertion tableau and commutes with the projection $\mathbf{Z} < a, b > \to \mathbf{Z}[a, b]$.

For example, the image by σ of the word baa **a** $bbaa$ **aa** b is baa **b** $bbaa$ **bb** b (we have marked the letters which change) because these two words have the same insertion tableau, equal to $\begin{smallmatrix} 1 & 6 & 7 \\ 0 & 2 & 3 & 4 & 5 & 8 & 9 & X \end{smallmatrix}$, and they project onto $a^7 b^4$ and $a^4 b^7$ in $\mathbf{Z}[a, b]$.

Since the column ba commutes (plactically) with a and b , shifting the factors ba of a word w in a, b generates the congruence class of w. This remark implies the following easy algorithm to compute $w \to w^\sigma$:

$$\left\{ \begin{array}{l} \text{fix the successive factors } ba \text{ of } w, \text{ then change the remaining} \\ \text{subword } a^k b^m \text{ into } a^m b^k. \end{array} \right. \tag{3.2}$$

For instance the preceding word gives $(ba)\ aa\ \big(b(ba)a\big)\ aab$ and we have to change the remaining word $aa\ aab$ into $ab\ bbb$ to get $(ba)\ ab\ \big(b(ba)a\big)\ bbb\ =\ w^{\sigma}$.

Consider now the more general case of a simple transposition σ_i of consecutive letters a_i, a_{i+1} . One defines w^{σ_i} to be the word in which the subword $w \cap \{a_i, a_{i+1}\}$ has been modified according to 3.1 or 3.2, the other letters being left unchanged. For example, denoting by $x...x$ any word in letters different from a and b, the above computation shows that the image of $bxaxax\mathbf{a}xbxbxaxax\mathbf{a}x\mathbf{a}xb$ is $bxaxax\mathbf{b}xbxbxaxax\mathbf{b}x\mathbf{b}xb$.

It is proven in **[L-S1]** that $w \rightarrow w^{\sigma_i}$ extends to an action of the symmetric group on $\mathbf{Z}\langle A\rangle$, i.e. that given a permutation μ and a word w, all factorizations of $\mu = \sigma\ \sigma' \dots\ \sigma''$ into simple transpositions produce the same word $\big((w^{\sigma})^{\sigma'} \dots\big)^{\sigma''}$ denoted w^{μ}.

One can note in reference to a previous remark that in section 2, we have acted on the insertion words to generate from a tableau the frank words which are congruent to it, thus preserving $w\mathbf{R}$, and that the action described here preserves $w@$.

At the commutative level, on $\mathbf{Z}[A]$, we have at our disposal other actions of the symmetric group $\mathcal{S}(A)$ (see **[L-S 2]**).

In particular, two operators $\overline{\pi}_{\mu}$ and π_{μ} on $\mathbf{Z}[A]$ are associated to each permutation μ. For a simple transposition σ_i the operator $\overline{\pi}_{\sigma_i}$ (abbreviated $\overline{\pi}_i$, and acting as always on its left) is

$$f \longrightarrow \big(f^{\sigma_i} - f\big) \Big/ (1 - a_i/a_{i+1}) = f\overline{\pi}_i \tag{3.3}$$

and the operator π_i is just the sum of $\overline{\pi}_i$ and the identity :

$$\pi_i = \overline{\pi}_i + 1 \tag{3.4}$$

Let $\underline{w} = \underline{v}a_i^k \in \mathbf{Z}[A]$, with $\underline{v}$ symmetrical in a_i and a_{i+1}.

Then direct computation gives

$$\underline{w}\pi_i \ = \ \underline{v}a_i^k + \underline{v}a_i^{k-1}a_{i+1} + \dots + \underline{v}a_{i+1}^k$$

i.e. $\underline{w}\pi_i$ is the sum of all monomials between $\underline{w}$ and $\underline{w}^{\sigma_i}$, and $\underline{w}\overline{\pi}_i$ is the same sum apart from the first term (=w) missing.

This indicates how we can lift $\overline{\pi}_i$ into an operator, denoted θ_i, on the free algebra. Given i and a word w, let its degree in a_{i+1} be m and its degree in a_i be $m + k$. Then w and w^{σ_i} differ by the exchange of a subword $\mathbf{a}_i^k$ into $\mathbf{a}_{i+1}^k$ if $k \geq 0$, or of $\mathbf{a}_{i+1}^{-k}$ into $\mathbf{a}_i^{-k}$ if $k \leq 0$.

In the first case, we define $w\theta_i$ to be the sum of all words in which the subword $\mathbf{a}_i^k$ has been changed respectively into $\mathbf{a}_i^{k-1}\mathbf{a}_{i+1}$, $\mathbf{a}_i^{k-2}\mathbf{a}_{i+1}^2$, $\cdots$, $\mathbf{a}_{i+1}^k$; in the second, we put $w\theta_i = -\big(w^{\sigma_i}\big)\theta_i$ as in the commutative case. In other terms, θ_i interpolates between the identity and σ_i for the words having more occurences of a_i than of a_{i+1}. The corresponding algorithm is in this case ($k \geq 0$), putting $a_i = a, a_{i+1} = b, \theta = \theta_i$:

(3.5) $\begin{cases} \text{fix the successive factors } ba \text{ of } w \text{ , then change the remaining} \\ \text{subword } a^{m+k}b^m \text{ into successively } a^{m+k-1}b^{m+1}, a^{m+k-2}b^{m+2}, \dots, \\ a^m b^{m+k} \text{ and take the sum of all the words so obtained.} \end{cases}$

For instance, for the word studied in 3.2, we have $(ba)aa\big(b(ba)a\big)aab\theta = (ba)aa\big(b(ba)a\big)abb + (ba)aa\big(b(ba)a\big)bbb + (ba)ab\big(b(ba)a\big)bbb$.

More generally, we can transform w by changing its subword $a^{m+k}b^m$, $k \in \mathbf{Z}$, into any row $a^r b^{2m+k-r}$ of the same degree. This operation will preserve the insertion tableau, as does σ_i (which is a special case). In particular, we shall need the projection of $a^{m+k}b^m$ onto a^{2m+k}, $k \in \mathbf{Z}$, that we shall denote λ (and λ_i for the pair of letters a_i, a_{i+1}):

(3.6) $\begin{cases} \text{fix the successive factors } ba \text{ of } w, \text{ then change the remaining} \\ a^{m+k}b^m \text{ into } a^{2m+k} \text{ to obtain } w\lambda. \end{cases}$

Since $\sigma_i = \sigma, \theta_i = \theta, \lambda_i = \lambda$ preserve the insertion tableau, they are also compatible with the right and left keys : if w is a frank word congruent to t, then w^σ and $w\lambda$ are also frank, and $w\theta$ is a sum of frank words; $w^\sigma\$$ and $w\lambda\$$ are equal to $w\$^\sigma$ or $w\$$. Thus $t^\sigma\mathbf{K}_+$, $t\lambda\mathbf{K}_+$ and $t'\mathbf{K}_+$, with any t' in the sum $t\theta$, are equal to $t\mathbf{K}_+$ or $(t\mathbf{K}_+)^\sigma$. We shall give a more precise statement in theorem 3.8.

The operators θ_i do not satisfy the Coxeter relations $\theta_i\theta_{i+1}\theta_i = \theta_{i+1}\theta_i\theta_{i+1}$, contrary to the operators $\overline{\pi}_i$, π_i and λ_i; thus, if $\sigma_i \cdots \sigma_j$ and $\sigma_h \cdots \sigma_k$ are two reduced decompositions of the same permutation, the operators $\theta_i \cdots \theta_j$ and $\theta_h \cdots \theta_k$ will in general be different and there is no canonical way of defining operators θ_μ by products of operators θ_i.

Nevertheless, we recover this lost Coxeter relation when acting on dominant monomials, as we shall see in 3.8.

DEFINITION 3.7. The *standard basis* $\mathfrak{U}(\mu, I)$ associated to the pair μ, I (μ permutation, I partition) is the sum in the free algebra of all tableaux having right key $\mathbf{K}(\mu, I)$. The *costandard basis* $\mathfrak{B}(\mu, I)$ is the sum of all contretableaux having right key $\mathbf{K}(\mu, I)$.

Since by definition all the elements in a plactic class have the same right key, it is clear that $\mathfrak{U}(\mu, I) \equiv \mathfrak{B}(\mu, I)$, and more precisely, that $\mathfrak{B}(\mu, I)\mathbf{R} = \mathfrak{U}(\mu, I)$.

To any partition $I = (1I, 2I, ...)$ on associates the *dominant* monomial $a^I = (a_{1I} \dots a_2 a_1)(a_{2I} \dots a_2 a_1)(a_{3I} \dots a_2 a_1) \dots$.

THEOREM 3.8. *Let* a^I be a dominant monomial and $\sigma_i\sigma_j \dots \sigma_k$ *be any reduced decomposition of a permutation* μ. Then

$$\mathfrak{U}(\mu, I) = a^I\theta_i\theta_j \cdots \theta_k.$$

Proof. Let μ and i be such that $\ell(\mu\sigma) > \ell(\mu)$, with $\sigma = \sigma_i$, $a_i = a, a_{i+1} = b$. If w is a frank word such that $w\mathbf{K}_+ = \mathbf{K}(\mu, I)$ or $\mathbf{K}(\mu\sigma, I)$, then $w\lambda\mathbf{K}_+ = \mathbf{K}(\mu, I)$. Let t be a tableau such that $t\mathbf{K}_+ = \mathbf{K}(\mu, I)$, $t^\sigma\mathbf{K}_+ \neq \mathbf{K}(\mu, I)$ (this implies that $t^\sigma\mathbf{K}_+ = \mathbf{K}(\mu\sigma, I)$). Then there exists a frank word $w \equiv t$ such that the right factor $w^\sigma\$$ of w^σ contains the letter b and not the letter a; thus w contains a and not b; this implies that $t\lambda = t$. One checks moreover that all the tableaux (not only t^σ) in the sum $t\theta$ have the same right key $\mathbf{K}(\mu, I)$.

Conversely, if t is such that $t\mathbf{K}_+ = t^\sigma\mathbf{K}_+ = \mathbf{K}(\mu, I)$, then $(t + t^\sigma)\theta = 0$. Supposing the theorem true for μ, it is also true for $\mu\sigma$. □

For instance, suppose that we already know $\mathfrak{B}(426135, 321)$; we compute $\mathfrak{B}(436125, 321)$ by using the operator $\theta = \theta_2$, the contretableaux t such that t^σ also belong to $\mathfrak{B}(426135, 321)$ give a zero contribution; the others are of the type $t = t\lambda_2$:

$$\begin{array}{lcl}
4\ 42\ 642 & \longrightarrow & 4\ 42\ 643\ +\ 4\ 43\ 643 \\
4\ 41\ 642 & \longrightarrow & 4\ 41\ 643 \\
3\ 42\ 642 & \longrightarrow & 3\ 42\ 643 \\
2\ 41\ 642 & \longrightarrow & 2\ 41\ 643\ +\ 3\ 41\ 643 \\
3\ 41\ 642 & \longrightarrow & 0 \\
3\ 32\ 642 & \longrightarrow & 0 \\
3\ 31\ 642 + 2\ 31\ 642 & \longrightarrow & 0
\end{array}$$

All the contretableaux belonging to a costandard basis $\mathfrak{B}(\mu, I)$ having the same right column (since it is the reordering of the factor of μ of length $1I$), we have a faster way to compute the costandard bases, by induction on the number of parts of I :

LEMMA 3.9. *Let p be a positive integer, $I = (1I, ..., rI)$ be a partition with $r \geq p$, I' the resulting partition after deletion of the part pI, μ a permutation , v the column such that $\{v\} = \{1\mu, ..., (pI)\mu\}$. Then there exist permutations $\nu, \eta \ldots$ such that*

$$\mathfrak{B}(\mu, I) = \left[\mathfrak{B}(\nu, I') + \mathfrak{B}(\eta, I') + \cdots\right]v$$

Proof. Two congruent frank words w, w' have the same right column $w\$ = w'\$$ iff $|w\$| = |w'\$|$. Thus, to compute the right key of a tableau, we need only to generate a set of frank words $w^{(1)}, w^{(2)}, \ldots$ such that $\{|w^{(1)}\$|, |w^{(2)}\$|, \ldots\} = \{1I, 2I, \ldots\}$. We can require that the shapes of these frank words be $(rI, \ldots, 2I, pI, 1I)$, $(rI, ..., 1I, pI, 2I), \ldots, ((r-1)I, ..., 1I, pI, rI)$. The images of $w^{(1)}, \ldots, w^{(r)}$ by the transposition (of columns) σ_{r-1} will be frank words with right column of degree pI. *Thus the right key of any frank word $w = v_1 \cdot \ldots \cdot v_r$ is equal* to that of the frank word $(v_1 \cdot \ldots \cdot v_{r-1}\mathbf{K}_+) \cdot v_r$. To describe a standard basis, we need only to look for frank words of the type $w = w' \cdot v$, w' being a key of shape I' and v the column: $\{v_r\} = \{1\mu, ..., (pI)\mu\}$, such that $w\mathbf{K}_+ = \mathbf{K}(\mu, I)$. □

This lemma gives a fast induction when we take $p = 1$ to factorize the column of maximal length. For example, let $\mu = 32514$, $I = 4321$. Then $v = 5321$, $I' = 321$; $\mathfrak{B}(32514, 4321) = (32\ 532\ v\ +\ 3\ 31\ 532\ v\ +\ 2\ 31\ 532\ v) + (3\ 32\ 432\ v\ +\ 3\ 31\ 432\ v\ +\ 2\ 31\ 432\ v)$ decomposes into $\left[\mathfrak{B}(32514, 321) + \mathfrak{B}(32415, 321)\right]\ v$.

4 . Postulation. Let $\mathcal{A}$ be a vector bundle on any variety $\mathcal{M}$, $\mathcal{F}(\mathcal{A}) \to \mathcal{M}$ the relative flag manifold of complete flags of quotient bundles of $\mathcal{A}$. If $\mathcal{A}$ is of rank n, one has from definition (see **[Gr]**) n tautological line bundles $L_1, \ldots, L_n$ on $\mathcal{F}(\mathcal{A})$. The Grothendieck ring $\mathcal{K}(\mathcal{F}(\mathcal{A}))$ of classes of vector bundles is a quotient of the ring of polynomials $\mathcal{K}(\mathcal{M})[\mathbb{A}]$, $\mathbb{A}$ being an alphabet of cardinal n, by a certain ideal $\mathfrak{I}$, the images of $a_1, \ldots, a_n$ being respectively the classes of $L_1, \ldots, L_n$.

Since all constructions given here are compatible with $\mathfrak{I}$, we can replace $\mathcal{K}(\mathcal{F}(\mathcal{A}))$ by $\mathbf{Z}[\mathbb{A}]$ and $K(\mathcal{M})$ by the ring of symmetric polynomials $\mathbf{Z}[\mathbb{A}]^{\mathfrak{S}(\mathbb{A})}$. The projection $p : \mathcal{F}(\mathbb{A}) \to \mathcal{M}$ induces a morphism $p_* : \mathcal{K}(\mathcal{F}(\mathbb{A})) \to \mathcal{K}(\mathcal{M})$ which corresponds in fact to the operator $\pi_\omega : \mathbf{Z}[\mathbb{A}] \to \mathbf{Z}[\mathbb{A}]^{\mathfrak{S}(\mathbb{A})}$ associated to the maximal permutation of $\mathfrak{S}(\mathbb{A})$. We can express π_ω as a product of simple operators 3.4, but it can be directly defined by the following global expression (see **[L-S2]**):

$$\mathbf{Z}[\mathbb{A}] \ni f \longrightarrow \sum_{\mu \in \mathfrak{S}(\mathbb{A})} [f / \prod_{i<j} (1 - a_j/a_i)]^{\mu} \tag{4.1}$$

In case that $\mathcal{M}$ is a point, the morphism p_* associates to any vector bundle $\mathcal{B}$ the Euler-Poincaré characteristics : $\sum_i (-1)^i \dim \mathcal{H}^i(\mathcal{B})$; in terms of polynomials, this should be interpreted as $\mathbf{Z}[\mathbb{A}] \ni f \to f\pi_\omega \varepsilon_{\mathbb{A}}$, f being any polynomial lifting the class of $\mathcal{B}$ and $\varepsilon_{\mathbb{A}}$ being the specialisation $a_1 \to 1, \ldots, a_n \to 1$.

Let J be a partition, I its conjugate, L the line bundle $L = L_1^{1J} \otimes L_2^{2J} \otimes \cdots$. From Demazure's construction, **[D1]** **[D2]** **[L−S5]** we have that the number $a^I \pi_\mu \varepsilon_A$ is the postulation (that is to say, the dimension of the cohomology $\mathcal{H}^0$; the other spaces $\mathcal{H}^i$ being null, the postulation coincide in that case with the Euler-Poincaré characteristics) of the line bundle L on the Schubert variety of index $\omega\mu^{-1}$.

More generally, considering simultaneously all the powers of L together, we have the *Hilbert series* $\mathcal{H}_{I,\mu}(z) = (1 - za^I)^{-1} \pi_\mu \varepsilon$ relative to L of the Schubert variety $Schub_{\omega\mu^{-1}}$ (L defines an embedding of the flag variety into a projective space if $1I > 2I > \ldots$).

From considerations of dimension, we know that the series $\mathcal{H}_{I,\mu}(z)$ is rational of the type $\mathcal{N}_{I,\mu}(z)/(1-z)^{\ell(\mu)+1}$, $\mathcal{N}_{I,\mu}(z)$ being a polynomial of degree $\leq \ell(\mu)$. However $(1-za^I)^{-1}\pi_\mu$ has in general a denominator of degree greater than $\ell(\mu)+1$. Raising up to the free algebra, we shall get a combinatorial interpretation (4.4) of the Hilbert series and clarify in particular this drop in the degrees.

From 3.8 , given any reduced decomposition $\sigma_i \ldots \sigma_j$ of μ , then $\underbrace{a^I \ldots a^I}_{k}(\theta_i + 1)\cdots(\theta_j + 1)$ is a sum of words having the same insertion tableau as $a^I \ldots \ldots a^I$, thus it is a product of k tableaux of shape I . On the other hand, again according to 3.8, $(a_{1I} \ldots a_1)^k (a_{2I} \ldots a_1)^k \cdots (\theta_i + 1) \ldots (\theta_j + 1)$ is the sum of tableaux $\mathcal{T}(\mu, I^k)$, I^k denoting the partition $\underbrace{1I \ldots 1I}_{k}\ \underbrace{1I \ldots 1I}_{k} \cdots$.

Since the operators θ_i are compatible with the plactic congruences, comparing the two sums gives that each tableau t in $\mathcal{T}(\mu, I^k)$ is congruent to a frank word which is a product $t_1 \cdots t_k$ of tableaux of shape I.

Conversely, from 2.11, we see that a product $t^{(1)} \cdots t^{(k)}$ of tableaux belonging to $\mathcal{T}(\mu, I)$ is congruent to a tableau $t \in \mathcal{T}(\mu, I^k)$ iff the following inequalities are satisfied:

$$(4.2) \qquad t^{(1)}\mathbf{K}_+ \leq t^{(2)}\mathbf{K}_- \; ; \; t^{(2)}\mathbf{K}_+ \leq t^{(3)}\mathbf{K}_- \; ; \ldots \; ; \; t^{(k-1)}\mathbf{K}_+ \leq t^{(k)}\mathbf{K}_-$$

Moreover, in such a case, if $v_1 \cdots v_r$ is the right key of $t^{(k)}$, then $v_1^k \cdots v_r^k$ is the right key of $t^{(1)} \ldots t^{(k)}$ because each frank word in the class of $t^{(1)} \cdots t^{(k)}$ has a right column which is one the columns $v_1, \ldots, v_r$.

Let us call *I-chain of length k* a product of tableaux of the same shape I satisfying the inequalities 4.2; the *right key* of a chain will be the right key of its last tableau, *the left key* of a chain being the left key of its first tableau.

The preceding results may be summarized in the following theorem:

THEOREM 4.3. *Let I be a partition, μ a permutation in $\mathcal{S}(\mathbf{A})$, $\sigma_i \ldots \sigma_j$ any reduced decomposition of μ . Then*

$$(1 - a^I)^{-1}\theta_i \cdots \theta_j \; = \; \sum_{\Gamma} \{\Gamma : \mathbf{K}_+(\Gamma) < \mathbf{K}(I, \mu)\}$$

sum of all I- chains Γ of right key $\mathbf{K}(I, \mu)$ and

$$(1 - a^I)^{-1}(\theta_i + 1) \cdots (\theta_j + 1) \; = \; \sum_{\Gamma} \{\Gamma : \mathbf{K}_+(\Gamma) \leq \mathbf{K}(I, \mu)\}$$

sum of all I- chains Γ of right key less or equal to $\mathbf{K}(I, \mu)$.

For instance, the 21 chains of length 2 for $\mathcal{S}(3)$ are all the 27 products $\neq \emptyset$ of two tableaux of shape 21 described below, and correspond bijectively to the 27 tableaux of shape 42. There are 8 tableaux of shape 21, only two being not keys; for them, one has $\left(\begin{smallmatrix}2\\1\,3\end{smallmatrix}\right)\mathbf{K}_- = \begin{smallmatrix}2\\1\,2\end{smallmatrix}$ and $\left(\begin{smallmatrix}2\\1\,3\end{smallmatrix}\right)\mathbf{K}_+ = \begin{smallmatrix}3\\1\,3\end{smallmatrix}$, $\left(\begin{smallmatrix}3\\1\,2\end{smallmatrix}\right)\mathbf{K}_- = \begin{smallmatrix}3\\1\,1\end{smallmatrix}$ and $\left(\begin{smallmatrix}3\\1\,2\end{smallmatrix}\right)\mathbf{K}_+ = \begin{smallmatrix}3\\2\,2\end{smallmatrix}$. On the second row, for example, one reads that the chain $\begin{smallmatrix}2\\1\,2\end{smallmatrix} \cdot \begin{smallmatrix}2\\1\,3\end{smallmatrix}$ factorizes the tableau $\begin{smallmatrix}2\,2\\1\,1\,2\,3\end{smallmatrix}$, its left key being $\left(\begin{smallmatrix}2\\1\,2\end{smallmatrix}\right)\mathbf{K}_-$ and its right key being $\left(\begin{smallmatrix}2\\1\,3\end{smallmatrix}\right)\mathbf{K}_+$.

	$\begin{smallmatrix}2\\11\end{smallmatrix}$	$\begin{smallmatrix}2\\12\end{smallmatrix}$	$\begin{smallmatrix}3\\11\end{smallmatrix}$	$\begin{smallmatrix}2\\13\end{smallmatrix}$	$\begin{smallmatrix}3\\13\end{smallmatrix}$	$\begin{smallmatrix}3\\12\end{smallmatrix}$	$\begin{smallmatrix}3\\22\end{smallmatrix}$	$\begin{smallmatrix}3\\23\end{smallmatrix}$
$\begin{smallmatrix}2\\11\end{smallmatrix}$	$\begin{smallmatrix}22\\1111\end{smallmatrix}$	$\begin{smallmatrix}22\\1112\end{smallmatrix}$	$\begin{smallmatrix}23\\1111\end{smallmatrix}$	$\begin{smallmatrix}22\\1113\end{smallmatrix}$	$\begin{smallmatrix}23\\1113\end{smallmatrix}$	$\begin{smallmatrix}23\\1112\end{smallmatrix}$	$\begin{smallmatrix}23\\1122\end{smallmatrix}$	$\begin{smallmatrix}23\\1123\end{smallmatrix}$
$\begin{smallmatrix}2\\12\end{smallmatrix}$	$\varnothing$	$\begin{smallmatrix}22\\1122\end{smallmatrix}$	$\varnothing$	$\begin{smallmatrix}22\\1123\end{smallmatrix}$	$\begin{smallmatrix}22\\1133\end{smallmatrix}$	$\varnothing$	$\begin{smallmatrix}23\\1222\end{smallmatrix}$	$\begin{smallmatrix}23\\1223\end{smallmatrix}$
$\begin{smallmatrix}3\\11\end{smallmatrix}$	$\varnothing$	$\varnothing$	$\begin{smallmatrix}33\\1111\end{smallmatrix}$	$\varnothing$	$\begin{smallmatrix}33\\1113\end{smallmatrix}$	$\begin{smallmatrix}33\\1112\end{smallmatrix}$	$\begin{smallmatrix}33\\1122\end{smallmatrix}$	$\begin{smallmatrix}33\\1123\end{smallmatrix}$
$\begin{smallmatrix}2\\13\end{smallmatrix}$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\begin{smallmatrix}23\\1133\end{smallmatrix}$	$\varnothing$	$\varnothing$	$\begin{smallmatrix}23\\1233\end{smallmatrix}$
$\begin{smallmatrix}3\\13\end{smallmatrix}$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\begin{smallmatrix}33\\1133\end{smallmatrix}$	$\varnothing$	$\varnothing$	$\begin{smallmatrix}33\\1233\end{smallmatrix}$
$\begin{smallmatrix}3\\12\end{smallmatrix}$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\begin{smallmatrix}33\\1222\end{smallmatrix}$	$\begin{smallmatrix}33\\1223\end{smallmatrix}$
$\begin{smallmatrix}3\\22\end{smallmatrix}$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\begin{smallmatrix}33\\2222\end{smallmatrix}$	$\begin{smallmatrix}33\\2223\end{smallmatrix}$
$\begin{smallmatrix}3\\23\end{smallmatrix}$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\begin{smallmatrix}33\\2233\end{smallmatrix}$

Reintroducing a parameter z , projecting to $\mathbf{Z}[\mathbf{A}]$ and using the specialization $\varepsilon_{\mathbf{A}} : \mathbf{A} \to \{1, \ldots, 1\}$, we get:

COROLLARY 4.4. *Let I be a partition, μ a permutation in $\mathcal{S}(\mathbf{A})$. Then the postulation $(1 - za^I)^{-1}\overline{\pi_\mu}\varepsilon_{\mathbf{A}}$ (resp. $(1 - za^I)^{-1}\pi_\mu\varepsilon_{\mathbf{A}}$) is equal to the generating function of the number of I-chains Γ having right key $\mathbf{K}(I, \mu)$ (resp. having right key less or equal to $\mathbf{K}(I, \mu)$) , i.e.*

$$(1 - za^I)^{-1}\ \overline{\pi_\mu}\ \varepsilon\ =\ \sum_{\Gamma} z^{\mathrm{length}\Gamma}\ \Gamma\ \varepsilon_A$$

sum on all I-chains Γ having right key $\mathbf{K}(I, \mu)$.

5. Avatars of standard bases. According to theorem 3.8, if μ and σ_k are such that $\ell(\mu\sigma_k) > \ell(\mu)$, then for any partition I, $\mathfrak{U}(\mu, I)\theta_k = \mathfrak{U}(\mu\sigma_k, I)$. Thus the operators θ_k allow to connect the standard bases corresponding to different permutations. Using the same induction $\mu \to \mu\sigma_k$, it is not too difficult, but we shall abstain from doing it, to check that standard bases can also be defined in the following two other manners 5.2 and 5.8.

First, according to **[L-M-S]**, a tableau can be considered as an increasing chain of permutations (with respect to the Ehresmann order 2.13). One says that a chain of permutations $\mu^{(1)} \leq \mu^{(2)} \leq \ldots \leq \mu^{(r)}$ *lifts* a tableau $t = v_1 \cdot \ldots \cdot v_r$ if $\widetilde{v}_1, \ldots, \widetilde{v}_r$ are respective left factors of $\mu^{(1)}, \ldots, \mu^{(r)}$, where, for a word $v = x_1 \cdots x_m$, the notation $\widetilde{v}$ stands for the reverse word $x_m \cdots x_1$.

It is clear that given a tableau, there exists a unique minimal lift of it. Indeed, putting $\mu^{(0)} = \mathit{identity}$ and having found the minimal chain $\mu^{(0)} \leq \mu^{(1)} \leq \ldots \leq$

$\mu^{(p-1)}$ with respective left factors $\widetilde{v}_1, \ldots, \widetilde{v}_{p-1}$, given moreover $v_p = x_1 \cdots x_m$, we see that the set of permutations μ such that $\mu \geq \mu^{(p-1)}$ and $1\mu = x_m, \ldots, m\mu = x_1$ admits a unique minimal element $\mu^{(p)}$. An induction on p thus gives a lift $\mu^{(1)}(t) \leq \cdots \mu^{(r)}(t)$ that we shall call the *canonical lift of* t. From the construction, for any other lift $\zeta^{(1)} \leq \cdots \leq \zeta^{(r)}$, one has $\mu^{(1)} \leq \zeta^{(1)}, \ldots, \mu^{(r)} \leq \zeta^{(r)}$, i.e. the canonical lift is minimal with respect to the Ehresmann order.

For example, the canonical lift of the tableau 531 62 4 is **135** 246 $\leq$ **26** 3145 $\leq$ **4** 62135. Let us illustrate on this example how to pass from $\mu^{(p-1)}$ to $\mu^{(p)}$, say for $p = 2$. The left reordered factors of $\mu^{(1)}$ are $1, 13, 135, 1235, 12345$; 236 is the minimum word having subword 26 bigger than 135, 1236 is the minimum word containing 236 bigger than 1235, and finally, 12346 is the minimum word containing 1235 bigger than 12345. These minimum words are the left reoredered factors of $\mu^{(2)} = 263145$ which therefore is the minimum permutation bigger than $\mu^{(1)}$ and beginning by **26**.

DEFINITION 5.1. *Given a partition I and a permutation μ , the L-M-S standard basis $\mathfrak{U}'(\mu, I)$ is the set of tableaux t such that the last permutation of their canonical lift is equal to μ.*

When $\mu = identity$, the set $\mathfrak{U}(\mu, I)$ reduces to the tableau $(1I \cdots 1)(2I \cdots 1) \times \cdots (rI \cdots 1)$ as well as $\mathfrak{U}(\mu, I)$; the induction $\mu \to \mu\sigma$ proves, as claimed in the beginning of this section, that $\mathfrak{U}(\mu, I)$ is the sum of the tableaux belonging to $\mathfrak{U}'(\mu, I)$. In other words, one has the following property showing that the L-M-S standard bases coincide with the one defined in 3.5, up to the change of the alphabet A with N.

PROPOSITION 5.2. *A key $\mathbf{K} = \mathbf{K}(\mu, I)$ is the right key of a tableau t iff t has shape I and μ is the last permutation in the canonical lift of t.*

For example, the last permutation 462135 in the canonical lift of the tableau $t = 531\ 62\ 4$ gives the key 642 64 4, which is the right key of t as seen in 2.9.

One may favor horizontals rather than verticals. Reading the successive horizontals of a tableau t , one gets a word which is a product of rows (as defined in sect.2) and which is congruent to t; we shall call this word the *row-word* of t.

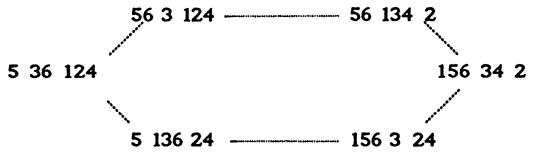
For example, the row-word of $\begin{smallmatrix} & & 5 \\ 3 & 6 & \\ 1 & 2 & 4 \end{smallmatrix}$ is 5 36 124. Row-words are characterized by their insertion tableau, as seen from property 2.5 :

LEMMA 5.3. *A word w is the row-word of a tableau t iff there exists a partition $J = 1J \geq 2J \geq \cdots \geq pJ$ such that $[(pJ + \ldots + 2J + 1) \cdots (pJ + \ldots + 1J)] \cdots [(pJ + 1) \cdots (pJ + (p-1)J)] [1 \cdots pJ]$ is an insertion word for w. In that case, J is the partition conjugate to the shape of t.*

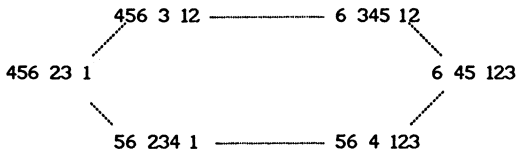
For example, (5 36 124)@ = $\begin{smallmatrix} & & 4 \\ 2 & 5 & \\ 1 & 3 & 6 \end{smallmatrix}$, and this tableau is congruent to the word [456] [23] [1].

Apart from the symmetry between rows and columns, which means taking instead of composition words their reverse, the same property as 2.8.*2* holds : in the

class of any tableau t of shape conjugate to a partition $J = (1J, \dots, pJ)$, for any permutation H of J, there exists a unique word w congruent to t, which admits $\left[(pH + \dots + 2H + 1) \cdots (pH + \dots + 1H)\right] \cdot_{\cdot} \cdot \left[1 \cdots pH\right]$ as an insertion word. This forces w to be a product $w_p \cdots w_1$ of rows of respective degrees $pH, \dots, 2H, 1H$. For standard tableaux, transposition (i.e. exchange of the two axes of coordinates) commutes this construction with the one given in section 2 The hexagon generated by the action of the symmetric group on the row-word 5 36 124 is now



The corresponding insertion words are respectively



Given $H \in \mathbf{N}^p$, let T_H be the sum of words w such that:

(5.4) w has the insertion word

$$\varphi = \left[(pH + \dots + 2H + 1) \cdots (pH + \dots + 1H)\right] \cdots \left[1 \cdots pH\right]$$

(5.5) For the factorization $w = w_p \cdots w_1$ corresponding to φ , every w_j, $1 \leq j \leq p$, belongs to the monoid generated by $\mathbf{A}_j = \{a_1, \dots, a_j\}$, i.e. $w_1 \in \mathbf{A}_1^*, w_2 \in \mathbf{A}_2^*, \dots, w_p \in \mathbf{A}_p^*$.

Because of the explicit value of φ, the above factorization is the row-factorization of w, apart from *void* factors that we must specify in order to fix the flag conditions 5.5.

For example, $T_{1302} = (44\ 222\ 1 + 34\ 222\ 1 + 44\ 122\ 1 + 34\ 122\ 1) + (44\ 112\ 1 + 34\ 112\ 1) + (24\ 122\ 1) + (33\ 222\ 1 + 33\ 122\ 1) + (24\ 112\ 1) + (33\ 112\ 1) + (23\ 122\ 1) + (23\ 112\ 1)$ is the sum of words $w = w_3 w_2 w_1$ such that $w@ \equiv 6\ 345\ 12$ $\left(w@ = \begin{smallmatrix} 6 \\ 3\ 4 \\ 1\ 2\ 5 \end{smallmatrix}\right)$ and $w_1 \in \{1\}^*, w_2 \in \{1,2\}^*, w_3 \in \{1,2,3\}^*$.

As we already said, the induction $\mu \rightarrow \mu\sigma$, starting from the case T_J with J partition (T_J is the single word $\cdots 2^{2J} 1^{1J}$), allows to obtain the general case, summarized in the following proposition:

PROPOSITION 5.6. *Let J be a partition, μ a permutation, $H = J^\mu$, I the partition conjugate to J . Then T_H is congruent to $\sum_{\nu \leq \mu} \mathfrak{U}(I, \mu)$.*

In the preceding example, $J = 321$, $\mu = 2413$. One has 8 permutations in the interval $[1234, 2413]$. According to the proposition, $T_{1302} \equiv \mathfrak{U}(321, 2413) +$

$\mathfrak{U}(321,1423)+\mathfrak{U}(321,2143)+\mathfrak{U}(321,2314)+\mathfrak{U}(321,1243)+\mathfrak{U}(321,1324)+\mathfrak{U}(321,2134)+\mathfrak{U}(321,1234) =$

$\{421422+321422+421412+321412\}+\{421411+321411\}+\{421212\}+\{321322+321312\}+\{421211\}+\{321311\}+\{321212\}+\{321211\}$.

These tableaux are respectively congruent to the words enumerated in the same order above.

Flags of alphabets or of modules naturally occur in the study of Schubert polynomials **[L-S2]** or of Schubert subvarieties of a flag manifold.

One can restrict the sum T_H to its component T'_H congruent to $\mathfrak{U}(\mu, I)$. Indeed, one has the following property, which is also proved through the induction $\mu \rightarrow \mu\sigma$:

LEMMA 5.7. *Let t be a tableau of shape I conjugate to J, $\mathbf{K} = \mathbf{K}(\mu, I)$ its right key, ζ a permutation, $H = J^{\zeta}$. Then there exists a word in T_H congruent to t iff $\zeta \geq \mu$.*

In other terms, for any word w, the set of H such that w is congruent to a word in T_H is either void or admits a unique minimum element (i.e. an $H = J^{\mu}$ such that μ is minimal for the Ehresmann order, J being the partition conjugate to the shape of $w\mathbf{R}$). One can now define T'_H to be the restriction of T_H to such words. For example, the tableau 4321 321 31 41 3 is congruent to the words 3344 11233 2 11 $\in T_{2154}$, 3344 11233 12 1 $\in T_{1254}$, 13344 1233 2 11 $\in T_{2145}$, 13344 1233 12 1 $\in T_{1245}$ which correspond to all the permutations above 3412 ; it is also congruent to the words 3344 23 2 11113 , 34 12334 2 1113, 3344 3 11223 11, 4 13334 1223 11 but these words do not belong to respectively $T_{5124}, T_{4152}, T_{2514}, T_{2451}$ (which are just below in the Ehresmann order) because the flag condition 5.5 is violated. Thus t is congruent to a word in T'_{2154}. Proposition 5.6 can now be reformulated:

PROPOSITION 5.8. *Let J be a partition, μ a permutation, $H = J^{\mu}$, I the partition conjugate to J. Then T'_H is congruent $\mathfrak{U}(I, \mu)$.*

The key of the preceding tableau is $\begin{smallmatrix} & & & 4 \\ & & 3 & 4 \\ 2 & 3 & 4 & 4 \\ 1 & 1 & 3 & 3 & 3 \end{smallmatrix}$, i.e. is equal to $\mathbf{K}(3412, 5421)$, in accordance with the fact that $(5421)^{3412}$ is equal to 2154.

6. Appendix. Let U, Ξ be two sets, Ξ^* the free monoid generated by Ξ. An *action* of Ξ^* on U is a *function* (not everywhere defined; we use the symbol $\varnothing$ for the points of indeterminacy) : $U \times \Xi^* \rightarrow U \cup \{\varnothing\}$ such that $u(\xi\xi') = (u\xi)\xi'$ and $u\xi = \varnothing \Rightarrow u\xi\xi' = \varnothing$ for any $u \in U, \xi, \xi' \in \Xi$.

Let Ξ be finite and totally ordered: $\Xi = \{\xi_1, \ldots, \xi_{p+1}\}$. Suppose that "Moore-Coxeter" relations hold, i.e. that for any pair $\xi_i = \sigma, \xi_j = \tau$ and any u in U, one has identically:

(6.1) $u\xi \neq \varnothing \Rightarrow u\xi\xi = u$

(6.2) if $|i - j| \geq 2$, $u\sigma\tau = u\tau\sigma$

(6.3) if $|i - j| = 1$, $u\sigma\tau\sigma = u\tau\sigma\tau$.

Remark 6.4. 1) Let $|i-j|=1$ and $u\sigma, u\tau, u\sigma\tau \neq \emptyset$, then $u\sigma\tau\sigma = u\tau\sigma\tau \neq \emptyset$.
2) Let $|i-j| \geq 2$ and $u\sigma, u\tau \neq \emptyset$. Then $u\sigma\tau = u\tau\sigma \neq \emptyset$.

Proof of 1): $u\tau \neq \emptyset$ implies $(u\tau)\tau = u$ according to 6.1; the hypothesis becomes $(u\tau)\tau, (u\tau)\sigma\tau, (u\tau)\tau\sigma\tau \neq \emptyset$ showing that $(u\tau)\sigma\tau\sigma = (u\tau)\tau\sigma\tau \neq \emptyset$ by 6.3. Therefore, $\emptyset \neq (u\tau)\sigma\tau\sigma\sigma = (u\tau)\tau\sigma\tau\sigma = u\sigma\tau\sigma$ as required.
Proof of 2): As above, we use 6.1 to write $u\sigma = (u\tau)\tau\sigma$; according to 6.2, $(u\tau)\tau\sigma = (u\tau)\sigma\tau$; since $u\sigma \neq \emptyset$, $u\tau\sigma\tau$ is different from $\emptyset$ as well as its factor $u\tau\sigma$, and $u\sigma\tau$ by symmetry. □

Choose any $u = u_0$ in U. The three preceding axioms allow to identify the orbit $\Omega = \{u\xi : u\xi \neq \emptyset\}$ to a quotient (the $u\xi$ need not to be all different) of a subset of $\mathcal{S}(p+1)$, u being sent to the identity element of $S(p+1)$. The following proposition gives a necessary and sufficient condition for the orbit to be a quotient of the full symmetric group.

PROPOSITION 6.5. *Let $n, m \geq 1$, $p = n+m$ and set $\rho = \xi_n, \Xi_1 = \{\xi_1, \ldots, \xi_{n-1}\}$, $\Xi_2 = \{\xi_{n+1}, \ldots, \xi_{p-1}\}$. Assume that both $u\Xi_1^*$ and $u\Xi_2^*$ do not contain $\emptyset$ and that $\xi_1 \in \Xi_1^*, \xi_2 \in \Xi_2^* \Rightarrow u\xi_1\xi_2\rho \neq \emptyset$.*

Then $u\Xi^*$ does not contain $\emptyset$.

Proof. We can suppose $n \leq m$ by symmetry, and deduce the general case from the case where all the points $\neq \emptyset$ in $u\Xi^*$ are different. Thus the orbit Ω is a subset of the symmetric group and we write its elements as permutations. If $n = m = 1$, there is nothing to prove. Consider the case where $n = 1, m = 2$. Then Ξ_1 is void, $\Xi_2 = \{\xi_2\}, \rho = \xi_1$. By hypothesis, $u = 123, u\rho = 213$, $u\xi_2 = 312$ and $u\xi_2\rho = 312$ are all different from $\emptyset$. Thus taking $u' = 213, \sigma = \rho, \xi_2 = \tau$ in 6.3, we get that $u'\tau = u\rho\xi_2 = 231$, $u'\tau\sigma = u\rho\xi_2\rho = 321$ are different from $\emptyset$; this proves the proposition in this case.

Let again $n = 1$ and $m \geq 3$. As above, $\rho = \xi_1$ and Ξ_1 is void. Using induction on m, we have that Ω contains all the permutations such that their rightmost letter is $\neq 1$. In particular, for any $i, j > 1$, Ω contains all the permutations such that their restriction to the third rightmost letters is $1ij, i1j, 1ji$ or $j1i$. Repeating the same argument with $\sigma = \xi_{p-2}$ and $\tau = \xi_{p-1}$, we conclude that Ω contains all the permutations such that their right factor of length 3 is $ij1$ or $ji1$, concluding the proof of the proposition for $n = 1$.

Consider now the general case where $n \geq 2, m \geq 1$. For any $k \leq n$, we can find some ξ in Ξ_1^* such that the first (ie. left) letter of $u\xi$ is k. Thus by induction on n, i.e. by considering the restriction of $u\xi$ to all its letters except the first, we have that Ω contains all the permutations such that their first letter is $h \leq k$. Considering now the first three letters on the left and applying the same argument as for the case of $n = 1$, we conclude that Ω is the full symmetric group. □

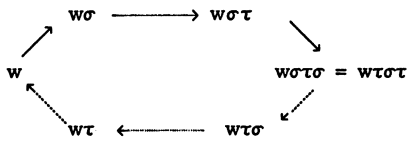
The action of "commutation" of columns seen in section 2 satisfy the axioms 6.1, 6.2 and 6.3 . Only 6.3 is not straightforward. Since it involves only triples of consecutive columns in a word, it needs to be checked only for 3-columns words. This we do just now.

LEMMA 6.6. *Let w be a 3-columns word, σ and τ be the two generators of $\mathcal{S}(3)$. Then* $\{w\sigma, w\sigma\tau, w\sigma\tau\sigma \neq \emptyset\} \Rightarrow \{w\tau, w\tau\sigma \neq \emptyset \ \&\ w\sigma\tau\sigma = w\tau\sigma\tau\}$.

Proof. One of the four words w , $w\sigma$, $w\sigma\tau$, $w\sigma\tau\sigma$ has its shape decreasing or increasing. Let it be $w\sigma = v_1 \cdot v_2 \cdot v_3$. Recall that a 2-columns word w is a tableau or a contretableau iff $w^{\flat} \neq \emptyset$, i.e. iff w is frank, and that a word is a tableau (resp. a contretableau) if each factor made of two consecutive columns is such. The two factors v_1v_2 and v_2v_3 being frank, $w\sigma$ is a tableau or a contretableau. According to 2.6.$\mathcal{J}$, the action of permutation of columns on a tableau or a contretableau generate the frank words in its class: thus $w, w\sigma, w\sigma\tau, w\sigma\tau\sigma = w\tau\sigma\tau, w\tau\sigma, w\tau$ are the frank words in the class of $w\sigma$.

Suppose now that this is $w = v_1 \cdot v_2 \cdot v_3$ which has a decreasing shape $\|w\| = ijh$, and let t be the insertion tableau of w and σ be the first generator of $\mathcal{S}(3)$. Since $v_1v_2\sigma \neq \emptyset$, the word $v_1 \cdot v_2$ is a tableau and this determines $t \cap \{1, \ldots, i+j\}$. Since $v_1 \cdot v_2 \cdot v_3\sigma\tau \neq \emptyset$, the digit $i+j+h$ cannot be in the first column of t; since $v_1 \cdot v_2 \cdot v_3\sigma\tau\sigma \neq \emptyset$, it cannot be either in the second column of t. It must be in the third, which means that t is equal to $[i \cdots 1][(i+j) \cdots (i+1)] \times [(i+j+h) \cdots (i+j+1)] = ijh\mathbf{M}$. Thus w is a tableau and we conclude as before. This reasoning also applies to the case where $\|w\|$ is increasing, since then $\|w\sigma\tau\sigma\|$ is decreasing and we can exchange the rôle of w and $w\sigma\tau\sigma$. □

Pictorially, hypothesis 6.6 is that if the four consecutive words $w \to w\sigma \to w\sigma\tau \to w\sigma\tau\sigma$ are different from $\emptyset$, then we can "close the hexagon":



Let us finish with an example of a word whose orbit (under commutation of columns) is not a quotient of the full symmetric group.

Let $w = 31 \cdot 42 \cdot 4 \cdot 51$, and σ, ρ, τ be the three generators of $\mathcal{S}(4)$ We get four double points: $w = w\sigma, w\rho = 31\ 4\ 42\ 51 = w\sigma\rho$, $w\rho\sigma = \omega\rho\sigma\rho = 3 \cdot 41 \cdot 42 \cdot 51, w\tau = w\tau\sigma = 31 \cdot 42 \cdot 41 \cdot 5$. Since the words $42 \cdot 41$ and $42 \cdot 51$ are not frank, all the neighbours $w\rho\tau, w\tau\rho, w\sigma\tau\rho, w\sigma\rho\tau, w\rho\sigma\tau$ and $w\sigma\rho\sigma\tau$ are $\emptyset$ and thus the orbit Ω of w is restricted to the enumerated four double points. Indeed, condition 2.8.$\mathcal{J}$ to ensure that w be frank is exactly that $42 \cdot 4$ (central factor of w) and $42 \cdot 41$ (central factor of $w\sigma$, $w\tau$ and $w\tau\sigma$) should be frank. Since this not the case for the last word, we already knew from th.2.8 that Ω could not be a quotient of the full symmetric group.

REFERENCES

[B-G-G] BERNSTEIN I.N., GELFAND I.M. GELFAND S.I., UMN, 28 (1973), pp. 1-26.
[B-K] A.BENDER, D.E.KNUTH, *Enumeration of plane partitions*, J. Comb. Th. A, 13 (1972), pp. 40–54.

[B] A.Björner, *Ordering of Coxeter Groups*, Contemp. M., 34 (1984), pp. 175–195.

[Bo] N.Bourbaki, *Eléments de Mathématiques modernes, Algèbre ch.1*, Paris, New York, C.C.L.S. 1971.

[D1] M.Demazure, *Désingularisation des variétés de Schubert*, Ann. E. N. S., 6 (1974), pp. 163–172.

[D2] M.Demazure, *Une formule des caractères*, Bull. Sc. M., 98 (1974), pp. 163–172.

[E] C.Ehresmann, *Sur la topologie de certains espaces homogènes*, Ann. M. (2), 35 (1934), pp. 396–443.

[Gr] A.Grothendieck, *Sur quelques propriétés fondamentales en théorie des intersections*, Séminaire Chevalley, Paris, 1958.

[K-L] D.Kazhdan and G.Lusztig, *Representations of Coxeter Groups and Hecke Algebras*, Invent., 53 (1979), pp. 165-184.

[K] D.E.Knuth, *Permutations matrices and generalized Young tableaux*, Pac. J. Math., 34 (1970), pp. 709–727.

[L-M-S] V.Lakshmibai, C.Musili and C.S.Seshadri, *Geometry of G/P IV*, Proc. Indian Acad. Sc., 88A (1979), pp. 280-362.

[L-S1] A.Lascoux & M.P.Schützenberger, *Le Monoide Plaxique*, Atti del C.N.R., Roma, 1981.

[L-S2] A. Lascoux & M.P.Schützenberger, *Symmetry and Flag Manifolds*, Lect. Notes in Math., 996 (1983).

[L-S3] A.Lascoux & M.P.Schützenberger, *Symmetrization operators on polynomial rings*, Funk. Anal., 21 (1987), pp. 77-78.

[L-S4] A.Lascoux & M.P.Schützenberger, *Tableaux and non commutative Schubert polynomials*, Funk. Anal (to appear).

[L-S5] A.Lascoux, *Anneau de Grothendieck de la variété de drapeaux*, submitted to the Comité d'évaluation des hommages à Grothendieck (1988).

[L-S6] A.Lascoux & M.P.Schützenberger, *Arêtes et tableaux*, Séminaire Lotharingien de Combinatoire Cagliari, 1988.

[L-W] V.Lakshmibai and J.Weyman, *Bases standards*, C. R. Acad. Sc. Paris, 1988.

[M] I.G.Macdonald, *Symmetric Functions and Hall Polynomials*, Oxford Mono., Oxford, 1979.

[Mc] Major P.Macmahon, *Combinatory Analysis*, Chelsea reprints, New York, 1960.

[Sche] C.Schensted, *Longest increasing and decreasing sequences*, Canad. J. Math., 13 (1961), pp. 179–191.

[Schu] M.P.Schützenberger, *Quelques remarques sur une construction de Schensted*, Math. Scand. 12 (1963), pp. 117–128.

LA SOCIÉTÉ PHILOMATHIQUE DE PARIS

et deux siècles d'histoire de la Science en France

Colloque du Bicentenaire de la Société Philomathique de Paris

Sous la direction de
André Thomas

puf

Sur les modèles mathématiques. Propos d'un mathématicien philomathe

par

MARCEL-PAUL SCHÜTZENBERGER

PHILOMATHE

Remontant d'un demi-siècle le cours du temps, on constate dans les archives de la Société Philomathique un phénomène assez curieux : à la différence de la plupart des autres disciplines, les mathématiciens que notre compagnie s'honore d'avoir comptés en son sein ont été tournés vers les applications – de la mécanique à la statistique – plus souvent que vers le courant principal des recherches de l'époque. Il n'est donc peut-être par irrelevant à l'histoire de notre société de proposer quelques interrogations sur les rapports que peuvent entretenir les mathématiques avec les autres sciences de la nature.

Ces questions n'ont pas qu'un intérêt historique ou contemplatif : la vogue – et le succès – des ordinateurs poussent à l'usage de modèles numériques : à tel point que l'on entend les anti-vivisectionnistes réclamer le remplacement des expériences pharmacodynamiques par des simulations et des calculs. A l'autre pôle – celui de l'abstraction – on a vu se constituer auprès de presque chaque domaine des sciences une sous-discipline purement mathématique, avec ses méthodes, ses problèmes et sa dynamique propre. Cas extrême, aux Etats-Unis, la respectable muse de l'histoire se trouve chaperonnée par une servante ou rivale répondant au doux nom de Cliométrie. Développement assez surprenant puisqu'en même temps qu'on s'efforce de tout mathématiser, la philosophie à la mode – j'entends la philosophie analytique – s'évertue à présenter les mathématiques comme un pur jeu logique c'est-à-dire comme une industrie de la tautologie sans autre contenu que formel.

Nous sommes ici aux confins de problèmes qui excèdent les compétences du technicien et je ne les évoque que pour marquer des limites

que je ne franchirai pas. Il s'agit ici seulement de présenter quelques exemples et de solliciter la réflexion collective pour aider les jugements qu'il nous faut bien porter, *volens nolens*, quand une revue scientifique demande notre avis sur tel ou tel manuscrit qu'on lui a soumis.

Qu'est-ce donc qu'appliquer les mathématiques ? La question apparaîtra bien sotte aux physiciens formés depuis Galilée et Descartes au va-et-vient constant entre les équations, les observations et les lois. Ce n'est donc pas à eux que je m'adresse sinon pour prendre conseil de leur succès. Mais qu'en est-il pour les autres sciences de la Nature ? Bien souvent une sous-discipline se répute « mathématique » parce qu'elle s'attache aux aspects de la discipline mère qui utilisent le plus intensément la physique et participent donc de ce fait de son emploi des nombres et des figures. Mon propos, non plus, ne les concerne pas. Mais pour le reste qui est encore fort large ? Est-ce appliquer les mathématiques que de faire passer une courbe de forme analytique simple par la série des points du diagramme obtenu par des expériences et des observations méthodiques ou fortuites ? En un certain sens, oui, bien sûr. Les élèves du philomathe G. Darmois qui fit tant pour introduire la statistique en France au lendemain de la guerre seront les premiers à souligner tout ce que la biologie et les sciences médicales doivent à l'emploi intelligent et systématique des méthodes rigoureuses de la statistique mathématique. A prédire aussi que le champ d'applications de ces techniques continuera à croître et à apporter une riche moisson de connaissances. Mais si l'on veut pousser plus loin l'analyse, on peut se demander si l'usage des méthodes statistiques est bien une application de la mathématique proprement dite et non pas une application seconde à travers cette physique du hasard qu'est le calcul des probabilités. Ainsi ce que l'on appelle parfois la psychologie mathématique n'est guère le plus souvent que l'étude des techniques statistiques spéciales motivées par certaines branches de la psychologie expérimentale. Il nous faut donc aller un peu plus loin et je vous propose l'exemple suivant tiré d'un article que l'on me soumet et que la déontologie m'empêche donc de citer.

Dans ce travail l'auteur constate que la croissance du nombre des cas dans une épidémie strictement contemporaine suit une loi cubique en fonction du temps. La première partie de l'étude est purement statistique et discute la validité de l'échantillonnage et la précision des chiffres évalués. La deuxième partie, la plus importante du point de vue qui nous occupe ici, est la construction d'un modèle et le travail

proprement mathématique sur celui-ci. Dans ce modèle l'auteur fait intervenir un coefficient exprimant l'hétérogénéité plus ou moins grande de la population par rapport à ce que les généticiens appelleraient la panmixie. Par là il faut entendre le degré avec lequel les sujets contagieux risquent de propager la maladie à des individus *quelconques* de la population, ou au contraire n'ont de contacts qu'à l'intérieur de groupes plus ou moins isolés et fermés sur eux-mêmes. Pour prendre une illustration imagée, disons que les rencontres qui se font dans la rue ou au marché sont beaucoup plus panmixiques que celles qui se font à l'occasion de la vie professionnelle.

La solution mathématique des équations montre clairement qu'une panmixie absolue entraînerait une croissance exponentielle du nombre des cas, c'est-à-dire une diffusion de l'épidémie beaucoup plus explosive que celle que l'on observe puisque celle-ci est de type cubique si l'on en croit mon auteur. D'où diverses conclusions sur les facteurs causaux et le devenir de cette épidémie, etc. Ce n'est pas mon propos ici de discuter la validité de cette recherche mais de montrer sur cet exemple simple – voire même simpliste – ce que peut être une application proprement dite des mathématiques : les moments clés étant ceux de la construction du modèle, du raisonnement mathématique sur les équations qu'il fournit et le retour vers les faits. De nouveau, sans juger la valeur technique de ce travail, c'est du point de vue purement conceptuel un bon exemple d'épidémiologie mathématique.

Il me faut maintenant donner des contre-exemples pour montrer ce que les mathématiciens considèrent comme des « non-applications » de leur discipline malgré les apparences typographiques et parfois des calculs fort savants. A vrai dire on n'a que l'embarras du choix : on pourrait considérer la célèbre équation d'Irving Fisher $P = MV/Q$ où P désigne le niveau des prix, Q la quantité des biens échangés, M la masse de la monnaie existante et Q sa vitesse de circulation. Telle qu'elle est présentée cette équation semble impliquer les mêmes relations arithmétiques (la multiplication et la division) que la loi de Mariotte, $P = RT/V$. Malheureusement on ne voit pas très bien comment on pourrait déterminer empiriquement les valeurs numériques des variables qui y figurent de manière à justifier que l'équation a un contenu arithmétique plus significatif que l'une quelconque de ses traductions, telle que par exemple : « Si les masses monétaires et les prix ne varient pas beaucoup alors moins il y a de monnaie plus il faut qu'elle circule vite. » Ceci n'est peut-être pas vrai mais ne heurte certainement pas le bon sens !

Je ne me hasarderai pas plus avant sur les vastes territoires de l'économie mathématique car la discussion nous entraînerait trop loin. Je mentionnerai cependant que des « équations » comme celle d'Irving Fisher ont été récemment l'objet d'une controverse violente à la National Academy of Sciences. Pour certains, conduits à l'assaut par le mathématicien renommé Serge Lang, c'est une « malhonnêteté intellectuelle » que d'écrire de semblables équations. Pour d'autres plus indulgents, dont je suis, ces formules et les phantasmes de calculs que déploient certaines sciences humaines sont un moyen symbolique parfois commode de résumer des lois tendancielles vagues. Le danger ne commence que quand on les manipule comme s'il s'agissait de vraies relations arithmétiques. On peut aussi voir dans l'abus verbal de la théorie mathématique des nœuds qu'a affectionnés une certaine psychanalyse comme un hommage rendu à la gloire de la géométrie et de l'analyse, ce dont nous ne pourrions que la remercier.

Revenons à des problèmes plus sérieux. Comme je ne veux offenser personne je choisirai un exemple fourni par un très grand mathématicien qui est depuis longtemps bien au-delà de toute critique : celui de la dynamique des populations de Vito Volterra. On connaît le scénario : les renards dévorent les lapins ce qui fait chuter le nombre de ces derniers. Privés de leur proie, les renards meurent de faim et les lapins débarrassés de leurs prédateurs se reproduisent à plaisir. Les quelques renards survivants suffisent pour faire redémarrer le cycle, etc.

Volterra traduit ceci en quelques équations différentielles simples qu'il résout avec virtuosité et il retrouve au bout de ses calculs le caractère périodique du processus dont il a construit un modèle.

Rares sont les enseignants de mathématiques faisant un cours à des étudiants naturalistes ou à des futurs médecins qui ont résisté à la tentation d'intéresser enfin leur auditoire en citant cette théorie et en évoquant à son sujet les fluctuations périodiques du marché des fourrures de la baie d'Hudson. Le succès est garanti car jusqu'à la fin du cours quelques étudiants auront cru aux vertus de la biologie mathématique. A mon avis à tort s'ils se sont laissés convaincre par ce seul exemple. En effet les équations prédisent une période constante qui ne s'observe pas dans la réalité, ce dont on donne pour explication que les paramètres figurant dans les équations (la probabilité élémentaire pour un lapin d'être dévoré, etc.) ont de grandes fluctuations d'années en années et de lieu en lieu. Mais ces paramètres existent-ils ? Si l'on augmente la durée ou bien l'étendue du territoire sur lequel

portent les observations, l'expérience montre que l'hétérogénéité de l'échantillonnage croît dans un rapport tel que la précision n'est pas accrue, bien au contraire. C'est là un phénomène général dont B. Mandelbrot a eu le mérite de souligner l'importance sur une série de cas remarquables dont les crues du Nil et les fluctuations du marché des valeurs en bourse. *A fortiori* aucune expérimentation ne permet de valider le choix de l'expression analytique des équations de Volterra sinon le fait même pour lesquelles elles ont été choisies à savoir que leur solution exhibe une certaine périodicité. Laquelle n'est d'ailleurs qu'une simple conséquence de bon sens du scénario que j'ai rappelé plus haut !

Bien différente est la situation de la plupart des modèles de la physique où chaque paramètre figurant dans les équations et les valeurs numériques que prévoient les calculs sont susceptibles d'une détermination assez précise pour justifier leur expression mathématique. Dans bien des cas cette précision est telle que l'histoire des mathématiques abonde en résultats où les théorèmes utilisés dans le raisonnement auraient pu être devinés (et l'ont parfois été) à partir des phénomènes observés et de leur modélisation.

Est-ce le propre de la physique ? Je n'en crois rien et je voudrais terminer par un exemple pris à l'autre extrémité de l'éventail des sciences : celui de la théorie des jeux de von Neuman que l'on doit considérer comme une application des mathématiques à la psychologie sociale. Le problème est de théoriser le comportement des joueurs dans les jeux de société où la ruse intervient en plus du raisonnement parce que chacun des acteurs choisit ses coups sans disposer des mêmes informations que son adversaire : l'exemple type est le poker contrasté ici avec le jeu d'échecs qui est de réflexion pure mais on ne s'est pas privé de conférer plus de gravité au sujet en prenant des illustrations dans la stratégie des batailles aériennes ou navales.

Après avoir modélisé le jeu considéré sous forme d'une matrice indiquant les gains et les pertes en fonction des coups joués par les deux adversaires dans l'ignorance mutuelle de leur choix, la théorie de von Neuman invoque un théorème hautement non trivial pour indiquer à chaque joueur sa stratégie optimale.

La validité de toute la construction est établie par le simple fait que l'on peut s'en servir pour programmer un ordinateur qui se conduise contre un adversaire humain avec autant de succès qu'en aurait le meilleur joueur professionnel. Notez que je n'affirme nullement que cette théorie soit utile dans les duels financiers ou militaires ;

seuls les jeux de société satisfont toutes les hypothèses nécessaires à son fonctionnement. Son mérite est ailleurs, sur le plan proprement conceptuel. Contrairement à tout ce que l'on pourrait croire *a priori*, le comportement de l'ordinateur qui joue avec succès au poker en utilisant la ruse et le bluff ne relève d'aucun élément de psychologie individuelle ou sociale : rien de semblable n'a été mis dans les axiomes du modèle hormis un principe général subtil d'optimisation qu'il est loisible de considérer comme exprimant la volonté de gagner, si l'on veut recourir à une interprétation anthropomorphique.

Je laisse à meilleur philosophe que moi de développer les conséquences – possiblement contradictoires – que l'on pourrait tirer de la théorie de von Neuman. En bon philomathe, je veux ici ne parler que de sciences et laisser à d'autres lieux tout autre type de discours.

Puissent les interrogations fragmentaires et les exemples que j'ai développés aider d'autres chercheurs à trouver des critères pour apprécier l'utilité ou la beauté des modèles mathématiques dans les nouveaux territoires qu'ils commencent à conquérir.

1990-3. Sens et évolution Année 1990

SCIENCE – HISTOIRE – PHILOSOPHIE

Publication de l'Institut Interdisciplinaire d'Etudes Epistémologiques

SCIENCE ET SENS

Actes du Colloque organisé dans le cadre de l'Académie Meudonnaise

par

Jacques ARSAC

Correspondant de l'Académie des Sciences

Philippe SENTIS

Docteur-ès-Sciences, Docteur-ès-Lettres

Librairie Philosophique J. VRIN
6, place de la Sorbonne
75005 PARIS

1990

Institut Interdisciplinaire
d'Etudes Epistémologiques
25, rue du Plat - 69002 LYON

SENS ET EVOLUTION

par

Marc-Pierre SCHUTZENBERGER

(d'après l'enregistrement de l'intervention)

Il s'est passé ces dernières années des phénomènes remarquables qui n'ont pas encore été intégrés dans la conscience générale des savants et qui font que le darwinisme a reçu un coup fatal des mains de ses partisans les plus convaincus. (Je profite de l'occasion pour faire de la réclame pour un livre qui paraîtra en septembre chez l'éditeur Londrès, et dont l'auteur est Denton. Il s'appelle "*evolution theory*" et sera traduit en français sous le titre Evolution.)

Le darwinisme a été atteint sous sa forme la plus moderne, le néodarwinisme, par les progrès d'une part de la théorie cladiste, d'autre part de la biologie moléculaire. Le néodarwinisme exposé d'abord par Simpson, qui a été relayé depuis par Ernst Mayer, et dont une vulgate tragique a été présentée par Monod, se résume en cette thèse : "L'univers biologique résulte par le seul jeu de la sélection naturelle de forces purement physico-chimiques animées par le hasard". Cette thèse implique qu'il n'existe aucune force autre que la sélection naturelle et doit donc être simulable par d'autres méthodes. Des deux éléments nouveaux qu'il faut prendre en compte l'un est la théorie cladiste développée par les paléontologistes darwiniens anglo-saxons contemporains. Elle met en cause de façon sérieuse l'une des bases du darwinisme classique, à savoir le gradualisme. Dans les textes de Darwin et de ses continuateurs cette évolution qui n'est guidée que par le hasard s'effectue par des modifications progressives. Les espèces se transforment lentement les unes dans les autres. On a objecté à Darwin que le passage d'un groupe à un autre s'effectue seulement au moyen de quelques espèces intermédiaires. Par exemple dans le passage des reptiles aux oiseaux on ne trouve guère que trois spécimens d'archéoptérix et non une graduation continue. Darwin répond que les fossiles que nous avons constituent une série imparfaite et que les étapes intermédiaires graduelles n'ont pas été isolées. A l'heure actuelle les cladistes semblent avoir établi que ce ne sont pas les conditions de fossilisation qui sont en cause, mais que des discontinuités brutales ont apparu au cours de l'évolution biologique, par exemple ce que Darwin appelle "le scandale abominable des angiospermes", c'est-à-dire l'apparition subite au milieu du tertiaire des plantes à fleurs et des arbres. On constate un épanouissement de formes extrêmement multiples et diverses sans qu'il y ait de transition douce et graduelle entre ces formes et les formes antérieures. Tout en se réclamant du darwinisme, Gould résume de façon décisive les arguments des cladistes.

L'autre élément factuel est apporté par la biologie moléculaire. Pour Darwin qui s'appuyait sur l'expérience des éleveurs l'hérédité était un phénomène continu. Le mendélisme, les théories de Morgan, la biologie moléculaire ont mis à jour les phénomènes de base de l'hérédité. Ceux-ci sont discontinus. Le patrimoine héréditaire d'un être vivant est une longue suite de phrases écrites dans un alphabet de 4 lettres dont la longueur est de l'ordre de ce que contient une bibliothèque. Les seules modifications dont la phrase soit susceptible sont d'ordre typographique. Certaines lettres sont transformées au hasard en d'autres lettres. D'après le schéma néodarwinien, la sélection naturelle, le succès reproductif de l'être qui s'est développé à partir de là, va conditionner le fait que cette modification persiste ou ne persiste pas.

On peut mesurer la similarité des êtres vivants en étudiant la proximité des patrimoines génétiques considérés comme des mots, ce qui nous ramène à une sorte de problème informatique. D'après les données de la chimie biologique, le patrimoine génétique est un programme qui serait modifié au hasard, conservé ou non selon qu'il assure ou non la reproduction de l'organisme. L'expérimentation de tels processus est faisable. Elle a même été faite. Depuis une quinzaine d'années on a essayé empiriquement sur ordinateur des programmes néodarwiniens. J'ai dans ma bibliothèque quelques livres datant des années 60 à 70. A cette époque de nombreux chercheurs avaient obtenu des crédits importants pour essayer des programmes autoadaptatifs. L'ordre de grandeur du nombre des itérations était comparable avec celui qu'exige l'évolution des êtres vivants. Le résultat a été répétitivement nul. La même technique a été utilisée sous le nom de *méthode delphique* du nom de l'oracle de Delphes. Animés de la même vision, des ingénieurs ont parié que, pour réaliser des améliorations technologiques, il suffisait de mettre les plans d'un appareil dans une machine qui ferait des modifications au hasard, qu'un autre ordinateur testerait l'efficacité de ces modifications et que petit à petit on ferait évoluer un poêle à mazout qui chauffe mal en un poêle à mazout qui chauffe bien. Conformément à l'"*ubris*" de leur race, les mathématiciens ont été enthousiasmés par les quelques théorèmes que cela leur donnait l'occasion d'écrire. De nombreuses équipes se sont adonnées à la méthode delphique pour l'amélioration de la technologie. L'histoire vous paraît comique. Elle est simplement sortie de votre mémoire.

J'affirme donc que la double connaissance du caractère discontinu de l'évolution, du caractère discontinu des enregistrements qui constituent le patrimoine génétique, et l'expérimentation possible sur des centaines de milliers de répétitions d'un cycle transformation au hasard/sélection ont rendu à peu près intenable la position darwinienne. La théorie darwinienne n'explique rien au-delà de la spéciation à l'intérieur des genres. De l'absence de signification ne peut naître aucune signification. Certaines théories flottent encore dans l'air du temps. Le darwinisme, l'intelligence artificielle, d'autres essais multiples depuis Démocrite pour évacuer le sens, pour réduire toute organisation à l'effet d'un *clinamen* aveugle, se confortent mutuellement. Chacune d'elles s'effrite. Je pense que, à une période que certains d'entre nous ne verront pas, le terrain sera libre pour discuter sérieusement de certains problèmes.

DISCUSSION

Francis JACQUES - Quelle différence faites-vous entre Darwin et Newton? Cettte question faussement naïve permet de déblayer le terrain entre les doctrines et les fausses théories. Faites-vous une différence entre les gnoses, les idéologies, les doctrines épistémologiquement fallacieuses et puis les théories falsifiées et falsifiables. J'apporterai de l'eau à votre moulin en disant que Darwin a proposé une doctrine et non une théorie falsifiable. Comment distingue-t-on les doctrines des théories qui ont une scientificité, qui sont construites pour être falsifiées. Si l'on croit Karl Popper c'est beau d'être falsifiable : les idéologies ne le sont pas. Le marxisme n'est pas falsifiable, le freudisme l'est si peu, parce qu'ils se sont immunisés de l'intérieur contre toute falsification possible, en incorporant des concepts et des méthodes vagues comme la dialectique ou le concept d'ambivalence qui vous permet de croiser le même et l'autre de telle manière que vous êtes infalsifiable. Newton avait proposé une théorie vérifiable et englobable dans un ensemble plus vaste ; Darwin aurait proposé une sécrétion interne, une idiosyncrasie spéculative.

Marc-Pierre SCHUTZENBERGER - Il est bien certain que Popper a formulé des règles d'hygiène que toute personne devrait cultiver. Je ne pense quand même pas que la falsifiabilité soit la pierre de touche irrécusable d'une connaissance scientifique. un critère aussi important serait : "Est-ce que cela permet d'agir sur le monde. Le darwinisme n'a aucun caractère opérationnel. Des règles encore plus importantes concernent les assertions non triviales. Par là j'entends celles qui sont irréductiblement nouvelles. Il y a dans le newtonisme des affirmations auxquelles vous êtes tellement habitués qu'elles vous semblent non-triviales ; par exemple le fait que l'attraction soit inversement proportionnelle à r^2 et non à une puissance quelconque, comme par exemple 2,1, est un fait non trivial. Si j'arrivais à expliquer les lois de Kepler au moyen d'un paramètre que l'on puisse ajuster, on retomberait sur une loi mathématiquement triviale. la trilogie darwinisme, freudisme , marxisme n'affirme rien de non-trivial. Si le marxisme était vrai il aurait dit des choses non-triviales. Il relève d'autres disciplines intellectuelles dans lesquelles la thèse et la thèse opposée sont l'une et l'autre aussi intéressantes. Dans le cas de la loi de Newton le contraire de la loi de Newton n'est pas intéressant. La biologie moléculaire est une théorie scientifique, non pas tellement parce qu'elle est falsifiable mais parce qu'elle affirme quelque chose de précis, de surprenant de non contenu avant sa découverte.

Raoul GIRET- Vous avez descendu Darwin en flammes. Je suis d'accord sur le fait que ses explications du moteur de l'évolution ne tiennent pas. Mais ne peut-on pas dire qu'il a joué un rôle très important en lançant le débat sur l'évolution et en provoquant des recherches tant pour défendre que pour combattre les théories ? Sans son intervention ne serait-on pas resté plus longtemps dans un certain fixisme ?

Marie-Dominique POPELARD - Je m'interroge sur sur le mode de testabilité que vous envisagez pour la théorie darwinienne. Vous disiez que tous les modes de tests par l'informatique que vous aviez envisagés avaient échoués. J'avais une notion banale sur la façon dont on testait une théorie qui était de la faire correspondre à une expérience, à quelque chose qui n'est pas de même type logique que la théorie.

Marc-Pierre SCHUTZENBERGER - Nous avons fait une expérience portant sur la structure des programmes et ses possibilités d'adaptation. Elle montre que des millions de cycles répétitifs du genre mutation-sélection ne mènent à rien.

Année 1991

Bibliographie

[1991-1] Christophe Reutenauer et Marcel-Paul Schützenberger. Minimization of rational word functions. *SIAM J. Comput.*, 20(4) :669–685, 1991.

SIAM J. COMPUT.
Vol. 20, No. 4, pp. 669–685, August 1991

MINIMIZATION OF RATIONAL WORD FUNCTIONS*

CHRISTOPHE REUTENAUER† AND MARCEL-PAUL SCHUTZENBERGER‡

Abstract. Rational functions from a free monoid into another are characterized by the finiteness of the index of some congruence naturally associated with the function. A sequential bimachine is constructed computing the function, which is completely canonical, and in some sense minimal. This generalizes the Nerode criterion and the minimal automaton of a rational language, and similar results for sequential functions.

Key words. rational function, sequential bimachine

AMS(MOS) subject classification. 68D15

1. Introduction. Sequential machines appear as a ubiquitous tool in data processing and in basic software, since they constitute the most general algorithm between words that can be executed in real time by a finite device. Their theory is one of the earliest well-developed chapters of Automata Theory [8], and their natural generalization, i.e., the rational functions from a free monoid A^* (set of input words) to another B^* (output words) plays a basic role in the study of context-free languages and compilation [1]. The present paper is a contribution to the understanding of rational functions.

Here and in the sequel, we follow Eilenberg's terminology as used in his treatise [7]. In particular, by *function* we mean a partial mapping, and we recall that a rational function α from a semigroup S into a semigroup T is a function such that its graph $\{(s, \alpha(s)) \mid s \in \mathrm{dom}(\alpha)\}$ is a *rational* subset of the product semigroup $S \times T$. This definition is not the most convenient for our present purposes, and we shall use other equivalent definitions, by means of automata and machines. In order to understand the concepts which motivate the study of these objects, we begin with an informal presentation of the topic.

Recall that a sequential automaton is a two-tape machine reading the input tape from left to right, and writing on the output tape from left to right; no left move, nor ε-move, is allowed. A sequential function is by definition a function $\alpha: A^* \to B^*$ which is realized by some sequential automaton. Sequential functions are closed under functional composition.

Strictly speaking, what we have just described are left sequential objects and one could consider right sequential ones in a symmetric way (read and write from right to left). However, the associated functions are quite different. For instance, in a fixed integer base, multiplication by a given integer can be carried out by a sequential automaton if and only if it reads from right to left, while it is the reverse that is true for the division.

This leads to a more intuitive definition of rational function as the closure under composition of left and right sequential functions. An early theorem of Elgot and Mezei on general rational relations (see [1, Chap. 4, Thm. 5.2]) shows that any rational function can be obtained by composing one left and one right sequential function. This is expressed in more compact fashion by the concept of a bimachine [12] according

* Received by the editors November 20, 1989; accepted for publication (in revised form) October 23, 1990.

† Département de Mathématique et d'Informatique, Université du Québec à Montréal, Montréal, Québec, Canada H3C 3P8.

‡ Académie des Sciences, Paris, France, and 97 rue du Ranelagh, 75016, Paris, France.

to Eilenberg's terminology [7]. A further basic property that we shall make use of is that if α is an injective rational function of its domain, its inverse α^{-1} is again a rational function. For instance, morphisms $\varphi: A^* \to B^*$ may be the simplest rational functions. They are both left and right sequential functions. Another way of stating that a morphism φ is injective is the condition that the image $\varphi(A)$ of the input alphabet is a code, and in this case the decoding function φ^{-1} has been intensively studied (see [2]).

The main result of this paper is a characterization of rational functions, which extends to functions the classical definition of recognizable languages in terms of finiteness of the index of a certain congruence (Theorem 1). As a byproduct, this shortens considerably the proof of a Hankel-like characterization of rational functions [13]. The second main result (Theorem 2) shows that it is possible to associate to a rational function α a bimachine that is completely canonical, up to the choice of a certain left congruence on A^* which must be compatible with the left *adjacency* relation of α. Among these congruences, there is one, the *syntactic congruence*, which is canonical. When α is a total function, the bimachine that we construct is minimal in the following sense: it has the minimum number of left states among all bimachines computing α and having the set of right states corresponding to the given congruence. In general, it is not true that α has a unique minimal device realizing it (see, for instance, [3] for the case of decoding functions) but our result is the first step in this direction. The existence of a canonical machine is far from being trivial because, in view of the two-sided action, there is an unbounded number of ways by which one can realize the necessary trade-off between the spaces of left and right states.

Of course, the construction of a canonical bimachine gives a decision procedure for the equivalence of two rational functions (the fact that this is decidable was already known, see [1]). One can expect that, similar to the close relation between combinatorial aspects of rational languages and algebraic properties of their syntactic monoid, there should exist connections between properties of a rational function and its canonical bimachine (see the open problems at the end of this paper).

2. Preliminary results. Recall that a subset of a monoid M is called *rational* if it may be obtained from the finite subsets of M by a finite sequence of the following three operations: union $\mathbf{K} \cup \mathbf{L}$, product $\mathbf{KL}$, star $\mathbf{K}^* = \cup_{n \geq 0} \mathbf{K}^n$ = the submonoid generated by $\mathbf{K}$ (see [1], [6]).

We prefer the terminology "rational" to "regular," because the former emphasizes the analogy with the theory of rational functions of classical analysis and of rational power series in noncommuting variables.

We consider here partial functions from a finitely generated free monoid into another. If $\alpha: A^* \to B^*$ is such a function, then it is called *rational* if its graph $\# \alpha = \{(u, v) \in A^* \times B^* \mid u \in \mathrm{dom}\,(\alpha), v = \alpha(u)\}$ is a rational subset of the product monoid $A^* \times B^*$.

In the sequel, we identify each word w and the subset $\{w\}$. We write $\alpha(w) = \varnothing$, if w is not in the domain of α.

A more effective characterization is the following: the function α is rational if and only if there exists a matrix representation (monoid homomorphism) $\mu: A^* \to (2^{B^*})^{n \times n}$, where 2^{B^*} is the boolean semiring of subsets of B^* (with union and product), a row vector λ, and a column vector ρ of length n with entries in the same semiring, such that for any word w, one has $\alpha(w) = \lambda \mu(w) \rho$ ((see [1, Chap. 3, Prop. 7.3]); the fact that α is a function forces each entry of μ, λ, ρ to be empty or a singleton, once the unnecessary states have been removed). The latter characterization shows that a

rational function has the following property, which is called the *Hankel property*, because it concerns the Hankel matrix $(\alpha(uv))_{u,v\in A^*}$.

LEMMA 1 (Hankel property). *For any rational function α, there exists an integer n and $2n$ functions $\beta_1, \cdots, \beta_n, \gamma_1, \cdots, \gamma_n : A^* \to B^*$ such that for any words x, y in A^**

$$\alpha(xy) = \bigcup_{1\leqq i\leqq n} \beta_i(x)\gamma_i(y).$$

Here and in the sequel, we consider each word, and $\varnothing$, to be embedded in the boolean semiring 2^{B^*}, with union and product; thus the previous equation means that for each i with $x \in \mathrm{dom}\,(\beta_i)$, $y \in \mathrm{dom}\,(\gamma_i)$, one has $\alpha(xy) = \beta_i(x)\gamma_i(y)$, and that $\alpha(xy) = \varnothing$ if for no i one has $x \in \mathrm{dom}\,(\beta_i)$ and $y \in \mathrm{dom}\,(\gamma_i)$.

Proof. Let μ, λ, ρ be as in the characterization before the lemma. Then

$$\alpha(xy) = \lambda\mu(xy)\rho = \lambda\mu x\mu y\rho = \bigcup_{1\leqq i\leqq n} (\lambda\mu x)_i(\mu y\rho)_i = \cup\, \beta_i(x)\gamma_i(y).$$

To conclude, note that if $|\beta_i(x)| \geqq 2$ for some x (in case β_i is not a function), one must have $\gamma_i = \varnothing$, because α is a function; so this index i can be omitted (the case is similar if some γ_i is not a function). □

A result of Schützenberger shows that the converse also holds [13]. We shall give a new proof of it in the next section. For the moment, let us point out what this Hankel property means in the case of characteristic functions, i.e., functions whose image is contained in $\{\varnothing, 1\}$ (we denote by 1 the empty word).

LEMMA 2. *Let $\alpha : A^* \to B^*$ be the characteristic function of its domain L. The following conditions are equivalent*:

(i) *α has the Hankel property.*

(ii) *$c(L)$ is a finite union $\cup H_i \times K_i$, where $c(w) = \cup_{w=xy} (x, y) \subset A^* \times A^*$.*

(iii) *L is a rational language.*

Note that (ii) is a Hopf-algebra-like characterization of rational languages.

Proof. (i)⇒(ii): Let $H_i = \mathrm{dom}\,(\beta_i)$ and $K_i = \mathrm{dom}\,(\gamma_i)$, where β_i and γ_i satisfy $\alpha(xy) = \cup_{1\leqq i\leqq n} \beta_i(x)\gamma_i(y)$. Then clearly $c(L) = \cup\, H_i \times K_i$.

(ii)⇒(iii): this is evident by "Nerode's criterion": if the set $\{x^{-1}L \mid x \in A^*\}$ is finite, then L is rational, where $x^{-1}L = \{y \mid xy \in L\}$. Now, $x^{-1}L$ is the union of the K_i's for which $x \in H_i$. Hence the $x^{-1}L$ are finite in number.

(iii)⇒(i) is a particular case of Lemma 1. □

The next lemma shows the functorial properties of the Hankel property.

LEMMA 3. (i) *If α and α' satisfy the Hankel property, then so does $\alpha' \circ \alpha$.*

(ii) *If α satisfies the Hankel property, then* $\mathrm{dom}\,(\alpha)$ *is rational.*

(iii) *If α satisfies the Hankel property, then α^{-1} preserves rationality.*

Proof. (i) We have

$$\alpha' \circ \alpha(xy) = \alpha'\left(\bigcup_i \beta_i(x)\gamma_i(y)\right) = \bigcup_i \alpha'(\beta_i(x)\gamma_i(y))$$

$$= \bigcup_i \bigcup_{i'} \beta_{i'}(\beta_i(x))\gamma_{i'}(\gamma_i(y)) = \bigcup_{i,i'} (\beta_{i'} \circ \beta_i)(x)(\gamma_{i'} \circ \gamma_i)(y).$$

(ii) In this case, the characteristic function of $\mathrm{dom}\,(\alpha)$ satisfies the Hankel property, so it is rational by Lemma 2.

(iii) Let L be a rational language in B^*, and let $\alpha : A^* \to B^*$ satisfy the Hankel property. Let α' be the characteristic function of L. Then by Lemma 2 and (i), $\alpha' \circ \alpha$ satisfies the Hankel property, hence by (ii), $\mathrm{dom}\,(\alpha' \circ \alpha)$ is rational. But $\mathrm{dom}\,(\alpha' \circ \alpha) = \alpha^{-1}(L)$. □

This lemma will enable us to prove the following implication: if α has the Hankel property, then α is a rational function. Proving it is much more difficult than in the case of characteristic functions (Lemma 2). It depends on a Nerode-like characterization of rational functions (the main result of § 3), and on Choffrut's theorem, which characterizes subsequential functions, and which is itself a generalization of the Ginsburg–Rose theorem on sequential functions. In order to state this theorem, define the *left distance* between two words by

$$\|u, v\| = |u| + |v| - 2|u \wedge v|,$$

where $|u|$ is the length of u and $u \wedge v$ the longest common left factor of u and v. In other words, $\|u, v\| = |s| + |t|$ where $u = ps$, $v = pt$, and $p = u \wedge v$. This can also be expressed by the equality $\|u, v\|$ = length of the reduced word (in the free group) $u^{-1}v$, or equivalently $v^{-1}u$. From this last fact, it is immediate that $\|u, v\|$ satisfies the triangular inequality. Hence, it is a distance (see also [1, Chap. 4, § 2, p. 104]).

A function $\alpha : A^* \to B^*$ will be said to be *uniformly bounded* if for any integer k, there exists an integer K such that for all $x, y \in \mathrm{dom}\,(\alpha)$, $\|x, y\| \leqq k \Rightarrow \|\alpha(x), \alpha(y)\| \leqq K$. The terminology stems from the fact that such a function maps each bounded subset of $\mathrm{dom}\,(\alpha)$ into a bounded subset of B^*, in a uniform way. Thus we do not use the terminology "bounded variation" of [4].

We shall give a formal definition of *subsequential functions* in § 4, but it seems advisable to recall now the following result.

THEOREM (Choffrut [4] or [1, Chap. 4, Thm. 2.7]). *A function α is subsequential if and only if it is uniformly bounded and α^{-1} preserves rationality.*

We say that two functions $\alpha, \beta : A^* \to B^*$ are *adjacent* if

$$\sup \{\|\alpha(f), \beta(f)\|, f \in \mathrm{dom}\,(\alpha) \cap \mathrm{dom}\,(\beta)\} < \infty.$$

The next result is a decidability result, which will imply that every construction in this paper is effective.

PROPOSITION 1. *If $\alpha, \alpha' : A^* \to B^*$ are rational functions, then one can decide if they are adjacent. In this case, the function $\alpha \wedge \alpha'$ defined by: $(\alpha \wedge \alpha')(f)$ equals the longest common left factor of $\alpha(f)$ and $\alpha'(f)$ when $f \in \mathrm{dom}\,(\alpha) \cap \mathrm{dom}\,(\alpha')$, and otherwise, $(\alpha \wedge \alpha')(f) = \alpha(f) \cup \alpha'(f)$, is rational and can be computed effectively.*

Remark 1. If α_1, α_2 are rational but not adjacent, then $\alpha_1 \wedge \alpha_2$ is not rational, in general. Define them, indeed, to be the homomorphisms $\{a_1, a_2\}^* \to t^*$ such that $\alpha_i(a_i) = t$, $\alpha_i(a_j) = 1$ for $j \neq i$.

Then $(\alpha_1 \wedge \alpha_2)(f)$ is equal to $t^{n(f)}$, where $n(f) = \inf(|f|_{a_1}, |f|_{a_2})$, which implies that $\alpha_1 \wedge \alpha_2$ is not rational (indeed, the inverse image of $(t^2)^*$, by the pumping lemma for finite automata, is not rational).

We shall need the following lemma, which is an easy consequence of a theorem of Fine and Wilf (see [9, Chap. 1, Prop. 3.5]).

LEMMA 4. *Let u, v, w, u', v', w' be words such that* $\sup \{\|uv^n w, u'v'^n w'\|, n \in \mathbb{N}\} < \infty$. *Then one has*:

(1) *For some word t, either $u' = ut$ and $tv' = vt$, or $u = u't$ and $tv = v't$.*

One of the referees pointed out that the lemma easily follows from the preliminary remark that $|v| = |v'|$.

Proof of Proposition 1. (1) Without loss of generality, we may assume that α and α' have the same domain and that $\alpha(1) = \alpha'(1) = \varnothing$. Indeed, we may restrict α and α' to $\mathrm{dom}\,(\alpha) \cap \mathrm{dom}\,(\alpha') \setminus \{1\}$ and test the adjacency of these new functions. In this case, there exist transducers T and T' for α and α', with set of states Q, Q', initial states q_0, q_0', and unique final states q_f, q_f' (see [1, Chap. 3, Thm. 7.1]).

Define the "Kronecker product" of T and T': it is the "transducer" $\bar{T}$, with set of states $\bar{Q} = Q \times Q'$, inputs in A^*, and outputs in $B^* \times B^*$; there is a path $(p, p') \xrightarrow{x/(u,u')} (q, q')$ in $\bar{T}$ if and only if there is a path $p \xrightarrow{x/u} q$ in T and $p' \xrightarrow{x/u'} q'$ in T'; moreover, all the unnecessary states of $\bar{T}$ are removed, so that all states of $\bar{T}$ are accessible and coaccessible, with initial state $\bar{q}_0 = (q_0, q'_0)$ and final state $\bar{q}_f = (q_f, q'_f)$.

A *simple* path is a path without repetition of states, and a *simple* circuit is a closed path with no repetition of internal states.

We show that α and α' are adjacent if and only if $\bar{T}$ satisfies the following condition:

(C) For any simple path $(q_0, q'_0) \xrightarrow{x/(u,u')} (q, q')$ and any simple circuit $(q, q') \xrightarrow{y/(v,v')} (q, q')$, we have equation (1) of Lemma 4.

Clearly, if α, α' are adjacent, and with the notations of (C), there exists a path

$$(q, q') \xrightarrow{z/(w,w')} (q_f, q'_f).$$

Then $\alpha(xy^n z) = uv^n w$ and $\alpha'(xy^n z) = u'v'^n w'$. As α, α' are adjacent, Lemma 4 shows that (1) holds.

Conversely, suppose that (C) holds. Then, for each long enough word m in $\mathrm{dom}(\alpha) = \mathrm{dom}(\alpha')$, there is a factorization $m = xyz$, a simple path and a simple circuit as in (C) above, and a path $(q, q') \xrightarrow{z/(w,w')} (q_f, q'_f)$.

Then $\alpha(m) = uvw$, $\alpha'(m) = u'v'w'$. By (1), we have, e.g., $u' = ut$ and $tv' = vt$. Then $u'v'w' = utv'w' = uvtw'$, hence $\|\alpha(m), \alpha'(m)\| = \|uvw, uvtw'\| = \|w, tw'\| = \|uw, utw'\| = \|uw, u'w'\| = \|\alpha(xz), \alpha'(xz)\|$, which allows us to conclude by induction on the length of m.

Clearly, condition (C) is decidable, which completes the first part of the proof.

(2) We construct now a transducer for $\alpha \wedge \alpha'$, which will imply that it is a rational function. This construction is a rather classical covering construction, so we shall not be very formal.

We call a path in $\bar{T}$ *elementary* if it starts from (q_0, q'_0) and if only the last vertex is allowed to appear more than once, and in this case, only twice. Hence, such a path is either a simple path, or the concatenation of a simple path with a simple circuit, as in condition (C).

Denote by $u \wedge v$ the longest common left factor of the words u and v. We construct a tree T^* having the set of elementary paths in $\bar{T}$ as a set of nodes; there is an edge from π to π' in T^* if $\pi' = \pi e$, with e an edge in $\bar{T}$. Note that π, π' correspond to paths $(q_0, q'_0) \xrightarrow{x/(u,u')} (p, p')$ and $(q_0, q'_0) \xrightarrow{xa/(v,v')} (q, q')$, with u (respectively, u') a left factor of v (respectively, v'); so we have an equation $v \wedge v' = (u \wedge u')s$, for some word s in B^*: then the previously created edge in T^* will be labelled by a/s.

Call an elementary path *complete* if its last state is repeated. Now, in T^*, merge the node corresponding to such a state with its first occurrence in the path: in this way, we obtain a transducer S; let β be the function computed by S.

We show that $\beta = \alpha \wedge \alpha'$. Clearly, $\beta(m) = (\alpha \wedge \alpha')(m)$ for any word m such that there is in $\bar{T}$ an elementary path $(q_0, q'_0) \xrightarrow{m/\cdots} (q_f, q'_f)$.

It follows that this equality is true for each short enough word m. Now, let m be such that there is a nonelementary path $(q_0, q'_0) \xrightarrow{m/\cdots} (q_f, q'_f)$. Then this path may be decomposed as

$$(q_0, q'_0) \xrightarrow{x/(u,u')} (q, q') \xrightarrow{y/(v,v')} (q, q') \xrightarrow{z/(w,w')} (q_f, q'_f),$$

where the first two factors form an elementary path, for some factorizations $m = xyz$, $\alpha(m) = uvw$, $\alpha'(m) = u'v'w'$. Moreover, $\alpha(xz) = uw$ and $\alpha'(xz) = u'w'$.

This corresponds in S to a path

$$(q_0, q_0') \xrightarrow{x/\bar{u}} (q, q') \xrightarrow{y/\bar{v}} (q, q') \xrightarrow{z/\bar{w}} (q_f, q_f').$$

By construction, we have $\bar{u} = u \wedge u'$, $\bar{u}\bar{v} = uv \wedge u'v'$. By induction on $|m|$, we also have $(\alpha \wedge \alpha')(xz) = \beta(xz) = \bar{u}\bar{w}$. Now, condition (C) holds, so we have, e.g., $u' = ut$ and $tv' = vt$. Hence, $\bar{u}\bar{w} = uw \wedge u'w' = uw \wedge utw' = u(w \wedge tw')$. As $\bar{u} = u \wedge u' = u$, we obtain $\bar{w} = w \wedge tw'$. Moreover, $\alpha(m) \wedge \alpha'(m) = uvw \wedge u'v'w' = uvw \wedge uvtw' = uv(w \wedge tw') = uv\bar{w}$. Now, we have also $\bar{u}\bar{v} = uv \wedge u'v' = uv \wedge uvt = uv$, so that $\alpha(m) \wedge \alpha'(m) = \bar{u}\bar{v}\bar{w} = \beta(xyz) = \beta(m)$, which had to be shown. □

3. A characterization of rational functions. We give a characterization of rational functions, which has some formal analogy with the Nerode criterion for rational languages and which is related to Choffrut's theorem (see § 2).

As we consider partial functions, it will be convenient to use symbol $\varnothing$, and the distance will be extended by setting

$$\|\varnothing, \varnothing\| = 0, \qquad \|\varnothing, u\| = \|u, \varnothing\| = \infty$$

for any word u. By convention, we have $n < \infty$ for any number n and $n + \infty = \infty$. Then, the triangular inequality remains valid. Now, let α be a fixed (partial) function $A^* \to B^*$, where A, B are finite alphabets. Define a relation

$$u \sim v$$

on A^* by the condition

$$\sup \{\|\alpha(fu), \alpha(fv)\|, f \in A^*\} < \infty.$$

Note that, by the above conventions, $u \sim v$ implies that $\alpha(fu) = \varnothing$ if and only if $\alpha(fv) = \varnothing$. This implies, by the triangular inequality, that $\sim$ is transitive. Moreover, it is clearly reflexive and symmetric and it is not difficult to show that $\sim$ is left compatible, i.e., $u \sim v \Rightarrow xu \sim xv$ for any word x. Hence $\sim$ is a left congruence of A^*.

We call it the *syntatic left congruence* of α. The terminology is justified by the following observation: if α is the characteristic partial function of a language L (i.e., $\alpha(w) = 1$ if $w = L$, $= \varnothing$ if $w \notin L$), then its syntactic left congruence is the usual syntactic left congruence of L. One could, of course, also define the right syntactic congruence in a symmetric way.

The main result of this section is given in the following theorem.

THEOREM 1. *A partial function $\alpha : A^* \to B^*$ is rational if and only if its syntactic left congruence is of finite index and if $\alpha^{-1}(L)$ is rational for any rational language $L \subset B^*$.*

A consequence of this result is a new proof of the Hankel-like characterization of [13].

COROLLARY. *A partial function $\alpha : A^* \to B^*$ is rational if and only if there exists an integer n and partial functions $\beta_i, \gamma_i : A^* \to B^*$, $1 \leqq i \leqq n$, such that for any words x, y*

$$\alpha(xy) = \bigcup_{1 \leqq i \leqq n} \beta_i(x)\gamma_i(y). \tag{2}$$

Proof. We prove the theorem and its corollary at the same time by showing that α rational $\Rightarrow$ α satisfies the Hankel property $\Rightarrow$ $\sim$ of finite index and α^{-1} preserves rationality $\Rightarrow$ α rational. The first implication is Lemma 1 and one-half of the second is Lemma 3. So, assuming (2), we show that the syntactic congruence $\sim$ of α is of finite index.

We show that the condition

$$\forall i, \quad 1 \leqq i \leqq n : \gamma_i(u) \neq \varnothing \quad \text{iff} \quad \gamma_i(v) \neq \varnothing \tag{3}$$

implies $u \sim v$: this will imply that the index of $\sim$ is less than or equal to 2^n. So, let (3) be satisfied and define N to be some integer greater than the lengths of the words $\gamma_i(u)$, $\gamma_i(v) \neq \emptyset$, $1 \leqq i \leqq n$. Let f be any word; we show that $\|\alpha(fu), \alpha(fv)\| < 2N$. Indeed, if $\alpha(fu) = \emptyset$, then by (2), for any i, either $\beta_i(f) = \emptyset$ or $\gamma_i(u) = \emptyset$. By (3) we obtain: for all i, $\beta_i(f)$ or $\gamma_i(v) = \emptyset$, and again by (2), $\alpha(fv) = \emptyset$. In this case, $\|\alpha(fu), \alpha(fv)\| = 0 < 2N$. On the other hand, if $\alpha(fu) \neq \emptyset$, then there exists by (2) an i such that $\alpha(fu) = \beta_i(f)\gamma_i(u)$ and $\beta_i(f) \neq \emptyset \neq \gamma_i(u)$. Hence, by (3), we have $\gamma_i(v) \neq \emptyset$, which implies by (2) that $\alpha(fv) = \beta_i(f)\gamma_i(v)$. Hence

$$\|\alpha(fu), \alpha(fv)\| = \|\beta_i(f)\gamma_i(u), \beta_i(f)\gamma_i(v)\| = \|\gamma_i(u), \gamma_i(v)\| < 2N.$$

Finally, we have $\sup\{\|\alpha(fu), \alpha(fv)\|, f \in A^*\} < \infty$ and thus $u \sim v$.

We now show the last implication: if $\sim$ is of finite index and if α^{-1} preserves rationality, then α is a rational function.

Since $\sim$ is a left congruence of finite index on A^*, the set

$$Q = A^*/\sim$$

is a finite set with a left action $(w, q) \mapsto wq$ of A^* on Q. Consider the finite alphabet $A \times Q$ and define a length-preserving function

$$\gamma : A^* \to (A \times Q)^*$$

by

$$\gamma(a_n \cdots a_1) = (a_n, q_{n-1}) \cdots (a_2, q_1)(a_1, q_0),$$

where $a_i \in A$, q_0 is the class of 1 mod $\sim$ and where $q_i = a_i q_{i-1}$ for $i = 1, \cdots, n-1$. This function γ is clearly sequential from right to left, and hence a rational function (see [1, Chap. 4, Cor. 2.3]). Clearly, γ is injective, hence γ^{-1} is a partial function. Actually, $\gamma^{-1} = \pi | \mathrm{Im}\,(\gamma)$, where π is the canonical projection

$$\pi : (A \times Q)^* \to A^*.$$

Define $\beta = \alpha \circ \gamma^{-1} : (A \times Q)^* \to B^*$. We have $\alpha = \beta \circ \gamma$ since γ is a total function. We show that β is a subsequential function, hence it is rational (see [1, Chap. 4, Prop. 2.4]); this will imply that α is rational, as a product of rational functions. (See [1, Chap. 3, Thm. 4.4 and Def., § 1].)

We use Choffrut's theorem, stated in § 2. As β^{-1} clearly preserves rationality (because $\beta^{-1} = \gamma \circ \alpha^{-1}$ and γ and α^{-1} both preserve rationality), it is enough to show that β is uniformly bounded.

CLAIM. *If $FU \in \mathrm{Im}(\gamma)$ with $F \neq 1$, then the last letter of F is of the form (a, uq_0) where $u = \pi(U)$.*

This is immediate from the definition of γ.

Let k be an integer. Define K to be some integer greater than $\|\alpha(fu), \alpha(fv)\|$ for any word f and any words u, v such that $u \sim v$ and $|u| + |v| \leqq k$, and greater than $\|\beta(X), \beta(Y)\|$ for $|X| + |Y| \leqq k$ and $X, Y \in \mathrm{dom}\,(\beta)$.

This is possible by the definition of $\sim$ and the fact that the words u, v with $|u| + |v| \leqq k$ (respectively, the words X, Y with $|X| + |Y| \leqq k$) are finite in number.

We show that

$$(4) \qquad \forall X, Y \in \mathrm{dom}\,(\beta), \qquad \|X, Y\| \leqq k \Rightarrow \|\beta(X), \beta(Y)\| \leqq K,$$

which will imply that β is uniformly bounded. By the definition of K, it is enough to prove (4) for $|X| + |Y| > k$.

So, let X, Y with $X, Y \in \mathrm{dom}(\beta)$, $|X|+|Y| > k$, $\|X, Y\| \leqq k$. We may write $X = FU$, $Y = FV$, where F is the longest common left factor of X and Y. Since $\|X, Y\| \leqq k$, we have $|U|+|V| \leqq k$. Since $|X|+|Y| > k$, we also have $F \neq 1$.

Let $u = \pi(U)$, $v = \pi(V)$, $f = \pi(F)$. Since $X, Y \in \mathrm{dom}(\beta)$, we have $X, Y \in \mathrm{Im}(\gamma)$; hence, by the claim, the last letter of F is $(a, uq_0) = (a, vq_0)$, and thus $uq_0 = vq_0$, which implies $u \sim v$. By the definition of β, we have $\beta(X) = \alpha(fu)$ and $\beta(Y) = \alpha(fv)$. Since $|u|+|v| = |U|+|V| \leqq k$, we have by the definition of K, $\|\alpha(fu), \alpha(fv)\| \leqq K$, i.e., $\|\beta(X), \beta(Y)\| \leqq K$, which proves (4). □

4. A canonical bimachine. We modify slightly the definition of a generalized bimachine, as given in [1] and [7]. One of the reasons for this is that we want to give an arbitrary image to the empty word under the function computed by the bimachine.

A bimachine is given by

- A finite set L of *left states*, with right action $L \times A^* \to L$, $(l, w) \mapsto lw$, and a *left initial state* l_0.
- A finite set R of *right states*, with a left action $A^* \times R \to R$, $(w, r) \mapsto wr$, and with a *right initial state* r_0.
- An *output function* $\omega : \mathbf{L} \times A \times \mathbf{R} \to B^*$.
- A *final left function* $\lambda : \mathbf{R} \to B^*$ and a *final right function* $\rho : L \to B^*$.

The output function is extended to $L \times A^* \times R$ by the formula

$$\omega(l, uv, r) = \omega(l, u, vr)\omega(lu, v, r). \tag{5}$$

In particular, $w(l, 1, r) = 1$. The function computed by the bimachine is $\alpha : A^* \to B^*$ defined by

$$\alpha(w) = \lambda(wr_0)\omega(l_0, w, r_0)\rho(l_0 w). \tag{6}$$

If $w = a_1 \cdots a_n (a_i \in A)$, this may be written more algorithmically (using (5)) as

$$\alpha(a_1 \cdots a_n) = \lambda(a_1 \cdots a_n r_0) \cdot \prod_{i=1}^{n} \alpha(l_0 a_1 \cdots a_{i-1}, a_i, a_{i+1} \cdots a_n r_0) \times \rho(l_0 a_1 \cdots a_n). \tag{7}$$

When R is reduced to a single element, then a bimachine is simply a subsequential transducer, as in [1] (a subsequential transducer is sometimes called a generalized sequential machine with endmarker, see [5, Thm. 2.2]). A bimachine in the sense of [1], [7] is a bimachine as above, where λ and ρ are constant functions equal to 1.

Let $\alpha : A^* \to B^*$ be a function. We define on A^* a relation, which will be reflexive, symmetric, compatible with left multiplication, *but not transitive* in general. We call it the (*left*) *syntactic adjacency relation* of α, denoted by

$$u \leftrightarrow v.$$

It is defined by

$$\sup\{\|\alpha(fu), \alpha(fv)\|, f \in A^*, \alpha(fu) \neq \varnothing \neq \alpha(fv)\} < \infty. \tag{8}$$

Note that, in view of the definition of adjacent functions (§ 2), one has $u \leftrightarrow v$ if and only if the two functions $f \mapsto \alpha(fu)$ and $f \mapsto \alpha(fv)$ are adjacent. It is also easy to see that α is uniformly bounded if and only if $u \leftrightarrow v$ for any words u and v. Note, moreover, that if $\mathrm{dom}(\alpha) = A^*$, then $\leftrightarrow$ is transitive and equal to the left syntactic congruence of α.

We call a left congruence $\sim$ on A^* *compatible* with $\leftrightarrow$ if for any words u, v,

$$u \sim v \Rightarrow u \leftrightarrow v.$$

In terms of their graphs, this means that $\#(\sim)$ is contained in $\#(\leftrightarrow)$. Recall that when $\sim$ is a left congruence, then $R = A^*/\sim$ is naturally equipped with a left action $A^* \times R \to R$.

THEOREM 2. *Let $\alpha : A^* \to B^*$ be a rational function. Let $\sim$ be a left congruence of finite index on A^* and $R = A^*/\sim$ and r_0 the class of* 1 mod $\sim$. *The following conditions are equivalent*:

(i) *$\sim$ is compatible with the syntactic adjacency relation of α.*

(ii) *R, together with the natural left action and r_0 as initial right state, is the set of right states of some bimachine computing α.*

It will turn out that the bimachine that we obtain in the proof is completely canonical, once $\sim$ is given. Moreover, one may choose for $\sim$ the congruence considered in the previous section, thus obtaining a completely canonical bimachine. On the other hand, we shall verify that this bimachine is minimal, in the sense stated in the introduction, when α is a total function.

Proof of Theorem 2 (first part). (ii)$\Rightarrow$(i): Let R be the set of right states of a bimachine computing α. We have, by the definition of R,

$$u \sim v \Leftrightarrow ur_0 = vr_0.$$

We have to show that $u \sim v$ implies (8). Suppose that $u \sim v$, that is, $ur_0 = vr_0 = r$, for some r in R. Let N be some integer greater than the lengths of the words (if defined) $\omega(l, u, r_0)\rho(l')$ and $\omega(l, v, r_0)\rho(l')$, for l, l' in L. We have, by (5) and (6),

$$\begin{aligned}\alpha(fu) &= \lambda(fur_0)\omega(l_0, fu, r_0)\rho(l_0 fu)\\ &= \lambda(fur_0)\omega(l_0, f, ur_0)\omega(l_0 f, u, r_0)\rho(l_0 fu)\\ &= \lambda(fr)\omega(l_0, f, r)\omega(l_0 f, u, r_0)\rho(l_0 fu).\end{aligned}$$

Similarly,

$$\alpha(fv) = \lambda(fr)\omega(l_0, f, r)\omega(l_0 f, v, r_0)\rho(l_0 fv).$$

If $\alpha(fu) \neq \varnothing \neq \alpha(fv)$, then $\alpha(fu)$ and $\alpha(fv)$ have $\lambda(fr)\omega(l_0, f, r)$ as a common left factor, hence

$$\|\alpha(fu), \alpha(fv)\| < 2N.$$

This shows (8), and thus $\sim$ is compatible with the left adjacency of α. □

Before continuing the proof, we need several lemmas.

LEMMA 5. *If α is a rational function and $\sim$ is a left congruence on A^* of finite index, then there exist nonempty rational functions β_i, γ_i, $1 \leqq i \leqq n$, such that*

(i) $\forall u, v \in A^*$, $\alpha(uv) = \bigcup_{1 \leqq i \leqq n} \beta_i(u)\gamma_i(v)$.

(ii) *Each set* dom (γ_i) *is contained in a single class* mod $\sim$.

Proof. (i) follows from Lemma 1 and its proof, which show that β_i, γ_i may be chosen rational. Now, note that each class mod $\sim$ is a rational language, and that the restriction of a rational function to a rational language is still rational. So, replacing in (i) each γ_i by the union of its restrictions to each class mod $\sim$, we obtain (ii). □

Remark 2. Using this lemma, it is easy to prove that *the graph of the syntactic adjacency relation of a rational function is a recognizable subset of $A^* \times A^*$* (in the sense of [1, Chap. 3, Thm. 1.5] and [7], i.e., a finite union of sets $K \times L$, where K, L are rational languages).

Indeed, define $i \leftrightarrow j$ if the functions β_i, β_j are adjacent. Now, for $I, J \subset \{1, \cdots, n\}$, define $I \leftrightarrow J$ if for any i in I, j in J, one has $i \leftrightarrow j$. Finally, let $I(u) = \{i \mid u \in \text{dom}(\gamma_i)\}$.

Then one shows that $u \leftrightarrow v$ if and only if $I(u) \leftrightarrow I(v)$. This implies that the graph of $\leftrightarrow$ is equal to

$$\bigcup_{I \leftrightarrow J} \{u \in A^* \mid I(u) = I\} \times \{v \in A^* \mid I(v) = J\},$$

which is recognizable.

We need to define the operator "longest common left factor" for sets of words rather than only pairs of words. For technical reasons, it should also be defined on the empty set. Each singleton set will be identified with its element. So, for a nonempty language L, let $\bigwedge L$ denote the longest common left factor of the words in L equal to $\emptyset$ if $L = \emptyset$.

For $x_1, \cdots, x_n \in A^* \cup \{\emptyset\}$, we define $x_1 \wedge \cdots \wedge x_n$ to be $\bigwedge L$, where L is the underlying set of the sequence. So $x_1 \wedge \cdots \wedge x_n \neq \emptyset$ if and only if at least one x_i is not equal to $\emptyset$. Note that if L is a language, then $\bigwedge L = \bigwedge L'$ for some sublanguage L' of cardinality less than or equal to 2 (indeed, if $|L| \geqq 2$, there exist words u, v in L such that $u \wedge v = \bigwedge L$). If $\alpha_1, \cdots, \alpha_n$ are functions $A^* \to B^*$, then the function $\alpha = \alpha_1 \wedge \cdots \wedge \alpha_n$ will be defined by $\alpha(f) = \alpha_1(f) \wedge \cdots \wedge \alpha_n(f)$. Note that $\mathrm{dom}\,(\alpha) = \bigcup_{1 \leqq i \leqq n} \mathrm{dom}\,(\alpha_i)$, in view of the definitions.

We shall use the easily verified identities

$$\bigwedge \left(\bigcup_{i \in I} L_i \right) = \bigwedge_{i \in I} \left(\bigwedge L_i \right)$$

for any languages L_i, $i \in I$, and

$$\bigwedge (gL) = g\left(\bigwedge L\right)$$

for any language L and g in $A^* \cup \{\emptyset\}$.

LEMMA 6. *Let $\alpha_1, \cdots, \alpha_n : A^* \to B^*$ be pairwise adjacent functions such that each α_i^{-1} preserves rationality.*

(i) *For any words g_1, g_2 in B^*, the language*

$$\{f \mid \exists w \in B^*, \alpha_1(f) = wg_1, \alpha_2(f) = wg_2\}$$

is rational.

(ii) *If the functions α_i are, moreover, rational, then $\alpha_1 \wedge \cdots \wedge \alpha_n$ is rational.*

Note that this gives an alternative proof of the following: α, α' rational and adjacent implies $\alpha \wedge \alpha'$ rational (see Proposition 1).

Remark 3. Let α_1, α_2 be as in Remark 1. Then the language $\{f \in A^* \mid \alpha_1(f) = \alpha_2(f)\}$ (this is the case $g_1 = 1 = g_2$ of the lemma) is equal to $\{f \in A^*, |f|_{a_1} = |f|_{a_2}\}$, and hence is not rational. This shows that the adjacency hypothesis is not superfluous in Lemma 6.

Proof. (i) Let p be an integer such that $|g_1|, |g_2| < p$ and that for any f in A^*, $\alpha_1(f)$ and $\alpha_2(f)$, if defined, differ only by a right factor of length less than p.

We show that for f in A^*, the condition

(a) $\exists w \in B^*, \quad |w| \geqq p, \quad \alpha_1(f) = wg_1$ and $\alpha_2(f) = wg_2$

is equivalent to the condition

(b) $\exists i \in \{0, \cdots, 2p-1\}, \quad \exists u \in B^p$ such that $\alpha_1(f) \in B^i(B^{2p})^* ug_1$ and $\alpha_2(f) \in B^i(B^{2p})^* ug_2$.

Suppose that this is proved. Then the language L of the lemma is equal to $L_1 \cup L_2$, where $L_1 = \{f \in A^* \mid f \text{ satisfies (a)}\}$ and $L_2 = \{f \in L, |\alpha_1(f)| \leqq 2p \text{ or } |\alpha_2(f)| \leqq 2p\}$. By the hypothesis that the α_i^{-1} preserve rationality and by (b), L_1 is rational. Moreover, if $\alpha_1(f)$ is short, then so is $\alpha_2(f)$ and vice versa. Hence, L_2 is contained in a finite union of languages of the form $L_w = \{f \in A^* \mid \alpha_1(f) = wg_1 \text{ and } \alpha_2(f) = wg_2\}$, which are also rational; since each L_w is contained in L, we conclude that L is rational.

It is clear that (a) implies (b). Suppose that (b) holds, that is, $\alpha_1(f) = s_1 u g_1$, $\alpha_2(f) = s_2 u g_2$ with $|s_1|, |s_2| \equiv i \bmod 2p$. We must show that $s_1 = s_2$. By adjacency, we have $\alpha_1(f) = th_1$, $\alpha_2(f) = th_2$ with $|h_1|, |h_2| < p$. As $|g_1|, |g_2| < p$, the difference between $|s_1 u|$ and $|t|$ is less than p. The case is similar for $|s_2 u|$ and $|t|$. Thus $\|s_1| - |s_2\| = \|s_1 u| - |s_2 u\| < 2p \Rightarrow |s_1| = |s_2|$.

Now, $|h_1| \leqq p \leqq |u g_1|$, which implies, by $s_1 u g_1 = th_1$, that $|s_1| \leqq |t|$, hence s_1 is a left factor of t. Similarly, s_2 is a left factor of t. As they are of equal length, they are equal.

(ii) We have, by a previous formula,

$$\alpha_1 \wedge \cdots \wedge \alpha_n = (\alpha_1 \wedge \alpha_2) \wedge \alpha_3 \wedge \cdots \wedge \alpha_n,$$

hence we may assume that $n = 2$, because each α_i is adjacent to $\alpha_1 \wedge \alpha_2$.

Without loss of generality, we may assume that $\mathrm{dom}(\alpha_1) = \mathrm{dom}(\alpha_2) = D$. Then D is a finite union of languages $D(g_1, g_2)$, where $D(g_1, g_2) = \{f \in A^* \mid \exists w \in B^*, \alpha_1(f) = w g_1, \alpha_2(f) = w g_2\}$ and where g_1 and g_2 have no common left factor. Each of these languages is rational by (i), and if $f \in D(g_1, g_2)$, then $(\alpha_1 \wedge \alpha_2)(f) = \alpha_1(f) g_1^{-1}$. Hence, the restriction of $\alpha_1 \wedge \alpha_2$ to $D(g_1, g_2)$ is rational, and finally $\alpha_1 \wedge \alpha_2$ is rational, as the union of a finite number of rational functions. □

LEMMA 7. *Let $\alpha : A^* \to B^*$ be a rational function, and $\sim$ a left congruence on A^* of finite index that is compatible with the left syntactic adjacency relation of α. Let $R = A^*/\sim$ and define for each r in R a function α_r by*

$$\alpha_r(f) = \bigwedge \{\alpha(fu) \mid u \in A^*, ur_0 = r\},$$

where r_0 is the class of 1 mod $\sim$. *Then there exists a finite language L_r such that*

(i) $u \in L_r \Rightarrow ur_0 = r$,

(ii) $\alpha_r(f) = \bigwedge_{u \in L_r} \alpha(fu)$.

As a consequence, the function α_r is rational.

The point of the lemma is that L_r does not depend on f (otherwise, it is immediate, using a previous remark on $\bigwedge L$).

Proof. Suppose there exists a finite language L_r such that (i) and (ii) are satisfied. By (i) and compatibility of $\sim$, the words in L_r are pairwise in relation $\leftrightarrow$, that is, the functions $f \mapsto \alpha(fu)$ are, for u in L_r, pairwise adjacent. Since these functions are rational, we obtain by (ii) and Lemma 6(ii) that α_r is a rational function.

In order to prove that there exists a finite language L_r satisfying (i) and (ii), take β_i, γ_i as in Lemma 5. By condition (ii) of this lemma, there exists for each i a unique $r(i)$ such that $u \in \mathrm{dom}(\gamma_i) \Rightarrow ur_0 = r(i)$. We know that for each i, there exists a finite language $L_i \subset \mathrm{dom}(\gamma_i)$ such that $\bigwedge \gamma_i(A^*) = \bigwedge \gamma_i(L_i)$. Let $L_r = \bigcup_{r(i)=r} L_i$. We thus have $\bigwedge \{\gamma_i(u) \mid u \in \mathrm{dom}(\gamma_i)\} = \bigwedge \{\gamma_i(u) \mid u \in L_r\}$. Moreover, (i) holds by definition. We have also

$$\begin{aligned}
\alpha_r(f) &= \bigwedge \{\alpha(fu) \mid ur_0 = r\} \\
&= \bigwedge \{\beta_i(f)\gamma_i(u) \mid ur_0 = r, 1 \leqq i \leqq n \text{ and } u \in \mathrm{dom}(\gamma_i)\} \\
&= \bigwedge \{\beta_i(f)\gamma_i(u) \mid r(i) = r, u \in \mathrm{dom}(\gamma_i)\} \\
&= \bigwedge_{r(i)=r} (\bigwedge \{\beta_i(f)\gamma_i(u) \mid u \in \mathrm{dom}(\gamma_i)\}) \\
&= \bigwedge_{r(i)=r} \beta_i(f)(\bigwedge \{\gamma_i(u) \mid u \in \mathrm{dom}(\gamma_i)\}) \\
&= \bigwedge_{r(i)=r} \beta_i(f)(\bigwedge \{\gamma_i(u) \mid u \in L_r\}) \\
&= \bigwedge_{r(i)=r} (\bigwedge \{\beta_i(f)\gamma_i(u) \mid u \in L_r\}) \\
&= \bigwedge \{\beta_i(f)\gamma_i(u) \mid r(i) = r, u \in L_r\} \\
&= \bigwedge \{\alpha(fu) \mid u \in L_r\} \quad \text{(because } u \in L_r \text{ and } u \in \mathrm{dom}(\gamma_i) \Rightarrow r(i) = r\text{)} \\
&= \bigwedge_{u \in L_r} \alpha(fu).
\end{aligned}$$

□

LEMMA 8 (Notations of Lemma 7). *There exist a function* $\omega : A^* \times A^* \times R \to B^*$ *and a function* $\rho : A^* \to B^*$ *such that*

(i) *For any words* f, g *in* A^* *and state* r *in* R

$$\alpha_r(fg) = \alpha_{gr}(f)\omega(f, g, r);$$

(ii) *For any word* f *in* A^*

$$\alpha(f) = \alpha_{r_0}(f)\rho(f).$$

Proof. The second assertion is immediate, because by definition, $\alpha_{r_0}(f)$ is a left factor of $\alpha(f)$. If $\alpha(f) \neq \emptyset$, we define $\rho(f) = (\alpha_{r_0}(f))^{-1}\alpha(f)$. If $\alpha(f) = \emptyset$, we pose $\rho(f) = \emptyset$. Note that the set

$$\{\alpha(fgu) \mid u \in A^*, ur_0 = r\}$$

is contained in the set

$$\{\alpha(fv) \mid v \in A^*, vr_0 = gr\}.$$

Hence, by definition, $\alpha_{gr}(f)$ is a left factor of $\alpha_r(fg)$. If $\alpha_r(fg) \neq \emptyset$, we define $\omega(f, g, r) = (\alpha_{gr}(f))^{-1}\alpha_r(fg)$. If $\alpha_r(fg) = \emptyset$, we pose once again $\omega(f, g, r) = \emptyset$. □

LEMMA 9 (Notations of Lemma 7). *Define a relation* $\equiv$ *on* A^* *by*

$$f \equiv g$$

if and only if

$$\omega(fu, a, r) = \omega(gu, a, r)$$

for any word $u \in A^*$, *letter* $a \in A$, *and state* r *in* R, *and if*

$$\rho(fu) = \rho(gu)$$

for any word u. *Then* $\equiv$ *is a right congruence of finite index.*

Proof. Recall that when $\delta_1, \cdots, \delta_p$ are functions $A^* \to B^*$ such that

(i) Each $\delta_i(A^*)$ is finite;

(ii) For each g in B^* and i, $\delta_i^{-1}(g)$ is a rational language;

then by Nerode's criterion, the right congruence on A^*, defined by $f \equiv g$ if and only if $\delta_i(fu) = \delta_i(gu)$ for any i and u, is of finite index.

Hence, it is enough to show that the functions $\omega(\cdot, a, r) : f \mapsto \omega(f, a, r)$ and ρ have finite image and that for any a, r, g in B^*, the languages $\{f \in A^* \mid \omega(f, a, r) = g\}$ and $\{f \in A^* \mid \rho(f) = g\}$ are rational.

For this, it is enough, in view of Lemma 6(i) and Lemma 7, to show that the functions $f \mapsto \alpha_r(fa)$ and $f \mapsto \alpha_{ar}(f)$ are adjacent for any $a \in A$ and $r \in R$, and that the functions α and α_{r_0} are adjacent.

By Lemma 7, we have $\alpha_r(fa) = \bigwedge_{u \in L_r} \alpha(fau)$ and $\alpha_{ar}(f) = \bigwedge_{v \in L_{ar}} \alpha(fv)$.

Note that $u \in L_r$ and $v \in L_{ar}$ implies that $ur_0 = r \Rightarrow aur_0 = ar$, and $vr_0 = ar$. Hence $au \sim v$, which implies $au \leftrightarrow v$ and the functions $f \mapsto \alpha(fau)$ and $f \mapsto \alpha(fv)$ are adjacent. Moreover, for $w, w' \in L_r$, one has $w \sim w'$ (by Lemma 7 (i)), hence $w \leftrightarrow w'$ (by compatibility of $\sim$), hence the functions $f \mapsto \alpha(fw)$ and $f \mapsto \alpha(fw')$ are adjacent. This shows that the functions $f \mapsto \alpha_r(fa)$ and $f \mapsto \alpha_{ar}(f)$ are adjacent, because of the following easily verified fact: if $\alpha_1, \cdots, \alpha_n$ (respectively, $\beta_1, \cdots, \beta_p$) are pairwise adjacent, and if each α_i is adjacent to each β_j, then $\alpha_1 \wedge \cdots \wedge \alpha_n$ is adjacent to $\beta_1 \wedge \cdots \wedge \beta_p$.

Moreover, $\alpha_{r_0}(f) = \bigwedge_{u \in L_{r_0}} \alpha(fu)$ and a similar proof shows that this function is adjacent to α. □

Proof of Theorem 2 (Second part). Let $L = A^*/\equiv$, where $\equiv$ is the right congruence of Lemma 9. Then L is finite, and equipped with a right action $L \times A^* \to L$. For l in L, a in A, and r in R, we may define $\omega(l, a, r) = \omega(f, a, r)$ and $\rho(l) = \rho(f)$, where f is a representative of l mod $\equiv$.

Let l_0 be the class of 1 mod $\equiv$. Define a function $\lambda : R \to B^*$ by $\lambda(r) = \alpha_r(1)$.

With these pointed sets (L, l_0), (R, r_0) and functions ω, λ, ρ, we obtain a bimachine for which we have only to verify that it computes α, that is, formulas (5) and (6). For this, it is enough to show that the functions ω and ρ of Lemma 8 satisfy

$$\omega(f, gh, r) = \omega(f, g, hr)\omega(fg, h, r) \tag{9}$$

and

$$\alpha(f) = \lambda(fr_0)\omega(1, f, r_0)\rho(f). \tag{10}$$

But we have, by Lemma 8,

$$\alpha_r(fgh) = \alpha_{ghr}(f)\omega(f, gh, r)$$

and

$$\begin{aligned}\alpha_r(fgh) &= \alpha_{hr}(fg)\omega(fg, h, r)\\ &= \alpha_{ghr}(f)\omega(f, g, hr)\omega(fg, h, r).\end{aligned}$$

So (9) is true as soon as $\alpha_{ghr}(f) \neq \varnothing$. When $\alpha_{ghr}(f) = \varnothing$, then $\alpha_r(fgh) = \varnothing$, and by the definition of ω, we have $\omega(fg, h, r) = \varnothing = \omega(f, gh, r)$. So, (9) is also true.

For (10), we have, by Lemma 8,

$$\alpha(f) = \alpha_{r_0}(f)\rho(f) = \alpha_{r_0}(1 \cdot f)\rho(f) = \alpha_{fr_0}(1)\omega(1, f, r_0)\rho(f) = \lambda(fr_0)\omega(1, f, r_0)\rho(f),$$

which proves (10). □

Remark 4. (1) Note that when r_0 in R is replaced by r, and ρ by the constant function ρ' equal to 1, then this new bimachine computes α_r. Indeed, by Lemma 8,

$$\alpha_r(f) = \alpha_r(1 \cdot f) = \alpha_{fr}(1)\omega(1, f, r) = \lambda(fr)\omega(l_0, f, r)\rho'(l_0 f).$$

(2) When α is a subsequential function, then its left syntactic adjacency is universal (i.e., $u \leftrightarrow v$ for any word u, v), hence a left congruence. If one takes this congruence for $\sim$ in Theorem 2, then the bimachine constructed in the proof is exactly the minimal subsequential transducer of α, as constructed by Choffrut [4] (see also [11]).

5. Example, remarks, and open problems. (a) Let $A = \{a, b\}$ and $\alpha : A^* \to A^*$ be the function which removes odd runs in a word. More formally, if

$$w = a^{i_1}b^{j_1} \cdots a^{i_k}b^{j_k}$$

where the exponents are greater than or equal to 1, except possibly i_1 and j_k, then define

$$i'_s = \begin{cases} i_s & \text{if } i_s \text{ is even} \\ 0 & \text{otherwise;} \end{cases}$$

$$j'_s = \begin{cases} j_s & \text{if } j_s \text{ is even} \\ 0 & \text{otherwise.} \end{cases}$$

Then $\alpha(w) = a^{i'_1}b^{j'_1} \cdots a^{i'_k}b^{j'_k}$. Moreover, $\alpha(1) = 1$.

We leave to the reader the verification of the following facts.

(1) The left syntactic congruence $\sim$ of α is generated by the relations

$$a^2 \sim 1, \qquad b^2 \sim 1, \qquad ab \sim a, \qquad ba \sim b.$$

(2) Identify $R = A^*/\sim$ with $\{1, a, b\}$. The functions $\alpha_1, \alpha_a, \alpha_b$ are defined by $\alpha_1 = \alpha$, $\alpha_a(f) = \alpha(fa)$, $\alpha_b(f) = \alpha(fb)$.

(3) The function ρ is constant and equal to 1, and

$$\omega(f, a, 1) = \omega(f, b, 1) = \omega(f, a, b) = \omega(f, b, a) = 1.$$

Moreover,

$$\omega(f, a, a) = \begin{cases} a^2 & \text{if the last run of } f \text{ is an even run of } a\text{'s or if} \\ & f \text{ does not end with } a. \\ 1 & \text{otherwise;} \end{cases}$$

$$\omega(f, b, b) = \begin{cases} b^2 & \text{if the last run of } f \text{ is an even run of } b\text{'s or if} \\ & f \text{ does not end with } b. \\ 1 & \text{otherwise.} \end{cases}$$

(4) The right congruence $\equiv$ is generated by the relations

$$a^2 \equiv 1, \qquad b^2 \equiv 1, \qquad ab \equiv b, \qquad ba \equiv a.$$

Actually, it is the *right* syntactic congruence of α (this is not a general fact, even for everywhere-defined functions).

(5) The function λ is constant equal to 1 and if $L = A^*/\equiv$ is identified with $\{1, a, b\}$, then ω is described by the following tables

l \ r	1	a	b
1	1	a^2	1
a	1	1	1
b	1	a^2	1

$\omega(l, a, r)$

l \ r	1	a	b
1	1	1	b^2
a	1	1	b^2
b	1	1	1

$\omega(l, b, r)$

5.1. Minimization. We verify that, when α is a *total function*, then the bimachine constructed in the proof of Theorem 2 has the minimum number of left states among all bimachines computing α, with R as a set of right states (with its natural left action), with r_0 as initial right state.

So let α be computed by the bimachine B' with a set of left states L', initial left state l'_0, set of right states R, initial right state r_0, output function ω', final left function λ', and final right function ρ'.

We show that for any words g, f in A^*, the equality $l'_0 f = l'_0 g$ implies $f \equiv g$ (where $\equiv$ is the right congruence of Lemma 9). This will imply that $L = A^*/\equiv$ has fewer elements than $l'_0 A^*$, hence fewer than L' (because $l'_0 A^* \subset L$).

We work in the free group generated by A. With the notations of Lemma 7, we have

$$\alpha_r(f) = \bigwedge \{\alpha(fu) \mid u \in A^*, ur_0 = r\}. \tag{11}$$

By (5) and (6) applied to bimachine B', we have

$$\alpha(fu) = \lambda'(fur_0)\omega'(l'_0, f, ur_0)\omega'(l'_0 f, u, r_0)\rho'(l'_0 fu).$$

This, along with (11), implies that

$$\alpha_r(f) = \lambda'(fr)\omega'(l'_0, f, r)\beta(l'_0 f, r) \tag{12}$$

where $\beta: L' \times R \to B^*$ is the function defined by

$$\beta(l', r) = \bigwedge \{\omega'(l', u, r_0)\rho'(l'u) \mid ur_0 = r\}.$$

From (12) we deduce

$$\begin{aligned} \alpha_r(fg) &= \lambda'(fgr)\omega'(l'_0, fg, r)\beta(l'_0 fg, r) \\ &= \lambda'(fgr)\omega'(l'_0, f, gr)\omega'(l'_0 f, g, r)\beta(l'_0 fg, r), \end{aligned} \tag{13}$$

where we have used (5) again. From (12) again, we deduce

$$\alpha_{gr}(f)\omega(f, g, r) = \lambda'(fgr)\omega'(l'_0, f, gr)\beta(l'_0 f, gr)\omega(f, g, r). \tag{14}$$

Recall that we have, by Lemma 8(i),

$$\alpha_r(fg) = \alpha_{gr}(f)\omega(f, g, r).$$

Using this and comparing (13) and (14), we therefore deduce that

$$\omega(f, g, r) = \beta(l'_0 f, gr)^{-1}\omega'(l'_0 f, g, r)\beta(l'_0 fg, r). \tag{15}$$

Indeed, α is a total function, so α_r and α_{gr} are total functions as well, and every factor in (13) and (14) is defined; we thus may simplify by $\lambda'(fgr)\omega'(l'_0, f, gr)$, and multiply (in the free group) by $\beta(l'_0 f, gr)^{-1}$.

By Lemma 8(ii), we have

$$\alpha(f) = \alpha_{r_0}(f)\rho(f).$$

As α is computed by β', and by (12), we thus obtain

$$\lambda'(fr_0)\omega'(l'_0, f, r_0)\rho'(l_0 f) = \lambda'(fr_0)\omega'(l'_0, f, r_0)\beta(l'_0 f, r_0)\rho(f).$$

Thus, we deduce

$$\rho(f) = \beta(l'_0 f, r_0)^{-1}\rho'(l_0 f). \tag{16}$$

Now, let f, g, u, a, r be as in Lemma 9, and suppose that $l'_0 f = l'_0 g$. Then by (15), used twice (with $f \to fu$, $g \to a$, and after $f \to gu$, $g \to a$), we obtain

$$\begin{aligned} \omega(fu, a, r) &= \beta(l'_0 fu, ar)^{-1}\omega'(l'_0 fu, a, r)\beta(l'_0 fua, r) \\ &= \beta(l'_0 gu, ar)^{-1}\omega'(l'_0 gu, a, r)\beta(l'_0 gua, r) = \omega(gu, a, r). \end{aligned}$$

Moreover, by (16), we have

$$\begin{aligned} \rho(fu) &= \beta(l'_0 fu, r_0)^{-1}\rho'(l_0 fu) \\ &= \beta(l'_0 gu, r_0)^{-1}\rho'(l_0 gu) = \rho(gu). \end{aligned}$$

This shows, by Lemma 9, that $f \equiv g$, which was to be shown.

5.2. Counterexample. We show that when α is not a total function, then the minimization result of § 5.1 is no longer valid. This is a mystery which should be elucidated elsewhere.

Let $\alpha : a^* \to a^*$ be defined by $\alpha(a^{2n}) = a^{2n}$, $\alpha(a^{2n+1}) = \varnothing$. Take $R = a^*/a^2 \sim 1$ ($\sim$ is the syntactic left congruence) and identify R with $\{1, a\}$. Then

$$\begin{aligned}
\alpha_1(1) &= \bigwedge \{\alpha(u),\ u.1 = 1\} \\
&= \bigwedge \{\alpha(a^{2n}),\ n \in \mathbb{N}\} = 1 \\
\alpha_1(a) &= \bigwedge \{\alpha(au),\ u.1 = 1\} \\
&= \bigwedge \{\alpha(aa^{2n}),\ n \in \mathbb{N}\} = \varnothing \\
\alpha_a(a^2) &= \bigwedge \{\alpha(a^2u),\ u.1 = a\} \\
&= \bigwedge \{\alpha(a^2a^{2n+1}),\ n \in \mathbb{N}\} = \varnothing \\
\alpha_a(a) &= \bigwedge \{\alpha(au),\ u.1 = a\} \\
&= \bigwedge \{\alpha(aa^{2n+1}),\ n \in \mathbb{N}\} = a^2.
\end{aligned}$$

Using Lemma 8, we have $\alpha_a(a) = \alpha_1(1)\ \omega(1, a, a)$ and $\alpha_a(a^2) = \alpha_1(a)\ \omega(a, a, a)$. Hence, $\omega(1, a, a) = a^2$, and $\omega(a, a, a) = \varnothing$ (see the proof of Lemma 8). We deduce, by Lemma 9, that $a \not\equiv 1$.

However, the function is subsequential in both directions, hence, it may be computed with R as a set of right states, and a trivial set of left states (i.e., a singleton).

The reader may find it instructive to compare the previous example to the two following ones:

$$\begin{cases} a^{2n} \to a^{2n} \\ a^{2n+1} \to b^{2n+1} \end{cases} \qquad \begin{cases} a^{2n} \to 1 \\ a^{2n+1} \to a \end{cases}.$$

The first function is not subsequential, in either direction, while the second is subsequential in both directions.

5.3. Open problem. A theory of morphisms between bimachines computing the same function α should be developed, keeping in mind the following possible conjecture: there are only a finite number of minimal bimachines computing α (minimal would mean universally attractive in the category of these bimachines).

One cannot expect a single minimal bimachine: evidence for this is given by the rational languages; there is no "morphic" relation between the left and the right minimal automaton.

5.4. Open problem. A bimachine has two sets of states, hence there are two finite monoids attached to it. Call a bimachine *aperiodic* such that these monoids are aperiodic (i.e., with trivial subgroups, or period equal to 1). Characterize the rational functions α, which are computed by some aperiodic bimachine. A tentative conjecture could be: α is as above if and only if for any rational language L, the period of $\alpha^{-1}(L)$ divides that of L (recall that p is a period of L if the cardinality of each cyclic subgroup of the syntactic monoid of L divides p).

More generally, a theory of varieties of rational functions could be made, as has been done for rational languages and finite monoids [10]. A first step would be to study sequential and subsequential functions.

5.5. Open problem. Characterize rational functions which are both left-to-right and right-to-left subsequential. These functions simultaneously generalize rational languages (by their characteristic function) and biprefix codes (by their decoding functions).

An answer in the case of numerical functions (i.e., with image in a cyclic free monoid) has been given by Choffrut and Schützenberger [6].

Acknowledgments. We want to thank the two referees for many valuable comments and suggestions.

REFERENCES

[1] J. Berstel, *Transductions and Context-Free Languages*, Teubner, Stuttgart, Germany, 1979.
[2] J. Berstel and D. Perrin, *Theory of Codes*, Academic Press, New York, 1985.
[3] J.-M. Boë, J. Boyat, J.-P. Bordat, and Y. Césari, *Une caractérisation des sous-monoïdes libérables*, in Théorie des codes, D. Perrin, ed., Laboratoire d'Informatique Théorique et de Programmation, Paris, (1979), pp. 9–20.
[4] C. Choffrut, *A generalization of Ginsburg and Rose's characterization of g.-s.-m. mappings*, Lecture Notes in Computer Science 71, Springer-Verlag, Berlin, New York, 1979, pp. 88–103.
[5] C. Choffrut and K. Culik, *Properties of finite and push-down transducers*, SIAM J. Comput., 12 (1983), pp. 300–315.
[6] C. Choffrut and M. P. Schutzenberger, *Counting with rational functions*, Theoret. Comput. Sci., 58 (1988), pp. 81–101.
[7] S. Eilenberg, *Automata, Languages and Machines*, Vol. A, Academic Press, New York, 1974.
[8] S. Ginsburg, *An Introduction to Mathematical Machine Theory*, Addison-Wesley, Reading, MA, 1962.
[9] M. Lothaire, *Combinatorics on Words*, Addison-Wesley, Reading, MA, 1983.
[10] J.-E. Pin, *Variétés de langages formels*, Masson, Paris, 1984.
[11] C. Reutenauer, *Subsequential functions: Characterizations, minimization, examples*, in Proc. International Meeting of Young Computer Scientists, Lecture Notes in Computer Science, J. Kelemen, ed., to appear.
[12] M. P. Schutzenberger, *A remark on finite transducers*, Inform. and Control, 4 (1961), pp. 185–196.
[13] ———, *Une propriété de Hankel des relations fonctionnelles entre monoïdes libres*, Adv. in Math., 24 (1977), pp. 274–280.

Année 1992

Bibliographie

[1992-1] Dominique Perrin et Marcel-Paul Schützenberger. Synchronizing prefix codes and automata and the road coloring problem. In *Symbolic dynamics and its applications (New Haven, CT, 1991)*, volume 135 of *Contemp. Math.*, pages 295–318. Amer. Math. Soc., Providence, RI, 1992.

[1992-2] Alain Lascoux et Marcel-Paul Schützenberger. Décompositions dans l'algèbre des différences divisées. *Discrete Math.*, 99(1-3) :165–179, 1992.

[1992-3] Christophe Reutenauer et Marcel-Paul Schützenberger. Rational word functions : characterization and minimization. In *Words, Languages and Combinatorics (Kyoto, 1990)*, pages 435–443. World Sci. Publishing, River Edge, NJ, 1992.

Contemporary Mathematics
Volume **135**, 1992

SYNCHRONIZING PREFIX CODES AND AUTOMATA AND THE ROAD COLORING PROBLEM

Dominique Perrin, Marcel-Paul Schützenberger
LITP
Institut Blaise Pascal
Paris

Abstract

We prove two new results concerning the existence of synchronizing words for prefix codes. Both results assert that any finite aperiodic maximal prefix code is equivalent to a synchronizing one under two equivalence relations to be defined more precisely below. One of these equivalence relations is that of tree isomorphism and is the subject of a conjecture, known as the road coloring conjecture, that is settled in the case corresponding to our hypotheses.

1. INTRODUCTION

The notion of a *synchronizing word* is a basic and elementary notion in automata theory. Given a finite deterministic automaton, a word x is called synchronizing if the state reached after processing the word x is independent of the initial state in which the automaton was started. This notion has been studied since the beginning of automata theory and appeared with E.F. Moore's "gedanken experiments". It also appears in many recent developments concerning automata (see e.g. Aho, 1988 or Eppstein, 1990). The term "synchronizing word" is however not universally in use and one may find instead *resolving block* (Adler, Marcus, 1979) or *reset sequence* (Eppstein, 1990).

From the abstract point of view, synchronizing words correspond, in the semigroup of transitions of the automaton, to elements of minimal possible rank. This algebraic formulation allows a generalization to non-deterministic automata (see Berstel, Perrin, 1985). From another viewpoint, the existence of synchronizing words guarantees an almost everywhere one-to-one correspondance between paths and their labels in an

1991 Mathematics Subject Classification. Primary 68Q70; Secondary 20M05.

This paper is in final form and no version will be submitted for publication elsewhere.

0271-4132/92 $1.00 + $.25 per page

appropriate measure space. It is this property which is of interest in the applications to coding since it guarantees stability against errors.

It is curious that such a simple notion gives rise to several unsolved problems. We mention two of them in this introduction : The Cerny-Pin conjecture and the road coloring conjecture.

The Cerny conjecture asserts that any n-state synchronizing automaton has a synchronizing word of length at most $(n-1)^2$. It is easy to prove the existence of a synchronizing word of length bounded by a cubic polynomial in n but no quadratic bound has yet been obtained. The simple example of the automaton of Figure 1.1 shows that the bound $(n-1)^2$ cannot be improved.

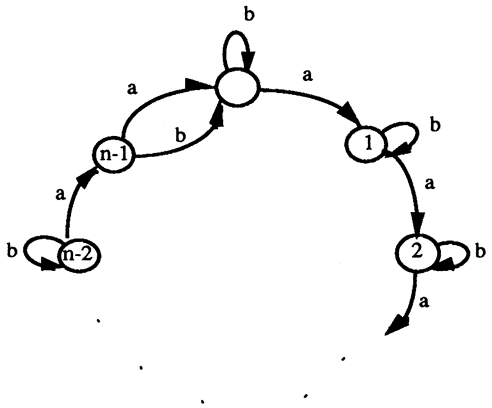


Figure 1.1. A worst case for Cerny's problem

The conjecture has been put in a more general form by Pin : if there is a word of rank d (as a mapping from the state set into itself) then there is one of length at most $(n-d)^2$. A bibliography on this problem can be found in (Berstel, Perrin, 1985). A recent result by A. Carpi (1988)shows that a cubic bound also holds in the case of unambiguous automata.

The road coloring problem is encountered in the study of isomorphism of symbolic dynamical systems (Adler, Goodwin, Weiss, 1977). It is conjectured that, except for the trivial case of periodicity, it is always possible to modify the labeling of the graph underlying a deterministic automaton to make it synchronizing. The name comes from the analogy

where the states of the automaton are cities and the edges roads connecting them. An appropriate coloring would allow a traveller to find his way to some city by following a fixed rule specifying the appropriate succession of colors, irrespective of his starting point. The conjecture is presently unsettled.

In this paper, we prove two new results on synchronizing words. Our results start with a prefix code instead of an automaton. Both notions are strongly related since, for any deterministic automaton, the set of first returns to a given state is a prefix code. However, our hypothesis are more easily formulated in terms of prefix codes.

We introduce an equivalence on prefix codes, called *the flipping equivalence*. It corresponds to isomorphism of the associated unlabeled trees.

Our first result is that any finite aperiodic maximal prefix code is flipping equivalent to a synchronizing one. The proof uses in a crucial way a theorem of Reutenauer (1985) giving a non-commutative factorization of the polynomial associated with a prefix code.

Our second result is a modification of the first one for another equivalence relation : the commutative equivalence which identifies words differing only in the relative ordering of their letters. The proof is quite similar to that of the previous result.

The first result settles, under our hypotheses, the road coloring problem. In terms of the original formulation, it settles it in the case of graphs satisfying the additional assumption that all vertices except one have exactly one entering edge. Such graphs are sometimes refered to as "renewal systems" in symbolic dynamics.

Our paper is organized as follows. In Section 2, we recall the definitions and results to be used later, especially the factorization theorem of Reutenauer. In Section 3, we discuss the case of an equivalence relation which is a common refinement of the two equivalence relations considered above. We reproduce a result of (Schützenberger, 1967) with part of its proof with the intention both of updating the statement and to prepare the study of the road coloring problem given in Section 6. In Section 4, we prove our main result concerning flipping equivalence. The corresponding result for commutative equivalence is proved in Section 5. Finally, in Section 6 we discuss the exact relationship of our results with the road

coloring problem.

2. PREFIX CODES

In all that follows we use the notation and terminology of (Berstel, Perrin, 1985). For the sake of readability we recall most of the definitions.

Let A be an alphabet. We denote by A^* the free monoid on the set A, which is the set of all finite sequences on A equipped with the concatenation as a product, the neutral element being the empty sequence, called the empty word. We denote by 1 the empty word and by $A^+ = A^* - 1$ the free semigroup on A. In general, we recall that a monoid is a set with a binary associative operation and a neutral element whereas a semigroup is the same but without the necessity of a neutral element.

A *prefix code* on A is a subset X of A^+ which contains no proper prefix of any of its elements. A prefix code can be identified with a labeled tree. Thus the prefix code $X = \{aa, ab, baa, bab\}$ on $A = \{a, b\}$ corresponds to the binary tree represented on Figure 2.1 with an obvious convention for the labeling using

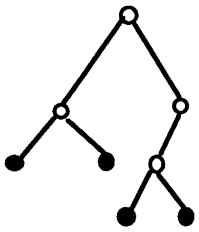


Figure 2.1. A prefix code

a for left and b for right. The words of X are in 1-1 correspondance with the leaves of the associated tree.

A *prefix* of X is a proper prefix of some word of X. The set of prefixes thus corresponds bijectively to the internal nodes of the associated tree.

For a subset X of A^*, we denote by X^* the submonoid generated by X. When X is a prefix code, X^* is free with basis X. This is the origin of the term "code" which refers in general to the uniqueness of parsing or deciphering.

A prefix code is said to be *maximal* when it is maximal under inclusion among the prefix codes on the alphabet A. It is easy to verify that a prefix

code X is maximal iff it is *right complete*, that is to say that for each word w in A^* one has

$$wA^* \cap XA^* \neq \emptyset \tag{2.1}$$

Equation (2.1) means that every word is comparable to a codeword for the prefix ordering. It is not difficult to prove that it is equivalent to the fact that each word w in A^* is a prefix of some word in X^*, i.e.

$$wA^* \cap X^* \neq \emptyset \tag{2.2}$$

In terms of trees, a prefix code is maximal iff the associated tree is a complete k-ary tree, where $k = Card(A)$.

We shall mainly discuss here *finite* prefix codes. We shall however occasionnally consider a much weaker condition defined as follows. A prefix code X on the alphabet A is called *thin* if there exists a word w in A^* that does not appear inside words of X, i.e. such that

$$A^*wA^* \cap X = \emptyset \tag{2.3}$$

A finite prefix code X is thin since only words of bounded length may appear inside words of X.

We now come to the definition of the objects of central interest to us. A word x is said to be *synchronizing* for a prefix code X if wx is in X^* for all words w in A^*. Hence x is synchronizing iff

$$A^*x \subset X^* \tag{2.4}$$

A prefix code X is called synchronizing if there exists a synchronizing word for X. A synchronizing prefix code is obviously maximal since Formula (2.4) is a uniformisation of Formula (2.2) It is also thin since no element of X contains x properly.

For instance, the prefix code $X = \{aa, ab, baa, bab, bb\}$ represented on Figure 2.2. (i) admits $x = baa$ as a synchronizing word as the reader may check by a little reasonning. On the contrary, the code $X = \{aa, ab, ba, bb\}$ of Figure 2.2 (ii) is not synchronizing and the same is true of any code in which all words have the same length not equal to one.

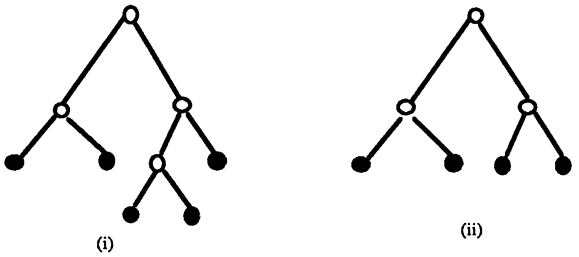


Figure 2.2. (i) A synchronizing prefix code and (ii) a non synchronizing one

We shall see below how to systematically look for synchronizing words.

We also need some terminology from automata theory. Let Q be a set. An *automaton* on Q is given by a function

$$\delta : Q \times A \to Q$$

This function defines a right action of A^* on Q. We denote this action by a dot, writing $q.a$ instead of $\delta(q, a)$.

Given an element $i \in Q$, the *stabilizer* of i is the set

$$Stab(i) = \{x \in A^* \mid i.x = i\}$$

It can be verified that $Stab(i)$ has the form $Stab(i) = X^*$ with X a prefix code, sometimes called the set of *first returns*. Conversely any prefix code can be obtained in this way. One may further assume that all elements q of Q play a role in the sense that there exist u, v in A^* such that $i.u = q$ and $q.v = i$. We say in this case that the automaton is *trim* or *irreducible*.

We define the *rank* $r(w)$ of a word w as the number of elements of Q reachable through w, i.e.

$$r(w) = Card\{q.w \mid q \in Q\}$$

A word $x \in X^*$ is clearly synchronizing iff $r(x) = 1$. In general, the *degree* of X denoted $d(X)$ is the minimal non-zero value of the ranks of the words of A^*. It can proved that it does not depend on the automaton used to obtain X (provided it is trim). Hence X is synchronizing iff $d(X) = 1$.

A finite prefix code can be obtained from a finite automaton. It is synchronizing iff its degree is equal to one. In this case, the automaton itself is also called synchronizing. For example, the prefix code of Figure 2.2 (i) corresponds the first return at node 1 in the automaton given on Figure 2.3.

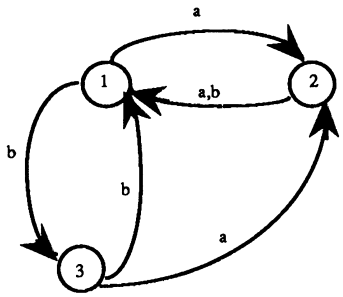


Figure 2.3. A finite automaton

The search for a synchronizing word is easily done with a finite automaton. It reduces to a search in the graph obtained by considering the action of the letters on the subsets of the state set. A synchronizing word is one that is the label of a path from the set of all states to a singleton set. The graph corresponding to the automaton of Figure 2.3 is represented on Figure 2.4 with only part of the edges represented. It allows one to find easily the synchronizing word $x = baa$.

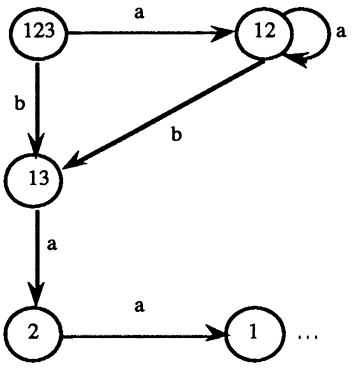


Figure 2.4. The action on subsets(partial drawing)

It is of course not true that, conversely a prefix code obtained from a finite automaton is itself finite, since there may be cycles in the graph of

the automaton that do not use the special state i. One may show however that the code is thin when the automaton is finite (see Berstel, Perrin, 1984).

The *period* of a prefix code X is the gcd of the lengths of its elements. It is known that, *for a maximal prefix code of finite degree, the period is a divisor of the degree* (see Berstel, Perrin, 1984 p. 242). This implies that a prefix code can be synchronizing only when it is of period 1. The study of synchronizing automata or codes deals with the problem of finding additional conditions ensuring that the converse implication holds.

Several other properties relating the degree to other parameters are also known. A useful one is the following : For a finite maximal prefix code X, *the degree is a divisor of each of the integers n such that $a^n \in X$ for $a \in A$* (see Berstel, Perrin, 1984 p. 117).

We will use on several occasions non-commutative polynomials and series. We recall here the basic notions on this subject. A systematic exposition can be found in (Cohn, 1985) or (Berstel, Reutenauer, 1988).

We denote by $\mathbb{Z} << A >>$ the ring of series with coefficents in $\mathbb{Z}$ and non-commutative variables in A and by $\mathbb{Z} < A >$ the corresponding ring of polynomials. For a serie S, we denote by (S, w) the value of S on the word w, also called the coefficient of w in S. We shall write

$$S = \sum_{w \in A^*} (S, w)w$$

The *support* of a series S, denoted $supp(S)$ is the set of words w such that $(S, w) \neq 0$. A serie is a polynomial iff its support is finite.

We shall not distinguish between a subset X of A^* and its characteristic series, writing therefore

$$X = \sum_{x \in X} x$$

We denote by $|P|$ the *degree* of a polynomial P, which is the maximum of the lengths $|w|$ of the elements w in its support. We also denote by $\widehat{P}$ the homogeneous component of P of maximum degree. Therefore

$$(\widehat{P}, w) = \begin{cases} (P, w) & \text{if } |w| = |P| \\ 0 & \text{otherwise} \end{cases}$$

For u in A^* and S in $\mathbb{Z} << A >>$ we denote $u^{-1}S$ the series defined by

$$(u^{-1}S, w) = (S, uw)$$

with the symmetric definition for Su^{-1}.

We shall use several times the fact that the set of homogeneous polynomials is a *free* subsemigroup of $\mathbb{Z} < A >$.

We now show the interplay between codes and polynomials.

Let X be a maximal prefix code on A and let P be the set of its proper prefixes including the empty prefix. We have the equality

$$X - 1 = P(A - 1) \tag{2.5}$$

in which 1 denotes the empty word.

Formula (2.5) expresses a factorisation property. It is easy to derive from the equality between sets

$$PA + 1 = X + P$$

expressing the fact that a prefix followed by a letter is either still a prefix or is a word of X.

A much deeper factorisation property was given by Reutenauer(1985). We state it below in its simplified version concerning prefix codes although his result is more general and holds for general codes.

THEOREM 2.1 (REUTENAUER). — *Let X be a finite maximal prefix code on the alphabet A. There exists two polynomials $L, D \in \mathbb{Z} < A >$ such that*

$$X - 1 = L(d + (A - 1)D)(A - 1) \tag{2.6}$$

where d denotes the degree of X.

A proof of the result is presented in the book of (Berstel, Reutenauer, 1988). It is important to see that when X is not synchronizing, i.e. when $d > 1$, the central factor in the right handside of (2.6) is non trivial. In fact, assuming that the constant term of L is 1, the constant term of D must be $d - 1$, which implies $D \neq 0$.

Also comparing (2.5) and (2.6), we obtain the equality

$$P = L(d + (A - 1)D) \tag{2.7}$$

which expresses a factorisation of the polynomial of prefixes of X.

Equality (2.6) can be rewritten

$$X - 1 = L(A - 1)(d + D(A - 1)) \tag{2.8}$$

By inverting both sides and using the identity $X^* = (1 - X)^{-1}$ we obtain

$$A^* = (d + D(A - 1))X^*L \tag{2.9}$$

We conjecture that for any finite maximal prefix code X of degree d there exist a finite collection of d disjoint maximal prefix codes $T_i (1 \leq i \leq d)$ and a set L such that

$$A^* = (\sum_{i=1}^{d} T_i)X^*L \tag{2.10}$$

Such an equality implies the existence of a factorization like (2.9) since, letting $T_i - 1 = U_i(A - 1)$ we have

$$A^* = (d + (\Sigma U_i)(A - 1))X^*L \tag{2.11}$$

It implies the stronger property that the polynomials L, D in (2.6) can be chosen to have positive coefficients. It also implies that the degree of X is at least equal to d according to the following observation.

PROPOSITION 2.3.. — *Let X be a finite maximal prefix code on the alphabet A such that*

$$X - 1 = L(A - 1)R \tag{2.12}$$

with L, R two subsets of A^*. If R the disjoint union of d maximal prefix codes, then X is of degree at least equal to d.

Proof : We first show that each element of R is a suffix of an element of X. Let indeed r be in R an let $l \in L$ be chosen of length $|L|$. Then, for any letter a in A, lar has coefficient at least one in $X + LR$. Since l is of maximal length, this implies that either r is a suffix of X or it is a suffix of some other element of R. This proves the property by ascending induction on $|r|$.

We now consider an automaton on Q such that X is the set of first returns to a state i. We will show that any word in A^* has at least d states in its range. Let $w \in A^*$ be longer than $|X|$. Then w has d prefixes $t_1, \ldots, t_d$ in R. Since each t_k is a suffix of an element of X, there is a state q_k such that $q_k.t_k = i$.

For each $k = 1, \ldots, d$, let r_k be the state defined by

$$r_k = q_k.w$$

We will verify that all r_k are distinct and this will prove the claim. Let indeed k, ℓ be such that $r_k = r_\ell$. Since we may concatenate w on the right by any word we may suppose that $r_k = r_\ell = i$. Let $w = t_k x_k = t_\ell x_\ell$. Then x_k, x_ℓ are in X^* since they stabilize i. But then the word w has two distinct factorizations in the product RX^*L namely (t_k, x_k, ε) and $(t_\ell, x_\ell, \varepsilon)$, (see Figure 2.5). This is a contradiction since (2.12) is equivalent to the equation

$$A^* = RX^*L$$

□

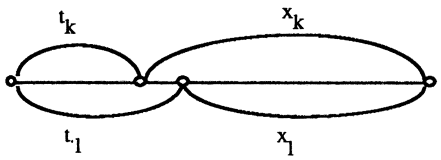


Figure 2.5. Two parsings of w

It is known that a factorization like Eq. (2.10) holds for biprefix codes with $L = 1$ (see Berstel, Perrin, 1985). In the general case, the answer is not known. It is a particular case of a more general conjecture on codes known as the factorization conjecture (ibid. p. 423).

3. LENGTH DISTRIBUTIONS

For a subset X of A^*, the sequence of numbers $\alpha = (\alpha_n)_{n \geq 0}$ given by

$$\alpha_n = Card(X \cap A^n)$$

is called the *length distribution* of X. We also denote

$$f_X(t) = \sum_{n \geq 0} \alpha_n t^n$$

the corresponding generating series. We denote by ρ_X or ρ_α the radius of convergence of the series $f_X(t)$. Let $q = Card(A)$. Since $\alpha_n \leq q^n$, we have $\rho_X \geq 1/q$.

When X is thin, we have $\rho_X > 1/q$ (see Eilenberg, 1974 p. 230 or Berstel, Perrin 1985 p. 67).

A sequence $(\alpha_n)_{n\geq 0}$ is the length distribution of a prefix code on a q-letter alphabet iff it satisfies the inequality

$$\sum_{n\geq 1} \alpha_n q^{-n} \leq 1 \tag{3.1}$$

Inequality (3.1) goes back to C. Shannon and it is at times referred to as *Kraft Inequality*. When X is a thin maximal prefix code, we have

$$\sum_{n\geq 1} \alpha_n q^{-n} = 1 \tag{3.2}$$

Indeed, by Equality (2.5) we have

$$f_X - 1 = f_P(qt - 1) \tag{3.3}$$

Since X is thin, P is thin and therefore $\rho_P > 1/q$. Evaluating both sides of (3.3) at $t = 1/q$ gives the desired equality. Conversely, we have the following

THEOREM 3.1 (SCHÜTZENBERGER, 1967). — *If α is a sequence satisfying Equality (3.2) and $\rho_\alpha > 1/q$, it is the enumerating sequence of some thin maximal prefix code. Moreover, the code can also be chosen synchronizing provided the sequence $(\alpha_n)_{n\geq 0}$ satisfies the additional requirement that the integers α_n are relatively prime.*

We shall reproduce here the part of the proof of this result needed for the purpose of a discussion presented in Section 6.

It is not difficult to see that the first part is true. Indeed, if $\rho_\alpha > 1/q$, we may build a prefix code X with length distribution α such that some word w does not appear within any word of X. Then X is thin and maximal. We may always choose $w = a^k$ for some letter a in A. Then X satisfies the following inclusion

$$A^*w \subset X^*a^*$$

and to choose X synchronizing, we only need a word $x \in X^*$ such that

$$a^*x \subset X^*$$

One may show that except for a trivial case where the sequence α_n is ultimately equal to one, we may rearrange the words of X in a length-preserving way so that for some $b \in A$ and some integer $n \geq 0$ the prefix code $Y = X \cap (a^* \cup a^*ba^*)$ satisfies

$$Y = a^n \cup \{y_0, y_1, \cdots, y_{n-1}\} \tag{3.6}$$

where each $y_i = a^i b a^{\lambda_i - i - 1}$ is a word of length λ_i satisfying

$$i + 1 \leq \lambda_i \leq n \tag{3.7}$$

and there is an integer t with $1 \leq t \leq n$ such that $\lambda_i = n$ iff $i \geq n - t$ and finally the number λ_i are relatively prime.

The above conditions are satisfied in particular when $\lambda_0 \leq \lambda_1 \leq \cdots \leq \lambda_{n-1}$ and the λ_i are relatively prime.

The following lemma therefore completes the proof of Theorem 3.1.

LEMMA 3.2. — *If Y satisfies the above conditions, there exists a word y in Y^* such that $a^*y \subset Y^*$*

Proof : We denote $Q = \{0, 1, \cdots, n-1\}$ and we define an action on Q by

$$i.a = (i + 1) \mod n$$
$$i.b = (i - \lambda_i + 1) \mod n$$

The corresponding automaton is such that $Y^* = Stab(0)$. Let M be the transition monoid of the automaton, which is the monoid of all mappings from Q into Q obtained by the action of all words. For each d with $1 \leq d \leq n$, let

$$I_d = \{n - d, \cdots, n - 2, n - 1\}$$

and let M_d be the monoid

$M_d = \{m \in M \mid Q.m = I_d$ and $i.m = i$ for all $i \in I_d\}$.

We want to prove that M_1 is not empty. This implies our conclusion since a word z defining an element of M_1 satisfies

$$a^*(za) \subset Y^*$$

In the sequel we do not distinguish between a word and the element of M that it defines. We first observe that for all $i \in Q$ we have

$$i.ba^{n-1} \geq i$$

with equality iff $i \in I_t$. Thus ba^{n-1} has a power which belongs to M_t. This proves that M_t is not empty. We shall now prove that if M_s with $1 < s \leq t$ is not empty, then some M_r with $1 \leq r < s$ is not empty. For q in Q, we denote $[q]_s$ the integer in $\{1, 2, \cdots, s\}$ congruent to q mod. s. Let m be an element of M_s.

Case 1. There exists a p with $1 \leq p \leq n$ such that $(n-p).m \neq n - [p]_s$. We choose the smallest p satisfying this inequality. Then $p > s$ by the definition of M_s. Let

$$m' = ma^{n+s-p}m$$
$$J_s = I_s - (n - [p]_s)$$

Since $Q.m = I_s.m$, we have $Q.m' = I_s.m'$. For all s' with $1 \leq s' < s$ we have

$$\begin{aligned}(n-s').m' &= (n-s').a^{n+s-p}m \\ &= (n + (s-s') - p).m \\ &= n - [p + s']_s\end{aligned}$$

and

$$\begin{aligned}(n-s).m' &= (n-s).a^{n+s-p}m \\ &= (n-p).m \\ &\neq n - [p]_s\end{aligned}$$

Hence $Q.m' = J_s$. If $[p]_s = 1$, the element $m_1 = m'a$ belongs to M_{s-1}. Otherwise, let $[p]_s = k > 1$, and let

$$m_2 = m'(a^{n-1}m)^{s-k}$$

We have, for $1 \leq s' < s$,

$$(n-s').m' = n - [k + s']_s$$

and for $1 \leq s' \leq s$

$$(n-s').(a^{n-1}m) = (n-s'-1).m = n - s' - 1$$

whence

$$(n-s').(a^{n-1}m)^{s-k} = n - s' - k$$

and finally

$$(n - s').m_2 = n - s' .$$

Hence m_2 belongs to M_{s-1} whence the desired conclusion in this case also.

Case 2. For all p with $1 \leq p \leq n$ we have $(n-p).m = n - [p]_s$. We first suppose that s does not divide n. Let then $n = n's + d$ with $1 \leq d \leq s$. For all d' with $1 \leq d' \leq d$ we have

$$\begin{aligned}(n - d').a^d m &= (d - d').m \\ &= n - d'\end{aligned}$$

Hence $a^d m$ fixes pointwise the set I_d. Also for $d < d' \leq s$ we have

$$\begin{aligned}(n - d').a^d m &= (n + d - d').m \\ &= n + d - d'\end{aligned}$$

Hence some power of $a^d m$ belongs to M_d.

We are finally left with the case where s divides n. It is easy to see that this implies that $p.m \equiv p$ mod.s for all $p \in I$ and $m \in M$. Since the λ_i are relatively prime, this implies $s = 1$, a contradiction. □

An additional problem concerning length distributions is the following. When a prefix code X is the stabilizer of a state in a finite automaton, then the series $f_X(t)$ is rational (see Eilenberg, 1974). It is not completely known under which conditions the converse holds, i.e. under which additional assumptions Theorem 3.1 holds with the additional conclusion that the prefix code is a stabilizer in a finite automaton. See (Perrin, 1989) for a partial answer.

4. FLIPPING EQUIVALENCE

We introduce a transformation on prefix codes called *flipping*. It is defined as follows. Let X be a prefix code on the alphabet A. Let $a, b \in A$ be two letters and let u be a proper prefix of X. Let

$$X = X' + uaR + ubS$$

with X', R, S prefix codes. One has in fact $R = (ua)^{-1}X, S = (ub)^{-1}X$.

The prefix code

$$Y = X' + uaS + ubR$$

is said to be the image of X under an *elementary flip*. A flip is a composition of elementary flips. The flipping transformation defines an equivalence called the *flipping equivalence*. We denote

$$X \sim Y$$

two prefix codes X, Y which are flipping equivalent.

The flipping transformation is of course a very natural and simple one on the trees associated with prefix codes. Indeed, an elementary flip is just an exchange of two subtrees rooted at the sons of some vertex.

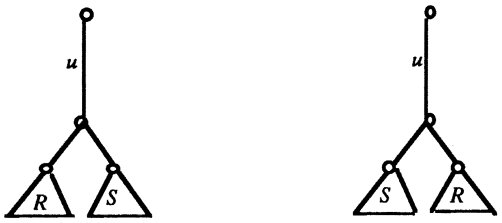


Figure 4.1. An elementary flip

We have represented on Figure 4.2 an equivalence class of the flipping equivalence. Actually two unlabeled complete binary trees correspond to flipping equivalent maximal prefix codes iff they are isomorphic, as one may easily verify.

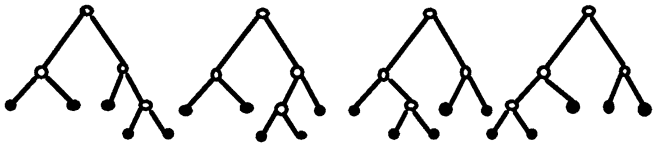


Figure 4.2. A flipping equivalence class

The flipping equivalence preserves some of the properties of prefix codes. First of all, two flipping equivalent pregix codes have the same length distribution (the converse implication is however not true). As a consequence, equivalent prefix codes have the same period. Also, two equivalent prefix codes are simultaneously maximal or not maximal.

We are going to prove the following result. It is, in the case of finite prefix codes, a reinforcement of Theorem 3.1

THEOREM 4.1. — *The flipping equivalence class of any finite maximal prefix code of period 1 contains at least one synchronizing prefix code.*

The proof relies on two lemmas. In the first lemma we start with a Reutenauer's factorization (2.8)

$$X - 1 = L(A-1)(d + (A-1)D)$$

and consider $R = (d+(A-1)D)$. The homogeneous component of highest degree is, when $D \neq 0$

$$\widehat{R} = A\widehat{D}$$

The lemma shows that, except for the periodic case, the homogeneous polynomial $\widehat{R}$ is not equal to A^n. The condition given is the lemma is of course also sufficient.

LEMMA 4.2. — *If X is a finite maximal prefix code of period p such that*

$$X - 1 = L(A-1)R$$

where $\widehat{R} = A^n$ for some $n \geq 1$, then R is a polynomial in A dividing $1 + A + \ldots + A^{p-1}$.

Proof.Let $E = (A-1)R$. We first show that E is a polynomial in A. Let us suppose by induction on $m < n$ that

$$E = E' + \sum_{i=m+1}^{n} s_i A^i \tag{4.1}$$

with $\mid E' \mid \leq m$. Let g be in the support of $\widehat{L}$ and let h be a word of length m. For all words k of length $n-m$ we have $ghk \in supp(\widehat{L}\widehat{E}) \subset supp(X)$ and thus $ghk \in X$. Since X is prefix, we have $(LE, gh) = 0$.

But, by Formula (4.1) we have

$$(LE, gh) = (L, g)(E', h) + \sum_{i=m+1}^{n} r_{t+m-i} s_i \tag{4.2}$$

where r_i is the coefficient in L of the prefix of length i of g and $t = \mid g \mid$. Since $(LE,gh) = 0$, we deduce from (4.2) the Formula

$$(E', h) = -(1/(L, g)) \sum_{i=m+1}^{n} r_{t+m-i} s_i$$

It shows that (E', h) does not depend on the word h but only on its length m and proves that Equality (4.1) is true for $m-1$. Thus we have proved by induction that E is a polynomial in A, i.e.

$$E = \sum_{i=0}^{n} s_i A^i$$

Let x be a word of X of length q. Let r, s be the polynomials in the variable z

$$r(z) = \sum_{i=0}^{q} r_i z^i \quad s(z) = \sum_{i=0}^{n} s_i z^i$$

where r_i is the coefficient in L of the prefix of length i of x. We have for each integer m such that $0 < m < q$ the equality similar to (4.2)

$$\sum_{i+j=m} r_i s_j = 0$$

since, X being prefix, the coefficient of the prefix of length m of x in LE is zero. We therefore have

$$z^q - 1 = r(z)s(z)$$

and the lemma is proved. □

We now prove a second lemma. It shows that, in the non periodic case, we may use the flipping transformation to destroy the possibility of a non trivial factorization of the polynomial $X - 1$. For a finite maximal prefix code X, we denote by $e(X)$ the integer defined by

$$e(X) = \max\{e \geq 0 \mid X - 1 = L(A-1)R, e = \mid R \mid\}$$

Thus, $e(X) > 0$ iff X has a non-trivial factorization. Consequently, $e(X) = 0$ implies that X is synchronizing.

LEMMA 4.3. — *Let X be a finite maximal prefix code such that*

$$X - 1 = L(A-1)R \tag{4.3}$$

with $\mid R \mid = n \geq 1$ and $\widehat{R} \neq A^n$ Then there exists a prefix code X' flipping equivalent to X such that

$$e(X') < e(X)$$

Proof.Let $E = (A - 1)R$. We first note that Eq. (4.3) implies that $\widehat{X} = \widehat{L}A\widehat{R} = \widehat{L}\widehat{E}$. Therefore the homogeneous polynomials $\widehat{L}, \widehat{E}$ are unambiguous, i.e. have 0-1 coefficients. Let $g \in \widehat{L}$ and let Y be the finite maximal prefix code $Y = g^{-1}X$. We have $\widehat{Y} = \widehat{E}$. Since $\widehat{Y} \neq A^{n+1}$, there exists a prefix code Y' flipping equivalent to Y such that $\widehat{Y} \neq \widehat{Y}'$. Let X' be the maximal prefix code defined by the equality

$$X' - gY' = X - gY \tag{4.4}$$

We have $X' \sim Y'$. Consider a non trivial factorization

$$X' - 1 = L'E' \tag{4.5}$$

and suppose by contradiction that $| E | \leq | E' | < | X |$. Since $g\widehat{Y}' \subset \widehat{X}' = \widehat{L}'\widehat{E}'$, the set $\widehat{L}'$ contains a prefix g' of g. Let $g = g'h$ (see Figure 4.3).

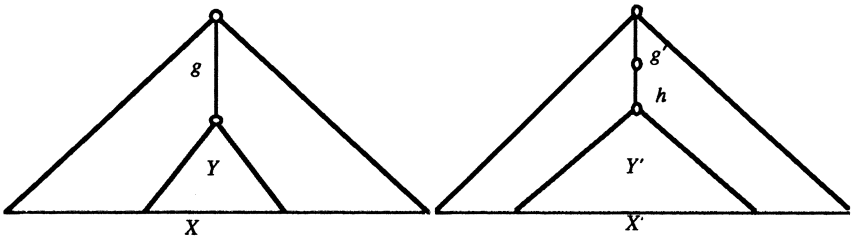


Figure 4.3. The codes X and X'

Let $F = h^{-1}E', H = g'^{-1}L - h$ and let L_1, E_1', L_1' be defined by the following equalities

$$L = L_1 + g'H + g'h$$
$$E' = E_1' + hF$$
$$L' = L_1' + g'$$

Substituting into (4.3) and (4.5), we obtain

$$\widehat{X} = (\widehat{L}_1 + g'\widehat{H} + g'h)\widehat{E} \tag{4.6}$$

$$\widehat{X}' = \widehat{L}'(\widehat{E}_1' + h\widehat{F}) \tag{4.7}$$

By restricting Equality (4.4) on both sides to the words of maximal length beginning with g', we derive

$$\widehat{E}'_1 = \widehat{H}\widehat{E} \tag{4.8}$$

And by restricting (4.4) to the words of maximal length that do not begin by g' we obtain

$$\widehat{L}'_1(\widehat{E}'_1 + h\widehat{F}) = \widehat{L}_1\widehat{E} \tag{4.9}$$

Substituting in (4.9) the value of $\widehat{E}'_1$ given by (4.8) we have

$$\widehat{L}'_1 h\widehat{F} = (\widehat{L}_1 - \widehat{L}'_1\widehat{H})\widehat{E} \tag{4.10}$$

Since $|\ \widehat{F}\ | = |\ \widehat{E}\ |$, we deduce from (4.10) that $\widehat{F} = \widehat{E}$.

This contredicts the hypothesis $\widehat{Y} \neq \widehat{Y}'$ since on one hand $\widehat{Y} = \widehat{E}$ and on the other hand $\widehat{F} = \widehat{Y}'$.□.

We can now complete the proof of Theorem 4.1. We use an induction on the integer $e(X)$. The property is true when $e(X) = 0$ since then X itself is synchronizing. When $e(X) \geq 1$, we have $X - 1 = L(A - 1)R$ with $|\ R\ | = n \geq 1$. If $\widehat{R} = A^n$, then by Lemma 4.2, R divides $1 + A + \ldots + A^{p-1}$ with p the period of X. Hence, $p \geq n + 1 \geq 2$ in contradiction with the hypothesis $p = 1$. Therefore, $\widehat{R} \neq A^n$ and by Lemma 4.3, there exists an X' flipping equivalent to X such that $e(X') < e(X)$ whence the property by induction.

5. COMMUTATIVE EQUIVALENCE

There is another equivalence on prefix codes which is also a refinement of the length distxribution equivalence. This equivalence, called *commutative equivalence* is of more general interest since it applies to all subsets of the free monoid. We first recall its definition.

Two words u, v in A^* are said to be commutatively equivalent if for all a in A the number of occurrences of a in u is equal to the number of occurrences of a in v. We denote this equivalence by the symbol $\equiv$. Two subsets X, Y of A^* are said to be commutatively equivalent if there is a one-to-one mapping f from X onto Y such that for all x in X, one has $f(x) \equiv x$. We again denote $X \equiv Y$. Figure 5.1 represents two commutatively

equivalent maximal prefix codes. Actually their equivalence class does not contain other prefix codes (compare with Figure 4.2)

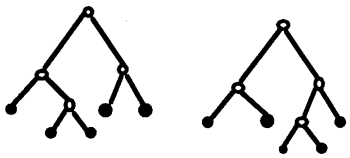


Figure 5.1. Two commutatively equivalent prefix codes

We will basically use the same arguments as in the preceding section to prove the following result.

THEOREM 5.1. — *The commutative equivalence class of any finite maximal prefix code of period 1 contains at least one synchronizing prefix code.*

The proof goes along the same lines as the proof of Theorem 4.1. We choose X such that the integer $e(X)$ is minimal in its commutative equivalence class. Suppose, by contradiction, that X is not synchronizing. Then we have

$$X - 1 = L(A - 1)(d + D(A - 1))$$

with $\mid D \mid \geq 2$. By Lemma 4.2 we have $\widehat{D} \neq A^n$ since otherwise X would be of period $p \geq 2$. Consequently, there exists a word h such that for some pair of letters a, b in A we have

$$(ha)^{-1}\widehat{D} \neq (hb)^{-1}\widehat{D}$$

Let $U = (ha)^{-1}\widehat{D}, V = (hb)^{-1}\widehat{D}$. Let $g \in \widehat{G}$ and $Y = g^{-1}X$. We have $\widehat{Y} = A\widehat{D}$ and therefore

$$Y = W + ahbU + bhaV$$

Let

$$Y' = W + ahbV + bhaU$$

Since $ahb \equiv bha$, we have $Y \equiv Y'$. Let X' be the prefix code commutatively equivalent to X defined by

$$X' - gY' = X - gY$$

Then, one may use the same proof as in Lemma 4.3 to show that $e(X') < e(X)$, a contradiction. This proves Theorem 5.1

To close this section, we mention the fact that the commutative equivalence is the object of an important open problem about codes. It is indeed conjectured that any finite maximal code is commutatively equivalent to a prefix code (see Berstel, Perrin, 1985).

6. THE ROAD COLORING PROBLEM

We finally discuss the road coloring problem mentioned in the introduction and we relate it to the results of the previous sections.

Let $\mathcal{A}$ be a finite automaton given by a function

$$\delta : Q \times A \to Q$$

The underlying graph of $\mathcal{A}$ is the directed graph having Q as set of vertices and an edge (p, q) iff there is an $a \in A$ such that $\delta(p, a) = q$. It is therefore the graph obtained from the familiar diagram associated with the automaton after removing the labels of the edges. It has the property that all its vertices have the same outdegree, in fact equal to the number of symbols in A.

A graph is said to be *road colorable* if it is the underlying graph of some synchronizing automaton.

Recall that a graph is called aperiodic if there is an integer n such that the n-th power of its adjacency matrix has all its elements strictly positive. This is of course equivalent to the graph being strongly connected and the g.c.d of the cycle lengths being equal to one.

The conjecture formulated in (Adler, Goodwin, Weiss, 1977) is the following : *any aperiodic graph with all vertices of the same outdegree is road colorable.*

We reformulate Theorem 4.1 as follows to obtain a solution of this conjecture in a particular case.

THEOREM 6.1. — *Any aperiodic graph such that*
(*i*) *all vertices have the same outdegree*
(*ii*) *all vertices except one have indegree one*
is road colorable.

Proof. We define the *renewal automaton* of a finite maximal prefix code X to be the automaton having the set P of prefixes of X as set of states and

the transition function defined by $\delta(p,a) = pa$ if $pa \in P$ and $\delta(p,a) = 1$ otherwise. The graph underlying the renewal automaton of X is therefore obtained from the unlabeled tree associated with X by merging all leaves with the root. Clearly, an elementary flip does not affect this graph.Hence, when X and X' are flipping equivalent, the underlying graphs of their renewal automata are the same and the result follows from Theorem 4.1.□

The road coloring conjecture is known to be true in some other particular cases. One of them (O'Brien, 1981) is that of graphs satisfying the additional assumptions

(i) there are no multiple edges

(ii) there is a simple cycle of prime length.

Another case, proved by Friedman (1990) is that of graphs containing a simple cycle of length prime to the weight of the graph. The weight of a graph is defined to be the sum of the components of an integer Perron left eigenvector chosen with its components relatively prime.

Some further particular cases have been investigated by A. Mahieux (1986).

In the paper of (Adler et al., 1977) the following result is proved : let G be an aperiodic graph with constant outdegree. Let M be the adjacency matrix of G and let n be an integer such that M^n has all its coefficients positive. For $k > 0$, let $G^{(k)}$ denote the graph having as vertices the paths of length h in G and edges the pairs (s,t) with $s = (s_1,\ldots,s_k), t = (s_2,\ldots,s_k,s_{k+1})$. Then $G^{(2n)}$ is road colorable. In terms of symbolic dynamics, this means that the system of finite type associated with G is conjugate to one that is road colorable. This result can actually also be proved using the construction of (Schützenberger, 1967) reproduced in Theorem 3.1. Indeed a splitting of the states of the graph will allow to label the cycles in such a way as to obtain a set of first returns containing the words described by Equations (3.3.6-7)

REFERENCES

[1] Adler R.L., Goodwin L.W., Weiss, B.,1977, Equivalence of topological Markov shifts,*Israel J. Math.* t.**27**, p. 49-63.

[2] Adler R.L., Marcus, B., 1979, Topological entropy and equivalence of dynamical systems, *Memoirs AMS*, **219**.

[3] Aho A., Dahbura, A., Lee, D., Uyar, M., 1988, An optimization technique for protocol conformance test generation based on UIO sequences and rural chinese postman tours, in *Protocol Specification, Testing and Verification VIII*, S. Aggarwal and K. Sabnani eds., North Holland.

[4] Berstel J., Perrin D., 1985,*Theory of Codes*, Academic Press.

[5] Berstel J., Reuteneauer, C., 1988, *Rational Series and their Languages*, Springer.

[6] Carpi, A., 1988, On synchronizing unambiguous automata, *Theoret. Comput. Sci.*,**60**, p.285-296.

[7] Cohn, P.M., 1985, *Free Rings and their Relations*, Academic Press (2nd edition).

[8] Eilenberg, S., 1974, *Automata, Languages and Machines*, Vol. A, Academic Press.

[9] Eppstein, D., 1990, Reset sequences for monotonic automata, *SIAM J. Comput.*, **19**, p. 500-510.

[10] Friedman, J., 1990, On the road coloring problem, *Proc. Amer. Math. Soc.* **110**, 1133-35.

[11] Mahieux, A., 1986, unpublished manuscript.

[12] O'Brien, G.L., 1981, The road coloring problem, *Israel J. Math*, t. **39**, p. 145-154.

[13] Perrin, D., 1989, Arbres et séries rationnelles, *C.R. Acad. Sci. Paris*, **309**, 713-716.

[14] Reutenauer, C.,1985, Noncommutative factorisation of variable-length codes *J. Pure applied Algebra* t.*36*, p.167-186.

[15] Schützenberger, M.P.,1967, On synchronizing prefix codes, *Information and Control*, t. **11**, p.396-401.

Discrete Mathematics 99 (1992) 165–179
North-Holland

Décompositions dans l'algèbre des différences divisées

Alain Lascoux et Marcel-Paul Schützenberger
L.I.T.P., Université Paris 7, 2 Place Jussieu 75251, Paris Cedex 05, France

Received 6 July 1989
Revised 26 June 1990

Abstract

Lascoux, A. et M.-P. Schützenberger, Décompositions dans l'algèbre des différences divisées, Discrete Mathematics 99 (1992) 165–179.

The group algebra of the symmetric group on the ring of rational functions has, apart from its canonical basis of permutations, several bases of *symmetrizing operators*, among which the classical Newton's *divided differences*. We deal here with the explicitation of the matrices of change of bases. Our main result is that, in the case of Gl(n), the components of the matrices associated to the classical bases are just specializations of *Schubert* or *Grothendieck polynomials*. We refer to the work of Arabia, Bernstein–Gelfand–Gelfand, Kac, Kostant, Kumar, Rossmann for the interpretation of these matrices in terms of (equivariant) cohomology and K-theory rings of the flag manifold, or equivariant singularities of Schubert varieties. Our main technical tool is the simple observation that all but one specialization of the maximal twofold Schubert polynomial $\mathscr{X}$ vanish.

1. Introduction

L'algèbre du groupe symétrique $\mathfrak{G}(A)$ d'un ensemble d'indéterminées A est étudiée depuis Frobenius et Young. De nouvelles propriétés apparaissent lorque l'on prend le produit tensoriel *tordu* ([6, III.180, ex.11] dit *produit croisé*; [13, 19] emploient le terme *smash product*) avec le corps des fractions rationnelles $\mathscr{R}$(A) de l'algèbre symétrique associée à A, les coefficients dans le corps des fonctions rationnelles en les variables sur lesquelles agit le groupe, au lieu de coefficients dans le corps des complexes. Cette algèbre, que nous notons $\mathscr{E}$ admet d'autres bases que la base canonique des permutations, en particulier les différences divisées de Newton; c'est pourquoi nous l'appelons 'Algèbre des différences divisées'.

Un point de vue alternatif consiste en la caractérisation des opérateurs sur l'anneau des polynômes, vérifiant les relations de Coxeter: on retrouve, après tensorisation par $\mathscr{R}(A)$, l'algèbre $\mathscr{E}$, cf. [23], cette fois-ci comme réalisation concrète de l'algèbre de Hecke du groupe symétrique.

La géométrie fournit différentes interprétations de l'algèbre $\mathscr{E}$ comme algèbre d'opérateurs sur l'anneau de cohomologie, de Grothendieck, la cohomologie équivariante ou la K-théorie équivariante de la variété de drapeaux. Suivant l'interprétation choisie, il faudra identifier $\alpha, e^{\alpha}, \ldots$ au quotient de deux variables consécutives: $a_1/a_2, \ldots,$ et les opérateurs de $\mathscr{E}$ aux opérateurs naturels pour ces différentes théories cohomologiques. L'avantage présent de la combinatoire est que l'on mène simultanément les calculs dans les différentes théories, et même, que l'on obtient par exemple, des relations explicites entre les polynômes qui relèvent les cycles de Schubert et ceux qui relèvent les caractères de Demazure [25] quoique ces objets appartiennent de fait à des catégories différentes. Plus encore, on peut étendre les constructions à *l'algèbre libre* [24] et retrouver ainsi *tableaux de Young, bases standard,* etc. en liaison avec l'algèbre $\mathscr{E}$.

Un des problèmes intéressants de la théorie consiste en l'explicitation des différentes matrices de changement de base.

Nous montrons ici que les principales de ces matrices, considérées en particulier par [2–3, 13–14, 16, 27] sont données par les polynômes de Schubert et ceux de Grothendieck (Proposition 3.2, formules 3.8, 3.9, 4.6, 4.7, 4.11).

Rappelons que les polynômes de Schubert interviennent par ailleurs:

- comme base de l'anneau des polynômes en tant que module libre sur l'anneau des polynômes symétriques [19] (résultat implicite dans [5], décrit dans un autre contexte par [1, p. 42]).
- comme base de la cohomologie des variétés de drapeaux associées aux groupes linéaires [5, 7, 19].
- comme coefficients dans la formule d'interpolation de Newton à plusieurs variables [22].
- comme caractères irréductibles [15].
- comme généralisation des fonctions de Schur dans la troisième édition du livre de [26].

Attention: Les opérateurs agissent sur tout ce qu'ils trouvent sur leur gauche.

2. Différences divisées

Soient $A = \{a_1, \ldots, a_{n+1}\}$ un ensemble totalement ordonné d'indéterminées (un *alphabet*) et $\mathscr{R}(A)$ l'anneau des fonctions rationnelles en A. On note $\mathfrak{S}(A)$ le groupe symétrique sur A, ω son élément maximal. Pour tout $f \in \mathscr{R}(A)$, f^{μ} est l'image de f par la permutation μ.

Soit $\mathscr{E}$ l'algèbre des opérateurs D sur $\mathscr{R}(A)$, du type $D = \sum_{\zeta \in S(A)} \zeta R_{\zeta}(D)$, où les coefficients $R_{\zeta}(D)$ appartiennent à $\mathscr{R}(A)$. L'anneau $\mathscr{R}(A)$ s'injecte canoniquement dans $\mathscr{E}$:

$$\mathscr{R}(A) \ni f \rightarrow \text{`}\textit{opérateur multiplication par } f\text{'}.$$

Pour éviter les exposants trop volumineux, nous noterons aussi $f\mu \in \mathcal{R}(A)$ la fonction f^{μ}, ou dirons 'la fonction $f\mu$' ou 'le polynôme $f\mu$' lorsque nous voudrons distinguer ces derniers de l'opérateur composé de 'multiplication par f' par 'permutation μ'.

L'algèbre $\mathcal{E}$ est un $\mathcal{R}(A)$-module à gauche, aussi bien qu'à droite, les deux structures s'échangeant par l'égalité

$$\text{Pour tout couple } (f, \mu): f \in \mathcal{R}(A),\ \mu \in \mathfrak{G}(A), \quad \mu f = f^{\mu^{-1}}\mu.$$

Le produit dans $\mathcal{E}$ est donné par

$$\sum_{\zeta} \zeta R_{\zeta}(D) \cdot \sum_{\nu} \nu R_{\nu}(D') = \sum_{\zeta,\nu} \zeta\nu (R_{\zeta}(D))^{\nu} R_{\nu}(D') \tag{2.1}$$

On a dans $\mathcal{E}$ des opérateurs, indexés par les éléments de $\mathfrak{G}(A)$, remis à l'honneur par l'étude des variétés de drapeaux: les *différences divisées* ∂_{μ} dues à Newton, les *symétriseurs convexes* π_{μ}, les *symétriseurs concaves* ψ_{μ}.

La définition de ces opérateurs est, dans le cas où μ est la transposition simple σ_i échangeant a_i et a_{i+1}, en employant alors la notation ∂_i, π_i, ψ_i:

$$\begin{aligned}
\partial_i &= \frac{1}{(a_i - a_{i+1})}(1 + \sigma_i), \\
\pi_i &= \frac{1}{(1 - a_{i+1}/a_i)}(1 + \sigma_i) = a_i\partial_i, \\
\psi_i &= (\sigma_i - 1)\frac{1}{(1 - a_i/a_{i+1})} = \partial_i a_{i+1} = \pi_i - 1.
\end{aligned} \tag{2.2}$$

Il faut compléter (2.2) par les valeurs en $\mu = \textit{identité}$ qui sont respectivement $\partial_{\mathrm{id}} = 1$, $\pi_{\mathrm{id}} = 1$, $\psi_{\mathrm{id}} = 0$.

Chaque famille d'opérateurs $\{\sigma_i\}$, $\{\partial_i\}$, $\{\pi_i\}$, $\{\psi_i\}$ vérifie séparément les relations de Moore/Coxeter (en écrivant $\{D_i\}$ pour l'une quelconque de ces familles):

$$D_iD_j = D_jD_i \textit{ si } |i - j| \geqslant 2, \tag{2.3}$$

$$D_iD_{i+1}D_i = D_{i+1}D_iD_{i+1}. \tag{2.4}$$

Les relations (2.3) et (2.4) impliquent que les ∂_{μ}, π_{μ}, ψ_{μ} peuvent s'écrire comme le produit d'opérateurs *élémentaires* ∂_i, π_i, ψ_i correspondant à une décomposition réduite arbitraire de μ (i.e., écriture de μ comme un produit de longueur minimale de transpositions simples).

On peut remarquer que

$$\begin{aligned}
\partial_i\partial_i &= 0, \\
\pi_i\pi_i &= \pi_i, \\
\psi_i\psi_i &= -\psi_i.
\end{aligned} \tag{2.5}$$

Dans [23] (voir aussi [10]), on donne des opérateurs plus généraux satisfaisant, en plus des relations de Coxeter, la relation de Hecke

$$D_iD_i = qD_i + r. \tag{2.6}$$

Les opérateurs correspondant à la permutation maximale ω de $\mathfrak{G}(A)$, ont une expression globale, outre leurs différentes expressions comme produits d'opérateurs élémentaires [21]:

$$\partial_\omega = \frac{1}{\Delta} \sum_{\mu \in \mathfrak{G}(A)} \mu, \tag{2.7}$$

$$\pi_\omega = \frac{\rho}{\Delta} \sum_{\mu \in \mathfrak{G}(A)} \mu, \tag{2.8}$$

$$\psi_\omega = \frac{1}{\Delta} \sum_{\mu \in \mathfrak{G}(A)} \mu\rho^\omega, \tag{2.9}$$

où Δ le *Vandermonde*: $\Delta = \prod_{i<j}(a_i - a_j)$ et ρ le monôme $a_1^n a_2^{n-1} \cdots a_{n+1}^0$ (qui correspond à la demi-somme des racines positives), de sorte que $\rho^\omega = a_1^0 a_2^1 \cdots a_{n+1}^n$.

En d'autres termes, pour toute fonction $f \in \mathcal{R}(A)$, son image $f\partial_\omega$ par ∂_ω est la somme des transformées de f/Δ par toutes les permutations $\mu \in \mathfrak{G}(A)$, $f\psi_\omega$ s'obtient en multipliant $f\partial_\omega$ par ρ^ω tandis que $f\pi_\omega$ est la somme des transformées de $f\rho/\Delta$ par les $\mu \in \mathfrak{G}(A)$.

On simplifie beaucoup les calculs dans $\mathscr{E}$ en faisant agir les éléments de $\mathscr{E}$ sur un élément approprié de $\mathcal{R}(A)$ plutôt que d'utiliser les relations (2.3)–(2.5). Pour cela, on introduit un deuxième alphabet $Y = \{y_1, \ldots, y_{n+1}\}$ de même cardinal que A, les éléments de Y étant supposés invariants par les éléments de $\mathscr{E}$ et $\mathcal{R}(A)$ désignant dorénavant les fonctions rationnelles en A à coefficients les fonctions rationnelles en Y. Soit de plus θ la spécialisation $Y \to A$, i.e., $y_1 \to a_1, \ldots, y_{n+1} \to a_{n+1}$.

Dans le cas des différences divisées, on part du polynôme

$$\mathscr{X} = \prod_{i+j \leqslant n+1} (a_i - y_j),$$

dont la faculté essentielle, qui montre que $\mathscr{X}$ est la 'polarisation' du Vandermonde, est la propriété d'annulation suivante (provenant directement de ce qu'un des facteurs au moins du polynôme $\mathscr{X}^\mu\theta$ s'annule, sauf lorsque $\mu = \omega$).

Lemma 2.10. *Les opérateurs $\mathscr{X}\mu\theta$ sont tous nuls, sauf $\mathscr{X}\omega\theta = \Delta\omega$.*

Le lemme permet de décomposer tout élément de $\mathscr{E}$ dans la base canonique $\{\zeta\}$, ainsi que nous l'avons indiqué dans [23].

Corollaire 2.11. *Soit* $D = \sum \zeta R_\zeta(D)$ *un élément de* $\mathscr{E}$. *Alors*

$$R_\zeta(D) = \mathscr{X}\omega\zeta^{-1}D\theta/\Delta^\omega = \mathscr{X}\frac{1}{\Delta}\omega\zeta^{-1}D\theta \in \mathscr{R}(A).$$

Preuve. L'image par θ de la somme $\sum_\nu \mathscr{X}\omega\zeta^{-1}\nu R_\nu(D)$ se réduit à un seul terme d'après le Lemme 2.10. □

En d'autres termes, le coefficient $R_\zeta(D)$ s'obtient comme image du polynôme $\mathscr{X}$ par la suite d'opérations: multiplication par $1/\Delta$, permutation par $\omega\zeta^{-1}$, application de D et spécialisation θ. On pourrait donner les formules similaires en échangeant structure droite et structure gauche de $\mathscr{E}$ en tant que $\mathscr{R}(A)$-module libre.

Les coefficients $R_\zeta(D)$ sont compatibles avec la composition par les éléments de $\mathscr{E}$, ainsi que le montre le lemme suivant dont la preuve est la même que celle du Corollaire 2.11.

Lemme 2.12. *Soient* $P \in \mathscr{R}(A)$, $\eta \in \mathfrak{G}(A)$. *Alors, pour toute permutation* ζ, *pour tout élément* D *de* $\mathscr{E}$, *on a*

$$R_\zeta(\eta PD) = P\eta^{-1}\zeta R_{\eta^{-1}\zeta}(D).$$

3. Polynômes de Schubert

Les images de $\mathscr{X}$ par les différences divisées ∂_μ sont par définition les *Polynômes de Schubert* (doubles). Plus précisément [17]:

Définition 3.1. Le polynôme de Schubert X_μ d'indice $\mu \in \mathfrak{G}(A)$ est égal à $\mathscr{X}\partial_{\omega\mu}$.

L'indexation est choisie de sorte que $X_\omega = \mathscr{X}$; cet élément doit s'interpréter, en cohomologie, comme la classe de la diagonale pour le plongement diagonal de la variété de drapeaux. L'élément $X_{\omega\omega}$ est quant à lui égal à 1 ($\omega\omega$ = identité). La base des *cycles de Schubert* s'obtient par spécialisation des X_μ en $y_1 = \cdots = y_{n+1} = 0$; comme les éléments de Y sont des scalaires pour les différences divisées, les cycles de Schubert sont donc les images par les différences divisées de la spécialisation de X_ω, i.e., du monôme ρ [21].

Par exemple, pour $A = \{a, b, c, d\}$ et $Y = \{x, y, z, \check{z}\}$ de cardinal 4, on a, en écrivant en indice *ijhk* plutôt que $a_i a_j a_j a_k$:

$$\mathscr{X} = X_{4321} = (a-x)(a-y)(a-z)(b-x)(b-y)(c-x).$$
$$X_{3421} = X/(a-z); \quad X_{4321} = X/(b-y); \quad X_{4312} = X/(c-x).$$
$$X_{2431} = (a-x)(b-x)(c-x)(a+b-y-z); \quad X_{3241} = X/(a-z)(b-y);$$
$$X_{3412} = X/(a-z)(c-x); \quad X_{4132} = (a-x)(a-y)(a-z)(b+c-x-y);$$

$$X_{4213} = X/(b-y)(c-x).$$
$$X_{2341} = (a-x)(b-x)(c-x);$$
$$X_{1432} = a^2b + a^2c + ab^2 + abc + b^2c - (a^2+ab+b^2)(x+y) - (ab+ac+bc)(x+y+z) + (a+b)(x^2+xy+y^2) + (a+b+c)(xy+xz+yz) - (x^2y+x^2z+xy^2+xyz+y^2z);$$
$$X_{2413} = (a-x)(b-x)(a+b-y-z);$$
$$X_{3142} = (a-x)(a-y)(b+c-x-y);$$
$$X_{3214} = (a-x)(a-y)(b-x); \quad X_{4123} = (a-x)(a-y)(a-z).$$
$$X_{1342} = ab+ac+bc-(x+y)(a+b+c)+x^2+xy+y^2;$$
$$X_{1423} = a^2+ab+b^2-(a+b)(x+y+z)+xy+xz+yz;$$
$$X_{2143} = (a-x)(a+b+c-x-y-z); \quad X_{2314} = (a-x)(b-x);$$
$$X_{3124} = (a-x)(a-y).$$
$$X_{1243} = a+b+c-x-y-z; \quad X_{1324} = a+b-x-y;$$
$$X_{2134} = a-x.$$
$$X_{1234} = 1.$$

Les polynômes de Schubert sont invariants par le plongement

$$\mathfrak{G}(\{a_1, \ldots, a_n\}) \to \mathfrak{G}(\{a_1 \cdots a_{n+1}\})$$

(adjonction du point fixe a_{n+1}); ainsi, les polynômes pour $\mathfrak{G}(\{a, b, c\})$ correspondent-ils, dans la table précédente, aux permutations μ telles que $d\mu = d$.

Le Corollaire 2.11 donne la décomposition des différences divisées dans la base canonique $\{\zeta\}$ en fonction des polynômes $X\nu\partial_\mu\theta$. Combinant avec Lemme 2.12, on obtient cette décomposition en fonction des spécialisations des polynômes de Schubert.

Proposition 3.2. *Pour tout couple de permutations μ, ζ, les coefficients $R_\zeta(\partial_\mu)$ sont égaux à $(X/\Delta)\omega\zeta^{-1}\partial_\mu\theta = X_{\omega\mu}\zeta^{-1}\omega\theta\zeta/\Delta^\zeta$, c'est-à-dire l'on a*

$$\partial_\mu = \sum_\zeta \zeta(X_{\omega\mu}\zeta^{-1}\omega\theta\omega\zeta/\Delta^\zeta).$$

Par exemple, le polynôme de Schubert $X_{1423} = X_{4321}\partial_3\partial_2\partial_1\partial_3 = a^2+ab+b^2-(a+b)(x+y+z)+xy+xz+yz$ a comme seules spécialisations non nulles tous les

$$X_{1423}\nu^{-1}\omega\theta\omega\nu = (a-c)(a-d) \quad \text{et} \quad X_{1423}\sigma_1\nu^{-1}\omega\theta\omega\nu\sigma_1 = (b-c)(b-d),$$

où ν parcourt $\mathfrak{G}(a) \times \mathfrak{G}(\{b, c, d\})$, i.e., où ν est telle que $a\nu = a$. La Proposition 3.2 entraîne donc le développement

$$\partial_3\partial_2\partial_1\partial_3(1-\sigma_2-\sigma_3+\sigma_2\sigma_3+\sigma_3\sigma_2-\sigma_2\sigma_3\sigma_2)\left(\frac{(a-c)(a-d)}{\Delta} - \sigma_1\frac{(b-c)(b-d)}{\Delta}\right).$$

On prendra garde que les polynômes $X\omega\zeta^{-1}\partial_\mu$ et $X_{\omega\mu}\zeta^{-1}\omega$ sont différents, quoique leurs images par θ coïncident à permutation près d'après la Proposition 3.2.

Pour le groupe symétrique $\mathfrak{G}(a, b, c)$, la matrice de changement de base est:

$$1\Delta = (a-b)(a-c)(b-c),$$
$$\partial_1\Delta = (1-\sigma_1)(a-c)(b-c),$$
$$\partial_2\Delta = (1-\sigma_2)(a-b)(a-c),$$
$$\partial_1\partial_2\Delta = (1-\sigma_1)(a-c) + (\sigma_1-1)\sigma_2(a-b),$$
$$\partial_2\partial_1\Delta = (1-\sigma_2)(a-c) + (\sigma_2-1)\sigma_1(b-c),$$
$$\partial_1\partial_2\partial_1\Delta = 1-\sigma_1-\sigma_2+\sigma_1\sigma_2+\sigma_2\sigma_1-\sigma_1\sigma_2\sigma_1.$$

Ces coefficients sont notés $c_{\mu,\zeta}$ par [13, 16], et $q_\mu^{\zeta^{-1}}$ par [3].

On voit aisément que le terme dominant de Proposition 3.2 est μ (le calcul par induction à partir de (3.10) donne aussi cette propriété). On a donc

$$\nu > \mu \Rightarrow R_\nu(\partial_\mu) = 0$$

(l'ordre sur les permutations est celui d'Ehresmann, dit aussi *de Bruhat*, dit aussi *strong order*). Comme l'application réciproque est aussi vrai, on a là, ainsi que le remarque le rapporteur, une caractérisation intéressante de l'ordre de Ehresmann/Bruhat (voir aussi [13–14, 27, 16]).

Il suit de (3.3) que l'on peut reformuler Lemme 2.10 en:

Lemme 3.4. *Les opérateurs $\mathscr{X}\partial_\mu\theta$, où les $\mu \in \mathfrak{G}(A)$, sont nuls, sauf $\mathscr{X}\partial_\omega\theta = \omega$.*

En particulier, considérant l'image de 1 par les opérateurs $\mathscr{X}\partial_\mu\theta$, on obtient:

Lemme 3.5. *Pour toute permutation μ, le polynôme $X_{\omega\mu}\theta$ est nul, sauf $X_{\omega\omega}\theta = X_{\omega\omega} = 1$.*

La relation (2.5) implique que $\partial_\mu\partial_\nu = \partial_{\mu\nu}$ ou 0 suivant que $l(\mu\nu) = l(\mu) + l(\nu)$ ou non. Du Lemme 3.4 s'ensuit donc le développement de tout élément de $\mathscr{E}$ dans la base $\{\partial_\mu\}$:

Lemme 3.6. *Soit $D = \sum_\zeta Q_\zeta(D)\partial_\zeta$, avec $Q_\zeta(D) \in \mathscr{R}(A)$, un élément de $\mathscr{E}$. Alors $Q_\zeta(D) = \mathscr{X}D\partial_{\zeta^{-1}\omega}\theta\omega$.*

Preuve. La somme $\mathscr{X}\sum_\nu Q_\nu(D)\partial_\nu\partial_{\zeta^{-1}\omega}\theta_\omega = \sum_\nu Q_\nu(D)\mathscr{X}\partial_\nu\partial_{\zeta^{-1}\omega}\theta\omega$ se réduit au seul terme $Q_\zeta(D)\omega\omega = Q_\zeta(D)$ puisque tous les opérateurs $\mathscr{X}\partial_\mu\theta$ sont nuls, sauf $\mathscr{X}\partial_\omega\theta$. □

Nous avons déjà en [23] attiré l'attention sur le fait que la matrice des coefficients $Q_\zeta(\mu)$ est auto-inverse à symétrie et à multiplication par Δ près, ce

que l'on retrouve ici en comparant Proposition 3.2 et Lemme 3.6 (Kumar a aussi remarqué cette propriété).

$$\frac{1}{\Delta} Q_\zeta(\mu) = R_{\mu^{-1}\omega}(\partial_{\zeta^{-1}\omega})\omega. \tag{3.7}$$

Ainsi, du développement des ∂_μ donné plus haut déduit-on:

$$\begin{aligned}
&\sigma_1 = (a-b)\partial_1 - 1,\\
&\sigma_2 = (b-c)\partial_2 - 1,\\
&\sigma_1\sigma_2 = (a-b)(a-c)\partial_1\partial_2 - (a-b)\partial_1 - (a-c)\partial_2 + 1,\\
&\sigma_2\sigma_1 = (a-c)(b-c)\partial_2\partial_1 - (a-c)\partial_1 - (b-c)\partial_2 + 1,\\
&\sigma_1\sigma_2\sigma_1 = \omega = \Delta\partial_\omega - (a-b)(a-c)\partial_1\partial_2 - (a-c)(b-c)\partial_2\partial_1\\
&\qquad\qquad + (a-c)(\partial_1+\partial_2) - 1.
\end{aligned} \tag{3.8}$$

Les ∂_μ sont les opérateurs naturels en cohomologie de la variété de drapeaux (pour [5], la différence divisée ∂_μ est A_μ, pour [9], c'est D_μ et enfin, chez [13] on trouve x_μ). Voir aussi [11, 12] ainsi que les commentaires détaillés du rapporteur en fin de cet article.

On peut en fait relever les différences divisées en des opérateurs agissant sur la cohomologie T-équivariante de la variété de drapeaux [1, 2], la théorie pouvant même être faite dans le cas plus général d'une algèbre de Kac–Moody [3, 14]. Aux différences divisées, on préfère alors les opérateurs $\Delta\partial_\mu$. Le Lemme 2.12 donne le développement de ces derniers dans la base $\{\zeta\}$ à partir de celui des ∂_μ obtenu en Proposition 3.2:

$$R_\zeta(\Delta\partial_\mu) = R_\zeta(\partial_\mu)\Delta^\zeta = X_{\omega\mu}\zeta^{-1}\omega\theta\omega\zeta. \tag{3.9}$$

Ces coefficients sont donc les spécialisations des polynômes de Schubert par le morphisme $y_i \to a_i\omega\zeta$. Les travaux de Berline–Vergne [4], Arabia [1, 2] et [14] ont très fortement suggéré que les $R_\zeta(\Delta\partial_\mu)$ doivent pouvoir s'interpréter comme des invariants géométriques attachés aux points fixes des variétés de Schubert. Ce point de vue est développé par Rossmann [27] qui donne une définition des multiplicités équivariantes dans le contexte de la géométrie algébrique.

Indépendamment de toute géométrie, l'induction $\mu \to \mu\sigma_i$ permet d'obtenir les coefficients $R_\zeta(\Delta\partial_\mu)$ à l'aide des sous-mots d'une décomposition réduite arbitraire de μ [19; 16 , Lemma 4.4; 3, Proposition 3.3].

Le morphisme qui envoie la variété de Schubert d'indice μ sur l'opérateur $\Delta\partial_\mu$ est une injection de la cohomologie équivariante de la variété de drapeaux dans l'algèbre $\mathscr{E}$ [14]; dans le cas que nous considérons (le groupe linéaire), cette injection résulte des formules explicites que nous donnons ci-dessus.

Le développement (3.9) peut aussi s'obtenir à partir de la *Formule de Leibniz*

dans l'algèbre $\mathscr{E}$:

$$\forall f, \ldots, g, h \in \mathscr{R}(A), f \cdots gh\partial_i = f \cdots g(h^{\partial_i}) + f \cdots (g^{\partial_i})h\sigma_i b + \cdots + (f^{\partial_i}) \cdots gh\sigma_i + \partial_i f \cdots gh\sigma_i \tag{3.10}$$

où $f, \ldots, g, h$ dénotent des éléments de $\mathscr{R}(A)$, et du fait que les fonctions symétriques en a_i et a_{i+1} sont des scalaires pour ∂_i.

Par exemple, pour $\mathfrak{S}(\{a, b, c\})$, on obtient successivement

$$\begin{aligned}
(a-b)\partial_1 &= a\partial_1 - b\partial_1 + \partial_1(b-a) = 1 + \sigma,\\
(a-b)(a-c)(b-c)\partial_1 &= (1+\sigma_1)(a-c)(b-c),\\
(a-b)(a-c)(b-c)\partial_1\partial_2 &= (1+\sigma_1)(a-c)(1+\sigma_2)\\
&\quad + (1+\sigma_1)(a\partial_2 - c\partial_2)(c-b) + (1+\sigma_1)\partial_2\\
&= (1+\sigma_1)(a-c) + (1+\sigma_1)\sigma_2(a-b).
\end{aligned}$$

Ce dernier calcul donne en fait l'expression de $\Delta\partial_\mu$ en fonction des sous-mots d'une décomposition réduite de μ, et coïncide avec l'algorithme de Arabia et Kostant–Kumar mentionné plus haut.

Les résultats de ce paragraphe peuvent aussi s'écrire à l'aide du produit scalaire: $\forall P, Q \in \mathscr{R}(A)$, $(P, Q) := PQ\partial_\omega$ pour lequel la base des polynômes de Schubert est auto-adjointe [19, 13].

4. Polynômes de Grothendieck

L'anneau de Grothendieck de la variété de drapeaux fait intervenir de manière naturelle les opérateurs π_μ et ψ_μ ([9] note Λ^0_μ pour π_μ; [7, 1] emploie l'opérateur conjugué de ψ_μ par ω, qu'il note L_μ). Le Corollaire 2.11 donne le développement de ces opérateurs dans la base canonique $\{\zeta\}$:

$$R_\zeta(\pi_\mu) = \mathscr{X}\pi_\mu\zeta^{-1}\omega\theta\omega\zeta/\Delta^\zeta. \tag{4.1}$$

Il se trouve que ce sont d'autres polynômes que les $\mathscr{X}\pi_\mu$ qui interviennent en K-théorie [20, 18]:

Définition 4.2. Le polynôme de Grothendieck d'indice μ est

$$G_\mu = \prod_{i+j\leqslant n+1} (1 - y_i/a_j)\pi_{\omega\mu} = \frac{\mathscr{X}}{\rho}\pi_{\omega\mu}.$$

Les polynômes de Grothendieck sont des polynômes en les $\{1/a_i\}$ et $\{y_j\}$; en fait, $G_\omega = \prod_{i+j\leqslant n+1}(1 - y_i/a_j) = X/\rho$ et l'on peut éviter de recourir aux inverses en remarquant que les ρG_μ sont des polynômes en les $\{a_i\}$ et $\{y_j\}$.

Les polynômes de Grothendieck, tout comme les polynômes de Schubert, sont des généralisations des *fonctions de Schur*. Inversement, les *multifonctions de Schur* permettent de donner des expressions condensées de ces polynômes.

Définition 4.3. Soient A et Y deux alphabets finis. Les *fonctions symétriques complètes* $S_j(A-Y)$ sont les coefficients de la série génératrice

$$\frac{\prod_{y\in Y}(1-\xi y)}{\prod_{a\in A}(1-\xi a)}=\sum_{-\infty}^{+\infty}\xi^j S_j(A-Y),$$

où ξ est une indéterminée supplémentaire.

Définition 4.4. Soient r un entier, $H=(h_1,\dots,h_r)$ un r-uplet d'entiers rationels, $A^1,\dots,A^r$, $Y^1,\dots,Y^r$ des alphabets finis. Alors, la (*multi-*)*fonction de Schur* $S_H(A^1-Y^1,\dots,A^r-Y^r)$ est la valeur du déterminant

$$|S_{h_j+j-i}(A^j-Y^j)|_{1\leqslant i,j\leqslant r}$$

Dans le cas de $S(\{a_1,\dots,a_4\})$, notons en outre $(ijh\ddagger mnp)$ la fonction $(a_1a_2a_3)^{-3}S_{333}(A_i-Y_m,A_j-Y_n,A_h-Y_p)$, où, pour tout k, A_k est l'alphabet des k-premières lettres de A: $A_k=\{a_1,\dots,a_k\}$, mutatis mutandis pour Y. Alors

$$G_{4321}=(321\ddagger 123).$$
$$G_{3421}=(321\ddagger 122);\quad G_{4231}=(321\ddagger 113);\quad G_{4312}=(321\ddagger 023).$$
$$G_{2431}=(322\ddagger 113);\quad G_{3241}=(321\ddagger 112);\quad G_{3412}=(321\ddagger 022);$$
$$G_{4132}=(331\ddagger 023);\quad G_{4213}=(321\ddagger 013).$$
$$G_{1432}=(332\ddagger 023);\quad G_{2341}=(321\ddagger 111);\quad G_{2413}=(322\ddagger 013);$$
$$G_{3142}=(331\ddagger 022);\quad G_{4123}=(321\ddagger 003);\quad G_{3214}=(321\ddagger 012).$$
$$G_{1342}=(332\ddagger 022);\quad G_{1423}=(322\ddagger 003);\quad G_{2143}=G_{2134}\cdot G_{1243};$$
$$G_{2314}=(321\ddagger 011);\quad G_{3124}=(321\ddagger 002).$$
$$G_{1243}=(333\ddagger 003);\quad G_{1324}=(322\ddagger 002);\quad G_{2134}=(321\ddagger 001).$$
$$G_{1234}=(321\ddagger 000)=1.$$

On remarquera que, mis à part G_{2143}, les polynômes de Grothendieck s'expriment à l'aide d'une seule fonction de Schur. Pour un groupe $\mathfrak{G}(A)$ quelconque, les permutations μ telles que G_μ ou X_μ soient égaux à une fonction de Schur sont dites *vexillaires* (cf. [20] pour la définition et [19] pour les différentes caractérisations de ces permutations).

Le Lemme 2.11 permet de décomposer les $(1/\rho)\pi_\mu$ dans la base $\{\zeta\}$:

$$R_\zeta\left(\frac{1}{\rho}\pi_\mu\right)=G_{\omega\mu}\zeta^{-1}\omega\theta\zeta/\Delta^\zeta, \tag{4.5}$$

d'où, à l'aide du Lemme 2.12:

$$R_\zeta(\pi_\mu) = G_{\omega\mu}\zeta^{-1}\omega\theta\zeta\rho^\zeta/\Delta^\zeta. \tag{4.6}$$

En d'autres termes, le développement de π_μ dans la base canonique $\{\zeta\}$ est fourni par les spécialisations des polynômes de Grothendieck—par le morphisme

$$\zeta^{-1}\omega\theta\omega\zeta : y_1 \to a_1\zeta, \ldots, y_{n+1} \to a_{n+1}\zeta.$$

Ainsi le polynôme de Grothendieck $G_{321}\pi_1\pi_2 = G_{213} = (1 - x/a)$ a comme spécialisations non nulles

$$G_{213}\omega\theta\omega = 1 - c/a = G_{213}\sigma_1\omega\theta\omega\sigma_1$$

et

$$G_{213}\sigma_2\omega\theta\omega\sigma_2 = 1 - b/a = G_{213}\sigma_2\sigma_1\omega\theta\omega\sigma_1\sigma_2,$$

ce qui entraîne d'après (4.6) le développement

$$\pi_1\pi_2 = \frac{ab}{(a-b)(a-c)} - \sigma_1\frac{b^2}{(a-b)(b-c)} - \sigma_2\frac{ac}{(a-c)(b-c)} + \sigma_1\sigma_2\frac{c^2}{(a-c)(b-c)}.$$

Les $R_\zeta(\pi_\mu)$ sont notés $b_{\mu,\zeta}$ par [2, 16, 14].

La définition des opérateurs π_μ et ψ_μ peut s'étendre à la K-théorie équivariante des variétés de drapeaux, et même des algèbres de Kac–Moody [14, 16]. Brion nous a fait remarquer que le principe de localisation s'étend à la K-théorie; en d'autres termes, le morphisme qui associe à la variété de Schubert d'indice μ l'élément $(\Delta/\rho)\pi_\mu$ est l'injection naturelle de la K-théorie T-équivariante de la variété de drapeaux dans $\mathscr{E}$ [16, Théorème 2.2].

Tenant compte du facteur Δ/ρ, on obtient à partir de (4.1) le développement de ces opérateurs dans la base $\{\zeta\}$:

$$R_\zeta\left(\frac{\Delta}{\rho}\pi_\mu\right) = G_{\omega\mu}\zeta^{-1}\omega\theta\omega\zeta. \tag{4.7}$$

Les images des variétés de Schubert dans $\mathscr{E}$ ont donc pour composantes (dans la base $\{\zeta\}$) les spécialisations des polynômes de Grothendieck par le morphisme $y_1 \to a_1\omega\zeta, \ldots, y_{n+1} \to a_{n+1}\omega\zeta$.

On peut noter que la spécialisation $y_1 \to 1, \ldots, y_{n+1} \to 1$ du polynôme de Grothendieck G_μ est la classe du *faisceau structural* de la variété de Schubert d'indice μ [7, 18, 20], les indéterminées $a_1, \ldots, a_{n+1}$ devant s'interpréter comme les classes respectives des fibrés inversibles, dits tautologiques, de la variété de drapeaux.

On peut retrouver les cycles de Schubert à partir des classes des faisceaux structuraux, à l'aide du changement de variables $1 - 1/a_i = \beta_i$. Soient ∂^β_μ les différences divisées associées à l'alphabet $B = \{\beta_1, \ldots, \beta_{n+1}\}$. Il est facile de vérifier que

$$\pi_i = (1 - \beta_{i+1})\partial^\beta_i. \tag{4.8}$$

Ainsi donc l'image de $(1-1/a_1)^n \cdots (1-1/a_{n+1})^0 = \beta_1^n \cdots \beta_{n+1}^0$ par π_μ a pour terme de plus bas degré en B le polynôme $\beta_1^n \cdots \beta_{n+1}^0 \partial_\mu^\beta$, c'est-à-dire le cycle de Schubert d'indice $\omega\mu$. Ce résultat s'obtient classiquement en prenant le terme de degré minimum du polynôme de Grothendieck en les variables $e^\alpha = 1 + \alpha + \cdots$. Cependant la formule (4.8) permet d'obtenir l'expression exacte des polynômes de Grothendieck en fonction des polynômes de Schubert, et pas seulement leur terme dominant.

On sait par ailleurs [18] que $\psi_\mu = \sum_{\nu \leqslant \mu} = (-1)^{l(\nu)} \pi_\nu$, où l'inégalité est relative à l'ordre d'Ehresmann. Réciproquement, $\pi_\mu = \sum_{\nu \leqslant \mu} \psi_\nu$; on pourrait aisément retrouver ces deux égalités à l'aide des formules de décomposition dans les bases $\{\pi_\mu\}$ ou $\{\psi_\mu\}$ données ci-dessous. Comme corollaire, on a que la fonction de Möbius du groupe symétrique (pour l'ordre d'Ehresmann) prend ses valeurs dans $\{+1, -1\}$ suivant la longueur [28].

Le développement de ψ_μ provient donc de celui des π_ν:

$$R_\zeta(\psi_\mu) = \sum_{\nu \leqslant \mu} (-1)^{l(\nu)} G_{\omega\nu} \zeta^{-1} \omega\theta\omega\zeta\rho^\zeta / \Delta^\zeta. \tag{4.9}$$

On a en fait une identité plus compacte, à l'aide de l'involution suivante permettant d'échanger les opérateurs π et ψ (il suffit de prouver (4.10) pour une transposition simple [18]:

$$\omega \frac{1}{\rho} \pi_\mu \rho \omega = (-1)^{l(\mu)} \psi_{\omega\mu\omega}. \tag{4.10}$$

Rassemblant (4.6) et (4.10), on obtient ainsi:

$$R_\zeta(\psi_\mu) = (-1)^{l(\mu)} G_{\mu\omega} \omega \zeta^{-1} \theta \zeta \omega \frac{\rho}{\Delta^\zeta} \omega. \tag{4.11}$$

Inversement, le développement des éléments de $\mathscr{E}$ en fonction des π_μ ou ψ_μ est donné par les deux lemmes, corollaires de Lemme 2.10.

Lemme 4.12. *Soit $D = \sum_\mu P_\mu(D)\pi_\mu$, avec $P_\mu \in \mathscr{R}(A)$, un élément de $\mathscr{E}$. Alors $\mu \neq \omega \Rightarrow P_\mu(D) = G_\omega D \psi_{\mu^{-1}\omega} \theta\omega$ et $P_\omega(D) = G_\omega D \theta\omega$.*

Ainsi, pour $D = \psi_1\psi_2 = (\pi_1 - 1)(\pi_2 - 1)$, on trouve $G_{321}D = G_{213} - G_{231} - G_{312} + G_{321}$, d'où $G_{321}D\pi_1 = G_{123} - G_{132}$ et $G_{321}D\pi_2 = 0 = G_{321}D\pi_1\pi_2$, ce qui donne bien $\psi_1\psi_2 = \pi_1\pi_2 - \pi_1 - \pi_2 + 1$.

Les $P_\mu(\zeta)$ sont notés $e^{\mu,\zeta}$ par [14].

Similairement, le développement dans la base des $\{\psi_\mu\} \cup \{1\}$ est:

Lemme 4.13. *Soit $D = \sum_{\mu, \mu \neq \mathrm{id}} \check{P}_\mu(D)\psi_\mu + \check{P}_{\mathrm{id}} 1$, avec $\check{P}_\mu \in \mathscr{R}(A)$, un élément de $\mathscr{E}$. Alors $\check{P}_\mu(D) = G_\omega D \pi_{\mu^{-1}\omega} \theta\omega$ et $\check{P}_{\mathrm{id}}(D) = G_\omega D \pi_\omega \theta\omega$.*

Par exemple, soit $D = \partial_2\partial_1$. Alors

$$\begin{aligned} G_{321}D &= (1-x/b)(1-x/a)(1-y/a)\partial_2\partial_1 \\ &= (1-x/b)\partial_2(1-x/a)(1-y/a)\partial_1 \\ &= (x/bc)(1-x/a)(1-y/a)\partial_1 \\ &= (x/abc)(1-xy/ab). \end{aligned}$$

On a donc $G_{321}D = G_{321}D\pi_2$ et $G_{321}D\pi_1 = G_{321}D\pi_2\pi_1 = G_{321}D\pi_1\pi_2 = G_{321}D\pi_1\pi_2\pi_1 = x/abc$, d'où en prenant l'image de ces fonctions par $\theta\omega$, le développement:

$$\partial_2\partial_1 = (1/ab)(\psi_2\psi_1 + \psi_1 + \psi_2 + 1).$$

Les résultats de cette section peuvent aussi s'obtenir à l'aide du produit scalaire sur $\mathcal{R}(A)$: $\forall P, Q \in \mathcal{R}(A)$, $\langle P, Q\rangle := PQ\pi_\omega$; en effect, la base des polynômes de Grothendieck et sa base adjointe sont échangées par une involution élémentaire [18], ce qui permet de décomposer explicitement les éléments de $\mathcal{R}(A)$ dans chacune de ces deux bases.

Outre de nombreuses remarques destinées à améliorer l'exposition, le rapporteur a bien voulu apporter les précisions géométriques suivantes que nous avons adaptées de son rapport car elles motivent les formules données dans cet article:

There is a very important conceptual nuance in the definition of operators acting on the different cohomology groups $H^*(X)$ of a flag manifold X. In [5], the A_i are a priori defined on an algebra $S(\mathfrak{h}^*)$ and the existence of the generalizations A_μ is obtained only through the combinatorics associated with the Bruhat order on the Weyl group. Therefore what we have at the start are algebraic objects. [5] used Borel's result, which shows that the characteristic morphism (Chern–Weil morphism) $\alpha : S(\mathfrak{h}^*) \to H^*(X)$ is surjective and has as kernel the ideal $\mathcal{I}$ generated by the symmetric polynomials without constant terms; after noticing that the A_μ stabilize $\mathcal{I}$, they use them as 'natural' operators on the cohomology of X. Incidentally, we recall that these cohomological operators are in fact denoted $\bar{A}_\mu$. The main result of [5] is the equality, which has become classical,

$$\langle X_\mu, \alpha(P)\rangle = A_\mu(P)(0),$$

for every $P \in S(\mathfrak{h}^*)$. Their proof uses cohomological and geometrical techniques, but these techniques are not intrinsic to the definition of the A_μ. In other words, one can say that this cohomological action, though natural, is 'a posteriori'.

There have been numerous works generalizing [5] in different directions; more precisely as concerns the flag varieties associated with the Kac–Moody groups, the work of Kostant–Kumar [13] is rather satisfactory. Nevertheless, here too, these operators, now denoted x_μ are introduced in a purely algebraic context and still act on the cohomology of X only a posteriori. The same remark applies to the cited Demazure's articles. In all these works, one can rightly consider that the A_μ are purely algebraico–combinatorial objects. The right a priori cohomological

definition appears in Demazure's unpublished notes (cf. Marlin for the geometric finite dimensional non-equivariant case, Arabia for the topological, equivariant and Kac–Moody case; cf. also Kac (with Peterson) for the topological case as well as the Kac–Moody case. Unfortunately, the reference "*Cohomology of infinite-dimensional groups and their flag varieties*' has never been published to my knowledge). There is however a nonnegligible factor in favor of Demazure's approach. Though Demazure and Kac define the A_i through the composition $\pi_i^*\pi_{i*}$ for the canonical projection π_i of G/B on G/P_i, only Demazure has succeeded in defining the A_μ for the cohomology and for every μ, *without having recourse to the combinatorics of Coxeter groups*. Indeed, let $\mathcal{S}_\mu$ be the adherence of the G-orbit of the point (e, μ) in the variety $X \times X$ on X. Let us denote p_i the restrictions to T_μ of the canonical projections of $X \times X$ on X. Then one has $A_\mu = p_{1*}p_2^*$ (confer [3]). Thus it appears that among the numerous ways of introducing the operators in question, there is one, derived from Demazure's work, which is truly specific to the cohomological context. On the other hand, the explicitation of the coefficients $R_\xi(\Delta\partial_\mu)$ by Arabia is obtained from a 'desingularisation of Schubert varieties. This has the consequence that his computations are intrinsic only for the smooth case (e.g., if μ is the product of mutually distinct simple transpositions, or if μ is the longest element of the Weyl group in the finite dimensional case), but then the interpretation of the rational functions in equivariant cohomology results from a paper by Atiyah–Bott (The moment map and equivariant cohomology, Topology 23 (1984) 1–28—there must exist earlier references) where these coefficients are identified with equivariant analogs of Euler classes of subvarieties of fixed points (result rediscovered by Berline–Vergne: Fourier transforms of orbits of the coadjoint representation, Proceedings of the conference on 'Representation of reductive groups', Park City, Utah, 1982 in the context of differential geometry, when the fixed points are isolated). A closer inspection shows that the only justification one can give for the fact that these invariants are of a cohomological nature in the singular case, if we wanted to obtain this from Arabia's work, would come exclusively from the Atiyah–Segal isomorphism.

In fact, the work of Berline–Vergne [4], Arabia [2, 3] and Kostant–Kumar [19], in that order, strongly suggests that the coefficients $R_\xi(\Delta\partial_\mu)$ should in all cases, regular as well as singular, be interpreted as geometrical and even topological, invariants, and that they should be given an intrinsic definition. This is this idea which is behind the theory developed by Rossmann, who gives a definition of *equivariant multiplicities* in the framework of algebraic geometry.

References

[1] A. Arabia, Cycles de Schubert et cohomologie K-équivariante de K/T, Thèse, Université Paris 7, 1985.

[2] A. Arabia, Cohomologie T-équivariante de G/B pour un groupe G de Kac–Moody, Invent. Math. 85 (1986) 39–52.
[3] A. Arabia, Cohomologie T-équivariante de la variété de drapeaux d'un groupe de Kac–Moody, preprint, 1986.
[4] N. Berline et M. Vergne, Zéros d'un champ de vecteurs et classes caractéristiques équivariantes, Duke Math. 50 (1983) 539–549.
[5] I.N. Bernstein, I.M. Gelfand et S.I. Gelfand Schubert cells and cohomology of the spaces G/P, Uspekhi. Mat. Nauk 28 (1973) 3–26.
[6] N. Bourbaki, Algèbre (Hermann, Paris).
[7] M. Demazure, Désingularisation des variétés de Schubert, Ann. Économ. Statist. 6 (1974) 163–172.
[8] M. Demazure, Une nouvelle formule des caractères, Bull. Sci. Math. 98 (1974) 163–172.
[9] M. Demazure Invariants symétriques entiers des groupes de Weyl et torsion, Invent. Math. 21 (1973) 287–301.
[10] E. Gutkin, Operator calculi associated with reflection groups; Reflection groups, generalized BGG calculus, preprints, 1986.
[11] E. Gutkin et P. Slodowy, Cohomologie des variétés de drapeaux infinies, C.R. Acad. Sci. Paris 296 (1983) 625.
[12] V. Kac, Torsion in cohomology of compact Lie groups and Chow rings of reductive algebraic groups, Invent. Math. 80 (1985) 69–79.
[13] B. Kostant et S. Kumar, The Nil Hecke ring and cohomology of G/P for a Kac–Moody group G, Adv. in Math. 62 (1986) 187–237.
[14] B. Kostant et S. Kumar, T-equivariant K-theory of generalized flag varieties, J. Differential Geom. (1990) 549–603.
[15] W. Kraskiewicz et P. Pragacz, Foncteurs de Schubert, C.R. Acad. Sci. Paris 304 (1987) 209–212.
[16] S. Kumar, A connection of equivariant K-theory with the singularity of Schubert varieties, preprint, 1988.
[17] A. Lascoux, Classes de Chern des variétés de drapeaux, C.R. Acad. Sci. Paris 295 (1982) 393–398.
[18] A. Lascoux, Anneau de Grothendieck de la variété de drapeaux, dans: The Grothendieck Festschrift, Progr. Math., Vol. 88 (Birkhäuser, Boston, 1990) 1–34.
[19] A. Lascoux et M.P. Schützenberger, Polynômes de Schubert, C.R. Acad. Sci. Paris 294 (1982) 447.
[20] A. Lascoux et M.P. Schützenberger, Structure de Hopf. . . , C.R. Acad. Sci. Paris 295 (1982) 629.
[21] A. Lascoux et M.P. Schützenberger, Symmetry and Flag manifolds, in: Invariant Theory, Lecture Notes in Mathematics 966 (Springer, Berlin, 1983) 118–149.
[22] A. Lascoux et M.P. Schützenberger, Interpolation de Newton à plusieurs variables, Séminaire d'Algèbre M.P. Malliavin 1983–84, Lecture Notes in Mathematics 1146 (Springer, Berlin, 1985) 161–175.
[23] A. Lascoux et M.P. Schützenberger, Symmetrization operators on polynomial rings, Funct. Anal. Appl. 21 (1987) 77–78.
[24] A. Lascoux et M.P. Schützenberger, Keys and standard bases, in: D. Stanton, ed., Invariant Theory and Tableaux, Mathematics and its Applications 19 (Springer, Berlin, 1990) 125–144.
[25] A. Lascoux et M.P. Schützenberger, Tableaux and non commutative Schubert polynomials, Funct. Anal. Appl. 23 (1989) 63–64.
[26] I.G. Macdonald, Symmetric Functions and Hall Polynomials, Oxford Mathematical Monographs (Oxford Univ. Press, Oxford, 1979).
[27] W. Rossmann, Equivariant multiplicities on complex varieties, prépublication, 1987.
[28] D.N. Verma, Möbius inversion for the Bruhat ordering on a Weyl group, Ann. École Normale Superieure 4 (1971) 393–399.

WORDS, LANGUAGES AND COMBINATORICS

Kyoto, Japan 28 – 31 August 1990

Editor

Masami Ito
Faculty of Science
Kyoto Sangyo University
Japan

World Scientific
Singapore • New Jersey • London • Hong Kong

RATIONAL WORD FUNCTIONS: CHARACTERIZATION AND MINIMIZATION

CHRISTOPHE REUTENAUER
Mathématiques et Informatique
Université du Québec à Montréal
Montréal, Canada H3C 3P8

and

MARCEL-PAUL SCHÜTZENBERGER
Académie des Sciences
Paris, France

ABSTRACT

A function from a free monoid is rational if its graph is a rational subset of the product monoid. We show that a function is rational if and only some congruence, canonically attached to it, is of finite index, and if the function preserves rationality of languages under inverse image. We construct a canonical bimachine computing a given rational function. This bimachine is minimal, in some precise sense, when the function is total.

1.Rational languages

It is well-known that a language $L \subseteq A^*$ is rational if it satisfies the Nerode criterion. This characterization may be equivalently expressed using the Hankel matrix of the language. This matrix is an A^* by A^* matrix, with a 1 or a 0 in the (u, v) - entry, depending whether uv is in L or not. For example, for $L = \{a, ba, bb\}^*$, the Hankel matrix is the following

436

	1	a	b	aa	ab	ba	bb	aaa	aab	aba	abb	baa	bab	bba	bbb	...
1	1	1	0	1	0	1	1	1	0	1	1	1	0	1	0	
a	1	1	0	1	0	1	1	1	0	1	1	1	0	1	0	
b	0	1	1	1	0	1	0	1	0	1	1	1	0	1	1	
aa	1	1	0	1	0	1	1	1	0	1	1	1	0	1	0	
ab	0	1	1	1	0	1	0	1	0	1	1	1	0	1	1	
ba	1	1	0	1	0	1	1	1	0	1	1	1	0	1	0	
bb	1	1	0	1	0	1	1	1	0	1	1	1	0	1	0	
aaa	1	1	0	1	0	1	1	1	0	1	1	1	0	1	0	
aab	0	1	1	1	0	1	0	1	0	1	1	1	0	1	1	
aba	1	1	0	1	0	1	1	1	0	1	1	1	0	1	0	
abb	1	1	0	1	0	1	1	1	0	1	1	1	0	1	0	
baa	1	1	0	1	0	1	1	1	0	1	1	1	0	1	0	
bab	0	1	1	1	0	1	0	1	0	1	1	1	0	1	1	
bba	1	1	0	1	0	1	1	1	0	1	1	1	0	1	0	
bbb	0	1	1	1	0	1	0	1	0	1	1	1	0	1	1	

A language is rational if and only if its Hankel matrix has only finitely many distinct lines; this also holds with columns. In the example, there are 2 different rows, and 4 different columns.

The terminology "Hankel matrix" stems from classical analysis: it is well-known that a series

$$\sum_{n\geq 0} a_n x^n$$

whith coefficients in a field is rational (i.e. quotient of two polynomials) if and only if its Hankel matrix

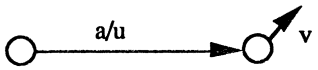
$$(a_{i+j})_{i,j} \geq o$$

has finite rank; this rank is equal to the dimension of the vector space generated by the columns (resp. of the rows), or to the maximum order of a non-vanishing subdeterminant of the matrix.

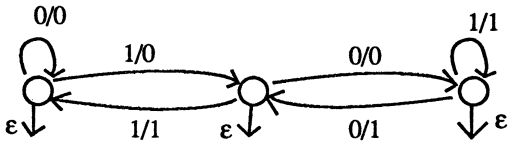
2.Subsequential functions

a.Hankel characterization

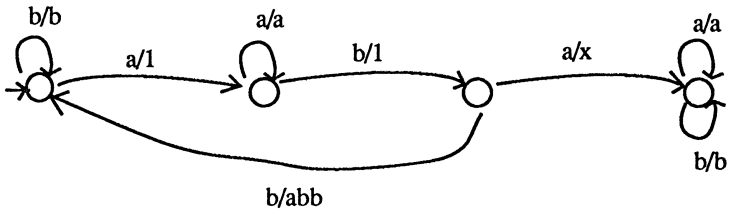
A (partial) function x: $A^* \longrightarrow B^*$ is (left-to-right) **subsequential** if is is computed by some subsequential transducer (i.e. a generalized sequential machine with endmarker). Locally, a subsequential transducer looks like this:



When input letter a is read, than output word u is produced, and in case a is the last letter of the input word, a final output v is produced.
Examples of subsequential transducers are integer division in a given base by a given integer, and pattern substitution.



integer division by 3 in base 2



pattern substitution: first occurrence of aba is replaced by x

Define the Hankel matrix of the function α: $A^* \longrightarrow B^*$ to be the $A^* \times A$ - matrix

$$(\alpha(u\ v))_{u,v \in A^*}$$

438

The Hankel matrix of the pattern substitution above is

1	a	b	aa	ab	ba	bb	aaa	aab	x	abb	baa
a	aa	ab	aaa	aab	x	abb	aaaa	aaab	ax	aabb	xa
b	ba	bb	baa	bab	bba	bbb	baaa	baab	bx	babb	bbaa
aa	aaa	aab	aaaa	aaab	ax	aabb	aaaaa	aaaab	aax	aaabb	axa
ab	x	abb	xa	xb	abba	abbb	xaa	xab	xba	xbb	abbaa
ba	baa	bab	baaa	baab	bx	babb	baaaa	baaab	bax	baabb	bxa
bb	bba	bbb	bbaa	bbab	bbba	bbbb	bbaaa	bbaab	bbx	bbabb	bbbaa
aaa	aaaa	aaab	aaaaa	aaaab	aax	aaabb	aaaaaa	aaaaab	aaax	aaaabb	aaxa
aab	ax	aabb	axa	axb	aabba	aabbb	axaa	axab	axba	axbb	aabbaa
x	xa	xb	xaa	xab	xba	xbb	xaaa	xaab	xaba	xabb	xbaa
abb	abba	abbb	abbaa	abbab	abbba	abbbb	abbaaa	abbaab	abbx	abbabb	abbbaa
baa	baaa	baab	baaaa	baaab	bax	baabb	baaaaa	baaaab	baax	baaabb	baxa
bab	bx	babb	bxa	bxb	babba	babbb	bxaa	bxab	bxba	bxbb	babbaa
bba	bbaa	bbab	bbaaa	bbaab	bbx	bbabb	bbaaaa	bbaaab	bbax	bbaabb	bbxa
bbb	bbba	bbbb	bbbaa	bbbab	bbbba	bbbbb	bbbaaa	bbbaab	bbbx	bbbabb	bbbbaa

There are not a finite number of distinct lines. However, a function is subsequential if and only if there exist a finite number of lines L_1,.., L_n such that each line of its Hankel matrix is of the form uL_i for some word u.

The analogue property for the columns holds only when the function is subsequential from right to left; for example, multiplication by a given integer in a given base.

b.Choffrut's characterization of subsequential functions

Define the (left) distance between two words by

$$\| u, v, \| = |u'| + |v'|$$

where $u = xu'$, $v = xv'$ and x is the longest common left factor of u and v. We say that a function α: $A^* \longrightarrow B^*$ is uniformly bounded if for any integer k, there exists an integer K such that

$$\forall\ u, v \in \mathrm{dom}\ (\alpha),\ |u, v| \leq k \Rightarrow |\alpha u, \alpha v| \leq K$$

Intuitively, this means that if u, v have a long common prefix, then so are also α u and α v. Choffrut's theorem states that a function α is subsequential if and only if α is uniformly bounded and α^{-1} preserves rationality of languages. This theorem admits as a corollary the theorem of Ginsburg and Rose characterizing sequential functions.

3.Rational functions

Rational functions are obtained by closure under composition of left-to-right and right-to-left subsequential functions. Elgot and Mezei have shown that actually one composition is enough (for a direct proof, see Arnold and Latteux). Equivalently, a function α: $A^* \longrightarrow B^*$ is rational if its graph is a rational subset of the monoid $A^* \times B^*$ (i.e α is a functional rational transduction). Equivalently, α is obtained by a matrix representation, that is, there exists an homromrorphism u: $A^* \longrightarrow M_n\ (2^{B^*})$ (the matrix semiring over the subsets of B^*, with union and product), a lign matrix λ and column matrix γ of size n, such that for any word

$$\alpha\ (w) = \lambda\ \mu\ (w)\ \gamma$$

(where we identify a word u and the singleton {u}).

4.Schützenberger's Hankel characterization of rational functions

This theorem characterizes rational functions through a Hankel property. In order to justify the terminology "Hankel property", recall that a Hankel matrix $(a_{i+j})_{i,j\geq 1}$ over a field has finite rank if and only if there exist functions $\beta_1,\ldots\beta_n,\ldots\gamma_1,\ldots,\ \gamma_n$ from N into the field such that for any integers i, j, one has

$$a_{i+j} = \sum_{r=1}^{n} \beta_r\ (i)\ \gamma_r\ (j)$$

Schützenberger's theorem is the following: a function α: $A^* \longrightarrow B^*$ is rational if and only if there exist functions $\beta_1,..., \beta_n, \gamma_1,..., \gamma_n$: $A^* \longrightarrow B^*$ such that for any words u, v

$$\alpha (u\, v) = \bigcup_{1 \le r \le n} \beta_r (u)\, \gamma_r (v)$$

We call this latter property the Hankel property. The direct part of the theorem follows directly from a matrix representation for α. The converse is more difficult, and we give a new proof through our new characterization of rational functions (next section).

5.A Nerode-like characterization of rational functions

Define the syntactic left conquence of a function α: $A^* \longrightarrow B^*$ by : $u \sim v$ iff

$$\sup \{ \mid \alpha (fu), \alpha (fv) \mid, f \in A^* \} < \infty$$

(the convention with $\varnothing$ is that $\mid \varnothing, w \mid = \infty$ for any word w and $\mid \varnothing, \varnothing \mid = 0$). As an example take the function x: $\{a, b\}^* \longrightarrow \{a, b\}^*$ which removes odd runs in a word, e.g. α (a b b a a a b a a) = b b a a (the odd runs a, aaa, b are removed). Then $a^2 \sim 1$, because $\alpha (f\, a^2) = \alpha (f)\, 1\, a^2$ or $\alpha (f)$, depending on the parity of number of a's at the end of f; so $\sup \{ \mid \alpha (fa^2), \alpha (f) \mid, f \in A^* \} = 2 < \infty$. On the other hand, we don't have $a \sim 1$, because for even n, $\alpha (a^n\, a) = 1$ and $\alpha (a^n\, 1) = a^n$, so that $\mid \alpha (fa), \alpha (f) \mid$ is unbounded.

Note that if α is the characteristic function of a language L (α (w) = 1 if w $\in$ L, and = $\varnothing$ otherwise), then $\sim$ is the syntactic left congruence of L.

Theorem 1 A function α is rational if and only if its syntactic left congruence has finite index and if α^{-1} preserves rationality.

One part of the proof is to show that the Hankel property (see previous section) is preserved under composition, implies that dom (α) is rational, and more generally that α^{-1} preserves rationality. Another part relies on Choffrut's theorem.

6.Effectiveness

Our constructions are effective. To see it, let us say that two functions α,β: $A^* \longrightarrow B^*$ are adjacent if $\sup \{ \mid \alpha(f), \beta(f) \mid , f \in \mathrm{dom}(\alpha) \cap \mathrm{dom}(\beta) \} < \infty$

Proposition One can decide if two rational funcitons α, β are adjacent. In case they are, the function

$$\alpha \wedge \beta : \mathrm{dom}(\alpha) \cap \mathrm{dom}(\beta) \longrightarrow B^*$$
$$w \longrightarrow \text{longest common prefix of } \alpha(w) \text{ and } \beta(w)$$

is rational and may be effectively constructed.

As an application, note that for the syntactic left congruence $\sim$ of a function α, one has $u \sim v$ if and only if the two functions $f \longrightarrow \alpha(fu)$ and $f \longrightarrow \alpha(fv)$ have same domain and are adjacent.

7.Bimachines

A bimachine reads the input word in some sense simultaneously from left to right and from right to left. Formally, it means that there are two sets of states, left and right states L and R (which are respectively right and left A^* - modules), with initial states l_o, r_o, an output function $\omega: L \times A \times R \longrightarrow B^*$, and left and right final functions λ and ρ. The function α computed by the bimachine is given by:

$$\alpha(a_1 \ldots a_n) = \lambda(a_1 \ldots a_n r_o) \prod_{i=1}^{n} \omega(l_o a_1 \ldots a_{i-1}, a_i, a_{i+1} \ldots a_n r_o) \rho(l_o a_1 \ldots a_n)$$

When R is a singleton, then the bimachine is a (left-to-right) subsequential transducer. A bimachine in the sense of Eilenberg has $\lambda = \rho = 1$ (constant function).

As is well-known, a function is rational if and only if it is ocmputed by some bimachine.

8.A canonical bimachine

The syntatic (left) adjacency of α is the relation on A^* defined by $u \longleftrightarrow v$ if $\sup \{ \mid \alpha(fu), \alpha(fv) \mid , f \in A^*, \alpha(fu) \neq \emptyset \neq \alpha(fv) \} < \infty$

If α is a total function, then $\longleftrightarrow$ is the syntactic left congruence, and α is uniformly bounded if and only if u $\longleftrightarrow$ for any words u and v. Note that $\longleftrightarrow$ is however not transitive in general.

It is verified that if R is the set of right states of some bimachine computing α, then the left congruence on A^* defined by r_0 and the left action of A^* on R is compatible with the syntactic adjacency relation of α, i.e:

$$u\, r_0 = v\, r_0 \Rightarrow u \longleftrightarrow v$$

The next result is a converse.

Theorem 2 let $\sim$ be a left congruence which is compatible with $\longleftrightarrow$. Then there exists a bimachine computing α with set of right states $R = A^* / \sim$.
The bimachine which we construct is canonical, once $\sim$ is chosen. If α is a total function, then it has the minimum number of left states among all bimachines computing α with set of right states R. The construction is long and technical.

9.Open problems

a.Find enough "morphisms" between bimachines such that the following result holds: there are only a finite number of "minimal" bimachines computing a given rational function.

b.Characterize the rational functions which may be computed by a bimachine whose transition monoid are both aperiodic. Tentative conjecture: α is as above $\Longleftrightarrow$ the period of α^{-1} (L) divides that of L, for any rational language L.

c.Characterize the rational functions which are both left-to-right and right-to-left subsequential. In the case of numerical functions (i.e. α (A^*) is contained in a cyclic submonoid), this has been done by Choffrut and Schützenberger.

Bibliography

A. Arnold, M. Latteux, A new proof of two theorems about rational transductions, Theor. Comput. Sci.8 (1979) 261-263.

J. Berstel, Transductions and context-free languages, Teubner (1979).

C. Choffrut, A generalization of Ginsburg and Rose's characterization of g. - s.-m. mappings, Lecture Notes Comput. Sci. 71 (1979) 88-103.

C. Choffrut, K. Culik, Properties of finite and pushdown transducers, Siam J. Comput. 12 (1983) 300-315.

C. Choffrut, M.-P. Schützenberger, Counting with rational functions, Theor. Comput. Sci. 58 (1988) 81-101.

S. Eilenberg, Automata, languages and machines, vol.A, Acad. Press (1974).

S. Ginsburg, An introduction to mathematical machine theory, Addison Wesley (1962).

G.N. Raney, Sequential functions, J. Assoc. Comput. Mach.5 (1958) 177-180.

C. Reutenauer, Subsequential functions: characterizations, minimization, examples, Intern. Meeting of Young Comput. Scientists, Proc., J. Kelemen ed., Lecture Notes Comput. Sci., to appear.

M.-P. Schützenberger, A remark on finite transducers, Information adn Control 4 (1961) 185-196.

M.-P. Schützenberger, Sur une variante des fonctions séquentielles, Theor. Comput. Sci. 4 (1977) 47-57.

M.-P. Schützenberger, Une propriété de Hankel des relations fonctionnelles entre monoïdes libres, Advances Maths 24 (1977) 274-280.

Année 1993

Bibliographie

[1993-1] Paul Moszkowski et Marcel-Paul Schützenberger. Planarity properties of the Schensted correspondence. *Adv. in Math.*, 102(1) :1–19, 1993.

[1993-2] Marcel-Paul Schützenberger. *"Et aussi avec Charles Darwin" Préface à "Pour en finir avec le darwinisme, une nouvelle logique du vivant", par Rosine Chandebois.* Editions Espaces 34, 1993.

ADVANCES IN MATHEMATICS **102**, 1–19 (1993)

Planarity Properties of the Schensted Correspondence

P. MOSZKOWSKI

C.N.R.S., Equipe de Combinatoire, Université Paris 6, U.F.R. 921, 4, Place Jussieu, 75005 Paris, France

AND

M.-P. SCHÜTZENBERGER

97, Rue du Ranelagh, 75016 Paris, France

We give a natural decomposition of the set of standard Young tableaux of a given shape into intervals with respect to the weak Bruhat order; each class is completely determined by a partial order on letters which admits a remarkable planar representation.

1. INTRODUCTION

Tableaux were introduced by A. Young in his fundamental papers on the representation of the symmetric groups; a slight modification was soon used by Richardson and Littlewood to provide a combinatorial definition of Schur functions. Since then tableaux have become an essential tool in related fields such as invariant theory or the representation of classical groups. The papers collected under the title "Invariant Theory and Young Tableaux" [8] provide an outlook of current research in this field. In the present paper we restrict our attention to the basic case in which the tableaux are standard in the sense of A. Young, meaning they are defined as "fillings" of the Ferrers diagram of a partition J of n with the letters of the totally ordered set $\mathscr{A} = \{1, 2, ..., n\}$ in such a way that letters appear in increasing order along each row and each column and that each letter of $\mathscr{A}$ appears exactly once. The partition J is the *shape* of the tableau. From Young's point of view tableaux are a convenient way of dealing with the chains of nested partitions of 1, 2, ... which are associated with the sequence of symmetric groups $\mathscr{S}_1 \subsetneq \mathscr{S}_2 \subsetneq \cdots \subsetneq \mathscr{S}_n$. At the same time tableaux summarize the systems of cosets linked with the Frobenius subgroups of $\mathscr{S}_n$ characterized by the shape J.

A different approach has been initiated by Schensted who discovered a bijection between permutations and pairs of tableaux of same shape, called

0001-8708/93 $9.00

respectively the P-symbol and the Q-symbol in Schensted [5]. Here permutations and tableaux are seen as words of the free monoid $\mathscr{A}^*$ generated by the alphabet $\mathscr{A}$. For instance the tableau t with rows 3, 5 and 1, 2, 4 is identified with the word 35124 and it is associated with the words 31524 (which is the reading of t by columns), 31254, 13254, and 13524, all of which have the same P-symbol. Knuth discovered a simple congruence $\cong$ on $\mathscr{A}^*$ which underlies Schensted's correspondence in the sense that two words are congruent if and only if they have the same P-symbol. The quotient $\mathscr{A}^*/\cong$ is the plactic monoid and the (semistandard) tableaux t make up a set of representatives of the classes W_t of the plactic congruence $\cong$; our (standard) tableaux correspond to the words in which each letter of A appears exactly once. A theorem due to C. Greene gives a very useful characterization of the shape of t in terms of families of increasing subwords of the words of W_t. These considerations bring us back to Littlewood's use of tableaux. The plactic algebra $Z(\mathscr{A}^*/\cong)$ turns out to be the proper set up for dealing with Schur functions and their q-generalizations, i.e., the Hall–Littlewood polynomials. In fact the plactic congruence can be defined directly as one of the two extremal congruences $\cong$ on $\mathscr{A}^*$ such that the symmetric polynomials make up a commutative subalgebra of $Z(\mathscr{A}^*/\cong)$.

Returning to the standard case, Schensted's construction reveals an interplay between the tableaux corresponding to a permutation w and to its inverse and it involves in an essential manner the descent set of $w = x_1 x_2 \cdots x_n$ $(x_i \in \mathscr{A})$, i.e., the set $\mathrm{Des}(w)$ of indices j for which $x_j > x_{j+1}$. Both notions are ingredients of the Kazhdan–Lusztig theory [2] which studies properties of the decomposition of $\mathscr{S}_n$ into the cells W_t. Several conjectures concerning the Kazhdan–Lusztig polynomials in the case of the symmetric group require a better understanding of the combinatorial properties of the plactic congruence $\cong$. It remains somewhat of a mystery why these purely algebraic concepts should have anything to do with several properties of the tableaux which derive from their interpretation as a planar disposition of letters. The present paper is an attempt to further analyze these relationships.

Say that a permutation σ acting on $\mathscr{A}$ is *admissible* for a tableau t if w and σw have the same descent set for every w in the plactic class W_t of t. This implies that σt is a tableau of same shape as t and we prove that when σ is admissible for t, then it is a bijection from W_t onto $W_{\sigma t}$. This defines a new equivalence relation on the set of tableaux of same shape; we call *plaques* its equivalence classes. It is remarkable that all tableaux of shape J are in the same plaque if and only if J is rectangular (i.e., all part of J are equal), a case which appears often in the study of tableaux. In this case we give a formula which links Schensted's correspondence to the product in the symmetric group. In the opposite direction every plaque reduces to

a single tableau if and only if the shape is a hook (i.e., $J = m1^k$). Our main result is that in the set of all permutations provided with the so-called weak Bruhat order, every plaque is an interval having unique extremal elements. Our second main claim is a construction which associates to each plaque a planar configuration describing a partial order on $\mathscr{A}$ on which the set of admissible permutations can be read in a direct manner.

In view of the elementary nature of our considerations we have preferred to give a complete exposition from scratch. Thus our paper includes a (partly) new presentation of Schensted's theory.

2. Jeu de Taquin

In this section we introduce the vocabulary of the *plactic classes* and we prove some basic properties which will be needed in the following sections. We also give an account of the equivalence between plactic classes and *Knuth classes*, although this would not be essential to the comprehension of the paper.

Consider two points $p = (i, j)$ and $p' = (i', j')$ on the discrete plane $Z \times Z$. We write $p \nearrow p'$ if p precedes p' in the natural order, that is to say if $i \leqslant i'$ and $j \leqslant j'$ and we say then that p' lies on the nort-east of p (or equivalently that p lies on the south-west of p'). An *interval* is a subset $\mathscr{I}$ of $Z \times Z$ such that the relation $p \nearrow p' \nearrow p''$ entails $p' \in \mathscr{I}$ when $p, p'' \in \mathscr{I}$. Remark that if an interval has a unique minimal element it may be viewed as the Ferrers diagram of a partition. We also need the similar relation $\searrow$ which is defined in the same manner, except for the exchange of north and south. Thus any two points of $Z \times Z$ are comparable with respect to either $\nearrow$ or $\searrow$ and they are comparable with respect to both if and only if they lie on the same row or on the same column.

If $\mathscr{I}$ is an interval and if $\mathscr{B}$ is a set of integers, an *inscription* s with *content* $\mathscr{B}$ and *domain* $\mathscr{I}$ is an order preserving bijection from $\mathscr{I}$ to $\mathscr{B}$:

$$a \nearrow b \Rightarrow s(a) < s(b).$$

Two inscriptions which differ only by a translation of their domain will be said to represent the same *skew tableau*. If the domain of an inscription is a Ferrers diagram, then the inscription represents a *Young tableau*. Similarly, if the domain of the inscription has a unique maximal element, then the inscription represents a *contretableau*. Trivially, reversing the order $\nearrow$ as well as the natural order on contents exchanges tableaux and contretableaux.

We now define a family of operations τ_p indexed by the points $p \in Z \times Z$ that act injectively on the set of all inscriptions. Since this construction is

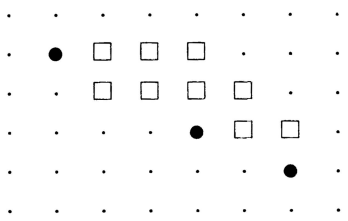
basic to all what follows we describe it with more details than would be strictly necessary. Let w be an inscription with domain $\mathscr{I}$. We set $w\tau_p = w$ unless p satisfies the following three conditions, which characterize what we call a *starting point*:

(1) $p \notin \mathscr{I}$;

(2) $\{p\} \cup \mathscr{I}$ is an interval;

(3) $p \nearrow p'$ for at least one $p' \in \mathscr{I}$.

For instance, if $\mathscr{I}$ consists of the points marked □ in the figure below, $\mathscr{I}$ admits exactly three starting points indicated by the symbol ●



Consider now a starting point p and define its *trail* as the unique maximal sequence $(p_0, .., p_s)$ of $\nearrow$-consecutive points of $\mathscr{I}$ such that, letting $p_0 = p$, the letter x_i lying on p_i in w is the least of the letters lying on the points on the north-east of p_{i-1} $(i = 1, ...)$. By construction, the last point p_s is a $\nearrow$-maximal point of $\mathscr{I}$. Finally we define $w\tau_p$ by moving each letter x_r from p_r to p_{r-1} for $r = 1, ..., s$, with the result that the domain of $w\tau_p$ is the union of $\{p_0\}$ with $\mathscr{I} \setminus \{p_s\}$. In the sequel τ_p will be called the *jeu de taquin* of starting point p, and the moving of x_r will be called a *switch*.

The proofs of the following three remarks are left to the reader.

Remark 1. If $w\tau_p \neq w$, then $w\tau_p$ is the unique inscription w' such that:

(1) its domain contains p and is contained in $\{p\} \cup \mathscr{I}$.

(2) the location of every letter in w' is on the south-west of its location in w.

Remark 2. If $w\tau_p \neq w$, then the inscription w and the point p are completely determined by the data of $w' = w\tau_p$ and of the last point $\bar{p}$ of the trail (which by construction does not belong to the domain of w').

We now have at hand two different jeux de taquin, allowing to move inscriptions towards the south-west or towards the north-east. For the dual version we will use the letter γ instead of τ.

Remark 3. If $\mathscr{A}$ is an interval of the content $\mathscr{B}$ of the inscription w, then there is a point p' such that the restriction of $w\tau_p$ to $\mathscr{A}$ is equal to $w'\tau_{p'}$, where w' is the "restriction" of w to A.

PROPOSITION 1. *If p is a starting point of w and if p' is a starting point of $w\tau_p$ with corresponding final points $\bar{p}$ and $\bar{p}'$ and if one has $p \searrow p'$ (respectively $p' \searrow p$), then one has also $\bar{p} \searrow \bar{p}'$ (respectively $\bar{p}' \searrow \bar{p}$).*

Proof. If the points (i, j) and $(i, j+1)$ (respectively (i, j) and $(i+1, j)$) are on the trail of p, then in case the *cell* $(i-1, j+1)$ (respectively $(i+1, j-1)$) is not empty in $w\tau_p$, the letter occupying the cell (i, j) in $w\tau_p$ is greater than that occupying the cell $(i-1, j+1)$ (respectively $(i+1, j-1)$). This ensures that the trail of p and that of p' do not "properly" cross, whence the result. ∎

Remark that by the same argument if p and p' are starting points of w and if the trails of p and p' (in w) are disjoint, then $w\tau_p\tau_{p'} = w\tau_{p'}\tau_p$.

We also need the following remarks whose proofs are left to the reader.

PROPOSITION 2. *The starting points of any inscription w are completely ordered with respect to $\searrow$. Moreover, if $p \searrow p'$ are starting points of w, then there is at least one point p'' which is a starting point of both $w\tau_p\tau_{p'}$ and $w\tau_{p'}\tau_p$, with $p \searrow p'' \searrow p'$.*

PROPOSITION 3. *By using the jeu de taquin, it is possible to translate any inscription w by one unit, horizontally as well as vertically.*

We consider in more details the case when w, p', and p'' satisfy the conditions of Proposition 2 and the additional condition that the trails corresponding to p and p' are disjoint except for their last point $\bar{p} = \bar{p}'$.

LEMMA 1. *Under the above conditions we have*

$$w\tau_p\tau_{p'}\tau_{p''} = w\tau_{p'}\tau_p\tau_{p''}.$$

Proof. Let (i, j) be the coordinates of $\bar{p} = \bar{p}'$ and let P and P' be the respective trails of p and p'. We may suppose that $(i-1, j)$ is on P and $(i, j-1)$ is on P'. If we erase the letter z in w, obtaining the inscription $\underline{w}$, the endpoints of the trails of p and p' are $(i-1, j)$ and $(i, j-1)$, and τ_p and $\tau_{p'}$ commute, by the remark following Proposition 1. By Proposition 1, the endpoint q of the trail of p'' (in $\underline{w}\tau_p\tau_{p'}$) is such that $(i-1, j) \searrow q$ and $q \searrow (i, j-1)$, whence $q = (i-1, j-1)$ and $w\tau_p\tau_{p'}\tau_{p''} = w\tau_{p'}\tau_p\tau_{p''}$. ∎

THEOREM 1. *If w is an inscription and if $p \searrow p'$ are two starting points of w, then for any starting point p'' of $w\tau_p\tau_{p'}$ lying between p and p' with respect to the order $\searrow$ we have*

$$w\tau_p\tau_{p'}\tau_{p''} = w\tau_{p'}\tau_p\tau_{p''}.$$

Proof. We reason by induction on the cardinality of the domain $\mathscr{I}$ of w. We may suppose that the trails of p and p' intersect. Suppose that the

letter z occupies the first intersection (i, j) of the trails of p and p'. We may suppose that the trail of p contains $(i-1, j) = a$ and that the trail of p' contains $(i, j-1) = b$. Let $\mathscr{J}$ be the interval consisting of the points which are (strictly) on the north-east of a or b. Still, by the above remark and Lemma 1, we may suppose that $\mathscr{I} = \mathscr{J}$, so z is the smallest element of the content of w. If we erase z in $w\tau_a$ or $w\tau_b$, we obtain the same inscription $\underline{w}$. By induction we have $\underline{w}\tau_a\tau_b\tau_c = \underline{w}\tau_b\tau_a\tau_c$, with $c = (i-1, j-1)$. Remark that $\underline{w}\tau_a\tau_b\tau_c$ may be obtained by erasing z in $w\tau_b\tau_a\tau_c$, then applying τ_c. It follows (by induction) that if $w\tau_a\tau_b\tau_c \neq w\tau_b\tau_a\tau_c$, then we may suppose that all integers of $\mathscr{I}$ occupy the same cell in $w\tau_a\tau_b\tau_c$ and $w\tau_b\tau_a\tau_c$ except for the largest element of $\mathscr{I}$, say n, with n occupying the cell $(k-1, l)$ in $w\tau_a\tau_b\tau_c$ and the cell $(k, l-1)$ in $w\tau_b\tau_a\tau_c$. Then (by considering the dual jeu de taquin) n occupies the cell (k, l) in $w\tau_a$ and $w\tau_b$ and the endpoints of the trails of b and a in $w\tau_a$ and $w\tau_b$ are both equal to (k, l). This contradicts Proposition 1, since the endpoints of the trails of a and b in w are also equal. ∎

THEOREM 2 [7]. *For any inscription w, the set of inscriptions that may be deduced from w by a succession of jeux de taquin (respectively dual jeux de taquin) contains one and only one tableau (respectively contretableau).*

Proof. By a preliminary translation we may suppose that w is in the quadrant $N \times N$. It is then easy to "push" w towards the south-west in order to obtain an inscription with the unique minimal point $(0, 0)$. As for the unicity, let us suppose to the contrary that w may be transformed into two different tableaux t and t' by pushing it towards the "corner" of $N \times N$. By considering the sets of inscriptions leading from w to t and to t', we may suppose that these "paths" have no common point except w. We put $t = w\tau_p\Theta$ and $t' = w\tau_{p'}\Theta'$, where p and p' are starting points of w and Θ and Θ' are products of jeux de taquin. Now by the above theorem for some p'' we have $w\tau_p\tau_{p'}\tau_{p''} = w\tau_{p'}\tau_p\tau_{p''} = w'$, unless the distance from w to t is less than 3, in which case there is only one way to push w. It is now easy to reason by induction on the distance from w to t or t': Θ joins $w\tau_p$ to t, so there must be some path joining w' to t; in the same manner there must be some path joining w' to t', a contradiction. The rest of the theorem follows by duality. ∎

We define the *reading* of any inscription w as the word obtained by reading the consecutive rows of w from north to south and from west to east. Similarly, the *column reading* of w is obtained by reading the consecutive columns of w from east to west and from north to south. For instance, the reading and the column reading of $\begin{smallmatrix} 2 & 4 \\ 1 & 3 \end{smallmatrix}\ \begin{smallmatrix} \\ 5 \end{smallmatrix}$ are respectively 2, 4, 1, 3, 5 and 2, 1, 4, 3, 5. We will need the following properties of readings extensively; here $a < b < c$ are consecutive letters of the content of the inscription s, and p is a point in $Z \times Z$.

LEMMA 2. (1) *If ab (or ba) is a subword of the reading w of s, then the same holds for the reading of* $s\gamma_p$.

(2) *If bca is a subword of w, then the same holds for the reading of* $s\gamma_p$.

(3) *If bac is a subword of w and if* $s' = s\gamma_{p_1}\cdots\gamma_{p_k}$, *the following properties are equivalent*:

- *bca is a subword of the reading w′ of s′.*
- *bc is a factor of the reading of* $s\gamma_{p_1}\cdots\gamma_{p_l}$ *for some* $l \leqslant k$.

Proof. Part (1) is left to the reader. If *bca* is a subword of *w*, then by (1), *bca* or *bac* is a subword of $s\gamma_p$. In the latter case we have necessarily $\begin{smallmatrix} c & \cdot \\ a & b' \end{smallmatrix} \to \begin{smallmatrix} \cdot & c \\ a & b' \end{smallmatrix} \to \begin{smallmatrix} a & c \\ \cdot & b' \end{smallmatrix}$ with $a < b' < c$, a contradiction. We suppose now that *bac* is a subword of *w*. If *bca* is a subword of the reading *w′* of $s' = s\gamma_{p_1}\cdots\gamma_{p_k}$, then at some point along the path $s, s\gamma_{p_1}, \ldots, s'$ we have $bac \to bca$ and $\begin{smallmatrix} b' & \cdot \\ a & c \end{smallmatrix} \to \begin{smallmatrix} b' & c \\ a & \cdot \end{smallmatrix} \to \begin{smallmatrix} b' & c \\ \cdot & a \end{smallmatrix}$, with $a < b' < c$; consequently $b' = b$ and *bc* is a factor of the reading of $s\gamma_{p_1}\cdots\gamma_{p_l}$ for some $l \leqslant k$. Inversely, if *b* and *c* "meet" somewhere along the path joining *s* and *s′*, then at this point, say *t*, *bca* is a subword of the reading of *t*; then by (2), *bca* is a subword of the reading of *s′*. ∎

Remark that a dual version of this lemma exists, since the jeu de taquin is symmetrical with respect to the *x*- and *y*-axis.

Considering both the jeu de taquin and its dual version allows us to define an equivalence relation on inscriptions; this relation extends trivially to readings: by definition, two permutations *w* and *w′* belong to the same *plactic class* if they are the respective readings of inscriptions *s* and *s′* which are themselves equivalent. In the sequel this relation will be denoted by the symbol ≡. Remark that the reading and the column reading of any inscription are equivalent, since it is always possible to transform any inscription by sliding its consecutive columns in such a way that the new domain contains at most one point in each row of $Z \times Z$ and that accordingly the new reading coincides with the former column reading. Another classical relation is defined by the equivalences $wbacw' \cong wbcaw'$ and $wacbw' \cong wcabw'$ for any permutation *wbacw′* or *wacbw′* where $a < b < c$ and *w*, *w′* represent factors [4]. Now if *w* is a permutation, let $w\Pi$ and $w\amalg$ represent Schensted's *P*- and *Q*-symbols of *w*, respectively [5]. The interesting fact about this equivalence is that we have $w \cong w' \Leftrightarrow w\Pi = w'\Pi$ [4].

PROPOSITION 4 [7]. *We have* $w \cong w' \Leftrightarrow w \equiv w'$.

Proof. We will use the following lemma:

LEMMA 3. *The reading and the column reading of any inscription are equivalent with respect to* ≅.

Proof. Let $b_l, ..., b_2, b_1$ be the first column of an inscription w. If $b_2, a_1, ..., a_k$ is the row containing b_2, the reading of w contains the factor $b_2, a_1, ..., a_k, b_1$; by using the equivalences defined above, we can switch the letter b_1 to the "left" until it lies next to b_2. In other words, it is possible to "pull out" the first column of the reading of any inscription with two rows. The lemma follows by an easy induction, remarking that it is then possible to pull out b_3, b_2, b_1 in the same way, etc. ▮

We can now make the following useful remarks:

(1) Suppose there is a row immediately "below" that containing b_1 whose first letter c is smaller than b_1; then it is possible to pull out not only the first column of w, but the whole sequence $b_l, ..., b_1, c$ in exactly the same manner.

(2) A dual operation consists in pulling out (from the right side) the last row of the column reading of w, and as above, if the last row of w is $c_1, ..., c_m$ and if the row above that starts with the letter $c < c_1$, then it is possible to pull out the sequence $c, c_1, ..., c_m$ from the column reading of w.

We wish to prove that $w\tau_p \cong w$. Suppose that p is a starting point of w. If p does not precede the whole domain of w (with respect to $\nearrow$), it is easy to conclude by induction on the number of letters in w, using the above lemma. In the other case we may suppose that the first column of w is $b_l, ..., b_1$ and that the last row of w is $c_1, ..., c_m$, with the cell p just below b_1 and just on the left of c_1. If $c_1 < b_1$, then we can pull out the sequence $b_l, ..., b_1, c_1$ from the reading of w. Remarking that this sequence is exactly the first column of $w\tau_p$, we conclude by induction, still using the above lemma. If $b_1 < c_1$, it suffices to use a dual reasoning. It follows that we have $w \equiv w' \Rightarrow w \cong w'$. Now let $w = w_0, ..., w_n$ be a permutation containing the factor bac with $a < b < c$. By placing the letter w_0 in the cell $(0, n)$, the letter w_1 in the cell $(1, n-1)$, ..., the letter w_n in the cell $(n, 0)$ we obtain a inscription whose reading (or column reading) is w (this inscription will be said to be *canonical*). By considering the canonical inscription of w we see that the relation $\equiv$ applied to any factor of w extends to w. It follows that the easily checked relation $bac \equiv bca$ implies $w \equiv (a, c)w$ where $(a, c)w$ denotes the permutation obtained by transposing the letters a and c in w. In the same way, if w contains the factor acb, then $w \equiv (a, c)w$. It follows that $w \cong w' \Rightarrow w \equiv w'$, which concludes the proof of the proposition. ▮

3. Admissible Permutations, Plaques, Plaque Order

We remind the reader that the *descent set* of the permutation w in $\mathcal{S}_n$ is the set $\{i, 1 \leqslant i \leqslant n-1, w(i) > w(i+1)\}$. If W is a subset of the symmetric

group $\mathscr{S}_n$ we say that a permutation σ is *admissible* for W if and only if w and σw have the same descent set for every w in W. In what follows we consider the elements of $\mathscr{S}_n$ as (standard) words in the letters of $\mathscr{A} = \{1 < 2 < \cdots < n\} = [1, n]$.

DEFINITION 1. The *plaque order induced by* W is the least order $\leqslant_W$ on $\mathscr{A}$ such that for all a, b in $\mathscr{A}$ one has $a \leqslant_W b$ if $a < b$ and if ab or ba is a factor of a least one w in W.

We let $\mathscr{G}_W$ be the graph of $\leqslant_W$ and we denote by $\sigma\mathscr{G}_W$ the image of $\mathscr{G}_W$ by any permutation σ acting on A.

PROPOSITION 5. *For any* $W \subseteq \mathscr{S}_n$, *the permutation* σ *is admissible for* W *if and only if we have* $\mathscr{G}_{\sigma W} = \sigma\mathscr{G}_W$.

Proof. Let $\sigma = s_p s_{p-1} \cdots s_1$ be a reduced expression, meaning that the s_i's are of the form $s_i = (k, k+1)$, $1 \leqslant k \leqslant n-1$, with p minimum. By reasoning by induction on p, it is easy to see that for i, j in $[1, n]$, if $w(i) < w(j)$ and $\sigma w(i) < \sigma w(j)$, then for any k $(1 \leqslant k \leqslant p)$ we have also $s_k \cdots s_1 w(i) < s_k \cdots s_1 w(j)$, a property that holds for any Coxeter group [9]. The following two lemmas are direct consequences of this fact.

LEMMA 4. *With* σ *as above,* σ *is admissible for* W *if and only if* s_1 *(respectively* $s_2, \ldots, s_p$*) is admissible for* W *(respectively* $s_1 W, s_2 s_1 W, \ldots, s_{p-1} \cdots s_1 W$*).*

LEMMA 5. *If* G *is a graph whose vertices are the letters* $1, 2, \ldots, n$, *then* σ *preserves the orientation of* G *(meaning that for any edge* (i, j) *we have* $i < j \Leftrightarrow \sigma(i) < \sigma(j)$*) if and only if* s_1 *(respectively* $s_2, \ldots, s_p$*) preserves the orientation of* G *(respectively* $s_1 G, s_2 s_1 G, \ldots, s_{p-1} \cdots s_1 G$*).*

If $\sigma = (i, i+1)$, then w and σw have the same descent set for any w in W if and only if $i \leqslant_W i+1$ does not hold, so the result is verified in this case. By Lemmas 4 and 5 the proposition follows by induction on p. ∎

In the same way we have:

PROPOSITION 6. *For any* W *in* $\mathscr{S}_n$, σ *is admissible for* W *if and only if* σ *preserves the orientation of* $\mathscr{G}_W$.

THEOREM 3. *If* W *is a plactic class, then* σ *is admissible for* W *if and only if for any* w *in* W *we have*

$$(\sigma w)\Pi = \sigma(w\Pi); \qquad (\sigma w)\amalg = w\amalg.$$

Proof. By induction we may suppose that $\sigma = (i, i+1)$. In this case the first formula is trivially verified. For any w in W, the letters i and $i+1$ cannot become adjacent along the bumping process of w, whence the second formula. If σ is not admissible for W, then there exists at least one element of W containing the factor $i, i+1$ or $i+1, i$. Suppose for instance that w contains the factor $i, i+1$, with $w(j) = i$ and $w(j+1) = i+1$. If the formulas are verified, then we have $w^{-1}\Pi = (w^{-1}\sigma)\Pi$, but since w^{-1} contains the factor $j, j+1$ and $w^{-1}\sigma$ contains the factor $j+1, j$, this contradicts Lemma 2. ▮

Remark that by Theorem 3, if W is a plactic class with σ admissible for W, then σW is a plactic class.

4. Plaques and Weak Bruhat Order

Definition 2. If W is a plactic class and if σ is admissible for W, then W and σW belong to the same plaque.

We will prove now that the plaques are intervals with respect to the weak Bruhat order $\leqslant_B$. We remind the reader that this order is defined tansitively by the relation $\forall w \in \mathcal{S}_n$, $w \leqslant_B (i, i+1)w \Leftrightarrow w^{-1}(i) < w^{-1}(i+1)$ (cf. [1]). Let $\mathcal{I}(w)$ be the set $\{(i, j),\ 1 \leqslant i < j \leqslant n,\ w(i) < w(j)\}$; w is completely determined by $\mathcal{I}(w)$, and we have the characterization $w \leqslant_B w' \Leftrightarrow \mathcal{I}(w) \supseteq \mathcal{I}(w')$ (cf. [1]), which implies that the set of Young tableaux of a given shape is an interval with respect to $\leqslant_B$ (identifying tableaux with their readings). In the sequel this identification is left to the reader, whenever necessary. We suppose that W is a plactic class of tableau T and contretableau T^c.

Theorem 4. *With respect to the weak Bruhat order every plaque is an interval having a unique maximal element and a unique minimal element.*

Proof. If $s = (i, i+1)$ is admissible for the plactic class W, then for every w in W we have $sw \leqslant_B w$ or else for every w in W we have $w \leqslant_B sw$, so we can write $W \leqslant_B sW$ or $sW \leqslant_B W$.

Lemma 6. *If $sW \leqslant_B W$ and $tW \leqslant_B W$ with $s = (i, i+1)$, $t = (j, j+1)$, $i < j$, then*

- *if $j > i+1$, s and t commute and we have $tsW \leqslant_B sW$ and $stW \leqslant_B tW$.*
- *if $j = i+1$, $sts = tst$ and we have $stsW \leqslant_B tsW \leqslant_B sW$ and $tstW \leqslant_B stW \leqslant_B tW$.*

Proof. Left to the reader. ▮

Now let us suppose that σ is admissible for W. By Lemma 4, it is possible to construct a path from W to σW that stays in the same plaque. Suppose such a path contains the factor $sW' \leqslant_B W' \geqslant_B tW$. By the above lemma it is always possible to "lower" that portion of the path, and by iterating this process we conclude that there exists a plactic class W'' in the plaque of W with $W'' \leqslant_B W$ and $W'' \leqslant_B \sigma W$. ∎

We will now study the order $\preccurlyeq_W$, and particularly its graph $\mathscr{G}_W$. The study will lead to an alternative proof of Theorem 4. A byproduct will be an efficient algorithm for the computation of the plaque of a given plactic class. The following reduction theorem is the first step towards this end. Remark that since every plactic class contains one and only one tableau, we may as well adopt the notation $\mathscr{G}(T)$ for $\mathscr{G}_W$.

THEOREM 5. *For any path $C = t, t\gamma_1, ..., t\gamma_p = u$ joining an inscription t representing T to an inscription u representing T^c, the orders $\preccurlyeq_W$ and $\preccurlyeq_C$ are identical (identifying C with the set of readings of the inscriptions contained in C).*

Proof. In turns we will need the two lemmas below.

LEMMA 7. *With the notations above, we have*

$$i \preccurlyeq_W i+1 \Leftrightarrow i \preccurlyeq_C i+1 \qquad (1 \leqslant i \leqslant n-1).$$

Proof. We may suppose that i and $i+1$ are adjacent for neither t nor u. By symmetry around the axes we may suppose that $i, i+1$ is a subword of the reading of t. Let us erase from t the letters $1, 2, ..., i+1$. There exists an inscription t' with content $\{i-1, i, ..., n\}$ such that the restriction of t' to $i, i+1, ..., n$ is t and the reading of t' has $i, i-1, i+1$ as a subword. Now the jeux de taquin used along C provide a path C' joining t' to u', with t' representing some tableau T' and u' representing T'^c. From Lemma 2, $i, i+1$ is a factor of some inscription in C' if and only if $i, i+1, i-1$ is a subword of the reading of u'. Remark that i and $i+1$ are adjacent for some inscription of C if and only if the same holds for C'. It follows that for any two paths C_1 and C_2 joining t to u, we have $i \preccurlyeq_{C_1} i+1 \Leftrightarrow i \preccurlyeq_{C_2} i+1$. Now let s be an inscription in W such that there exists a path C_1 joining t to s and let r be an inscription representing T^c which is on the north-east of both s and u and has no common cell with them. There exists certainly a path C_2 joining s to r and a path C_3 joining u to r and such that the elements of C_3 are obtained from u by a sequence of translations of rows and columns. Remark that we have $\preccurlyeq_{C_3} = \preccurlyeq_u$. Now, we have $i \preccurlyeq_{C_1 \cup C_2} i+1 \Leftrightarrow i \preccurlyeq_{C \cup C_3} i+1 \Leftrightarrow i \preccurlyeq_C i+1$, whence Lemma 7. ∎

We use the notation $i \not\preccurlyeq_C j$ *if* $i \preccurlyeq_C j$ does not hold.

LEMMA 8. *Let t, u, C be as above. If $i \leqslant_C j$, then there exists an admissible permutation σ for W with a reduced expression $\sigma = s_p \cdots s_1$ such that for some k $(i \leqslant k \leqslant j-1)$ we have*

$$\sigma(i) = k, \qquad \sigma(j) = k+1, \qquad \sigma(l) = l \quad \text{if } l < i \text{ or } l > j.$$

Proof. We will reason by induction on $j-i$. Suppose that $i \not\leqslant_C j$ with $j-i>1$. If $i \not\leqslant_C i+1$, then by Lemma 7, $i \not\leqslant_W i+1$ and $s=(i, i+1)$ is admissible for W. Since $s(j)-s(i)=j-i-1$, the proposition holds true by induction. We suppose now that $i \leqslant_C i+1$, which implies that $i+1 \not\leqslant_C j$. Let σ' be a product promised by the lemma for the pair $(i+1, j)$. If $\sigma'(j)<j$, we can conclude by induction, since $\sigma'(i)=i$. If not then $\sigma'(j)=j$, so $\sigma'(i+1)=j-1$. We have $j-1 \not\leqslant_{\sigma' C} j$, so by Lemma 7, $j-1 \not\leqslant_{\sigma' W} j$ and the product $\sigma=(j-1, j)\sigma'$ is admissible for W. We have $\sigma(i)=i$ and $\sigma(j)=j-1$, so induction applies in this case also. ∎

We can now conclude the proof of Theorem 5: supposing that $i \not\leqslant_C j$, let C, t, u, $\sigma = s_p \cdots s_1$ and k be as above. Since the product σ is admissible for W, σC is a path joining σt to σu. We have $k \not\leqslant_{\sigma C} k+1$, so by Lemma 7, $k \not\leqslant_{\sigma W} k+1$; it follows that $i \not\leqslant_W j$. ∎

If a and b are letters written on the plane with coordinates x_a, y_a and x_b, y_b, we put $a \downarrow b$ if $x_a < x_b$ and $y_a > y_b$. From now on we identify T with the inscription representing T such that the letter 1 lies on the point (1, 1). If $a_1 > \cdots > a_p$ is the shape of T, we identify T^c with the inscription representing T^c such that the letter n lies on the point (a_1, p). Let C be a path joining T to T^c. By Theorem 5, we have $\leqslant_W = \leqslant_C$. We can write $C=(T_0, T_1, \ldots, T_k)$ with $T_0=T$, $T_{i+1}=T_i\gamma_{x_i}$ $(0 \leqslant i \leqslant k-1)$, $T_k=T^c$. We denote by $\mathcal{T}_{0,i}=T_i, \mathcal{T}_{1,i}, \ldots, \mathcal{T}_{n_i,i}=T_{i+1}$ the consecutive "tableaux with a blank" which allow us to pass from T_i to T_{i+1} through a sequence of elementary switches. The blank of T_i is by convention the starting point of T_i. We denote by C_i the word $\mathcal{T}_{0,i}, \mathcal{T}_{1,i}, \ldots, \mathcal{T}_{n_i-1,i}$ and by C' the word $C_0, C_1, \ldots, C_{k-1}, T^C$; C' will be called the *detailed path* of C. For example, if $T=\begin{smallmatrix}3\\1&2&4\end{smallmatrix}$, then

$$C=\begin{pmatrix}3 & \cdot & \cdot & 1 & 3 & \cdot & 1 & 3 & 4\\ 1 & 2 & 4' & \cdot & 2 & 4' & \cdot & \cdot & 2\end{pmatrix}$$

$$C'=\begin{pmatrix}3 & \bullet & \cdot & \bullet & 3 & \cdot & 1 & 3 & \bullet & 1 & 3 & 4 & 1 & 3 & 4\\ 1 & 2 & 4' & 1 & 2 & 4' & \cdot & 2 & 4' & \cdot & 2 & \bullet' & \cdot & \cdot & 2\end{pmatrix},$$

where the sign $\bullet$ stands for blanks. For sake of simplicity let us relabel the elements of C': $C'=C'_1, \ldots, C'_q$. We put $D_l=\{C'_1, \ldots, C'_l\}$ for $1 \leqslant l \leqslant q$. We have $\leqslant_{C'} = \leqslant_{D_q} = \leqslant_W$, so $\mathcal{G}_{D_q}=\mathcal{G}(T)$. We will use the notation $\mathcal{G}_l$ for $\mathcal{G}_{D_l}$.

THEOREM 6. *It is possible to draw the graph $\mathcal{G}(T)$ on the plane in such a way that*:

(1) *$\mathcal{G}(T)$ is planar.*

(2) *The vertices of $\mathcal{G}(T)$ are drawn on $N \times N$.*

(3) *If $i<j$ are consecutive with respect to $\preccurlyeq_W$, then the edge(i, j) is either vertical or horizontal and ij or (respectively) ji is a subword of some element of W.*

(4) *$i \nearrow j$ on $\mathcal{G}(T)$ if and only if $i \preccurlyeq_W j$.*

(5) *If $i \downarrow j$ on $\mathcal{G}(T)$, then ij is a subword of any element of W.*

Proof. Parts (3) and (5) are equivalent to (3′) and (5′):

• (3′) If $i<j$ are consecutive with respect to $\preccurlyeq_W$, then the edge (i, j) is either horizontal or vertical and ij or (respectively) ji is a subline or (respectively) a subcolumn of some element of $C' = D_q$.

• (5′) If $i \downarrow j$ on $\mathcal{G}(T)$, then $i \downarrow j$ for any element of $C' = D_q$.

The following proof by induction yields an algorithm in q steps to construct $\mathcal{G}(T)$.

We suppose that (1), (2), (3′), (4), (5′), are verified when replacing $\mathcal{G}(T)$ by $\mathcal{G}_l$ and W and D_q by D_l $(1 \leqslant l \leqslant q-1)$. If $\preccurlyeq_{D_{l+1}} \neq \preccurlyeq_{D_l}$, then the blank of C'_l has an immediate left neighbour (say j) and an immediate bottom neighbour (say i). Suppose first that $j>i$. The lth switch moves j on top of i, and we have $i \not\preccurlyeq_{D_l} j$ an $i \preccurlyeq_{D_{l+1}} j$,

$$\begin{array}{cc} j & \bullet \\ \cdot & i \end{array} \rightarrow \begin{array}{cc} \bullet & j \\ \cdot & i \end{array}$$

$$C'_l \rightarrow C'_{l+1}$$

(α) Let $\preccurlyeq_{i,j}$ be the order defined by the single relation $i \preccurlyeq_{i,j} j$. The order $\preccurlyeq_{D_{l+1}}$ is the transitive closure of the union $\preccurlyeq_{D_l} \cup \preccurlyeq_{i,j}$. It follows that i and j are consecutive with respect to $\preccurlyeq_{D_{l+1}}$.

(β) If for some x we have $j \downarrow x \downarrow i$ on $\mathcal{G}_l$, then by (5′) $j \downarrow x \downarrow i$ for any element of D_l; in particular $j \downarrow x \downarrow i$ on C'_l, a contradiction.

(γ) If $\mathcal{G}_l$ has a vertical edge (x, j) with $x<j$, then by (3′), x and j are consecutive with respect to $\preccurlyeq_{D_l}$ and there is an element C'_r of D_l for which jx is a subcolumn. For $r \leqslant v \leqslant l$, either C'_v contains the subcolumn jx or $j \downarrow x$ since if not we would have for some w, $r \leqslant w \leqslant l-1$,

$$\begin{array}{cc} j & \bullet \\ x & y \end{array} \rightarrow \begin{array}{cc} \bullet & j \\ x & y \end{array}$$

$$C'_w \rightarrow C'_{w+1}$$

and $x \preccurlyeq_{D_l} y \preccurlyeq_{D_l} j$, a contradiction. Keeping track of the respective locations of i, j, x along D_l, we conclude that we have necessarily $x \preccurlyeq_{D_l} i$, and finally $x \nearrow i$ on $\mathcal{G}_l$ (by 4).

(δ) Let us consider in $\mathcal{G}_l$ the rectangle with horizontal and vertical sides and ji as a diagonal:

$$\begin{array}{ccccc} j & \square & \cdots & \square & \eta) \\ \square & \diamond & \cdots & \diamond & \square \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \square & \diamond & \cdots & \diamond & \square \\ \zeta) & \square & \cdots & \square & i \end{array}$$

By (β), the region marked $\diamond$ on the above figure is empty and by (γ) the left side of the rectangle is empty, except for j and possibly for the cell ζ. In a similar way it is easy to check that the other sides are also empty, except for i and possibly for the cell η.

Now let us erase the edges of $\mathcal{G}_l$, and define the set X_l as the set of vertices x of $\mathcal{G}_l$ such that ($j \nearrow x$) or ($i \nearrow x$ and $i \neq x$) or $i \downarrow x$. By translating X_l to the right until j lies above i, we obtain a set of points Y_l which by (δ) and (4) has the following property: $x \preccurlyeq_{D_{l+1}} y$ if and only if $x \nearrow y$ on Y_l. We state that if we create an edge between each pair of points in Y_l lying on the same row or on the same column, we obtain the graph of $\preccurlyeq_{D_{l+1}}$ and that this graph verifies all the required properties. This can be checked by reasoning by cases. In case we have $z \nearrow j$ on $\mathcal{G}_l$ with z on the north-west of the cell ζ, then the last edge of every path joining z to j on $\mathcal{G}_l$ is horizontal, so moving j does not create any difficulty. The other cases are easy. Finally, if $j < i$ a similar construction applies, and the case $l = 1$ is trivial, which concludes the proof. ∎

The mechanism of the proof allows us to derive a fast algorithm for constructing $\mathcal{G}(T)$ (see Fig. 1 for an example of computation). Remark that it follows from the theorem that $\preccurlyeq_W$ is a lattice order, and that $(i, i+1)$ is admissible for W if and only if i and $i+1$ are not comparable with respect to $\nearrow$ on $\mathcal{G}(T)$.

We give now an alternative proof of Theorem 4 which yields an algorithm for the computation of plaques. We denote by $\mathcal{G}(\mathcal{P})$ the graph obtained from $\mathcal{G}(T)$ by erasing the labels $1, 2, \ldots, n$ on its vertices. This notation is valid because by Proposition 6 the set $\mathcal{P}^* = \{\mathcal{G}(R), R \in \mathcal{P}\}$ is the set of those labellings L of $\mathcal{G}(P)$ sucht that we have ($i \nearrow j$ on $L \Rightarrow i < j$).

We call *column graph* (respectively *row graph*) of $\mathcal{G}(\mathcal{P})$ and we denote by $\mathcal{G}_1$ (respectively $\mathcal{G}_2$) the labelling in $\mathcal{P}^*$ such that if $i \downarrow j$ on $\mathcal{G}_1$ (respectively

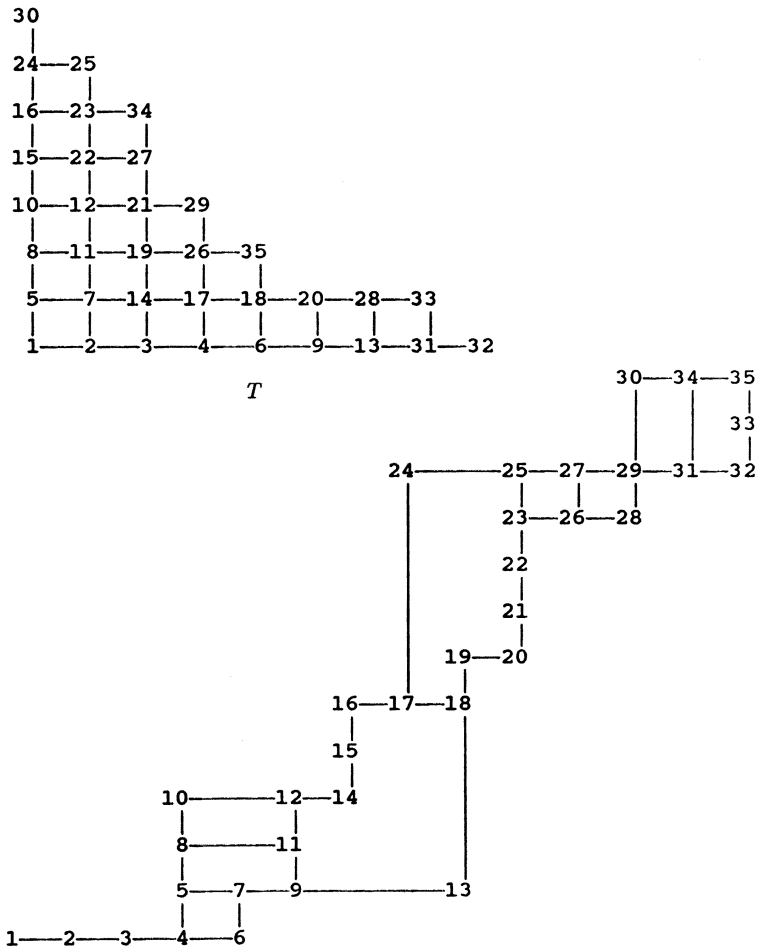


FIG. 1. The graph $\mathscr{G}(T)$.

$\mathscr{G}_2$), then $i<j$ (respectively $j<i$); $\mathscr{G}_1$ and $\mathscr{G}_2$ are uniquely determined by these conditions because the inversions of their reading permutations are completely defined, so these permutations are themselves uniquely determined. Let g_1, g_T, g_2 be the readings of $\mathscr{G}_1, \mathscr{G}(T), \mathscr{G}_2$. Since $\mathscr{I}(g_1)\subseteq\mathscr{I}(g_T)\subseteq\mathscr{I}(g_2)$, we have $g_1\leqslant_B g_T\leqslant_B g_2$. Let σ_1 and σ_2 be the permutations such that $g_1=\sigma_1 g_T$ and $g_2=\sigma_2 g_T$; σ_1 and σ_2 are admissible for W and we have $\sigma_1 T\leqslant_B T\leqslant_B \sigma_2 T$, by induction. Now suppose that $w\in\mathscr{S}_n$ is such that $\sigma_1 T\leqslant_B w\leqslant_B \sigma_2 T$. By Lemma 5, w is a tableau of same shape as T, and by Lemma 4, w is in $\mathscr{P}$, which concludes the proof. ∎

As claimed, this proof provides an algorithm for computing the plaque of a given Young tableau. For example, if

$$T = \begin{array}{cccc} 9 & & & \\ 6 & 8 & & \\ 2 & 5 & 10 & \\ 1 & 3 & 4 & 7 \end{array} \qquad \text{then } \mathcal{G}(T) = \begin{array}{ccccc} & & & & 9-10 \\ & & & & | \\ & & & 6 & -- 8 \\ & & & | & \quad | \\ & & & | & 5-7 \\ & & & | & \quad | \\ & & 2-3-4 & & \\ & & | & & \\ & & 1 & & \end{array}$$

$$\mathcal{G}_1 = \begin{array}{ccccc} & & & & 9-10 \\ & & & & | \\ & & & 4 & -- 8 \\ & & & | & \quad | \\ & & & | & 6-7 \\ & & & | & \quad | \\ & & 2-3-5 & & \\ & & | & & \\ & & 1 & & \end{array} , \qquad \mathcal{G}_2 = \begin{array}{ccccc} & & & & 9-10 \\ & & & & | \\ & & & 7 & -- 8 \\ & & & | & \quad | \\ & & & | & 5-6 \\ & & & | & \quad | \\ & & 2-3-4 & & \\ & & | & & \\ & & 1 & & \end{array} ,$$

and $\sigma_1 = (4, 5)(5, 6)$, $\sigma_2 = (6, 7)$, so

$$\sigma_1 T = \begin{array}{cccc} 9 & & & \\ 4 & 8 & & \\ 2 & 6 & 10 & \\ 1 & 3 & 5 & 7 \end{array} \qquad \text{and} \qquad \sigma_2 T = \begin{array}{cccc} 9 & & & \\ 7 & 8 & & \\ 2 & 5 & 10 & \\ 1 & 3 & 4 & 6 \end{array} ,$$

and the plaque of T is the interval $\{(9, 4, 8, 2, 6, 10, 1, 3, 5, 7), (9, 7, 8, 2, 5, 10, 1, 3, 4, 6)\}$. Figure 2 contains the plaques corresponding to the shape 3, 3, 1.

If P is a Young tableau then $P\mathrm{II} = I$ depends on the shape of P only. In particular $I\Pi = \Pi I$, so I is an involution [6]; I is in fact the only Young tableau of same shape as P which is an involution, and it can be obtained by an easy algorithm.

PROPOSITION 7. *Let P, Q, and I be Young tableaux of same shape, with I as above. Then if P or Q is in the plaque of I, we have*

$$(P \cdot I \cdot Q^{-1})\Pi = P \qquad \textit{and} \qquad (P \cdot I \cdot Q^{-1})\mathrm{II} = Q.$$

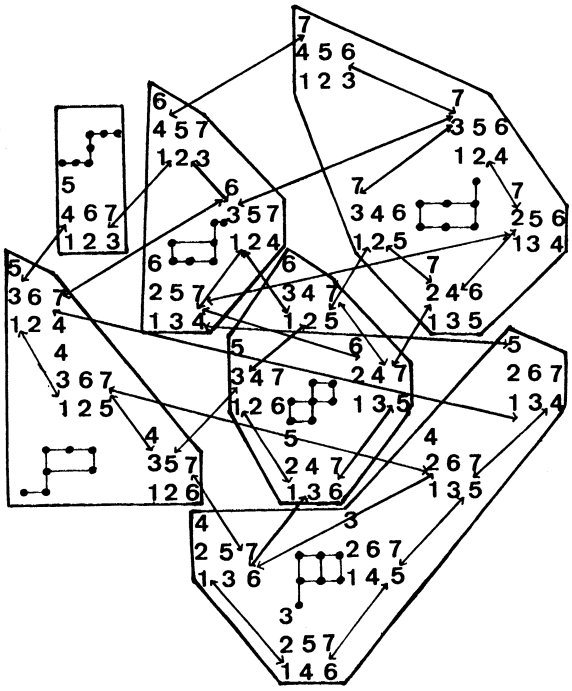


FIG. 2. The plaques of shape 3, 3, 1.

Proof. Suppose for instance that P is in the plaque of I, and let σ be the permutation such that $\sigma I = P$. We have $Q^{-1}\Pi = I$, $Q^{-1}\amalg = Q$ [6], and Theorem 3 allows us to conclude. ∎

In the case the shape of P is rectangular the proposition has a startling corollary:

THEOREM 7. *If P and Q are rectangular tableaux of same shape, then*

$$(P \cdot I \cdot Q^{-1})\Pi = P \qquad \text{and} \qquad (P \cdot I \cdot Q^{-1})\amalg = Q.$$

Proof. It suffices to remark that $P = P^c$, so by Theorem 5, P, I, and Q are necessarily in the same plaque. ∎

Remark that in the rectangular case, I has a particularly simple form, since it is the top element of the set of tableaux of that shape, or *hyper-standard* tableau. For example, if $P = \begin{smallmatrix} 2 & 5 & 6 \\ 1 & 3 & 4 \end{smallmatrix}$ and $Q = \begin{smallmatrix} 3 & 4 & 6 \\ 1 & 2 & 5 \end{smallmatrix}$, then $I = \begin{smallmatrix} 4 & 5 & 6 \\ 1 & 2 & 3 \end{smallmatrix}$ and $P \cdot I \cdot Q^{-1} = (256134)(456123)(451263) = (251364)$.

PROPOSITION 8. *The set of all tableaux of a given shape form a plaque if and only if that shape is rectangular.*

Proof. It remains to verify that the tableaux of a non-rectangular shape decompose into more than one plaque. The domain corresponding to such a shape contains necesseraly two cells $a-1$, b and $a, b-1$ with a, b a starting point for the (dual) jeu de taquin. It is then easy to construct a tableau of that same shape containing two consecutive letters i and $i+1$ in those two cells. Now for that particular tableau the transposition $(i, i+1)$ is not admissible. ▮

Another extremal situation is met when the shape is a hook (see the Introduction), in which case every tableau makes up a plaque of its own.

PROPOSITION 9. *For a given shape, every plaque is reduced to one element if and only if the shape is a hook.*

Proof. If the shape of a tableau is a hook, then no transposition $(i, i+1)$ may be admissible, by an easy induction. Inversely, given a shape that is not a hook, there exists a tableau of that particular shape containing the subword 342, and by Lemma 2(2) and Theorem 5, if a tableau contains the subword *bca*, then *ab* is admissible (with the notations of Lemma 3). ▮

EXAMPLES. (1) *The graph* $\mathcal{G}(T)$. Figure 1 contains an example of the graph $\mathcal{G}(T)$.

(2) *Plaques and permutohedron.* The graph of the weak Bruhat order is sometimes called *permutohedron*. Figure 2 represents the subinterval of the permutohedron of $\mathcal{S}_7$ consisting of the Young tableaux of shape 3, 3, 1. Within every plaque $\mathcal{P}$ the graph $\mathcal{G}(\mathcal{P})$ is represented.

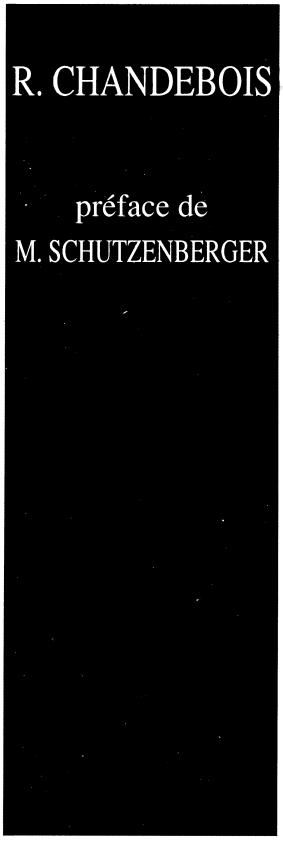
REFERENCES

1. A. BJÖRNER, Orderings of Coxeter groups, *in* "Contemporary Mathematics," Vol. 34, Birkhäuser, Boston, 1984.
2. D. KAZHDAN AND G. LUSZTIG, Representations of Coxeter groups and Hecke algebras, *Invent. Math.* **55** (1979).
3. Deleted in proof.
4. D. KNUTH, Permutation matrices and Young tableaux, *Pacific J. Math.* **34**, No. 3, 1970.
5. C. SCHENSTED, Longest increasing and decreasing subsequences, *Canad. J. Math.* **13** (1961).
6. M.-P. SCHÜTZENBERGER, Quelsques remarques sur une construction de Schensted, *Math. Scand.* **12** (1963).

7. M.-P. SCHÜTZENBERGER, La correspondance de Robinson, *in* "Combinatoire et représentation du groupe symétrique," Lecture Notes in Mathematics, Vol. 579, Springer-Verlag, Berlin, 1977.
8. D. STANTON, (Ed.), Invariant theory and Young tableaux, *in* "The IMA Volumes in Mathematics and Its Applications," Vol. 19, Springer-Verlag, Berlin, 1990.
9. J. TITS, Buildings of spherical type and finite *BN*-pairs, *in* "Lecture Notes in Mathematics," Vol. 386, Springer-Verlag, Berlin, 1974.

POUR EN FINIR AVEC LE DARWINISME

une nouvelle logique du vivant



Editions espaces 34

PRÉFACE

Et aussi avec Charles Darwin

Il paraît tous les ans plusieurs livres consacrés au darwinisme que l'on présente comme un acquis de la science aussi indubitable que la théorie atomique ou la fonction glycogénique du foie. On y chercherait en vain des réponses aux multiples critiques que des générations de naturalistes ont opposées à ces thèses. Au mieux les contradicteurs sont ridiculisés par quelque anecdote spirituelle. Au pire, on les accuse de « faire le jeu » d'un Grand Satan du jour. Le plus souvent ce sera le silence. Ainsi la bibliographie d'un très récent Traité dont je respecte l'auteur contient une douzaine de références à P. Grassé. Mais, allant au texte, le lecteur s'aperçoit que ce ne sont que des renvois insignifiants et il ne verra même pas mentionnés les puissants arguments contre le darwinisme développés par celui qui fut l'un des maîtres de la zoologie contemporaine dans son grand livre, *l'Evolution du vivant*. Non pas que ces critiques et d'autres plus anciennes aient été invalidées par les progrès des connaissances. Au contraire. Mais il est plus facile de les oublier que d'y répondre. Elles proviennent de toutes les disciplines des sciences de la vie. Les plus connues ont été formulées par les paléontologistes mais les plus graves bien que plus discrètes sont dues aux embryologistes. C'est l'immense mérite du livre du Professeur Chandebois que de les rassembler et de les enrichir grandement avec la compétence que lui confère une fructueuse carrière de chercheur.

*
* *

De quoi s'agit-il ? La thèse fondamentale commune aux diverses versions actuelles du darwinisme est que l'évolution des êtres vivants résulte du seul hasard filtré par la sélection naturelle. Et pour convaincre on multiplie les exemples mineurs qui ne prouvent rien quant au fond de la question. Nul en effet n'a assez mauvais cœur pour nier que la sélection puisse avoir des effets importants. Il n'est pas besoin de Darwin pour savoir que la désertification d'une zone en fera d'abord disparaître celles

des variétés végétales qui ont le plus besoin d'eau. Mais ceci n'explique pas la genèse des particularités anatomiques et physiologiques dont sont douées les xérophytes et ne justifie en rien qu'on en attribue l'origine au seul hasard. On a élaboré des récits touchants à l'usage des enfants des écoles. Voyez l'histoire des chevaux. Ils ont commencé par être de petites créatures grosses comme des lapins. Celles qui avaient la chance d'être nées un peu plus grandes couraient plus vite et échappaient ainsi à la dent des méchantes bêtes qui voulaient les manger. Elles avaient donc plus de descendants et c'est ainsi, dit-on, que, progressivement, au long de milliers de siècles, les chevaux ont atteint leur taille actuelle. L'emploi de termes plus savants permet d'éviter les questions que les enfants ne doivent pas poser, c'est-à-dire d'avoir à fournir l'énoncé explicite des hypothèses sans lesquelles la valeur probante de cette histoire est nulle. Par exemple, comment sait-on :

– Que la capture par un prédateur est une cause importante et constante d'une moindre fécondité ?

– Que la réduction de sa probabilité est fortement liée à la vitesse de fuite et celle-ci à la taille ?

– Que l'augmentation de la taille n'a pas de conséquences subsidiaires telles que l'accroissement des besoins alimentaires, qui compensent son effet final sur la fécondité ?

– Que d'autres modifications (un autre mode de vie, une meilleure vigilance, un goût exécrable de la viande, etc, etc.) n'interagissent pas avec le facteur sélectif choisi et brouillent son action ? etc, etc.

Manifestement rien de ceci n'est vérifiable et la réponse aux questions ne saurait être que la récitation d'une série d'exemples à laquelle pourrait être opposée une autre série tout aussi convaincante (et d'ailleurs utilisée quand il s'agit d'« expliquer » le plafonnement de la taille). La controverse dégénérant en un échange d'anecdotes, l'orateur darwinien aurait à conclure son discours par l'assertion tautologique que ces objections doivent être écartées puisque les chevaux sont plus grands aujourd'hui que jadis (quand ils n'étaient pas encore des chevaux).

J'ouvre ici une parenthèse pour marquer par un exemple que ce n'est pas le schéma logique du raisonnement ni son statut métaphysique que récusent les savants soucieux de la rigueur vers laquelle on tend dans les autres domaines de la nature.

La situation est abstraitement analogue mais de fait toute différente pour le mécanisme généralement admis de la synthèse des noyaux atomiques à l'intérieur des étoiles et des supernovae. C'est pourtant un processus que l'on pourrait qualifier de darwinien. Le choc (aléatoire) des particules produit des noyaux de plus en plus gros et les différents modes de désintégrations radioactives (encore le hasard) déterminent la fréquence ultime des espèces atomiques et de leurs isotopes compte tenu de leur stabilité. Les physiciens et les cosmologistes ont la chance de pou-

voir tester leurs hypothèses et déterminer ou calculer avec assez de précision les paramètres en cause pour que ce modèle soit tout autre chose qu'un système conjectural. Il n'en est pas de même en biologie mais il serait paradoxal de considérer comme un garant de la véracité de la théorie néo-darwinienne la seule et pure impossibilité d'en apporter la preuve ! Une théorie s'appelle une hypothèse tant qu'elle n'a d'autre argument que le charme de sa rhétorique.

Or le darwinisme est surtout un genre littéraire. Il est né en Angleterre comme le roman policier, et tout l'art est de dissimuler les invraisemblances que requiert l'enchaînement des épisodes. Un auteur fort réputé est R. Dawkins dont les amateurs ont apprécié l'explication de l'absence d'un os pénien chez l'homme. Les lecteurs plus prudes préfèreront celle du développement des ailes et des plumes chez les oiseaux : l'ancêtre Archéopterix vivant dans les marais en tirait grand avantage car il s'en servait comme d'un écran pour éviter les reflets du soleil sur la surface des eaux et mieux voir ainsi les poissons nageant entre ses pattes. Bernardin de Saint Pierre n'avait point tant d'esprit ni Rudyard Kipling une telle fantaisie.

Mais revenons aux chevaux. Pour les zoologistes, les équidés ont entre autres particularités la possession de sabots. Ceux-ci sont de véritables organes dont l'efficacité implique une anatomie fine, complexe et un remaniement de la partie distale des membres. Comment a pu se constituer une semblable structure qui exige des modifications qualitatives autrement plus compliquées que la fusion de deux ou trois noyaux d'hélium ? C'est là le grand problème dont tous les progrès des connaissances depuis Darwin n'ont fait que d'augmenter le mystère depuis l'enlacement des boucles de contrôles chez les phages* jusqu'aux organes des animaux supérieurs en passant par les organelles des cellules et les tissus différenciés des êtres multicellulaires. Dans tous les cas on doit faire le double constat d'une énorme complexité structurelle et d'une surprenante fonctionnalité.

Essayons de voir les choses de plus près. On admet que le patrimoine héréditaire d'un vertébré est constitué de quelques dizaines de milliers de gènes. Une mutation de l'un d'eux modifie, bloque ou déclenche la production d'une protéine qui elle-même le plus souvent interagit avec d'autres productions dans un système complexe de contrôles positifs ou négatifs. Nous devons donc considérer l'ensemble comme une sorte d'usine automatisée dans laquelle cinquante mille manettes commandent des robinets et l'action de machines outils élémentaires selon des modalités diverses qui rendent leur action plus ou moins globale et plus ou moins impérative et selon un réseau multiple d'asservissements réciproques et de transformations récursives de circuits de commande.

* M. PTASHNE (1987), *A genetic Switch*, Blackwell scientific publications.

M'autorisant à mon tour d'une licence rhétorique, je propose d'imaginer cette usine comme une fabrique d'automobiles dépourvue de bureau d'études. Elle est régie par le service commercial qui tire ou pousse les manettes au hasard dans la plus joyeuse ignorance des processus technologiques. D'après les chiffres de ventes on intensifie la production du modèle (= fécondité accrue sous contrôle de la sélection naturelle) ou l'on recommence à manœuvrer aveuglement les manettes (= mutations au hasard). Peut-être admettrez-vous qu'un tel système puisse répondre aux demandes du marché en ce qui concerne la couleur ou la forme de la carosserie. Comment concevriez-vous l'interaction des commandes s'il s'agit de changer le nombre de portes ? ou de faire passer le moteur de l'avant à l'arrière ? Comment imaginer que la seule ouverture de nouveaux robinets ajoutant du plomb et de l'acide sulfurique à la liste des matières premières introduites suffise pour que finissent par être usinées les batteries électriques que l'on avait oubliées ? Pourtant il y a quelques années on a présenté comme une confirmation du darwinisme la découverte d'une protéine ubiquitaire — la cristalline — comme si sa seule abondance expliquait la mise en place du cristallin de l'œil dont le fonctionnement exige une balance rigoureuse entre la géométrie et l'hétérogénéité interne. Retour de la tautologie : puisque, d'après le grand Ernst Mayr des appareils visuels efficaces sont apparus une quarantaine de fois dans des phylums différents c'est bien, dit-on, que de tels miracles sont possibles. Certes !

*
* *

J'aurais pu choisir une autre licence poétique en vous infligeant longuement la métaphore informatique.

Voici le point où je présente au lecteur les excuses du mathématicien auquel on a fait l'honneur de demander une préface à un livre sérieux de biologie : c'est que l'on consomme beaucoup de mathématiques chez les néo-darwiniens depuis Sir Ronald Fisher, J.B.S. Haldane et les disciples de Sewall Wright, et que l'on ne fait pas fi de présenter des calculs ou des programmes d'ordinateurs pour entraîner la conviction. *Je tiens ces exercices pour mystifiants* : tous reposent de façon tacite sur des hypothèses simplificatrices grossières, biologiquement infondées et sans lesquelles les effets annoncés ne se produiraient pas.

La sagesse nouvelle que nous avons acquise depuis les précurseurs que je viens de citer est que les systèmes dynamiques complexes tendent vers le chaos en dehors de cas infiniment spéciaux. L'ordre que l'on croit voir surgir par un habile programme y était caché à très faible profondeur et il reste vulnérable à la moindre perturbation agissant à son niveau. Ou bien, plus subtilement, cet ordre est fondamentalement très élémentaire comme l'est celui des cristaux ou des flocons de neige, quelque puisse

être sa valeur esthétique ou sa complication apparente. Or l'ordre qui importe du point de vue biologique n'est pas élémentaire (la beauté symétrique des lys n'est pas en cause) et surtout il est *fonctionnel*, un concept qu'aucun logicien ou informaticien ne saurait formuler de façon efficace avec la moindre généralité. Ceci n'est pas qu'une autre histoire mais, peut-être, le cœur du débat. Des dizaines d'équipes de programmeurs ont essayé d'appliquer le schéma darwinien à des systèmes auto-adaptatifs divers. La vitesse des ordinateurs leur permet d'opérer avec des nombres de cycles ayant un ordre de grandeur supérieur à ceux que l'on rencontre dans l'évolution de certaines lignées (au plus quelques centaines de milliers de générations pour l'homme). Le résultat de tous ces efforts n'a pas dépassé le stade d'exemples jouets aussi insignifiants pour notre propos que les canards en bois de Vaucansson quant à l'écologie des palmipèdes.

Revenons à la biologie.

Les apôtres du darwinisme appartiennent à deux écoles.

L'une, la plus classique, est gradualiste. Elle plaide l'immensité des populations et de l'échelle des temps géologiques pour affirmer qu'après tout, tout finit bien par arriver par une suite de modifications imperceptibles à condition d'attendre assez longtemps.

La paléontologie se prête bien à ces jeux car il est très tentant de déformer plus ou moins continuement un squelette en un autre. Ce serait beaucoup plus difficile si l'on devait tenir compte des artères et des autres parties molles et de la nécessité de respecter un minimum de viabilité à chaque génération. Les darwiniens ont, semble-t-il, renoncé à imaginer comment auraient pu être faits des êtres intermédiaires entre les cétacés et leurs ancêtres terrestres.

En outre les ordres de grandeur n'y sont pas : il y a longtemps que mon ami le Professeur M. Eden, Directeur de la division d'ingéniérie bio-médicale du National Institute of Health a calculé que pour aboutir au génome humain il fallait que depuis l'aurore des temps pré-cambriens se soit capitalisé en moyenne un bit d'information à chaque génération*.

L'autre école, celle des saltationistes, est plus jeune et plus révolutionnaire. Elle admet des discontinuités majeures ce qui s'accorde mieux avec les progrès de la paléontologie depuis Darwin. Son coryphée, S.J. Gould, revient au style du drame élisabéthain. On aura donc une mise en scène à grand spectacle avec déluges, comètes, chaînes de volcans en feu, chutes de météores et autres cataclysmes afin d'imposer une ambiance de fureur aveugle et de chaos. Car la mode post-moderne veut que l'histoire apparaisse comme un désordre absurde dénué de tout sens et signification. Cette vision est contredite par les grandes tendances que les naturalistes ont mises en évidence. Pour ne citer que quelques-unes parmi les plus connues :

* Se reporter à *Mathematical Challenges to the Neo-Darwinian Interpretation of Evolution* (P.S. Moorehead and M.M. Kaplan, ed., 1967).

– chez les vertébrés, l'encéphalisation progressive, mais aussi l'intériorisation du processus reproductif depuis la fécondation externe des poissons jusqu'au placenta des mammifères en passant par le stade larvaire des amphibiens et la poche des marsupiaux.

– chez les végétaux, la complexification croissante des synthèses biochimiques grâce à laquelle seuls les plus récemment apparus disposent de la lignine, donc du bois, ou des pigments subtils qui colorent les bleuets.

Cette contradiction est grave puisque l'existence d'une seule tendance lente et diffuse de ce type, se manifestant au niveau des catégories les plus hautes de l'arbre taxonomique, impose celle d'un principe *global* polarisant les mutations (grandes ou petites) tout au long de centaines ou de milliers de milliards de générations. Ce dont ne peut rendre compte le tandem hasard x sélection dont tout effet ne saurait être que relativement *local*, c'est-à-dire opérant au niveau des catégories plus basses des familles et des genres. Ainsi le simple fait que les dinosaures aient été remplacés non pas par des amphibiens mais par les mammifères qui les suivent selon les tendances qui viennent d'être évoquées ne peut pas être écarté par la seule plaisanterie que les tendances observées ne seraient que l'effet apparent d'une vision anthropomorphique de la Vie.

La même école croit aux « monstres prometteurs » chez lesquels apparaîtrait *ex abrupto* un organe nouveau. L'obstacle est qu'il faut beaucoup de ces monstres car presque tous les ordres ou les classes (au sens de la systématique) se caractérisent par la présence d'un organe singulier dont étaient dépourvus leurs ancêtres et dont on voit mal la possibilité d'une formation progressive par étapes (pensez à l'anatomie fine de la plume, au bras hectocotyle des céphalopodes, à l'œuf amniotique, etc. etc. et à la riche collection de cas rassemblée par Andrée Tetry*). On peut, bien sûr, parler d'un « bricolage » de la nature. C'est un joli mot d'auteur mais avec toute la considération que je dois à François Jacob je n'y vois qu'un constat ou qu'une pirouette verbale pour échapper au dilemme auquel sont confrontés les néo-darwinistes :

– ou bien l'évolution de la vie est le résultat de milliers de macro-mutations dont chacune aurait une improbabilité quasiment inchiffrable (« la chance qu'a une tornade d'assembler un Boeing 747 en s'abattant sur un cimetière de voitures » a dit un cosmologue réputé) ;

– ou bien ces mutations n'étaient ni tout à fait fortuites ni tout à fait indépendantes.

La première position était, je crois, celle de J. Monod. C'est une thèse philosophique éminemment respectable mais dont la relevance à la science paraît égaler celle du solipsisme (« Je suis le seul être existant et le monde extérieur ne fut que mon rêve »).

---

* CUENOT Lucien et TÉTRY Andrée (1951), *L'évolution biologique, les faits, les incertitudes*, Paris, Masson.

La seconde a été présentée de la façon la plus explicite par Waddington. Elle postule l'existence de contraintes (physico-chimiques ?) pesant sur les modifications du génome et canalisent l'évolution dans le sens que nous présentent les documents paléontologiques. Mais ici encore c'est une habileté dialectique pour fournir un placebo intellectuel. S'il existait des contraintes sur le génome des poissons primitifs orientant préférentiellement leurs descendants vers la possession des organes beaucoup plus complexes qui sont requis pour être un oiseau, un kangourou ou un primate, ce sont ces contraintes qui sont les vrais moteurs de l'évolution même si le hasard et la sélection semblent en surface jouer ce rôle et ce sont elles qui doivent alors constituer l'objet de la science et non pas les accidents fortuits qui ont déclenché leur intervention. Au demeurant ces transitions brusques (en moins de quelques milliers de générations) restent incompréhensibles et l'on voit mal comment le génome des êtres primitifs aurait pu receler en puissance la quantité d'informations nécessaire aux formidables accroissements ultérieurs de la complexité fonctionnelle. Sauf à invoquer un ou des principes inconnus dont personne n'a la moindre idée. On retombe alors sur la thèse d'un préformationisme radical dont s'accommode fort bien l'idéalisme hégélien mais c'est encore une option philosophique qui est loin d'être neutre.

*
* *

En présence de ces faits – et de bien d'autres que j'ai omis ou que j'ignore – une position minimaliste serait d'admettre que nous n'avons pas encore les concepts ni sans doute, la connaissance de faits élémentaires insoupçonnés, qui seraient nécessaires pour commencer à théoriser l'évolution de la vie dans son ensemble. Bref d'admettre que les biologistes d'aujourd'hui sont dans la même situation que pouvaient l'être les (paléo) chimistes du XVIème siècle. C'est bien inconfortable devant les étudiants. S'il faut aller plus loin et si l'on veut tenter de prévoir l'aboutissement futur des recherches, il n'est d'autre recours que la philosophie individuelle.

Dans la toute dernière partie de son ouvrage le Professeur Chandebois a l'honnêteté de déclarer ses convictions. Qui lui en fera reproche alors que le nombre d'auteurs darwiniens confessent fièrement leur foi matérialiste*. Cette prise de position évitera que l'on ait le moindre doute sur le système du monde à l'intérieur duquel le Professeur Chandebois a poursuivi ses recherches. Celui-ci est partagé par de très nombreux savants et il est admis avec la même franchise par certains qui comptent en France parmi les partisans les plus éminents du néo-darwinisme.

---

* Se reporter au livre de PHILLIP E. JOHNSON de l'université de Californie à Berkeley, *Darwin on Trial*, Regnery Gateway, Washington, D.C., 1991, qui suscite tant de débats depuis un an ou deux.

Il serait impropre de lire à l'envers le livre du Professeur Chandebois qui n'est en rien construit comme un préambule à une apologétique. Si le darwinisme voulait être une science c'est la partie critique, à mon avis difficilement contestable, qui devrait être discutée au fond.

Et pour décliner mes propres opinions et expliquer le sous-titre de cette préface, je soumets aux lecteurs ce petit texte délicieusement pré-post-moderne.

« En ce qui concerne les peuples civilisés, la réduction des mâchoires à cause de leur moindre usage, le jeu constant des différents muscles servant à exprimer des émotions diverses, enfin la taille accrue du cerveau résultant d'une plus grande activité intellectuelle, tout ceci dans son ensemble a produit un effet considérable sur leur apparence générale en comparaison avec celle des sauvages (*). »

M. Schützenberger
de l'Académie des Sciences

* « With civilised nations, the reduced size of the jaws from lessened use, the habitual play of different muscles serving to express different emotions, and the increased size of the brain from greater intellectual activity, have together produced a considerable effect on their general appearence in comparison with savages. » Charles Darwin. *The descent of man* (1871). Part I chap. VII, p. 247.

Année 1994

Bibliographie

[1994-1] Marcel-Paul Schützenberger. Une sotie au sujet de la théorie des nombres parfaits. *Conjonctures*, 20-21 :215–223, 1994. aussi dans "Acte créateur".

Une sotie au sujet de la théorie des nombres parfaits*

par Marco Schützenberger

Certes les mœurs sont devenues plus douces. Mais s'il ose parler au milieu des poètes, un informaticien n'en redoute pas moins de se voir pelé, et sa défroque suspendue aux branches. Sa seule ambition ne peut être donc que de divertir au risque de détourner le débat sur la création. Je m'avance à l'abri d'un texte classique.

« Deux tours énormes s'apercevaient dans la vallée. En les multipliant par deux le produit était quatre. Mais je ne saisissais pas très bien la nécessité de cette opération d'arithmétique, et je continuais ma route avec la fièvre au visage et je m'écriais sans cesse : "Non, non, je ne distingue pas très bien la nécessité de cette opération d'arithmétique" » Je confesse que moi non plus ou du moins pas encore, pas ici.

C'était bien sûr un extrait d'un chant de Maldoror, et les méthodes de la critique moderne prouveront qu'indubitablement il s'agit du quatrième (où $4 = 2 \times 2 = 2^2$).

---

* Ce texte a été présenté au colloque sur la création poétique de l'institut collégial européen lors de sa réunion à Loches en juillet 1992. Il sera sans doute publié dans les actes du colloque. Nous remercions l'auteur et l'institut collégial et, en particulier, le professeur Gilbert Gadoffre.

Veuillez avoir l'indulgence d'admettre que le calculateur, c'est-à-dire celui qui aligne des calculs comme d'autres des pensées ou des vers, n'est ni un faune, ni un satyre, ni un sciapode, ni Fafner tapi au fond de ses ateliers. Qu'il est doué d'une espèce de parole, bien qu'elle diffère de celle des poètes par le mode et le temps, et surtout par la contrainte de pouvoir supporter à l'infini paraphrases et retraductions.

Ce qui implique que son mode ne soit pas l'optatif, ni le subjonctif, ni le jussif. Ce n'est même pas l'indicatif des naturalistes, mais seulement l'interrogatif et encore de façon fort restreinte. Lautréamont demande « Pourquoi », ce qui serait trop ambitieux pour les calculateurs dont la réponse n'a le droit d'être que « OUI », « NON », ou le plus souvent « ?? ». C'est bien peu, trop *unidimentionnel*, décident les communicateurs, mais c'est la loi de notre cité telle que nous la tenons d'Euclide.

L'histoire que je vous soumets remonte d'ailleurs à lui.

*

Six est un nombre parfait parce que $6 = 3 + 2 + 1$ est égal à la somme de ses diviseurs. Huit ne l'est pas parce que la somme correspondante, $4 + 2 + 1 = 7$, et que huit n'est pas sept.

Il y a une excellente explication qui est fournie par Alcuin : six est parfait, parce que la création s'est faite en six jours. Ce n'est pas le cas de huit et d'ailleurs la seconde création, celle qui eut lieu après le Déluge, a impliqué les huit âmes qui étaient dans l'Arche. Alcuin est très clair sur ces points mais il ne fait que rassembler ce que bien d'autres avaient écrit avant lui, car le thème des nombres parfaits est un grand topique depuis Euclide. Il a été développé par

Philon, inlassablement investigué par les gnostiques et commenté par Boèce que je tiens à citer pour montrer fièrement que nous avons au moins un poète avec nous.

Dans ses trois livres d'arithmétique, Euclide commence par établir la théorie des nombres premiers et conclut par la démonstration qu'il n'en existe pas un qui soit plus grand que tous les autres, c'est-à-dire, en langage codé, qu'il y en a une infinité. Le mouvement surprenant de cette preuve en préfigure d'autres qui, à travers Du Bois-Raymond et Cantor, mèneront aux grands théorèmes de Gödel. Puis viennent quelques propositions irrelevantes à notre propos et enfin l'énoncé dramatique que si l'entier p est tel que 2^{p-1} est premier alors $2^{p-1} \times (2^p - 1)$ est parfait. C'est le cas pour p = 2, 3, 5, 7 mais pas 9, et les quatre (encore) plus petits nombres parfaits sont connus depuis l'Antiquité. Les voici :
$6 = 2^1 \times (2^2 - 1) = 2 \times 3$; $28 = 2^2 \times (2^3 - 1) = 4 \times 7$
qui admet des explications évidentes dès que l'on a abandonné le vieux rythme des semaines de cinq jours;
$496 = 2^4 \times (2^5 - 1) = 16 \times 31$ et
$8128 = 2^6 \times (2^7 - 1) = 64 \times 127$.
Observez 127.

Oui, je le sais, hélas, ces choses-là sont rudes dans nos siècles de fer, de verre et de plastique. Pourtant, elles faisaient partie des connaissances des clercs passés par le trivium et le quadrivium. D'ailleurs, assis à cette table, j'ai un garant que l'Abbesse Hroswitha ne négligeait pas d'en informer ses moniales, ce qui était d'autant plus méritoire que l'on ne disposait pas encore de la limpidité des notations modernes. En particulier, manquait la convention d'écriture que 2^{k+1} désigne le résultat de la multiplication têtue de deux par lui-même k fois, grande simplification prosaïque

de ce qui fit, dit-on, l'amusement du roi Gélon, et de divers sages princes orientaux.

Aussi personne ne pouvait alors s'aviser que $1 = 2^0 \times (2^1 - 1)$ peut être considéré comme un nombre parfait, le zéro-ième et, c'est là encore un très profond mystère, peut-être le seul nombre parfait qui soit impair (cf. Lautréamont).

Euclide est trop classique pour poser une question. D'ailleurs la question se pose d'elle-même. Existe-t-il un nombre parfait qui soit plus grand que tous les autres ?

Les auteurs du Moyen Âge restent dans le vague. Certains croient que les nombres parfaits se terminent alternativment par 6 ou par 8, ce qui est une séduisante hypothèse attribuant un rôle privilégié à DIX = DEUX que multiplie CINQ. Mais elle n'est pas vraie. Pire, les auteurs affirment que le cinquième nombre parfait est $2^{10} \times (2^{11} - 1)$. Or $2^{11} - 1 = 2047$ n'est pas un nombre premier comme tout écolier pouvait le vérifier sans trop de peine puisqu'il suffit de constater qu'il est divisible par 23.

Sans doute la majorité des sorbonniques ne faisait que recopier ce qu'elle avait lu, mais j'y vois une faute d'une tout autre gravité, celle de croire que le monde est trop simplement facile. La suite 2, 3, 5, 7, pas 9,... appelle 11 de façon trop voyante. Aurez-vous la dureté d'y dénoncer une erreur Pélagienne ? Il est curieux que Lefèvre d'Étaples soit tombé dans ce piège. Bovilius aussi, mais il a eu le mérite d'observer que les nombres parfaits sont des gnomons (c'est-à-dire des surfaces de triangles rectangles isocèles). Euclide le savait bien, mais il écrit hors du temps, donc sans citer ses prédécesseurs, et il ne manifeste aucune sympathie pour les Pythagoriciens.

Autre marque du temps chez les calculateurs. Chez vous les poèmes sont éternels, mais moins que les poètes et depuis les âges épiques, il n'y a plus de poèmes sans poètes alors que chez nous les théorèmes deviennent vite orphelins anonymes. Et nous ignorerons toujours qui a fait joyeusement quelque matin au moyen âge la découverte que $2^{12} \times (2^{13} - 1)$ est un nombre parfait, le vrai *cinquième* nombre parfait.

Permettez un excursus dans le jardin de l'Amitié. Un nombre parfait est un nombre égal à la somme de ses parties aliquotes, comme on disait avant que les Conciles de Bourbaki n'aient exclu les mots aux allures pédantes qui effaroucheraient les gentils étudiants. Deux nombres sont amicables, *inter se amat*, si chacun est la somme des parties aliquotes de l'autre. La paire la plus connue est (220, 284). Les meilleurs commentateurs la réfèrent à la Genèse car c'est le nombre des brebis et des autres présents que s'échangent Jacob et Ésau. Autres temps, autres usages. J'extrais de l'histoire de l'arithmétique que El-Magriti en 1107 rapporte avoir observé sur lui-même l'effet érotique des nombres amicables « quand on donne à manger le plus petit et qu'on consomme soi-même le plus grand ». Ibn Khaldun malgré son scepticisme habituel commente leur influence en notant la nécessité de tenir compte des thèmes astrologiques. Je passe vite à Descartes qui a trouvé une méthode pour obtenir de nouvelles paires. C'est un filon qui restera exploité jusqu'à nos jours.

Je reviens au nombre parfait. L'époque moderne commence avec Cataldi qui, en 1558, construit les premières tables des nombres premiers et découvre les deux nombres parfaits suivants. Ceux-ci correspondent à $p = 17$ et à $p = 19$. Ce n'est pas un mince travail, car Cataldi accomplit une à une toutes les divisions qu'il convient. Cinquante ans plus tard,

Fermat démontre des théorèmes grâce auxquels ces calculs auraient été considérablement allégés, mais il ne trouve pas de nombres parfaits nouveaux, car il se présente une lacune inattendue.

C'est le grand Euler qui en 1771, montrera que le nombre parfait suivant est $2^{30} \times (2^{31} - 1)$. Il se trouve, pour l'anecdote, que le nombre 2^{31} est exactement la limite de ceux que les ordinateurs acceptent sans que l'on ait à invoquer des procédures spéciales.

Et puis, plus de découvertes pendant un siècle jusqu'à Édouard Lucas, qui n'a pourtant aucune réputation chez les mathématiciens professionnels car il est inspecteur de l'enseignement, et ne publie que des livres de mathématiques amusantes. Vers 1875, il invente une méthode entièrement originale pour dépister les nombres parfaits. Elle relie de façon encore mystérieuse leur quête (que les lettrés ne manqueraient pas de dire initiatique) à l'antique Nombre d'Or, c'est-à-dire au pentacle. Est-ce une partialité sectaire que de croire qu'il était pythagoricien ? En était-il de même pour Fibonacci ? Sa méthode réduit à presque rien les calculs exigés pour la vérification des cas déjà connus, mais il se borne à en montrer la vertu en prouvant que $2^{126} \times (2^{127} - 1)$ est parfait. Vous avez reconnu 127, mais évitez des hypothèses trop hâtives; en particulier, à un étage subalterne, que l'auteur de ces lignes serait moindrement cabbaliste. Très vite, d'autres appliquent la méthode et débusquent quelques nombres parfaits nouveaux.

Voyez comme notre temps est plus lent que celui des Arts. Pendant plus d'un demi-siècle, on ne trouvera rien malgré des efforts nombreux et bien d'autres qui demeurent des échecs inavoués. Malgré l'outil forgé par Lucas la masse des calculs est trop écrasante.

Mais en 1952, en Angleterre, Robinson, montre que $2^{520} \times (2^{521} - 1)$ est parfait. Il a utilisé un ordinateur, et c'est aussi la première fois que ces machines fournissent un résultat proprement mathématique. Depuis, le domaine est devenu une petite industrie où amateurs et professionnels rivalisent pour enrichir la liste des nombres parfaits toujours grâce à la méthode de Lucas, et mille ingéniosités dans sa programmation.

Il est convenable (parce que $25 = 5^2$) de citer le *vingt-cinquième* nombre parfait. Il correspond au nombre premier 21701, et il suffit pour l'écrire d'aligner une quinzaine de milliers de chiffres.

*

Désormais, la technique intervient dans cette longue procession. On s'active aujourd'hui autour de $p = 33843$, et des mathématiciens s'acharnent à trouver, à l'instar de Lucas, des propriétés permettant d'avancer vers la solution de l'énigme. Dans ce travail, il faut beaucoup d'ardeur et une confiance inébranlable dans l'espoir du succès. On connaît d'ailleurs l'histoire du Rabbin Luria qui, en Bessarabie, la veille de la fête des Tabernacles, rassemble ses disciples et leur dit : « Prions, et demain nous serons à Jerusalem. » Le premier disciple demande : « Est-ce bien vrai Rabi ? ». Et le Rabbin soupire : « C'eût été si beau de passer Sukhot à Jérusalem ».

Mais s'il n'y a pas d'autre voie que le test de Lucas, le temps de cette question ne sera plus que celui des machines. Et comme l'observe Daniel Shanks, auquel j'ai fait plus qu'emprunter, on pourrait évaluer le degré d'avancement technologique d'une civilisation extra-terrestre sans en savoir rien

d'autre que la taille du plus grand nombre parfait qu'elle est capable de nommer.

Ce serait humiliant. (Ne gronde pas, Fafner !) Et pour certains, absurde.

Pourquoi perdre du temps à résoudre ces problèmes ? Entre Euler et Lucas un mathématicien anglais, Peter Barlow, en 1814, écrit dans une encyclopédie que : « Les nombres parfaits étant seulement curieux, sans être utiles, il est peu vraisemblable qu'il se trouve des personnes pour essayer d'en trouver de nouveaux ». Je n'ai pas tenté d'établir le contraire ni de vous convaincre que le calcul soit autre chose que la drogue des calculateurs. Ni de dire que les merveilleux miracles que nous y voyons ne sont pas de misérables merveilles pour reprendre le mot de Michaux. Misérables aux yeux du dieu qui est à Delphes. Du dieu qui n'est qu'à Delphes.

Car quel est le statut des nombres parfaits correspondant à des nombres premiers ayant deux cents chiffres, comme nous pouvons maintenant en produire en série, et non pas cinq comme 33843 ? Il n'y a pas assez de matière dans l'univers visible pour construire un ordinateur permettant la vérification au moyen du test de Lucas. Peut-être même, Gödel l'autorise, la réponse est « ?? ». Ultime, ou provisoire ?

Il y a une autre loi, ésotérique, qui dans notre cité, n'oblige que ceux qui la connaissent. Elle est l'un des sens de la Parabole du Rabbin Luria et présuppose que la découverte et la preuve d'un théorème sont actes de volonté dans l'absolue liberté que laisse un Créateur auquel n'importe rien de ce qui est fini. Ce qui leur fait tenir pour vains les propos de Barlow, calculateur honorable mais homme par trop appliqué,

même pour avoir dit une phrase fatale. Après la fin des temps...

*

(Ici la bande du magnétophone est devenue inaudible. Vengeance de Fafner, ou sagesse éditoriale supérieure, car rien n'est futile comme le bavardage d'un calculateur sur le calcul. On reconnaît cependant une référence majeure à George Steiner faisant lui-même, par récursion, référence à un Château, puis des segments d'une longue phrase embrouillée évoquant des calculateurs à l'œuvre, sans nulle inconscience, devant la septième porte, celle qui donne sur la nuit.)

Année 1995

Bibliographie

[1995-1] Marcel-Paul Schützenberger. Pour en finir avec le darwinisme. *Conjonctures*, 22 :115–126, 1995.

[1995-2] Christophe Reutenauer et Marcel-Paul Schützenberger. Variétés et fonctions rationnelles. *Theoret. Comput. Sci.*, 145(1-2) :229–240, 1995.

Pour en finir avec le Darwinisme[1]

par Marco Schützenberger

Il paraît tous les ans plusieurs livres consacrés au darwinisme que l'on présente comme un acquis de la science aussi indubitable que la théorie atomique ou la fonction glycogénique du foie. On y chercherait en vain des réponses aux multiples critiques que des générations de naturalistes ont opposées à ces thèses. Au mieux les contradicteurs sont ridiculisés par quelque anecdote spirituelle. Au pire, on les accuse de « faire le jeu » d'un Grand Satan du jour. Le plus souvent ce sera le silence. Ainsi la bibliographie d'un très récent Traité dont je respecte l'auteur contient une douzaine de références à P. Grassé. Mais, allant au texte, le lecteur s'aperçoit que ce ne sont que des renvois insignifiants et il ne verra même pas mentionnés les puissants arguments contre le darwinisme développés par celui qui fut l'un des maîtres de la zoologie contemporaine dans son grand livre, *l'Evolution du vivant*. Non pas que ces critiques et d'autres plus anciennes aient été invalidées par les progrès des connaissances. Au contraire. Mais il est plus facile de les oublier que d'y répondre. Elles proviennent de toutes les disciplines des sciences de la vie. Les plus connues ont été formulées par les paléontologistes mais les plus graves, bien que

[1] Ce texte a été repris, après quelques modifications, de la préface de l'ouvrage *Pour en finir avec le Darwinisme : une nouvelle logique du vivant* de R. Chandebois, édition Espace 74, Montpellier. Nous remercions l'éditeur (M. Laurent Chevalier), l'auteur du livre (Mme R. Chandebois, professeur d'embryologie à l'université d'Aix-Marseille) et M. Marco Schützenberger pour nous en avoir autorisé la publication.

plus discrètes, sont dues aux embryologistes. C'est l'immense mérite du livre du Professeur Chandebois que de les rassembler et de les enrichir grandement avec la compétence que lui confère une fructueuse carrière de chercheur.

*

De quoi s'agit-il ? La thèse fondamentale commune aux diverses versions actuelles du darwinisme est que l'évolution des êtres vivants résulte du seul hasard filtré par la sélection naturelle. Et pour convaincre on multiplie les exemples mineurs qui ne prouvent rien quant au fond de la question. Nul en effet n'a assez mauvais cœur pour nier que la sélection puisse avoir des effets importants. Il n'est pas besoin de Darwin pour savoir que la désertification d'une zone en fera d'abord disparaître celles des variétés végétales qui ont le plus besoin d'eau. Mais ceci n'explique pas la genèse des particularités anatomiques et physiologiques dont sont douées les xérophytes et ne justifie en rien qu'on en attribue l'origine au seul hasard. On a élaboré des récits touchants à l'usage des enfants des écoles. Voyez l'histoire des chevaux. Ils ont commencé par être de petites créatures grosses comme des lapins. Celles qui avaient la chance d'être nées un peu plus grandes couraient plus vite et échappaient ainsi à la dent des méchantes bêtes qui voulaient les manger. Elles avaient donc plus de descendants et c'est ainsi, dit-on, que, progressivement, au long de milliers de siècles, les chevaux ont atteint leur taille actuelle. L'emploi de termes plus savants permet d'éviter les questions que les enfants ne doivent pas poser, c'est-à-dire d'avoir à fournir l'énoncé explicite des hypothèses sans lesquelles la valeur probante de cette histoire est nulle. Par exemple, comment sait-on :

— Que la capture par un prédateur est une cause importante et constante d'une moindre fécondité ?

— Que la réduction de sa probabilité est fortement liée à la vitesse de fuite et celle-ci à la taille ?

— Que l'augmentation de la taille n'a pas de conséquences subsidiaires telles que l'accroissement des besoins alimentaires, qui compensent son effet final sur la fécondité ?

— Que d'autres modifications (un autre mode de vie, une meilleure vigilance, un goût exécrable de la viande, etc. etc.) n'interagissent pas avec le facteur sélectif choisi et brouillent son action ? etc. etc.

Manifestement rien de ceci n'est vérifiable et la réponse aux questions ne saurait être que la récitation d'une série d'exemples à laquelle pourrait être opposée une autre série tout aussi convaincante (et d'ailleurs utilisée quand il s'agit d'« expliquer » le plafonnement de la taille). La controverse dégénérant en un échange d'anecdotes, l'orateur darwinien aurait à conclure son discours par l'assertion tautologique que ces objections doivent être écartées puisque les chevaux sont plus grands aujourd'hui que jadis (quand ils n'étaient pas encore des chevaux).

J'ouvre ici une parenthèse pour marquer par un exemple que ce n'est pas le schéma logique du raisonnement ni son statut métaphysique que récusent les savants soucieux de la rigueur vers laquelle on tend dans les autres domaines de la nature.

La situation est abstraitement analogue mais de fait toute différente pour le mécanisme généralement admis de la synthèse des noyaux atomiques à l'intérieur des étoiles et des supernovæ. C'est pourtant un processus que l'on pourrait qualifier de darwinien. Le choc (aléatoire) des particules produit des noyaux de plus en plus gros et les différents modes de désintégrations radioactives (encore le hasard) déterminent la fréquence ultime des espèces atomiques et de leurs isotopes compte tenu de leur stabilité. Les physiciens et les cosmologistes ont la chance de pouvoir tester leurs hy-

pothèses et déterminer ou calculer avec assez de précision les paramètres en cause pour que ce modèle soit tout autre chose qu'un système conjectural. Il n'en est pas de même en biologie mais il serait paradoxal de considérer comme un garant de la véracité de la théorie néo-darwinienne la seule et pure impossibilité d'en apporter la preuve ! Une théorie s'appelle une hypothèse tant qu'elle n'a d'autre argument que le charme de sa rhétorique.

Or le darwinisme est surtout un genre littéraire. Il est né en Angleterre comme le roman policier, et tout l'art est de dissimuler les invraisemblances que requiert l'enchaînement des épisodes. Un auteur fort réputé est R. Dawkins, dont les amateurs ont apprécié l'explication de l'absence d'un os pénien chez l'homme. Les lecteurs plus prudes préféreront celle du développement des ailes et des plumes chez les oiseaux : l'ancêtre Archéopterix vivant dans les marais en tirait grand avantage car il s'en servait comme d'un écran pour éviter les reflets du soleil sur la surface des eaux et mieux voir ainsi les poissons nager entre ses pattes. Bernadin de Saint Pierre n'avait point tant d'esprit ni Rudyard Kipling une telle fantaisie.

Mais revenons aux chevaux. Pour les zoologistes, les équidés ont entre autres particularités la possession de sabots. Ceux-ci sont de véritables organes dont l'efficacité implique une anatomie fine, complexe et un remaniement de la partie distale des membres. Comment a pu se constituer une semblable structure qui exige des modifications qualitatives autrement compliquées que la fusion de deux ou trois noyaux d'hélium ? C'est là le grand problème dont tous les progrès des connaissances depuis Darwin n'ont fait qu'augmenter le mystère depuis l'enlacement des boucles de contrôle chez les phages[2] jusqu'aux organes

[2] M. Ptashne (1987), *A genetic Switch*, Blackwell scientific publications.

des animaux supérieurs en passant par les organelles des cellules et les tissus différenciés des êtres multicellulaires. Dans tous les cas on doit faire le double constat d'une énorme complexité structurelle et d'une surprenante fonctionnalité.

Essayons de voir les choses de plus près. On admet que le patrimoine héréditaire d'un vertébré est constitué de quelques dizaines de milliers de gènes. Une mutation de l'un d'eux modifie, bloque ou déclenche la production d'une protéine qui elle-même le plus souvent interagit avec d'autres productions dans un système complexe de contrôles positifs ou négatifs. Nous devons donc considérer l'ensemble comme une sorte d'usine automatisée dans laquelle cinquante mille manettes commandent des robinets et l'action de machines-outils élémentaires selon les modalités diverses qui rendent leur action plus ou moins globale et plus ou moins impérative et selon un réseau multiple d'asservissements réciproques et de transformations récursives de circuits de commande.

M'autorisant à mon tour d'une licence rhétorique, je propose d'imaginer cette usine comme une fabrique d'automobiles dépourvue de bureau d'études. Elle est régie par le service commercial qui tire ou pousse les manettes au hasard dans la plus joyeuse ignorance des processus technologiques. D'après les chiffres de ventes on intensifie la production du modèle (= fécondité accrue sous la direction de la sélection naturelle) ou l'on recommence à manœuvrer aveuglément les manettes (= mutations au hasard). Peut-être admettrez-vous qu'un tel système puisse répondre aux demandes du marché en ce qui concerne la couleur ou la forme de la carrosserie. Comment concevriez-vous l'interaction des commandes s'il s'agit de changer le nombre de portes ? ou de faire passer le moteur de l'avant à l'arrière ? Comment imaginer que la seule ouverture de nouveaux robinets ajoutant du plomb et de l'acide sulfurique à la liste des matières premières in-

troduites suffise pour que finissent par être usinées les batteries électriques que l'on avait oubliées. Pourtant il y a quelques années on a présenté comme une confirmation du darwinisme la découverte d'une protéine ubiquitaire — la cristalline — comme si la seule abondance expliquerait la mise en place du cristallin de l'œil dont le fonctionnement exige une balance rigoureuse entre la géométrie et l'hétérogénéité interne. Retour de la topologie : puisque, d'après le grand Ernst Mayr, des appareils visuels efficaces sont apparus une quarantaine de fois dans des phylums différents, c'est bien, dit-on, que de tels miracles sont possibles. Certes !

*

J'aurais pu choisir une autre licence poétique en vous infligeant longuement la métaphore informatique.

Voici le point où je présente aux lecteurs les excuses du mathématicien auquel on a fait l'honneur de demander une préface à un livre sérieux de biologie : c'est que l'on consomme beaucoup de mathématiques chez les néo-darwiniens depuis Sir Ronald Fisher, J.B.S. Haldane et les disciples de Sewall Wright, et que l'on ne fait pas fi de présenter des calculs ou des programmes d'ordinateur pour entraîner la conviction. *Je tiens ces exercices pour mystifiants* : tous reposent de façon tacite sur des hypothèses simplificatrices grossières, biologiquement non fondées et sans lesquelles les effets annoncés ne se produiraient pas.

La sagesse nouvelle que nous avons acquise depuis les précurseurs que je viens de citer est que les systèmes dynamiques complexes tendent vers le chaos en dehors de cas infiniment spéciaux. L'ordre que l'on croit voir surgir par un habile programme y était caché à très faible profondeur et il reste vulnérable à la moindre perturbation agissant à son niveau. Ou bien, plus subtilement, cet ordre est fondamentalement très élé-

mentaire comme l'est celui des cristaux ou des flocons de neige, quelle que puisse être sa valeur esthétique ou sa complication apparente. Or l'ordre qui importe du point de vue biologique n'est pas élémentaire (la beauté symétrique des lys n'est pas en cause) et surtout il est *fonctionnel*, un concept qu'aucun logicien ou informaticien ne saurait formuler de façon efficace avec la moindre généralité. Ceci n'est pas qu'une autre histoire mais, peut-être, le cœur du débat. Des dizaines d'équipes de programmeurs ont essayé d'appliquer le schéma darwinien à des systèmes auto-adaptifs divers. La vitesse des ordinateurs leur permet d'opérer avec des nombres de cycles ayant un ordre de grandeur supérieur à ceux que l'on rencontre dans l'évolution de certaines lignées (au plus quelques centaines de milliers de générations pour l'homme). Le résultat de tous ces efforts n'a pas dépassé le stade d'exemples jouets aussi insignifiants pour notre propos que les canards en bois de Vaucansson quant à l'écologie des palmipèdes.

Revenons à la biologie. Les apôtres du darwinisme appartiennent à deux écoles. L'une, la plus classique, est gradualiste. Elle plaide l'immensité des populations et de l'échelle des temps géologiques pour affirmer qu'après tout, tout finit bien par arriver par une suite de modifications imperceptibles à condition d'attendre assez longtemps.

La paléontologie se prête bien à ces jeux car il est très tentant de déformer plus ou moins continuellement un squelette en un autre. Ce serait beaucoup plus difficile si l'on devait tenir compte des artères et des autres parties molles et de la nécessité de respecter un minimum de viabilité à chaque génération. Les darwiniens ont, semble-t-il, renoncé à imaginer comment auraient pu être faits des êtres intermédiaires entre cétacés et leurs ancêtres terrestres.

En outre les ordres de grandeur n'y sont pas : il y a longtemps que mon ami le Professeur M. Eden, Di-

recteur de la division d'ingénierie biomédicale du National Institute of Health a calculé que pour aboutir au génome humain il fallait que depuis l'aurore des temps précambriens se soit capitalisé en moyenne un bit d'information à chaque génération[3].

L'autre école, celle des saltationistes, est plus jeune et plus révolutionnaire. Elle admet des discontinuités majeures, ce qui s'accorde mieux avec les progrès de la paléontologie depuis Darwin. Son coryphée, S. J. Gould, revient au style du drame élisabéthain. On aura donc une mise en scène à grand spectacle avec déluges, comètes, chaînes de volcans en feu, chutes de météores et autres cataclysmes afin d'imposer une ambiance de fureur aveugle et de chaos. Car la mode post-moderne veut que l'histoire apparaisse comme un désordre absurde dénué de tout sens et signification. Cette vision est contredite par les grandes tendances que les naturalistes ont montrées. Pour ne citer que quelques-unes parmi les plus connues :

— chez les vertébrés, l'encéphalisation progressive, mais aussi l'intériorisation du processus reproductif depuis la fécondation externe des poissons jusqu'au placenta des mammifères en passant par le stade larvaire des amphibiens et la poche des marsupiaux;

— chez les végétaux, la complexification croissante des synthèses biochimiques grâce à laquelle seuls les plus récemment apparus disposent de la lignité, donc du bois, ou des pigments subtils qui colorent les bleuets.

Cette contradiction est grave puisque l'existence d'une seule tendance lente et diffuse de ce type, se manifestant au niveau des catégories les plus hautes de l'arbre taxonomique, impose celle d'un principe *glo-*

[3] Se reporter à *Mathematical Challenges to the neo-Darwinian Interpretation of Evolution* (P.S. Moorehead and M.M. Kaplan, ed, 1967),

bal polarisant les mutations (grandes ou petites) tout au long de centaines ou de milliers de milliards de générations. Ce dont ne peut rendre compte le tandem hasard X sélection dont tout effet ne saurait être que relativement *local*, c'est-à-dire opérant au niveau des catégories plus basses des familles et des genres. Ainsi le simple fait que les dinosaures aient été remplacés non pas par des amphibiens mais par les mammifères qui les suivent selon les tendances qui viennent d'être évoquées ne peut pas être écarté par la seule plaisanterie que les tendances observées ne seraient que l'effet apparent d'une vision anthropomorphique de la Vie.

La même école croit aux « monstres prometteurs » chez lesquels apparaîtrait *ex abrupto* un organe nouveau. L'obstacle est qu'il faut beaucoup de ces monstres car presque tous les ordres ou les classes (au sens de la systématique) se caractérisent par la présence d'un organe singulier dont étaient dépourvus leurs ancêtres et dont on voit mal la possibilité d'une formation progressive par étapes (pensez à l'anatomie fine de la plume, au bras hectocolyte des céphalopodes, à l'œuf amniotique, etc. etc. et à la riche collection de cas rassemblée par Andrée Tetry[4]). On peut, bien sûr, parler d'un « bricolage » de la nature. C'est un joli mot d'auteur mais, avec toute la considération que je dois à François Jacob, je n'y vois qu'un constat ou qu'une pirouette verbale pour échapper au dilemme auquel sont confrontés les néo-darwinistes :

— ou bien l'évolution de la vie est le résultat de milliers de macro-mutations dont chacune aurait une improbabilité quasiment inchiffrable (« la chance qu'a une tornade d'assembler un Boeing 747 en s'abattant sur un cimetière de voitures » a dit un cosmologue réputé);

— ou bien ces mutations n'étaient ni tout à fait fortuites ni tout à fait indépendantes.

---

[4] Lucien Cuenot et Andrée Tétry (1951), *L'évolution biologique, les faits, les incertitudes*, Paris, Masson.

La première position était, je crois, celle de Jacques Monod. C'est une thèse philosophique éminemment respectable mais dont la pertinence à la science paraît égaler celle du solipsisme (« Je suis le seul être existant et le monde extérieur ne fut que mon rêve »).

La seconde a été présentée de la façon la plus explicite par Waddington. Elle postule l'existence de contraintes (physico-chimiques ?) pesant sur les modifications du génome et canalisant l'évolution dans le sens que nous présentent les documents paléontologiques. Mais ici encore c'est une habileté dialectique pour fournir un placebo intellectuel. S'il existait des contraintes sur le génome des poissons primitifs orientant préférentiellement leurs descendants vers la possession des organes beaucoup plus complexes qui sont requis pour être un oiseau, un kangourou ou un primate, ce sont ces contraintes qui sont les vrais moteurs de l'évolution, même si le hasard et la sélection semblent en surface jouer ce rôle, et ce sont elles qui doivent constituer l'objet de la science et non pas les accidents fortuits qui ont déclenché leur intervention. Au demeurant ces transitions brusques (en moins de quelques milliers de générations) restent incompréhensibles, et l'on voit mal comment le génome des êtres primitifs aurait pu receler en puissance la quantité d'informations nécessaire aux formidables accroissements ultérieurs de la complexité fonctionnelle. Sauf à invoquer un ou des principes inconnus dont personne n'a la moindre idée. On retombe alors sur la thèse d'un préformationisme radical dont s'accomode fort bien l'idéalisme hégélien, mais c'est encore une option philosophique qui est loin d'être neutre.

*

En présence de ces faits — et de bien d'autres que j'ai omis ou que j'ignore — une position minimaliste serait d'admettre que nous n'avons pas encore les concepts ni, sans doute, la connaissance de faits élémentaires

insoupçonnés, qui seraient nécessaires pour commencer à théoriser l'évolution de la vie dans son ensemble. Bref d'admettre que les biologistes d'aujourd'hui sont dans la même situation que pouvaient l'être les (paléo) chimistes du XVIème siècle. C'est bien inconfortable devant les étudiants. S'il faut aller plus loin et si l'on veut tenter de prévoir l'aboutissement futur des recherches, il n'est d'autre recours que la philosophie individuelle.

Dans la toute dernière partie de son ouvrage le Professeur Chandebois a l'honnêteté de déclarer ses convictions. Qui lui en fera reproche alors que nombre d'auteurs darwiniens confessent fièrement leur foi matérialiste[5] . Cette prise de position évitera que l'on ait le moindre doute sur le système du monde à l'intérieur duquel le Professeur Chandebois a poursuivi ses recherches. Celui-ci est partagé par de très nombreux savants et il est admis avec la même franchise par certains qui comptent en France parmi les partisans les plus éminents du néo-darwinisme.

Il serait impropre de lire à l'envers le livre du Professeur Chandebois qui n'est en rien construit comme un préambule à une apologétique. Si le darwinisme voulait être une science c'est la partie critique, à mon avis difficilement contestable, qui devrait être discutée au fond.

Et pour décliner mes propres opinions et expliquer le sous-titre de cette préface, je soumets aux lecteurs ce petit texte délicieusement pré-post-moderne.

---

[5] Se reporter au livre de Philipp E. Johnson de l'université de Californie à Berkeley, *Darwin on trial*, Regnery Gateway, Washinbgton, D.C., 1991, qui suscite tant de débats depuis un an ou deux.

« En ce qui concerne les peuples civilisés, la réduction des mâchoires à cause de leur moindre usage, le jeu constant des différents muscles servant à exprimer des émotions diverses, enfin la taille accrue du cerveau résultant d'une plus grande activité intellectuelle, tout ceci dans son ensemble a produit un effet considérable sur leur apparence générale en comparaison avec celle des sauvages, »[6].

[6] « With civilised nations, the reduced size of the jaws from lessened use, the habitual play of different muscles serving to express different emotions, and increased size of the brain from greater intellectual activity, have together produced a considerable effect on their general appearence in comparison with savages ». Charles Darwin, *The descent of man* (1871), Part 1,chap. VII, p. 247.

ELSEVIER

Theoretical Computer Science 145 (1995) 229–240

Theoretical Computer Science

Variétés et fonctions rationnelles

Christophe Reutenauer[a,*,1], Marcel Paul Schützenberger[b]

[a] *Université du Québec à Montréal, C.P. 8888, succursale Centre Ville, Montréal, Québec, Canada H3C 3P8*
[b] *97 rue du Ranelagh, 75016 Paris, France*

Reçu avril 1994
Communiqué par M. Nivat

Abstract

We say that a rational (resp. a subsequential) function α from a free monoid into another one is in the variety of monoids V if it may realized by some unambiguous (resp. subsequential) transducer whose monoid of transitions is in V. We characterize these functions when V is the variety of aperiodic monoids, and the variety of groups. In the first case, the period of $\alpha^{-1}(L)$ divides that of L, for each rational language L on the outputs. In the second case, $\alpha^{-1}(L)$ is a group-language for each group language L; equivalently, α is continuous for the pro-finite topology. Examples of such functions are: the multiplication by a given number in a given basis, which is aperiodic; the division, which is a group-function.

1. Introduction

Dans la théorie des variétés de langages et de monoïdes, le théorème d'Eilenberg met en correspondance les (pseudo-) variétés de monoïdes finis et les variétés de langages rationnels. Ces dernières sont closes par image inverse des morphismes de monoïdes libres.

Dans le contexte des automates finis, les morphismes se généralisent en les fonctions rationnelles. Ceci suggère le problème de caractériser l'action par image inverse des fonctions rationnelles sur les variétés. À toute fonction rationnelle, on peut associer un monoïde. Notre résultat principal caractérise, en termes de leur action, les fonctions rationnelles pour lesquelles ce monoïde est apériodique ou un groupe: dans le premier cas la fonction divise les périodes des langages rationnels (en particulier, elle préserve les langages apériodiques). Dans le second cas, elle préserve les rationnels à groupe; de manière équivalente, elle est continue pour la topologie pro-finie; incidemment, nous montrons qu'elle est aussi pluri-sous-séquentielle. Un corollaire du résultat principal

*Auteur correspondant.

[1] Le premier auteur a bénéficié d'une subvention CRSNG (Canada) et d'une subvention Action Concerté FCAR-BNR-CRSNG.

SSDI 0304-3975(94)00180-4

est une caractérisation des morphismes: une fonction rationnelle est un morphisme dès qu'elle divise les périodes et préserve les rationnels à groupe par image inverse.

Deux exemples bien connus des écoliers illustrent les deux classes de fonctions rationnelles considérées dans cet article.

Il s'agit de la multiplication et de la division, qui sont respectivement des fonctions rationnelles apériodiques et à groupe. Classiquement, elles se font respectivement de droite à gauche, et de gauche à droite: ce sont des fonctions sous-séquentielles. Cette problématique sur les quatre opérations arithmétiques est évoquée dans une question de Placiard et dans les réponses données par Lagrange et Monge lors des cours à l'École normale de l'an III, [6, pp. 197–198) et l'incidente mentionnée ci-dessus y ajoute les remarques suivantes: la division peut *presque* se faire de droite à gauche, c'est-à-dire qu'elle est pluri-sous-séquentielle de droite à gauche; par contre, la multiplication n'est pas pluri-sous-séquentielle de gauche à droite.

2. Fonctions rationnelles dans une variété de monoïdes

Soit V une variété de monoïdes, c'est-à-dire [8] une classe de monoïdes finis fermée pour les opérations "quotient", "sous-monoïde" et "produit direct fini". Nous ferons de plus l'hypothèse que V est fermée pour le produit semi-direct. Soit $\alpha: A^* \to B^*$ une fonction (partielle) d'un monoïde libre (finiment engendré) dans un autre.

Si α est sous-séquentielle (de gauche à droite), nous dirons que α *est dans* V si α est réalisée par un transducteur sous-séquentiel dont le monoïde des transitions (obtenu en oubliant les sorties du transducteur) appartient à V; de manière équivalente, le transducteur minimal de α a cette propriété.

Pour la notion de transducteur sous-séquentiel minimal, voir l'article de Choffrut [4, Prop. 4] ou [13, Th. 2]. De manière équivalente, en utilisant les notations de ce dernier article, l'action à droite de A^* sur l'ensemble fini $\{\alpha \cdot w | w \in A^*\}$ détermine un monoïde dans V. Dans le cas où α est séquentielle, cette définition généralise celle d'Eilenberg [8, p. 81; 7, Th. XII.4.2].

Lorsque α est une fonction rationnelle, nous dirons que α *est dans* V si elle satisfait à l'une des conditions équivalentes suivantes:

- α est réallisée par un transducteur non ambigu dont le monoïde des transitions (obtenu en oubliant les sorties) est dans V.
- α est réalisée par une bimachine dont les monoïdes de transitions gauche et droit sont dans V.
- α est le produit de deux fonctions séquentielles (ou sous-séquentielles) dans V, l'une de gauche à droite et l'autre de droite à gauche.

Pour les notions de transducteurs non-ambigus et de bimachines, voir [7, IX.7; 1, IV. 4 et 5]; il faut ici prendre les bimachines comme dans [14], afin de pouvoir réaliser toutes les fonctions rationnelles. L'équivalence de ces définitions résulte des construc-

tions classiques démontrant qu'une fonction est rationnelle si et seulement si elle est réalisée par un transducteur non ambigu (resp. par une bimachine, resp. est produit d'une fonction séquentielle gauche et d'une droite); voir [1, Th. IV. 5.1 et 5.2; 17, 2.3].

Nous nous intéresserons ici aux cas où V est soit la variété A des monoïdes finis apériodiques, soit la variété G des groupes finis.

Nous dirons α *apériodique* pour α dans A, et *à groupe* pour α dans G.

Rappelons que par le théorème des variétés d'Eilenberg, il correspond à toute variété V de monoïdes finis, une variété V de langages rationnels; voir [8, Th. VII. 3.4] ou [10, Th. 2.27]. Rappelons aussi que la *période* d'un langage rationnel $L \subseteq A^*$ est le plus petit multiple commun des exposants des groupes de son monoïde syntaxique, ou de manière équivalente, le plus petit $p \geqslant 1$ tel que: $\forall u, x, v \in A^*$, $ux^n v \in L \Leftrightarrow ux^{n+p}v \in L$, pour tout n assez grand. Enfin, rappelons qu'un *langage rationnel à groupe* est un langage rationnel dont le monoïde syntaxique est un groupe.

Théorème: *Soit $\alpha : A^* \to B^*$ une fonction sous-séquentielle (resp. rationnelle).*

(i) *α est apériodique si et seulement si pour tout langage rationnel L dans B^*, la période du langage $\alpha^{-1}(L)$ divise celle de L.*

(ii) *α est à groupe si et seulement si pour tout langage rationnel à groupe L dans B^*, $\alpha^{-1}(L)$ est un langage rationnel à groupe.*

La partie (ii) est une extension d'un théorème de Choffrut [3, Prop. III. 2.2], qui l'a démontré dans le cas d'une fonction séquentielle.

La partie directe de ces deux assertions est classique; elle résulte des faits suivants:

- Lers variétés A et G sont fermées par produit en couronne (ou de manière équivalente, par produit semi-direct); voir [8, V.8]. Plus généralement, le produit en couronne d'un monoïde de période p par un monoïde de périoide q est de période divisant pq.
- Si α (resp. β) sont des fonctions rationnelles dans V (resp. W), alors la fonction rationnelle produit $\alpha \circ \beta$ est dans $V * W$, la variété engendrée par les produits semi-directs $M * N$, $M \in V$, $N \in W$; voir [8, Prop. VI. 2.1 et Th. 7.3; 16 et 11].
- Le domaine de $\alpha \circ \beta$ est $\alpha^{-1}(\mathrm{dom}\,\beta)$, et la fonction caractéristique β d'un langage rationnel est une fonction rationnelle.

La deuxième partie du théorème mérite un commentaire. Rappelons que *la topologie pro-finie* (ou topologie de Hall, ou de Krull) de A^* est la topologie pour laquelle une base d'ouverts est formée par les rationnels à groupe; voir [12, 15].

On a alors le corollaire suivant.

Corollaire 1. *Soit $\alpha : A^* \to B^*$ une fonction sous-séquentielle (resp. rationnelle). Alors α est à groupe si et seulement si $\alpha|\mathrm{dom}(\alpha)$ est continue pour la topologie profinie et si $\mathrm{dom}(\alpha)$ est un rationnel à groupe.*

La nécessité de cette condition découle des considérations précédentes, puisque α^{-1} préserve alors les rationnels à groupe, donc α est continue. Il n'est pas difficile de voir qu'en fait α est même uniformément continue.

Nous verrons aussi qu'une telle fonction α est presque sous-séquentielle, en ce sens qu'elle est réunion de fonctions sous-séquentielles dont les domaines sont des rationnels à groupe disjoints: elle est donc *pluri-sous-séquentielle*, dans le sens de [5].

Appelons *morphisme affine* $\alpha: A^* \to B^*$ une fonction de la forme $\alpha(w) = u\,\beta(w)\,v$, où $u, v \in B^*$ et β est un morphisme $A^* \to B^*$.

Corollaire 2. *Une fonction rationnelle non vide $\alpha: A^* \to B^*$ est un morphisme affine (resp. un morphisme) si et seulement si α^{-1} divise les périodes et préserve les rationnels à groupe (resp. et si de plus $\alpha(1) = 1$).*

Preuve. Sous ces hypothèses, α est apériodique et à groupe; on peut donc la réaliser par un transducteur dont le monoïde des transitions est le groupe trivial. Comme le mot vide induit l'identité sur l'ensemble des états, il en est de même pour toute lettre de A. Si donc α est non vide, on obtient par suppression des états inutiles, des états qui sont à la fois initiaux et finaux. Comme le transducteur est non ambigu, il y a en fait un seul tel état et α est un morphisme affine. □

3. Généralités

Un transducteur sera pour nous un graphe orienté avec ensemble d'états (sommets) Q, avec arêtes étiquetés dans $A \times B^*$, muni de deux fonctions (partielles) i et f (les *sorties initiales* et *finales*). Ce transducteur réalise la relation $\alpha: A^* \to B^*$ dont le graphe est l'ensemble des couples $(u, i(p)\,v\,f(q))$, pour tous les couples d'états p et q, et tous les chemins de p vers q d'étiquette (u, v). Une telle relation est dite rationnelle, et c'est une fonction rationnelle si elle est de plus fonctionnelle. Une fonction rationnelle peut toujours être réalisée par un transducteur non ambigu, i.e. tel que pour tout mot u, il existe au plus un chemin d'un état initial à un état final d'étiquette de la forme (u, v) (un état q est initial si $i(q) \neq \emptyset$, et final si $f(q) \neq \emptyset$).

La nécessité (mathématique) de la variante ci-dessus des définitions usuelles est illustrée par les transducteurs dans la Fig. 1. Dans celui de gauche, on illustre le fait qu'on a besoin des sorties initiales et finales, car il n'est pas raisonnable d'ajouter un état pour s'en dispenser; dans celui de droite, visiblement à groupe, on voit qu'il faut plusieurs états initiaux et finaux pour avoir un transducteur à groupe.

Le résultat suivant est bien connu. On identifie $\mathbb{N}$ avec le monoïde libre à un générateur.

Lemme 3.1. *Soit $\alpha: \mathbb{N} \to B^*$ une fonction rationnelle. Il existe alors une partie finie F de $\mathbb{N}$, des entiers a, b_i avec $a \geqslant 1$, et des mots x_i, y_i, z_i pour $i = 0, \ldots, r-1$, tels que* $\mathrm{dom}(\alpha)$ *soit la réunion disjointe de F et des $a\,\mathbb{N} + b_i$ et que pour tout n dans $\mathbb{N}$,*

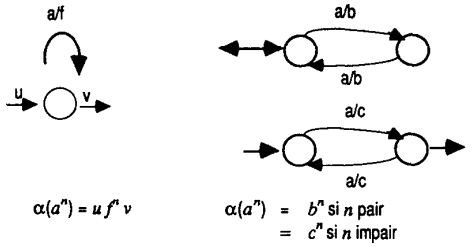


Fig. 1. (a) $\alpha(a^n) = u f^n v$; (b) $\alpha(a^n) = b^n$ si n pair $= c^n$ si n impair.

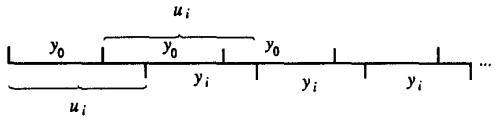


Fig. 2.

$\alpha(an + b_i) = x_i y_i^n z_i$. *On peut borner* $|x_i|$ (*resp.* $|y_i|$, *resp.* $|z_i|$, *resp.* $a, b_i, \max(F)$) *par une fonction ne dépendant que des sorties initiales et des étiquettes* (*resp. que des étiquettes, resp. que des sorties finales et des étiquettes, resp. que du nombre d'états*) *d'un transducteur pour* α.

Pour deux mots u, v, nous notons $\lambda(u, v)$ leur plus long facteur gauche commun. La *distance préfixielle* est définie par $\|u, v\| = |u| + |v| - 2|\lambda(u, v)|$, où $|u|$ est la longueur de u. On définit de manière symétrique la *distance suffixielle*. Nous aurons besoin du lemme combinatoire sur les mots suivants.

Lemme 3.2. *Soient* x_i, y_i, z_i, $0 \leqslant i \leqslant a - 1$, *des mots tels que pour tous* i, j, *les suites* $d(x_i y_i^n z_i, x_j y_j^n z_j)$ *soient bornées, quand* d *est la distance préfixielle et la distance suffixielle. Il existe alors des mots* h, v, w, *et des entiers* s, r_i $(0 \leqslant i \leqslant a - 1)$ *tels que pour tout* n $x_i y_i^n z_i = v h^{sn} h^{r_i} w$.

Preuve. Clairement, les y_i ont tous la même longueur. Pour n grand, $x_i y_i^n z_i$. et $x_j y_j^n z_j$ ont un long préfixe commun, qui excède x_i et x_j: les x_i sont donc tous comparables pour l'ordre préfixiel. Soit x_0 le plus petit d'entr'eux: nous avons $x_i = x_0 u_i$; comme $|y_0| = |y_i|$ et que pour n grand, $y_0^n z_0$ et $u_i y_i^n z_i$ ont un long préfixe commun, nous obtenons $u_i y_i = y_0 u_i$(voir Fig. 2).

Par suite, $x_i y_i^n z_i = x_0 u_i y_i^n z_i = x_0 y_0^n u_i z_i$, et nous sommes ramenés au cas où les suites sont de la forme $v y^n z_i$. Comme ci-dessus, les z_i sont tous comparables pour l'ordre suffixiel, et nous écrivons $z_i = p_i z_0$, ce qui donne: $v y^n z_i = v y^n p_i z_0$. Comme

précédemment, $v\,y^n\,z_0$ et $v\,y^n\,p_i z_0$ ont un long facteur droit commun et ceci implique $y\,p_i = p_i\,y$. Mais alors $y = h^s$, $p_i = h^{r_i}$, d'où finalement $x_i\,y_i^n\,z_i = v\,h^{sn}\,h^{r_i}\,z_0$. □

Rappelons qu'une fonction $\alpha: A^* \to B^*$ est sous séquentielle si et seulement si la congruence à droite $\sim$ de A^* définie par: $u \sim v \Leftrightarrow \exists g \in B^{(*)}$ (le groupe libre sur B) tel que $\forall f \in A^*$, $\alpha(uf) = g\alpha(vf)$, est d'index fini (voir [4]).

On a $u \sim v \Leftrightarrow \alpha \cdot u = \alpha \cdot v$, où $\alpha \cdot u$ est la fonction obtenue à partir de la fonction $f \mapsto \alpha(uf)$ en enlevant à tous les mots $\alpha(uf)$ leur plus long préfixe commun (voir [13]); $(\alpha, u) \mapsto \alpha \cdot u$ est une action à droite du monoïde libre A^*.

Le fait que α est dans une variété V se traduit par le fait que l'action de A^* sur l'ensemble fini $\{\alpha \cdot u | u \in A^*\}$ induit un monoïde dans V. Donc α est apériodique si et seulement si: $\forall f \in A^*$, $\exists n \in \mathbb{N}$ tel que $\forall u \in A^*$, $\alpha \cdot uf^n = \alpha \cdot uf^{n+1}$. Et α est à groupe si et seulement si: $\forall f \in A^*$, $\exists n \in \mathbb{N}^*$ tel que $\forall u \in A^*$, $\alpha \cdot u = \alpha \cdot uf^n$. Dans les deux cas, on peut légèrement affaiblir la condition en mettant "$\forall u \in A^*$ "avant "$\exists n \in \mathbb{N}^*$", puisque l'ensemble $\{\alpha \cdot u | u \in A^*\}$ est fini; on fera ainsi dépendre n de u, mais il n'y a qu'un nombre fini de cas, et on prendra le maximum (resp. le *ppmc*) de tous ces n.

4. Le cas apériodique

Nous disons que α^{-1} *divise les périodes* si pour tout langage rationnel L, la période de $\alpha^{-1}(L)$ divise celle de L. Nous commençons par traiter le cas d'une fonction rationnelle $\mathbb{N} \to \mathbb{N}$. La preuve n'utilise que de l'arithmétique élémentaire.

Lemme 4.1. *Soit $\alpha: \mathbb{N} \to \mathbb{N}$ une fonction rationnelle telle que α^{-1} divise les périodes. Alors α est soit de domaine fini, soit de la forme $\alpha(n) = \rho n + \beta_0$ pour n assez grand, où $\rho, \beta_0 \in \mathbb{N}$.*

Le lecteur se convaincra que l'hypothèse "α^{-1} préserve l'apériodicité" ne suffit pas à assurer la conclusion.

Preuve. Nous pouvons supposer sans perte de généralité que $\mathrm{dom}(\alpha)$ est infini. De même, comme α^{-1} divise les périodes, $\mathrm{dom}(\alpha) = \alpha^{-1}(\mathbb{N})$ est apériodique, donc co-fini, et nous pouvons supposer que $\mathrm{dom}(\alpha) = \mathbb{N}$. Utilisant le Lemme 3.1, nous avons donc pour n dans $\mathbb{N}$, $\alpha(an + i) = \pi_i n + \beta_i$, $i = 0, \ldots, a-1$, où $\pi_i, \beta_i \in \mathbb{N}$.

Rappelons qu'une partie reconnaissable de $\mathbb{Z}$ est une réunion de classes mod. p ($p \in \mathbb{N}^*$), et que sa période est le plus petit tel p. Nous pouvons prolonger α à $\mathbb{Z}$ en prenant la formule ci-dessus pour n dans $\mathbb{Z}$; alors l'hypothèse sur α implique que $\alpha^{-1}(q\mathbb{Z} + d)$ est une partie reconnaissable de $\mathbb{Z}$ de période divisant q. Nous prenons pour q un nombre premier avec a et les π_i, et assez grand.

Notons π_i^1 un entier tel que $\pi_i\,\pi_i^1 \equiv 1 \bmod q$. Les solutions $n \in \mathbb{Z}$ de l'équation $\pi_i n + \beta_i \equiv d \bmod q$ forment l'ensemble $\pi_i^1(d - \beta_i) + q\mathbb{Z}$; par suite $\alpha^{-1}(d + q\mathbb{Z}) = \bigcup_{0 \leqslant i \leqslant a-1} (aq\mathbb{Z} + c_i)$, avec $c_i = i + (d - \beta_i)\,\pi_i^1\,a$. Par hypothèse, la période de cet ensemble divise q. Il faut donc que, pour un entier k,

$\{c_0, \ldots, c_{a-1}\} \equiv \{k, k+q, \ldots, k+q(a-1)\}$ mod. aq Par suite $c_i - c_j \equiv 0 \bmod q$, c'est-à-dire $d\,a(\pi_i^1 - \pi_j^1) + i - j - \beta_i \pi_i^1\, a + \beta_j \pi_j^1\, a \equiv 0$. Ceci n'est possible pour tout d que si $\pi_i^1 \equiv \pi_j^1$, donc $\pi_i \equiv \pi_j$ et enfin $\pi_i = \pi_j$ par le choix de q.

Nous avons donc $\pi_0 = \ldots \pi_{a-1} = \pi$. Par suite, en prenant $j = 0$ ci-dessus, nous obtenons $0 \equiv c_i\pi - c_0\pi = i\pi - a(\beta_i - \beta_0)$. Comme q est grand, on a $i\,\pi = a(\beta_i - \beta_0)$; pour $i = 1$, nous trouvons que a divise π, $\pi = \rho a$, donc $\beta_i = \beta_0 + i\rho$.

Enfin, $\alpha(an+i) = \rho\, an + i\rho + \beta_0 = \rho(an+i) + \beta_0$. Donc α est de la forme voulue. □

Le cas suivant est celui d'une fonction $\mathbb{N} \to B^*$.

Lemme 4.2. *Soit $\alpha : N \to B^*$ une fonction rationnelle telle que α^{-1} divise les périodes. Il existe alors des mots x, y, z dans B^* et un entier N tels que $\forall n \geqslant N$, $\alpha(n) = x\,y^n z$. On peut borner $|x|$ (resp. $|y|$, resp. N) comme dans le Lemme* 3.1.

Preuve. Comme dans la preuve précédente, nous pouvons supposer que dom(α) est infini, donc co-fini.

Par le Lemma 3.1, nous avons alors pour tout n dans $\mathbb{N}$ assez grand,

$$\alpha_i(an+i) = x_i y_i^n z_i, \quad i = 0, 1, \ldots, a-1.$$

Appliquant le Lemme 4.1 à la fonction rationnelle $n \to |\alpha(n)|$, nous obtenons que $|y_i| = \rho a$ et $|x_i| + |z_i| = \beta_0 + i\rho$.

Supposons que $u_i = x_i y_i^n$ et $u_j = x_j y_j^n$ ne soient pas comparables pour l'ordre préfixiel. Alors les langages apériodiques $u_i B^*$ et $u_j B^*$ sont disjoints, et par suite $\alpha^{-1}(u_i B^*)$ contient $a\mathbb{N} + an + i$ et ne rencontre pas $a\mathbb{N} + an + j$. Donc $\alpha^{-1}(u_i B^*)$ n'est apériodique que si $a = 1$.

Nous en concluons que soit $a = 1$ (auquel cas le lemme est démontré), soit que $x_i y_i^n$ et $x_j y_j^n$ sont comparables pour l'ordre préfixiel: donc l'un est préfixe de l'autre et $d(x_i y_i^n z_i, x_j y_j^n z_i)$ est borné pour $n \in \mathbb{N}$, quand d est la distance préfixielle. Il en est de même pour la distance suffixielle.

Nous appliquons le Lemme 3.2 et obtenons que $x_i z y_i^n z_i = v h^{sn} h^{r_i} w$. Par suite, $a\rho = |y_i| = s|h|$ et $|v| + |w| + r_i|h| = \beta_0 + i\rho$. On en déduit $\rho = (r_1 - r_0)|h| = r|h|$, d'où $s = ar$ et $r_i = ir + t$. Finalement, $\alpha_i(an+i) = x_i y_i^n z_i = v\,h^{arn + ir} h^t w = v(h^r)^{an+i} h^t w$, donc $\alpha(n) = v(h^r)^n h^t w$ pour n assez grand, ce qu'il fallait démontrer.

Les assertions sur les bornes découlent des assertions analogues dans le Lemme 3.1. □

Nous pouvons maintenant démontrer le théorème dans le cas apériodique.

Nous supposons d'abord que α est sous-séquentielle. Fixons les mots u et f. Alors pour tout mot v, la fonction $\beta : \mathbb{N} \to B^*$, $n \mapsto \alpha(uf^n v)$ est rationnelle et β^{-1} divise les périodes car β est composée de deux fonctions ayant cette propriété. On a donc d'après le Lemme 4.2: $\alpha(uf^n v) = x_v y_v^n z_v$ pour n assez grand. Comme α est sous-séquentielle, donc uniformément bornée pour la distance préfixielle (voir [14]; à variation bornée selon [4, 1], nous pouvons choisir x_v et y_v indépendamment de v.

On a donc $\alpha(uf^n v) = xy^n z_v$ et $\alpha(uf^{n+1}v) = xy^{n+1}z_v$, ce qui prouve que α est apériodique (cf. la fin du Section 3).

Prenons maintenant une fonction α rationnelle. Dans [14] a été définie la *congruence syntaxique gauche* $\sim$ de α, qui est une congruence à gauche de A^*. Nous montrons que $\sim$ est apériodique, i.e. que pour tout mot f, il existe n tel que pour tout mot v, on ait $f^n v \sim f^{n+1}v$. Ceci revient à montrer que $d(\alpha(uf^n v), \alpha(uf^{n+1}v))$ est borné quand u parcourt A^*, où d est la distance préfixielle. Nous pouvons fixer v (car d'après [14], $\sim$ est d'index fini) et f.

D'après le Lemme 4.2 (appliqué à $\beta_u : n \mapsto \alpha(uf^n v)$), nous avons $\alpha(uf^n v) = x_u y_u^n z_u$ pour $n \geqslant N_u$. On obtient un transducteur T_u pour β_u simplement à partir d'un transducteur pour α, et quand u varie, seul varient l'ensemble des états initiaux et les sorties initiales de T_u.

Donc d'après le même lemme, les mots y_u, z_u sont en nombre fini quand u varie, et N_u est borné. Par suite, $d(\alpha(uf^n v), \alpha(uf^{n+1}v)) = d(x_u y_u^n z_u, x_u y_u^{n+1} z_u) = d(z_u, y_u z_u)$ est borné quand $u \in A^*$, pour $n \geqslant \max_u(N_u)$. Ceci montre que $\sim$ est apériodique.

Nous suivons maintenant la construction de [14, p. 675]. On obtient une transduction séquentielle injective de droite à gauche γ, dont l'automate des entrées est $A^*/\sim$ (donc γ est apériodique), dont l'inverse γ^{-1} est la restriction d'un morphisme à un langage local (donc γ^{-1} est apériodique et γ divise les périodes), et une fonction sous-séquentielle de gauche à droite β telle que $\alpha = \beta \circ \gamma$ et $\beta = \alpha \circ \gamma^{-1}$. Alors $\beta^{-1}(L) = \gamma(\alpha^{-1}(L))$, pour tout langage L, et β divise les périodes. Par ce qui précède, β est apériodique, et il en est donc de même pour α.

Remarque. Soit n un entier et V la variété des monoïdes finis dont la période divise n (cf. [8, p. 280]). Il serait intéressant de caractériser les fonctions rationnelles dans V; la partie (i) du théorème concerne le cas $n = 1$.

5. Le cas des groupes

Rappelons que la topologie pro-finie de B^* est compatible avec sa structure de monoïde, et que $\lim g^{n!} = 1$.

Lemme 5.1. *Soit* $\alpha : \mathbb{N} \to B^*$ *une fonction rationnelle telle que* $\mathrm{dom}(\alpha)$ *soit un rationnel à groupe* $\neq \emptyset$ *et que* $\alpha|\mathrm{dom}(\alpha)$ *est continue pour la topologie pro-finie. Il existe alors* $a \geqslant 1$, $D \subseteq \{0, 1, \ldots, a-1\}$ *et des mots* x_i, y_i, z_i *tels que pour* i *dans* D *et* n *dans* $\mathbb{N}$, $\alpha(an + i) = x_i y_i^n z_i$, *et que* $\mathrm{dom}(\alpha) = \bigcup_{i \in D}(a\mathbb{N} + i)$. *Les nombres* $|x_i|$ *(resp.* $|y_i|$, *resp.* $|z_i|$, *resp.* a*) peuvent être bornés comme dans le Lemme* 3.1.

Preuve. Comme $\mathrm{dom}(\alpha)$ est un rationnel à groupe, le Lemme 3.1 nous donne que $\mathrm{dom}(\alpha) = \bigcup_{i \in D}(a\mathbb{N} + i)$, $D \subseteq \{0, 1, \ldots, a-1\}$ et que pour $i \in D$, $\alpha(an + i) = x_i y_i^n z_i$ sauf peut-être pour un nombre fini de n; mais cette formule est valable pour tout

n, par continuité de α, car $\alpha(an+i) = \lim_{k\to\infty} \alpha(a(n+k!)+i) = \lim_{k\to\infty} x_i y_i^n y_i^{k!} z_i = x_i y_i^n z_i$. □

Pour démontrer le théorème dans le cas (ii), il suffit de démontrer le Corollaire 1, puisque si α^{-1} préserve les langages rationnels à groupe, $\mathrm{dom}(\alpha)$ est un rationnel à groupe, et $\alpha|\mathrm{dom}(\alpha)$ est continue.

Soit d'abord α sous-séquentielle. Pour tout mot f, il existe des entiers p et N tels que pour tout mot u, $\alpha\cdot uf^n = \alpha\cdot uf^{n+p}$ pour $n \geqslant N$. Nous montrons qu'on peut prendre $N=0$, ce qui prouvera que α est à groupe.

Fixons u et f. Il existe un élément g du groupe libre $B^{(*)}$ tel que $\alpha(uf^{n+p}v) = g\alpha(uf^n v)$ pour tout $n \geqslant N$ et tout mot v. Fixons v. La fonction (partielle) $\gamma: \mathbb{N} \to B^{(*)}$, $n \mapsto \alpha(uf^{n+p}v)\alpha(uf^n v)^{-1}$ satisfait donc à $\gamma(n) = g$ si $n \in \mathrm{dom}(\gamma)$ et $n \geqslant N$.

Or, la fonction $n \mapsto uf^n v$ est sous-séquentielle à groupe, donc $\beta: n \mapsto \alpha(uf^n v)$ est sous-séquentielle, son domaine est un rationnel à groupe et $\beta|\mathrm{dom}(\beta)$ est continue. Nécessairement, $\mathrm{dom}(\beta)$ est une réunion de classes mod. p. Alors, $\mathrm{dom}(\gamma) = \mathrm{dom}(\beta)$, pour n dans $\mathrm{dom}(\beta)$, $\gamma(n) = \beta(n+p)\,\beta(n)^{-1}$ et $\gamma|\mathrm{dom}(\gamma)$ est continue.

Si $0 \notin \mathrm{dom}(\beta)$, nous avons $p \notin \mathrm{dom}(\gamma)$ et $\beta(p) = g\beta(0)$. Si $0 \in \mathrm{dom}(\beta)$, alors $p\,\mathbb{N} \subseteq \mathrm{dom}(\beta)$, et par continuité, $\gamma(0) = \lim_{n\to\infty} \gamma(pn!) = g$. Donc $\beta(p) = g\beta(0)$. Nous avons donc $\alpha(uf^p v) = g\,\alpha(uv)$ pour tout v, ce qui montre que $\alpha\cdot uf^p = \alpha\cdot u$. Donc α est à groupe.

Soit maintenant α une fonction rationnelle, avec $\mathrm{dom}(\alpha)$ rationnel à groupe et $\alpha|\mathrm{dom}(\alpha)$ continue. Nous montrons que la congruence syntaxique gauche de α définit un groupe. Il s'agit de montrer que pour tous mots f et v, il existe $p \geqslant 1$ tels que $d(\alpha(uf^p v), \alpha(uv))$ est borné quand u parcourt A^* (d est la distance préfixielle). Fixons f et v et considérons la fonction $\beta_u: \mathbb{N} \to B^*$, $\beta_u(n) = \alpha(uf^n v)$.

Elle satisfait aux hypothèses du Lemma 5.1, et nous en concluons l'existence de mots x_{iu}, y_{iu}, z_{iu}, d'un entier a_u et de $D_u \subseteq \{0,1,\ldots,a_u-1\}$ tels que $\mathrm{dom}(\beta_u) = \bigcup_{i\in D_u}(a_u\mathbb{N}+i)$ et $\beta_u(a_u n+i) = x_{iu}y_{iu}^n z_{iu}$ pour $n \in \mathbb{N}$ et $i \in D_u$. Un transducteur pour β_u s'obtient simplement à partir d'un transducteur pour α, et quand u varie, seuls varient l'ensemble des états initiaux et les sorties initiales. Par suite, les y_{iu}, z_{iu}, a_u et D_u sont en nombre fini quand u parcourt A^*.

Soit p le *ppmc* des a_u. Alors, soit $\beta_u(0) = \beta_u(p) = \emptyset$, soit $\beta_u(0) = x_{0u}z_{0u}$ et $\beta_u(p) = x_{0u}y_{0u}z_{0u}$. Donc $d(\alpha(uv), \alpha(uf^p v)) = d(\beta_u(0), \beta_u(p)) = d(x_{0u}z_{0u}, x_{0u}y_{0u}z_{0u}) = d(z_{0u}, y_{0u}z_{0u})$ qui est borné quand u parcourt A^*.

Comme la congruence syntaxique gauche de α est à groupe, il existe un groupe fini G et un homomorphisme $\varphi: A^* \to G$ tel que: $\forall x,\ y \in A^*,\ \varphi(x) = \varphi(y) \Rightarrow d(\alpha(fx), \alpha(fy))$ est borné quand f parcourt A^*.

Soit $L_g = \varphi^{-1}(g)$. Nous montrons que $\alpha|L_g$ est sous-séquentielle à groupe. On en déduira que α est à groupe: on obtient en effet un transducteur non ambigu pour α en prenant la réunion des transducteurs non ambigus des $\alpha|L_g$, $g \in G$.

Il suffit de monter que $\alpha|L_g$ est sous-séquentielle, puisqu'alors son domaine est le rationnel à groupe $\mathrm{dom}(\alpha)\cap L_g$, et que sa restriction à ce domaine est continue. D'après le théorème de Choffrut [4], il est suffisant de montrer que $\alpha|L_g$ est

uniformément bornée, i.e. $\forall k$, $\exists K$ tel que $\forall u,\ v \in L_g,\ \alpha(u) \neq \emptyset \neq \alpha(v)$ et $d(u,v) \leqslant k \Rightarrow d(\alpha(u), \alpha(v)) \leqslant K$. Si $d(u,v) \leqslant k$ et $u, v \in L_g$, nous avons $u = f\,x$, $v = f\,y$ avec $|x| + |y| \leqslant k$. De plus, $\varphi(u) = \varphi(v) = g \Rightarrow \varphi(x) = \varphi(y)$. De la relation après la définition de φ et de la finitude de l'ensemble des mots x, y sujets à $|x| + |y| \leqslant k$, nous pouvons déduire l'existence d'une borne K, ne dépendant pas de f, telle que $d(\alpha(u), \alpha(v)) \leqslant K$.

"*... Je désirerais que vous développassiez les raisons pour lesquelles on commence plutôt cette dernière par la gauche que par la droite ...*"
Placiard [6, *p.* 197]

6. Exemples

Soit b un entier $\geqslant 2$ fixé, et $A = \{0, 1, \ldots, b-1\}$. Pour un entier $a \geqslant 1$ fixé, soit $d_a : A^* \to A^*$ la *division euclidienne par a en base b*, i.e. la fonction qui à un mot u, représentant l'entier n en base b, associe l'unique mot v de même longueur que u, représentant l'entier q tel que $n = qa + r$, $0 \leqslant r < a$.

La fonction d_a est séquentielle de gauche à droite. Si a et b sont premiers entr'eux, elle est sous-séquentielle à groupe, et le groupe associé est le groupe des transformations de $\mathbb{Z}/a\mathbb{Z}$ engendré par les b transformations $r \mapsto rb + i$ mod. a, pour $i = 0, 1, \ldots, b-1$.

La fonction d_a est donc pluri-sous-séquentielle de droite à gauche, et l'on peut faire la division de droite à gauche, pourvu qu'on ait sur n une information supplémentaire: à savoir n mod. a. Voir Fig. 3, où il faut lire le nombre binaire n de droite à gauche, en partant de l'état n mod. 3.

Lorsque a et b ne sont pas premiers entr'eux, la division se fait en deux temps: on écrit $a = a'\,a''$, $(a', b) = 1$, où tout diviseur premier de a'' divise b. Alors, comme on l'a vu, $d_{a'}$ est pluri-sous-séquentielle de droite à gauche, et $d_{a''}$ est sous-séquentielle de droite à gauche (voir [13] par exemple). On a $d_a = d_{a'} d_{a''}$, et l'on observe que le produit de deux fonctions pluri-sous-séquentielles l'est aussi.

Venons-en à la *multiplication par a en base b* $m_a : A^* \to A^*$.

Cette fonction est sous-séquentielle de droite à gauche comme on le sait intuitivement (voir [13] pour une preuve formelle). Elle est apériodique. Nous le vérifions pour $1 \leqslant a \leqslant b-1$.

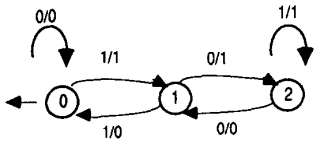


Fig. 3. La division par 3 en base 2 de droite à gauche.

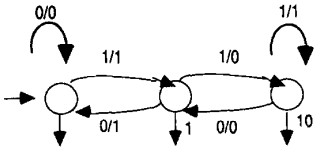


Fig. 4. La multiplication par 3 en base 2.

Dans ce cas, on réalise la fonction m_a à l'aide d'un transducteur sous-séquentiel de droite à gauche, dont l'ensemble des états est $R = \{0, 1, \ldots, a-1\}$, i.e. les reports, ou retenues, possibles quand on multiplie par a. Chaque lettre i de l'alphabet $\{0, 1, \ldots, b-1\}$ induit sur R la fonction $f_i(r) = [(ai + r)/b]$. Chaque fonction $f = f_i$ satisfait à $r \leqslant r' \Rightarrow f(r) \leqslant f(r')$, et il en est de même pour toute fonction dans le sous-monoïde engendré par les f_i. Donc aucune de ces fonctions n'induit de bijection non triviale sur une partie de R, ce qui montre que ce monoïde est apériodique.

Ainsi m_a est apériodique.

Dans la Fig. 4, nous donnons l'exemple de la multiplication par 3 en base 2 (cet automate nous a été aimablement communiqué par Colin de la Higueira, et simplifie celui de [13]); il faut y lire les nombres binaires de droite à gauche. On peut vérifier que l'automate de gauche à droite associé (obtenu en renversant les flèches) a des branchements absolus et par suite [5, Th. IV. 1] la multiplication n'est pas pluri-sous-séquentielle de gauche à droite.

Aux exemples précédents, il faut rajouter les travaux de [2], qui considère divers types d'addition, ainsi que ceux de [9], pour la base Fibonacci; il s'y pose aussi le problème de la normalisation dans cette base, qui est une fonction rationnelle.

Références

[1] J. Berstel, *Transductions and Context-Free Languages* (Teubner, Leipzig, 1979).
[2] J. Berstel, Fonctions rationnelles et addition, École de Printemps d'Informatique Théorique, Murol, Litp/Ensta, Paris, 1981.
[3] C. Choffrut, Contribution à l'étude de quelques familles remarquables de fonctions rationnelles, Thèse Doctorat d'Etat, Univ. Paris VII, 1978.
[4] C. Choffrut, A generalization of Ginsburg and Rose's characterization of *g-s-m* mappings, dans: Lecture Notes in Computer Science, Vol. 71 (Springer, Berlin, 1979) 88–103.
[5] C. Choffrut et M.P. Schützenberger, Décomposition des fonctions rationnelles, dans: Lecture Notes in Computer Science, Vol. 210 (Springer, Berlin, 1986) 213–226.
[6] J. Dhombres, *L'École Normale de l'An III, Leçons de Mathématiques* (Laplace, Lagrange et Monge) (Dunod, Paris, 1992).
[7] S. Eilenberg, *Automata, Languages and Machines, Vol. A* (Academic Press, New York, 1974).
[8] S. Eilenberg, *Automata, Languages and Machines, Vol. B* (Academic Press, New York 1976).
[9] C. Frougny, Representation of numbers and finite automata, *Math. Systems Theory* **25** (1992) 37–60.
[10] J.-E. Pin, *Variétés de Langages Formels* (Masson, Paris, 1984).

[11] J.-E. Pin, J. Sakarovitch, Une application de la représentation matricielle des transductions, *Theoret. Comput. Sci.* **35** (1985) 271–293.
[12] J.-E. Pin, Topologies for the free monoid, *J. Algebra* **137** (1991) 297–337.
[13] C. Reutenauer, Subsequential functions: characterizations, minimization, examples, dans Lecture Notes in Computer Science, Vol. 464 (Springer, Berlin, 1990) 62–79.
[14] C. Reutenauer et M.P. Schützenberger, Minimization of rational word functions, *SIAM J. Comput.* **20** (1991) 669–685.
[15] L. Ribes et P.A. Zaleskii, On the profinite completion on a free group, *Bull. London Math. Soc.* **25** (1993) 37–43.
[16] J. Sakarovitch, Sur la définition du produit en couronne, dans: G. Pirillo, éd., *Actes du Colloque "Codages et Transductions"* (CNR, Rome, 1979) 285–300.
[17] M.P. Schützenberger, Sur les relations rationnelles entre monoïdes libres, *Theoret. Comput. Sci.* **3** (1976) 243–259.

Années 1996-2000

Bibliographie

[1996-1] Alain Lascoux et Marcel-Paul Schützenberger. Treillis et bases des groupes de Coxeter. *Electron. J. Combin.*, 3(2) :Research paper 27, approx. 35 pp. (electronic), 1996.

[1997-1] Marcel-Paul Schützenberger. Une sotie au sujet de la théorie des nombres parfaits. In R. Ellrodt, G. Gadoffre et J.-M. Maulpoix, editors, *L'acte créateur*, Collection Écriture, pages 233–140. Presses Universitaires de France, 1997. aussi parue dans Conjonctures.

[1997-1] Marcel-Paul Schützenberger. Pour le monoïde plaxique. *Math. Inform. Sci. Humaines*, 140 :5–10, 1997.

[2000-1] Alain Connes, André Lichnerowicz et Marcel-Paul Schützenberger. *Triangle de pensées*. Odile Jacob, Paris, 2000.

1996-1. Treillis et bases des groupes de Coxeter Année 1996

Treillis et bases des groupes de Coxeter

Alain Lascoux(*) et Marcel-Paul Schützenberger

A Dominique Foata,
pionnier de la combinatoire
à qui elle doit tant

1. Introduction. — Le présent travail est une contribution à l'étude de l'ordre fort (dit aussi de Bruhat) dans un groupe de Coxeter fini W.

Les définitions et propriétés relatives aux treillis, aux ensembles ordonnés, aux *bases* et aux *treillis enveloppants*, &c. sont rassemblées de manière minimale dans la section 2, les preuves et quelques exemples étant présentés en annexe, également de façon minimale.

La *base* B d'un ensemble ordonné fini $(X, \leq)$ est le plus petit sous-ensemble tel que la comparaison de deux éléments pour l'ordre $\leq$ soit donné par l'ordre d'inclusion des projections (dans 2^B) de ces éléments sur la base. La section 3 décrit les rapports entre les ordres faibles et fort sur les groupes de Coxeter, en les reliant à diverses algèbres de Hecke dégénérées. La base (pour l'ordre fort) est contenue dans l'ensemble de ce que nous appelons les *bigrassmanniennes* (éléments $w \in W$ tels qu'il existe une seule paire de générateurs σ, σ' tels que $\ell(\sigma\mu) < \ell(\mu)$, $\ell(\mu\sigma') < \ell(\mu)$).

La section 4 détaille le cas du groupe symétrique, pour lequel l'ordre fort a été décrit par Ehresmann en termes d'objets combinatoires que nous appelons *clefs*. La base est exactement l'ensemble des bigrassmanniennes. Ces dernières dépendent de 4 paramètres (en incluant l'ordre n du groupe), et leur nombre est $\binom{n+1}{3}$. Nous montrons que le treillis enveloppant est distributif, en application d'un énoncé plus général sur les propriétés de clivage des treillis enveloppants.

Dans la section suivante, nous identifions les éléments du treillis enveloppant à des objets combinatoires très intéressants, les *triangles*, qui ont déjà été rencontrés dans un autre contexte, celui des matrices alternantes. Nous montrons que les permutations vexillaires se caractérisent de façon simple en terme de leur projection sur la base.

La section 6 utilise la même notion de clivage pour découper de façon itérée le groupe symétrique en intervalles remarquables, isomorphes aux intervalles inférieurs des bigrassmanniennes. Nous donnons les polynômes de Poincaré de ces intervalles.

La section 7 étend les résultats des sections 4 et 5 aux groupes de type B_n. Cette fois-ci, la base ne contient pas toutes les bigrassmanniennes,

(*) Soutenu par le PRC Math-Info et la bourse CEE n^0 ERBCHRXCT930400

mais le treillis enveloppant reste distributif. Le treillis de B_n est en fait un sous-treillis du treillis enveloppant de $\mathfrak{S}(2n)$.

Les bases de tous les groupes de Coxeter finis viennent d'être obtenues dans un article récent de M. Geck et S. Kim [G-Ki].

2. Treillis enveloppant. — Renvoyant les preuves à une annexe, nous nous limitons ici à énoncer les propriétés des treillis dont nous aurons besoin. La plupart de celles ci sont bien connues et nous faisons référence au grand traité de G.Birkhoff [Bi] (et spécialement aux chapitres III et IX) pour une théorie plus complète ainsi que pour les attributions de priorité.

Si $(X, \leq)$ est un ensemble ordonné et $x \in X$, nous notons $[x \leq]$ l'intervalle supérieur $\{y \in X : x \leq y\}$ et symétriquement, $[\leq x] := \{y \in X : y \leq x]\}$. L'*infimum* $\wedge Y = Inf(Y)$ d'une partie Y de X est l'unique élément $x \in X$ tel que

$$[\leq x] = \cap\{[\leq y] : y \in Y\}$$

s'il en existe un, et $\wedge Y = \emptyset$ sinon. Symétriquement, le *supremum* $\vee Y = Sup(Y)$ est l'unique $x' \in X$ tel que

$$[x' \leq] = \cap\{[y \leq] : y \in Y\}$$

s'il en existe un, $\emptyset$ sinon.

Un ensemble ordonné $(X, \leq)$ est un treillis (sous-entendu *complet*) ssi toute partie Y non vide admet un *Inf* (et donc ausi un *Sup*, ainsi qu'on le voit facilement, en prenant le *Inf* de l'ensemble des z tels que $Y \subset [\leq z]$).

C'est un théorème classique dû à Mac Neille qu'il existe un treillis minimal unique $(T, \leq)$ et un isomorphisme d'ordre $X \to T$ commutant avec les opérations $\wedge$ et $\vee$ quand leur valeur est un élément de X.

Ce treillis $(T, \subset)$ est la plus petite famille de parties de X qui contienne X, tous les intervalles supérieurs $[x \leq]$, $x \in X$, et qui soit fermée par l'intersection ensembliste $\cap$. L'injection naturelle $x \longrightarrow [x \leq]$ de $(X, \leq)$ dans $(T, \subset)$ fait donc correspondre à l'opération *Sup* de $(X, \leq)$ l'opération $\cap$ de $(2^X, \subset)$ qui est l'opération *Inf* de $(T, \subset)$; l'opération *Inf* de $(X, \leq)$ correspond quant à elle au *Sup* de $(T, \subset)$, où cette dernière opération est définie de façon indirecte, ainsi que nous l'avons indiqué plus haut.

Nous appelerons T le *treillis enveloppant de* $(X, \leq)$ bien que l'usage soit d'appeler T la "complétion de $(X, \leq)$)", parce que cette construction, qui ne fait appel à aucune hypothèse de finitude, constitue une généralisation

naturelle de la construction de Dedekind (correspondant elle-même au cas où l'ordre sur X est un ordre total).

On sait que de façon équivalente dans le cas fini, un treillis fini est un monoide *commutatif idempotent finiment engendré* (pour l'une quelconque des deux opérations), la relation d'ordre et la seconde opération étant alors canoniquement construites en terme de la première opération.

L'apport de la théorie des treillis au présent travail consiste essentiellement en les deux définitions suivantes et la proposition 2.5 :

Définition 2.1. — Une *relation basique* est un relation $\mathcal{R}$ entre deux ensembles $\bar{B}$ et B telle que, en considérant $\mathcal{R} \in \bar{B} \times B$ comme une matrice booléenne, aucune ligne de $\mathcal{R}$ ne soit l'intersection de lignes, que la ligne composée entièrement de $\mathbf{1}$ n'appartienne pas à $\mathcal{R}$, et que les conditions symétriques soient satisfaites par les colonnes de $\mathcal{R}$.

Définition 2.2. — La *base* B (resp. la *cobase* $\bar{B}$) de $(X, \leq)$ est l'ensemble des $x \in X \setminus \wedge X$ (resp. $x \in X \setminus \vee X$) tels que x ne puisse être obtenu comme le Sup (resp. le Inf) d'autres éléments, c'est-à-dire $x \in B$ (resp. $x \in \bar{B}$) si pour toute partie Y,

$$x \notin Y \Rightarrow x \neq Sup(Y) \text{ (resp. } x \neq Inf(Y) \text{) } .$$

Nous supposerons désormais que tous les ensembles considérés sont finis.

Nous utiliserons la caractérisation suivante de la base, qui permet le calcul de cette dernière par simple inspection des triples d'éléments de X, puisque l'assertion que x est minimal dans $X \setminus [\leq z]$ pour un $z \notin [x \leq]$ équivaut à $[< x] \setminus [\leq z] = \emptyset$.

Lemme 2.3. — *Un élément $x \neq \wedge X$ appartient à la base B ssi il est un élément minimal de $X \setminus [\leq z]$ pour au moins un $z \in X$.*

Dans le cas particulier où $(X, \leq)$ est un treillis, on a que $x \in B$ ssi x couvre un et un seul élément de X, c'est-à-dire ssi x est un $\vee$-générateur.

La base satisfait de plus une propriété de minimalité :

Proposition 2.4. — *La projection $\beta : X \ni x \to B \cap [\leq x] \in (2^B, \subset)$ est un isomorphisme d'ordre et l'on a $B \subset C$ pour toute partie C de X ayant la même propriété.*

Ceci permet de coder chaque élément x par l'ensemble des élements maximaux de $x\beta$, c'est à dire par ce que nous appelerons ses *rectrices*.

On a de même la projection $\bar{\beta}$ de chaque élément de X sur la cobase.

Soit $\mathcal{R}' \subset \bar{B} \times B$ la relation définie par $(\bar{b}, b) \in \mathcal{R}'$ ssi $\bar{b} \geq b$, c'est-à-dire, de façon équivalente, ssi $b \in \bar{b}\beta$ ou $\bar{b} \in b\bar{\beta}$.

PROPOSITION 2.5. — *La relation $\mathcal{R}'$ est une relation basique.*

Nous appelerons désormais la relation $\mathcal{R}'$ précédente la *relation basique* de l'ensemble ordonné $(X, \leq)$.

THÉORÈME 2.6. — *Chaque ensemble ordonné a même relation basique que son treillis enveloppant.*

Nous introduisons encore la

Définition 2.7. — La paire d'éléments $(\bar{x}, x)$ de l'ensemble ordonné $(X, \leq)$ *clive* X ssi X est l'union disjointe de $[\leq \bar{x}]$ et $[x \leq]$.

Les clivages de X sont en bijection avec ceux de son treilis enveloppant, et les paires clivantes $(\bar{x}, x)$sont nécessairement des éléments de $\bar{B} \times B$, ce qui permet d'énoncer un résultat classique de Birkhoff sous la forme modifiée suivante:

THÉORÈME 2.8. — *Une condition nécessaire et suffisante pour que le treillis enveloppant d'un ensemble ordonné $(X, \leq)$ soit distributif est qu'il existe un isomorphisme d'ordre bijectif entre sa base et sa cobase tel que chaque paire d'éléments associés donne un clivage.*

Comme il est bien connu, il y a bijection, pour un treillis distributif, entre les antichaînes de la restriction de la relation d'ordre à la base et les éléments du treillis: c'est un cas particulier de la correspondance entre les éléments et leurs rectrices.

3. Ordres sur les groupes de Coxeter et algèbres de Iwahori-Hecke dégénérées. — Soit (W, S) un groupe de Coxeter fini, S un système de générateurs. L'algèbre d' Iwahori-Hecke $\mathcal{H}(W, p, q)$ est l'algèbre engendrée par des éléments T_s vérifiant les relations de Coxeter, plus les relations de Hecke (homogénéisées)

$$T_s^2 = (p+q)T_s - pq \ ,$$

où p, q sont deux constantes commutant avec les T_s. Pour le groupe symétrique, nous nous sommes attachés à développer les cas $T_s^2 = 0$ (différences divisées), $T_s^2 = T_s$ (différences divisées isobares), $T_s^2 = -T_s$, sans oublier l'algèbre du groupe ($T_s^2 = 1$) , cf. [L-S 1], [L-S 2], et aussi [Ch] pour ce qui concerne les algèbres de Hecke affines.

Employons des notations différentes pour distinguer les quatre cas spéciaux ci-dessus (pour les valeurs des paramètres p, q respectivement égales à $(0,0)$, $(0,1)$, $(0,-1)$ et $(1,-1)$):

$$\partial_s\ ,\ \pi_s\ ,\ \bar{\pi}_s\ ,\ s$$

vérifiant respectivement

$$\partial_s^2 = 0\ ,\ \pi_s^2 = \pi_s\ ,\ \bar{\pi}_s^2 = -\bar{\pi}_s\ ,\ s^2 = 1\ .$$

Pour chacune de ces algèbres, nous considérerons aussi le monoide engendré par les générateurs T_i.

L'algèbre d' Iwahori-Hecke admet une base linéaire $\{T_w\}_{w\in W}$, en bijection avec les éléments du groupe, que nous noterons respectivement $\{\partial_w\}$, $\{\pi_w\}$, $\{\bar{\pi}_w\}$ et $\{w\}$ dans les cas spéciaux, l'algèbre étant elle-même $\mathcal{H}^\partial$, $\mathcal{H}^\pi$, $\mathcal{H}^{\bar{\pi}}$ et $\mathcal{H}^s$ respectivement.

Les ∂_w permettent de définir la *longueur* des éléments de W, les *décompositions réduites* et l'ordre *faible* droit ou gauche sur W.

Définitions. — Etant donné $w \in W$, la longueur maximum d'une factorisation dans le monoide des ∂_i: $\partial_w = \partial^1\partial^2\cdots\partial^k$ (en facteurs $\neq 1$) est dite *longueur* de w et notée $\ell(w)$. Une factorisation de longueur maximum est telle que les facteurs $\partial^1, \ldots, \partial^k$ sont des générateurs. La factorisation correspondante dans W : $w = s^1\cdots s^k$ est une *décomposition réduite* de w.

Deux éléments sont comparables pour l'ordre *faible* droit : $v \leq_R w$ ssi ∂_v est facteur gauche de ∂_w, i.e. s'il existe $u \in W$ tel que

$$\partial_v\,\partial_u = \partial_w\ .$$

Symétriquement, $v \leq_L w$ ssi ∂_v est facteur droit de ∂_w.

Etant donnés deux éléments w, w' de W, il existe un plus petit $v \in W$ (pour l'ordre droit) tel que ∂_v ait pour facteur gauche ∂_w et $\partial_{w'}$. En d'autres termes, l'intersection des idéaux $\partial_w\mathcal{H}^\partial$ et $\partial_{w'}\mathcal{H}^\partial$ est un idéal principal ($= \partial_v\mathcal{H}^\partial$).

Similairement, il existe un plus grand facteur gauche ∂_v de ∂_w et $\partial_{w'}$.

L'existence d'un plus grand facteur gauche et d'un plus petit commun multiple signifie que W, muni de l'ordre $<_R$, est un treillis. Cette propriété a été montré par Guilbaud & Rosensthiel [G-R] pour le groupe symétrique, et est due à Björner pour les autres groupes de Coxeter finis [Bj].

Symétriquement, l'ordre faible gauche donne une deuxième structure de treillis, image de la précédente par inversion des permutations.

A chacune des deux structures de treillis correspond une base.

Définitions. — Pour $w \in W$, l'ensemble des *descentes* (resp *reculs*) de w est le sous-ensemble des générateurs de W tels que $\partial_w\partial_s = 0$ (resp.

$\partial_s \partial_w = 0$). Un élément est dit *grassmannien* s'il n'a qu'une descente. Une *bigrassmannienne* est un élément de W ayant une seule descente et un seul recul.

La base de W, muni de l'ordre $<_R$, est constituée des éléments grassmanniens, puisque ceux-ci sont exactement les $w \in W$ ayant un et un seul successeur.

Soit s un générateur du groupe de Coxeter $(W, \mathcal{S})$. Le sous-ensemble des éléments grassmanniens ayant s pour descente, auquel on adjoint l'identité, est un treillis pour l'ordre $<_L$ (cf. [B-W]). Cet ensemble est usuellement noté W^s; ses éléments sont les représentants de longueur minimum des classes $W \,/\, W(\mathcal{S}\backslash s)$, où $W(\mathcal{S}\backslash s)$ est le parabolique engendré par tous les générateurs sauf s.

Le morphisme $p_s : W \to W^s$ qui à chaque élément de W associe l'élément de longueur minimum de sa classe modulo $W(\mathcal{S} \setminus s)$ est défini par

$$p_s(w) = g \;\Leftrightarrow\; \partial_g \text{ est le plus grand facteur gauche de } w,\ g \in W^s$$

Il est équivalent de rechercher les décompositions $\partial_w = \partial_g \, \partial_v$, $v \in W(\mathcal{S} \setminus s)$, telles que ∂_v soit de longueur maximale parmi les facteurs droits de ∂_w appartenant à $W(\mathcal{S} \setminus s)$.

On peut aussi munir W du plus petit ordre (*ordre bifaible*) contenant $<_L$ et $<_R$ et étudier les propriétés des *facteurs* des ∂_w.

La considération des *sous-mots* conduit, quant à elle, à définir un ordre dit *fort* ou *de Bruhat* que nous noterons désormais $\leq$.

Définitions. — On a a $v \leq w$ ssi ∂_v est un sous-mot de ∂_w, i.e. s'il existe deux factorisations

$$\partial_v = \partial_{v_1} \, \partial_{v_2} \cdots \partial_{v_k} \quad \text{et} \quad \partial_w = \partial_{w'} \, \partial_{v_1} \, \partial_{w''} \, \partial_{v_2} \, \partial_{w'''} \cdots \partial_{v_k} \, \partial_{w''''}.$$

Il suffit en fait de ne considérer que les sous-mots d'une seule décomposition réduite arbitraire de w pour obtenir tous les éléments $v \leq w$ (cf. [Bo]).

Les idéaux d'ordre pour l'ordre fort se décrivent aisément dans l'algèbre $\mathcal{H}^{\bar{\pi}}$. On a en effet la récurrence suivante ([Vr]):

LEMME 3.1. — *Soient $w \in W$, $s \in \mathcal{S}$, tels que $\ell(w) < \ell(ws)$. Alors l'intervalle inférieur $[\leq w]$ se décompose en deux sous-ensembles $\{v : v < w, vs < w\}$ et $\{u : u \leq w, us \not< w\}$, et l'intervalle $[\leq ws]$ est égal à*

$$[\leq w] \cup \{us : u \leq w, us \not< w\} \quad .$$

COROLLAIRE 3.2. — *Pour tout* w,

$$\pi_w = \sum_{v \le w} \bar{\pi}_v$$

et

$$\bar{\pi}_w = \sum_{v \le w} (-1)^{\ell(w)-\ell(v)}\, \pi_v \quad .$$

En effet, soient v et s tels que $\ell(v) < \ell(vs)$. Alors $(\bar{\pi}_v + \bar{\pi}_{vs})\pi_s = \bar{\pi}_v + \bar{\pi}_{vs}$, $\bar{\pi}_v \pi_s = \bar{\pi}_v + \bar{\pi}_{vs}$; $(\pi_{vs} - \pi_v)\bar{\pi}_s = -\pi_{vs} + \pi_v$, $\pi_v \bar{\pi}_s = \pi_{vs} - \pi_v$ □

Ce corollaire est utilisé de manière essentielle par Fokko du Cloux [Fo] pour implémenter l'ordre fort sur les groupes de Coxeter.

L'ordre fort peut s'obtenir à partir de la restriction de l'ordre aux sous-ensembles W^s, $s \in \mathcal{S}$, ainsi que l'établit le lemme suivant dû à Deodhar [De], qui généralise la définition géométrique de l'ordre fort donnée par Ehresmann [Eh] pour le groupe symétrique.

LEMME 3.3. — *Soient* $v, w \in W$. *Alors* $w \ge v$ *ssi pour tout* $s \in \mathcal{S}$, $p_s(w) \ge p_s(v)$.

Comme les morphismes p_s sont des morphismes d'ordre, on peut écrire la propriété précédente

$$w \ge v \;\Leftrightarrow\; \forall s \in \mathcal{S},\; w \ge p_s(v) \tag{3.4}$$

Plus symétriquement en la droite et la gauche, soient deux générateurs $r, s \in \mathcal{S}$ et ${}^rW^s$ l'ensemble des bigrassmanniennes ayant recul r, descente s, ensemble auquel on adjoint l'identité. Cet ensemble est formé des éléments minimaux des classes $W(\mathcal{S}\backslash r) \setminus W / W(\mathcal{S}\backslash s)$.

On dispose d'une projection $p_{r,s} : W \to {}^rW^s$ telle que

$$p_{r,s}(w) = g \;\Leftrightarrow\; \partial_w = \partial_{w'} \partial_g \partial_{w''} \ ,$$

où ∂_g est un facteur de ∂_w de plus grande longueur parmi les $g \in {}^rW^s$.

L'unicité d'un tel facteur provient de ce que les deux projections $W \to W / (\mathcal{S}\backslash s)$ et $W \to W(\mathcal{S}\backslash r) \setminus W$ commutent.

La propriété (3.4) implique

$$w \ge v \;\Leftrightarrow\; \forall r, \forall s \in \mathcal{S},\; w \ge p_{r,s}(v) \ . \tag{3.5}$$

A tout élément $w \in W$, on associe l'élément

$$p_{\mathcal{G}}(w) := \{g \in \mathcal{G},\, g \le w\} \subseteq 2^{\mathcal{G}} \ ,$$

où $\mathcal{G}$ est l'ensemble des bigrassmanniennes.

THÉORÉME 3.6. — *Soit $(W, \mathcal{S})$ un groupe de Coxeter fini. Alors la base B de W, en tant qu'ensemble muni de l'ordre fort, est contenue dans l'ensemble $\mathcal{G}$ des bigrassmanniennes.*

Une bigrassmannienne b ayant recul r et descente s appartient à la base ssi elle n'est pas le supremum d'un sous-ensemble de bigrassamnniennes ($\neq b$) de mêmes descente et recul.

Preuve. — La propriété (3.5) implique que $p_{\mathcal{G}}$ soit un morphisme d'ordre. En outre $p_{\mathcal{G}}$ est injectif, car chaque élément w est déterminé par l'ensemble des $p_{r,s}(w)\,, r, s \in \mathcal{S}$, qui est un sous-ensemble de $p_{\mathcal{G}}(w)$. La caractérisation par minimalité de la base donnée en (2.4) implique que $\mathcal{G}$ contienne la base.

Les éléments de l'ensemble $W \backslash B$ sont les éléments de W dont l'ensemble des rectrices est de cardinal $\neq 1$. Soit g une bigrassmanienne de descente s et recul r, et soit $\{b_1, \ldots, b_k\}$ l'ensemble de ses rectrices. Supposons que $k > 1$. Alors tous les b_i, $i = 1 \ldots k$, ont mêmes descente et recul que g . En effet, s'il existe i tel que b_i ait descente $s' \neq s$, alors $b_i > b_i s'$ et $w < ws'$. Soient $b_{k+1}, \ldots, b_h$ les rectrices de $b_i s'$. La condition $w \geq b_i$ est équivalente à $w \geq b_i s'$, elle même équivalente à $w \geq b_{k+1}, \ldots, w \geq b_h$. L'élément w est donc le supremum de l'ensemble $\{b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_h\}$, ce qui est impossible puisque cet ensemble ne contient pas la rectrice b_i.

Réciproquement, si une bigrassmannienne dans ${}^rW^s$ est le supremum de $\{g_1, \ldots, g_k\} \subseteq {}^rW^s$, $k > 1$, alors elle est le supremum de leurs rectrices qui appartiennent toutes à ${}^rW^s$. Ainsi donc une bigrassmannienne de descente s et recul r n'appartient pas à la base ssi elle est le supremum d'un ensemble de cardinal > 1 de bigrassmanniennes dans ${}^rW^s$ deux à deux incomparables □

Nous détaillons par la suite les bases des groupes classiques de type A_n et B_n.

4. Ehresmannoedre. — L'ordre fort, dit aussi de Bruhat, sur le groupe symétrique est usuellement défini comme la clôture transitive des relations de consécutivité

$$\{\nu \rightarrow \mu\} \;\Leftrightarrow\; \{\exists \tau : \mu = \nu\tau \;,\; \ell(\mu) = \ell(\nu) + 1\} \;,$$

où ν, μ sont deux permutations et τ une transposition, plutôt que par sous-mots des décompositions réduites comme au paragraphe 2.

Le groupe symétrique, muni de cet ordre, est dit *Ehresmannoedre*. Nous allons voir que sa base consiste en l'ensemble des bigrassmanniennes. La base est donc exactement l'intersection des bases pour les ordres faibles droit et gauche.

La définition originelle d'Ehresmann [Eh] de l'ordre sur le groupe symétrique repose quant à elle sur la comparaison des ensembles.

Deux sous-ensembles A et B d'un ensemble totalement ordonné sont *comparables* : $A \leq B$ ssi il existe un morphisme injectif de A dans B. Une suite d'ensembles se représente planairement par une suite de colonnes décroissantes justifiée par le haut, ces colonnes étant les ensembles réordonnés composant la suite. La suite d'ensembles est une *chaîne* (i.e. est croissante) si l'objet planaire est un *contretableau*, i.e. si les colonnes sont de longueurs croissantes, et si toutes les lignes sont croissantes de gauche à droite.

Etant donnés deux contretableaux t et t' de même forme, on dit que $t \leq t'$ ssi chaque composante de t est inférieure à la composante de t' situéee au même endroit. On notera que la restriction de l'ordre au sous-ensemble des colonnes coïncide bien avec l'ordre sur les ensembles sous-jacents.

Les facteurs gauches successifs d'une permutation μ sont une suite d' ensembles emboîtés (un *drapeau*). Le contretableau associé est dit $clef(\mu)$.

Ainsi $\mu = 2413$ a pour clef

$$\begin{array}{cccc} 2 & 4 & 4 & 4 \\ & 2 & 2 & 3 \\ & & 1 & 2 \\ & & & 1 \end{array}$$

Le lemme suivant montre que l'ordre fort coïncide avec la comparaison des clefs, qui est la définition choisie par Ehresmann.

LEMME 4.1. — $\mu \leq \nu$ *ssi* $clef(\mu) \leq clef(\nu)$

Chaque colonne de la clef d'une permutation détermine une permutation grassmannienne. Ansi la clef de $\mu = 2413$ correspond-elle à la suite des grassmanniennes $2\,143$, $24\,13$, $124\,3$, 1234. La comparaison de deux clefs correspond donc à la comparaison de grassmanniennes ayant même descentes. C'est aussi la comparaison des partitions obtenues en soustrayant $1, 2 \ldots$ aux colonnes de la clef.

De manière symétrique, la comparaison des inverses des permutations peut se décrire en coupant l'alphabet $\{1, \ldots, n\}$ en deux intervalles. Soit en effet $\{x < y\}$ un alphabet à deux lettres, et p_h la projection de $\mathfrak{S}(n)$ (considéré comme un ensemble de mots en $1, \ldots, n$) sur le monoïde $\{x, y\}^*$ induite par le morphisme

$$i \to x \text{ si } i \leq h \ , \ i \to y \text{ si } i > h \ .$$

L'ordre sur les mots en $\{x, y\}$ se définit en comparant les degrés en y des facteurs gauches respectifs de même longueur des deux mots :

$$v \leq w \text{ si } \{v = v'v'', \ w = w'w'', \ |v'| = |w'|\} \Rightarrow |v'|_y = |w'|_y \ .$$

On a alors

LEMME 4.2. — *$\mu \leq \nu$ ssi pour tout h, tout k,*

$$|\, p_h(\mu_1 \cdots \mu_k)\,|_y \leq |\, p_h(\nu_1 \cdots \nu_k\,|_y \ .$$

Ainsi $2143 \leq 4132$, car, écrivant $\{1 \dots i | i+1 \dots n\}$ pour la projection $1, \dots, i \to x$, $i+1, \dots, n \to y$, on a :
pour $\{1 \,|\, 234\}$, $yxyy \leq yxyy$; pour $\{12 \,|\, 34\}$, $xxyy \leq yxyx$; pour $\{123 \,|\, 4\}$, $xxyx \leq yxxx$.

Le lemme 4.2 n'est autre que l'explicitation des projections p_{hk} (vues en 3.5) de $\mathfrak{S}(n)$ sur l'ensemble des éléments de longueur minimum des classes $\mathfrak{S}(h) \times \mathfrak{S}(n-h) \setminus \mathfrak{S}(n) / \mathfrak{S}(k) \times \mathfrak{S}(n-k)$.

On peut maintenant rétablir la symétrie (pour l'inversion des permutations) de l'Ehresmannoedre, qu'avait mise à mal la comparaison des clefs de μ et ν.

Voyons tout d'abord la comparaison d'une permutation et d'une bigrassmannienne. Comme une bigrassmannienne b de $\mathfrak{S}(n)$ est une permutation qui a pour code un rectangle $0^{r_0} r_2^{r_1} 0^{r_3}$, avec $r_0 + r_1 + r_2 + r_3 = n$, $r_1 \geq 1$, $r_2 \geq 1$, on la désignera plutôt par le symbole $b = [r_0, r_1, r_2, r_3]$. Alors

LEMME 4.3. — *Une permutation μ est supérieure à une bigrassmannienne $b = [r_0, r_1, r_2, r_3]$ ssi il y a au moins r_1 valeurs $> r_0 + r_2$ dans le facteur gauche de longueur $r_0 + r_1$ de μ.*

Preuve. — On utilise le critère 4.2. Pour la coupure de l'alphabet $\{1 \cdots r_0 + r_2 \,|\, r_0 + r_2 + 1 \cdots n\}$, le mot $x^{r_0} y^{r_1} x^{r_2} y^{r_3} = p_{r_0+r_2}(b)$ est clairement le minimum des $p_{r_0+r_2}(\mu)$, pour $\mu \geq b$. □

On peut tout autant optimiser la négation NEG de la condition $\mu \geq b$ (nous prions le lecteur de se reporter à la dernière partie de l'annexe où est traitée la notion de clivage). En effet, le mot $y^{r_1-1} x^{r_0+1} y^{r_3+1} x^{r_2-1}$ est le maximum des $p_{r_0+r_2}(\zeta)$, $\zeta \not\geq b$, et a pour maximum dans sa fibre la permutation
$c_{[r_0 r_1 r_2 r_3]} =$
$n \cdots (n - r_1 + 2)(r_0 + r_2) \cdots r_2 (r_0 + r_2 + r_3 + 1) \cdots (r_0 + r_2 + 1)(r_2 - 1) \cdots 1.$

Ainsi donc les bigrasmanniennes constituent la base de l'Ehresmannoedre, car à chaque bigrassmannienne b correspond bijectivement une cobigrassmannienne qui est le *Sup* du complémentaire de l'intervalle supérieur $[b \ \leq]$. En d'autres termes, on a le théorème suivant.

THÉORÈME 4.4. — *Le treillis enveloppant du groupe symétrique est distributif et a pour générateur les bigrassmanniennes.*

Plus précisément, soit $[r_0, r_1, r_2, r_3] \in \mathbb{N}^4$, $r_1, r_2 \geq 1$, $r_0 + r_1 + r_2 + r_3 = n$. *Alors le groupe symétrique* $\mathfrak{S}(n)$ *clive en les deux intervalles* $[b \leq]$ *et* $[\leq c]$, *où* b *et* c *sont les bigrassmannienne et cobigrassmannienne codées par* $[r_0, r_1, r_2, r_3]$.

Une permutation μ *appartient à l'un ou l'autre de ces deux intervalles selon que la composante de sa clef de coordonnées* $r_0 + r_1, r_1$ *(pour les axes* $\downarrow^{\rightarrow}$*) est strictement supérieure à* $r_0 + r_2$ *ou non.*

Pour $\mathfrak{S}(4)$, l'ensemble B des bigrassmanniennes est :

$$\{2134, 1324, 1243, 1342, 1423, 2314, 3124, 2341, 4123, 3412\}$$

La restriction de la relation d'incidence à $\mathfrak{S}(4) \times B$, dont les lignes sont les projections par β des éléments sur la base B est représentée par la matrice:

```
4321 : 1 1 1 1 1 1 1 1 1 1
4312 : 1 1 1 0 1 1 1 1 1 1
4231 : 1 0 1 1 1 1 1 1 1 1
4213 : 1 0 1 0 1 1 1 0 1 1
4132 : 1 0 1 0 0 1 1 1 1 1
4123 : 1 0 1 0 0 1 1 0 1 1
3421 : 0 1 1 1 1 1 1 1 1 1
3412 : 0 1 1 0 1 1 1 1 1 1
3241 : 0 0 1 1 1 1 0 1 1 1
3214 : 0 0 1 0 1 1 0 0 1 0
3142 : 0 0 1 0 0 1 0 1 1 1
3124 : 0 0 1 0 0 1 0 0 1 0
2431 : 0 0 0 1 1 1 1 1 1 1
2413 : 0 0 0 0 1 1 1 0 1 1
2341 : 0 0 0 1 1 1 0 1 1 1
2314 : 0 0 0 0 1 1 0 0 1 0
2143 : 0 0 0 0 0 1 0 0 0 1
2134 : 0 0 0 0 0 1 0 0 0 0
1432 : 0 0 0 0 0 0 1 1 1 1
1423 : 0 0 0 0 0 0 1 0 1 1
1342 : 0 0 0 0 0 0 0 1 1 1
1324 : 0 0 0 0 0 0 0 0 1 0
1243 : 0 0 0 0 0 0 0 0 0 1
1234 : 0 0 0 0 0 0 0 0 0 0
```

Enfin, les dix clivages correspondant aux bigrassmanniennes sont :

$$\begin{aligned}
\mathfrak{S}(4) = [2134 \leq] \cup [\leq 1432] &= [1324 \leq] \cup [\leq 2143] = [1243 \leq] \cup [\leq 3214] \\
= [1342 \leq] \cup [\leq 4213] &= [1423 \leq] \cup [\leq 3241] = [2314 \leq] \cup [\leq 4132] \\
= [3124 \leq] \cup [\leq 2431] &= [2341 \leq] \cup [\leq 4312] = [4123 \leq] \cup [\leq 3421] \\
&= [3412 \leq] \cup [\leq 4231]
\end{aligned}$$

Par ailleurs, les bigrassmanniennes étant codées bijectivement par les vecteurs $[r_0, r_1, r_2, r_3] \in \mathbb{N}^4$, $r_1, r_2 \geq 1$, la fonction génératrice du nombre de bigrassmanniennes, pour n variable, est

$$\sum_{n\geq 2} z^{n-2} card\big(Base(\mathfrak{S}(n))\big) \;=\; (1-z)^{-4}$$

L'image d'une permutation par la projection p_{ij} vue en 3.5 est soit l'identité, soit une bigrassmannienne b ayant recul i et descente j (i.e. b a le sous-mot $i{+}1 \ldots i$ et $b_j > b_{j+1}$). En outre, si b est une bigrassmannienne de recul i et descente j, alors $b \leq \mu \;\Rightarrow\; b \leq p_{ij}(\mu)$. Les rectrices d'une permutation μ sont donc les éléments maximaux de l'ensemble $\{p_{ij}(\mu)\}_{1\leq i,j\leq n-1}$. Il existe un algorithme pour déterminer ces rectrices, sans calculer l'ensemble précédent, qui repose sur le lemme suivant:

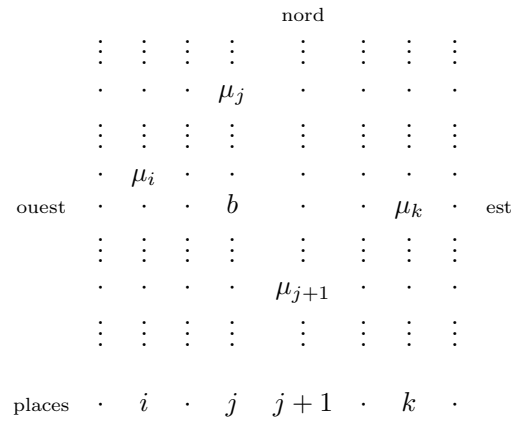
LEMME 4.5. — *Il y a bijection entre les rectrices d'une permutation μ et les triples d'entiers $i \leq j < j+1 \leq k$ tels que*

$$\mu_{j+1} \leq \mu_k < \mu_i = 1 + \mu_k \leq \mu_j \ .$$

A un tel triple correspond la rectrice $b = [r_0, r_1, r_2, r_3]$, où $r_0 = card\{h < j \ : \mu_h < \mu_k\}$, $r_1 = j - r_0$, $r_2 = \mu_k - r_0$.

Nous laissons au lecteur le soin de vérifier que la bigrassmannienne associée au couple : descente ($\mu_j > \mu_{j+1}$), recul ($\mu_k + 1 \ldots \mu_k$) est bien maximale sous les hypothèses du lemme 4.5.

Graphiquement, une rectrice b correspond à une configuration



pour les axes de coordonnées cartésiens $\uparrow_{\rightarrow}$, le couple (μ_k, j) étant dit les *coordonnées* de la rectrice.

Outre l'ordre de Bruhat, on peut lire certaines propriétés des permutations sur l'ensemble de leurs rectrices. Par exemple, la proposition suivante décrit l'appartenance à un sous-groupe de Young, sous des conditions que l'on peut qualifier de *géographiques* car elles ne font intervenir que les coordonnées $r_0 + r_1$, $r_0 + r_2$ des rectrices.

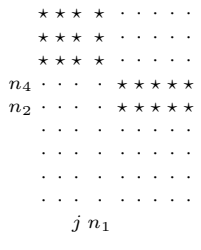
PROPOSITION 4.6. — *Soit μ une permutation, $R = R' \uplus R''$ une décomposition de l'ensemble de ses rectrices ($R', R'' \neq \emptyset$).*
Soient n_1, n_2 deux entiers tels que

$$\begin{array}{rcll} r_0 + r_1 \leq n_1 & \& & r_0 + r_2 \leq n_2 & si \ [r_0, r_1, r_2, r_3] \in R' \\ > n_1 & & > n_2 & sinon \end{array}$$

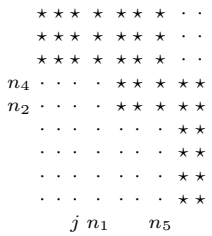
Alors il existe un entier n_3 tel que l'on ait les mêmes relations en remplaçant (n_1, n_2) par (n_3, n_3), et μ appartient au sous-groupe $\mathfrak{S}(n_3) \times \mathfrak{S}(n - n_3)$.

Preuve. — Soient n_4 et n_5 les deux entiers : $n_4 = Max\big(\{\mu_j$: il existe une rectrice de μ dans R' avec $r_0 + r_1 = j\}\big)$; $n_5 = Max\big(\{kj$: il existe une rectrice de μ dans R' avec $r_0 + r_2 = \mu_k\}\big)$.

Par maximalité de $n_4 = \mu_j$, on a $\mu_j > \mu_{j+1}$. D'après le lemme 4.5 et l'hypothèse 4.6, on a $\mu_{j+1} < n_2$. Pour les mêmes raisons, on a aussi $\mu_k > n_4$ pour tout $h > n_1$, ce qui entraine que les zones $\star$ ne contiennent pas de point (i, μ_i):



Le même argument s'applique à n_5 grâce à la symétrie $\mu \to \mu^{-1}$. Le domaine permis pour les points (i, μ_i) est donc finalement (zone "·") :



Ceci montre que $n_3 = Max(n_4, n_5)$ satisfait l'énoncé 4.6, et que $i \leq n_3 \Rightarrow \mu_i \leq n_3$ □

5. Triangles. — On peut identifier chaque permutation μ à sa clef $K(\mu)$. La comparaison d'une permutation μ et d'une bigrassmannienne $b = [r0, r_1, r_2, r_3]$ se réduit à tester une seule composante de $K(\mu)$, d'après le théorème 4.4 :

$$\mu \geq b \text{ ssi } K(\mu)_{r0+r1,r_1} > r_0 + r_2 \ . \tag{5.1}$$

Le *Sup* ou l' *Inf*, dans le treillis enveloppant, d'une famille $\{\mu\}$ de permutations se calcule aisément, étant le *Sup* ou l'*Inf* composante à composante des $\{K(\mu)\}$.

Plus précisément, un contretableau t de forme $12\cdots n$ est le sup de la famille $\{\mu\}$ ssi

$$\forall i, j : 1 \leq i \leq j \leq n, \ t_{ij} = Sup_\mu\{K(\mu)_{ij}\} \ .$$

Il est aisé de contrôler qu'un tel contre-tableau vérifie, pour chaque sous-triangle élémentaire (i.e. triple de composantes adjacentes de coordonnées respectives (i, j), $(i, j+1)$ et $(i+1, j+1)$ pour les axes $\downarrow^{\rightarrow}$) les inégalités suivantes

$$\begin{smallmatrix} & yz \\ x & \end{smallmatrix} \Rightarrow \{x < z \ \& \ x \leq y \ \& \ y \leq z\} \ . \tag{5.2}$$

Réciproquement, tout contre-tableau de forme $12\cdots n$ vérifiant les conditions 5.2 (que l'on appelera *triangle*) est le *Sup* de la famille de bigrassmanniennes déterminée par chacune de ses composantes :

$$t_{ij} \ \rightarrow \ b = [j - i, \ i, \ t_{ij} + i - j - 1, \ n - t_{ij} - i + 1] \tag{5.3}$$

On a donc

LEMME 5.4. — *Le treillis enveloppant du groupe symétrique* $\mathfrak{S}(n)$ *est isomorphe au treillis des triangles de forme* $12\cdots n$*, remplis avec des lettres dans* $\{1, 2, \ldots, n\}$.

D'après les travaux de Mills, Robbins & Rumsey [MRR] les triangles (qu'ils appellent *triangles monotones*) sont en bijection avec les *matrices alternantes*, dont le cardinal, pour l'ordre n, est

$$\prod_{0}^{n-1} (3k+1)!\,/\,(n+k)!$$

Cette formule, qu'ils conjecturaient, a depuis été prouvée.

Pour $\mathfrak{S}(3)$, le treillis enveloppant comprend un seul élément qui n'est pas une permutation : c'est le *Sup* de $213 \leftrightarrow {}^{22}_{1}$ et $132 \leftrightarrow {}^{13}_{1}$, ainsi que l'*Inf* de $231 \leftrightarrow {}^{23}_{2}$ et $312 \leftrightarrow {}^{33}_{1}$. C'est donc ${}^{23}_{1}$ qui correspond à la seule matrice alternante d'ordre trois qui ne soit pas une permutation : $\begin{smallmatrix} 0 & 1 & 0 \\ 1 & -1 & 1 \\ 0 & 1 & 0 \end{smallmatrix}$.

Le treillis enveloppant de $\mathfrak{S}(4)$ est constitué de 42 triangles, dont nous énumérons les 18 qui ne sont pas des clefs:

$$\begin{array}{cccccccccc}
2\,3\,3 & 1\,3\,4 & 2\,3\,4 & 2\,3\,4 & 3\,3\,4 & 2\,3\,4 & 3\,3\,4 & 2\,3\,4 & 3\,3\,4 \\
1\,2 & 1\,2 & 1\,2 & 2\,2 & 1\,2 & 1\,3 & 2\,2 & 2\,3 & 2\,3 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}$$

$$\begin{array}{cccccccccc}
2\,4\,4 & 3\,4\,4 & 2\,4\,4 & 3\,4\,4 & 2\,4\,4 & 3\,4\,4 & 3\,4\,4 & 3\,4\,4 & 4\,4\,4 \\
1\,2 & 1\,2 & 1\,3 & 2\,2 & 2\,3 & 1\,3 & 2\,3 & 2\,3 & 2\,3 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 1
\end{array}$$

L'application 5.3 décrit, pour un contre-tableau t, une famille de bigrassmanniennes dont t est le *Sup*. Les éléments maximaux de cet ensemble de bigrassmanniennes, c'est-à-dire les *rectrices* du triangle, correspondent bijectivement aux composantes t_{ij} telles que l'image de t par $t_{ij} \to t_{ij} - 1$ soit encore un triangle.

Ces composantes seront appelées *points essentiels* du triangle; un triangle est donc le *Sup* des bigrassmanniennes correspondant à ses points essentiels et tout ensemble de composantes dont le triangle est le *Sup* contient les points essentiels. Dans le cas où t est la clef d'une permutation μ, les points essentiels ont été définis par Fulton [Fu] (en terme de la fonction de rang de la matrice représentant la permutation).

Un triangle sera dit *vexillaire* ssi l'ensemble de ses points essentiels $\mathcal{E}$ vérifie la condition suivante (qui est géographique au sens donné plus haut à ce terme):

$$\forall (i,j) \in \mathcal{E} \;\Rightarrow\; \{(i',j') : i' \leq i,\, j' > j\} \cap \mathcal{E} = \emptyset \; . \tag{5.5}$$

En d'autres termes, il n'y a pas de point essentiel dans le cadran nord-est d'un point essentiel (le domaine d'exclusion comprend le demi axe-est).

Dans le cas d'une permutation vexillaire μ, cette définition, appliquée à la clef de μ, correspond à l'une des nombreuses caractérisations des permutations vexillaires (cf. [Fu]).

6. Pavés. — On a remarqué que le clivage associé à une transposition simple σ induit le clivage de tout intervalle $[\leq \mu]$. Cet idéal se décompose en un idéal $[\leq \nu]$ (où ν est la permutation maximum $\nu \leq \mu$ dont aucune décomposition réduite ne contient σ) et son complémentaire $[\leq \mu] \cap [\sigma \leq]$.

Nous donnons dans ce paragraphe une décomposition du groupe symétrique transversale au clivage précédent.

Pour ce faire, considérons l'algèbre des différences divisées isobares.

A tout ensemble $\mathcal{J} \subset \{1, \ldots, n-1\}$ correspond le groupe parabolique $\mathcal{P}_{\mathcal{J}}$ engendré par les transpositions simples $\{\sigma_i | i \in \{1 \ldots n-1\} \setminus \mathcal{J}\}$, ainsi que la projection $p_{\mathcal{J}}$ du monoide engendré par les $\pi_i \, , i \in \{1 \ldots n-1\}$ sur le monoide engendré par les $\pi_i \, , i \notin \mathcal{J}$ déterminée par $\pi_j \to 1$ pour tous les $j \in \mathcal{J}$.

Cette projection est clairement compatible aux relations de Coxeter, ainsi qu'aux relations $\pi_i^2 = \pi_i$ et donc l'image des π_μ est bien définie.

Définition. — Soit k un entier, $1 \leq k \leq n-1$. Un *k-pavé* est une classe d'équivalence pour la relation

$$\mu \sim_k \nu \;\Leftrightarrow\; p_k(\pi_\mu) = p_k(\pi_\nu) \; .$$

Deux permutations μ, ν appartiennent au même k-pavé ssi, pour deux décompositions réduites quelconques $\mu = \sigma_i \sigma_j \cdots \sigma_h$ et $\nu = \sigma_l \cdots \sigma_m$, on a

$$p_k(\pi_i \pi_j \cdots \mu_h) = p_k(\pi_l \cdots \pi_m) \; .$$

Par exemple, le groupe $\mathfrak{S}(4)$ se décompose en six 1-pavés :
$[1432, 4321], [1342, 3241], [1423, 4213], [1324, 3214], [1243, 2143], [1234, 2134]$,
qui sont des intervalles booléens de cardinaux respectifs 8,4,4,4,2,2 .

Des pavés plus généraux apparaissent pour $k \neq 1, n-1$.

Définition. — Soit μ une permutation et $k \leq n-1$. Les places *k-saillantes gauches* de μ sont les indices $1 \leq i \leq k$ pour lesquels $\mu_i = max(\{\mu_i, \ldots, \mu_k\})$; les places *k-saillantes droites* de μ sont les indices $k < j \leq n$ pour lesquels $\mu_j = min(\{\mu_{k+1}, \ldots, \mu_j\})$.

PROPOSITION 6.1. — *Soit k un entier $\leq n-1$, ν une permutation dans $\mathcal{P}_k = \mathfrak{S}(k) \times \mathfrak{S}(n-k)$. Soit ζ la permutation obtenue à partir de ν en permutant circulairement les points saillants de ν de sorte à en faire une suite décroissante.*

Alors le k-pavé contenant ν est égal à l'intervalle $[\nu, \zeta]$ et est isomorphe à l'idéal de la bigrassmannienne $[0, r, p, 0]$ de $\mathfrak{S}(p+r)$, où p est le nombre de points saillants gauches de ν, r le nombre de points saillants droits.

Une permutation μ appartient au pavé de ν ssi $\zeta_i = \nu_i \Rightarrow \mu_i = \nu_i$ et l'image de μ par la projection de $\mathfrak{S}(n)$ sur $\mathfrak{S}(p+r)$ qui consiste en l'effacement des valeurs communes à ν et ζ, est supérieure (pour l'ordre de Bruhat) à l'image de ν.

Ainsi, pour $k = 5$ et

ν	$=$	**5**	3	**4**	1	**2**	**11**	**9**	12	**7**	8	**6**	10
places		1	2	3	4	5	6	7	8	9	10	11	12

(les point saillants sont en gras) , le maximum du pavé est

$$\zeta = \mathbf{11}\ 3\ \mathbf{9}\ 1\ \mathbf{7}\ \mathbf{6}\ \mathbf{5}\ 12\ \mathbf{4}\ 8\ \mathbf{2}\ 10\ .$$

Une permutation μ appartient au pavé ssi $\mu_2 = 3$, $\mu_4 = 1$, $\mu_8 = 12$, $\mu_{12} = 10$ et $(\mu_1, \mu_3, \mu_5, \mu_6, \mu_7, \mu_9, \mu_{11}) \geq (5, 4, 2, 11, 9, 7, 6)$.

Preuve. — La permutation ν est le produit direct des deux permutations $\nu' = \nu_1 \ldots \nu_k\, k+1 \ldots n$ et $\nu'' = 1 \ldots k\, \nu_{k+1} \ldots \nu_n$. Une permutation μ est dans la fibre de ν ssi $p_{k \ldots n-1}(\mu) = \nu'$ et $p_{1 \ldots k}(\mu) = \nu''$. Or le code de $p_{k \ldots n-1}(\mu)$ est l'inf du code de μ et du vecteur $[k-1, \ldots, 1, 0, \ldots, 0]$, ainsi qu'on le voit en considérant le décomposition réduite de μ associée au code (i.e. le code considéré est le vecteur $[inf(c_1, k-1), \ldots, inf(c_k, 0), \ldots, 0]$, où $[c_1, \ldots, c_n]$ est le code de μ).

Il s'ensuit que la condition nécessaire et suffisante que μ soit dans la fibre de ν est que

- l'inf du code de μ et $[k-1 \ldots 0 \ldots 0]$ est égal au code de ν'
- l'inf du code de $\omega\mu\omega$ et $[n-k-1 \ldots 0 \ldots 0]$ est égal au code de $\omega\nu''\omega$.

Il n'est pas difficile de vérifier que ζ satisfait à ces deux conditions.

Comme les morphismes de spécialisation $p_{\mathcal{J}}$ sont des morphismes d'ordre (i.e. $\mu \leq \eta \Rightarrow p_{\mathcal{J}}(\mu) \leq p_{\mathcal{J}}(\eta)$), on en déduit que l'intervalle $[\nu, \zeta]$ est contenu tout entier dans une seule fibre.

Nous épargnerons au lecteur la vérification que toute permutation appartient à un et un seul de ces intervalles.

Par ailleurs, l'intervalle $[\nu, \zeta]$ a pour image dans $\mathfrak{S}(p+r)$, après effacement des points fixes et retour à l'alphabet $\{1, 2, \ldots, p+r\}$ l'intervalle $[(p \ldots 1)\,,\,(p+r \ldots p+1)]$. L'image de cet intervalle, par multiplication à gauche par ω, est l'intervalle $[(1 \ldots p)\,,\,(p+1 \ldots p+r)]$ qui n'est autre que l'intervalle inférieur de la bigrassmannienne $[0, r, p, 0]$ □

L'énumération des pavés isomorphes à l'idéal de la bigrassmannienne $[0, r, p, 0]$ (disons de *type* $[0, r, p, 0]$) est donné par le lemme suivant, en désignant par $\Lambda^i(k)$ le nombre de Stirling égal à la $i-$ème fonction élémentaire des entiers $0, 1, \ldots, k-1$.

LEMME 6.2. — *Le nombre de $k-$pavés de type $[0, r, p, 0]$ est égal au produit des nombres de Stirling $\Lambda^{k-p}(k)\,\Lambda^{n-k-r}(n-k)$*

Preuve. — Soit $n(k, r, p)$ le nombre de pavés de type $[0, r, p, 0]$. La projection "effacement de la lettre 1" :

$$\mathfrak{S}(n) \ni \mu \to \mu\backslash 1 \in \mathfrak{S}(n-1)$$

donne une récurrence sur le nombre de pavés.

En effet, soit ν le minimum d'un $k-$pavé. Si $\nu_k = 1$, alors le pavé est de type $[0, r, p, 0]$ ssi le pavé contenant $\nu\backslash 1$ est de type $[0, r, p-1, 0]$.

Si $\nu_k \neq 1$, l'effacement de 1 donne un pavé isomorphe. Comme il y a $k-1$ permutations μ qui se projettent sur $\nu\backslash 1$, et telles que $\nu_k \neq 1$, on a la récurrence $n(k, r, p) = (k-1)n(k-1, r, p) + n(k-1, r, p-1)$ □

Exemple. — Les fibres de la projection $p_3 : \mathfrak{S}(7) \to \mathfrak{S}(3) \times \mathfrak{S}(4)$ sont les bigrassmanniennes suivantes. On regroupe les pavés de type $[0, r, p, 0]$ et $[0, p, r, 0]$ qui sont isomorphes, et on écrit Λ^{ij} pour $\Lambda^i(3)\Lambda^j(4)$:

$[p, r]$	[11]	[12]	[13]	[14]	[22]	[23]	[24]	[33]	[34]
card	12	40	18	2	33	29	3	6	1
$=$	Λ^{23}	$\Lambda^{22}+\Lambda^{13}$	$\Lambda^{21}+\Lambda^{03}$	Λ^{20}	Λ^{12}	$\Lambda^{02}+\Lambda^{11}$	Λ^{10}	Λ^{01}	Λ^{00}

Molev [Mo] a utilisé une décomposition du groupe symétrique en intervalles booléens pour développer le déterminant de Sklyanin et décrire le centre de l'algèbre enveloppante dans le cas des groupes orthogonaux et symplectiques. Quoique le nombre des pavés soit encore un nombre de Stirling, cette décomposition est différente de celle que nous venons d'exposer.

Ayant décomposé le groupe symétrique en pavés, il nous reste à décrire ceux-ci en tant qu'intervalles pour l'ordre de Bruhat. Nous nous contenterons de donner la fonction génératrice du nombre d'éléments dans l'intervalle, classés par nombre d'inversions, autrement dit le *Polynôme de Poincaré* de l'intervalle.

Soit une bigrassmannienne $b = [0, r, p, 0]$. Notons $G(r, p)$ le polynôme de Poincaré $:= \sum_{\mu \leq b} z^{\ell(\mu)}$ de b.

Nous voulons décrire l'intervalle inférieur de b. Celle dernière a une décomposition réduite canonique que l'on peut écrire planairement dans un rectangle (lisant par colonnes, de gauche à droite):

$$\begin{array}{cccc} \sigma_p & \sigma_{p+1} & \cdots & \sigma_{p+r-1} \\ \vdots & \vdots & & \vdots \\ \sigma_1 & \sigma_2 & \cdots & \sigma_r \end{array}$$

Comme l'intervalle se calcule à l'aide de (3.2), c'est-à-dire de la décomposition des produits de π_i dans la base des $\bar{\pi}_\mu$, le polynôme de Poincaré $G(r, p)$ est obtenu par récurrence à partir du lemme suivant.

LEMME 6.3. — *Soient p et r deux entiers. Alors on a l'identité*

$$\begin{array}{cccc|c} \pi_p & \pi_{p+1} & \cdots & \pi_{p+r-1} & \cdot \\ \pi_{p-1} & \pi_p & \cdots & \pi_{p+r-2} & \bar{\pi}_{p+r-1} \\ \vdots & \vdots & & \vdots & \vdots \\ \pi_1 & \pi_2 & \cdots & \pi_r & \bar{\pi}_{r+1} \end{array} = \begin{array}{cccc} \bar{\pi}_{p-1} & \bar{\pi}_p & \cdots & \bar{\pi}_{p+r-1} \\ \vdots & \vdots & & \vdots \\ \bar{\pi}_1 & \bar{\pi}_2 & \cdots & \bar{\pi}_{r+1} \\ \cdot & \pi_1 & \cdots & \pi_r \end{array}$$

Preuve. — Ecrivons i pour π_i, i' pour $\bar{\pi}_i$. On a, pour deux entiers consécutifs quelconques,

$$434' = 43'4' = 3'4'3 \ ,$$

et donc, pour deux lignes,

$$\begin{array}{cccc} 2 & 3 & 4 & \cdot \\ 1 & 2 & 3 & 4' \end{array} = \begin{array}{cccc} & & 2 & \\ 1 & 2 & 3' & 4' \\ & & 3 & \end{array} = \begin{array}{cccc} & & 2 & \\ 1 & 2' & 3' & 4' \\ & & 3 & \end{array} = \begin{array}{cccc} & & & \\ 1' & 2' & 3' & 4' \\ & 1 & 2 & 3 \end{array}$$

Finalement, pour un nombre quelconque de lignes,

$$\begin{array}{cccc} 3 & 4 & 5 & \cdot \\ 2 & 3 & 4 & 5' \\ 1 & 2 & 3 & 4' \end{array} = \begin{array}{cccc} 2' & 3' & 4' & 5' \\ \cdot & 2 & 3 & 4 \\ \cdot & 1 & 2 & 3 \end{array} = \begin{array}{cccc} 2' & 3' & 4' & 5' \\ 1' & 2' & 3' & 4' \\ \cdot & 1 & 2 & 3 \end{array} \ ,$$

ce qui est bien le lemme □

On intialise la récurrence sur les polynômes de Poincaré en écrivant que la dernière colonne de l'expression planaire de π_b, disons $\pi_6\pi_5\pi_4\pi_3$ est égale à

$$\pi_6\pi_5\pi_4\pi_3 = (1+\overline{\pi_6})(1+\overline{\pi_5})(1+\overline{\pi_4})(1+\overline{\pi_3})$$

Par application répétée de 6.3, en regroupant les termes et en employant les notations des λ-anneaux (les fonctions $S^i(r+x)$ sont les coefficients de la série en z $1/(1-zx)(1-z)^r$, i.e.
$1/(1-zx)(1-z)^r = S^0(r+x) + zS^1(r+x) + z^2S^2(r+x) + \ldots)$,
on obtient

PROPOSITION 6.4. — *Soient r, p des entiers ≥ 1 et $Z = z^{r+1}$. Alors*
$G(r+1,p) = (S^{p-1}(1+z) + z^p)G(r,p) + ZS^{p-2}(2+z)G(r,p-1) + Z^2S^{p-3}((3+z)G(r,p-2) + \cdots + Z^{p-2}S^1(p-1+z)G(r,2) + Z^{p-1}S^0(r,1)$

Le cas initial $G(r,1)$, c'est à dire de l'idéal d'un cycle $b = (2,\ldots,r+1,1)$ est donné par la spécialisation $\pi_i = 1 + z\,\forall i$. En effet, $\pi_b = (1+\overline{\pi_1})\cdots(1+\overline{\pi_r}) = \sum_{\mu\leq b}\overline{\pi_\mu}$ est une expression dont le développement ne fait apparaître aucun carré $\overline{\pi_i}^2$. Les éléments de l'intervalle $[\leq b]$ sont en correspondance bijective avec les sous-mots de la décomposition réduite $b = \sigma_1\sigma_2\cdots\sigma_r$. Cet intervalle est booléen et l'on a $G(r,1) = (1+z)^r$, ce qui résulte aussi du fait bien connu que l'idéal d'un cycle b est un intervalle booléen.

Comme exemple de la proposition, on a
$G(7,4) = (1+z+z^2+z^3+z^4)G(6,4) + z^7(3+2z+z^2)G(6,3) + z^{14}(3+z)G(6,2) + z^{21}G(6,1) = 1+10z+54z^2+209z^3+\ldots+252z^{26}+28z^{27}+z^{28}$
est le polynôme de Poincaré d'un pavé de cardinal 1315666 de $\mathfrak{S}(11)$ que nous nous dispenserons d'énumérer.

Table des coefficients des $G(r,p)$, pour $4 \geq r \geq p \geq 2$

														card
2)	1	3	5	4	1									14
2)	1	4	9	13	12	6	1							46
3)	1	5	14	29	45	53	46	27	9	1				230
2)	1	5	14	26	35	34	22	8	1					146
3)	1	6	20	49	95	150	195	206	173	110	48	12	1	1066
4)	1	7	27	76	174	337	562	815	1029	1125	1052	823	521	
										252	84	16	1	6902

7. Groupe B_n. — Le goupe B_n est engendré par n générateurs $s_1,\ldots,s_n$ qui satisfont aux mêmes relations que les générateurs du groupe symétrique, mis à part le remplacement de $(s_1s_2)^3 = 1$ par

$$(s_1s_2)^4 = 1$$

Chaque élément peut être décrit par sa décomposition réduite lexicographiquement minimale (*drlm*). Ecrivant i pour s_i, celle-ci est un sous-mot de la décomposition de l'élément maximal :

$$(1)\,(212)\,(32123)\,\cdots(n\ldots212\ldots n)$$

qui est formé de facteurs gauches de chacun des blocs indiqués entre parenthèses.

On peut donc coder bijectivement un élément de B_n par la suite des longueurs des facteurs successifs de sa *drlm* ; les éléments de B_n sont en bijection avec les vecteurs c dans $\mathbb{N}^n$, $c \leq [1,3,5,\ldots,2n+1]$ que nous appelerons *codes*.

Les éléments de B_n peuvent aussi être représentés par les permutations signées de $\{1,\ldots,n\}$, en interprétant s_1 comme le morphisme de $\mathbb{Z}^n$:

$$u=[u_1,\ldots,u_n] \rightarrow us_1=[-u_1,u_2,\ldots,u_n]$$

et s_i, $i=2,\ldots,n$, comme la transposition simple échangeant les composantes u_{i-1} et u_i.

Une deuxième représentation est le plongement dans $\mathfrak{S}(2n)$ défini par

$$s_1 \rightarrow \sigma_n,\ s_2 \rightarrow \sigma_{n-1}\sigma_{n+1},\ \ldots,\ s_n \rightarrow \sigma_1\sigma_{2n-1}\ ,$$

où les σ_i sont les transpositions simples de $\mathfrak{S}(2n)$. L'image de B_n est alors l'ensemble des permutations μ *palindromes*, i.e. telles que $\mu_i+\mu_{2n-i}=2n+1$, $i=1,\ldots,n$.

Le passage du code à chacune de ces deux représentations est immédiat et correspond à compter les inversions. Ainsi le code $[1,0,5,2]$ correspond à la décomposition réduite $(1)()(32123)(43)$, à la permutation signée $[-1,4,2,-3]$ et au palindrome 73154862. En effet, $c_4=2$ indique la place de 4 (à partir de la droite) dans la permutation signée et la place de 8 dans le palindrome; $c_3=5$ donne la place de -3 dans $[-1,2,-3]$, le signe - impliquant que l'on compte la place à partir de la gauche en ajoutant l'ordre (=3), ainsi que la place de 7 dans le palindrome 735462.

On passe de la permutation signéee au palindrome par duplication et retour à l'alphabet $\{1,2,\ldots,2n\}$ par translation de n:

$$[-1,4,2,-3]\rightarrow[3,-2,-4,1]\ ,\quad [-1,4,2,-3]\sim 73154862$$

Le générateur s_1 joue un rôle particulier, ce qui conduit à distinguer deux types de facteurs v d'une *drlm* :

- *colonne* si $s_1 \notin v$ (i.e. $v = s_k \cdots s_{k-i}$, $i < k-1$)
- *équerre* sinon.

Le produit d'une colonne ou d'une équerre par un générateur s_i est instantané et permet ainsi de d'expliciter l'action, à gauche ou à droite, de B_n sur les codes.

Soit un élément de B_n dont le code n'a que deux composantes non nulles. Cet élément n'est une bigrassmannienne que dans les seuls cas suivants:

(cc) $c_1 = 0 = c_{k-1}; c_k = c_{k+1} < k; c_{k+2} = 0 = \cdots = c_n$

(ee) $c_1 = 0 = c_{k-1}; = c_{k+1} = c_k + 1 \geq k + 1 < k; c_{k+2} = 0 = \cdots = c_n$

(ec) $c_1 = 0 = c_{k-1}; c_k \geq k, c_{k+1} = 2k + 1 - c_k; c_{k+2} = 0 = \cdots = c_n$

Les facteurs correspondants de la *drlm* sont respectivement (colonne, colonne); (équerre, équerre); (équerre, colonne).

Par exemple, pour $k = 5$, avec i au lieu de s_i, les *drlm* suivantes illustrent ces trois types :

(cc) (543) (654)

(ee) (5432123) (65432123)

(ec) (5432123) (654)

Par récurrence sur le nombre de facteurs, on en déduit la caractérisation des codes des bigrassmanniennes de B_n :

LEMME 7.1. — *Un vecteur c dans $\mathbb{N}^n$ est le code d'une bigrassmannienne de B_n ssi*

i) $c \leq [1, 3, \ldots, 2n + 1]$; ses composantes non nulles sont consécutives et constituent une suite d'équerres suivie par une suite de colonnes (l'une de ces deux suites peut être vide)

ii) chaque paire de composantes adjacentes non nulles vérifie la condition cc), ee) ou ec) indiquée par son type.

Par exemple, l'ensemble des codes des bigrassmanniennes de B_3 est

$\{[0,3,4]; [1,2,3]; [0,0,5], [0,2,3], [1,2,2]; [0,0,4], [0,3,1], [0,2,2];$
$[0,0,3], [0,3,0], [1,2,0], [1,1,1]; [0,0,2], [0,1,1], [0,2,0], [1,1,0];$
$[0,0,1], [0,1,0], [1,0,0]\}$

Du lemme précédent, on déduit la fonction génératrice du nombre des bigrassmanniennes :

LEMME 7.2. — *La fonction $\sum_{n=1}^{\infty} z^{n-1} card(\{bigr(B_n)\})$ est égale à*

$$(1-z)^{-5} + z(1-z)^{-4} = 1 + 6z + 19z^2 + 45z^3 + 90z^4 + \ldots$$

Nous allons voir que l'ensemble des bigrassmanniennes contient strictement la base de B_n, pour $n \geq 4$.

Comme l'ordre de Bruhat sur B_n coïncide avec la restriction de l'ordre de Bruhat sur $\mathfrak{S}(2n)$ au sous-ensemble des permutations palindromes [Lak], [Pr], on peut décrire l'ordre de B_n en utilisant les bigrassamnniennes de $\mathfrak{S}(2n)$.

Tout d'abord, on remarque que pour les permutations palindromes

$$\mu \geq bigr[r_0, r_1, r_2, r_3] \Leftrightarrow \mu \geq bigr[r_3, r_2, r_1, r_0] \ .$$

Appelons *couple miroir* un tel couple de bigrassmanniennes, invariant par le retournement $[r_0, r_1, r_2, r_3] \rightarrow [r_3, r_2, r_1, r_0]$.

En particulier, l'ensemble des rectrices d'une permutation palindrome est formé de couples miroirs dont il suffit de se donner un seul des deux éléments.

Définition. — Les rectrices d'un élément de B_n sont les rectrices $[r_0, r_1, r_2, r_3]$ de son image palindrome qui sont telles que
$\{r_0 < r_3\}$ ou $\{r_0 = r_3 \,\&\, r_1 \leq r_2\}$.

Les éléments de B_n sont déterminés par leurs rectrices, puisque les éléments de $\mathfrak{S}(2n)$ le sont. L'ordre de Bruhat sur les éléments de B_n est induit par l'ordre sur les bigrassmanniennes de $\mathfrak{S}(2n)$. Plus explicitement, tenant compte de ce que l'on n'a pris que la moitié des rectrices des palindromes par raison de symétrie, on a

$$[r_0, r_1, r_2, r_3] \leq_{B_n} [p_0, p_1, p_2, p_3]$$

ssi

$$[r_0, r_1, r_2, r_3] \leq_{\mathfrak{S}(2n)} [p_0, p_1, p_2, p_3] \text{ ou } [r_0, r_1, r_2, r_3] \leq_{\mathfrak{S}(2n)} [p_3, p_2, p_1, p_0]$$

LEMME 7.3. — *Soit $b = [r_0, r_1, r_2, r_3]$ une bigrassmannienne de $\mathfrak{S}(2n)$. Alors l'ensemble des permutations palindromes $\geq b$ admet un élément inférieur, noté b_+. Symétriquement, l'ensemble des permutations palindromes inférieures à une cobigrassmannienne c de $\mathfrak{S}(2n)$ a un supremum, noté c_-.*

De plus l'élément correspondant à b_+ (resp c_-) dans B_n est une bigrassmannienne (resp. cobigrassmannienne).

Preuve. — On peut supposer que $b = [r_0, r_1, r_2, r_3]$ avec $r_0 < r_3$ ou $r_0 = r_3$ & $r_1 \leq r_2$. On a quatre cas possibles, suivant que $r_0 + r_1 \leq n$ ou non, et $r_0 + r_2 \leq n$ ou non.

Prenons par exemple $r_0 + r_1 > n$ et $r_0 + r_2 \leq n$. On cherche les palindromes tels que le facteur gauche de longueur $r_0 + r_1$ contienne au moins r_1 valeurs $> r_0 + r_2$. L'ensemble des valeurs $\{1, \ldots, 2n\}$ est coupé en trois intervalles $X = \{1, \ldots, r_0 + r_2\}$, $Y' = \{r_0 + r_2 + 1, \ldots, r_1 + r_3\}$, $Y'' = \{r_1 + r_3 + 1, \ldots, 2n\}$.

De même, les permutations, considérées comme mots, sont coupées en trois segments de longueurs respectives r_2+r_3, $r_0+r_1-r_2-r_3$, r_2+r_3. Pour la projection $p : X \to x$, $Y' \to y'$, Y'' sur l'alphabet $\{x < y' < y''\}$, on a que $\mu \geq b$ implique que le facteur gauche de longueur $r_0 + r_1$ contient au moins r_1 valeurs dans $Y' \cup Y''$. Tenant compte de ce que μ est palindrome, cela implique que

$$\mu \geq [r_0, r_1, r_2, r_3] \Leftrightarrow p(\mu) \geq v := x^{r_0} y'^{\alpha} y''^{r_2} y'^{2\beta} x^{r_2} y'^{\alpha} y''^{r_0} ,$$

avec $\alpha = r_3 - r_0$, $\beta = r_0 + r_1 - n$.

Ce mot est l'inf des palindromes d'évaluation $x^{r_0+r_2} y'^{r_1+r_3-r_0-r_2} y''^{r_0+r_2}$ qui soient plus grands que $p(b)$. Le palindrome minimum qui se projette sur v est, en marquant les mêmes coupures que v,
$b_+ := 1 \dots r_0 \,|\, r_0 + r_2 + 1 \dots, r_2 + r_3 \,|\, r_1 + r_3 + 1 \dots r_1 + r_2 + r_3 \,|$
$r_2 + r_3 + 1 \dots r_0 + r_1 \,|\, r_0 \dots r_0 + r_2 \,|\, r_0 + r_1 + 1 \dots r_1 + r_3 \,|\, 2n - r_0 + 1 \dots 2n.$

Comme dans le cas du groupe symétrique, on termine l'analyse en vérifiant que $p(b_+)$ reste bien minimum lorsque l'on fait varier la projection d'alphabet $p : \{1 \dots 2n\} \to \{x, y\}$.

Les trois autres cas se traitent explicitement de la même manière.

Etant donnée une bigrassmannienne $b = [r_0, r_1, r_2, r_3]$ de $\mathfrak{S}(2n)$, la cobigrassmannienne qui clive avec elle est $c = \omega b'$, avec $b' = [r_1 - 1, r_0 + 1, r_3 + 1, r_2 - 1]$. De l'existence de b'_+, on déduit donc par multiplication par ω l'existence d'une permutation palindrome maximale dans l'idéal $[\leq c]$ complémentaire de $[b \leq]$, qui n'est autre que $\omega b'_+$.

Enfin, on voit, sur son expression explicite, que b_+ a deux descentes, lesquelles sont à des places symétriques, de même que son inverse. En d'autres termes, l'élément correspondant de B_n est une bigrassmannienne □

THÉORÈME 7.4. — *L'image de la base de B_n dans $\mathfrak{S}(2n)$ est l'ensemble des palindromes $\{b_+\}$ qui sont les Sup respectifs des couples miroirs de bigrassmanniennes de $\mathfrak{S}(2n)$, et en correspondance bijective avec ces derniers.*

Le treillis enveloppant de B_n est distributif, i.e. chaque élément de la base clive B_n en une union disjointe de deux intervalles.

La base est un sous-ensemble strict de l'ensemble des bigrassmanniennes de B_n.

Remarque. — Le cardinal de la base de B_n est $n(2n^2 + 1)/3$, et donc la fonction génératrice des cardinaux est

$$(1 + z)^2/(1 - z)^4 = 1 + z + 19z^2 + 44z^3 + 85z^4 + \cdots .$$

Le rapport $card(base(B_n))/card(Bigr(B_n))$ tend vers 0 comme $1/n$ lorsque n tend vers l'infini.

La seule bigrassmannienne de B_4 qui n'appartient pas à la base a pour code [0042] et *drlm* $s_3s_2s_1s_2s_4s_3$; elle est le sup des deux éléments de la base [0050] $= s_3s_2s_1s_2s_3$ et [0022] $= s_3s_2s_4s_3$. Les cinq bigrassmanniennes de B_5 exclues de la base ont pour codes respectifs

$$[00053],\ [00420],\ [00062],\ [00422],\ [00453]$$

8. Annexe. — Commençons par rappeler brièvement la preuve classique du théorème de Mac Neille fournie par la méthode de O.Ore.

Soit donnée une relation $\mathcal{R} \subset \bar{X} \times X$ entre deux ensembles $\bar{X}$ et X. Pour chaque $x \in X$, nous posons $x\bar{\rho} = \{\bar{x} \in \bar{X} : (\bar{x}, x) \in \mathcal{R}\}$ et $Y\bar{\rho} = \cap\{y\bar{\rho} : y \in Y\}$ pour chaque partie $Y \neq \emptyset, X$ de X. On convient de plus que $\emptyset\bar{\rho} = \bar{X}$ et $X\bar{\rho} = \emptyset$.

On définit de même ρ en échangeant le rôle de X et de $\bar{X}$, et tous les énoncés qui suivent restent valides par cet échange, un phénomène que nous nous dispenserons souvent de mentionner.

Il est clair que $\bar{\rho} : 2^X \to 2^{\bar{X}}$ est décroissante

$$(Y' \subset Y \in 2^X \ \Rightarrow\ Y\bar{\rho} \subset Y'\bar{\rho})$$

et que $\bar{\rho}\rho : 2^X \to 2^X$ est croissante ($Y \in 2^X \ \Rightarrow\ Y \subset Y\bar{\rho}\rho$).

On a donc $\bar{\rho}\rho\bar{\rho} = \bar{\rho}$ (et $\rho\bar{\rho}\rho = \rho$) puisque

$$Y\bar{\rho} \subset (Y\bar{\rho})\rho\bar{\rho} = Y\bar{\rho}\rho\bar{\rho} = (Y\bar{\rho}\rho)\bar{\rho} \subset Y\bar{\rho}$$

identiquement.

Soit maintenant $\bar{T} = \{Y\bar{\rho} : Y \in 2^X\} \in 2^{2^{\overline{X}}}$. D'après la définition de $\bar{\rho} : 2^X \to 2^{\overline{X}}$, la famille $(\bar{T}, \subset)$ de parties de $\bar{X}$ munie de l'ordre d'inclusion, est un treillis dans lequel l'opération *Inf* est l'intersection ensembliste $\cap$. Plus précisément, $(\bar{T}, \subset)$ est le plus petit treillis contenant tous les $x\bar{\rho}$ $(x \in X)$.

Symétriquement, $T = \{\bar{Y}\rho : \bar{Y} \in 2^{\bar{X}}\} \in 2^{2^X}$ est le treillis engendré par les $\bar{x}\rho$ $(\bar{x} \in \bar{X})$. Si $Y \in T$, on a, par définition, $Y\bar{\rho} \in \bar{T}$ et $Y = \bar{Y}'\rho$ pour une certaine partie $\bar{Y}'$ de $\bar{X}$. On a donc

$$Y\bar{\rho}\rho = \bar{Y}'\rho\bar{\rho}\rho = \bar{Y}'\rho = Y\ ,$$

ce qui montre que les restrictions $\bar{\rho} : T \to \bar{T}$ et $\rho : \bar{T} \to T$ sont deux antiisomorphismes (de la relation d'ordre $\subset$) inverses l'un de l'autre.

Autrement dit, si $\{Y_i : i \in \mathcal{J}\}$ est une famille d'éléments de T, on a $Inf\{Y_i : i \in \mathcal{J}\} = \cap\{Y_i : i \in \mathcal{J}\} \in T$, cependant que $Sup\{Y_i : i \in \mathcal{J}\} = \bar{Z}\rho$, avec $\bar{Z} = \cap\{Y_i\bar{\rho} : i \in \mathcal{J}\} \in \bar{T}$.

Nous appelerons T et $\bar{T}$ le X-treillis et le $\bar{X}$-treillis engendrés par $\mathcal{R}$ et nous utiliserons l'abréviation

$$Diag(\mathcal{R}) = \{(\bar{Y}, Y) \in 2^{\bar{X}} \times 2^X \ : \ \bar{Y}\rho = Y; Y\bar{\rho} = \bar{Y}\} \subset \bar{T} \times T \ .$$

En considérant, comme ci-dessus, $\mathcal{R}$ comme une matrice booléenne, une paire de parties $(\bar{Y}, Y)$ sera appelé un rectangle (de **1**) ssi $\bar{Y} \times Y$ est contenu dans $\mathcal{R}$. Par construction, les paires $(\bar{Y} \times Y) \in Diag(\mathcal{R})$ sont les rectangles maximaux de $\mathcal{R}$, en ce sens que, étant donné $Y \subset X$, $\bar{Y}$ est la plus grande partie de $\bar{X}$ telle que $\bar{Y} \times Y$ soit un rectangle, et que l'on ait la condition symétrique sur Y par rapport à $\bar{Y}$. Par définition, les éléments de $\bar{T}$ et T sont les projections de $Diag(\mathcal{R})$ sur $2^{\overline{X}}$ et 2^X.

Considérons deux parties $\bar{X}_1$ de $\bar{X}$ et X_2 de X.
Elles définissent par restriction trois autres relations

$$\mathcal{R}_1 = \mathcal{R} \cap (\bar{X}_1 \times X) \ ; \ \mathcal{R}_2 = \mathcal{R} \cap (\bar{X} \times X_2) \ ; \ \mathcal{R}_3 = \mathcal{R} \cap (\bar{X}_1 \times X_2)$$

engendrant les paires de treillis $(\bar{T}_1, T_1)$, $(\bar{T}_2, T_2)$, $(\bar{T}_3, T_3)$.

Par définition T_1 (resp. $\bar{T}_2$) est une famille de parties de X (resp. $\bar{X}$) contenue dans T (resp. dans $\bar{T}$) et l'injection naturelle $T_1 \to T$ (resp. $\bar{T}_2 \to \bar{T}$) est un morphisme pour l'opération *Inf* puisque cette dernière n'est autre que l'opération ensembliste $\cap$.

On a de même des morphismes canoniques $\bar{T}_3 \to \bar{T}_1$ et $T_3 \to T_2$.

LEMME 8.1. — *Si $\bar{X}_1$ et X_2 sont tels que $T_1 = T$ et $\bar{T}_2 = \bar{T}$, on a*

$$T_3 = T \quad \text{et} \quad \bar{T}_3 = \bar{T} \ .$$

Preuve. — En posant $X_1 = X$, $\bar{X}_2 = \bar{X}$, $\bar{X}_3 = \bar{X}_1$ et $X_3 = X_2$, les hypothèses et la conclusion peuvent s'écrire

$$Diag(\mathcal{R}) = Diag(\mathcal{R}) \cap \{2^{\overline{X_i}} \times 2^{X_i}\} \ (= Diag(\mathcal{R}_i)) \ ,$$

respectivement pour $i = 1, 2$ et pour $i = 3$.

Supposons que $(\bar{Y}, Y)$ soit un rectangle maximal dans $\bar{X}_2 \times X_1$. On a d'une part $\bar{Y} \times Y \subset \mathcal{R}_3$, donc $\subset \mathcal{R}$, et d'autre part que pour chaque $z \in X_1 \setminus Y$, il y au moins un $\bar{y} \in \bar{Y}$ pour lequel $(y, z) \notin \mathcal{R}_3$, donc $\notin \mathcal{R}$, et symétriquement pour chaque $z \in \bar{X}_2 \setminus \bar{Y}$. Ceci implique que $(\bar{Y}, Y)$ est la

restriction à $X_2 \times Y$ du rectangle maximal $(Y\bar{\rho}, \bar{Y}\rho) \in Diag(\mathcal{R})$ et établit que

$$Diag(\mathcal{R}_3) \subset Diag(\mathcal{R}) \cap (2^{\overline{X_1}} \times 2^{X_2}) \ .$$

Réciproquement, soit maintenant $\bar{Y} \times Y \in Diag(\mathcal{R})$. Sa restriction à $\bar{X}_1 \times X_2$ est encore un rectangle dont il suffit de prouver qu'il est maximal pour chaque $z \in X \setminus Y$. Or la maximalité de $\bar{Y} \times Y$ implique l'existence d'au moins un $\bar{y} \in \bar{Y}$ tel que $(\bar{y}, z) \notin \mathcal{R}$ et l'hypothèse $Diag(\mathcal{R}_1) = Diag(\mathcal{R})$ implique que l'on puisse prendre un tel $\bar{y}$ dans $\bar{Y} \cap \bar{X}_1$.

Un argument symétrique s'applique aux $\bar{z} \in \bar{X} \setminus \bar{Y}$, ce qui achève la preuve □

Nous en venons maintenant à la preuve des résultats énoncés au paragraphe 2.

LEMME 2.3. — *Soit $(X, \leq)$ un ensemble ordonné. Un élément $x \neq \wedge X$ appartient à la base B ssi il est un élément minimal de $X \setminus [\leq z]$ pour au moins un $z \in X$.*

Quand $(X, \leq)$ est un treillis, cette condition est remplie ssi x couvre exactement un autre élément de X.

Preuve. — Soit x un élément de $X \setminus \wedge X$. Par définition, il appartient au complément de $X \setminus B$ de la base ssi il existe une partie $Y \neq \emptyset$ de X telle que

$$(\star) \qquad x \notin Y \quad \& \quad [x \leq] = \cap\{[y \leq] : y \in Y\} \ .$$

On observe d'abord que cette relation est vraie pour un $Y \neq \emptyset$ ssi elle est vraie pour le cas particulier de $Y = [< x]$ $(:= [x \leq] \backslash x)$. En effet, si Y satisfait $(\star)$ on a $y \in [< x]$ pour chaque $y \in Y$, et d'autre part $Y \cup \{y\}$ satisfait encore $(\star)$ pour chaque $y \in [< x]$. On a donc $x \in X \setminus B$ ssi

$$[x \leq] = Z \ , \text{ où} \quad Z :== \cap\{[y \leq] : y \in [< x]\} \ .$$

Par construction $Z \setminus [\leq x]$ est l'ensemble des $z \in X$ tel que x soit un élément minimal de $X \setminus [\leq z]$. On a donc $x \in X \setminus B$ ou $x \in B$ selon que $Z \setminus [\leq x]$ est vide ou non. Il est clair que $x \in B$ quand x $(\neq \wedge X)$ est un élément minimal de X, car il suffit de prendre n'importe quel $z \in X \setminus [\leq x]$. Il en est de même quand x couvre un seul élément, qui est alors $Sup([< x])$. Le cas particulier où $(X, \leq)$ est un treillis est trivial puisque l'on a alors $\wedge X \neq \emptyset$ et pour tout $x \in X \setminus \wedge X$, $Sup([< x] \neq \emptyset)$ □

PROPOSITION 2.4. — *La projection sur la base $\beta : X \ni x \to B \cap [\leq x] \in (2^B, \subset)$ est un isomorphisme d'ordre et l'on a $B \subset C$ pour toute partie C de X ayant la même propriété.*

Preuve. — Soient $y, z \in X$. Si $Y := [\leq y] \setminus [< z]$ est vide, c'est-à-dire si $y \leq z$ on a $y\beta \subset z\beta$. Pour établir que β est isomorphisme il suffit donc de montrer que Y contient au moins un élément de la base quand $Y \neq \emptyset$.

Or comme Y est fini, il contient au moins un élément minimal b. On a $b \neq \wedge X$ puisque $\wedge X \in [\leq z]$ quand $\wedge X \neq \emptyset$, et donc $b \in B$ d'après le lemme 2.3.

Soit maintenant C une partie de X telle que l'application $\gamma : X \ni x \longrightarrow x\gamma = C \cap [\leq x]$ soit un isomorphisme. Supposons qu'il existe un $b \in B \setminus C$. D'après le lemme 2.3 il existe au moins un $z \in X \setminus [b \leq]$ tel que $[< b] \subset [\leq z]$. On a alors $b\gamma = C \cap [< b] \subset z\gamma = C \cap [\leq z]$, contredisant l'hypothèse que γ est un isomorphisme. Donc C contient B. □

On définit de même l'application $\bar{\beta} : X \in x \longrightarrow \bar{B} \cap [x \leq]$, et l'on a pour $\bar{\beta}$ des énoncés symétriques de ceux pour β. On notera que $x\beta = \emptyset$ ssi $x = \wedge X$, et $x\beta = X$ ssi $x = \vee X$.

Exemples. — Soit $X = \{1, 2, 3, 4\}$ avec la relation d'ordre $\leq$ définie par $\{1, 2, 3\} = [\leq 3]$ et $\{1, 2, 4\} = [\leq 4]$. Tous les éléments de X appartiennent à la base et à la cobase. La projection γ sur $C = \{1, 2, 3\}$ est injective, mais elle n'est pas un isomorphisme puisque $4\gamma = \{1, 2\} \subset 3\gamma = \{1, 2, 3\}$ bien que 3 et 4 soient incomparables. Le treillis enveloppant de X est obtenu en ajoutant à X un plus petit et un plus grand élément, et aussi un élément t tel que

$$t = Sup(\{1, 2\}) = Inf(\{3, 4\}) \ .$$

Ce treillis est le treillis enveloppant de $\mathfrak{S}(3)$ (muni de l'ordre fort) vu au 5.

La proposition 2.4 requiert une condition topologique quand X n'est pas fini. Ainsi elle n'est pas vraie quand $(X, \leq)$ est un intervalle de la droite réelle $\mathbb{R}$ puisque dans ce cas la base et la cobase sont des ensembles vides. Par contre elle est vraie pour $(\mathbb{Z}, \leq)$ qui est égal à sa base, puisque la condition des chaînes descendantes est vérifiée pour toute partie $[\leq y] \setminus [\leq z]$ non vide. Le treillis enveloppant est obtenu en ajoutant à $\mathbb{Z}$ un plus petit et un plus grand élément.

La proposition 2.4 est aussi vérifiée par le treillis distributif $(2^{\mathbb{Z}}, \subset)$ dont les éléments sont les parties de $\mathbb{Z}$.

Enfin soit X l'ensemble union de l'intervalle $[0, 1]$ de $\mathbb{R}$, muni de son ordre naturel et d'un ensemble $B = \{b_x : x \in [0, 1]\}$, d'éléments incomparables. On ajoute les relations croisées $0 < b_x$ et $b_x < x'$ ssi $x \leq x' \in [0, 1]$. Alors B est à la fois la base et la cobase de X. L'application $\beta : X \longrightarrow B$ est un isomorphisme d'ordre, ce qui n'est pas le cas de $\bar{\beta} : X \longrightarrow B$.

C'est un problème ouvert de trouver des catégories non triviales de treillis pour lesquelles la proposition 2.4 et sa symétrique sont vraies.

Soit $\mathcal{R}' \subset \bar{B} \times B$ la relation définie par $(\bar{b}, b) \in \mathcal{R}'$ ssi $\bar{b} \geq b$, c'est-à-dire, de façon équivalente, ssi $b \in \bar{b}\beta$ ou $\bar{b} \in b\bar{\beta}$.

PROPOSITION 2.5. — *La relation $\mathcal{R}'$ est une relation basique.*

Preuve. — Comme $X \setminus [\leq x] \neq \emptyset$, sauf si $x = \wedge X$, la preuve précédente montre que $\bar{b}\beta \neq B$ pour chaque $\bar{b} \in \bar{B}$. Supposons qu'un élément $\bar{b} \in \bar{B}$ et une partie $\bar{C}$ de $\bar{B}$ soient tels que $\bar{b}\beta = \cap\{\bar{c}\beta : \bar{c} \in \bar{C}\}$. Comme β est un isomorphisme d'après (2.4), on a $\bar{c} \in [\bar{b} \leq]$ pour tout $\bar{c} \in \bar{C}$, et réciproquement $\bar{b}\beta \subset x\beta$ pour tout $x \in [\bar{b} \leq]$; l'hypothèse implique que $\bar{b}\beta = \cap\{x\beta : x \in [\bar{b} \leq]\}$ et enfin $\bar{b} \in \bar{C}$ d'après la définition de $\bar{B}$.

Autrement dit, aucune ligne de $\mathcal{R}'$ n'est l'intersection d'autres lignes. Ceci achève la preuve par symétrie entre B et $\bar{B}$ □

Nous appelerons désormais la relation $\mathcal{R}'$ précédente la *relation basique* de l'ensemble ordonné $(X, \leq)$.

On voit facilement qu'un élément $x \in X$ appartient à $\bar{B} \cap B$ ssi $x\bar{\beta} \times x\beta$ est un rectangle de **1** (au sens donné plus haut à ce terme) dans la relation basique.

Donnons maintenant à la preuve du théorème 2.6.

Prenant une copie $\bar{X}$ de X et une bijection $X \ni x \to \bar{x} \in \bar{X}$, nous associons à $(X, \leq)$ sa *matrice d'incidence*, c'est-à-dire la relation $\mathcal{R}$ dans $\bar{X} \times X$ telle que $(\bar{x}_1, x_2) \in \mathcal{R}$ ssi $x_1 \geq x_2$. La relation basique de $(X, \leq)$ est simplement la restriction de $\mathcal{R}$ à $\bar{B} \times B$.

Utilisant les conventions du début de cette annexe, on voit que pour chaque $x \in X$, on peut identifier la colonne $x\bar{\rho}$ à l'intervalle supérieur $[x \leq]$ et la ligne $\bar{x}\rho$ à $[\leq \bar{x}]$. Le treillis T et le treillis antiisomorphe $\bar{T}$ de la construction de Ore sont donc respectivement le treillis enveloppant de $(X, \leq)$ et celui de l'ensemble antiisomorphe $(\bar{X}, \geq)$.

Comme les applications β et $\bar{\beta}$ sont injectives, les relations $\mathcal{R} \cap (\bar{X} \times B)$ et $\mathcal{R} \cap (\bar{B} \times X)$ engendrent des paires de treillis isomorphes à $\bar{T} \times T$. Les hypothèses du lemme 2.8 sont donc satisfaites, ce qui permet de conclure que la relation basique $\mathcal{R} \cap (\bar{B} \times B)$ de $(X, \leq)$ est aussi celle du treillis T □

Nous en venons maintenant au clivage.

Soit $\mathcal{R} \subset \bar{B} \times B$ la relation basique d'une relation d'ordre $(X, \leq)$.

Le lemme 2.2 montre que deux éléments $\bar{x}, x \in X$ sont tels que X n'est l'union disjointe de $[\leq \bar{x}]$ et $[x \leq]$ que si $(\bar{x}, x) \in \bar{B} \times B$. En ce cas, x détermine $\bar{x}$ et réciproquement.

Il est clair que si $(\bar{b}_1, b_1)$ et $(\bar{b}_2, b_2)$ sont deux paires clivantes, on a $b_1 \leq b_2$ ssi $\bar{b}_1 \leq \bar{b}_2$. Ceci conduit à définir le morphisme partiel NEG de B dans $\bar{B}$ en posant :

$$NEG(b) = \bar{b} \text{ s'il existe } \bar{b} \in \bar{B} \text{ tel que } (\bar{b}, b) \text{ soit un clivage}$$
$$= \emptyset \text{ sinon}$$

Nous supposons désormais que X est le treillis défini par R.

Soient $b \in B$, $Y := X \setminus [b \leq]$ et $s := Sup(Y)$. L'ensemble X est l'union de $[\leq s]$ et de $[b \leq]$, cette union étant disjointe ssi $b \notin [\leq s]$. Donc $NEG(b) = s$ ou $\emptyset$ selon que $b \notin [\leq s]$ ou non.

Considérons alors l'unique élément b_- couvert par b. Comme $b_- \in Y$, on a $Inf(b_-, s) \in \{b, b_-\}$ et d'autre part $Sup(Inf(b, y) : y \in Y) = b_-$.

Par conséquent la relation de distributivité

$$Inf\big(b_-,\, Sup(Y)\big) = Sup\big(\{Inf(b_-,\, y) : y \in Y\}\big)$$

implique $b \notin [\leq s]$ et enfin $NEG(b) = s \neq \emptyset$.

Compte tenu de la symétrie entre B et $\bar{B}$, cette remarque établit la partie directe du théorème 2.8.

Revenant au cas général, nous isolons le

Lemme 8.5. — *Pour chaque $b \in B$, on a $NEG(b) \neq \emptyset$ ssi il existe un $\bar{b} \in \bar{B}$ tel que $\bar{b}\,\beta = B \setminus [b \leq]$.*

Preuve. — Il suffit d'observer qu'avec les notations introduites plus haut, on a $b \notin [\leq s]$ ssi $s\beta = Y \cap B$ □

Comme $B \cap [b \leq]$ est l'ensemble des $b' \in B$ tels que $b'\bar{\beta} \subset b\bar{\beta}$, il en résulte que la fonction NEG se calcule directement à partir de la relation $\mathcal{R}$ et, de plus, que si $NEG(b) \neq \emptyset$ pour chaque $b \in B$, la restriction de $\mathcal{R}$ à $NEG(B) \times B$ est déterminée par la seule donnée de la restriction de l'ordre $\leq$ à B.

Pour achever la preuve, nous supposons désormais $\mathcal{R}$ telle que $NEG(b) \neq \emptyset$ pour chaque $b \in B$.

Soit $T \in 2^{2^B}$ le plus petit treillis pour les opérations $\cup$ et $\cap$ de $(2^B, \subset)$ qui contienne tous les sous-ensembles $b_0 := [b \leq]$ $(b \in B)$ de B; il est classique que $(T, \subset)$ est un treillis distributif en tant que sous-treillis du treillis distributif $(2^B, \subset)$. En outre $b \longrightarrow b_0$ est un isomorphisme (d'ordre) de B sur une partie B_0 de T.

Posons aussi $b^0 := B \setminus [b \leq] \subset 2^B$ pour chaque $b \in B$. Cet ensemble appartient à T et il est l'union des $b'_0 \in B_0 \setminus [b_0 \subset]$, ce qui montre que (b^0, b_0) est un clivage de T et que la base et la cobase de ce treillis sont B_0 et $B^0 = \{b^0 : b \in B\}$.

D'après le lemme 8.5, la relation basique $R_0 \subset B^0 \times B_0$ de T est isomorphe à la restriction $\mathcal{R}'$ de $\mathcal{R}$ à $\bar{B}' \times B$ où $\bar{B}' = NEG(B) \subset \bar{B}$.

On vérifie maintenant que $\bar{B}' = \bar{B}$. Soit $\bar{b}$ un élément de la cobase $\bar{B}$. Si $b \in \bar{b}\beta$, on a $b' \in \bar{b}\beta$ pour tout $b' \in B \cap [\leq b]$ d'après la définition de $\leq$. Par conséquent, l'image de $\bar{b}\beta$ dans 2^B par l'isomorphisme $b \longrightarrow b_0$ est un élément du treillis T. On a donc $\bar{b} \in \bar{B}'$, montrant que $\bar{B}' = \bar{B}$, c'est-à-dire que T est bien le treillis engendré par $\mathcal{R}$ □

Les calculs dans le treillis distributif T sont facilités par l'identité de Morgan

$$t\bar{\beta} = NEG(B \setminus t\beta) \quad (t \in T)$$

que l'on déduit immédiatement du lemme 8.5 en identifiant, par complémentation ensembliste, le treillis antiisomorphe $\bar{T} \in 2^{2^{\overline{B}}}$ à un sous treillis de $(2^B, \subset)$.

Il est curieux que l'égalité numérique $card(B) = card(\bar{B})$ entre la base et la cobase reste vraie dans la variété des treillis modulaires dont les treillis distributifs sont une sous variété.

Pour avoir des exemples plus substantiels, nous considérons le treillis des partitions d'un entier n. Nous faisons référence à un article récent de C.Greene et Kleitman [G-K] dans lequel le lecteur trouvera exposés les principaux résultats sur l'ensemble des partitions en tant que treillis (cf. aussi S.Kim dans un article à paraître).

Nous adoptons la notation exponentielle pour les partitions, et appelons *équerre* une partition du type $1^k c$, i.e. une partition qui a au plus une part différente de 1.

PROPOSITION 8.6. — *La base du treillis des partitions d'un entier fixé n est constituée des partitions, ayant trois parts différentes au plus, du type $ab^k c$, où $k \geq 2$ et $a < b < c$, avec les cas dégénérés suivants : ab^k, $b^k c$, b^k, ($k \geq 2$), et bc.*

La cobase est formée des partitions transposées des éléments de la base. L'intersection de la base et de la cobase est constituée par les équerres.

Pour que deux partitions g, $\bar{g}$, déterminent un clivage, il faut que l'une d'entre elles soit une équerre. Réciproquement, chaque équerre donne deux clivages, selon qu'elle est considérée comme un élément de la base ou de la cobase.

Preuve. — En effet, deux partitions sont consécutives dans le diagramme des partitions ssi l'on obtient le diagramme de l'une à partir de celui de l'autre en déplaçant de manière minimale une boîte. Si la partition a au moins quatre parts différentes, elle ne peut être irréductible pour $\vee$. On exclut ensuite les cas $a^h b^k c^l$ où $hl > 1$. Les cas restants se vérifient sans difficulté.

Soit maintenant un clivage $[g \leq]$, $[\leq \bar{g}]$. La partition g appartient à la base, supposons la du type $g = ab^k c$, $a < b \leq c$ où $2 \leq k$ si $b \neq c$ et

$1 \leq k$ si $b = c$. Considérons $h = 1^{n-c-1}c + 1$. L'élément g ne vérifie pas $g \leq h$, puisque $a < a + 1$. Or h est couverte par une seule partition, à savoir $h_+ := 1^{n-c-2}2\,c$ et l'on a $g \leq h_+$. Donc h est un élément maximal du complément de $[g \leq]$. Comme par hypothèse, ce complément est égal à $[\leq \bar{g}]$, on doit avoir $\bar{g} = h$. De plus alors $g = ac^m$, où m est la partie entière de n/c et a le reste. Par conjugaison des partitions, on vérifie que symétriquement, le complément de $[h \leq]$ est un intervalle inférieur □

Par exemple, les rectrices de $1^5 24^2$ sont 34^3, $13^3 5$, $12^4 6$ et $1^7 8$. Le lecteur pourra vérifier que le nombre des rectrices d'une partition est au plus égal à la valeur de sa deuxième plus grande part.

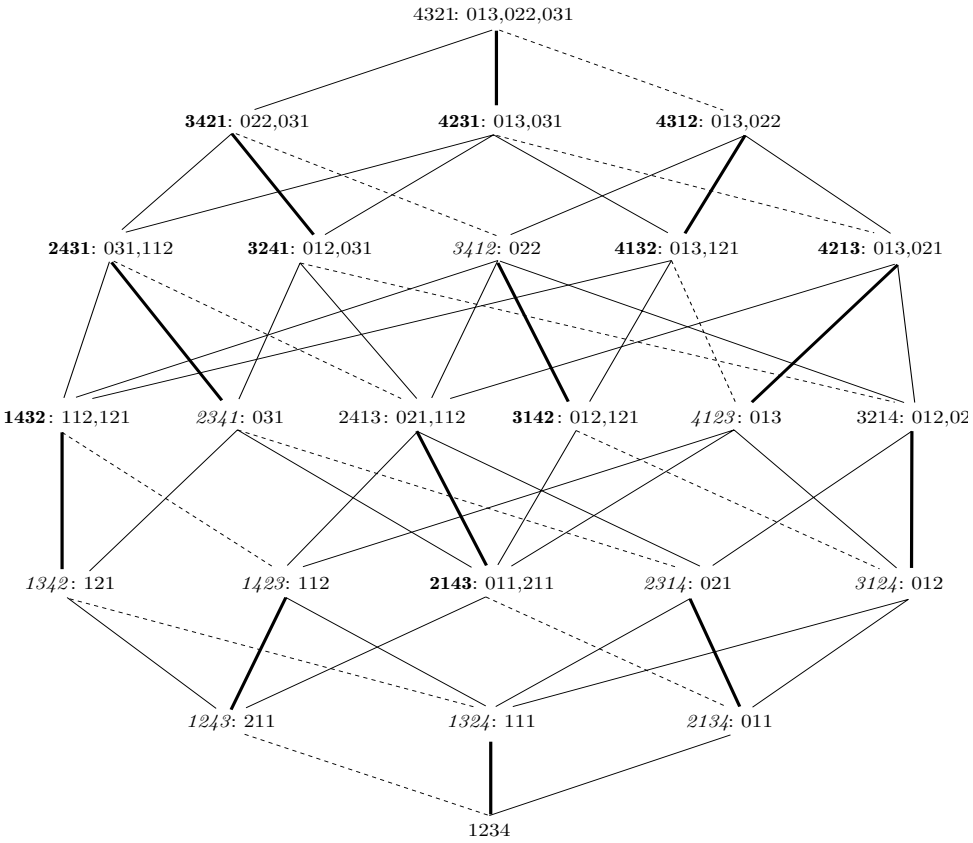
Bibliographie

[Bi] G. Birkoff, *Lattice theory*, 3ème ed., Am. Math. Soc., Providence (1967).
[Bj] A. Björner, *Ordering of Coxeter groups*, Contemp. Math. **34**, A.M.S. (1984) 175-195.
[B-W] A. Björner, M. Wachs, *Generalized quotients in Coxeter groups*, Trans. A.M.S. **308** (1988) 1-37.
[Bo] N. Bourbaki, *Groupes et Algèbres de Lie*, Fasc *34*, Hermann, Paris (1968).
[De] V.V. Deodhar, *Some characterizations of Bruhat ordering on a Coxeter group*, Invent. Math. **39** (1977) 187-198.
[Ch] I. Cherednik, *A unification of Knizhnik-Zamolodchikov and Dunkle operators via affine Hecke algebras*, Invent. Math. **106** (1991) 411-431.
[Eh] C. Ehresmann, *Sur la topologie de certains espaces homogènes*, Ann. Math. **35** (1934) 396-443.
[Er] H. Eriksson, *Computational and combinatorial aspects of Coxeter groups*, thèse, KTH Stockholm (1994).
[Fo] Fokko du Cloux, *A transducer approach to Coxeter groups*, prépublication (1995).
[Fu] W. Fulton, *Flags, Schubert polynomials, degeneraci loci* Duke Math. **65** (1992) 381-420.
[G-Ki] M. Geck, S. Kim, *On the Bruhat order of finite Coxeter groups*, prépublication (1996).
[G-K] C. Greene, D. Kleitman, *Longest chains in the lattice of integer partitions ordered by majorization*, Europ. J. Comb. **7** (1986) 1-10.
[G-R] G. Guilbaud, P. Rosenstiehl, *Analyse algébrique d'un scrutin*, in *Ordres totaux finis*, Gauthiers-Villars, Paris (1971).
[Lak] V. Lakshmibai, *Geometry of G/P. The symplectic group and the involution* σ, J. Alg. **108** (1987) 403-434.
[L-S 1] A. Lascoux, M.P. Schützenberger, *Structure de Hopf de l'anneau*

de cohomologie de la variété de drapeaux, C.R. Acad. Sc. Paris **295** (1982) 629-633.
[L-S 2] A. Lascoux, M.P. Schützenberger, *Symmetrization operators on polynomial rings*, Funk. Anal. **21** (1987) 77-78.
[Mo] A. Molev, *On Stirling partitions of the symmetric group*, prépublication, Australian National University (1995).
[MRR] W.H. Mills, D.P. Robbins, H. Rumsey, *Alternating sign matrices and descending plane partitions*, J. Comb. Th. A (1983) 340-359.
[Pr] R.A. Proctor, *Classical Bruhat orders and lexicographic shellability*, J. Alg. **77** (1982) 104-126.
[Vr] D.N Verma, *Möbius inversion for the Bruhat ordering on a Weyl group*, Ann. Sc. Ec. Norm. Sup **4** (1971) 393-398.

THE ELECTRONIC JOURNAL OF COMBINATORICS 3 (1996), #R27 34

Rectrices des permutations de S_4

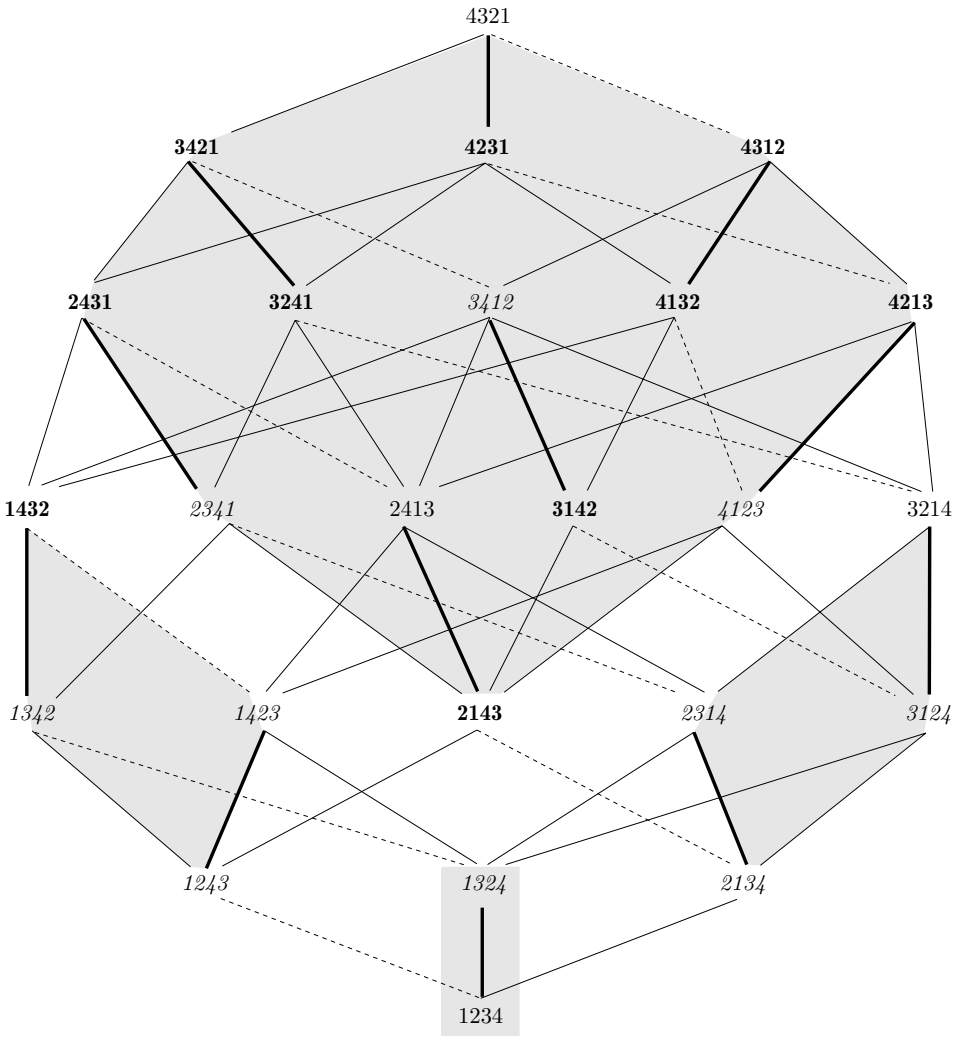


bigrassmanniennes en italique
cobigrassmannienne en gras

une rectrice $[r_0, r_1, r_2, r_3]$
se note $r_0\, r_1\, r_2$

THE ELECTRONIC JOURNAL OF COMBINATORICS 3 (1996), #R27 35

Pavage de $\mathbf{S}_4$



L'acte créateur

ÉTUDES RÉUNIES PAR

GILBERT GADOFFRE
ROBERT ELLRODT
JEAN-MICHEL MAULPOIX

puf écriture

Une sotie au sujet de la théorie des nombres parfaits

par Marcel Paul Schützenberger

Certes les mœurs sont devenues plus douces. Mais s'il ose parler au milieu des poètes, un informaticien n'en redoute pas moins de se voir pelé, et sa défroque suspendue aux branches. Sa seule ambition ne peut donc être que de divertir au risque de détourner le débat sur la création. Je m'avance à l'abri d'un texte classique.

« Deux tours énormes s'apercevaient dans la vallée. En les multipliant par deux le produit était quatre. Mais je ne saisissais pas très bien la nécessité de cette opération d'arithmétique, et je continuais ma route avec la fièvre au visage et je m'écriais sans cesse: "Non, non, je ne distingue pas très bien la nécessité de cette opération d'arithmétique". » Je confesse que moi non plus ou du moins pas encore, pas ici.

C'était, bien sûr, un extrait d'un chant de Maldoror, et les méthodes de la critique moderne prouveront qu'indubitablement il s'agit du quatrième (où $4 = 2 \times 2 = 2^2$).

Veuillez avoir l'indulgence d'admettre que le calculateur, c'est-à-dire celui qui aligne des calculs comme d'autres des pensées ou des vers, n'est ni un faune, ni un satyre, ni un sciapode, ni Fafner, tapi au fond de ses ateliers. Qu'il est doué d'une espèce de parole, bien qu'elle

diffère de celle des poètes par le mode et le temps et surtout par la contrainte de pouvoir supporter à l'infini paraphrases et retraductions.

Ce qui implique que son mode ne soit pas l'optatif, ni le subjonctif, ni le jussif. Ce n'est même pas l'indicatif des naturalistes, mais seulement l'interrogatif et encore de façon fort restreinte. Lautréamont demande « Pourquoi » ce qui serait trop ambitieux pour les calculateurs dont la réponse n'a le droit d'être que OUI, NON, ou le plus souvent « ?? ». C'est bien peu, trop *unidimensionnel*, décident les communicateurs, mais c'est la loi de notre cité telle que nous la tenons d'Euclide.

L'histoire que je vous soumets remonte d'ailleurs à lui.

Six est un nombre parfait parce que $6 = 3 + 2 + 1$ est égal à la somme de ses diviseurs. Huit ne l'est pas parce que la somme correspondante, $4 + 2 + 1 = 7$ et que huit n'est pas sept.

Il y a une excellente explication qui est fournie par Alcuin : six est parfait, parce que la Création s'est faite en six jours. Ce n'est pas le cas de huit et d'ailleurs la seconde création, celle qui a lieu après le Déluge, a impliqué les huit âmes qui étaient dans l'Arche. Alcuin est très clair sur ces points mais il ne fait que rassembler ce que bien d'autres avaient écrit avant lui, car le thème des nombres parfaits est un grand topique depuis Euclide. Il a été développé par Philon, inlassablement investigué par les gnostiques et commenté par Boèce que je tiens à citer pour montrer fièrement que nous avons au moins un poète avec nous.

Dans ses trois livres d'arithmétique, Euclide commence par établir la théorie des nombres premiers et conclut par la démonstration qu'il n'en existe pas un qui soit plus grand que tous les autres, c'est-à-dire, en langage codé, qu'il y en a une infinité. Le mouvement surprenant de cette preuve en préfigure d'autres qui, à travers Du Bois-Raymond et Cantor, mèneront aux grands théorèmes de Gödel. Puis viennent quelques propositions irrelevantes à

notre propos et enfin l'énoncé dramatique que si l'entier p est tel que $2^p - 1$ est premier alors $2^{p-1} \times (2^p - 1)$ est parfait. C'est le cas pour $p = 2, 3, 5, 7$ mais pas 9, et les quatre (encore) plus petits nombres parfaits sont connus depuis l'Antiquité.

Les voici :

$$6 = 2^1 \times (2^2 - 1) = 2 \times 3\,; \quad 28 = 2^2 \times (2^3 - 1) = 4 \text{ x } 7$$

qui admet des explications évidentes dès que l'on a abandonné le vieux rythme des semaines de cinq jours ;

$$496 = 2^4 \times (2^5 - 1) = 16 \text{ x } 31 \quad \text{et}$$

$$8128 = 2^6 \times (2^7 - 1) = 64 \times 127.$$

Observez 127.

Oui, je le sais, hélas, ces choses-là sont rudes dans nos siècles de fer, de verre et de plastique. Pourtant elles faisaient partie des connaissances des clercs passés par le trivium et le quadrivium. D'ailleurs, assis à cette table, j'ai un garant que l'Abbesse Hroswitha ne négligeait pas d'en informer ses moniales, ce qui était d'autant plus méritoire que l'on ne disposait pas encore de la limpidité des notations modernes. En particulier, manquait la convention d'écriture que 2^{k+1} désigne le résultat de la multiplication têtue de deux par lui-même k fois, grande simplification prosaïque de ce qui fit, dit-on, l'amusement du roi Gélon, et de divers sages princes orientaux.

Aussi, personne ne pouvait alors s'aviser que $1 = 2^0 \times (2^1 - 1)$ peut être considéré comme un nombre parfait, le zéro-*ième* et, c'est là encore un très profond mystère, peut-être le seul nombre parfait qui soit impair (cf. Lautréamont).

Euclide est trop classique pour poser une question. D'ailleurs la question se pose d'elle-même. Existe-t-il un nombre parfait qui soit plus grand que tous les autres ?

Les auteurs du Moyen Age restent dans le vague. Certains croient que les nombres parfaits se terminent alter-

nativement par 6 ou par 8, ce qui est une séduisante hypothèse attribuant un rôle privilégié à DIX = DEUX que multiplie CINQ. Mais elle n'est pas vraie. Pire, les auteurs affirment que le cinquième nombre parfait est :

$$2^{10} \times (2^{11} - 1).$$

Or $2^{11} - 1 = 2\,047$ n'est pas un nombre premier comme tout écolier pouvait le vérifier sans trop de peine puisqu'il suffit de constater qu'il est divisible par 23.

Sans doute la majorité des sorbonniqueurs ne faisait que recopier ce qu'elle avait lu, mais j'y vois une faute d'une toute autre gravité, celle de croire que le monde est trop simplement facile. La suite 2, 3, 5, 7, pas 9..., appelle 11 de façon trop voyante. Aurez-vous la dureté d'y dénoncer une erreur Pélagienne ? Il est curieux que Lefèvre d'Étaples soit tombé dans ce piège. Bovilius aussi, mais il a eu le mérite d'observer que les nombres parfaits sont des gnomons (c'est-à-dire des surfaces de triangles rectangles isocèles). Euclide le savait bien, mais il écrit hors du temps, donc sans citer ses prédécesseurs, et il ne manifeste aucune sympathie pour les Pythagoriciens.

Autre marque du temps chez les calculateurs. Chez vous les poèmes sont éternels, mais moins que les poètes et depuis les âges épiques, il n'y a plus de poèmes sans poètes alors que chez nous les théorèmes deviennent vite orphelins anonymes. Et nous ignorerons toujours qui a fait joyeusement quelque matin au Moyen Age la découverte que $2^{12} \times (2^{13} - 1)$ est un nombre parfait, le vrai *cinquième* nombre parfait.

Permettez un excursus dans le jardin de l'Amitié. Un nombre parfait est un nombre égal à la somme de ses parties aliquotes, comme on disait avant que les Conciles de Bourbaki n'aient exclu les mots aux allures pédantes qui effaroucheraient les gentils étudiants. Deux nombres sont amicables, *inter se amant*, si chacun est la somme des parties aliquotes de l'autre. La paire la plus connue est (220, 284). Les meilleurs commentateurs la réfèrent à la Genèse

car c'est le nombre des brebis et des autres présents que s'échangent Jacob et Ésau. Autres temps, autres usages. J'extraie de l'histoire de l'arithmétique que El-Magriti en 1107 rapporte avoir observé sur lui-même l'effet érotique des nombres amicables « quand on donne à manger le plus petit et qu'on consomme soi-même le plus grand ». Ibn Khaldun, malgré son scepticisme habituel, commente leur influence en notant la nécessité de tenir compte des thèmes astrologiques. Je passe vite à Descartes qui a trouvé une méthode pour obtenir de nouvelles paires. C'est un filon qui restera exploité jusqu'à nos jours.

Je reviens au nombre parfait. L'époque moderne commence avec Cataldi qui, en 1558, construit les premières tables des nombres premiers et découvre les deux nombres parfaits suivants. Ceux-ci correspondent à $p = 17$ et à $p = 19$. Ce n'est pas un mince travail car Cataldi accomplit une à une toutes les divisions qu'il convient. Cinquante ans plus tard, Fermat démontre des théorèmes grâce auxquels ces calculs auraient été considérablement allégés, mais il ne trouve pas de nombres parfaits nouveaux, car il se présente une lacune inattendue.

C'est le grand Euler qui, en 1771, montrera que le nombre parfait suivant est $2^{30} \times (2^{31} - 1)$. Il se trouve pour l'anecdote, que le nombre 2^{31} est très exactement la limite de ceux que les ordinateurs acceptent sans que l'on ait à invoquer des procédures spéciales.

Et puis, plus de découvertes pendant un siècle jusqu'à Édouard Lucas, qui n'a pourtant aucune réputation chez les mathématiciens professionnels car il est inspecteur de l'enseignement, et ne publie que des livres de mathématiques amusantes. Vers 1875, il invente un méthode entièrement originale pour dépister les nombres parfaits. Elle relie de façon encore mystérieuse leur quête (que les lettrés ne manqueraient pas de dire initiatique) à l'antique Nombre d'Or, c'est-à-dire au pentacle. Est-ce une partialité sectaire que de croire qu'il était pythagoricien ? En était-il de même pour Fibonacci ? Sa méthode réduit à

presque rien les calculs exigés pour la vérification des cas déjà connus, mais il se borne à en montrer la vertu en prouvant que $2^{126} \times (2^{127} - 1)$ est parfait. Vous avez reconnu 127, mais évitez des hypothèses trop hâtives ; en particulier, à un étage subalterne, que l'auteur de ces lignes serait moindrement cabaliste. Très vite, d'autres appliquent la méthode et débusquent quelques nombres parfaits nouveaux.

Voyez comme notre temps est plus lent que celui des Arts. Pendant plus d'un demi-siècle, on ne trouvera rien malgré des efforts nombreux et bien d'autres qui demeurent des échecs inavoués. Malgré l'outil forgé par Lucas, la masse des calculs est trop écrasante.

Mais en 1952, en Angleterre, Robinson montre que $2^{520} \times (2^{521} - 1)$ est parfait. Il a utilisé un ordinateur, et c'est aussi la première fois que ces machines fournissent un résultat proprement mathématique. Depuis, le domaine est devenu une petite industrie où amateurs et professionnels rivalisent pour enrichir la liste des nombres parfaits toujours grâce à la méthode de Lucas, et mille ingéniosités dans sa programmation.

Il est convenable (parce que $25 = 5^2$) de citer le *vingt-cinquième* nombre parfait. Il correspond au nombre premier 21 701, et il suffit pour l'écrire d'aligner une quinzaine de milliers de chiffres.

Désormais la technique intervient dans cette longue procession. On s'active aujourd'hui autour de $p = 33\,843$, et des mathématiciens s'acharnent à trouver, à l'instar de Lucas, des propriétés permettant d'avancer vers la solution de l'énigme. Dans ce travail, il faut beaucoup d'ardeur et une confiance inébranlable dans l'espoir du succès. On connaît d'ailleurs l'histoire du Rabbin Luria qui, en Bessarabie, à l'occasion de la Fête des Tabernacles, rassemble ses disciples et leur dit : « Prions, et demain nous serons à Jérusalem. » Le premier disciple demande : « Est-ce bien vrai, Rabi ? » Et le rabbin soupire : « C'eût été si beau de passer Sukhot à Jérusalem. »

Mais s'il n'y a pas d'autre voie que le test de Lucas, le temps de cette question ne sera plus que celui des machines. Et comme l'observe Daniel Shanks, auquel j'ai fait plus qu'emprunter, on pourrait évaluer le degré d'avancement technologique d'une civilisation extraterrestre sans en savoir rien d'autre que la taille du plus grand nombre parfait qu'elle est capable de nommer.

Ce serait humiliant. (Ne gronde pas, Fafner !) Et pour certains, absurde. Pourquoi perdre du temps à résoudre ces problèmes ? Entre Euler et Lucas un mathématicien anglais, Peter Barlow, en 1814, écrit dans une encyclopédie que : « Les nombres premiers étant seulement curieux, sans être utiles, il est peu vraisemblable qu'il se trouve des personnes pour essayer d'en trouver de nouveaux. » Je n'ai pas tenté d'établir le contraire ni de vous convaincre que le calcul soit autre chose que la drogue des calculateurs. Ni de dire que les merveilleux miracles que nous y voyons ne sont pas de misérables merveilles pour reprendre le mot de Michaux. Misérables aux yeux du dieu qui est à Delphes, du dieu qui n'est qu'à Delphes.

Car quel est le statut des nombres parfaits correspondant à des nombres premiers ayant deux cents chiffres comme nous pouvons maintenant en produire en série et non pas cinq comme 33 843 ? Il n'y a pas assez de matière dans l'univers visible pour construire un ordinateur permettant la vérification au moyen du test de Lucas. Peut-être même, Gödel l'autorise, la réponse est « ?? ». Ultime ?, ou provisoire ?

Il y a une autre loi, ésotérique, qui, dans notre cité, n'oblige que ceux qui la connaissent. Elle est l'un des sens de la Parabole du Rabbin Luria et présuppose que la découverte et la preuve d'un théorème sont actes de volonté dans l'absolue liberté que laisse un Créateur auquel n'importe rien de ce qui est fini. Ce qui leur fait tenir pour vains les propos de Barlow, calculateur honorable mais homme par trop appliqué, même pour avoir dit une phrase fatale. Après la fin des temps...

(Ici la bande du magnétophone est devenue inaudible : vengeance de Fafner, ou sagesse éditoriale supérieure, car rien n'est futile comme le bavardage d'un calculateur sur le calcul. On reconnaît cependant une référence majeure à George Steiner faisant lui-même, par récursion, référence à un Château, puis des segments d'une longue phrase embrouillée évoquant des calculateurs à l'œuvre, sans nulle inconscience, devant la septième porte, celle qui donne sur la nuit.)

Math. Inf. Sci. hum., (35e année, n°140, *1997*, pp.5-10)

POUR LE MONOÏDE PLAXIQUE

Marcel-Paul SCHÜTZENBERGER

RÉSUMÉ — *Cet article est probablement le dernier texte de mathématiques écrit en vue de sa publication par M.P. Schützenberger, décédé en juillet 1996.*

Il était offert par son auteur en hommage à André Lentin, à l'occasion d'un colloque tenu en l'honneur de celui-ci le 23 février 1996 ; M.P. Schützenberger, déjà très malade, n'avait pu participer à cette rencontre, mais avait tenu à rédiger, non sans souffrances, une contribution scientifique qui témoignât de son amitié pour A. Lentin.

Lorsque je lui dis que certains des articles élaborés pour la "Journée Lentin", et le sien en particulier, seraient ultérieurement publiés dans Mathématiques, Informatique et Sciences humaines, *il en montra de la satisfaction.*

Voici la publication promise.

SUMMARY — A vote for the plactic monoid

This paper is most likely the last mathematical article published by the late M.P. Schützenberger, who died in July 1996.

It was writen in view of the celebration of André Lentin's jubilee, held in February 1996. M.P. Schützenberger, actually too sick, did not attend that scientific meeting. But he had the will despite distressing suffering, to prepare the present work and to offer it to his friend ; and did it.

He expressed to us his satisfaction to know that this work would be published in Mathématiques, Informatique et Sciences humaines.

Here it is.

Ce texte est une brève réponse à une question posée il y a bien longtemps par mon ami André Lentin et plus récemment par Gian-Carlo Rota :

"*Quelles raison as-tu de considérer le monoïde plaxique comme un des monoïdes fondamentaux de l'algèbre ?*".

Les origines et les propriétés de ce monoïde étant la théorie des permutations, sous divers aspects plantés ou cultivés dans le département où s'accomplit la part la plus universitaire de ta multiple carrière, je m'enhardis à te faire un hommage de ma réponse.

Trois sont les raisons de la faiblesse que j'ai pour le monoïde plaxique.

D'abord quelques notations ou conventions de style.

Soient :

- $\mathbb{A}^*$ = le monoïde libre engendré par l'alphabet totalement ordonné $\mathbb{A} = \{a_1 < a_2 < ...\}$ (ou plus commodément $\mathbb{A} = \{... a < ... < b < ... < c < ...\}$) ;
- $\mathbb{Z}(\mathbb{A}^*)$, son algèbre et *Ev*, le morphisme canonique (l'*évaluation*) de $\mathbb{Z}(\mathbb{A}^*)$ sur l'algèbre usuelle $Pol(\mathbb{A})$ des polynômes commutatifs en les variables de $\mathbb{A}$.

Un mot $w = w_1 ... w_n$, $(w_i \in \mathbb{A})$ est une *colonne* si et seulement si $w_1 > w_2 > ... > w_n$ et une *ligne* si et seulement si $w_1 \leq w_2 \leq ... \leq w_n$.

Les lignes (resp. colonnes) sont en bijection avec la base de $Pol(\mathbb{A})$, c'est-à-dire les monômes (resp. avec l'algèbre distributive libre, c'est-à-dire les parties de $\mathbb{A}$).

La congruence plaxique $\uparrow$ est définie par les relations suivantes dont le mérite de la découverte revient à D. Knuth :

Pour tout : $a, b, c \in \mathbb{A}$ $a < b \leq c \Rightarrow bca \equiv bac$

$$a \leq b < c \Rightarrow acb \equiv cab$$

De façon équivalente, d'après Kazhdan et Lusztig, si w est un mot de longueur 3, on a $w \equiv w'$ où $w' = w$ si w est une ligne ou une colonne, et où, dans le cas contraire, w' est l'unique mot ayant cette même propriété qui se déduise de w par permutation de deux lettres adjacentes.

L'algorithme de Schensted est une application directe des relations précédentes. P. Moszkowski en a donné une présentation originale qui rend extrêmement faciles les calculs à la main (un hommage à André Lentin !).

PREMIÈRE RAISON

Soit, dans $\mathbb{Z}(\mathbb{A}^*)$, L_k la somme des colonnes de longueur k (= 1, 2, ..., $card(\mathbb{A})$). Les images dans $Pol(\mathbb{A})$ des L_k sont les fonctions symétriques élémentaires des lettres de $\mathbb{A}$ et forment donc un ensemble minimal de générateurs de la sous-algèbre $Sym(\mathbb{A})$ des polynômes symétriques.

Par conséquent, si $\sim$ est une congruence sur $\mathbb{A}^*$ commutant avec l'évaluation telle que les images de L_k dans $\mathbb{Z}(\mathbb{A}^* / \sim)$ commutent deux à deux, la sous-algèbre de $\mathbb{Z}(\mathbb{A}^* / \sim)$ qu'elles engendrent est isomorphe à $Sym(\mathbb{A})$.

Or cette condition sur $\sim$ admet deux solutions extrémales :

- l'une est la congruence plaxique ;
- l'autre peut être récusée pour mille excellentes raisons, la plus simple étant peut-être que le nombre de ses classes croît (avec la longueur des mots) beaucoup moins vite que pour la congruence plaxique.

La valeur de cette première raison et appuyée par le fait qu'une variante des calculs précédents s'applique utilement à certaines algèbres de Hecke (je fais ici allusion au monoïde nilplaxique dont les relations de définition sont à peu près les mêmes que les relations plaxiques).

Un autre argument en faveur de la congruence plaxique est la propriété suivante, conséquence triviale de la définition, mais exceptionnelle parmi les monoïdes présentés. Notons $v(\mathbb{B}^*$ la restriction du mot v au sous-alphabet $\mathbb{B}$ (c'est-à-dire le sous-mot de v obtenu en y

effaçant les lettres qui n'appartiennent pas à $\mathbb{B}$). Dans le monoïde plaxique on a identiquement :

$$w \equiv w' \quad w \ (\mathbb{B}^* \equiv w' \ (\mathbb{B}^*$$

pour chaque sous-intervalle $\mathbb{B}$ de l'alphabet $\mathbb{A}$.

DEUXIÈME RAISON

Grâce à la théorie de Curtis Greene, nous savons associer à chaque mot $w \in \mathbb{A}^*$ une partition $p_k \leq p_{k-1} \leq \ldots \leq p_1$ de sa longueur n par la condition que $p_k + p_{k-1} + \ldots p_{i+1}$ soit le maximum de la longueur des sous-mots de w qui peuvent être obtenus en effaçant dans w i sous-mots qui sont des colonnes $(i = 1, 2, \ldots)$.

Notons $[\![w]\!]$ cette partition et appelons la *forme plaxique* de w. L'application $w \to [\![w]\!]$ est une *norme*, en ce sens que l'on a identiquement :

$$[\![ww']\!] \leq [\![w]\!] \oplus [\![w']\!]$$

où $\oplus$ est l'addition des partitions au sens de Philipp Hall. C. Greene a observé que :

$$w \equiv w' \quad [\![w]\!] = [\![w']\!].$$

Mais réciproquement, on peut caractériser la congruence plaxique par la propriété d'être la congruence *syntaxique* de la norme $[\![\ ]\!]$, c'est-à-dire d'être la congruence extrémale sur $\mathbb{A}^*$ telle que deux éléments de chacune de ses classes aient même forme plaxique.

J'intercale ici une digression. Le produit ww' de deux mots est *franc* si et seulement si $[\![ww']\!] = [\![w]\!] \oplus [\![w']\!]$. Un *contretableau* (resp. *tableau*) est un mot qui est un produit franc de colonnes de longueurs non décroissantes (resp. non croissantes). La construction de Schensted montre que chaque classe plaxique contient un et un seul contretableau (et un et un seul tableau). Enfin l'ensemble des colonnes est un treillis distributif pour l'ordre $v \preceq v'$ défini par $v \preceq v'$ si et seulement si il existe une injection non décroissante des lettres de v dans celles de v'.

Avec ces notations, un contretableau est simplement un produit $v_1\, v_2\, \ldots\, v_k$ de colonnes telles que $v_1 \preceq v_2 \preceq \ldots \preceq v_k$.

Comme on peut le penser, l'opération de shuffle sur les mots joue un grand rôle dans la théorie du monoïde plaxique. Elle a permis à A. Lascoux de donner une version non commutative (dans $\mathbb{Z}\langle\langle \mathbb{A}^* \rangle\rangle$) des fonctions symétriques, avec comme conséquence une compréhension meilleure de la structure de leur algèbre.

TROISIÈME RAISON

Un quotient extrémalement voisin de $Pol(\mathbb{A})$ de l'algèbre $\mathbb{Z}\langle\langle \mathbb{A}^* \rangle\rangle$ est obtenu en posant $u \to u'$ pour $u \approx u' \quad \mathbb{Z}\langle\langle \mathbb{A}^* \rangle\rangle$ si et seulement si $u\mu$ et $u'\mu$ coïncident en degré ≤ 2, où l'homomorphisme de Magnus m consiste à remplacer chaque variable $a \in \mathbb{A}$ par $a\mu = 1+a$. De façon équivalente, $\mathbb{Z}\langle\langle \mathbb{A}^* / \approx \rangle\rangle$ est isomorphe à l'algèbre de Lie libre nilpotente de classe 2,

c'est-à-dire au quotient de $Z(A^*)$ par l'idéal qui définit la condition que tous les commutants $[b,a]$ (= ba - ab) sont dans le centre.

La fonction génératrice de l'une des bases de $\mathbb{Z}(\mathbb{A}^* / \equiv)$ est le produit de Cauchy :

$$P = \prod_{a_i \in \mathbb{A}} (1 - a_i)^{-1} \prod_{\substack{a_i < a_j \\ a_i, a_j \in \mathbb{A}}} (1 - a_i a_j)^{-1}$$

(calculé dans l'algèbre commutative).

Comme P est la somme des fonctions de Schur sur $\mathbb{A}$, c'est-à-dire la somme des images commutatives des "tableaux", et comme ces derniers forment une section (= ensemble minimal des représentants des classes) de la congruence plaxique $\equiv$, on voit que $A^* / \equiv$ admet P comme fonction génératrice (commutative). Les autres quotients de $\mathbb{A}^*$ ayant la même propriété sont maintenant le domaine de Daniel Krob. Le monoïde plaxique est caractérisé parmi eux par la seule condition supplémentaire que, pour chaque mot

$$w = a_1^{m_1} a_2^{m_2} \ldots a_h^{m_h} \in \mathbb{A}^*$$

où l'un au moins des m_i est ≥ 2, il n'y ait qu'un seul mot qui soit seul dans sa classe de congruence parmi tous les mots ayant même évaluation (= image commutative) que w.

Une caractérisation dont la vérification est moins fastidieuse est que la congruence plaxique est la seule dont une section soit l'ensemble des tableaux.

Il y a certainement de meilleurs énoncés, mais les autres objets découverts par D. Krob sont fort hétéroclites et encore mal connus.

Telles étaient mes trois raisons pour affirmer la nécessité d'installer le monoïde plaxique parmi les structures remarquables. Il y en a une autre plus ténébreuse.

Il existe un monoïde présenté très évident dont les propriétés ne sont jamais données qu'à titre d'exercices mineurs. Il s'agit du *monoïde cycliste* B engendré par deux lettres a et b que relie la seule identité :

$$ba = 1.$$

Autrement dit, b est l'inverse à gauche de a.

Une section de B est formée des mots $a^n b^m$ ($n, m \in \mathbb{N}$). Ses deux propriétés fondamentales sont :

- Tout quotient de B est isomorphe à $\mathbb{Z}$ (par $a^n b^m \mapsto n - m$) ou à un quotient de $\mathbb{Z}$ à travers le quotient précédent ;
- B n'a pas d'idéaux stricts (c'est-à-dire $1 \in B\,x\,B$) pour tout $x \in B$ bien qu'il ne puisse pas être injecté dans un groupe, et tout monoïde sans idéaux stricts qui n'est pas un groupe contient au moins une copie de B.

Cette deuxième propriété implique qu'aucun monoïde compact ne contient une copie de B, donc que B n'admet aucune représentation linéaire de dimension finie.

Pour l'anecdote, je rappelle que B peut être défini comme le monoïde syntaxique du sous-ensemble des mots de $\{a, b\}^*$ dont tous les facteurs gauches contiennent au moins autant de b que de a.

Pour remonter B en un quotient de $\{a, b\}^*$ compatible avec le morphisme d'évaluation, on remplace la relation $ba = 1$ par les deux relations :

(*) $$baa \equiv aba \quad \text{et} \quad bba \equiv bab$$

exprimant que ba commute avec a et b. Or ces nouvelles relations ne sont autres que celles définissant le monoïde plaxique sur deux lettres a et $b > a$ (dont une section est d'ailleurs l'ensemble des tableaux $(ba)^p a^n b^m$, $(n, m, p \in \mathbb{Z})$).

Revenons au cas général de $\mathbb{A} = \{a_1 < a_2 < \ldots < a_n\}$. Tenant compte de la propriété rappelée à la fin de la première raison, on définit une congruence $\sim$ sur $\mathbb{A}^*$ par le morphisme envoyant chaque mot sur le produit direct de l'image dans le monoïde plaxique $\{a_i, a_{i+1}\}^* / \equiv$ de sa restriction $w \in \{a_i, a_{i+1}\}^* (i = 1, 2, \ldots)$. Le monoïde $A^* / \sim$ est le quotient cycliste du monoïde plaxique $A^* / \equiv$. Il a été utilisé avec succès par A. Lascoux, B. Leclerc et J.-Y. Thibon pour certains problèmes de représentations modulaires.

Reste à justifier les relations plaxiques élémentaires sur trois lettres, c'est-à-dire à retrouver $\equiv$ parmi les congruences contenues dans $\sim$.

La seule manière que je connaisse est d'utiliser le fait que pour tout sous-alphabet $\mathbb{B} \subset \mathbb{A}$, la colonne $v_{\mathbb{B}}$ contenant toutes les lettres de $\mathbb{B}$ engendre le centre du monoïde plaxique $\mathbb{B}^* / \equiv$.

J'aimerais beaucoup mieux une caractérisation du monoïde plaxique employant les prédicats utilisés pour énoncer les propriétés fondamentales du monoïde cycliste. Mais je ne sais pas le faire, bien que le quotient du monoïde plaxique par son centre n'ait pas d'idéaux propres.

Peut-être pourrait-on faire jouer le fait que pour chaque lettre c de $\mathbb{A}$, chaque classe plaxique admet un unique facteur gauche de longueur maximale dont toutes les lettres sont $\geq c$?

Et demain ?

En des lieux divers (le Japon, Strasbourg, le M.I.T., Marne la Vallée), les mathématiciens qui développent la théorie des groupes quantiques ont retrouvé le monoïde plaxique ou l'un de ses quotients comme cas particulier de leurs constructions : quand, dans leur poétique, ils font tendre la température q vers zéro pour les cristalliser.

J.-Y. Thibon et B. Leclerc remontent les grands fleuves de ce continent qu'ils sont en train de découvrir. A. Lascoux organise l'expédition que je regarde partir de mon hamac, entre deux palétuviers dans l'estuaire.

10

BIBLIOGRAPHIE

GREENE, C., "An extension of Schensted's theorem", *Advances in Math.*, 14, (1974), 254-265.

GREENE, C., "Some partitions associated with a partially ordered set", *J. Comb. Th.*, A 20, (1976), 69-79.

KAZDHAN, D., LUSZTIG, G., "Representations of Coxeter groups and Hecke algebras", *Inv. Math.*, 53, (1979), 165-184.

KNUTH, D., "The Art of Computer Programming", *Sorting and Searching*, vol.3, Addison-Wesley, (1973).

KROB, D., THIBON, J.-Y., "Representations of the Hecke algebra of type A and corepresentations of the quantum group $A_q(n)$ at q=0, and the hypoplactic algebra", prépublication L.I.T.P., (1995).

LASCOUX, A., LECLERC, B., THIBON, J.-Y., "Crystal Graphs and q-analogues of weight multiplicities for the root system A_n", *Letters in Math. Phys.*, 35, (1995), 359-374.

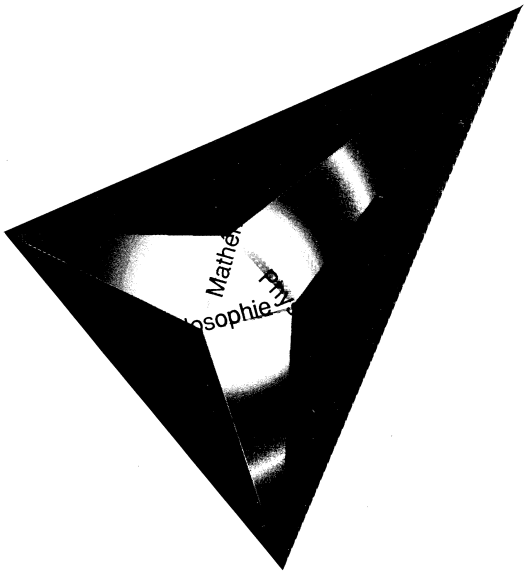
LASCOUX, A., SCHÜTZENBERGER, M.P., "Le monoïde plaxique", *Non commutative structures in Algebra and Combinatorics*, Quaderni della Ricerca Scientifica del CNR, Roma, (1981).

MOSZKOWSKI, P., "A bijection between trees and factorizations of cyclic permutations", *European Journal of Combinatorics*, 10, (1989), 13-16.

SCHENSTED, C., "Longest increasing and decreasing subsequences", *Canadian J. Math.*, 13, (1961), 179-191.

ALAIN CONNES

TRIANGLE DE PENSÉES



ANDRÉ LICHNEROWICZ
MARCEL PAUL SCHÜTZENBERGER

EDITIONS ODILE JACOB
SCIENCES

Table des matières

Tome XII

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 12 : 1990 –

Les travaux réunis dans ce tome portent sur la combinatoire du groupe symétrique.
L'article « Keys & standard bases » donne une interprétation, en terme de tableaux, des « polynômes clefs », c'est-à-dire des caractères de Demazure pour le système de racines de type A.
L'article fondamental « Treillis et bases des groupes de Coxeter » part d'un problème qui rejoint les premiers travaux de Schützenberger sur le clivage des treillis. La question examinée est : comment décomposer le groupe symétrique en deux intervalles complémentaires relativement à l'ordre d'Ehresmann–Bruhat ? La réponse exhibe un sous-ensemble minimal de permutations qui code toute l'information sur l'ordre, et aboutit à plonger le groupe symétrique dans un treillis distributif dont les éléments sont les matrices à signe alternant.
L'article « Pour le monoïde plaxique », sous forme d'une lettre à ses amis André Lentin et Gian-Carlo Rota, est un plaidoyer de Schützenberger pour justifier pourquoi il a consacré autant de ses efforts, dans les vingt dernières années, aux beautés du monoïde plaxique.