Marcel-Paul Schützenberger

ŒUVRES COMPLÈTES

éditées par
Jean Berstel, Alain Lascoux et Dominique Perrin

*

Tome 8 : 1971–1975

Institut Gaspard-Monge, Université Paris-Est
2009

Introduction
Tome VIII : 1971–1975

L'article *On the principle of equivalence of Sparre Andersen* [1971-1] se veut une algébrisation dudit principe, bien connu dans l'étude probabiliste des fluctuations de variables aléatoires, qui veut que le « nombre de sommes partielles strictement positives » et l'« indice du premier maximum » soient équidistribués.

On trouve dans ce tome, à la fois l'article *Nombres d'Euler et permutations alternantes* [1973-1] effectivement publié et le mémoire complet [1971-2], de 71 pages, portant le même nom. On y voit apparaître les polynômes d'André en variables non-commutatives, utilisés par la suite dans l'étude du cd-index des treillis, mais surtout exploités en tant que polynômes générateurs d'une classe de permutations dénombrées par les nombres tangents et sécants.

L'article *Le théorème de Lagrange selon G. N. Raney* [1971-5] reprend simplement la démonstration élémentaire qu'avait donnée Raney du théorème d'inversion de Lagrange dans le cadre naturel des langages formels et des mots de Lukasiewicz.

Les deux notes *Sur un théorème de G. de B. Robinson* [1971-3] et *Sur une construction de Gilbert de B. Robinson* [1973-3] constituent la genèse d'une longue étude sur l'algèbre des tableaux de Young. En fait, cette algèbre avait déjà été abordée dans l'article antérieur *Quelques remarques sur une construction de Schensted* [1963-6] (voir tome 5). Cependant, dans ces deux notes, on trouve déjà les propriétés de l'opération *évacuation* des tableaux, une opération qui s'avèrera fondamentale dans le traitement du monoïde plaxique (voir les articles suivants : *Evacuations* [1976-1] et *La correspondance de Robinson* [1977-4], tome 9).

La courte note *Quelques remarques sur une propriété d'équidistribution des permutations* [1975-4] contient essentiellement l'énoncé d'une conjecture, qui sera prouvée peu de temps après par Xavier Viennot [7].

L'article *A propos du relations rationnelles fonctionnelles* [1973-2] mérite un commentaire spécial. Tout d'abord, le titre contient une coquille mais surtout ne correspond pas au contenu qui est une contribution à la théorie des automates sur les mots infinis. Vraisemblablement, cet article, paru dans les actes du colloque *Automata, Languages and Programming* organisé à Paris, qui est le premier de la série des ICALP, ne correspond pas à la conférence prononcée à cette occasion, d'où le décalage. Le contenu est une construction algébrique (utilisant le produit de Schützenberger) permettant de donner une démonstration plus algébrique du théorème de McNaughton [5] (M.-P. Schützenberger parlait de la construction de McNaughton comme d'une « whistling machine »). Il s'agit

probablement d'un travail de préparation à la version donnée par Eilenberg pour le chapitre « Infinite behaviour of finite automata » du volume A de *Automata, Languages and Machines* paru en 1974.

La note *Une propriété des monoïdes libres* [1974-1] est l'annonce d'un résultat dont la preuve ne sera publiée que cinq ans plus tard ([1979-1]). Elle se termine par une question qui donnera lieu à des travaux de Césari et Vincent, puis de Duval pour devenir ce qui est maintenant connu comme le théorème du point critique et qui a été exposé par M.-P. Schützenberger dans un chapitre du livre *Combinatorics on Words* (voir [1983-2] dans le tome 11.

L'article *Sur les monoïdes finis dont les groupes sont commutatifs* [1974-2] donne deux caractérisations de la variété des ensembles dont le monoïde syntaxique ne contient que des groupes commutatifs. L'une des formulations utilise les codes à délai de synchronisation fini. La preuve utilise le théorème de Krohn-Rhodes. Ces résultats seront repris dans le livre de Lallement ([4], chapitre 7) ainsi que la généralisation aux monoïdes dont tous les groupes sont résolubles, obtenue par Straubing.

Cet article, ainsi que plusieurs autres de cette période, fut écrit pendant le séjour que Schützenberger fit à Naples en 1972–73. Il séjourna, à l'invitation d'Eduardo Caianiello, au Laboratorio di Cibernetica fondé après guerre par Norbert Wiener. Il y fit la connaissance d'Aldo de Luca et d'Antonio Restivo qui devinrent ses élèves.

L'article *Sur les relations rationnelles* [1975-2] contient une caractérisation des relations rationnelles qui ne sont pas une union finie de fonctions rationnelles. La preuve du résultat permet d'obtenir comme conséquence le fait qu'on peut décider si une relation rationnelle est une fonction (ce résultat sera obtenu indépendamment par Blattner et Head [2]).

Le résultat principal de *Sur certaines opérations de fermeture dans les langages rationnels* [1975-3] est une caractérisation des ensembles sans étoile qui n'utilise pas la complémentation mais en revanche une opération étoile restreinte aux codes à délai de synchronisation fini. Un énoncé voisin figure dans le volume B de *Automata, Languages and Machines* ([3], chapitre X). Une telle caractérisation est utile pour montrer l'équivalence entre la logique temporelle et la logique du premier ordre de l'ordre linéaire (voir [6]).

L'article *Sur un langage équivalent au langage de Dyck* [1973-4] est la dernière publication de M.-P. Schützenberger relative à la théorie des langages algébriques. L'objet de cet article est de montrer que le langage engendré par la grammaire $S \to aSSb + ab$ est équivalent au langage de Dyck sur deux paires de parenthèses. L'équivalence, appelée aussi équivalence rationnelle, signifie ici que les deux langages engendrent la même famille de langages au moyen de transductions rationnelles. Il en résulte facilement que le langage engendré par la grammaire $S \to aSbSc + d$ est également équivalent au langage de Dyck, mais Schützenberger montre que ce résultat vaut même si a, b, c et d sont des mots, pourvu que ces mots satisfassent des conditions assez peu restrictives.

Cet article inaugure toute une série de travaux, par divers auteurs, consacrés à la notion d'équivalence rationnelle, et sur d'autres langages équivalents au langage de Dyck). Le second générateur proposé dans l'article se révélera bien plus tard être un langage dont la place est remarquable dans la théorie des générateurs des langages algébriques, comme l'a montré Beauquier [1].

[1] Joffroy Beauquier. Générateurs algébriques et systèmes de paires itérantes. *Theoret. Comput. Sci.*, 8(3) :293–323, 1979.

[2] Meera Blattner and Tom Head. Single-valued a-transducers. *J. Comput. System Sci.*, 156(3) :310–327, 1977.

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

[4] Gérard Lallement. *Semigroups and Combinatorial Applications.* John Wiley & Sons, New York-Chichester-Brisbane, 1979. Pure and Applied Mathematics, A Wiley-Interscience Publication.

[5] Robert McNaughton. Testing and generating infinite sequences by a finite automaton. *Information and Control*, 9 :521–530, 1966.

[6] Dominique Perrin and Jean-Eric Pin. *Infinite Words, Automata, Semigroups, Logic and Games.* Elsevier, 2004.

[7] Xavier Viennot. Équidistribution des permutations ayant une forme donnée selon les avances et coavances. *J. Combinatorial Th. A*, 31 :43–55, 1981.

Année 1971

Bibliographie

[1] Dominique Foata and Marcel-Paul Schützenberger. On the principle of equivalence of Sparre Anderson. *Math. Scand.*, 28 :308–316 (1972), 1971.

[2] Dominique Foata and Marcel-Paul Schützenberger. Nombres d'Euler et permutations alternantes. Technical report, University of Florida, 1971. unabridged version, 71 pages.

[3] Marcel-Paul Schützenberger. Sur un théorème de G. de B. Robinson. *C. R. Acad. Sci. Paris Sér. A-B*, 272 :A420–A421, 1971.

[4] Marcel-Paul Schützenberger. Parties rationnelles d'un monoïde libre. In *Congrès International des Mathématiciens*, volume 3, pages 281–282. Gauthiers-Villars, Paris, 1971. Nice, septembre 1070.

[5] Marcel-Paul Schützenberger. Le théorème de Lagrange selon G. N. Raney. In *Séminaire IRIA, Automates et Langages*, pages 199–205. 1971.

[6] Marcel-Paul Schützenberger. On McNaughton's counter free languages. Technical report, Laboratorio di Cibernetica del C.N.R., Arco Felice, Napoli, 1971. 19 pages.

MATH. SCAND. 28 (1971), 308–316

ON THE PRINCIPLE OF EQUIVALENCE OF SPARRE ANDERSEN

D. FOATA and M. P. SCHÜTZENBERGER[1]

1. Introduction.

The present paper is concerned with the algebraic study of the so-called *equivalence principle* of Sparre Andersen [1] and of the theorem of Bohnenblust as presented by Farrell [3]. We recall the former in its simplest form and, letting X be a set of n distinct real numbers, we consider the set F' of the $n!$ sequences obtained when permuting the elements of X in all possible manners. To each sequence $f=(x_1,x_2,\ldots,x_n) \in F'$, $\{x_1,x_2,\ldots,x_n\}=X$, we associate the sequence of the $n+1$ partial sums

$$s_0 = 0,\ s_1 = x_1\,,$$
$$s_k = s_{k-1}+x_k \quad \text{for } k=2,\ldots,n\,,$$

and we use it to define the following two numbers:

$L(f)$ = the number of strictly positive terms in the sequence $(s_0,s_1,\ldots,s_n)$;

$\Pi(f)$ = the index of the first maximum among the terms of the same sequence, that is, $\Pi(f)=m$ iff $s_j<s_m$ for $j<m$ and $s_j \leqq s_m$ for $m \leqq j$, $m,j=0,1,\ldots,n$.

Thus for any permutation $f \in F'$, both $L(f)$ and $\Pi(f)$ are natural numbers at most equal to n. In general they are different but Sparre Andersen has discovered the surprising fact that their distributions over the $n!$ permutations of F' are identical. This is essentially the equivalence principle. One of the proofs is due to Richards (quoted by Baxter in [2]). It consists in constructing a bijective map ϱ of F' to itself that is such that $\Pi(\varrho f)=L(f)$ identically.

Bohnenblust's theorem is not so easy to state here but its proof in-

---

Received October 3, 1968.

[1] Research on this paper was supported by Contract No AF 61 (052)-945, U.S. Air Force.

volves a similar idea. In the present paper we give a common algebraic formulation of both theorems and proofs and we exhibit a large class of cases in which Richard's construction leads to a generalized "Equivalence Principle". For this purpose we use the terminology of free monoids. Given a set X we identify the finite sequences of (non necessarily distinct) elements of X with the elements (the "words") of the free monoid X^* generated by X. Then a subset F' of X^* such that it contains together with any of its members every word obtained by permuting its letters will be called an *abelian subset* of X^*.

With these notations, instead of starting with a set of real numbers, we consider an abstract set X, a fixed morphism σ of X^* into the additive group of R and we identify any word of length n, $f = x_1 x_2 \dots x_n \in X^*$, $x_1, x_2, \dots, x_n \in X$, and the sequence $(\sigma x_1, \sigma x_2, \dots, \sigma x_n)$ of R^n. The image by σ of the left factor f' of length m $f' = x_1 x_2 \dots x_m$, $0 \leqq m \leqq n$, of the word f is precisely the partial sum $\sigma x_1 + \sigma x_2 + \dots + \sigma x_m$. The empty word e is a factor of any word of X^* and $\sigma e = 0$ since σ is a morphism.

Thus if PP^* denotes the subsemigroup of X^* consisting of all $g \in X^*$ such that $\sigma g > 0$, we have that $L(f)$ is simply the *number of left factors of f that belong to PP^**.

Further, let A^* denote the set of all words f such that $\sigma f' < \sigma f$ for any proper (that is, $\neq f$) left factor f' of f. For the corresponding sequence of partial sums, this means that the maximum is reached at the last term.

It is clear that A^* is a submonoid of X^* and that every word f has one well defined left factor a of maximum length in A^* (possibly, it is the empty word e, corresponding to an empty sequence). The number Πf is precisely the length of a and we have now the terminology needed to state with greater generality the

EQUIVALENCE PRINCIPLE OF SPARRE ANDERSEN. *Let F', PP^* and A^* be as above. There exists a bijection $\varrho : F' \to F'$ such that $\Pi(\varrho f) = L(f)$ identically.*

The sets PP^* and A^* have been defined here with the help of the morphism σ. We shall see that this can be done for a larger class of objects. Interestingly enough, the submonoids A^* which we shall encounter appear also in a quite different context as special instances of "synchronising variable length codes" ([4], [6]).

2. *F*-partition and *F*-factorisation.

We consider a fixed set ("alphabet") X and the free monoid X^* generated by X. The empty word is noted e and $XX^* = X^* \setminus \{e\}$ is the

free semigroup generated by X. More generally, for any subset S of XX^*, S^* (resp. $SS^* = S^* \setminus \{e\}$) denotes the submonoid (resp. subsemigroup) of X^* generated by S. If M is a submonoid of X^*, the *basis* $(M \setminus \{e\}) \setminus (M \setminus \{e\})^2$ of M, is the least subset of XX^* that generates M.

We also consider a *fixed non empty abelian* subset F of XX^* having the property $(\mathscr{P})$:

($\mathscr{P}$) F contains every left and every right factor $\neq e$ of any of its members.

DEFINITION. 1. A pair (P^*, Q^*) of submonoids of X^* is an *F-partition* iff

$$F \subset P^* \cup Q^*, \quad \emptyset = F \cap P^* \cap Q^* .$$

DEFINITION 2. A pair (A^*, B^*) of submonoids of X^* is an *F-factorization* iff every word f of F has exactly one factorization $f = ab$ with $a \in A^*$, $b \in B^*$.

In this section we discuss the relationship between F-partition and F-factorization. The assumption $(\mathscr{P})$ is only introduced for convenience since we can always take the minimal abelian subset $\overline{F}$ satisfying $(\mathscr{P})$ and containing F. Then clearly any $\overline{F}$-partition ($\overline{F}$-factorization) is an F-partition (F-factorization). Furthermore all our statements have a trivial symmetric counterpart obtained by exchanging P^* and Q^*, A^* and B^* and left and right.

1. *Let (A^*, B^*) be an F-factorization. Then A^* satisfies the condition*

$$a \in A^*,\ f \in X^*,\ af \in A^* \cap F, \quad \textit{imply} \quad f \in A^* .$$

PROOF. Let a and f as above. If $f = e$, the conclusion $f \in A^*$ is trivially verified. If f is not the empty word, we have $f \in F$ since F contains every factor of its members. Since (A^*, B^*) is a F-factorization we have $f = a'b'$ with $a' \in A^*$, $b' \in B^*$.

Thus $af = a'' \in A^*$ and $af = aa'b'$. Because of the unicity of the factorization, this implies $b' = e$, that is $f = a' \in A^*$.

We call *right F-prefix* any submonoid of X^* that satisfies the condition stated in 1. and, we call *left F-prefix* any submonoid B^* that satisfies the symmetric condition $b \in B^*$, $f \in X^*$, $fb \in B^* \cap F$ imply $f \in B^*$.

This terminology comes from the fact that, for $F = XX^*$, the right F-prefix submonoids are precisely the prefix submonoids of the theory of variable length codes.

2. *Let A be the basis of a right F-prefix monoid A^*. Every $f \in F$ has exactly one factorization in the form $f = a_1 a_2 \dots a_m c$ with $m \geqq 0$; $a_1, a_2, \dots, a_m \in A$; $c \in X^* \setminus AX^*$.*

Proof. We proceed by induction on the largest $m \geqq 0$ such that $f \in A^m X^*$. If $m = 0$, there is nothing to prove. If $m > 0$, suppose $f = a_1 g = a_1' g'$ with $a_1, a_1' \in A$. One of a_1 and a_1' must be a left factor of the other, say $a_1 = a_1' h$, $h \in X^*$. We have $a_1 \in F$, and since A^* is right F-prefix, it follows that $h \in A^*$. By the hypothesis $a_1, a_1' \in A =$ the basis of A^*; this implies $h = e$ that is $a_1 = a_1'$.

3. *A* n.a.s.c. *that (A^*, B^*) be an F-factorization is that A^* and B^* be submonoids that satisfy the following three conditions*:
3.1. $\emptyset = A^* \cap B^* \cap F$;
3.2. *A^* is right F-prefix and B^* is left F-prefix*;
3.3. $F \subset A^* B^*$.

Proof. The necessity of these conditions follows from the definition for 3.1. and 3.3. and from 1. for 3.2. To prove that they are sufficient we have only to show that under 3.1., 3.2. and 3.3. any relation $ab = a'b' \in F$ $(a, a' \in A^*, b, b' \in B^*)$ implies $a = a'$, $b = b'$. Indeed, if $ab = a'b'$ the word a must be a left factor of a' or a' must be a left factor of a, say $a = a'h$ for instance. Then $b' = hb$. We have $h \in \{e\} \cup F$. Thus $h \in A^*$ since A^* is right F-prefix. Also $h \in B^*$ since B^* is left F-prefix. By 3.1. we conclude that $h = e$.

4. *Let (A^*, B^*) be an F-factorization. Then*:
4.1. *Every right factor of a word of $A^* \cap F$ is in A^**;
4.2. *Every proper left factor of a word of $A \cap F$ is in B^**;
4.3. $(B^m A^n) \cap F \subset A \cup A^2 \cup \dots \cup A^n \cup B \cup B^2 \cup \dots \cup B^m$, $0 \leqq n, m$.

Proof. Consider a word $a = fg \in A^* \cap F$. Clearly g is in A^* if either f or g is the empty word. If f and g are different from e, we have $f, g \in F$ hence $f = a'b'$, $g = a''b''$, $a', a'' \in A^*$, $b', b'' \in B^*$. Further $a'b'a'' \in F$, hence $a'b'a'' = a_1 b_1$, $a_1 \in A^*$, $b_1 \in B^*$. Thus we can write $a = ae \in A^* B^*$ and $a = a_1 b_1 b'' \in A^* B^*$. Because of the unicity of the factorization, this implies $b_1 b'' = e$, that is $g = a'' \in A^*$ and it proves 4.1. In similar fashion, we have $b'a''b'' = a_2 b_2 \in A^* B^*$, and from $a = ae = a' a_2 b_2$ we conclude that $b_2 = e$. Since $g \neq e$ and $b'' = e$, it implies $a'' \neq e$, hence $a_2 \neq e$ because of $b_2 = e$. Thus $a = a' a_2$ belongs to the basis A only if $a' = e$, that is, only if $f = b' \in B^*$ and 4.2. is proved since the empty left factor of a obviously belongs to B^*.

Now let $a \in A$, $b \in B$ be such that $ba \in F$. We have $ba = a_3 b_3$, $a_3 \in A^*$, $b_3 \in B^*$. By 4.1., either $b_3 = e$ or b_3 is *not* a right factor of a_3, that is, it admits a as a proper right factor. Symmetrically either $a_3 = e$ or it admits b as a proper left factor. Thus one of a_3 and b_3 must be the empty word e. Suppose for instance $b_3 = e$. We can write $a_3 = a'a''$ where $a' \in A$, $a'' \in A^*$. By the symmetric version of 4.1. and $ba = a_3 = a'a''$ we see that b must be a *proper* left factor of a', that is $a' = bh$, where $h \neq e$ and where $h \in A^*$ by 4.1. However $ba = bha''$ shows that $a = ha''$. Since $a \in A$, 4.2. asserts that $h \in B$ or $h = a$. Since the first case is excluded, we have $a = h$, hence $a'' = e$ and finally $ba = a' \in A$. This proves $BA \cap F \subset A \cup B$ and 4.3. follows by induction on m and n.

Recall that two words $g, g' \in X^*$ are *conjugate* iff one can find $h, h' \in X^*$ satisfying $g = hh'$; $g' = h'h$. Clearly conjugacy is an equivalence relation. It is in fact the restriction to X^* of the usual conjugacy relation in the free group generated by X.

5. *Let (A^*, B^*) be an F-factorization. A word $f \in F$ has a conjugate in A^* iff it has no conjugate in B^*.*

Proof. Let $f \in F$. We have $f = ab$, where $a \in A^*$, $b \in B^*$. By 4.3. the conjugate ba of f belongs to A^* or to B^*. Thus it suffices to show that none of the conjugates of a word $a \in A^* \cap F$ belongs to B^*. Indeed we can write $a = a_1 a_2 \dots a_m$, $m > 0$, $a_1, a_2, \dots, a_m \in A$, and any conjugate of a has the form $f' = h' a_{k+1} a_{k+2} \dots a_m a_1 a_2 \dots a_{k-1} h$, where $h' \neq e$ and $hh' = a_k \in A$. By 4.1. and 4.2. we know that $h' \in A^*$ and that $h \in BB^*$ unless $h = e$, in which case $f' \in A^*$. Thus $f' \in AA^*BB^* \neq B^*$.

We now relate F-factorization and F-partition. To this effect, given a submonoid M of X^*, we call *right* (resp. *left*) *associate* of M the set of all words in X^* such that any of their right (resp. left) factors belongs to M.

The reader can verify that the monoid A^* mentioned in the introduction is the right associate of the monoid $P^* = \{e\} \cup \{f \in X^* : 0 < \sigma f\}$.

6. *The right associate of a submonoid P^* is a right prefix monoid whose basis A is such that $X^* \setminus AX^*$ is contained in the submonoid $(X^* \setminus P^*)^*$ generated by $X^* \setminus P^*$.*

Proof. Let a and a' belong to the right associate of P^*. Any right factor of aa' is a right factor of a' or a product ha' where h is a right factor of a. Since P^* is a monoid this shows that its right associate A^*

is also a monoid. Further A^* is right prefix since by definition it satisfies the stronger condition that $f'f \in A^*$ implies $f \in A^*$ for any $f, f' \in X^*$. Finally if $f \in XX^* \setminus AX^*$, it does not belong to A^*. Thus it has a right factor $f'' \neq e$ which belongs to $X^* \setminus P^*$ and letting $f = f'f''$ we have also $f' \in X^* \setminus AX^*$. Induction on the length of f completes the proof.

7. *A n.a.s.c. that (A^*, B^*) be an F-factorization is that there exists an F-partition (P^*, Q^*) such that $F \cap A^*$ and $F \cap B^*$ coincide respectively with the intersections with F of the right associate of P^* and of the left associate of Q^*.*

Proof. Let (A^*, B^*) be an F-factorization; we set $P^* =$ the submonoid generated by $X^* \setminus B^*$ and $Q^* = B^*$.

We have $F \subset P^* \cup Q^*$. Let f belong to $F \cap P^*$. By the definition of P^* we have $f = f_1 f_2 \dots f_m$ where $m > 0$ and $f_1, f_2, \dots, f_m \in F \setminus B^*$. Since (A^*, B^*) is an F-factorization we have $f_1 = ab$ with $a \in AA^*$ and $b \in B^*$. Thus $f \in aA^*B^*$ and accordingly $f \notin B^*$. This proves that $\emptyset = F \cap P^* \cap Q^*$ and consequently that (P^*, Q^*) is an F-partition.

The fact that $B^* \cap F$ is the intersection of F with the left associate of $Q^* (= B^*)$ follows from the symmetric version of 4.1.

By 4.1. and $A^* \cap F \subset P^*$, $A^* \cap F$ is contained in the right associate of P^*. Finally let $f \in F$ belong to the right associate of P^*. We have $f \notin A^*BB^*$ since every word of A^*BB^* has a right factor in B^* and since $B^* \cap F \subset F \setminus P^*$. Thus $f \in A^*$ since $f \setminus A^*BB^* \subset A^*$ and the necessity of the condition is proved.

Reciprocally let (P^*, Q^*) be an F-partition and let A and B be the basis of the associated monoids. We show that (A^*, B^*) satisfies the conditions of 3.

First $F \cap A^* \cap B^* \subset F \cap P^* \cap Q^*$. Since this last intersection is empty this gives 3.1. Condition 3.2 follows from 6. and its symmetric. Thus to verify 3.3 it suffices by induction on the length to consider a word f satisfying the condition $f \in F \setminus AX^*$ and to show that it belongs to B^*. Indeed, the condition $f \notin AX^*$ implies $f' \notin AX^*$ for any left factor f' of f. Thus, by 6., f and any of its left factors belong to $(X^* \setminus P^*)^*$. Since $F \setminus P^* \subset Q^*$ because (P^*, Q^*) is an F-partition, we see that f and any of its left factors belong to Q^*, that is, that $f \in B^*$ by definition.

3. Richards' construction.

We keep the same notations and the same set F. We let (P^*, Q^*) be a fixed F-partition and (A^*, B^*) be the associated F-factorization.

We introduce the restrictive assumption that $P^* \cap F$ (hence $Q^* \cap F$)

are abelian sets. (Counter examples show that Richards' map ϱ is not always bijective without this hypothesis.)

DEFINITION 3. Let the map ϱ of $\{e\}\cup F$ to itself be defined by induction on the length by:

$$\varrho e = e \text{ and for } f = f'x \in F,\ x \in X\ ,$$
$$\varrho f = x\varrho f' \text{ or } = (\varrho f')x \text{ depending upon } f \in P^* \text{ or } f \in Q^*\ .$$

8. *The map ϱ is a bijection.*

PROOF. It is clear that ϱf is a word obtained by permutation of the letters of f. Thus by our assumption that $P^*\cap F$ is abelian, f and ϱf always belong to the same monoid P^* or Q^*.

Assume the result proved for every word shorter than $f \in F$. If $\varrho f = g \in P^*$, we know that $f \in P^*$ and there exists one and only one pair $(x,f') \in X \times X^*$ such that $g = xg'$, $g' = \varrho f'$ and $f = f'x$. In similar fashion, if $\varrho f = g \in Q^*$ we have $f = f'x$ with $\varrho f'x = g$ in a unique manner.

9. *For any $f \in F$, the number $L(f)$ of left factors in PP^* of f is equal to the length $\Pi(\varrho f)$ of a in the factorization $g = ab$, $a \in A^*$, $b \in B^*$, of $g = \varrho f$.*

PROOF. The result is true for $f \in F\cap X$ and we can suppose that it is proved for any word shorter than f.

Let f_1 be the left factor of maximal length of f that belongs to Q^* or to P^* depending upon $f \in P^*$ or $f \in Q^*$. If $f = f_1 h$, it is a straightforward consequence of the definition of ϱ that $\varrho f = \bar{h}\varrho f_1$ for $f \in P^*$ and $\varrho f = \varrho f_1 h$ for $f \in Q^*$, where $\bar{h} = x_m x_{m-1} \dots x_1$ if $h = x_1 x_2 \dots x_m$, $m > 0$, $x_1, x_2, \dots, x_m \in X$. Further any left factor $h' \neq e$ of h belongs to the same monoid P^* or Q^* as f does. Thus by our definition of A^* and B^* as the associated monoids of P^* and Q^*, we have $\bar{h} \in A^*$ (resp. $h \in B^*$) for $f \in P^*$ (resp. $\in Q^*$). Now letting λh be the length of h and recalling 4, we have

$$\begin{aligned} L(f) &= L(f_1)+\lambda h \text{ and } \Pi(\varrho f) = \lambda h + \Pi(\varrho f_1) && \text{for } f \in P^*\ , \\ L(f) &= L(f_1),\ \Pi(\varrho f) = \Pi(\varrho f_1) && \text{for } f \in Q^*\ , \end{aligned}$$

4. Concluding remarks.

This completes our proof of the generalized equivalence principle. For F consisting of the words in which each letter of X appears at most once, the reader will recognize in $P^*\cap F$ the set $\varepsilon^{-1}0$ of Bohnenblust and Farrell, for a function ε taking only values 0 or 1. The general case

follows since one can always represent the "set function" ε used by these authors as finite sums $\varepsilon = \sum r_i \varepsilon_i$ where r_i is real and the range of the set function ε_i is the set $\{0,1\}$ for all i.

For this reason it would be quite interesting to be able to give explicitly all the abelian F-partitions of an arbitrary abelian subset F containing the factors of its members. We limit ourselves here to the case of $F = XX^*$, that is to the case where Richards' construction gives the validity of the equivalence principle for *any* abelian subset of X^*. To simplify notations we suppose $\mathrm{Card}\, X = k$ finite and we recall Hahn's Theorem [5].

THEOREM. *Let M be a submonoid of R^k and $\leq$ a total preorder on M. There exists a morphism $\nu\colon \mathsf{R}^k \to \mathsf{R}^k$ and a lexicographic order $\leq$ on R^k such that for $m, m' \in M$ one has $m \leq m'$ iff $\nu m \leq \nu m'$.*

We prove

10. *A* n.a.s.c. *that (P^*, Q^*) be an abelian XX^*-partition is that there exists a morphism μ of X^* into the additive group R^k and a lexicographic order $\leq$ on R^k such that $P^* = \{f \in X^* : 0 \leq f\}$; $QQ^* = \{f \in X^* : \mu f < 0\}$.*

PROOF. The condition is sufficient. Any lexicographic order $\leq$ on R^k is compatible with the additive group structure (that is, $r \leq r'$ implies $r + r'' \leq r' + r''$, identically for r, r', $r'' \in \mathsf{R}^k$). Thus in particular $\{r \in \mathsf{R}^k : 0 \leq r\}$ $(= R_1)$ and $\{r \in \mathsf{R}^k : r < 0\}$ $(= R_2)$ are respectively a submonoid and a subsemigroup. These two sets are disjoint and, since $\leq$ is a total order, their union is R^k. It follows that $P^* = \mu^{-1} R_1$ and $Q^* = \mu^{-1} R_2$ satisfy $P^* \cap Q^* = \{e\}$ and $P^* \cup Q^* = X^*$. Finally, P^* and Q^* are abelian subsets since they are inverse images by a morphism μ into a commutative monoid.

The condition is necessary. Let α be the canonical homomorphism of X^* onto the free *abelian* monoid X^+ generated by X and suppose that the abelian submonoids P^* and Q^* give an XX^*-partition. Then αP^* and αQ^* are submonoids of X^+ such that $\alpha P^* \cup \alpha Q^* = X^+$ and $\alpha P^* \cap \alpha Q^* = \{0\}$. Thus we are left to show that there exists a morphism $\theta\colon X^+ \to \mathsf{R}^k$ and a lexicographic order $\leq$ on R^k such that $\alpha P^* = \{a \in X^+ : 0 \leq \theta a\}$ and $\alpha Q^* \setminus \{0\} = \{a \in X^+ : \theta a < 0\}$. First we define a binary relation $\leq$ on X^+ by letting $a \leq a'$ iff for any $b \in X^+$, $a + b \in \alpha P^*$ implies $a' + b \in \alpha P^*$. Clearly $\leq$ is a preorder and we can then find a morphism $\theta\colon X^+ \to \mathsf{R}^k$ and a preorder $\leq$ on R^k such that $a \leq a'$ iff $\theta a \leq \theta a'$ in R^k.

Now we have $\alpha P^* = \{a \in X^+ : 0 \leq a\}$ since on one hand, $0 \leq a$ and

$0 \in \alpha P^*$ imply $a+0 \in \alpha P^*$ proving $\{a \in X^+ : 0 \leq a\} \subset \alpha P^*$ and on the other hand, for any $c \in \alpha P^*$ we have $0 \leq c$ because $0+b \in \alpha P^*$ implies $b \in \alpha P^*$ and $c+b \in \alpha P^*$. Thus we can write $\alpha P^* = \{a \in X^+ : 0 \leq \theta a\}$ and we have only to show that the preorder $\leq$ (on X^+, hence on R^k) is total. Again this is equivalent with the statement that for $a, a' \in X^+$, not $a \leq a'$ implies $a' \leq a$ that is $a+b \in \alpha P^*$ for any b such that $a'+b \in \alpha P^*$. Suppose not $a \leq a'$ and $a'+b \in \alpha P^*$. The first relation entails the existence of at least one $c \in X^+$ such that $a+c \in \alpha P^*$ and $a'+c \notin \alpha P^*$. Thus $a'+b+a+c \in \alpha P^*$. Since $a'+c \notin \alpha P^*$ implies $a'+c \in \alpha Q^* \setminus \{0\}$ and since αQ^* is a submonoid we cannot have $a+b \in \alpha Q^*$ because it would give $a'+b+a+c \in \alpha Q^* \setminus \{0\}$ in contradiction with $a'+b+a+c \in \alpha P^*$ and the relation $\alpha P^* \cap \alpha Q^* = \{0\}$.

REFERENCES

1. E. Sparre Andersen, *The equivalence principle in the theory of fluctuations of sums of random variables*, Colloquium on Combinatorial Methods in Probability Theory, [August 1962], Aarhus Universitet, Matematisk Institut, 13–16.
2. G. Baxter, *Notes for a seminar in stochastic processes*, Department of Mathematics, University of Minnesota, 1957.
3. R. H. Farrell, *Notes on a combinatorial theorem of Bohnenblust*, Duke Math. J. 32 (1965), 333–339.
4. S. W. Golomb and B. Gordon, *Codes with bounded synchronization delay*, Information and Control 8 (1965), 355–372.
5. H. Hahn, *Über die nichtarchimedischen Grössensysteme*, S. B. Akad. Wiss. Wien IIa 116 (1907), 601–655.
6. M. P. Schützenberger, *Sur une question concernant certains sous-monoïdes libres*, C. R. Acad. Sci. Paris 261 (1965), 2414–2420.

DÉPARTEMENT DE MATHÉMATIQUES, UNIVERSITÉ DE MONTRÉAL, CANADA

ET

INSTITUT DE RECHERCHE MATHÉMATIQUE AVANCÉE, UNIVERSITÉ DE STRASBOURG, FRANCE

FACULTÉ DES SCIENCES, UNIVERSITÉ DE PARIS, FRANCE

Nombres d'Euler
et permutations alternantes

par D. Foata
University of Florida
et M.-P. Schützenberger
Université de Paris VII

DEPARTMENT
of
MATHEMATICS

UNIVERSITY OF FLORIDA

(Gainesville, Florida)

Nombres d'Euler et permutations alternantes

par D. Foata
University of Florida
et M.-P. Schützenberger
Université de Paris VII

University of Florida, Gainesville
November 15, 1971.

Nombres d'Euler et permutations alternantes

par D. Foata
University of Florida

et M.-P. Schützenberger
Université de Paris VII

TABLE DES MATIÈRES

1. INTRODUCTION.

Les nombres d'Euler définis par le développement en série de tg u

$$\operatorname{tg} u = (u/1!)\ 1 + (u^3/3!)\ 2 + (u^5/5!)\ 16 + (u^7/7!)\ 272 + (u^9/9!)\ 7936 + \ldots$$

et les nombres sécants définis par celui de 1/cos u

$$1/\cos u = 1 + (u^2/2!)\ 1 + (u^4/4!)\ 5 + (u^6/6!)\ 61 + (u^8/8!)\ 1385 + \ldots$$

ont fait l'objet de très nombreuses recherches mathématiques dont un exposé d'ensemble a été donné par Niels Nielsen dans son "Traité élémentaire des nombres de Bernoulli" (1923).

En effet, le nombre d'Euler (noté ici D_{2n}) qui est le coefficient de $u^{2n-1}/(2n-1)!$ dans le développement de tg u est égal à $2^{2n-1}\ (2^{2n} - 1)\ n^{-1}\ B_n$ où

$$B_n = 2\ \zeta(2n)\ (2n)!\ /\ (2\pi)^{2n}$$

est le nombre de Bernoulli correspondant. D'autre part, les nombres sécants (dits aussi parfois nombres d'Euler et notés ici D_{2n+1}) sont reliés aux précédents par la formule remarquable

(1) $$\operatorname{Exp} D = D'' = (1/2)\ (1 + D'^2)$$

où la fonction D de u , donnée par la série

$D = \sum_{1 \leq n} (u^n/n!)\, D_n$ est définie par

$$D = \int_0^u (\mathrm{tg}\, u + 1/\cos u)\, du$$

$$= u + (u^2/2!) + (u^3/3!) + (u^4/4!)2 + (u^5/5!)5 + \ldots$$

et où $D' = (\partial/\partial u)\, D = (1 + \mathrm{tg}\, u/2) / (1 - \mathrm{tg}\, u/2)$,

$D'' = (\partial/\partial u)\, D'$.

Ainsi qu'on le verra plus loin, la formule (1) entraîne les identités

(2) $\quad \mathrm{Exp}\, D_{(2)} = D_{(1)}'$;

(3) $\quad D_{n+3} = \sum_{0 \leq i \leq n} \begin{bmatrix} n \\ i \end{bmatrix} D_{i+1}\, D_{n+2-i}$;

(4) $\quad 2\, D_{n+2} = \sum_{0 \leq i \leq n} \begin{bmatrix} n \\ i \end{bmatrix} D_{i+1}\, D_{n-i+1}$;

(5) $\quad D_{2n+1} = \sum_{0 \leq i \leq n-1} \begin{bmatrix} 2n-1 \\ 2i \end{bmatrix} D_{2i+1}\, D_{2n-2i}$;

où, dans la première, l'on a posé

$$D_{(2)} = \sum_{1 \leq n} (u^{2n}/(2n)!)\, D_{2n} \quad \left(= \int_0^u \mathrm{tg}\, u\, du \right)$$

et

$$D_{(1)} = \sum_{0 \leq n} (u^{2n+1}/(2n+1)!)\, D_{2n+1} = D - D_{(2)} .$$

A leur tour, ces identités fournissent les congruences élémentaires suivantes valables pour tout nombre premier

impair p

(6) $D_{p+3} \equiv D_{p+2} + D_{p+1}$;

(7) $D_{p+2} \equiv D_{p+1} \equiv D_p + 1$.

Enfin, Désiré André (1879, 1881) a montré que D_{n+1} est le nombre des <u>permutations alternantes</u> sur $[n]$, c'est-à-dire des permutations $x_1 x_2 \ldots x_n$ des éléments de $[n] = \{1,2, \ldots, n\}$ telles que x_{2j} soit à la fois inférieur à x_{2j-1} et à x_{2j+1} pour tout entier j tel que $0 < 2j < n$ et, en plus, si n est pair, telles que $x_n < x_{n-1}$.

Dans le présent travail, nous nous proposons de montrer que les formules précédentes restent vraies pour une famille $(D_n(s,t))_{n \geq 0}$ de polynômes à deux variables s , t et qui se réduisent aux entiers D_n pour $s = t = 1$. Comme le nom d'Euler n'a jusqu'ici été associé qu'à des problèmes autrement prestigieux (ceci dit, sans vouloir offenser la modestie de notre Maître Bose), nous appellerons les $D_n(s,t)$ <u>polynômes d'André</u>.

Dans le chapitre 2 suivant, nous établissons l'analogue des formules (1) à (7) pour les polynômes d'André $D_n(s,t)$ en variables <u>commutatives</u>. De plus, une formule explicite pour leur fonction génératrice exponentielle est donnée, ainsi qu'une relation entre ces polynômes et les

polynômes eulériens. Ce chapitre est de nature analytique et ne contient aucune considération géométrique.

En revanche, dans les chapitres ultérieurs 3, 4 et 5, nous étudions une version non commutative des polynômes d'André et là, il est naturel de faire apparaître ces nouveaux polynômes, en les variables non commutatives s et t, comme des polynômes générateurs d'une certaine fonction U sur une famille de permutations. Ceci nous permet de donner une contre-partie purement ensembliste aux formules qui viennent d'être rappelées. Ce mémoire est destiné dans notre esprit à préparer une analyse des propriétés arithmétiques des nombres D_n.

Le contenu des trois derniers chapitres est le suivant. Le chapitre 3 contient la définition d'une classe de permutations, appelées permutations d'André. Lorsque f est une telle permutation, on lui associe un mot fU en les lettres (non commutatives) s et t. Ce mot fU, appelé variation réduite de f, sert à repérer la position des montées ($jf<(j+1)f$) et des descentes ($jf>(j+1)f$) de f. Soit A_n l'ensemble des permutations d'André sur $[n]$; le polynôme $A_nU = \sum \{fU : f \in A_n\}$ est précisément une version non commutative de $D_n(s,t)$ et est appelé n-ème polynôme d'André non commutatif. On établit enfin l'analogue de la

formule (3) pour les polynômes $A_n U$.

Pour tout mot $w = u_1 u_2 \ldots u_k$ du monoïde $\{s,t\}^*$, on note $\tilde{w}$ le mot retourné $w = u_k u_{k-1} \ldots u_1$. D'autre part, on désigne par $c_n(w)$ le nombre de permutations f dans A_n telles que $Uf = w$. Le polynôme d'André $A_n U$ peut s'écrire

$$A_n U = \sum \{ w\, c_n(w) : w \in \{s,t\}^* \} \quad .$$

On a alors la propriété de symétrie suivante

$$c_n(\tilde{w}) = c_n(w) \quad .$$

En d'autres termes, si dans l'expression du polynôme $A_n U$ on retourne tous les mots w , le polynôme $A_n U$ ne change pas. De cette propriété remarquable, on déduit l'équivalent non commutatif de la formule (4) pour les polynômes $A_n U$. En fait, les permutations d'André se prêtent mal à la démonstration de cette propriété de symétrie. On est ainsi amené, dans ce chapitre 4 , à définir la notion de complexe d'André et à établir une bijection canonique entre deux complexes d'André. L'ensemble des permutations d'André est un tel complexe. Un autre exemple est fourni par l'ensemble des permutations d'André dites de seconde espèce définies dans la section 4.3 . Soit B_n la classe des permutations d'André de seconde espèce sur $[n]$ $(n \geq 0)$. Dans la section 4.4 , on établit une bijection ρ de B_n sur

lui-même telle que si f est dans B_n, de variation réduite $fU = w$, alors $f\rho U = \tilde{w}$.

Le chapitre 5 contient deux autres exemples de complexes d'André, la classe des arborescences binaires décroissantes et enfin celle des permutations alternantes. La correspondance entre arborescences binaires décroissantes et les permutations d'André des deux espèces peut être obtenue par un argument géométrique simple. Enfin, quelques tables numériques terminent cet article.

Comme il est rare dans un tel domaine qu'un résultat soit radicalement nouveau, puisque toute formule peut et doit être vue comme cas particulier d'une autre plus générale, ou banale extension d'une autre déjà classique, nous ne prétendons à aucun mérite, sauf de cohérence. En fait, les polynômes d'André (commutatifs) ont été déjà rencontrés sous une forme un peu différente par Kermack et McKendrick (1938) comme nous l'a obligeamment signalé John Riordan. Le problème traité était celui de la distribution du nombre des creux $((j-1)f > jf < (j+1)f)$ et des pics $((j-1)f < jf > (j+1)f)$ pour une substitution f de l'ensemble $[n]$. Sous cet aspect, il figure dans l'ouvrage de David et Barton (1962). Il est clair que la plupart de nos énoncés

pourraient aussi bien être présentés dans le langage statistique qui fut celui d'une grande partie de notre carrière. Notre choix d'une formulation moins spéciale est un hommage à notre Maître Bose dont l'oeuvre a tant illustré les enrichissements mutuels de la Mathématique et de ses applications.

2. LES POLYNÔMES D'ANDRÉ.

1. Définition et propriétés élémentaires.

Soit f une fonction réelle de la variable u, analytique à l'origine et satisfaisant l'équation différentielle

(2.1) $f'' = t \operatorname{Exp} f$

avec les conditions initiales

(2.2) $0 = f(0)$, $s = f'(0)$,

où s et t sont des constantes. En raison de $0 = f(0)$, la relation (2.1) est équivalente à

(2.3) $f''' = f' f''$.

Nous posons

$$f = \sum_{0 \leqslant n} (u^n/n!) f_n$$

où, d'après (2.2) $f_0 = 0$, $f_1 = s$, $f_2 = t$.
Considérant s et t comme des paramètres, les relations (2.1) et (2.3) déterminent de façon univoque par récurrence sur n les f_n comme polynômes en s et t. Ce sont eux que nous appellerons polynômes d'André et que nous désignerons, dans ce chapitre, par D_n $(n \geqslant 0)$. La liste des premiers d'entre eux est la suivante :

$$D_0 = 0 \; ; \; D_1 = s \; ; \; D_2 = t \; ; \; D_3 = st \; ;$$
$$D_4 = s^2t + t^2 \; ; \; D_5 = s^3t + 4\,st^2 \; ;$$
$$D_6 = s^4t + 11\,s^2t^2 + 4\,t^3 \; ; \; D_7 = s^5t + 26\,s^3t^2 + 34\,st^3 \; .$$

Les valeurs $D_n(1,1)$ sont entières et sont bien les coefficients de la fonction $D(u)$ présentée dans l'introduction puisque celle-ci était définie par l'équation différentielle

$$D'' = \mathrm{Exp}\, D$$

avec les valeurs initiales

$$D(0) = 0 \ , \ D'(0) = 1 \ (= s)$$

et que l'on avait donc

$$D''(0) = \mathrm{Exp}\, 0 = 1 \ (= t) \ .$$

Soit maintenant l'opérateur

$$\Delta = st\,(\partial/\partial t) + t\,(\partial/\partial s) \ .$$

On a

$$\Delta D_1 = t = D_2 \quad \text{et} \quad \Delta D_2 = st = D_3 \ .$$

Observant que (2.3) équivaut à l'identité binomiale

$$(2.4) \qquad D_{n+3} = \sum_{0 \le j \le n} \begin{bmatrix} n \\ j \end{bmatrix} D_{j+1}\, D_{n+2-j} \qquad (n \geqslant 0) \ ,$$

on en conclut que

$$(2.5) \qquad D_{n+1} = \Delta D_n \qquad (n \geqslant 1) \ ,$$

soit encore, en tenant compte de la valeur initiale $D_1 = s$,

$$(2.6) \qquad s + \Delta D = (\partial/\partial u)\, D \ .$$

Ces relations montrent que les polynômes d'André ont les propriétés élémentaires suivantes.

- 11 -

PROPRIÉTÉ 2.1. Les polynômes D_n sont homogènes de degré total n en les variables s et $\sqrt{t}$. Ils sont divisibles par t pour $n \geqslant 2$ et leurs coefficients sont des entiers positifs.

Faisons maintenant le changement de variable $\bar{t} = ts^{-2}$, $\bar{u} = us$ et posons $\bar{D}_n = D(s,\bar{t})\, u^n$. L'opérateur Δ devient

$$s^2\bar{t}\,(\partial/\partial s) + s\bar{t}\,(1 - 2\bar{t})\,(\partial/\partial t) + stu\,(\partial/\partial\bar{u})$$

et $(\partial/\partial u) = s\,(\partial/\partial\bar{u})$. Comme $(\partial/\partial s)\,\bar{D}_n = 0$, par raison d'homogénéité la relation (2.5) mise sous la forme

$$(\partial/\partial u)\,(u^{n+1}/(n+1)!)\,D_{n+1} = \Delta\,(u^n/n!)\,D_n$$

devient après simplification

$$\bar{D}_{n+1} = \bar{u}\,(\bar{t}\,\bar{u}\,(\partial/\partial\bar{u}) + \bar{t}\,(1-2\bar{t})(\partial/\partial\bar{t})\,\bar{D}_n\,. \tag{2.7}$$

Introduction les coefficients $d_{n,k} \in \mathbb{N}$ par

$$D_n = \sum_{0\leqslant k\leqslant n/2} s^{n-2k}\, t^k\, d_{n,k}\,,$$

la relation (2.5) donne les formules de récurrence indiqué dans la propriété suivante.

PROPRIÉTÉ 2.2. Pour $n \geqslant 2$, on a $d_{n,1} = 1$ et pour $k \geqslant 2$, $n \geqslant 2k$, on a

$$d_{n+1,k} = k\, d_{n,k} + (n+2-2k)\, d_{n,k-1}\,. \tag{2.8}$$

Tous les coefficients des D_n sont donc positifs et D_n est divisible par s pour n impair.

2. Une relation différentielle.

Nous établissons maintenant la généralisation naturelle de la deuxième égalité dans la relation (1).

PROPRIÉTÉ 2.3. On a l'identité

(2.9) $$2\,D'' = 2t - s^2 + D'^2 .$$

PREUVE. D'après (2.4) et (2.5), on a pour tout $n \in \mathbb{N}$

$$D_{n+3} = \Delta D_{n+2} = \sum_{0 \leq j \leq n} \begin{bmatrix} n \\ j \end{bmatrix} (\Delta D_j)\, D_{n+2-j} .$$

Tenant compte de la symétrie des indices et de $\begin{bmatrix} n \\ j \end{bmatrix} = \begin{bmatrix} n \\ n-j \end{bmatrix}$, ceci donne

$$2\,\Delta D_{n+2} = \sum_{0 \leq j \leq n} \begin{bmatrix} n \\ j \end{bmatrix} \Delta(D_{j+1}\, D_{n+1-j})$$

d'où

(2.10) $$2\,D_{n+2} = \sum_{0 \leq j \leq n} \begin{bmatrix} n \\ j \end{bmatrix} D_{j+1}\, D_{n+1-j} + K_n$$

où K_n est une fonction de s et t telle que $\Delta K_n = 0$. Comme les D_j sont des polynômes, K_n est un polynôme. D'autre part, comme

$$\Delta(t^p s^q) = p\, t^p s^{q+1} + q\, t^{p+1} s^{q-1} \qquad (p, q \in \mathbb{N}),$$

on voit que le terme de plus bas degré de K_n en t ne peut s'annuler que si ce degré est zéro. Comme, d'après la propriété 2.1 on a $D_{n+2}(s,0) = 0$ pout tout $n \geq 0$, le

polynôme K_n est nul pour $n \geqslant 1$. Enfin, on vérifie directement que $K_0 = 2t-s^2$. Ceci fait, la formule (2.9) s'obtient par sommation. ∎

On notera que pour $n+2 = 2m+1$ impair; l'expression (2.10) , avec $K_n = 0$, est symétrique et peut par conséquent s'écrire sous la forme (5) de l'introduction, soit de façon équivalente

$$D_{2m+1}/(2m-1)! = \sum_{0 \leq j \leq m-1} (D_{2j+1}/(2j)!)\ (D_{2m-2j}/(2m-2j-1)!)$$

c'est-à-dire

(2.11) $$D_{(1)}'' = D_{(1)}'\ D_{(2)}'$$

avec les notations déjà introduites dans le cas particulier de $s = t = 1$,

$$D_{(2)} = \sum_{0 \leq m} (u^{2m}/(2m)!)\ D_{2m}(s,t) \quad ,$$

$$D_{(1)} = D - D_{(2)} \quad .$$

Nous en déduisons la formule suivante qui est la contre-partie polynomiale de (2) .

PROPRIÉTÉ 2.4. On a

(2.12) $$D_{(1)}' = s\ \mathrm{Exp}\ D_{(2)} \quad .$$

PREUVE. La formule (2.11) peut s'écrire

$$(\partial/\partial u)\ \mathrm{Log}\ D_{(1)}' = (\partial/\partial u)\ D_{(2)}' \quad .$$

D'où

$$D_{(1)}' = K(s,t)\ \mathrm{Exp}\ D_{(2)}$$

où $K(s,t)$ est une fonction de s et t qui est déterminée en faisant $u = 0$ et en constatant que $D_2(u=0) = 0$ et $D_{(1)}'(u=0) = s$. ∎

3. Fonction génératrice des polynômes d'André.

Nous donnons maintenant des formules explicites pour D , D' et D'' .

PROPRIÉTÉ 2.5. Posant $r = (s^2-2t)^{1/2}$, $w = (s-r)/(s+r)$ et $E = \mathrm{Exp}\ ru$, on a les formules

$$D = ru + 2\ \mathrm{Log}\ (\ (1-w)/(1-wE)\ ) \quad ; \tag{2.13}$$

$$D' = r\ (1+wE)/(1-wE) \quad ; \tag{2.14}$$

$$D'' = wr^2E/(1-wE)^2 \quad . \tag{2.15}$$

PREUVE. L'équation (2.9) peut s'écrire

$$r = D''\ (\ (D'-r)^{-1} - (D'+r)^{-1}\ )\ ,$$

d'où par intégration

$$ru = \mathrm{Log}\ (\ (D'-r)/(D'+r)\ ) + K(s,t)$$

où la fonction $K(s,t)$ est déterminée en faisant $u = 0$ et se trouve par conséquent égale à $-\mathrm{Log}\ w$. Donc $(D'-r)/(D'+r) = w\ \mathrm{Exp}\ ru$, ce qui est équivalent à (2.14) . Maintenant le membre de droite de cette dernière équation peut s'écrire sous la forme

r (1 + (2w Exp ru)/(1-w Exp ru)) ,

d'où par une nouvelle intégration

D = ru - 2 Log(1 - w Exp ru) + K(s,t) .

Faisant de nouveau u = 0 , on trouve

K(s,t) = 2 Log(1-w) .

On obtient ainsi la formule (2.13) . Enfin, la formule (2.15) s'obtient par simple dérivation. ∎

Désignons par $D_{(0)}'$ la valeur du membre de droite de (2.14) pour s = 0 . Posant $v = \sqrt{2t}\,u$ et observant que w = -1 pour s = 0 on trouve

$$(2.16) \qquad D_{(0)}' = \sqrt{2t}\,.\,\sqrt{-1}\;(1 - \mathrm{Exp}\, v\sqrt{-1})/(1 + \mathrm{Exp}\, v\sqrt{-1})$$

soit

$$(2.16) \qquad D_{(0)}' = \sqrt{2t}\;\mathrm{tg}(v/2) .$$

Ce résultat a la conséquence très remarquable suivante.

PROPRIÉTÉ 2.6. Pour tout k positif, les coefficients $d_{2k-1,k-1}$ et $d_{2k,k}$ sont égaux à $2^{1-k}[D_{2k}]_{s=t=1}$, c'est-à-dire à 2^{1-k} fois le k-ème nombre d'Euler.

PREUVE. Prenant n = 2k-1 , la récurrence (2.8) donne

$$d_{2k,k} = k\, d_{n,k} + (2k-1+2-2k)\, d_{n,k-1} = d_{2k-1,k-1}$$

puisque $d_{n,k} = 0$ en vertu de $n < 2k$. Les deux coefficients d mentionnés dans l'énoncé sont donc égaux.

Maintenant pour vérifier leur égalité avec le nombre $[D_{2k}]_{s=t=1}$, il suffit d'observer que pour $s = 0$, tous les polynômes D_{2k-1} sont nuls et chacun des polynômes D_{2k} se réduit à $d_{2k,k}\, t^k$. Par conséquent

$$D_{(0)}' = \sum_{1 \leqslant k} (u^{2k-1}/(2k-1)!)\, d_{2k,k}\, t^k \ .$$

On peut alors appliquer la formule (2.16) qui s'écrit

$$D_{(0)}' = \sqrt{2t}\ \sum_{1 \leqslant k} (u^{2k-1}/(2k-1)!)\ (t/2)^{(2k-1)/2}\ D_{2k}$$

soit

$$D_{(0)}' = \sum_{1 \leqslant k} (u^{2k-1}/(2k-1)!)\ 2^{1-k}\ D_{2k}\ t^k \ .$$

Nous donnons enfin la formule binomiale

$$2\, d_{2n+2,n+1} = \sum_{0 \leqslant i \leqslant n-1} \begin{bmatrix} 2n \\ 2i+1 \end{bmatrix} d_{2i+1,i+1}\ d_{2n-2i,n-i} \qquad (n \geqslant 1) \tag{2.17}$$

qui se déduit immédiatement de la formule (2.9) lorsqu'on y fait $s = 0$ et $t = 1$, grâce à la propriété 2.6 .

4. Relations avec les polynômes eulériens.

Nous terminons ce chapitre en établissant une relation entre les polynômes d'André et les polynômes eulériens. Pour la définition de ces derniers, nous renvoyons le lecteur à notre précédent mémoire (Foata,Schützenberger (1970)).

PROPRIÉTÉ 2.7. Pour tout entier $n>0$ le n-ème polynôme eulérien $A_n(x)$ est égal à

$$\sum_{1\leq k\leq (n+1)/2} d_{n+1,k}\,(2x)^{k-1}\,(1+x)^{n+1-2k}$$

où les $d_{n+1,k}$ sont les coefficients du $(n+1)$-ème polynôme d'André.

PREUVE. Faisons la substitution

$$s = 1\ ,\quad t = 2x/(1+x)^2\ ,\quad u = (1+x)v$$

dans l'expression de $(D'-s)/t$ donnée par (2.14). Notant que la substitution envoie r sur $(1-x)/(1+x)$ et w sur x, on trouve

$$(1+x)\,(\mathrm{Exp}((1-x)v) - 1)/(1 - x\,\mathrm{Exp}((1-x)v))\ .$$

Divisant par $(1+x)$ et ajoutant 1 on obtient

$$(\,(1-x)\,\mathrm{Exp}((1-x)v)\,)/(\,1 - x\,\mathrm{Exp}((1-x)v)\,)$$

qui est l'expression classique de la fonction génératrice exponentielle des polynômes eulériens. Donc, pour $n\geq 0$, $A_n(x)$ est le polynôme obtenu en faisant la substitution $s = 1$, $t = 2x/(1+x)^2$ dans $(1+x)^{n-1}\,t^{-1}\,D_{n+1}$, ce qui est précisément le résultat annoncé. ∎

On pourra noter que la relation de symétrie $x^n A_n(x^{-1}) = A_n(x)$ correspond à l'invariance $t = 2x^{-1}/(1+x^{-1})^2$.

3. LES PERMUTATIONS D'ANDRÉ

1. Quelques notions générales.

Nous commençons par décrire en détail quelques notions de base.

Soit X un ensemble totalement ordonné ayant un nombre fini n d'éléments. Une permutation de X est une bijection $f : [n] \to X$ où $[n]$ désigne l'ensemble ordonné $\{1, 2, \ldots, n\}$ ($= \emptyset$ si $n = 0$). Nous l'identifierons au mot $1f \cdot 2f \cdot \ldots \cdot nf$ en les lettres de X. Puisque f est une bijection, chaque élément de X figurera exactement une fois dans ce mot. Pour abréger, nous écrirons $f \in X^!$ pour indiquer que f est une permutation de X ou son mot associé.

Soient maintenant $n \geq 2$ et $f \in X^!$; la variation de f est le mot $fV = v_1 v_2 \ldots v_{n-1}$ de longueur n-1 en les symboles $v_j = (+)$ et $(-)$ qui est défini pour chaque $j \leq n-1$ par $v_j = +$ si $jf < (j+1)f$

$= -$ si $jf > (j+1)f$.

Il est classique de dire que $[j, j+1]$ est une montée (resp. descente) ssi $v_j = +$ (resp. $= -$) .

Soit maintenant $1 < j < n$:

- $[j-1, j+1]$ est une double descente ssi $[j-1, j]$ et $[j, j+1]$ sont deux descentes;

- j est un creux ssi $[j-1, j]$ est une descente et $[j, j+1]$ une montée;

De façon analogue, la variation circulaire $f\overset{\circ}{V}$ est le mot de longueur n défini par $f\overset{\circ}{V} = fV.\, v_n$ où $v_n = +$ ou $-$ selon que $nf < 1f$ ou $nf > 1f$; autrement dit, v_n est défini pour $[n, 1]$ de la même manière que v_j était défini pour $[j, j+1]$.

D'une manière générale, une notion sera dite circulaire ssi dans sa définition il est convenu que "n+1" signifie "1" . Par exemple pour $X = [8]$ et $f : [8] \to X$ identifié à 5 8 1 6 9 2 3 4 7 on a $fV = +-++-+++$ $(\in \{+, -\}^8)$, 1 et 2 sont les deux creux et f n'a pas de double descente. Comme $7 > 5$ on a $v_n = -$ et $f\overset{\circ}{V} = +-++-+++-$ $(\in \{+, -\}^9)$; enfin comme $7 > 5$, mais $5 < 8$, la permutation f est sans double descente circulaire, donc aussi sans double descente.

Nous introduisons maintenant une notion plus spéciale et nous définissons la variation réduite de f comme le mot fU de longueur $\leq n-1$ en les symboles t et s qui est obtenu à partir de la variation fV en remplaçant d'abor toutes les paires $v_i\, v_{i+1}$ telles que $v_i = -$, $v_{i+1} = +$ par t , ensuite en remplaçant par s les v_i restants. Par construction $fU = s$ ssi $n = 2$. Dans notre exemple $fU = st\ st\ ss$ puisque $fV = +(-+)+(-+)+\ +$.

Rappelons la notation standard $|f|_x$ pour désigner le nombre d'occurrences d'une lettre x dans un mot f .

PROPRIÉTÉ 3.1. Le nombre des creux de f est $|fU|_t$, celui des montées est $\leq |fU|_t + |fU|_s$ avec égalité ssi f est sans double descente et se termine par une montée (c'est-à-dire $v_{n-1} = +$) .

La preuve est immédiate.

On définit de la même manière la variation réduite circulaire $f\mathring{U}$ en convenant d'écrire la lettre t à la fin du mot fU quand n est un creux circulaire (c'est-à-dire quand $v_{n-1} = -$ et $v_n = +$) et au début quand 1 est un creux circulaire (c'est-à-dire quand $v_n = -$ et $v_1 = +$).

C'est ce second cas qui se produit dans notre exemple et l'on a donc

$$f\mathring{U} = t\ t\ s\ t\ s\ s$$

puisque $f\mathring{V} = +)\ (-+)\ +\ (-+)\ ++\ (-\quad$.

On notera que si $n = 2$, $f\mathring{U}$ est toujours t .

On conviendra pour $n = 1$, $f\mathring{U} = s$ et $fU = e$ (c'est-à-dire le mot vide du monoide libre $\{s, t\}^*$).

2. Définition des permutations d'André.

Nous appellerons permutation d'André sur X ($0 \leq \mathrm{Card}\ X = n < \infty$) toute permutation $f : [n] \to X$ sans double descente satisfaisant la condition caractéristique suivante.

(A) Soient $j, j' \in [n]$ tels que $1 < j < j'$ et

$$(j-1)f = \mathrm{Max}\{(j-1)f\ ,\ jf\ ,\ (j'-1)f\ ,\ j'f\}$$

$$j'f = \mathrm{Min}\{(j-1)f\ ,\ jf\ ,\ (j'-1)f\ ,\ j'f\}\ .$$

Il existe un j'' tel que $j < j'' < j'$ et que $j''f < j'f$.

De façon intuitive, en tenant compte de ce que f n'a pas de double descente, la condition peut être reformulée ainsi.

Si j et $j' > j$ sont deux creux tels que $jf > j'f$ et $(j-1)f > (j'-1)f$, il existe un creux j'' entre j et j' ($j < j'' < j'$) tel que $j''f < j'f$ et la même condition vaut

quand $j' = n$ et que $[j'-1, j']$ est une descente.

Il résulte immédiatement de la définition que toute permutation ayant 0 ou 1 descente est une permutation d'André, car elle n'a pas de double descente et la deuxième condition est trivialement vérifiée.

Une permutation f ayant exactement deux descentes $[j,j+1]$ et $[j',j'+1]$ $(j<j')$ est une permutation d'André ssi les deux conditions suivantes sont réalisées

(i) $j+1$ et $j'+1$ sont des creux ou bien $j+1$ est un creux et $[j',j'+1]$ est une descente finale ;

(ii) l'on a $jf<j'f$ ou bien $jf>j'f$ et $(j-1)f<(j'-1)$

Pour avoir une idée concrète de cette condition, le lecteur pourra vérifier que parmi les six permutations de $[6]$ qui sont de la forme $x\ 2\ y\ 3\ z\ 1$ $(\{x, y, z\} = \{4, 5, 6\})$ et qui sont donc sans double descente puisqu'alternées, les permutations d'André sont les deux pour lesquelles $z = 6$.

En effet, puisque $2 = 2f<3 = 4f$, la condition caractéristique ne s'applique qu'aux paires de creux $j = 2$ ou 4 et $j' = 6>j$. Comme $jf = 2$ ou $4 > j'f = 1$ et comme il n'existe aucun creux j'' entre j et j' tel que $j''f<jf$ (puisque $4f = 3>6f = 1$) , on doit avoir $(j-1)f<(j'-1)f$, c'est-à-dire $x<z$ et $y<z$.

Nous noterons D_n $(0\leq n)$ l'ensemble des permutations d'André sur $[n]$ et $D^* = \bigcup_{0\leq n} D_n^*$, en faisant comme d'usage la convention naturelle que pour $n = 0$, D_0^* est un singleton. Voici une table des D_n^* pour $n = 0, 1, 2, 3, 4$.

$D_0^* = \{e\}$; $D_1^* = \{1\}$; $D_2^* = \{12 , 21\}$;
$D_3^* = \{123 , 132, 213, 231, 312\}$;
$D_4^* = \{1234, 1243, 1324, 1342, 1423,$
$2134, 2143, 2314, 2341, 2413,$
$3124, 3142, 3241, 3412,$
$4123, 4132\}$.

On notera que $1 = \text{Card } D_0^* = \text{Card } D_1^*$; $2 = \text{Card } D_2^*$; $5 = \text{Card } D_3^*$; $16 = \text{Card } D_4^*$.

Par abus de notation, si $I = \{n'+1, \ldots, n'+m\}$ est un intervalle de $[n]$ et $f : [n] \to X$ une permutation, nous identifierons la restriction $f|I$ à la permutation $f' : [m] \to If$ ($If \subset X$) telle que $jf' = (n'+j)f$ identiquement.

LEMME 3.2. Soit $f : [n] \to X$ une permutation d'André. Pour tout intervalle I de $[n]$, la restriction $f' = f|I$ de f à I est une permutation d'André.

PREUVE. Ceci découle de la structure des conditions "être sans double descente" et (A) qui ne font intervenir que les éléments d'un intervalle. □

Nous introduisons maintenant deux familles spéciales de permutations d'André que nous appellerons respectivement (par abus de langage) circulaires et augmentées. Soit X un ensemble fini de cardinal n $(n \geq 0)$; une permutation d'André f sur X

est dite circulaire (resp. augmentée) ssi son dernier élément nf est égal à Min f (resp. Max X) . On note D (resp. A) l'ensemble des permutations d'André appartenant à D qui sont circulaires (resp. augmentées) ; on pose $D_n = D \cap D_n^*$ et $A_n = A \cap D_n^*$ $(n > 0)$ et l'on convient que D_0 est vide et que $A_0 = D_0 = \{e\}$. On voit sur la liste ci-dessus que Card D_j = Card $A_j = 1$ pour $j = 1,2$; Card $D_3 = 1$; Card $A_3 = 2$; Card $D_4 = 2$; Card $A_4 = 5$.

PROPRIÉTÉ 3.3. Soient $n \in \underset{\sim}{N}$ et $f : [n+2] \to X$ une permutation quelconque telle que

(i) $(n+2)f = \text{Min } X$.

Les trois conditions suivantes sont équivalentes

(1) La permutation f est une permutation d'André (qui est nécessairement circulaire) ;

(2) La restriction $f' = f\big|[n+1]$ est une permutation d'André augmentée ;

(3) La restriction $f'' = f\big|[n] = f'\big|[n]$ est une permutation d'André et

(ii) $j \in [n] \Rightarrow jf'' < (n+1)f'$.

PREUVE. Le lemme 3.2 donne immédiatement les implications

$f \in D^* \Rightarrow f' \in D^* \Rightarrow f'' \in D^*$.

Supposons (1) et prenons $j' = n+2$. D'après (i), d'une part $[j'-1, j']$ est une descente, d'autre part on ne peut pas avoir $j''f < j'f$ pour $j'' < j'$. Donc d'après (A) on aura $(j-1)f < (j'-1)f$ pour tout $j < j'$ tel que $[(j-1), j]$ soit une descente.

Considérons $\bar{j}$ tel que $(\bar{j}-1)f = \text{Max } X$; le couple $[\bar{j}-1 , \bar{j}]$ est une descente et par conséquent $\bar{j} = j'$, c'est-à-dire $(n+1)f = \text{Max } X$. La condition (1) implique donc (2).

Réciproquement supposons (3) , c'est-à-dire que la restriction $f|[n]$ est une permutation d'André et que l'on a $(n+1)f = \text{Max } X$, $(n+2)f = \text{Min } X$.
Il est clair que f n'a pas de double descente.
D'autre part, prenant encore $j' = n+2$, la condition (A) est toujours satisfaite car il ne peut pas exister de creux $j < j'$ pour lequel $(j-1)f > (j'-1)f$.
Donc (3) $\Rightarrow$ (1) et comme (2) $\Rightarrow$ (3) trivialement d'après $f' \in D^* \Rightarrow f'' \in D^*$, le résultat est établi. ∎

COROLLAIRE 3.4. Pour tout $n \geq 0$ les ensembles D_{n+2} , A_{n+1} et D_n^* ont même cardinalité.

3. Polynômes d'André en variables non commutatives.

Pour simplifier, on appellera polynômes d'André non commutatifs les polynômes

$$A_n U = \sum \{fU : f \in A_n\} \qquad \text{et}$$
$$D_n \overset{\circ}{U} = \sum \{f\overset{\circ}{U} : f \in D_n\} \qquad (n \geq 0)$$

en les variables non commutatives s et t. Dans la propriété 3.10 ci-après, on trouvera deux relations de récurrence sur ces polynômes. Enfin, la liste des polynômes pour les premières valeurs de n est donnée à la fin de ce chapitre.

LEMME 3.5. Soit $f : [n+1] \longrightarrow X$ une permutation d'André. Il existe exactement une valeur $m \leq n$ telle que

(i) $f\big|[m] \in D$;

(ii) $m' \geq m$, $f\big|[m'] \in D \Longrightarrow m' = m$.

PREUVE. Il suffit de prendre $m = (\mathrm{Min}\ X)f^{-1}$ et d'observer que $m = (\mathrm{Min}([m']f))f^{-1}$ pour tout $m' \geq m$. ∎

On notera $f^{(1)}$ la restriction $f\big|[m]$ $(m = (\mathrm{Min}\ X)f^{-1})$ et on appellera $f^{(1)}$ le premier facteur de f . La restriction $f\big|[n] \setminus [m]$ sera le cofacteur de $f^{(1)}$ dans f et on utilisera souvent pour abréger la notation $f^{(1)-1}$ pour désigner $[m]$. L'importance de ce lemme est dans sa réciproque.

PROPRIÉTÉ 3.6. Une permutation $f : [n+1] \to X$ est une permutation d'André ssi posant $m = (\mathrm{Min}\ X)f^{-1}$, les deux restrictions $f^{(1)} = f\,|\,[m]$ et $f' = f\,|\,[n]\setminus[m]$ sont des permutations d'André. Si ces hypothèses sont vérifiées et $n \geqslant 1$, f est augmentée si et seulement s'il en est de même de f'.

PREUVE. La partie directe résulte des lemmes 3.5 et 3.2 Supposons donc $f^{(1)}, f' \in D^*$ et sans perte de généralité $m < n$. Comme $mf = \mathrm{Min}\ X$, $[m, m+1]$ est une montée. Donc f n'a pas de double descente puisque ni $f^{(1)}$ ni f' n'en ont.

Soit maintenant j et j' deux valeurs justiciables de la condition (A). Si $j, j' \in [m]$ ou $\in [n]\setminus[m]$, la condition (A) est satisfaite par f d'après l'hypothèse $f^{(1)}, f' \in D^*$. Si au contraire $j > m > j'$, la condition (A) est satisfaite par l'existence du creux $j'' = m$ entre j et j'. ∎

LEMME 3.7. Soit $f : [n+1] \to X$ une permutation d'André circulaire. Si $n = 0$, $f\mathring{U} = s$ et si $n > 0$, $f\mathring{U} = (f'U)t$ où $f' = f\,|\,[n]$. Par conséquent,

$$D_{n+1}\mathring{U} = (A_n U)t \quad \text{pour} \quad n > 0 .$$

PREUVE. Le cas de $n = 0$ résulte de la définition même de $\mathring{U}$. Si $n \geqslant 1$, la variation de f se termine

par une descente puisque $nf = \mathrm{Max}\ X$, $(n+1)f = \mathrm{Min}\ X$.
Comme $(n+1)f < 1f$, la formule est encore une conséquence de la définition de $\overset{\circ}{U}$. ∎

LEMME 3.8. Soit $f : [n+3] \to X$ une permutation d'André circulaire. On a

$$f\overset{\circ}{U} = g^{(1)}\overset{\circ}{U} \,.\, \overline{f}\overset{\circ}{U}$$

où $g^{(1)}$ est le premier facteur de $g = f\big|[n+1]$ et $\overline{f}$ le cofacteur de $g^{(1)}$ dans f .

PREUVE. Le facteur $g^{(1)}$ est la restriction de f à $[m']$ où $m'f$ est le minimum de X privé de $\mathrm{Min}\ X = (n+3)$ et de $\mathrm{Max}\ X = (n+2)f$. Donc $[m,m+1]$ est toujours une montée de f .

Distinguons maintenant deux cas

(i) $m' = 1$. On a $fV = +\overline{f}V$. Comme $\overline{f}\overset{\circ}{U}$ se termine par t puisque $n+3-m' \geqslant 2$, on a donc $f\overset{\circ}{U} = s.\overline{f}\overset{\circ}{U}$ et le résultat est établi.

(ii) $m' > 1$. Comme $g^{(1)} \in D$, $g^{(1)}$ se termine par la descente $[m-1,m]$. Donc $fU = (g^{(1)}U)'\ t\ (\overline{f}U)$ où $(g^{(1)}U)'$ désigne le mot obtenu en supprimant le dernier s de $g^{(1)}U$. De façon équivalente $fU = g^{(1)}\overset{\circ}{U}.\overline{f}U$, d'où encore $f\overset{\circ}{U} = g^{(1)}\overset{\circ}{U}.\overline{f}\overset{\circ}{U}$. ∎

COROLLAIRE 3.9. Soit $f : [n+2] \to X$ une permutation d'André augmentée. On a

$$fU = f^{(1)}\overset{\circ}{U} \cdot f'U$$

où $f^{(1)}$ est le premier facteur de f et f' son cofacteur.

PREUVE. Définissons la permutation $g : [n+3] \to X'$ par $g\big|[n+2] = f$ et $(n+3)g = \text{Min } X'$. Il est clair que g est une permutation d'André circulaire. Soient $g^{(1)}$ le premier facteur de $g\big|[n+1]$ et $\bar{g}$ le cofacteur de $g^{(1)}$ dans g. On a $g\overset{\circ}{U} = (fU)t$ (d'après le lemme 3.7), $f^{(1)} = g^{(1)}$ et enfin $\bar{g}\overset{\circ}{U} = (f'U)t$. Le lemme précédent donne d'autre part l'identité

$$g\overset{\circ}{U} = g^{(1)}\overset{\circ}{U} \cdot \bar{g}\overset{\circ}{U}$$

c'est-à-dire

$$(fU)t = f^{(1)}\overset{\circ}{U} \cdot (f'U)t .$$

Le corollaire est donc établi en supprimant la dernière lettre t de l'identité précédente. ∎

PROPRIÉTÉ 3.10. Pour tout $n \geq 0$ on a les identités

$$(3.1) \qquad A_{n+2}U = \sum \begin{bmatrix} n \\ j \end{bmatrix} D_{j+1}\overset{\circ}{U} \cdot A_{n+1-j}U$$

$$(3.2) \qquad D_{n+3}\overset{\circ}{U} = \sum \begin{bmatrix} n \\ j \end{bmatrix} D_{j+1}\overset{\circ}{U} \cdot D_{n+2-j}\overset{\circ}{U} \quad .$$

PREUVE. La propriété 3.6 donne une bijection entre A_{n+2} et les triplés $(X' \cup X'', f^{(1)}, f')$ où $X' \cup X''$ est une partition de $X \setminus \{\mathrm{Min}\ X, \mathrm{Max}\ X\}$, $f^{(1)}$ une permutation circulaire d'André sur $X' \cup \{\mathrm{Min}\ X\}$ et f' une permutation augmentée sur $X'' \cup \{\mathrm{Max}\ X\}$. La première formule découle alors du corollaire 3.9 et la deuxième de la première et du lemme 3.7. ∎

REMARQUE 3.11. On a $D_1 \overset{\circ}{U} = s$ et $D_2 \overset{\circ}{U} = t$. D'autre part, la formule de récurrence (3.2) a la même structure formelle que la relation binomiale sur les polynômes commutatifs D_n qui s'écrivait en effet (voir formule (2.4))

$$(3.3) \qquad D_{n+3} = \sum \begin{bmatrix} n \\ j \end{bmatrix} D_{j+1}\, D_{n+2-j} \qquad (n \geq 0).$$

Ceci montre que les polynômes $D_n \overset{\circ}{U}$ constituent bien une version non commutative des polynômes d'André $D_n(s,t)$.

REMARQUE 3.12. Lorsque les variables s et t commutent, on a aussi la formule exponentielle

$$(3.4) \qquad \sum_{0 \leq n} (u^n/n!)\, D_{n+2} = t\, \mathrm{Exp}\Big[\sum_{0 \leq n} (u^n/n!)\, D_n \Big]$$

(voir formule (2.1)). En fait, les formules (3.3) et (3.4) sont équivalentes. On peut s'en convaincre par l'argument suivant. La série formelle égale à t fois l'exponentielle de $\sum_{0 \leq n} (u^n/n!)\, D_n$ est unique. Ceci résulte du fait

que l'exponentielle est une bijection de l'ensemble des série formelles sans terme constant sur l'ensemble des séries formelles de terme constant égal à 1 . Or par dérivation de (3.4) par rapport à u , et identification des termes de même puissance en u , on obtient justement les formules (3.3) .

Cette équivalence n'est plus valable lorsqu'on suppose s et t non commutatifs. Plus exactement, on n'a pas de formule exponentielle ayant même structure formelle que (3.4) avec les polynômes $D_n^{\circ}U$. Seule subsiste la formule (3.2) , qui doit donc être regardée comme la généralisation non commutative de la formule exponentielle.

REMARQUE 3.13. Une autre façon d'établir directement la formule exponentielle (3.4) sans recourir aux arguments analytiques du chapitre 2 est de faire appel aux techniques purement combinatoires du composé partitionnel, développées dans notre précédent mémoire (Foata, Schützenberger (1970)). L'ensemble D^* est, en effet, le composé partitionnel de l'ensemble D des permutations d'André circulaires. Indiquons rapidement comment on peut le démontrer. Soit $f = {}^1f \cdot {}^2f \cdot \ldots \cdot {}^nf$ $(n>0)$ une permutation d'André. Elle admet une factorisation unique $(g^{(1)} , g^{(2)} , \ldots , g^{(k)})$ telle que

(1) le produit de juxtaposition $g^{(1)}\ g^{(2)}\ \dots\ g^{(k)}$ soit égal à f ;

(2) chaque $g^{(j)}$ est une permutation d'André circulaire

(3) la suite formée par les dernières lettres des mots $g^{(j)}$ est croissante.

Par exemple, la factorisation de

f = 8 6 9 7 12 13 1 2 4 11 14 15 3 10 5

est donnée par

(8 6 9 7 12 13 1 , 2 , 4 11 14 15 3 , 10 5) .

L'existence et l'unicité de cette factorisation peuvent être démontrées en utilisant le lemme 3.8 . Supposant s et t commutatifs, on pose pour tout $f \in D_n^*$ $(n>0)$

$$f\mu.\ t = (f.\overline{n+1}.0)\mathring{U} \quad .$$

Là encore, à l'aide du lemme 3.8 , on peut vérifier que μ est multiplicative. D'après la proposition 3.12 de la référence citée plus haut, on en déduit l'identité

$$1 + \sum_{0<n} (u^n/n!)\ D_n^*\mu = \mathrm{Exp}\left[\sum_{0<n} (u^n/n!)\ A_n\mu\right] .$$

L'identité (3.4) en résulte en observant que

$$D_n^*\mu.t = D_{n+2}(s,t) \quad \text{et} \quad A_n\mu = D_n(s,t) \quad \text{pour} \quad n>0 .$$

TABLES 3.13. Pour terminer ce chapitre, nous donnons la liste des polynômes A_nU et $D_n\mathring{U}$ pour les premières valeurs de n . Ces polynômes peuvent être évidemment

calculés à partir des formules de récurrence (3.1) et (3.

$A_1U = 1$

$A_2U = s$

$A_3U = s^2 + t$

$A_4U = s^3 + 2\,st + 2\,ts$

$A_5U = s^4 + 3\,s^2t + 5\,sts + 3\,ts^2 + 4\,t^2$

$A_6U = s^5 + 4\,s^3t + 9\,s^2ts + 9\,sts^2 + 4\,ts^3 + 12\,st^2 + 10\,tst + 12\,t^2s$.

$D_1\overset{\circ}{U} = s$

et pour $n > 0$, on a $D_{n+1}\overset{\circ}{U} = (A_nU)t$.

4. COMPLEXES D'ANDRÉ ET FORMULES DE SYMÉTRIE.

L'objet de ce chapitre est de trouver un équivalent non commutatif à l'identité (2.9) qui s'écrivait

$$2\,D'' = 2\,t - s^2 + D'^2 \ ,$$

c'est-à-dire un équivalent non commutatif à l'ensemble des identités

$$D_1 = s \ , \quad D_2 = t \ , \quad 2\,D_{n+2} = \sum_{0\le i\le n} \begin{bmatrix} n \\ i \end{bmatrix} D_{i+1}\, D_{n-i+1} \quad (n>0)$$

Les permutations d'André définies dans le précédent chapitre se prêtent mal à une telle extension. Nous allons donc leur faire correspondre, de façon bijective, d'autres permutations dites permutations d'André de seconde espèce, qui, elles, permettent cette extension. Pour définir cette correspondance, il semble plus aisé de considérer un modèle abstrait, appelé complexe d'André, de construire ensuite la bijection naturelle entre deux complexes d'André (section 4.1), enfin, de montrer que les permutations d'André et celles de seconde espèce sont deux complexes d'André particuliers (sections 4.2 et 4.3). Nous aurons en fait encore besoin de cette bijection dans le chapitre 5 . Enfin, la formule non commutative qui généralise la formule (2.9) est donnée dans la section 4.4 . Elle apparaît comme une simple application de la propriété de symétrie qui veut que dans l'ensemble A_n des permutations

d'André augmentées, il y a autant de permutations f telles que $fU = w$ que de permutations g telles que $gU = \tilde{w}$, le symbole $\tilde{w}$ désignant le mot retourné déduit de w .

1. Définition des complexes d'André.

Supposons donné pour tout $n \geqslant 0$ un ensemble Y_n d'applications de $[n]$ dans $[n]$. Pour $n = 0$, on suppose que Y_n est un singleton $\{e\}$ et l'on pose $Y = \bigcup_{n\geqslant 0} Y_n$.

DÉFINITION 4.1. On appelle composé bipartitionnel de Y de degré n $(n \geqslant 1)$, l'ensemble, noté $Y_n^{(2)}$, de toutes les paires $\{(f_1,X_1)\ ,\ (f_2,X_2)\}$ satisfaisant aux deux conditions suivantes

(1) X_1 et X_2 sont deux ensembles disjoints de réunion $[n] \setminus \{1\}$;

(2) $f_j \in Y_{n_j}$ avec $n_j = \mathrm{Card}\ X_j$ pour $j = 1,2$.

On pose $Y_0^{(2)} = Y_0 = \{e\}$ et l'ensemble $Y^{(2)} = \bigcup_{n\geqslant 0} Y_n^{(2)}$ est appelé composé bipartitionnel de Y .

Dans la définition qui suit, nous conservons les mêmes notations.

DÉFINITION 4.2. Si pour tout $n \geqslant 0$, les ensembles Y_n et $Y_n^{(2)}$ ont même cardinal, on dit que l'ensemble Y a la propriété d'André. Si, de plus, φ est une bijection de Y

sur $Y^{(2)}$ qui envoie Y_n sur $Y_n^{(2)}$ pour tout $n \geqslant 0$, on dit alors que le couple (Y,φ) est un complexe d'André.

Notons que le composé bipartitionnel de degré 1 est réduit à l'élément $\{(e,\emptyset),(e,\emptyset)\}$. Si donc Y a la propriété d'André, on a nécessairement Card $Y_1 = 1$.

NOTATION 4.3.. Soit (Y,φ) un complexe d'André. Si $\{(f_1,X_1)\ ,\ (f_2,X_2)\}$ est l'image par φ d'un élément f de Y_n $(n \geqslant 2)$, il sera commode de noter

$f\varphi_1$ le couple (ordonné) (f_1,f_2) si l'on a $2 \in X_2$ et

$f\varphi_2$ le couple (ordonné) (f_1,f_2) si l'on a $n \in X_2$.

Dans la définition qui suit, on trouvera l'équivalent abstrait de la notion de variation réduite, comme nous le verrons dans la section 4.2 .

DÉFINITION 4.4. Soit $\{s,t\}^*$ le monoïde libre engendré par les deux variables s et t . Etant donné un complexe d'André (Y,φ) , on définit par récurrence deux applications W_1 et W_2 de Y dans $\{s,t\}^*$ de la façon suivante :

d'abord $fW_1 = fW_2 = 1$ (élément neutre de $\{s,t\}^*$) si f appartient à $Y_0 \cup Y_1$; ensuite, si f est dans Y_n ($n \geqslant 2$) et si $f\varphi_j = (f_1, f_2)$ $(j = 1,2)$, on pose

$fW_j = s.f_2W_j$ si $X_1 = \emptyset$ (i.e. si $f_1 \in Y_0$)

$= f_1W_j.t.f_2W_j$ si $X_1 \neq \emptyset$ (i.e. si $f_1 \notin Y_0$)

pour $j = 1,2$.

En fait, il y a deux bijections naturelles θ et θ' à construire entre deux complexes d'André (Y,φ) et (Z,ψ). La première vérifie $\theta W_j = W_j$ pour $j = 1,2$ et la deuxième $\theta' W_1 = W_2$. Leur construction se fait de la façon suivante :

d'abord θ et θ' envoient l'élément unique de Y_0 (resp. Y_1) sur l'élément unique de Z_0 (resp. Z_1) ;

ensuite, pour $f \in Y_n$ $(n \geqslant 2)$, on construit par récurrence les suites

$$(4.1)\quad f \xrightarrow{\varphi} \{(f_1,X_1),(f_2,X_2)\} \to \{(f_1\theta,X_1),(f_2\theta,X_2)\} \xrightarrow{\psi^{-1}} g$$

$$(4.2)\quad f \xrightarrow{\varphi} \{(f_1,X_1),(f_2,X_2)\} \to \{(f_1\theta',X_1'),(f_2\theta',X_2')\} \xrightarrow{\psi^{-1}} g'$$

où $X_1' = X_1$ et $X_2' = X_2$ si l'un des deux ensembles X_1, X_2 contient à la fois 2 et n et où

$$X_j' = X_j \setminus \{2\} \cup \{n\} \quad \text{et} \quad X_k' = ([n]\setminus\{1\}) \setminus X_j'$$

$(j,k = 1,2 \ ; \ j \neq k)$ si X_j contient 2 mais pas n.

Dans les deux suites (4.1) et (4.2), on pose $g = f\theta$ et $g' = f\theta'$. Les deux applications θ et θ' sont bien définies par récurrence sur n, car si f appartient à Y_n et si l'on a $f\varphi = \{(f_1,X_1),(f_2,X_2)\}$, les deux fonctions f_1 et f_2 appartiennent à des ensembles Y_j tels que $0 \leqslant j < n$.

THÉORÈME 4.5. *Les deux applications* $\theta : f \to g$ *et* $\theta' : f \to g'$ *définies par récurrence en* (4.1) *et* (4.2) *sont des bijections de* Y *sur* Z, *envoyant* Y_n *sur* Z_n *pour tout* $n \geqslant 0$ *et satisfaisant à*

$fW_1 = gW_1$, $fW_2 = gW_2$ et $fW_1 = g'W_2$.

PREUVE. Par récurrence les applications

$\{(f_1,X_1),(f_2,X_2)\} \to \{(f_1\theta,X_1),(f_2\theta,X_2)\}$

et $\{(f_1,X_1),(f_2,X_2)\} \to \{(f_1\theta,X_1'),(f_2\theta,X_2')\}$

sont des bijection de $Y_n^{(2)}$ sur $Z_n^{(2)}$. Par conséquent, en appliquant φ et ψ^{-1} aux deux bouts de la chaîne d'applications en (4.1) et (4.2) , on obtient bien des bijections de Y_n sur Z_n .

On a, d'autre part, $fW_1 = gW_1$ (resp. $fW_2 = gW_2$) car la définition de W_1 et W_2 ne dépend que du caractère vide ou non vide de l'ensemble qui ne contient pas l'élément 2 (resp. n) .

Reste à vérifier $fW_1 = g'W_2$. Supposons $2 \in X_2$. Si X_2 contient aussi n , on a $X_1' = X_1$ et $X_2' = X_2$. Par conséquent,

$$fW_1 = s.f_2W_1 = s.f_2\theta W_2 = g'W_2 \quad \text{si} \quad X_1 = \emptyset$$
$$= f_1W_1.t.f_2W_1 = f_1\theta W_2.t.f_2\theta W_2 = g'W_2 \quad \text{si} \quad X_1 \neq \emptyset .$$

Si au contraire X_2 contient 2 mais pas n , on a

$X_2' = X_2 \setminus \{2\} \cup \{n\}$ et $X_1' = X_1 \cup \{2\} \setminus \{n\}$.

De là, X_1 n'est pas vide et l'on a

$fW_1 = f_1W_1.t.f_2W_1 = f_1\theta W_2.t.f_2\theta W_2 = g'W_2$. ∎

On pose $Y_nW_j = \sum \{fW_j : f \in Y_n\}$ pour $n \geq 0$ et $j = 1,2$.

Les polynômes $(Y_nW_j)_{n\geq 0}$ satisfont une identité binomiale ($j = 1,2$) décrite dans la proposition suivante.

PROPOSITION 4.6. Soit (Y,φ) un complexe d'André. On a $Y_1W_j = 1$ $(j = 1,2)$ et pour $n \geq 0$ et $j = 1,2$, on a l'identité

(4.3) $$Y_{n+2}W_j = s.Y_{n+1}W_j + \sum_{1\leq i\leq n}\begin{bmatrix} n \\ i \end{bmatrix} Y_iW_j \,.\, t \,.\, Y_{n+1-i}W_j \,.$$

PREUVE. Soit (f_1,f_2) un couple d'applications telles que $f_1 \in Y_{n_1}$, $f_2 \in Y_{n_2}$ et $n_1 + n_2 = n+2$. Utilisant la notation 4.3, on voit que le nombre d'applications f appartenant à Y_{n+2} telles que $f\varphi_1 = (f_1,f_2)$ est égal au nombre de couples (X_1,X_2) de parties de $\underline{N}$ satisfaisant à $X_1 \cap X_2 = \emptyset$, $2 \in X_2$, $X_1 \cup X_2 = [n+2]\setminus\{1\}$. Ce nombre est égal au coefficient binomial $\begin{bmatrix} n \\ i \end{bmatrix}$ avec $i = \mathrm{Card}\, X_1$. On a par conséquent

$$\begin{aligned} Y_{n+2}W_1 &= \sum \{fW_1 : f \in Y_{n+2}\} \\ &= \sum \{s.f_2W_1 : f \in Y_{n+2},\ f\varphi_1 = (f_1,f_2),\ f_1 = e\} \\ &\quad + \sum_{1\leq i\leq n}\begin{bmatrix} n \\ i \end{bmatrix} \sum \{f_1W_1.t.f_2W_1 : f \in Y_{n+2},\ f\varphi_1 = (f_1,f_2),\ f_1 \in Y_i\}. \end{aligned}$$

Soit $$\begin{aligned} Y_{n+2}W_1 &= s.Y_{n+1}W_1 + \sum_{1\leq i\leq n}\begin{bmatrix} n \\ i \end{bmatrix} \sum \{f_1W_1.t.f_2W_1 : f_1 \in Y_i,\ f_2 \in Y_{n+1-i}\} \\ &= s.Y_{n+1}W_1 + \sum_{1\leq i\leq n}\begin{bmatrix} n \\ i \end{bmatrix} Y_iW_1.t.Y_{n+1-i}W_1 \,. \end{aligned}$$

La relation binomiale pour W_2 se démontre de la même façon en échangeant les rôles des éléments 2 et $n+2$. ∎

REMARQUE 4.7. On a vu dans la propriété 3.10 la formule

$$A_{n+2}U = \sum \begin{bmatrix} n \\ j \end{bmatrix} D_{j+1}\overset{\circ}{U} \cdot A_{n+1-j}U \cdot$$

Comme $D_1\overset{\circ}{U} = s$ et $D_{j+1}\overset{\circ}{U} \equiv A_jU.t$ pour $j > 0$, cette formule peut encore s'écrire

$$A_{n+2}U = s.A_{n+1}U + \sum_{1 \leq j \leq n} \begin{bmatrix} n \\ j \end{bmatrix} A_jU \cdot t \cdot A_{n+1-j}U \cdot$$

D'autre part, comme on a $A_1U = Y_1W_j = 1$, on voit que les familles des polynômes $(A_nU)_{n>0}$ et $(Y_nW_j)_{n>0}$ sont identiques ($j = 1,2$). Dans la section suivante, nous allons justement vérifier que les permutations d'André augmentées forment un complexe d'André et que la fonction W_2 associée est précisément la variation réduite U.

2. Le complexe des permutations d'André.

Les permutations d'André ont été définies dans la section 3.2. Soit X un ensemble de cardinal n ; on désigne par $\omega_X : X \to [n]$ l'unique application strictement croissante de X sur $[n]$. Soit $f : [n] \to X$ une permutation d'André augmentée sur X. Comme la définition des permutations d'André ne fait intervenir que l'ordre mutuel des éléments de X, l'applications $f\omega_X$ est aussi une permutation d'André augmentée, mais sur l'ensemble $[n]$.

Considérons maintenant l'ensemble $A = \bigcup_{n \geq 0} A_n$ où A_n

désigne toujours ensemble des permutations d'André augmentées sur $[n]$ $(n \geq 0)$ et formons le composé bipartitionnel $A^{(2)}$ de A. Pour f dans A_n $(n > 0)$, on pose $m = (1)f^{-1}$, puis $g_1 = f\big|[m-1]$, $g_2 = f\big|[n]\setminus[m]$, $X_1 = [m-1]f$, $X_2 = ([n]\setminus[m])f$ et enfin $f_1 = g_1\omega_{X_1}$, $f_2 = g_2\omega_{X_2}$.

PROPRIÉTÉ 4.8. L'application

$$\psi : f \longrightarrow \{(f_1,X_1),(f_2,X_2)\}$$

est une bijection de A_n sur $A_n^{(2)}$ pour tout $n > 0$.

PREUVE. D'après la propriété 3.6, les applications g_1 et g_2 sont des permutations d'André ssi f est une permutation d'André. D'autre part, g_2 est augmentée ssi f l'est. Il résulte donc de la propriété 3.3 que f est une permutation augmentée ssi g_1 et g_2 le sont aussi. D'autre part, $f_1 = g_1\omega_{X_1}$ et $f_2 = g_2\omega_{X_2}$ sont aussi des permutations d'André augmentées respectivement sur $[\mathrm{Card}\ X_1]$ et $[\mathrm{Card}\ X_2]$ Il est enfin clair que les couples (f_1,X_1) et (f_2,X_2) caractérisent complètement les fonctions g_1 et g_2.

COROLLAIRE 4.9. Le couple (A,ψ) où ψ est défini dans la précédente propriété est un complexe d'André.

L'application U défini dans la section 3.1 servait à repérer les descentes et les montées des permutations

d'André. Elle est en fait égale à l'application W_2 (Cf. définition 4.4) .

PROPOSITION 4.10. Sur l'ensemble A , les deux applications U et W_2 sont identiques.

PREUVE. D'abord $fU = fW_2 = 1$ pour $f \in A_0 \cup A_1$. Soit $f \in A_n$ ($n \geq 2$) et $f\psi_2 = (f_1, f_2)$. Si l'on a $f_1 \in Y_0$, alors $fW_2 = s.fW_2$, soit $fW_2 = s.fU$ par récurrence. D'autre part, la première lettre de f étant 1 , le mot f débute par une montée. On a donc $fU = s.f_2U$, d'où $fW_2 = fU$. Si l'on a $f_1 \notin Y_0$, par récurrence, il vient $fW_2 = f_1U.t.f_2U$.

D'autre part, on a $fU = f_1U.t.f_2U$ d'après le corollaire 3.9 et le lemme 3.7 . La proposition 4.10 en découle. ∎

3. Les permutations d'André de seconde espèce.

Nous introduisons dans cette section une deuxième classe de permutations appelées permutations d'André de seconde espèce. L'ensemble de ces permutations sur $[n]$ sera noté B_n ($n \geq 0$) . Soit $f : [n] \to X$ une permutation. On note $x_1, x_2, \ldots, x_n$ la suite croissante des éléments de l'ensemble totalement ordonné X . Pour $n>0$ on désigne par fT la permutation déduite de f par suppression du plus grand élément x_n de la suite $1f . 2f . \ldots . nf$. En d'autres termes, si l'on a $mf = x_n$ pour un certain $m \in [n]$, alors

$fT = 1f \cdot 2f \cdot \ldots \cdot (m-1)f \cdot (m+1)f \cdot \ldots \cdot nf$. Notons que si $n = 1$, fT est le mot vide noté e .

DÉFINITION 4.11. On dit qu'une permutation $f : [n] \longrightarrow X$ a la propriété (Δ) si elle n'a pas de double descente et ne finit pas par une descente, c'est-à-dire s'il n'existe pas d'entier j tel que $1 \leq j < n-1$ et $jf > (j+1)f > (j+2)f$ et si d'autre part on a toujours $(n-1)f < nf$ lorsque $n > 1$.

DÉFINITION 4.12. Une permutation $f : [n] \longrightarrow X$ $(n > 0)$ est une permutation d'André de seconde espèce si les $(n+1)$ permutations f , fT , ... , fT^n ($= e$) ont la propriété (Δ) .

Par exemple, la permutation $f = 3\ 1\ 2\ 6\ 4\ 5$ est une permutation d'André de seconde espèce, car elle-même, ainsi que les permutations déduites de f par suppression successive de 6 , 5 , ..., 1 , à savoir

$fT = 3\ 1\ 2\ 4\ 5$, $fT^2 = 3\ 1\ 2\ 4$, $fT^3 = 3\ 1\ 2$,

$fT^4 = 1\ 2$, $fT^5 = 1$, $fT^6 = e$

ont toutes la propriété (Δ) .

PROPRIÉTÉ 4.13. Une permutation $f : [n] \longrightarrow X$ est une permutation d'André de seconde espèce ssi posant $m = (\mathrm{Min}\ X)f^{-1}$, les deux restrictions $g_1 = f\big|[m-1]$ et $g_2 = f\big|[n] \setminus [m]$ sont des permutations d'André de seconde espèce. Si ces hypothèses sont vérifiées et si $n \geqslant 2$, on a $kf = x_2 = \mathrm{Min}\{X \setminus \mathrm{Min}\ X\}$ pour un indice k tel que $1 \leq m < k \leq n$.

PREUVE. D'abord, si $n = 1$, on a $g_1 = g_2 = \varepsilon$ et il n'y a rien à démontrer. Supposons $n > 1$. Par définition de T, on a toujours pour $1 \leq i < n-1$

$$fT^i = g_1 T^{i_1} \cdot x_1 \cdot g_2 T^{i_2}$$

pour $i_1 \geqslant 0$, $i_2 \geqslant 0$ et $i_1 + i_2 = i$. Supposons $g_1 T^{i_1}$ de longueur $(m_1 - 1)$, c'est-à-dire $(m_1)(fT^i) = x_1$. Si $g_1 T^{i_1}$ finit par une descente, la permutation fT^i a une double descente $[m_1 - 2, m_1]$. D'autre part, du fait que $x_1 = \mathrm{Min}\, X$, la permutation fT^i ne peut avoir de descente en $[m_1, m_1 + 1]$. Il en résulte que fT^i a la propriété (Δ) si et seulement s'il en est de même pour $g_1 T^{i_1}$ et $g_2 T^{i_2}$. Par conséquent, f est une permutation d'André de seconde espèce ssi il en est de même pour g_1 et g_2.

Supposons enfin que f soit une permutation d'André de seconde espèce. La permutation fT^{n-2} ne contient que les éléments x_1 et x_2 ; comme, d'autre part, elle a la propriété (Δ), on a $fT^{n-2} = x_1 x_2$. L'élément x_2 est donc toujours après x_1 dans une permutation d'André de seconde espèce.

Comme précédemment, si X est un ensemble totalement ordonné de cardinal n, on note ω_X l'unique application strictement croissante de X sur $[n]$. Soit f une

permutation d'André de seconde espèce sur $[n]$ ($n>0$) .
On pose $m = (1)f^{-1}$, $g_1 = f \mid [m-1]$, $g_2 = f \mid [n]\setminus[m]$,
$X_1 = ([m-1])f$, $X_2 = ([n]\setminus[m])f$ et enfin $f_1 = g_1^{\omega_{X_1}}$, $f_2 = g_2^{\omega_{X_2}}$.

PROPRIÉTÉ 4.14. (1) L'application

$$\varphi : f \longrightarrow \{(f_1,X_1),(f_2,X_2)\}$$

est une bijection de B_n sur $B_n^{(2)}$ pour tout $n>0$.

(2) Le couple (B,φ) est un complexe d'André.

(3) Sur l'ensemble B les deux applications U et W_1 sont identiques.

PREUVE. (1) Si $n = 1$ la propriété est triviale. Supposons $n>1$; il résulte de la propriété 4.13 que φ envoie B_n dans $B_n^{(2)}$. Considérons un couple de parties (X_1,X_2) de $[n]$ telles que $X_1 \cap X_2 = \emptyset$, $X_1 \cup X_2 = [n]\setminus\{1\}$, $2 \in X_2$ et Card $X_1 = m-1$. Il est clair que φ envoie, de façon bijective, les permutations $f \in B_n$ telles que $mf = 1$ et $[m-1]f = X_1$ sur les paires $\{(f_1,X_1'),(f_2,X_2')\}$ de $B_n^{(2)}$ telles que $X_1' = X_1$, $X_2' = X_2$. D'autre part, si pour f , f' dans B_n , on a $1f = m$, $1f' = m'$ et $[m]f \neq [m']f'$, les deux images $f\varphi$ et $f'\varphi$ sont distinctes. Enfin, on obtient tout B_n et tout $B_n^{(2)}$ en faisant varier X_1 dans l'ensemble des parties de $[n]\setminus[2]$.

La partie (2) résulte immédiatement de (1) .

(3) Soit $f \in B_n$ et $f\varphi_1 = (f_1,f_2)$. Lorsque f est

dans $B_0 \cup B_1$, ou lorsque $f_1 = e$, il suffit de reprendre la preuve de la propriété 4.10 pour montrer que l'on a $fU = fW_1$. Reste à considérer le cas $f_1 \neq e$. Par définition de f_1 (voir notation 4.3) et par récurrence, on a $fW_1 = f_1U.t.f_2U$. Posons $1f = m$; on a $m > 1$. Comme f_1 ne finit pas par une descente et que le couple $[m,m+1]$ ne peut être une descente pour f , on a aussi $fU = f_1U.t.f_2U$. D'où encore $fW_1 = fU$. ∎

PROPOSITION 4.15. Posons $Y = B$ et $Z = A$. Alors l'application θ' définie en (4.2) est une bijection de l'ensemble B des permutations d'André de seconde espèce sur l'ensemble A des permutations d'André, satisfaisant à

$$fU = f\theta'U$$

pour tout f dans B .

PREUVE. D'après le corollaire 4.9 et la propriété 4.14 , les couples (A,ψ) et (B,φ) sont des complexes d'André. Comme, d'autre part, la fonction U est égale à W_1 sur B et à W_2 sur A , la proposition découle du théorème 4.5 . ∎

EXEMPLE 4.17. On vérifie d'abord que la bijection $\theta' : B \to A$ envoie les permutations 1 , 12 et 123 sur elles-mêmes.

De (4.2) , nous obtenons

$$312 \xrightarrow{\varphi} \{(1,\{3\}),(1,\{2\})\} \to \{(1,\{2\}),(1,\{3\})\} \xrightarrow{\psi^{-1}} 213$$

et $(312)U = (213)U = t$. De même,

$$45123 \xrightarrow{\varphi} \{(12,\{4,5\}),(12,\{2,3\})\} \to \{(12,\{2,4\}),(12,\{3,5\})\} \xrightarrow{\psi^{-1}} 24135$$

et $(45123)U = (24135)U = sts$.

A la fin du chapitre 5 , on trouvera la table de correspondance $\theta' : B_n \longrightarrow A_n$ pour $1 \leq n \leq 5$.

4. Propriétés de symétrie.

Soit $w = u_1 u_2 \ldots u_k$ $(k > 0)$ un mot du monoïde $\{s,t\}^*$; Le mot retourné $\tilde{w}$ est défini par

$$\tilde{w} = u_k u_{k-1} \ldots u_1 .$$

D'autre part, pour un entier i de l'intervalle $[k+1]$, on définit

$$\begin{aligned} w\Gamma_i &= u_1 \ldots u_{i-1}\ t\ u_{i+1} \ldots u_k \quad \text{si} \quad 1 \leq i \leq k \ , \ u_i = s \\ &= u_1 \ldots u_{i-1}\ s\ t\ u_{i+1} \ldots u_k \quad \text{si} \quad 1 \leq i \leq k \ , \ u_i = t \\ &= w\ s \quad \text{si} \quad i = k+1 . \end{aligned}$$

Posant $w' = w\Gamma_i$, le lemme suivant a pour but de déterminer la transformation Γ_j qu'il faut appliquer au mot retourné $\tilde{w}$ pour retrouver le mot retourné $\tilde{w}'$.

LEMME 4.18. Soit $w = u_1 u_2 \ldots u_k$ un mot de longueur k ($k > 0$) du monoïde $\{s,t\}^*$. A tout entier i de l'intervalle $[k+1]$ on associe l'indice j défini par

(1) $j = k-i+1$ si $1 \leq i \leq k$, $u_i = s$;

(2) $j = k-\ell+2$ si $1 \leq i \leq k$, $u_i = t$, où ℓ est le plus petit entier satisfaisant à $1 \leq \ell \leq i$ et

$$u_\ell u_{\ell+1} \ldots u_i = s^{i-\ell} t ;$$

(3) $j = k-\ell+2$ si $i = k+1$, où ℓ est, cette fois, le plus petit entier satisfaisant à $1 \leq \ell \leq k+1$ et

$u_1 \dots u_{\ell-1}\, s^{k-\ell+1} = u_1 u_2 \dots u_k$.

Alors l'application $i \to j$ est une bijection de $[k+1]$ sur lui-même satisfaisant à

$$\widetilde{w\Gamma_i} = \tilde{w}\Gamma_j \ .$$

PREUVE. Posons $w' = w\Gamma_i$. Dans le cas (1) , on a

$$\tilde{w} = u_k \dots u_{i+1}\, s\, u_{i-1} \dots u_1 \quad \text{et}$$
$$\tilde{w}' = u_k \dots u_{i+1}\, t\, u_{i-1} \dots u_1 \ .$$

Il est clair que l'entier $j = k-i+1$ est le seul entier de $[k+1]$ pour lequel on ait $\tilde{w}\Gamma_j = \tilde{w}'$. Dans le cas (2) , on a

$$\tilde{w} = u_k \dots u_{i+1}\, t\, u_{i-1} \dots u_1 \quad \text{et}$$
$$\tilde{w}' = u_k \dots u_{i+1}\, t\, s\, u_{i-1} \dots u_1 \ ;$$

soit encore, par définition de ℓ

$$\tilde{w} = u_k \dots u_{i+1} + s^{i-\ell}\, u_{\ell-1} \dots u_1 \quad \text{et}$$
$$\tilde{w}' = u_k \dots u_{i+1}\, t\, s^{i-\ell+1}\, u_{\ell-1} \dots u_1$$

avec $\ell = 1$ ou $\ell > 1$ et $u_{\ell-1} = t$. On voit donc que pour passer de $\tilde{w}$ à $\tilde{w}'$ il faut ajouter une lettre s à la séquence $s^{i-\ell}$. La seule façon d'obtenir ce rajout en appliquant une transformation Γ_j est de faire opérer $\Gamma_{k-\ell+2}$. En effet, si $\ell = 1$, on a $\tilde{w}\Gamma_{k-\ell+2} = \tilde{w}\Gamma_{k+1} = \tilde{w}\, s = \tilde{w}'$. Si $\ell > 1$, la lettre $u_{\ell-1}$ dans $\tilde{w}$ est transformée en st et l'on a encore $w\Gamma_{k-\ell+2} = \tilde{w}'$. Enfin, dans le cas (3) , on a

$$\tilde{w} = s^{k-\ell+1}\, u_{\ell-1} \dots u_1 \quad \text{et}$$
$$\tilde{w}' = s^{k-\ell+2}\, u_{\ell-1} \dots u_1 \ .$$

Là encore, on a $\tilde{w}\Gamma_j = \tilde{w}'$ pour le seul $j = k-l+2$.
Le caractère bijectif de $i \to j$ provient du fait que pour tout i dans $[k+1]$, il n'y a chaque fois qu'un seul entier j qui vérifie la propriété $\widetilde{w\Gamma_i} = \tilde{w}\Gamma_j$. ∎

Soit maintenant f une permutation d'André de deuxième espèce sur $[n]$ ($n \geq 2$) . Comme f n'a pas de double descente, sa variation (voir section 3.1) fV n'a jamais deux signes − consécutifs. Donc lorsqu'on remplace dans fV toutes les paires successives $-+$ par t , il ne reste plus dans le mot fV que des signes $+$, que l'on remplace alors par des lettres s pour obtenir la variation réduite fU . Les lettres égales à t du mot fU correspondent donc aux descentes de f et les lettres s aux montées non précédées de descentes. Appelons distingués (pour f) les entiers m de $[n+1]$ pour lesquels l'une des conditions suivantes est satisfaite

(4.4)
$$\begin{aligned} &(1)\quad m = 1 \ , \ mf < (m+1)f \ ; \\ &(1')\quad 1 < m \leq n-1 \ , \ (m-1)f < mf < (m+1)f \ ; \\ &(2)\quad 1 < m < n-1 \ , \ (m-1)f > mf \ ; \\ &(3)\quad m = n+1 \ . \end{aligned}$$

Les entiers définis en (1) et (1') sont les entiers qui correspondent aux montées non précédées de descentes ; ceux définis en (2) correspondent aux descentes de f . On a l'inégalité stricte $1 < m < n-1$ en (2) car f ne peut se terminer par une descente.

Si m est le i-ème élément distingué pour f, c'est-à-dire si l'intervalle $[m]$ contient exactement i indices distingués pour f, on pose $m\tau = i$.
La variation réduite fU de f sera notée $fU = u_1u_2 \dots u_k$, de longueur k ($k>0$). L'application τ est ainsi une bijection de l'ensemble des éléments distingués pour f sur l'intervalle $[k+1]$. On a en particulier $(n+1)\tau = k+1$. L'application inverse de τ est notée τ^{-1}. Pour $n \geqslant 2$, on désigne par $\bar{B}_n$ l'ensemble des couples (f,i) où f appartient à B_n et où, lorsque la variation réduite de f est de longueur k, l'entier i varie de 1 à $k+1$.

PROPOSITION 4.19. L'application

$$\sigma : (f,i) \longrightarrow g$$

définie par $m = i\tau^{-1}$ et

$$g = 1f \,.\, \dots \,.\, (m-1)f \,.\, n+1 \,.\, mf \,.\, \dots \,.\, nf$$

est une bijection de $\bar{B}_n$ sur B_{n+1} satisfaisant à

$$gU = fU\Gamma_i \,.$$

PREUVE. Soit f un élément de B_n ($n \geqslant 2$), de variation réduite $fU = u_1u_2 \dots u_k$ ($k>0$). On obtient un élément de B_{n+1} ssi l'on intercale $(n+1)$ dans le mot $1f.2f. \dots .nf$ sans engendrer de double descente et sans créer de descente finale. L'examen des conditions (4.4) nous montre que l'intercalement de $(n+1)$ entre les lettres de $(m-1)f$ et mf donne un élément g de B_{n+1} ssi l'entier m est distingué pour f.

De plus, l'application $(f,i) \to g$ est évidemment injective. Pour démontrer la surjectivité, on considère un élément g de B_{n+1} et l'on note m l'entier défini par $mg = n+1$. Par définition des permutations d'André de seconde espèce, la permutation $f = gT$ déduite de g par suppression de $(n+1)$ appartient à B_n. Il nous suffit donc de vérifier que l'entier m est distingué pour f.

Trois cas sont à considérer

(1) $m = 1$ ou $1 < m < n$ et $(m-1)g < (m+1)g$;

(2) $1 < m < n$ et $(m-1)g > (m+1)g$;

(3) $m = n+1$.

Dans les cas (1) et (2), *on a forcément* $(m+1)g < (m+2)g$, car autrement $[m,m+2]$ serait une double descente dans g. On voit encore que les trois précédentes conditions sur g impliquent les conditions (4.4) sur f, c'est-à-dire que m est distingué pour f.

Reste à comparer les variations réduites de f et g dans la correspondance $(f,i) \to g$. Dans le cas (1), on a

$$gU = u_1 \dots u_{i-1}\, t\, u_{i+1} \dots u_k$$

Dans le cas (2), on a $gU = u_1 \dots u_{i-1}\, st\, u_{i+1} \dots u_k$ et dans le cas (3) $gU = u_1 \dots u_{k+1}\, s$. Dans les trois cas, on a bien $gU = fU\Gamma_i$ par définition de Γ_i. ∎

REMARQUE 4.20. L'application inverse $g \to (f,i)$ de B_{n+1} sur $\overline{B}_n$ est évidemment donnée par

$f = gT$ (permutation déduite de g par suppression de $n+1$)

et l'entier i est le nombre d'éléments distingués pour f dans l'intervalle $[m]$ où $mg = n+1$.

Nous avons désormais tous les éléments pour définir la bijection ρ de B_n sur lui-même satisfaisant à

5) $\widetilde{gU} = g\rho U$ pour tout $g \in B_n$.

Pour $n = 1$, il n'y a rien à démontrer. Pour $n = 2$, l'ensemble B_n est réduit à la permutation 12, de variation réduite s et ρ est trivialement défini comme l'application identique de B_n. Supposons $n+1 \geqslant 3$ et soit g un élément de B_{n+1}. Si le mot gU est symétrique, c'est-à-dire si $\widetilde{gU} = gU$, on pose

(4.6) $g' = g\rho = g$.

Si le mot gU n'est pas symétrique, on considère la suite des applications

(4.7) $$g \xrightarrow{\sigma^{-1}} (i,f) \longrightarrow (j,f') \xrightarrow{\sigma} g'$$
$$B_{n+1} \quad \overline{B}_{n+1} \quad \overline{B}_n \quad B_{n+1}$$

dans laquelle

(1) σ^{-1} est l'inverse de la bijection définie dans la proposition 4.19 ;

(2) $i \to j$ est la bijection définie dans le lemme 4.18 ;

(3) $f \to f'$ est la bijection ρ de B_n sur lui-même qu'on suppose définie par récurrence jusqu'à l'ordre n ;

(4) σ est la bijection définie dans la proposition 4.19 .

Par récurrence, on $\widetilde{fU} = f'U$ et $f \longrightarrow f'$ est une bijection de B_n sur lui-même. Les deux mots fU et $f'U$ ont en particulier même longueur et l'application $(i,f) \longrightarrow (j,f)$ est donc bien une bijection de $\overline{B}_n$ sur lui-même. Le produit de composition défini par la suite (4.7) est donc bien une bijection de B_{n+1} sur B_{n+1} , qu'on notera $\rho : g \longrightarrow g'$.

D'autre part, on a successivement

$gU = fU\Gamma_i$ d'après la proposition 4.19 ; puis posant $w = fU$ et $w' = w\Gamma_i$, on a, d'après le lemme 4.18 , $\tilde{w}' = \tilde{w}\Gamma_j$, d'où par récurrence $f'U = \tilde{w}$ et $\widetilde{gU} = \tilde{w}' = \tilde{w}\Gamma_j = f'U\Gamma_j$ Enfin, d'après la proposition 4.19 de nouveau

$\widetilde{gU} = g'U$.

Rassemblons ces résultats dans un théorème.

THÉORÈME 4.20. L'application ρ de B dans B qui envoie sur eux-mêmes les éléments de $B_0 \cup B_1 \cup B_2$ et qui, lorsque g est dans B_{n+1} $(n+1 \geqslant 3)$ est définie par $g\rho = g'$ selon les relations (4.6) et (4.7), est une bijection de B sur lui-même ayant la propriété suivante :

si g est dans B_n et si $gU = w$, alors $g\rho$ est dans B_n et $g\rho U = \tilde{w}$.

EXEMPLE 4.21. Supposons $g = 12534$, appartenant à B_5, de variation réduite $gU = sst$. Déterminons $g' = g\rho$ définie en (4.7). D'abord $f = gT = 1234$ et $m = 3$.
Comme 3 est le troisième élément distingué pour f, on a $i = 3$. Par suite $g\sigma^{-1} = (3,1234)$. La variation réduite de f est $u_1u_2u_3 = sss$, de longueur $k = 3$ et symétrique. On a ainsi $f' = f = 1234$, d'après (4.6). Comme $u_i = u_3 = s$, l'entier j (d'après le lemme 4.18) est défini par

$$j = k-i+1 = 3-3+1 = 1 .$$

Par conséquent $g' = (1,f')\sigma = 5.1f'.2f'.3f'.4f' = 51234$ et l'on a bien $g'U = tss$. *Une table de correspondance* pour la bijection ρ est reproduite à la fin du chapitre 5.

D'après la propriété 3.1, si f est dans B_n ($n>0$), de variation réduite $fU = w$, on a

$$2|w|_t + |w|_s = n-1 .$$

Il en résulte que si l'on considère un mot quelconque w de $\{s,t\}^*$ il existe un et un seul entier $n \geq 0$ pour lequel l'ensemble $B_n \cap wU^{-1}$ n'est pas vide. Une des conséquences du théorème 4.20 est donc que l'on a

$$\text{Card } wU^{-1} = \text{Card } \tilde{w}U^{-1} \tag{4.8}$$

pour tout $w \in \{s,t\}^*$, c'est-à-dire que dans tout B_n il y a autant de permutations f telles que $fU = w$ que de permutations g telles que $gU = \tilde{w}$.

D'autre part, pour $n \geq 0$, on peut écrire

$$(4.9) \quad B_{n+2}U = \sum \{ w \text{ Card } wU^{-1} : w \in \{s,t\}^*, 2|w|_t + |w|_s = n+1 \}$$

et d'après (4.8) , ce polynôme ne change pas si l'on transforme dans son expression (4.9) tous les mots w en $\tilde{w}$. Prenant alors un complexe d'André (Y,φ) arbitraire, on voit que le polynôme $Y_{n+2}W_j$ (voir proposition 4.6) a la même propriété ($j = 1,2$) . Or on a d'après (4.3)

$$(4.10) \quad Y_{n+2}W_j = s.Y_{n+1}W_j + \sum_{1 \leq i \leq n} \begin{bmatrix} n \\ i \end{bmatrix} Y_iW_j.t.Y_{n+1-i}W_j$$

($j = 1,2$) . Si l'on retourne dans (4.10) tous les mots w , on obtient donc l'identité

$$(4.11) \quad Y_{n+2}W_j = Y_{n+1}W_j.s + \sum_{1 \leq i \leq n} \begin{bmatrix} n \\ i \end{bmatrix} Y_{n+1-i}W_j.t.Y_iW_j$$

soit

$$(4.12) \quad Y_{n+2}W_j = \sum_{1 \leq i \leq n} \begin{bmatrix} n \\ i-1 \end{bmatrix} Y_iW_j.t.Y_{n+1-i}W_j + Y_{n+1}W_j.s \quad ,$$

qui est en fait une nouvelle identité sur les polynômes $(Y_nW_j)_{n \geq 0}$. Par addition des identités (4.10) et (4.12) on obtient

$$(4.13) \quad 2\, Y_{n+2}W_j = s.Y_{n+1}W_j + \sum_{1 \leq i \leq n} \begin{bmatrix} n+1 \\ i \end{bmatrix} Y_iW_j.t.Y_{n+1-i}W_j + Y_{n+1}W_j.s$$

pour $j = 1,2$ et $n \geq 0$.

L'identité (4.13) est un équivalent non commutatif en les variables s et t de l'identité (4) de l'introduction. En effet, lorsqu'on prend le complexe d'André (A,ψ) et $W_2 = U$, cette identité s'écrit

$$2\,A_{n+2}U = s.A_{n+1}U + \sum_{1\leq i\leq n}\left[\begin{matrix}n+1\\ i\end{matrix}\right]A_iU.t.A_{n+1-i}U + A_{n+1}U.s\ .$$

Multipliant cette identité à droite par t, on obtient, d'après le lemme 3.7

$$2\,D_{n+3}\overset{\circ}{U} = s.D_{n+2}\overset{\circ}{U} + \sum_{1\leq i\leq n}\left[\begin{matrix}n+1\\ i\end{matrix}\right]D_i\overset{\circ}{U}.D_{n+2-i}\overset{\circ}{U} + D_{n+2}\overset{\circ}{U}.t^{-1}st\ ,$$

où t^{-1} a une interprétation évidente. D'après la remarque 3.11, on sait que l'image abélienne des polynômes $D_n\overset{\circ}{U}$ donne précisément les polynômes $D_n = D_n(s,t)$ considérés dans le second chapitre. L'image abélienne de la précédente identité donne donc

$$2\,D_{n+3} = D_1.D_{n+2} + \sum_{1\leq i\leq n}\left[\begin{matrix}n+1\\ i\end{matrix}\right]D_i.D_{n+2-i} + D_{n+2}.D_1\ ,$$

soit précisément l'identité (4) ou l'identité (2.10) écrite pour n+1 au lieu de n.

5. AUTRES COMPLEXES D'ANDRÉ.

1. Les arborescences binaires décroissantes.

Soit $x_1 , x_2 , \dots , x_n$ la suite croissante des éléments d'un ensemble fini X, totalement ordonné et de cardinal $n > 0$.

DÉFINITION 4.1. On dit qu'une application f de X dans X est une arborescence binaire décroissante sur X si f satisfait aux trois propriétés suivantes

(1) $xf < x$ pour tout $x \in X \setminus \{x_1\}$;

(2) $x_1 f = x_1$;

(3) $\mathrm{Card}\left[xf^{-1} \setminus \{x\}\right] \leqslant 2$ pour tout $x \in X$.

Les deux premières conditions impliquent que f est une arborescence (au sens usuel du terme) décroissante. Enfin, pour mentionner la troisième condition, à savoir que tout point x n'est l'image que d'au plus deux autres points, on dit que f est binaire. Si $n \geqslant 2$, on a toujours

$$x_2 f = x_1 .$$

Pour $n > 0$ on note S_n l'ensemble des arborescences binaires décroissantes sur $[n]$. On convient, de plus, que pour $n = 0$ l'ensemble S_n est un singleton $\{e\}$. On pose enfin $S = \bigcup_{n \geqslant 0} S_n$.

Il est coutumier d'associer à toute arborescence f sur X son graphe orienté. Les sommets du graphe sont les éléments

de X et l'on joint x à y par un arc ssi l'on a $x \neq y$ et $f(x) = y$. Enfin, une boucle entoure tout sommet fixé par f. Nous reproduisons dans la figure 1 les graphes des applications appartenant à S_n pour $1 \leq n \leq 4$.

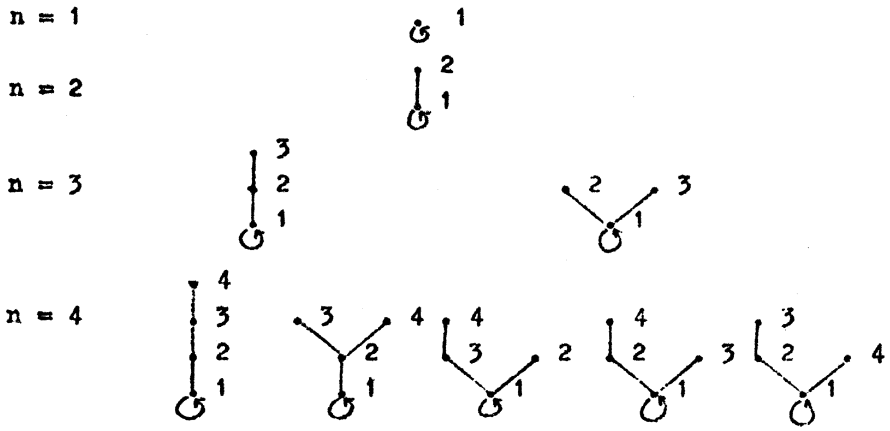


Figure 1.

Pour $n = 5$, on trouverait exactement 16 graphes.

Comme précédemment, l'application strictement croissante d'un ensemble fini totalement ordonné X sur l'intervalle $[\mathrm{Card}\ X]$ est noté ω_X. Considérons maintenant un élément f de S_n ($n \geq 2$). L'ensemble $1f^{-1}$ contient, par définition un ou deux éléments distincts de 1. Si $\mathrm{Card}\,[1f^{-1} \setminus \{1\}] =$ on a forcément $1f^{-1} \setminus \{1\} = \{2\}$. L'application g_2 définie par

$xg_2 = xf$ si $x \in [n] \setminus \{2\}$

$= x$ si $x = 2$

est trivialement une arborescence binaire décroissante sur l'intervalle $\{2,3, \ldots, n\}$. On pose dans ce cas

$$X_1 = \emptyset \ , \ f_1 = e \ , \ X_2 = [n] \setminus \{1\} \quad \text{et} \quad f_2 = \omega_{X_2}^{-1} g_2 \omega_{X_2} .$$

Lorsque $\mathrm{Card}\,[1f^{-1} \setminus \{1\}] = 2$, on a $1f^{-1} \setminus \{1\} = \{2,y\}$ avec $2 < y \leqslant n$. On pose alors

$$X_1 = \{x \in [n] : xf^k = 2 \ , \ k \geqslant 0\}$$

$$X_2 = \{x \in [n] : xf^k = y \ , \ k \geqslant 0\}$$

puis l'on définit deux applications respectivement sur X_1 et X_2 par

$xg_1 = xf$ si $x \in X_1 \setminus \{2\}$

$= x$ si $x = 2$;

$xg_2 = xf$ si $x \in X_2 \setminus \{y\}$

$= x$ si $x = y$.

Enfin, on pose $f_1 = \omega_{X_1}^{-1} g_1 \omega_{X_1}$ et $f_2 = \omega_{X_2}^{-1} g_2 \omega_{X_2}$.
Lorsque f est dans S_1, on pose $f_1 = f_2 = e$ et $X_1 = X_2 = \emptyset$.

PROPRIÉTÉ 5.2. L'application

$$\gamma : f \longrightarrow \{(f_1,X_1),(f_2,X_2)\}$$

est une bijection de S_n sur le composé bipartitionnel $S_n^{(2)}$ ($n \geqslant 1$) .

PREUVE. D'abord X_1 et X_2 sont bien deux sous-ensembles de $[n]$ satisfaisant à

(5.1) $X_1 \cap X_2 = \emptyset$, $X_1 \cup X_2 = [n] \setminus \{1\}$.

Identifions les arborescences avec leurs graphes. Si l'on "enracine" les sommets adjacents à 1 et l'on supprime le sommet 1 , on obtient bien deux arborescences (disjointes) binaires et décroissantes g_1 et g_2 . Réciproquement, si g_1 et g_2 sont deux arborescences binaires décroissantes ayant pour ensembles de sommets respectivement X_1 et X_2 satisfaisant à (5.1) , la seule façon d'obtenir une arborescence binaire décroissante sur $[n]$, qui contienne tous les arcs de g_1 et g_2 à l'exception des boucles, est de joindre les "racines" de g_1 et g_2 au nouveau sommet 1 qu'on prend pour racine. Enfin, les couples (f_1,X_1) et (f_2,X_2) caractérisent complètement g_1 et g_2 , puisque f_1 et f_2 se déduisent de g_1 et g_2 par une renumérotation canonique des sommets, qui conserve l'ordre mutuel de ceux-ci. □

COROLLAIRE 5.3. Le couple (S,γ) est un complexe d'André.

Les applications W_1 et W_2 (voir définition 4.4) n'ont pas d'interprétation intéressante lorsqu'on les définit sur S . On peut cependant introduire la notion de point double. Soit $f \in S_n$ et $x \in [n]$; on dit que x est un point double pour f si x est l'image par f de deux autres points. Si on reprend les définitions de W_1 et W_2 , on voit que l'on fait apparaître une lettre égale à t dans les mots fW_1 et fW_2 chaque fois

que l'on rencontre un point double, et une lettre s dans le cas contraire. Par conséquent, le nombre d'occurences de la lettre t dans les mots fW_1 et fW_2 est égal au nombre de points doubles de f . D'autre part, comme tout point est l'image par f d'au plus deux autres points, le nombre de points doubles est encore égal au nombre de bouts pendants dans f , c'est-à-dire de points qui ne sont l'image d'aucun autre point. On en déduit donc la propriété suivante.

PROPRIÉTÉ 5.4. Soit $P_n(t)$ le polynôme générateur du nombre des points doubles (ou des bouts pendants) sur S_n ($n>0$). On a alors $t.P_n(t) = D_{n+1}(s=1,t)$.

Pour terminer cette section, nous indiquons l'argument géométrique qu'on peut utiliser pour définir les bijections $\theta : S \longrightarrow B$ et $\theta' : S \longrightarrow A$, au lieu de recourir aux chaînes d'applications (4.1) et (4.2) . Considérons dans le plan xy l'ensemble H contenant l'origine, les points de coordonnées $(i/2^k , k)$ où k parcourt l'ensemble des entiers (strictement) positifs et où, pour k fixé, l'entier i parcourt l'ensemble des entiers impairs compris entre $-(2^k-1)$ et (2^k-1) . Soit f une arborescence binaire décroissante sur $[n]$ ($n>0$) . Les sommets du graphe de f vont être "placés" sur les points de H . D'abord, le sommet 1 est placé à l'origine. Supposons que tous les sommets de hauteur

h ($h \geq 0$) , c'est-à-dire des sommets x pour lesquels on a $xf^h = 1$ et $xf^{h-1} \neq 1$ si $h > 0$, aient été placés. Soit x un tel sommet. Il a été placé, disons, au point $(i/2^h , h)$ (avec $i = 0$ dans le seul cas où $h = 0$).

Trois cas sont à considérer :

(1) $xf^{-1} \setminus \{x\} = \emptyset$; alors ou bien $f \in S_1$ et le graphe entier (!) de f a été placé, ou bien x est un bout pendant de f ;

(2) $xf^{-1} \setminus \{x\} = \{y\}$; on place alors le sommet y au point $((2i+1)/2^{h+1} , h+1)$;

(3) $xf^{-1} \setminus \{x\} = \{y,z\}$; on pose alors

$X(y) = \{ v \in [n] : vf^k = y , k \geq 0 \}$

$X(z) = \{ v \in [n] : vf^k = z , k \geq 0 \}$.

Les deux ensembles X(y) et X(z) ne sont pas vides, puisqu'ils contiennent y et z . On a alors deux critères de "placement":

le sommet y va en $((2i-1)/2^{h+1} , h+1)$ et z va en $((2i+1)/2^{h+1} , h+1)$ suivant que

(3a) $\max X(y) < \max X(z)$

ou que

(3b) $y = \min X(y) < \min X(z) = z$.

Quelque soit le critère (3a) ou (3b) utilisé, les n sommets du graphe de f ont des abscisses différentes. Soient x , y deux sommets distincts du graphe. On pose $x \underset{a}{<} y$

(resp. $x <_b y$) ssi l'abscisse de x dans H est inférieure à l'abscisse de y dans H , lorsque le critère (3a) (resp. (3b)) est utilisé. On désigne alors par fH_a (resp. fH_b) la suite croissante (par rapport à l'ordre total $<_a$ (resp. $<_b$)) formée par les n sommets de f . De façon géométrique, les suites fH_a et fH_b sont obtenues en projetant verticalement les n sommets du graphe sur l'axe des x . Le lecteur pourra alors vérifier le résultat suivant.

PROPRIÉTÉ 5.5. Les images de $f \in S_n$ ($n>0$) par les bijections $\theta : S \to B$ et $\theta' : S \to A$ sont respectivement données par $f\theta = fH_b$ et $f\theta' = fH_a$.

Nous illustrons seulement ce résultat par un exemple. Les deux graphes de la figure 2 sont les graphes d'une même fonction $f \in S_9$. C'est le critère (3a) qui a été utilisé pour placer les sommets dans le premier, et le critère (3b) dans le second. Lorsqu'on projette les sommets sur l'axe des x dans le premier (resp. le second), on obtient la permutation d'André $f\theta'$ (resp. la permutation d'André de seconde espèce $f\theta$) .

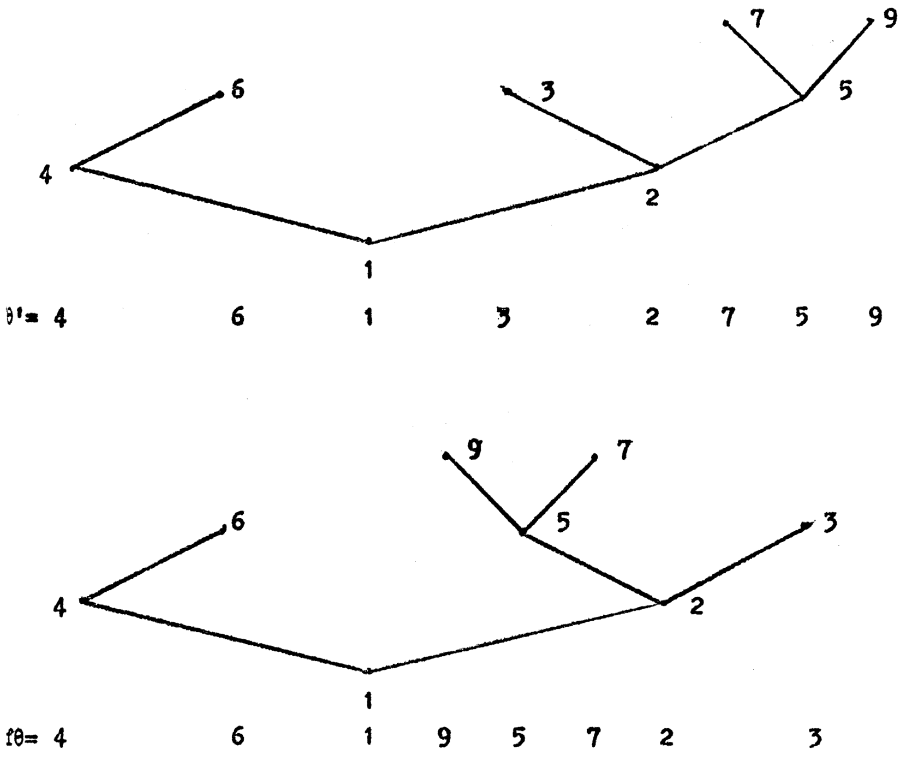


Figure 2.

2. Les permutations alternantes.

C'est André (1879, 1881) lui-même qui a introduit la notion de permutation alternante et qui a montré que le coefficient de $u^n/n!$ dans le développement de tg u + sec u était précisément égal au nombre de permutations alternantes sur [n] .

En fait, comme nous allons le montrer ici, l'ensemble des permutations alternantes est un exemple de complexe d'André. Utilisant tous les résultats du chapitre 4 , on peut donc mettre ces permutations en correspondance biunivoque avec les permutations d'André des deux espèces, ainsi qu'avec les arborescences binaires décroissantes.

L'ensemble X étant toujours un ensemble fini totalement ordonné de cardinal $n>0$, on dit qu'une permutation $f : [n] \to X$ est <u>alternante</u> (resp. <u>alternante montante</u>) sur X ssi l'on a $(2j)f < (2j-1)f$, $(2j+1)f$ (resp. $(2j)f > (2j-1)f$, $(2j+1)f$) pour tout j tel que $0< 2j < n$ et $(n-1)f > nf$ (resp. $(n-1)f < nf$) si, de plus, n est pair. On note $\omega_X : X \to [n]$ l'application strictement croissante de X sur $[n]$. Si f est une permutation alternante sur X , on pose pour tout $i \in [n]$

(5.2) $$i\bar{f} = (n+1-if\omega_X)\omega_X^{-1} \quad .$$

Par exemple, si $X = [n]$, on a $i\bar{f} = n+1-if$. Il est clair que l'application $f \to \bar{f}$ est une bijection de l'ensemble des permutations alternantes sur l'ensemble des permutations alternantes montantes. Pour tout $n>0$, on note E_n l'ensemble des permutations alternantes sur $[n]$. On suppose que E_0 est un singleton $\{e\}$

et l'on pose $E = \bigcup_{n\geq 0} E_n$.

Soit $f \in E_n$ ($n>1$) . Deux cas sont à considérer : (1) $1f^{-1} < nf^{-1}$; (2) $nf^{-1} > 1f^{-1}$. Dans le cas (1), on pose $m = 1f^{-1}$, puis $g_1 = f|[m-1]$, $g_2 = f|([n]\setminus[m])$. Dans le cas (2) , on pose $m = nf^{-1}$, puis $g_1 = f|[m-1]$. La permutation

$$g = mf \cdot (m+1)f \cdot \ldots \cdot nf$$

est alors une permutation alternante sur un ensemble X' qui contient 1 . De plus, la permutation g débute par n . D'après (5.2) , la permutation $\bar{g}$ est alternante montante. Elle débute, de plus, par 1 . On peut donc écrire

$$(5.3) \qquad \bar{g} = 1 \cdot (m+1)g_2 \cdot (m+2)g_2 \cdot \ldots \cdot (n)g_2$$

et la permutation g_2 définie par

$$g_2 = (m+1)g_2 \cdot (m+2)g_2 \cdot \ldots \cdot (n)g_2$$

est une permutation alternante sur l'ensemble $([n]\setminus[m-1])f \cup \{1\}$ Dans les deux cas, on pose, en outre,

$$X_1 = ([m-1])f \quad , \quad X_2 = [n] \setminus (X_1 \cup \{1\}) \text{ , puis}$$

$$f_1 = g_1\omega_{X_1} \quad \text{et} \quad f_2 = g_2\omega_{X_2} .$$

PROPRIÉTÉ 5.6. L'application $\mathcal{E}$ qui envoie l'élément f de E_1 sur la paire $\{(e,\emptyset),(e,\emptyset)\}$ et tout élément f de E_n ($n>1$) sur la paire $\{(f_1,X_1),(f_2,X_2)\}$ est une bijection de E_n sur le composé bipartitionnel $E_n^{(2)}$.

PREUVE. Le caractère injectif est évident. Revenons aux deux cas condisérés pour la définition de g_1 et de g_2 à partir de $f \in E_n$. Comme f est alternante, dans le cas (1), l'entier $m = 1f^{-1}$ est pair et dans le cas (2), l'entier $m = nf^{-1}$ est impair. Considérons donc un élément $\{(f_1,X_1),(f_2,X_2)\}$ de $E_n^{(2)}$ ($n>1$). On peut d'abord supposer que la numérotation a été faite de sorte que n est dans X_2. On pose $g_1 = f_1\omega_{X_1}^{-1}$, $g_2 = f_2\omega_{X_2}^{-1}$. Posons $m-1 = \text{Card } X_1$. Si m est pair, on définit f par

$$f = (1)g_1 \cdot \ldots \cdot (m-1)g_1 \cdot 1 \cdot (1)g_2 \cdot \ldots \cdot (n-m)g_2 .$$

Si m est impair, on transforme d'abord la permutation alternante montante

$$\bar{g} = 1 \cdot (1)g_2 \cdot \ldots \cdot (n-m)g_2$$

en une permutation alternante, en prenant l'inverse de la bijection définie en (5.2). On obtient

$$g = (1)g \cdot (2)g \cdot \ldots \cdot (n-m+1)g$$

qui débute par n puisque n est dans X_2. On pose alors

$$f = (1)g_1 \cdot \ldots \cdot (m-1)g_1 \cdot (1)g \cdot (2)g \cdot \ldots \cdot (n-m+1)g .$$

On a bien là une permutation alternante, car g_1 finit par une descente, puisque $m-1$ est pair. Dans les deux cas, on retrouve $f\mathcal{E} = \{(f_1,X_1),(f_2,X_2)\}$. □

Il résulte donc de la propriété 5.6 que le couple $(E,\mathcal{E})$ est un complexe d'André. En revanche, les applications W_1 et

W_2 n'ont pas sur E d'interprétation évidente.

Donnons une dernière application de l'identité (4.3) de la proposition 4.6 qui comporte un comptage d'une sous-famille de permutations alternantes. Soit w un mot de $\{s,t\}^*$ de la forme $w = t^p$ ($p \geqslant 0$) et soit (Y,φ) un complexe d'André. On pose $c(t^p) = \text{Card } (t^p)W_1^{-1} = \text{Card } (t^p)W_2^{-1}$. On sait que le seul entier $n+2$ pour lequel $Y_{n+2} \cap wW_j^{-1}$ n'est pas vide est donné par $2p = n+2-1$, soit $n = 2p-1$. La formule donne alors immédiatement

$$(5.4) \qquad c(t^p) = \sum_{1 \leq i \leq p} \begin{bmatrix} 2p-1 \\ 2i-1 \end{bmatrix} c(t^{i-1})\, c(t^{p-i}) .$$

Maintenant, les seules permutations f appartenant à $A \cup B$, pour lesquelles on a $fU = t^p$ ($p \geqslant 0$) sont des permutations alternantes. On a donc

$$c(t^p) = \text{Card } A_{2p+1} \cap E_{2p+1} = \text{Card } B_{2p+1} \cap E_{2p+1} \quad (p \geq 0) .$$

La formule (5.4) est donc une formule de récurrence pour le nombre de permutations d'André (resp. d'André de seconde espèce) qui sont aussi alternantes.

3. Tables.

La première table illustre la construction des bijections θ définies en (4.1) et (4.2) dans la section 4.1 .

(1) La première colonne contient la liste des permutations d'André de seconde espèce (voir section 4.3) appartenant aux ensembles B_n pour $1 \leqslant n \leqslant 5$.

(2) Dans la deuxième colonne, on trouve la liste des permutations d'André (voir section 3.2) qui correspondent aux éléments de la première colonne par la bijection $\theta' : B \to A$.

(3) La liste des permutations alternantes en correspondance biunivoque avec les permutations d'André (de la seconde colonne) par la bijection $\theta : A \to E$ est reproduite dans la colonne 3 .

(4) Soient respectivement f , g et h les éléments génériques des éléments des colonnes 1 , 2 et 3 . Comme $f\theta' = g$, on a $fU = fW_1 = gW_2 = gU$. Enfin, puisque $g\theta = h$, il vient $gU = gW_2 = hW_2$. D'où $fU = gU = hW_2$. La quatrième colonne contient donc la valeur commune de ces mots. On rappelle que fU et gU sont les variations réduites (voir section 3.1) des permutations f et g .

La seconde table illustre la construction de la bijection ρ définie en (4.7) (section 4.4) . Les différentes colonnes de la table donnent la valeur des différents paramètres qui interviennent dans la chaîne d'applications (4.7) . La correspondance n'a été établie que pour les permutations d'André de seconde espèce g appartenant à B_n pour $1 \leqslant n \leqslant 6$, pour lesquelles la variation réduite gU n'est pas symétrique.

- 69 -

	B_n	A_n	E_n	
	f	g	h	$fU = gU = hW_2$
n = 1	1	1	1	1
n = 2	12	12	21	s
n = 3	123	123	312	ss
	312	213	213	t
n = 4	1234	1234	4132	sss
	1423	1324	4231	st
	3412	2314	3241	st
	4123	2134	2143	ts
	3124	3124	3142	ts
n = 5	12345	12345	51423	ssss
	12534	12435	51324	sst
	14523	13425	52314	sst
	34512	23415	42315	sst
	15234	13245	53412	sts
	14235	14235	52413	sts
	34125	34125	43512	sts
	45123	24135	42513	sts
	35124	23145	32514	sts
	51234	21345	21534	tss
	41235	41235	41523	tss
	31245	31245	31524	tss
	51423	21435	21435	tt
	53412	32415	32415	tt
	41523	41325	41325	tt
	31524	31425	31425	tt

Table 1.

- 70 -

	gU	g	f	fU	i	j	f'	g'	g'U
l = 4	st	1423	123	ss	2	1	123	4123	ts
	st	3412	312	t	1	2	312	3124	ts
l = 5	sst	12534	1234	sss	3	1	1234	51234	tss
	sst	14523	1423	st	2	3	4213	42135	tss
	sst	34512	3412	st	2	3	3124	31245	tss
l = 6	ssst	123645	12345	ssss	4	1	12345	612345	tsss
	ssst	125634	12534	sst	3	4	51234	512346	tsss
	ssst	145623	14523	sst	3	4	42135	421356	tsss
	ssst	345612	34512	sst	3	4	31245	312456	tsss
	ssts	126345	12345	ssss	3	2	12345	162345	stss
	ssts	125346	12534	sst	4	1	51234	561234	stss
	ssts	145236	14523	sst	4	1	42135	462135	stss
	ssts	345126	34512	sst	4	1	31245	351245	stss
	ssts	156234	15234	sts	2	4	15234	152346	stss
	ssts	146235	14235	sts	2	4	14235	142356	stss
	ssts	346125	34125	sts	2	4	34125	341256	stss
	ssts	456123	45123	sts	2	4	45123	451236	stss
	ssts	356124	35124	sts	2	4	35124	351246	stss
	stt	162534	12534	sst	2	2	51234	516234	tts
	stt	164523	14523	sst	2	2	42135	426135	tts
	stt	364512	34512	sst	2	2	31245	316245	tts
	stt	152634	15234	sts	3	1	15234	615234	tts
	stt	142635	14235	sts	3	1	14235	614235	tts
	stt	341625	34125	sts	3	1	34125	634125	tts
	stt	451623	45123	sts	3	1	45123	645123	tts
	stt	351624	35124	sts	3	1	35124	635124	tts
	stt	561423	51423	tt	1	3	51423	514236	tts
	stt	563412	53412	tt	1	3	53412	534126	tts
	stt	461523	41523	tt	1	3	41523	415236	tts
	stt	361524	31524	tt	1	3	31524	315246	tts

Table 2.

RÉFÉRENCES

D. ANDRÉ (1879), Développements de sec x et de tang x, C.R. Acad. Sc. Paris, 88, pp. 965 - 967.

D. ANDRÉ (1881), Sur les permutations alternées, J. Math. Pures Appl., 7, pp. 167-184.

T.J. BUCKHOLTZ & D.E. KNUTH (1967), Computation of tangent, Euler and Bernoulli numbers, Math. Comp. 21, pp. 663-688.

F.N. DAVID & D.E. BARTON (1962), Combinatorial Chance, Griffin, London.

D. FOATA & M.-P. SCHÜTZENBERGER (1970), Théorie géométrique des polynômes eulériens, Springer-Verlag, Berlin.

W.O. KERMACK & A.G. McKENDRICK (1938), Some properties of points arranged on a Möbius surface, The Math. Gazette, 22, pp. 66-72.

N. NIELSEN (1923), Traité élémentaire des nombres de Bernoulli, Gauthier-Villars, Paris.

C. R. Acad. Sc. Paris, t. 272, p. 420-421 (8 février 1971). Série A

ALGÈBRE. — *Sur un théorème de G. de B. Robinson.* Note (*) de M. **Marcel Paul Schützenberger**, présentée par M. André Lichnerowicz.

On énonce deux propriétés nouvelles permettant de simplifier la correspondance établie par G. de B. Robinson entre permutations et tableaux de Young (1).

Un théorème de G. de B. Robinson (2) établit l'existence d'une bijection entre permutations $\sigma \in \mathfrak{S}_n$ et paires de tableaux (standards de Young) $(\sigma P, \bar{\sigma}^1 P)$ de même forme sur l'ensemble totalement ordonné $[n] = \{1, 2, \ldots, n\}$. On se propose ici de signaler deux propriétés nouvelles de cette correspondance qui permettraient d'en donner une définition plus géométrique.

Dans ce qui suit, on considère un ensemble ordonné fixe $(X, \leq)$ et pour chaque intervalle fini I de $\mathbf{Z}$, on désigne par $\Phi(I)$ la famille des injections $\varphi : I \to X$ telles qu'il existe un morphisme (d'ensemble ordonné) $\rho : X \to \mathbf{Z}$ pour lequel $\varphi = \bar{\rho}^1 \mid I$. Ceci implique que l'image $I\varphi$ soit un intervalle de X $(x, x' \in I\varphi,\ x \leq x'' \leq x' \Rightarrow x'' \in I\varphi)$ et on dira que φ est *principale* (resp. *coprincipale*), si et seulement si, il en est de même de $I\varphi$, c'est-à-dire, si et seulement si, $I\varphi$ a un élément minimal (resp. maximal) (unique).

Notant Φ l'union des $\Phi(I)$ sur tous les intervalles finis de $\mathbf{Z}$ on définit aussi une relation $\mathfrak{R}_1 \subset \Phi \times \Phi$ par la condition que $(\varphi, \psi) \in \mathfrak{R}_1$, si et seulement si,

(1) φ et ψ ont même domaine;

(2) $\varphi \leq \psi$ (c'est-à-dire $i \in I \Rightarrow i\varphi \leq i\psi$);

(3) $2 = \mathbf{Card}\,((I\varphi \cup I\psi) \setminus (I\varphi \cap I\psi))$.

On désigne par $\mathfrak{R}$ la relation d'ordre fermeture de transitivité de $\mathfrak{R}_1$ et on vérifie que tout coidéal $\varphi\mathfrak{R}^{-1} (= \{\psi \in \Phi : (\psi, \varphi) \in \mathfrak{R}\})$ contient au moins un élément principal, si et seulement si,

(4) Toute partie finie de X est contenue dans un intervalle principal fini.

Supposons maintenant que $(X, \leq)$ est le groupe $\mathbf{Z}^k$ ordonné de façon naturelle, ce qui implique (4). On considère le quotient $\bar{\Phi}$ de Φ par l'équivalence de translation $\sim$ ($\varphi \sim \varphi'$ ssi il existe $t \in \mathbf{Z}^k$ tel que $\varphi' = t + \varphi$) et on note $\bar{\mathfrak{R}}$ le préordre sur $\bar{\Phi}$ induit par $\mathfrak{R}$. Les énoncés substantiels de la théorie ne sont vrais que dans le cas classique de $k = 2$ auquel nous nous limitons désormais. Les tableaux de Young sont alors les éléments principaux de $\bar{\Phi}([n])$ $([n] = \{1, 2, \ldots, n\},\ n \in \mathbf{N})$ et la propriété que nous avons en vue est la suivante :

Propriété 1. — *Toute classe* $S \subset \bar{\Phi}$ *de l'équivalence fermeture de* $\bar{\mathfrak{R}} \cup \bar{\mathfrak{R}}^{-1}$ *contient exactement un élément principal* (*noté* S^p) *et la* $\bar{\mathfrak{R}} \cap \bar{\mathfrak{R}}^{-1}$*-classe de celui-ci est l'élément minimal de* S *pour* $\bar{\mathfrak{R}}$.

Pour rattacher ceci au théorème de G. de B. Robinson, considérons les deux projections $\pi_i : \mathbf{Z}^2 \to \mathbf{Z} (i = 1, 2)$ et notons qu'à chaque $\varphi \in \Phi([n])$ et $i = 1$ ou 2 correspond une et une seule surjection $\hat{\varphi}_i : [n] \to [m_i]$ (où $m_i = \mathbf{Card}([n]\varphi\pi_i)$ telle qu'il existe un morphisme surjectif $\zeta_i : \mathbf{Z} \to [m_i]$ satisfaisant $\hat{\varphi}_i = \varphi\pi_i\zeta_i (i = 1, 2)$. On écrira $\varphi \in \Phi_i$ ssi $\hat{\varphi}_i$ est une permutation (c'est-à-dire, si et seulement si, $m_i = n$).

Propriété 1 *bis*. — *Soit* S *comme ci-dessus. L'ensemble des permutations admettant* S^p *comme tableau de Robinson est précisément* $\{ \hat{\varphi}_2 : \varphi \in S \cap \Phi_2 \}$.

Le corollaire suivant correspond au cas où S consiste en une seule $\overline{\mathfrak{R}} \cap \overline{\mathfrak{R}}^{-1}$-classe et où les permutations telles que $\sigma P = S^p$ admettent une description particulièrement transparente [*cf.* (3), p. 120].

Corollaire 2. — *Soient* $n = pq$ *et* $\varphi \in \Phi([n])$ *tels que* $[n]\varphi = [p] \times [q]$. *Pour chaque* $\sigma \in \mathfrak{S}_n$ *tel que* $\sigma P = \varphi$ *la permutation* $\bar{\sigma}$ *définie par*

$$j \in [n] \Rightarrow j\bar{\sigma} = (n + 1) - (n + 1 - j)\sigma$$

satisfait $\bar{\sigma} P = \bar{\varphi}$ *où* $\bar{\varphi} \in \Phi([n])$ *est définie par*

$$j \in [n] \Rightarrow j\bar{\varphi} = (p + 1, q + 1) - (n + 1 - j)\varphi.$$

(*) Séance du 1er février 1971.

(1) Je profite de cette occasion pour m'excuser d'avoir commis dans une publication antérieure une attribution incorrecte de ce résultat par ignorance du Mémoire (2) de G. de B. Robinson.

(2) G. de B. Robinson, *Amer. J. Math.*, 60, 1938, p. 745-760.

(3) D. E. Knuth, *Pacific J. Math.*, 34, 1970, p. 709-727.

(9, *villa Poirier*, 75-*Paris*, 15e.)

ARTICLE EXTRAIT DES ACTES DU CONGRÈS INTERNATIONAL DES MATHÉMATICIENS

NICE - SEPTEMBRE 1970

ARTICLE FROM THE PROCEEDINGS OF THE INTERNATIONAL CONGRESS OF MATHEMATICIANS

NICE - SEPTEMBER 1970

GAUTHIER-VILLARS ÉDITEUR
55, quai des Grands-Augustins, Paris 6e
1971

Actes, Congrès intern. Math., 1970. Tome 3, p. 281 à 282.

PARTIES RATIONNELLES D'UN MONOIDE LIBRE

Par M. P. SCHUTZENBERGER

On résume certains résultats obtenus avec S. Eilenberg avec l'étude des *parties rationnelles* du monoïde libre X^* engendré par l'ensemble fini X. Par *partie*, A, on entend ici une fonction $A : X^* \to N$, c'est-à-dire une série formelle (à coefficients dans N) en les variables (non commutatives) $x \in X$. La famille des parties rationnelles **Rat** (X) est la plus petite famille **R** telle que :

(1) $$\{0\} \in \mathbf{R} \; ; s \in X^* \Rightarrow \{s\} \in \mathbf{R}$$

(2) $$A, B \in \mathbf{R} \Rightarrow A + B \in \mathbf{R} \quad \text{et} \quad A\,B \in \mathbf{R} \; ;$$

(3) $$A \in \mathbf{R}, A(0) = 0 \Rightarrow A^* = 1 + \sum_{0<n} A^n \in \mathbf{R}.$$

On sait que $A : X^* \to N$ appartient à **R** ssi il existe $k \in N$ et une représentation $\mu : X^* \to N^{k \times k}$, telle que pour chaque $s \in X^*$, la valeur $A(s)$ du coefficient de s dans A soit l'élément (s, k) de la matrice $s\mu$. On peut montrer que pour $A \in$ **Rat** (X) donné on peut choisir k et μ de telle sorte que tous les éléments de $x\mu$ $(x \in X)$ soient 0 ou 1. Le plus petit $k \in N$ pour lequel ceci est possible est le *nombre d'états* de A.

THEOREME 1. – *Soient donnés* $A, B \in$ **Rat** (X) *de nombre d'états* $\leqslant k$. *L'égalité* $A = B$ *est décidable. L'inégalité* $A \leqslant B$ *(c'est-à-dire* $s \in X^* \Rightarrow A(s) \leqslant B(s)$*) est indécidable.*

Soient maintenant p un entier positif et $A \in$ **Rat** (X). Les relations

$$A = p\,B + C, C \leqslant p\,X^*$$

définissent de façon unique deux parties $B, C : X^* \to N$. Généralisant un théorème bien connu de Kronecker, on a :

THEOREME 2. – B *et* C *appartiennent à* **Rat** (X^*).

La démonstration utilise le résultat suivant :

THEOREME 3. – *Soient* $F, G \in$ **Rat** (X^*) *où* G *est bornée (c'est-à-dire Sup* $\{G(s) : s \in X^*\} < \infty$*). Alors* $F \dot{-} G \in$ **Rat** (X^*) *où* $H = F \dot{-} G$ *est définie par*

$$s \in X^* \Rightarrow H(s) = \text{Max}\,\{0, F(s) - G(s)\}.$$

Des contre exemples montrent que l'hypothèse G bornée est effectivement nécessaire dans cet énoncé, et qu'en particulier $F, G \in$ **Rat** (X), $G \leqslant F$ n'implique pas $F \dot{-} G \in$ **Rat** (X^*).

Généralisant la notion de produit de Hadamard, définissons maintenant pour $A, B : X^* \to N$, leur "intersection" $G = A \cap B$ par la condition

$$s \in X^* \Rightarrow G(s) = A(s)\,B(s).$$

On sait que $A, B \in \mathbf{Rat}\ (X) \Rightarrow A \cap B \in \mathbf{Rat}\ (X)$. Le "problème inverse" n'est pas résolu (même dans le cas classique des fonctions rationnelles dont la série de Taylor a ses coefficients dans Z) et nous proposons les

CONJECTURES (1). – Si $A, A \cap B \in \mathbf{Rat}\ (X)$, il existe $C \in \mathbf{Rat}\ (X)$ telle que $A \cap B = A \cap C$;

(2). – Si $A \cap A \in \mathbf{Rat}\ (X)$ il existe $B \in \mathbf{Rat}\ (X)$ telle que $A \cap A = B \cap B$.

Faculté des Sciences de Paris
Institut de Programmation
9, Quai Saint-Bernard,
Paris 5e
France

Séminaires IRIA

logique et automates

1971

LE THÉOREME DE LAGRANGE SELON G.N. RANEY

M.P. Schützenberger

Soit $F(z) = \sum_{0<k} a_k z^k$ $(a_k \in \mathbb{R}\ ,\ a_k \geq 0)$ une série formelle. La formule de Lagrange affirme que la série formelle

$$\sum_{1\leq k} \frac{t^k}{k!} \left[\frac{\partial^{k-1}}{\partial t^{k-1}} (F(t))^k\right]_{t=0}$$

est la solution (à coefficients dans $\mathbb{R}$, s'annulant pour $t = 0$) de l'équation $z = tF(z)$.

Ce résultat s'établit classiquement par les méthodes de la théorie des fonctions analytiques. Une preuve élémentaire n'utilisant que des manipulations de séries formelles non commutatives à coefficients dans $\mathbb{N}$ est dûe à Raney (1960) (Functional composition patterns and power series reversion. Trans. American Math. Soc. 94 pp. 441-451). On en donne ici une rédaction allégée.

Soit désormais $X = \{x_k : k \in \mathbb{N}\}$ une famille de variables non commutatives et soit σ le morphisme dans $\mathbb{Z}$ du monoïde libre X^* envoyant chaque x_k sur $k-1$. La partie L de X^* définie ci-dessous généralise le langage de Lukasiewicz auquel elle se réduit en faisant $L \to L \cap \{x_0, x_2\}^*$.

Définition : L est la famille des mots $f \in XX^*$ tels que :

i. $f\sigma = -1$

ii. $f' \in XX^*$, $f \in f'XX^* \Rightarrow f'\sigma \geq 0$.

Propriété 1 : Pour chaque $p \in \mathbb{N}$

(1) tout mot de X^* a au plus un facteur gauche dans L^p .

(2) tout mot $f \in X^*$ tel que $f\sigma \leq -p$ a un facteur gauche dans L^p .

(3) L^p est la famille des mots f tels que :

(i') $f\sigma = -p$;

(ii') $f' \in XX^*$, $f \in f'XX^* \Rightarrow f'\sigma > -p$.

Preuve : L'énoncé est trivial pour $p = 0$ puisque pour toute partie A de X^* , A^0 est l'élément neutre 1 de X^* . Soit désormais p positif. L'assertion (1) résulte par induction sur p du cas où $p = 1$, qui est lui même une conséquence immédiate de la définition puisque celle-ci entraîne $LXX^* \cap L = \phi$, d'après ii. Soit $f \in X^*$ tel que $f\sigma = -p$ et soit g le plus court facteur gauche de f tel que $g\sigma < 0$. Comme $x_k\sigma \geq 0$ pour tout $k \geq 1$, on a $g = g'x_o$ où $g'\sigma = g\sigma + 1$ puisque $x_o\sigma = -1$. Donc, d'après l'hypothèse de minimalité de g on a d'abord $g'\sigma \geq 0$, donc, de fait $g'\sigma = g\sigma + 1 = 0$, ensuite $g''\sigma \geq 0$ pour tout facteur gauche g'' de g' . Par conséquent $g \in L$.

Définissant $f_1 \in X^*$ par $f = gf_1$, on a $f_1\sigma = f\sigma - g\sigma = -p+1$, ce qui établit l'assertion (2) par induction sur p .

Vérifions maintenant (3) . Soit $f = g_1g_2 \cdots g_p$ où $g_1, g_2, \ldots, g_p \in L$. Tout facteur gauche propre f' de f a la forme $f' = g_1g_2 \cdots g_{p'}g'$ où $p' \leq p-1$ $g_{p'+1} = g'g''$, $g'' \in XX^*$. Donc d'après la définition de L , $g'\sigma \geq 0$ et $f'\sigma = -p' + g'\sigma > f\sigma = -p$, ce qui montre que tout $f \in L^p$ satisfait (i') et (ii').

Réciproquement, si $f \in X^*$ satisfait ces relations, l'assertion (2) implique $f = f'f''$ où $f' \in L^p$ et la condition (ii') entraîne $f = f' \in L^p$ puisque $f'\sigma = -p = f\sigma$.

Identifions maintenant L à l'élément correspondant $L = \Sigma\{f : f \in X^*\}$ de l'algèbre large de X^*.

Propriété 2 : L est défini par l'équation :

$$L = \sum_{0\leq k} x_k L^k .$$

Preuve : D'après la proposition 1 (1), chaque mot de X^* admet au plus une factorisation de la forme $x_k g$ $(g \in L^k)$. Il suffit donc de montrer l'égalité des ensembles L et $\bigcup_{0\leq k} x_k L^k$.

Soit $f = x_k g$ où $g \in L^k$. Si $k = 0$ on a $g = 1$ et la conclusion $x_o \in L$ résulte de la définition de L. Si $k \geq 1$ on a $f\sigma = x_k\sigma + g\sigma = k-1-k = -1$. D'autre part, si $f' \in XX^*$ est facteur gauche propre de f, on a $f' = x_k g'$ où $x_k\sigma \geq 0$ et où $g'\sigma \geq -k+1$ puisque g' est facteur gauche propre de g. Donc $f'\sigma = x_k\sigma + g'\sigma = k-1+g'\sigma \geq 0$ prouvant $f \in L$ donc $\bigcup_{0\leq k} x_k L^k \subset L$.

Réciproquement, soit $f = x_k g \in L$ $(x_k \in X , g \in X^*)$. On a par hypothèse $f\sigma = k-1+g\sigma = -1$, $f'\sigma = k-1+g'\sigma \geq 0$ pour tout facteur gauche propre $f' = x_k g'$ de f. La première relation entraîne $g\sigma = -k$ et la seconde $g'\sigma \geq -k+1$. On a donc $g \in L^k$ d'après la proposition 1 (3) ce qui établit $L \subset \bigcup_{0\leq k} x_k L^k$.

Remarque : On vient de prouver l'existence de la solution. Son unicité (parmi les éléments de l'algèbre large de X^* sur $\mathbb{Z}$) est une conséquence facile du résultat (facile) d'existence et unicité des langages algébriques.

Propriété 3 : Pour tout k positif, chaque mot $f \in X^* \cap (-k)\bar{\sigma}^{-1}$ admet exactement k factorisations distinctes $f = f'_j f''_j$ $(f''_j \neq 1)$ telles que $f''_j f'_j \in L^* \left(= \bigcup_{0\leq p} L^p\right)$.

Preuve : Considérons d'abord un mot $f = g_1 g_2 \ldots g_k \in L^k$ $(g_1, g_2, \ldots, g_k \in L)$. Les k factorisations $f'_j = g_1 \ldots g_{j-1}$ $f''_j = g_j \ldots g_k$ $(j=1,2,\ldots,k ; f'_1 = 1 , f''_1 = f)$ satisfont trivialement $f''_j f'_j \in L^k$. Toute autre factorisation de f a la forme

$f'_j = g_1 \cdots g_{j-1}g' = h'g'$ $f''_j = g''g_{j+1} \cdots g_k = g''h''$ avec $g'g'' = g_j$, $g'' \neq 1, g_j$.

D'après la définition de L on a $g'\sigma \geq 0$, et par conséquent $g''\sigma = -1 - g'\sigma \leq -1$. Il en résulte que le facteur gauche $g''h''h'$ propre de $f''_j f'_j$ satisfait

$$g''h''h'\sigma = g''\sigma - (k-1) \leq f''_j f'_j \sigma = -k .$$

Donc d'après (3) ci-dessus $f''_j f'_j \notin L^*$ ce qui établit l'énoncé dans le cas considéré.

Considérons maintenant un $f \in X^* \cap (-k)\bar{\sigma}^{-1}$ quelconque. Il suffit de montrer $f = f'f''$ où $f''f' \in L^k$. Définissons f' par la condition que $f'\sigma \leq h\sigma$ pour tout facteur gauche h de f et que f' soit le plus court facteur gauche pour lequel ce minimum soit atteint.

La première partie de la condition implique $g\sigma \geq 0$ pour tout facteur gauche g . Il suffit maintenant de montrer que tout mot $f \in (-k)\bar{\sigma}^{-1}$ a une factorisation $f'f''$ telle que $f''f' \in L^k$.

Déterminons f' par la double condition que $f'\sigma \leq h\sigma$ pour tout facteur gauche h de f et que f' soit le plus court facteur ayant cette propriété.

La première partie de la condition entraîne que $f'\sigma \leq f\sigma = -k$ et que $g\sigma \geq 0$ pour tout facteur gauche g de f'' $(f'f'' = f)$. La deuxième partie implique $g'\sigma > f'\sigma$ pour tout facteur gauche propre g' de f' . Distinguant deux cas selon la longueur relative de h' et de f'' pour tout facteur gauche propre h' de $f''f'$, on en conclut que $h'\sigma > f''f'\sigma = -k$, donc, d'après (3) que $f''f' \in L^k$.

Corollaire 4 : Pour tout $m,k \geq 1$, on a

$$\text{Card}\,(X^m \cap L^k) = m^{-1}k\,\text{Card}\,(X^m \cap (-k)\bar{\sigma}^{-1}) .$$

Preuve : La classe de conjugaison d'un mot $f = y_1y_2 \cdots y_m \in X^m$ $(y_1,y_2,\ldots,y_m \in X)$ est l'ensemble des mots distincts de la forme $y_jy_{j+1} \cdots y_my_1 \cdots y_{j-1}$. Si $f = g_1g_2 \cdots g_k \in L^k$, sa classe de L-conjugaison est l'ensemble des mots distincts $g_ig_{i+1} \cdots g_kg_1 \cdots g_{i-1}$

$(g_1, g_2, \ldots, g_k \in L)$.

Il est clair que la classe de conjugaison de f contient m' mots distincts ssi d'une part $m'^{-1}m = q \in \mathbb{N}$ et d'autre part sa classe de L-conjugaison contient $k' = q^{-1}k$ mots distincts.

La formule résulte alors de la proposition 3 qui établit une bijection entre les classes de conjugaison et de L-conjugaison.

Soit maintenant t une nouvelle lettre et soit $\mathbb{C}$ l'algèbre large du monoïde commutatif libre engendré par $\{t\} \cup X$. Nous posons

$$F(t) = F = \sum_{0 \leq k} x_k t^k \in \mathbb{C}$$

et nous désignons par $\frac{\partial}{\partial t}$, la dérivation de $\mathbb{C}$ envoyant chaque t^n sur nt^{n-1} $(n \in \mathbb{N})$. Le morphisme naturel de X^* dans $\mathbb{C}$ sera noté α .

Formule 5 : Pour chaque $m, k \geq 1$

$$(X^m \cap L^k)\alpha = (m!)^{-1} \left[\frac{\partial^{m-1}}{\partial t^{m-1}} (kt^{k-1}(F(t))^m) \right]_{t=0} .$$

Preuve : Soit $\tau : X^* \to \mathbb{C}$ le morphisme envoyant chaque x_k sur $x_k t^k$, et par conséquent chaque $f \in X^n$ sur $f\alpha \cdot t^{n+f\sigma}$.

Comme $F(t) = X\tau$ on a donc identiquement

$$(F(t))^m = \sum_{0 \leq q} t^q \cdot (X^m \cap (q-m)\bar{\sigma}^{-1})\alpha .$$

Par conséquent, le membre de droite de la formule qui, par définition est égal à $(m!)^{-1} \times k \times$ (le coefficient de t^{m-1} dans $t^{k-1}(F(t))^m$) $\times (m-1)!$, c'est-à-dire à $m^{-1}k \times$ (le coefficient de t^{m-k} dans $(F(t))^m$) , se trouve être précisément $m^{-1}k(X^m \cap (m-k-m)\bar{\sigma}^{-1})\alpha = m^{-1}k(X^m \cap (-k)\bar{\sigma}^{-1})\alpha$, ce qui établit la formule d'après le corollaire 4.

Nous en venons maintenant à la preuve de la formule de Lagrange que nous établissons sous la forme plus générale de Bürmann (cf. Pólya et Szegö II. p. 125). Dans cette dernière $H(t) = \sum_{0 \leq k} h_k t^k$ $(h_k \in \mathbb{R})$ est une série formelle quelconque et l'on cherche $H(u)$ où u est la solution de

$u = tF(u)$.

Formule de Lagrange Bürmann.

$$H(u) = h_o + \sum_{1\leq m} \frac{t^m}{m!}\left[\frac{\partial^{m-1}}{\partial t^{m-1}}\left(\frac{\partial H(t)}{\partial t} \cdot (F(t))^m\right)\right]_{t=0} .$$

Preuve : Posons

$$L_q(t) = \sum_{1\leq m} t^m \cdot (X^m \cap L^q)\alpha \qquad (q \in \mathbb{N})$$

de telle sorte que

$$L_q(t) = L^q\theta = (L\theta)^q$$

où $\theta : X^* \to \mathbb{Q}$ désigne le morphisme envoyant chaque x_k sur tx_k .

Appliquant θ aux deux membres de l'équation

$$L = \sum_{0\leq k} x_k L^k$$

de la proposition 2 , on voit que $u = L_1(t) = L\theta$ satisfait l'équation

$$u = tF(u) .$$

$(F(u) = \sum_{0\leq k} x_k u^k)$.

D'autre part, d'après

$$\frac{\partial H(t)}{\partial t} = \sum_{1\leq q} q h_q t^{q-1} ,$$

le membre de droite de la formule peut s'écrire :

$$h_o + \sum_{1\leq q} h_q \sum_{1\leq m} \frac{t^m}{m!}\left[\frac{\partial^{m-1}}{\partial t^{m-1}} q t^{q-1}(F(t))^m\right]_{t=0}$$

c'est-à-dire, d'après la formule 5 ,

$$h_o + \sum_{1\leq q} h_q \sum_{1\leq m} t^m (X^m \cap L_q)\alpha$$

et enfin

$$h_o + \sum_{1\leq q} h_q L_q = h_o + \sum_{1\leq q} h_q \cdot (L\theta)^q$$

c'est-à-dire $H(L\theta)$.

Formule de L.-B.- Tutte (1963). (Canadian J. of Math. 15 pp. 249-271)

Soit s une nouvelle variable commutative. Définissons les séries formelles $F_t(s)$ et $H_t(s)$ par

$$F_t(s) = F(t+s)$$

$$H_t(s) = H(t+s) .$$

D'après la formule de Lagrange Bürmann on a :

$$H_t(u) = h_o + \sum_{1\leq m} \frac{t^m}{m!} \left[\frac{\partial^{m-1}}{\partial s^{m-1}} \left(\frac{\partial H_t(s)}{\partial s} (F_t(s))^m\right)\right]_{s=0}$$

où $u = tF_t(u)$ puisque le nom des variables employé dans les dérivations importe peu.

Comme $\frac{\partial^{m-1}}{\partial t^{m-1}} G(t)$ est égal à $\left[\frac{\partial^{m-1}}{\partial s^{m-1}} G(t+s)\right]_{s=0}$ pour toute série formelle G, la formule ci-dessus peut encore s'écrire :

$$H(t+u) = h_o + \sum_{1\leq m} \frac{t^m}{m!} \frac{\partial^{m-1}}{\partial t^{m-1}} \left(\left(\frac{\partial}{\partial t} H(t)\right)(F(t))^m\right)$$

où $u = tF(t+u)$.

Posant maintenant $t+u = v$, nous obtenons enfin la formule de Tutte :

$$H(v) = H(t) + \sum_{1\leq m} \frac{t^m}{m!} \frac{\partial^{m-1}}{\partial t^{m-1}} \left(\left(\frac{\partial}{\partial t} H(t)\right)(F(t))^m\right)$$

où v est définie par $v = t + tF(v)$.

ON McNAUGHTON'S COUNTER FREE LANGUAGES

M. P. SCHUTZENBERGER*

LABORATORIO DI CIBERNETICA DEL C. N. R.

ARCO FELICE - NAPOLI

ON McNAUGHTON'S COUNTER FREE LANGUAGES

M. P. SCHUTZENBERGER*

Laboratorio di Cibernetica del C.N.R. - Arco Felice (Napoli)

* Permanent address: Université de Paris VII and
Institut de Recherche en Informatique et Automatiq
Rocquencourt (France)

1. Introduction.

The family $\underline{A}_o$ of counter free language has been introduced long ago by Mc Naughton in connection with problems in Logic. It is the least family of subsets of the free monoid X^* that is closed under boolean operations and (set) product and that contains X^* and every subset of the alphabet X. In equivalent fashion it is the family of all subsets of X^* such that their syntactic monoid is finite and has no non trivial groups. Many further results can be found in the recent book of Mc Naughton and Pappert entitled "Counter free Automata". Some of the findings of these authors suggest generalizations and we propose here to examine one possible extension.

In what follows Π will be a fixed non empty set of positive integers that contains any divisor of its members and that is closed under the least common multiple (l.c.m.) operation. In equivalent manner Π can be defined by a partial function π into $\underset{\sim}{N}$ of the set of all primes. Then it contains every positive integer n such that for each prime p in the domain of π, the highest power of p dividing n is at most p^{π}.

We shall denote by $\underline{M}_\Pi$ the family of all finite monoid such that the order of the cyclic group in them belongs to Π. Since any group of a quotient monoid is itself a quotient of a group in the original monoid, $\underline{M}_\Pi$ contains any quotient monoid of its member. Finally $\underline{A}_\Pi$ will denote the family of all sets

in X^* whose syntactic monoid is in $\underline{M}_\pi$. One might may be call $\underline{A}_\pi$ a "periodic family" (with "period set" Π) but it is probably premature to give a name to a notion whose interest remains to be demonstrated.

Let us consider some examples. If $\Pi = \{1\}$, (i.e. if $p\pi = 0$ for every prime p) we have simply Mc Naughton's family $\underline{A}_0$. At the other extreme, if Π contains every positive integers, (i.e. if the domain of the function π is empty), $\underline{A}_\pi$ is simply Eilenberg's family $\underline{Rec}$ of all recognisable sets, i.e. of all sets whose syntactic monoid is finite. Families $\underline{M}_\pi$ where Π is closed under multiplication have been the object of deep investigations by B. Tilson within the framework of J. Rhodes' complexity theory. However the notions we shall be using here are unable to characterise these especially interesting types of sets Π. Further, the families $\underline{M}_\pi$ which we shall consider will fail in general to be closed under wreath product.

Anticipating upon Section 2, we give two other alternative definitions.

1.1. A recognizable set A belongs to $\underline{A}_\pi$ iff in equivalent fashion :

(i) For any words $f,g,h \in X^*$ such that $A \cap fh^*g$ is infinite, one has $fh^p(h^r)^*g \subset A$ for somme $p \in \underset{\sim}{N}$ and $r \in \Pi$.

(ii) For any words $f,g,h \in X^*$ and positive integer t such that $f(h^t)^*g \subset A$, one has $fh^p(h^s)^*g \subset A$ for some $p \in \underset{\sim}{N}$ and divisor $s \in \Pi$ of t.

We return to our main argument. It is clear that each family $\underline{M}_\pi$ is closed under direct product. Therefore $\underline{A}_\pi$ is closed under boolean operations and since $\{1\} \in \Pi$ for any Π, it contains $\underline{A}_o$. Since for any recognisable set $A,B \subset X^*$ each group in $Synt(AB)$ is a subdirect product of groups in $Synt(A)$ and $Synt(B)$, we have also that each family $\underline{A}_\pi$ is closed under product.

To proceed we need two more notions. First for each Π, we define the family $\underline{P}_\pi$ of the submonoids P of X^* which satisfy the condition

$(\underline{P}_\pi)$ $\quad h \in X^+$, $h^+ \cap P \neq \phi \Rightarrow h^r \in P$ for at least one $r \in \Pi$, where $X^+ = XX^* = X^*\backslash 1$, $h^+ = hh^* = h^*\backslash 1$ denotes the semigroups generated by X and by h.

This condition is vacuous iff Π contains every positive integer. When $\Pi = \{1\}$ one says at times in group theory that a subgroup which satisfies it is pure.

Second, along a different line, we recall that a subset A of X^* is a basis iff every word in X^* has at most one factorisation as a product of words from A. This requirement is satisfied when A is prefix, i.e. when $1 \notin A$ and $AX^+ \cap A = \phi$.

With this terminology explained we can now state our "Main Property".

- 4 -

Main Property.

For each Π and any subset A of X^+ one has :

(1) $A \in \underline{A}_\Pi$, $A^* \in \underline{P}_\Pi \Rightarrow A^* \in \underline{A}_\Pi$

and, reciprocally,

(2) A , a basis, $A^* \in \underline{A}_\Pi \Rightarrow A^* \in \underline{P}_\Pi$.

Therefore, when $A \in \underline{A}_\Pi$ is prefix one has $A^* \in \underline{A}_\Pi$ iff $A^* \in \underline{P}_\Pi$. This will be verified in Section 3. In Section 4, we shall give for the sake of completeness a proof of a (weakened form of a) Theorem of Eilenberg which we state now in the manner most suitable for our present goal. Here $\underline{M}$ is an arbitrary family of finite monoids containing the quotient of its members and $\underline{A}$ is the corresponding family of sets in X^* whose syntactic monoid is in $\underline{M}$. We recall that a product AB $(A,B \in X^*)$ is unambiguous iff each word in X^* has at most one factorisatio ab with $a \in A$, $b \in B$.

Theorem (Eilenberg) : Assume $\{1\} \in \underline{A}$ and that $\underline{A}$ is clos under boolean operations and product. Then $\underline{A}$ is equal to the least family $\underline{B}$ of subset of X^* that satisfies the two conditions :

(i) $\underline{B}$ contains every subset of X and it is closed under disjoint union and unambiguous product.

(ii) $\underline{B}$ contains every submonoid A^* such that $A \in \underline{B}$, A is prefix and $A^* \in \underline{A}$.

It is clear that any of our families $\underline{A}_\pi$ satisfies these conditions. Therefore, replacing in the theorem $\underline{A}$ by $\underline{A}_\pi$ and substituting in (ii), $A^* \in \underline{A}_\pi$ by $A^* \in \underline{P}_\pi$, which is allowed by the "Main Property", we get as a corollary an unambiguous expression of the members of $\underline{A}_\pi$.

The next section is devoted to recalling some known facts concerning cyclic groups in finite monoids and to a formal verification of 1.1 above. It will appear that some of the results do not depend upon the finiteness of Synt(A) or of its groups but only upon the finiteness of the orders of the one generators submonoids.

2. Alternative definitions.

In this section we consider a fixed recognisable set A in X^*. Its syntactic monoid will be denoted by S and we shall let $\alpha : X^* \to S$ be its syntactic morphism. We recall that for any $h,h' \in X^*$ one has $h\alpha = h\alpha'$ iff for each $f,g \in X^*$ the pair $\{fhg, fh'g\}$ is contained in A or in $X^* \setminus A$.

Therefore α is as well the syntactic morphism of $X^* \setminus A$ and all what will be said below could be dualised in this fashion. Since S is finite by hypothesis, the subsemigroup $(h\alpha)^+$ is finite for each $h \in X^*$. It contains a cyclic group H whose order will be written $\omega(h)$, or, when needed, $\omega(h,A)$.

For the same reason of finiteness, there is a number $p = p_A \in \underset{\sim}{N}$ such that $h^n\alpha$ is in its cyclic group for all $n \geq p$, irrespectiv of the element $h \in X^*$.

We now recall some known trivia. In what follows h is a fixed word in X^*.

2.1. For each pair $f,g \in X^*$, there is a divisor $s = \omega(h,f$ of the order $\omega(h)$ such that for any $t \geq 1$ and $n \in \underset{\sim}{N}$, the relation $fh^n(h^t)^*g \subset A$ implies $fh^m(h^s)^*g$ where m is the least integer $\geq p_A$ which is congruent to n modulo $\omega(h)$.

Proof : For each positive multiple r' of $\omega(h) = r$ that is larger than p_A, $h^{r'}\alpha$ is the idempotent of the group H. Therefore for all $m \geq p_A$ one has $h^m\alpha = h^{m+r}\alpha$.

Let K be the subset of the elements $a \in H$ such that $f\alpha.a.g\alpha$ is in $A\alpha$. There is a largest subgroup G such that $KG = K$. Letting $s = (\text{Card } H)(\text{Card } G)^{-1}$ be the index of G in H, we see that s is a divisor of t and of $\omega(h)$ and the result follows. Q.E.D.

We have proved the statement (ii) in the alternative definition 1.1, since the hypothesis $A \in \underset{\sim}{A_\Pi}$ is equivalent with $\omega(A) \in \Pi$ where $\omega(A)$ is the l.c.m. of the numbers $\omega(h)$, we have also proved (i). Indeed, we have shown that for each f,g,h the set of all $n \in \underset{\sim}{N}$ such that $fh^ng \in A$ is a union of a finite set and of arithmetic progressions of ratio $\omega(A)$. Because of

of the duality between A and $X^*\backslash A$ it is natural to set $\omega(h,f,g)$ when $fh^*g \cap A$ is finite.

2.2. The order $\omega(h)$ is the l.c.m. r of the numbers $\omega(h,f,g)$ overall pairs $f,g \in X^*$.

Proof : We have already seen that $\omega(h)$ is a multiple of every $\omega(h,f,g)$. It remains to check that is is exactly equal to r , i.e. that $h^m\alpha = h^{m+r}\alpha$ for all large enough m . However this is trivial because of the definition of α as the syntactic morphism of A since we have already $fh^ng \in A$ iff $fh^{n+s}g \in A$ for all large enough n , for each f,g and $s = \omega(h,f,g)$.

Q.E.

Another definition of $\underline{A}_{\pi}$ is suggested by Eilenberg's definition of $\underline{A}_o$.

2.3. Let A be a recognisable set. It belongs to $\underline{A}$ iff there is a $r \in \Pi$ such that for any $f,g,h \in X^*$ the set $f(h^r)^*g$ has a finite intersection with A or with $X^*\backslash A$. .

Proof : If $A \in \underline{A}_{\pi}$, we can take $r = \omega(A)$. Conversely if the condition is satisfied we have that $\omega(A) = r$ because $\omega(A)$ is the l.c.m. of the numbers $\omega(h,f,g)$ over all triples $f,g,h \in X^*$.

Q.E.

I submitt another similar definition. Let $\underline{\underline{S}}$ denote the family of all infinite sequences $\underline{s} = \{ s_n : n \in \underset{\sim}{N}\}$ of words $s_n \in X^*$ such that $s_n = 1$ for an infinity of $n \in \underset{\sim}{N}$.

For such a sequence let $\underline{s}^b$ denote the infinite sequence $\{t_n : n \in \underset{\sim}{N}\}$ where $t_o = s_o$. $t_{n+1} = t_n s_{n+1} t_n$ for all $n \in \underset{\sim}{N}$.

2.4. A recognisable set A belongs to $\underline{A}_\Pi$ iff there is a $r \in \Pi$ such that for any two words $f,g \in X^*$ and infinite sequence $\underline{s} \in \underline{\underline{S}}$, the set $M = \{n \in \underset{\sim}{N} : f(t_n)^r g \in A\}$ or its complement $\underset{\sim}{N} \backslash M$ is finite where $\{t_n\} = \underline{s}^b$.

Proof : Assume first $A \in \underline{A}_\Pi$. Consider an infinite sequence $\underline{s}$ and the associated sequence $\underline{s}^b$. The sequence of subsets $t_n\alpha . S . t_n\alpha = Q_n$ $(n \in \underset{\sim}{N})$ of the syntactic monoid $S = X^*\alpha$ satisfies identically $Q_{n+1} \subset Q_n$. Since S is finite, there is a set $Q \neq \phi$ such that $Q_n = Q$ for all large enough $n \in \underset{\sim}{N}$. Further any $t_n\alpha$ belongs to the minimal generating set Q' of the biideal Q . The hypothesis that $s_n = 1$ for an infinity of $n \in \underset{\sim}{N}$ implies that $t_{n+1} = t_n t_n$ for the same values of n . Therefore $Q'Q' \cap Q' \neq \phi$. By a standard argument from the theory of finite monoids, it shows that in fact Q' is a group in S . It now suffices to take $r = \omega(A) \in \Pi$.

Reciprocally, consider any set A and group G in Synt (A) . Take any $g \in G$. Since α is a surjective morphism we can choose an infinite sequence $\underline{s} \in \underline{\underline{S}}$ such that $s_{2n} = 1$, $s_{2n+1} = g^{-n'}$ where $n' = 1$ for $n = 0$ and $= 6n-5$ for n positive.

Instant computation shows that $t_{2n}\alpha = g^{2n+1}$; $t_{2n+1} = g^{4n+2}$. Therefore, $\{t_n\alpha : n \in \underset{\sim}{N}\}$ contains g itself infinitely often. Thus in order to satisfy the required condition over all triple of words we must take for r a multiple of $\omega(A)$.

Q.E.D.

Remark.

This could be applied to other questions. For instance, all the groups in the syntactic monoid of a recognisable set A are commutative iff for each infinite sequence $\underline{S} \in \underline{\underline{S}}$ there is a $m \in \underset{\sim}{N}$ such that for all $f,g \in X^*$, $n \geq m$ the set $\{ft_nt_{n+1}g , ft_{n+1}t_ng\}$ is contained in A or in $X^*\backslash A$.

3. Verifying the "Main Property".

Let $A \subset X^*$ and $h \in X^*$ arbitrary. The set of all $n \in \underset{\sim}{N}$ such that $h^n \in A^*$ is a submonoid of the additive monoid $\underset{\sim}{N}$. As such it has a finite minimum generating set $M \subset \underset{\sim}{N}$ and we can denote it by M^* .

Further, letting d be the greatest common divisor of the numbers in M , one knows that $d\underset{\sim}{N}\backslash M^*$ is finite. Clearly, $h^* \cap A = \{1\}$ iff $M = \{d\} = \emptyset$.

3.1. Assume $A^* \in \underline{A}_{\pi}$ and A a basis. Then A^* satisfies the condition :

$(\underline{P'}_{\pi})$. $h \in X^*$, $s \geq 1$ $h^s \in A^* \Rightarrow h^r \in A^*$

for some factor $r \in \Pi$ of s .

Therefore $A^* \in \underline{P}_{\neg\Pi}$.

Proof : Assume $h^s \in A^*$ for some positive s . Conditions $(\underline{P'}_\Pi)$ and $(\underline{P}_{\neg\Pi})$ are equivalent respectively with $M \subset \Pi$ and $M \cap \Pi \neq \phi$.

Because of $A^* \in \underline{A}_{\neg\Pi}$ we have $\omega(h,A^*) = p \in \Pi$, hence $h^n(h^p)^*\alpha \in A^*\alpha$ for some $n \in \underline{N}$ where α is the syntactic morphism of A^* . Therefore $p \in d\underline{N}$, hence $d \in \Pi$.

We recall the fact, which does not need being reproved once more, that iff A is a basis, one has the relation : $f \in X^*$, $fA^* \cap A^*f \cap A^* \neq \phi \Rightarrow f \in A^*$.

Suppose A a basis, $m,m' \in M$ and $m' = m+q$ $(q \in \underline{N})$. We have $h^q h^m = h^m h^q = h^{m'} \in A^*$ where $h^m \in A^*$ hence $h^q \in A^*$. Since M is a minimal generating set it implies $q = 0$, i.e. that M is the singleton $\{d\} \in \Pi$. Q.E.

This establishes the second assertion in the "Main Property". Instead of checking the first one by the fastest method, we indulge into a longer discussion. In what follows, A,B,C are recognisable sets in X^+ , f,g and $h \neq 1$ are words in X^* . We use the notations introduced in Section 2, except that we indicate explicetely by notations such as $\omega(h,A)$ or $\omega(h,A,f,g)$ which syntactic monoid Synt (A) is involved. In particular p_A is the least number m such that the m-t^n power of any word has its syntactic image in a group in Synt (A) .

lso q denotes here a fixed positive integer.

.2. Let $A = C^q$, $fh^n g \in A^*$, and assume that the length $|a'_i|$ of the longest word $a'_j \in A$ in some factorisation $h^n g = a'_1 a'_2 \dots a'_k$ $(a'_1, a'_2, \dots, a'_k \in A)$ satisfies

$$|a'_j| \geq q(|fg| + |h|p_C) .$$

hen $\omega(h, A^*, f, g)$ divides $\omega(h, C)$.

roof : Because of $A = C^q$, the word $fh^n g$ is a product of k words $c'_i \in C$ and because of our choice of $|a'_j|$, one f the factors c'_i of a'_j has at least $m = p_C$ factors in , i.e., there are words $c = c'_j \in C$, $c_1, c_2 \in C^*$, $f', g' \in X^*$ uch that $fh^n g = c_1 c c_2 \in A^*$; $c = f'h^m g' \in C$; $c_1 f' \in fh^*$; $c_2 \in h^* g$.

Therefore for any $t \in \underset{\sim}{N}$ we shall have $h^{n+t} g = c_1 f' h^{m+t} g' c_2$ and $fh^{n+t} g \in (C^p)^* \subset A^*$ where $f'h^{m+t} g' \in$

Because of our choice of $m = p_C$, this last relation s satisfied when t is a multiple of $\omega(h, C, f', g')$, hence when t is a multiple of $s = \omega(h, C)$. Therefore $fh^n (h^s)^* g \in c_1 C c_2 \subset A^*$ roving that $\omega(h, A^*, f, g)$ is a divisor of $\omega(h, C)$. Q.E.D.

.3. Let $A^* \subset C^*$ where $C^* \in \underset{\sim}{P_\pi}$ and further, either = C^q or $c \in C^+$, $c^+ \cap A^* \neq \phi \Rightarrow c^q \in A^*$. Assume $fh^n g \in A^k A^*$ here $k \geq |fhg|$. Then $\omega(h, A^*, f, g)$ divides q^r for some $\in \Pi$.

Proof : There is at least one factorisation $fh^n g = a_1 a a_2$, where the words $a_1, a, a_2 \in A^*$ are such that for some factorisation $h = h_1 h_2$ $(h_1, h_2 \in X^*)$ one has $a_1 \in fh^* h_1$, $a_2 \in h_2 h^* g$ and $a \in h_2 h^* h_1 = (h_2 h_1)^+$.

Therefore for all $t \in \underset{\sim}{N}$

$$fh^{n+t}g = a_1 a (h_2 h_1)^t a_2 .$$

Because of $A^* \subset C^*$ and $C^* \in \underline{P}_\pi$; the relations $a \in A^*$, $a \in (h_2 h_1)^+$ imply $(h_2 h_1)^r = c \in C^*$ for some $r \in \Pi$. If $A = C^q$ we have instantly $c^q \in A^*$. If $A^* \subset C^*$, the same conclusion follows because of $a^+ \subset A^*$ and $a^+ \cap c^+ \neq \phi$. Therefore in both cases :

$$fh^n (h^{rq})^* g = a_1 a (c^q)^* a_2 \in A^* .$$

Q.E.D.

Let us derive some conclusions, letting Π' denote the least set containing every divisor of all numbers of the form rq with $r \in \Pi$.

3.4. Assume $A = C^q$ where $C \in \underline{A}_\pi$, $C^* \in \underline{P}_\pi$. Then $A^* \in \underline{A}_{\pi'}$.

Proof : Π' contains the least common multiple of any two of its member. Therefore, to prove $A^* \in \underline{A}_{\pi'}$, i.e. $\omega(h, A^*) \in \Pi'$ for all $h \in X^*$, it suffices to check that one has identically $\omega(h, A^*, f, g) \in A^*$.

In the situation of 3.2, this follows from $\Pi \subset \Pi'$ and the hypothesis $C \in \underline{A}_\pi$. If the hypothesis of 3.2 are not met, we are in the situation of 3.3 and the result is already stated.

Q.E.D

Taking $q = 1$ in 3.4 gives the first assertion in the "Main Property".

3.5. Assume $A \subset B^q$, $A \in \underline{A}_\pi$ and $B^* \in \underline{P}_\pi$ where B is a basis. Then $A^* \in \underline{A}_\pi$.

Proof : Taking $q = 1$ shows $\omega(h,A^*,f,g) \in \Pi'$ when in the situation of 3.3. Let us shown that we are in the situation of 3.4 (with $C = B$) when these hypothesis are not satisfied. Suppose indeed $b \in B^*$ and, say $b^r \in A^*$. We have $b = b'_1 b'_2 \ldots b'_k$ ($k \in \underset{\sim}{N}$) where all the words b'_i are in B . Therefore $b^r = b'_1 b'_2 \ldots b'_k b'_1 \ldots b'_k \ldots b'_k \in A^*$. Because of the hypothesis that B is a basis, this factorisation is unique.

Therefore $rk = qk'$ for some $k' \in \underset{\sim}{N}$ since $A \subset B^q$, and all the k' successive products of q consecutive words b_i are in A^* . Since b^q is itself a product of these last products, we have shown $b^q \in A^*$. Q.E.D.

The next remarks have no relevance to the present problem.

.6. Assume $A \subset B$ whene B^* satisfies the condition $\in X^*$, $B^* f B^* \cap B^* \neq \phi \Rightarrow f \in B^*$. Then for any $h \in X^*$, (h,A^*) divides the l.c.m. of $\omega(h,A)$ and $\omega(h,B^*)$.

roof : Our condition on B^* implies in particular that $f \cap B^* \neq \phi$ only if $f \in B^*$. Therefore B is prefix, hence

basis. It follows that we can go directly to the case when
$h^n g = a_1 a a_2$ and $a = (h_2 h_1)^d \in (h_2 h_1)^+$ in the notations and
.th the hypothesis of 3.3.

Let $s = \omega(h, B^*, f, g)$. We have $fh^n h^t g \in B^*$ iff
$\in s\underset{\sim}{N}$. Since $fh^n h^d g = a_1 a a a_2 \in A^* \subset B^*$, it follows that
$\in s\underset{\sim}{N}$. Let $b = (h_2 h_1)^s$. We have $fh^n h^s g = a_1 a b a_2 \in B^*$
here $a_1 a, a_2 \in A^* \subset B^*$. Therefore $b \in B^*$ by our condition
B^* , implying as in 3.5 that $b \in A^*$, hence that
$h^n (h^s)^* g \in A^*$.

This shows that $\omega(h, A^*, f, g)$ divides $s = \omega(h, B^*, f, g)$.
In fact both numbers are equal since $A^* \subset B^*$. Q.E.D.

.7. Let the recognisable set A be such that
$\in X^+$, $c^+ \cap A^* \neq \phi \Rightarrow c \in A$. Then for all $h \in X^*$,
(h, A^*) divides $\omega(h, A)$.

Proof : Take $q = 1$, hence $C = A$ in 3.2. Under the hypo-
thesis of this statement we have that $\omega(h, A^*, f, g)$ divides
(h, A) . If they are not satisfied, take in 3.3, $C = X$; $q = 1$
and the second alternative in the hypothesis. Then we are in
the same situation as in the present case. Since $X^* \in \underset{\circ}{A}$, we
can take $\Pi = \{1\}$ and the conclusion gives $\omega(h, A^*, f, g) = 1$. Q.E.

In order to show some "raison d'être" to the last two
assertions we verify the following final remark.

3.8. Let $\alpha : X^* \to S$ and $\beta : X^* \to T$ be two surjective morphisms onto finite monoids and assume that for each $h \in X^*$ the order $\omega(h,S)$ is a divisor of $\omega(h,T)$. Then every group G in S is a homomorphic image of a group in T.

Proof : Let $K = G\alpha^{-1}$. It is a subsemigroup of X^*. Since $K\beta$ is finite, there exists an idempotent u and a group H in T such that $u.K\beta.u = H$.

Let ρ denote the application from H into the subsets of G that sends every $b \in H$ onto $b\rho = (b\beta^{-1} \cap K)\alpha$. Since $K\alpha = G$ it is surjective and since β is a morphism one has identically $b\rho \neq \phi$ and $b\rho.b'\rho \subset (bb')\rho$ for any $b,b' \in H$. Take in particular b' to be the inverse of b in H. We have $\omega(h,T) = 1$, hence $\omega(h,S) = 1$ by hypothesis, for any $h \in (bb')\beta^{-1} \cap K$. Therefore $(bb')\rho$ is the idempotent of G, hence a singleton. Since $b\rho$ and $b\rho'$ are non empty subsets of G, it shows that each of them is a singleton, i.e. that ρ is a morphism from H to G.

Q.E.D.

The example of the submonoid $\{x,xy,yx\}^*$ $(x,y \in X)$ of X^* which belongs to $\underline{A}_o$ shows that the condition of 3.7 does not imply that A^* be a free submonoid.

4. Verifying the Corollary.

We establish the theorem mentionned in the Introduction. What we give here is far from being optimal and we refer the reader to Eilenberg's theorem for deeper and more precise results. Let us recall a minimum of automatic machinery.

An automaton will be a triple $T = (Q,q_1,Q_+)$ where Q is a finite set, $q_1 \in Q$ is an initial state and $Q_+ \subset Q$ a terminal set. The set Q is provided with a morphism of X^* into the monoid of all partial applications of Q into itself. A modification of T will be another automaton $T' = (Q,q'_1,Q'_+)$ on the same set of states Q and it will be described in terms of T by indicating the initial and terminal elements q'_1 and Q'_+ and the value of the state qx for the pairs $(q,x) \in Q \times X$ such that qx is not the same in the morphisms of X^* into the monoids of action on states associated with T and with T'_o. The number of pairs $q,q' \in Q$ such that $q' \in qX$ will be denoted by $|T|$. We shall write $q^{-1}Q'$ $(q \in Q, Q' \subset Q)$ to denote the set $q^{-1}Q' = \{f \in X^* : qf \in Q'\}$. In particular, T recognises the set $q_1^{-1}Q_+$.

Any recognisable set A is recognised by at least one automaton. Among the automata who do this job there is a minimal one, say the syntactic automaton $T_A = (Q,q_1,Q_+)$ of A.

It has the following further properties :

(i) For any $q \in Q$, $Q' \subset Q$ the set $B = q^{-1}Q'$ satisfies $B\alpha^{-1}\alpha = B$ where α is the syntactic morphism of A.

(ii) $|T_A| \leq |T|$ for any other automaton T recognising A.

Let us now refer the reader to the families $\underline{A}$ and $\underline{B}$ described at the end of the Introduction. We make the observation that $X^* \in \underline{A}$ because $X^*\alpha^{-1}\alpha = X^*$ for any morphism α. Further, by hypothesis $\{1\} \in \underline{A}$, where $\underline{A}$ is closed under boolean operations. Therefore $X^+ = X^*\backslash\{1\} \in \underline{A}$ and $A \cap X^+ \in \underline{A}$ for any $A \in \underline{A}$. Also $\underline{A}$ is closed under product. Therefore $A,B \in \underline{A} \Rightarrow A\backslash BX^+ \in \underline{A}$.

We shall use repeatedly the fact that if $A \in \underline{A}$ and $B\alpha^{-1}\alpha \subset B$ (where α is the syntactic morphism of A), one has $B \in \underline{A}$. This immediately follows from the fact that by the very definition of Synt, $B\alpha^{-1}\alpha = B$ implies that Synt (B) is a quotient monoid of Synt (A) and from the hypothesis that $\underline{M}$ contains the quotient monoids of its members.

We are ready to prove that $\underline{B}$ contains any given member A of $\underline{A}$. This will be done by induction on $|T_A|$ where $T_A = (Q,q_1,Q_+)$ is the syntactic automaton of A.

First the initial case. Suppose $|T_A| = 0$. We have either $A = \phi$ or $A = \{1\}$. The empty set is a subset of X, therefore it is in $\underline{B}$ by the condition (i) stated in the Introduction. Also ϕ is a prefix set and since $\{\phi\}^* = \{1\} \in \underline{A}$

we have $\{1\} \in \underline{B}$ by condition (ii). We can henceforth assume $|T_A|$ positive.

Set $P = q_1^{-1}q_1$ and assume first $P \neq 1$. It belongs to $\underline{A}$ because $P = P\alpha\bar{\alpha}^{-1}$. Let Q' be the set of all states $q \in Q$ such that the set $X_q = q^{-1}q_1 \cap X$ is not empty. Modify the automaton T_A into a new automaton T' by letting $qX_q = \phi$ for every $q \in Q'$. If we take successively each $q \in Q'$ as a final state we obtain a set $B_q \subset X^*$ and the union of $B_q X_q$ over all $q \in Q'$ is a prefix set B such that $B^x = P$. Therefore by our induction hypothesis and $B_q\alpha^{-1}\bar{\alpha} = B_q$, we have $P \in \underline{B}$.

Now we have the unambigous product $A = PA'$ where A' is the set accepted by T' when restoring Q_+ as the set of final states. Therefore to conclude the argument we have only to show $A' \in \underline{B}$. This is already done by the induction hypothesis unless $T' = T_A$, i.e. unless $P = \{1\}$, and also $A' \neq 1$. Take any state q_2 such that $q_1^{-1}q_2 = X' \neq \phi$ and modify $T' = T_A$ to T'' by letting $q_1X' = \phi$, keeping the same final set of states.

We have that A' is the disjoint union of $q_1^{-1}Q_+$ and of $X'q_2^{-1}Q_+$; Both sets are in B by the induction hypothesis.

Q.E.D.

eferences.

1] R. Mc Naughton and S. Pappert, Counter free automata. MIT Press 1971.

2] S.W. Golomb and B. Gordon (1965), Codes with Bounded synchronisation delay. Information and Control (8), pp; 355-37

3] S. Eilenberg, Forth coming book.

4] Bret R. Tilson, p-length of p-solvable semigroups, in Semigroups, K.W. Folley Ed. Academic Press, 1969.

Année 1972

Bibliographie

[1] Marcel-Paul Schützenberger. Promotion des morphismes d'ensembles ordonnés. *Discrete Math.*, 2 :73–94, 1972.

DISCRETE MATHEMATICS – Volume 2, No. 1 (1972) 73–94

PROMOTION DES MORPHISMES D'ENSEMBLES ORDONNES

M.P. SCHÜTZENBERGER

Paris VII et IRIA, France

Reçu le 3 mai 1971

Resumé. Deux constructions de la théorie des tableaux de Young developpée par Robinson and Knuth sont étendues à d'autres ensembles ordonnés finis.

§ 1. Introduction

Dans tout ce mémoire, on considérera un ensemble ordonné fixe $(A, \leq)$ ayant un nombre fini $1+q$ d'éléments, et pour chaque $z \in \mathbf{Z}$, $\mathcal{M}_z$ désignera la famille des *morphismes* (d'ensemble ordonné) *bijectifs* de A sur l'intervalle $I_z = \{z, z+1, \ldots, z+q\}$ de $\mathbf{Z}$. On posera

$$\mathcal{M} = \bigcup_z \mathcal{M}_z \ .$$

Dans le cas particulier où $(A, \leq)$ est un intervalle du groupe ordonné $\mathbf{Z}^2$, les éléments de $\mathcal{M}_1$ (ou plutôt les classes de $\mathcal{M}_1$ pour l'équivalence de translation dans $\mathbf{Z}^2$) sont connus sous le nom de *tableaux gauches de Young*. La théorie de la correspondance de Robinson [1] entre permutations du groupe symétrique et tableaux de Young utilise entre autres (cf. [2]) deux bijections remarquables, notées ici

$$\partial : \mathcal{M}_z \to \mathcal{M}_{z+1} \ ,$$

$$\# : \mathcal{M}_z \to \mathcal{M}_{-z-q} \ .$$

L'objet du présent travail est de présenter celles des propriétés de ∂ et $\#$ que nous avons trouvées rester vraies dans le cas d'un ensemble ordonné $(A, \leq)$ quelconque.

De fait il sera commode de considérer non seulement les morphismes de $\mathcal{M}$ mais aussi la famille

$$\mathcal{B} = \bigcup_z \mathcal{B}_z ,$$

où $\mathcal{B}_z$ désigne l'ensemble des *bijections* $A \to I_z$. Les principales définitions sont données dans cette section. Les énoncés formels et les preuves sont rassemblés dans les deux sections suivantes.

Les deux notions de base sont celles de traînée C_φ et de promotion ∂.

Définition 1. Soit $\varphi : A \to \mathbf{Z}$ une injection. La *traînée* C_φ est la chaîne

$$C_\varphi = \{C_\varphi^i = c_1 < c_2 < \ldots < c_k = C_\varphi^u\} \subset A ,$$

dont l'élément initial C_φ^i est $c_1 = (\min (A\varphi))\varphi^{-1}$ et pour laquelle, inductivement:

c_j = l'élément ultime C_φ^u ssi $\{a \in A : c_j < a\} = \phi$ (c'est-à-dire $c_j \in \max (A)$), et sinon

$c_{j+1} = (\min \{a\varphi : a \in A : c_j < a\})\varphi^{-1}$.

Définition 2. Soient φ et C_φ comme dans la Définition 1. La *promotion* est l'application $\varphi\partial : A \to \mathbf{Z}$ définie par

$$a \in A - C_\varphi \Rightarrow a\varphi\partial = a\varphi ,$$

$$c_j \in C_\varphi - C_\varphi^u \Rightarrow c_j\varphi\partial = c_{j+1}\varphi ,$$

$$C_\varphi^u\varphi\partial = 1 + \max (A\varphi) .$$

Autrement dit, $\varphi\partial$ se déduit de φ en supprimant la plus petite valeur $C_\varphi^i = \min (A\varphi)$, puis en faisant avancer d'un pas le long de la traînée chacune des valeurs $c_{j+1}\varphi \in (C_\varphi - C_\varphi^i)$ portées par celle-ci et enfin en attribuant au dernier élément C_φ^u de la traînée la nouvelle valeur

$$1 + \max (A\varphi) = \min \{z \in Z : A\varphi < z\} = \max (A\varphi\partial) .$$

Il est clair que quand φ est une bijection $A \to I_z$, la promotion $\varphi\partial$ est une bijection sur

$$I_{z+1} = 1 + I_z = \{z + q + 1\} \cup I_z - \{z\} .$$

L'exemple suivant, où $\varphi \in \mathfrak{B}_z$ et où les traits symbolisent la relation de consécutivité associée à $\leq$, illustre les définitions précédentes (cf. figs. 1–3). On pourra noter que $\varphi\partial^2$ est un morphisme.

De façon duale, c'est-à-dire en considérant les structures d'ordre opposées, $(A, \geq) = \widetilde{A}$ et $(\mathbf{Z}, \geq)$, on définira la *traînée opposée*

$$\widetilde{C}_\varphi = \{\widetilde{C}^i_\varphi = c'_1 > c'_2 > \ldots > c'_{k'} = \widetilde{C}^u_\varphi\} ,$$

où $\widetilde{C}^i_\varphi = (\max(A\varphi))\varphi^{-1}$ et la *promotion opposée* $\widetilde{\partial}$,

$$c'_j\varphi\widetilde{\partial} = c'_{j+1}\varphi \; ; \; \widetilde{C}^u_\varphi\widetilde{\partial} = -1 + \min(A\varphi) .$$

Dans notre exemple, $\widetilde{C}_\varphi = \{11,6,3\}$ (cf. fig. 4).

Nous conviendrons que l'écriture $\varphi\partial^r$ désigne $\varphi\widetilde{\partial}^{-r}$ pour chaque $r \in -\mathbf{N}$ et il est clair qu'avec cette convention $\varphi\partial^r$ est une bijection sur I_{z+r} pour tout $r \in \mathbf{Z}$ et $\varphi \in \mathfrak{B}_z$. On verra que dans le cas particulier des morphismes l'on a $\partial^{-1} = \widetilde{\partial}$ et que $\partial^r = \widetilde{\partial}^{-r}$ est toujours une bijection

$$\mathfrak{M}_z \to \mathfrak{M}_{z+r} .$$

Pour tout morphisme $\varphi \in \mathfrak{M}$ on appellera *orbite* de φ l'ensemble

$$\overline{\varphi\partial}^* = \{\varphi\partial^r : r \in \mathbf{Z}\} = \Phi ,$$

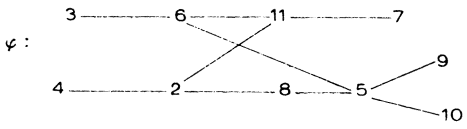


Fig. 1. $C_\varphi = \{2,5,9\}$.

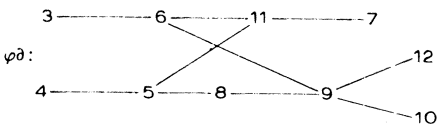


Fig. 2. $C_{\varphi\partial} = \{3,6,7\}$.

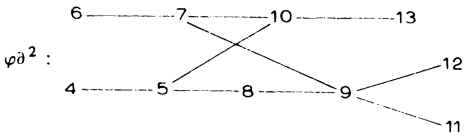


Fig. 3.

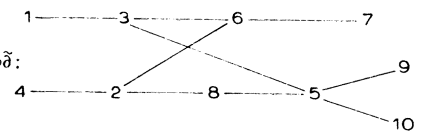


Fig. 4.

qui est donc une partie minimale non-vide de $\mathcal{M}$ satisfaisant $\Phi = \Phi\partial = \Phi\tilde{\partial}$. Une telle orbite $\Phi \subset \mathcal{M}$ contient exactement un morphisme dans chaque $\mathcal{M}_t$ ($t \in \mathbf{Z}$). Il sera commode de désigner la traînée C_φ de $\varphi = \Phi \cap \mathcal{M}_t$ comme étant la traînée $C(\Phi, t)$ de t dans Φ.

Définition 3. La *trajectoire* $T(\Phi, t)$ d'une valeur $t \in \mathbf{Z}$ dans une orbite Φ est la suite $\{v_1 < v_2 < \ldots < v_k\}$ des éléments distincts $v_j \in A$ de l'ensemble $\{t\psi^{-1} : \psi \in \Phi\}$.

Les traînées (pour les morphismes) et les trajectoires sont évidemmant des chaînes maximales dans A. Si (et seulement si) A lui-même est une chaîne, les trainées et les trajectoires coincident avec A, et, de plus, $\mathcal{M}$ se réduit à une seule orbite Φ. Donc, posant $\Phi\# = \Phi$, on a (trivialement) l'identité

$$C(\Phi, t) = T(\Phi\#, -t) , \qquad t \in \mathbf{Z} .$$

Notre résultat principal (Propriété 12) est la généralisation de cette identité à un ensemble $(A, \leq)$ quelconque: Nous montrerons que pour chaque orbite $\Phi \subset \mathcal{M}$ il existe une et une seule orbite, notée $\Phi\#$ satisfaisant l'identité ci-dessus, c'est-à-dire telle que pour chaque $t \in \mathbf{Z}$ la traînée de t dans Φ soit identique à la trajectoire de $-t$ dans $\Phi\#$. De fait, comme on le verra, l'opération $\#$ est involutive, et, par conséquent, l'on a aussi l'identité $T(\Phi, t) = C(\Phi\#, -t)$ (cf. l'exemple à la fin de cette section). Dans ce but, nous utiliserons une application $\#: \mathcal{B} \to \mathcal{M}$ que nous définissons maintenant en utilisant la notation $\varphi\partial^* = \{\varphi\partial^p : p \in \mathbf{N}\}$.

Définition 4. Soit $\varphi : A \to \mathbf{Z}$ une injection. Son *contraire* est l'application $\varphi\# : A \to \mathbf{Z}$ telle que pour chaque $a \in A$,

$$a\varphi\# = -\min \{A\psi : \psi \in \varphi\partial^*, a\psi\partial \notin A\varphi\} .$$

En d'autre terme, $-(a\varphi\#)$ est la valeur de $\min(A\psi)$, où $\psi = \varphi\partial^p$ et où p est le plus petit entier non négatif tel que $a\varphi\partial^{p+1}$ n'appartienne pas à $A\varphi$. De façon duale on définira le *contraire opposé* $\varphi\tilde{\#}$ par

$$a\varphi\tilde{\#} = -\max \{A\psi : \psi \in \varphi\partial^*, a\psi\partial^* \notin A\varphi\} .$$

Les figs. 5 et 6 illustrent, dans notre exemple, $\varphi\#$ et $\varphi\tilde{\#}$.

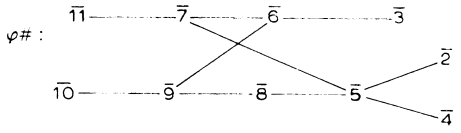


Fig. 5.

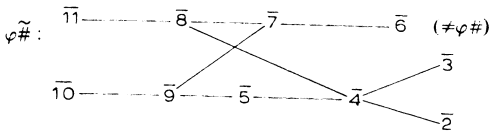


Fig. 6.

On voit facilement que $\varphi\#$ et $\tilde{\varphi\#}$ sont des morphismes bijectifs sur $-A\varphi$. Par conséquent, comme $-I_z = I_{-z-q}$, le contraire de chaque $\varphi \in \mathfrak{B}_z$ appartient à $\mathfrak{M}_{-z-q}$. On établira que pour toute orbite Φ l'ensemble des contraires $\psi\#$ ($\psi \in \Phi$) est une orbite que l'on désignera par $\Phi\#$.

Pour terminer nous introduisons encore la

Définition 5. Soit $\Phi \subset \mathfrak{M}$ une orbite. La *table de promotion* $\Delta(\Phi)$ est l'application partielle $\Delta : \mathbf{Z} \times \mathbf{Z} \to A \times A$ telle que, pour tout $z, t \in \mathbf{Z}$, on ait

$$(z, t)\Delta = (a, b) \neq \phi \qquad (a, b \in A)$$

ssi, posant $\psi = \Phi \cap \mathfrak{M}_z$, l'on a $t = b\psi$ et en outre soit $t(\psi\partial)^{-1} = a \neq b$, soit $a = b = C^i_\psi = C^u_\psi$.

Autrement dit, pour $z \in \mathbf{Z}$ donné, prenant $\psi \in \Phi$ tel que $\min(A\psi) = z$,

$$(z, t)\Delta = (a, b) \neq \phi$$

ssi soit la promotion ∂ déplace la valeur $t \in A\varphi$ de b à $a \neq b$, soit C_ψ se réduit au singleton $\{a\} = \{b\}$ et alors $z = t$. Par conséquent, $(z, t)\Delta$ ne peut être non vide que si d'une part t est une des valeurs portées par la traînée C_ψ ce qui implique en particulier $z \leq t \leq z+q$ (avec $z = t$ ssi cette traînée est un singleton) et d'autre part $a \leq b$.

On établira l'identité

$$(z, t)\Delta(\Phi) = (-t, -z)\Delta(\Phi\#) \qquad (z, t \in Z),$$

d'où l'on déduira sans peine la dualité entre traînée et trajectoire mentionnée plus haut.

Donnons pour terminer l'exemple très simple de l'ensemble

$$A = \{(i, j) : 1 \leq i \leq 3,\ 1 \leq j \leq 2\}$$

ordonné de façon naturelle $((i, j) \leq (i', j')$ ssi $i \leq i'$ et $j \leq j')$ et de l'orbite Φ du morphisme $\varphi \in \mathcal{M}_1$ représenté par:

$$\varphi = \begin{matrix} 2 & 5 & 6 \\ 1 & 3 & 4 \end{matrix}.$$

On trouve:

$$\varphi\partial = \begin{matrix} 5 & 6 & 7 \\ 2 & 3 & 4 \end{matrix}, \qquad \varphi\partial^2 = \begin{matrix} 5 & 6 & 8 \\ 3 & 4 & 7 \end{matrix}, \qquad \varphi\partial^3 = \begin{matrix} 5 & 6 & 8 \\ 4 & 6 & 7 \end{matrix},$$

$$\varphi\partial^4 = \begin{matrix} 8 & 9 & 10 \\ 5 & 6 & 7 \end{matrix}, \qquad \varphi\partial^5 = \begin{matrix} 8 & 9 & 11 \\ 6 & 7 & 10 \end{matrix}, \qquad \varphi\partial^6 = \begin{matrix} 8 & 11 & 12 \\ 7 & 9 & 10 \end{matrix},$$

(et plus généralement $\varphi\partial^{3r+s} = 3r + \varphi\partial^s$ quels que soient $r, s \in \mathbf{Z}$). Par conséquent,

$$\varphi\# = \begin{matrix} -4 & -3 & -1 \\ -6 & -5 & -2 \end{matrix} \in \mathcal{M}_{-6},$$

dont la trainée est la chaîne

$$(1,1) < (2,1) < (2,2) < (2,3)$$

d'éléments de A. Cette chaîne est précisément la trajectoire de 6 dans Φ. De même

$$\varphi\partial\# = \begin{matrix} -4 & -3 & -2 \\ -7 & -6 & -5 \end{matrix}$$

a pour traînée

$$(1,1) < (2,1) < (3,1) < (3,2)\ ,$$

ce qui est la trajectoire de 7 dans Φ.

§ 2. Propriétés générales de la promotion

L'objectif de cette section est de donner une définition plus maniable de la promotion ∂. Pour cela nous établissons d'abord deux énoncés très généraux dans lesquels φ et ψ sont deux applications $A \to \mathbf{Z}$ satisfaisant les deux conditions suivantes:

(i) l'une au moins de φ et ψ est injective;

(ii) $A\varphi - A\psi = z$ et $A\psi - A\varphi = t$ sont deux singletons.

La condition supplémentaire

$$a, b \in A\ , \qquad a\varphi = b\psi \Rightarrow a \leq b$$

sera notée en abrégé $\psi^{-1} \leq \varphi^{-1}$.

Propriété 1. *Les applications φ et ψ sont deux injections telles que $\psi^{-1} \leq \varphi^{-1}$ ssi il existe une chaîne non vide*

$$D = D(\psi\varphi^{-1}) = \{D^i = d_1 < d_2 < \ldots < d_k = D^u\} \subset A$$

telle que

(i) $a \in A - D \Rightarrow a\varphi = a\psi$,

(ii) $D^i\varphi = z$, $D^u\psi = t$,

(iii) $d_j \in D - D^u \Rightarrow d_j\psi = d_{j+1}\varphi$.

Preuve. Supposons d'abord que φ et ψ sont deux injections telles que $\psi^{-1} \leq \varphi^{-1}$ et posons $u = t\psi^{-1}$, $i = z\varphi^{-1}$. Comme φ et ψ sont des bijections sur $(A\varphi \cap A\psi) \cup \{z\}$ et $(A\varphi \cap A\psi) \cup \{t\}$ respectivement, la relation $\tau' = \psi\varphi^{-1} \subset A \times A$ peut être identifiée à une bijection de $A - u$ sur $A - i$. Nous étendons τ' à une permutation τ de A en posant $u\tau = i$.

Considérons un élément $a \in A - u$. Si $r = a\psi$ on a $r \in A\varphi$ puisque $r\psi \neq u\psi = A\psi - A\varphi$. Par conséquent $r\varphi^{-1} = b \in A$ existe et l'on a par hypothèse $a = r\psi^{-1} \leq r\varphi^{-1} = b$. Comme $b = r\varphi^{-1} = r\psi^{-1}\psi\varphi^{-1} = a\psi\varphi^{-1} =$

$= a\tau$, ceci prouve que

$$a \in A - u \Rightarrow a \leq a\tau \ .$$

Utilisant le fait que A est fini et qu'il en est donc de même de toutes les orbites de τ, on en conclut que ces dernières sont toutes des singletons sauf celle, désignée par D, qui contient u et i. Donc

$$a \in A - D \Rightarrow a\tau = a \ ,$$

c'est-à-dire $a\psi = a\varphi$.

En ce qui concerne D, ses éléments sont

$$i = d_1 < i\tau = d_2 < \ldots < i\tau^{k-1} = d_k = u \ .$$

Par conséquent, $d_j\psi = d_{j+1}\varphi$ pour $j = 1, 2, \ldots, k-1$, achevant la preuve de la nécessité de la condition indiquée.

La réciproque résulte immédiatement des définitions.

Nous supposons maintenant satisfaites les conditions de la Propriété 1 et en outre $z = \min(A\varphi) < t = \max(A\psi)$.

Propriété 1.1. *On a $\varphi \leq \psi$ ssi, de façon équivalente, la restriction $\varphi|D$ de φ à D ou la restriction $\psi \mid D$ est un morphisme.*

Preuve. Comme $\varphi \mid (A - D) = \psi \mid (A - D)$, on peut supposer que $A = D$. Sous cette hypothèse, l'équivalence des conditions indiquées est immédiate puisque

$$d_1\varphi = \min(A\varphi \cup A\psi) < d_k\psi = \max(A\varphi \cup A\psi) \ .$$

Lemme 2. *Soient $\varphi \in \mathfrak{B}_z$ et $\psi \in \mathfrak{B}_{z+1}$ deux bijections telles que $\psi^{-1} \leq \varphi^{-1}$. On a $\psi = \varphi\partial$ ssi*

$$(2.1) \qquad d \in D \ , \qquad b \in A(d) \Rightarrow d\psi \leq b\psi \ ,$$

où, pour abréger,

$$A(d) = \{b \in A : d < b\} .$$

Preuve. Soit $d = d_j \in D - D^u$. On a $d\psi = d_{j+1}\varphi$ où, par construction, $d_{j+1} \in A(d)$, avec

$$A(d)\varphi = (A(d)\varphi \cap A(d)\psi) \cup \{d_{j+1}\varphi\} ,$$

$$A(d)\psi = (A(d)\varphi \cap A(d)\psi) \cup \{D^u\psi\} .$$

Comme

$$D^u\psi = C^u\varphi\partial = I_{z+1} - I_z = \max(I_z \cup I_{z+1}) ,$$

la condition indiquée, c'est-à-dire $d\psi \leq \min(A(d)\psi)$, est satisfaite ssi $d\psi = d_{j+1}\varphi = \min(A(d)\varphi)$.

Procédant par induction sur $j = 1, 2, \ldots$ ceci montre que la condition (2.1) est satisfaite ssi $d_j = c_j$ ($c_j \in C_\varphi$ = la traînée définie dans § 1).

Soit maintenant $d = D^u$. Comme $d\psi = z + q + 1$ on ne peut avoir $d\psi \leq A(d)\psi$ que si $A(d) = \emptyset$, c'est-à-dire que si $D^u \in \max(A)$. Donc $D^u = C^u_\varphi$. Réciproquement $C^u_\varphi\psi \leq A(C^u_\varphi)\psi$ de façon triviale puisque $C^u_\varphi \in \max(A)$.

Corollaire 2.1. *Soient $\varphi \in \mathfrak{B}_z$ et $\psi \in \mathfrak{M}_{z+1}$. On a $\psi = \varphi\partial$ ssi $\psi^{-1} \leq \varphi^{-1}$.*

Preuve. Ceci résulte immédiatement du Lemme 2 puisque l'hypothèse que ψ est un morphisme équivaut à

$$a \in A , \quad b \in A(a) \Rightarrow a\psi \leq b\psi .$$

Lemme 3. *Soit $\varphi \in \mathfrak{B}$. Les restrictions de φ et $\varphi\partial$ à la traînée C_φ sont des morphismes, et de plus*

$$(3.1) \qquad a \in A , \quad b \in A(a) , \quad a\varphi \leq b\varphi \Rightarrow a\varphi\partial \leq b\varphi\partial .$$

Preuve. Le fait que la restriction $\varphi \mid C_\varphi$ est un morphisme résulte du Lemme 2 qui implique $c_j\varphi < c_{j+1}\varphi$ ($c_j, c_{j+1} \in C_\varphi$). D'après la Propriété 1.1, $\varphi\partial \mid C_\varphi$ est aussi un morphisme et l'on a $\varphi \leq \varphi\partial$.

Pour vérifier (3.1), il suffit maintenant de considérer un élément $a \in A - C_\varphi$. On a alors $a\varphi\partial = a\varphi$, d'où

$$a\varphi\partial = a\varphi \leq b\varphi \leq b\varphi\partial ,$$

où la dernière relation résulte de $\varphi \leq \varphi\partial$.

En application nous avons:

Remarque 4. Soit $\varphi \in \mathcal{B}$. Pour tout $p \geq q = -1 + \mathrm{card}(A)$, l'application $\varphi\partial^p$ est un morphisme.

Preuve. Posons $r(\varphi) = 0$ ssi φ est un morphisme et sinon

$$r(\varphi) = \max\{a\varphi - \min(A\varphi) : a \in A \text{ et } b\varphi < a\varphi \text{ pour au moins un } b \in A(a)\}.$$

Donc $r(\varphi) \leq q$. Comme

$$a\varphi\partial - \min(A\varphi\partial) = a\varphi - \min(A\varphi) - 1$$

pour $a \notin C_\varphi$, il résulte des énoncés précédents que

$$r(\varphi\partial) \leq \max\{0, r(\varphi) - 1\} ,$$

d'où le résultat par induction sur $r(\varphi)$.

Afin de faciliter les références ultérieures, nous rassemblons en un seul énoncé ce qui dans ce qui précède concerne des morphismes de $\mathcal{M}$.

Propriété 5. *Soit $\varphi \in \mathcal{M}_z$. On a $\varphi\partial \in \mathcal{M}_{z+1}$ et $\varphi \leq \varphi\partial$. De plus, $(\varphi\partial)^{-1} \leq \varphi^{-1}$ et $\varphi\partial$ est l'unique élément de $\mathcal{M}_{z+1}$ qui satisfasse cette dernière inégalité.*

Preuve. $\varphi \in \mathcal{M}_{z+1}$ et $\varphi \leq \varphi\partial$ résultent immédiatement du Lemme 3 et de la Propriété 1.1. La seconde partie est un cas particulier du Corollaire 2.1.

Nous en venons maintenant au principal résultat de cette section.

Propriété 5.1. *La restriction de ∂ à la sous-famille $\mathcal{M} \subset \mathcal{B}$ des mor-*

phismes est bijective et son inverse est la promotion opposée $\tilde{\partial}$.

Preuve. Soit $\varphi \in \mathcal{M}_z$. D'après le Corollaire 3.1, $\varphi\partial$ est un morphisme ($\in \mathcal{M}_{z+1}$). De plus d'après le Corollaire 2.1, $\varphi\partial$ est l'unique morphisme $\psi \in \mathcal{M}_{z+1}$ qui satisfasse $\psi^{-1} \leq \varphi^{-1}$.

Considérons la paire $((A, \geq), (\mathbf{Z}, \geq))$ de structures d'ordres opposées. Elle a les mêmes morphismes que la précédente, et la relation $\psi^{-1} \leq \varphi^{-1}$ équivaut à $\varphi^{-1} \geq \psi^{-1}$. Donc $\varphi\partial\tilde{\partial} = \varphi$. De façon duale, $\psi\tilde{\partial}\partial = \psi$ pour tout $\psi \in \mathcal{M}_{z+1}$. Par conséquent, $\tilde{\partial}$ est l'inverse de ∂ et ces deux applications sont des bijections.

Nous concluons cette section en établissant quelques propriétés supplémentaires de ∂. La première sera utilisée dans la section suivante; la seconde sert de base aux applications aux tableaux de Young.

Nous rappelons qu'un *intervalle* Y d'un ensemble ordonné $(X, \leq)$ est une partie Y de X telle que

$$y, y' \in Y, \quad x \in X, \quad y \leq x \leq y' \Rightarrow x \in Y.$$

Par conséquent, Y étant un intervalle, et y un élément de Y, l'ensemble $Y - \{y\}$ est un intervalle ssi $y \in \max(Y) \cup \min(Y)$.

Un *idéal* est ici une partie V de X telle que

$$x \in X, \quad v \in V, \quad x \leq v \Rightarrow x \in V.$$

C'est donc un intervalle.

Nous dirons qu'une application $\varphi : X \to \mathbf{Z}$ est *compatible* avec l'intervalle Y ssi $Y\varphi$ est un intervalle de $X\varphi$. Ainsi, quand φ est un morphisme, les intervalles avec lesquels il est compatible sont les images inverses des intervalles de $X\varphi$.

Lemme 6. *Soient* A' *un idéal de* A *et* $\varphi : A \to \mathbf{Z}$ *une injection compatible avec* A'. *Posant*

$$\varphi' = \varphi \mid A', \quad A'_p = A' \cap (A\varphi)(\varphi\partial^p)^{-1} \quad (p \in \mathbf{N}),$$

on a pour chaque p:

(6.1, p) *les traînées* $C_{\varphi\partial^p}$ *et* $C_{\varphi'\partial^p}$ *ont la même intersection avec* A'_p, *et* $\max(C_{\varphi\partial^p} \cap A'_p) \in \max(A'_p)$;

Références

[1] G. de B. Robinson, On the representations of the symmetric group, Am. J. Math. 60 (1938) 745–760.
[2] D. Knuth, Permutations, matrices and generalized Young tableaux, Pacific J. Math. 34 (1970) 709–727.

Année 1973

Bibliographie

[1] Dominique Foata and Marcel-Paul Schützenberger. Nombres d'Euler et permutations alternantes. In *A Survey of Combinatorial Theory (Proc. Internat. Sympos., Colorado State Univ., Fort Collins, Colo., 1971)*, pages 173–187. North-Holland, Amsterdam, 1973.

[2] Marcel-Paul Schützenberger. À propos du relation rationelles fonctionnelles. In *Automata, Languages and Programming (Proc. Sympos., Rocquencourt, 1972)*, pages 103–114. North Holland, Amsterdam, 1973.

[3] Marcel-Paul Schützenberger. Sur une construction de Gilbert de B. Robinson. In *Séminaire P. Dubreil, 25e année (1971/72), Algèbre, Fasc. 1*, Exp. No. 8, 4 pages. Secrétariat Mathématique, Paris, 1973.

[4] Marcel-Paul Schützenberger. Sur un langage équivalent au langage de Dyck. In P. Suppes et. al., editor, *Logic, Methodology and Philosophy of Science, IV (Proc. Fourth Internat. Congr., Bucharest, 1971)*, pages 197–203. Studies in Logic and Foundations of Math., Vol. 74. North-Holland, Amsterdam, 1973.

J. N. Srivastava et al., eds., *A Survey of Combinatorial Theory*

CHAPTER 16

Nombres d'Euler et Permutations Alternantes

D. FOATA†
University of Florida, Gainesville, Fla., U.S.A.
et
M.-P. SCHÜTZENBERGER
Université de Paris VII et I.R.I.A., France

1. Introduction

Les entiers apparaissant dans le développement de Taylor des fonctions élémentaires de l'analyse classique sont souvent susceptibles d'interprétations combinatoires, qui donnent une signification géométrique à certaines de leurs propriétés. Réciproquement, de nombreux problèmes d'énumération d'objets rudimentaires conduisent à des fonctions génératrices remarquables, et il parait utile d'explorer systématiquement ces liaisons.

Le présent travail est la première partie d'une étude sur les nombres D_n ($n \in \mathbf{N}$) définis par le développement

$$\sum_{1 \leqslant n} D_n u^n/n! = D(u)$$

de la fonction

$$D(u) = \int_0^u (\operatorname{tg} u + (\cos u)^{-1})\, du.$$

Pour $n = 2m$ pair, on retrouve donc les *nombres tangents* D_{2m}

$$D_{2m} = 2^{2m-1}(2^{2m}-1)m^{-1}B_m,$$

où

$$B_m = 2\zeta(2m)(2\pi)^{-2m}(2m)!$$

est le $2m$-ième *nombre de Bernoulli*. Pour $n = 2m+1$, les nombres D_{2m+1} sont les *nombres sécants*, dits aussi *nombres d'Euler*. Ces nombres ont fait l'objet de très nombreuses études arithmétiques dont un exposé systématique d'ensemble a été donné par Nielsen [1923] dans son *Traité élémentaire des nombres de Bernoulli*. D'autre part, la table la plus complète des premières valeurs de ces nombres apparaît dans Buckholtz et Knuth [1967].

Les relations

$$\exp D(u) = D''(u) = (\tfrac{1}{2})(1 + D'^2(u)), \tag{1.1}$$

$$D(0) = 0 \tag{1.2}$$

entraînent

$$D'(u) = (1 + tg\, \tfrac{1}{2}u)(1 - \operatorname{tg} \tfrac{1}{2}u)^{-1} \tag{1.3}$$

† On leave from the Université de Strasbourg, 1971–72.

et les identités

$$\exp D_{(2)} = D_{(1)'}, \tag{1.4}$$

$$D_{n+3} = \sum_{0\leqslant i\leqslant n} \left[{n \atop i}\right] D_{i+1} D_{n+2-i}, \tag{1.5}$$

$$2D_{n+2} = \sum_{0\leqslant i\leqslant n} \left[{n \atop i}\right] D_{i+1} D_{n-i+1} + \delta_{n,0}, \tag{1.6}$$

$$D_{2n+1} = \sum_{0\leqslant i\leqslant n-1} \left[{2n-1 \atop 2i}\right] D_{2i+1} D_{2n-2i}, \tag{1.7}$$

où, dans la première, l'on a posé

$$D_{(2)} = \sum_{1\leqslant n} (u^{2n}/(2n)!) D_{2n} \left(= \int_0^u \operatorname{tg} u \, du \right)$$

et

$$D_{(1)} = \sum_{0\leqslant n} (u^{2n+1}/(2n+1)!) D_{2n+1} = D - D_{(2)}.$$

A leur tour, ces identités fournissent les congruences élémentaires suivantes valables pour tout nombre premier impair p

$$D_{p+3} \equiv D_{p+2} + D_{p+1}; \tag{1.8}$$

$$D_{p+2} \equiv D_{p+1} \equiv D_p + 1. \tag{1.9}$$

D'un point de vue combinatoire, André [1879, 1881] a montré que D_{n+1} est le nombre des *permutations alternantes* sur $[n]$, c'est-à-dire des permutations $x_1 x_2 \ldots x_n$ des éléments de $[n] = \{1, 2, \ldots, n\}$ telles que x_{2j} soit à la fois inférieur à x_{2j-1} et à x_{2j+1} pour tout entier j tel que $0 < 2j < n$ et, en plus, si n est pair, telles que $x_n < x_{n-1}$.

De façon indépendante, Kermack et McKendrick [1938] ont étudié une distribution qui équivaut à celle des "pics" et des "creux" sur les permutations du groupe symétrique sur $[n]$: étant donnée une telle bijection f: $[n] \to [n]$, un pic (resp. creux) est une valeur $j \in [n]$ telle que jf soit plus *grande* (resp. *petite*) que les deux valeurs adjacentes $(j-1)f$ et $(j+1)f$. Sous cette forme, les calculs de Kermack et McKendrick ont été repris par David et Barton [1962] dans leur ouvrage *Combinatorial Chance*. Les fonctions génératrices associées sont des polynômes qui se rencontrent aussi dans la représentation des polynômes eulériens comme sommes de monômes $t^p(1+t)^m$ à coefficients entiers non négatifs (cf. Foata et Schützenberger [1970]). Une transformation simple les ramène à des polynômes à deux variables $D_n(s, t)$ prenant la valeur D_n pour $s = t = 1$. Ce sont ces derniers que nous appellerons *polynômes d'André* et dont nous nous proposons ici d'aborder l'étude.

Dans la section 2 suivante nous établissons les principales formules concernant les polynômes d'André. En particulier, une formule explicite pour leur fonction génératrice est donnée. Cette section est de nature purement analytique.

Ainsi qu'il se produit souvent dans ce domaine, une meilleure compréhension de objets est atteinte en opérant dans une algèbre non commutative.

Nous introduisons donc dans la section 3 les polynômes d'André *non commutatifs*, qui sont eux susceptibles de plusieurs interprétations. La place nous a manqué pour donner toutes celles qu'exigerait une vérification géométrique des identités données à la deuxième section. Nous nous sommes donc bornés à discuter ce que nous appelons les "permutations d'André", grâce auxquelles diverses identités binomiales au sens de Mullin et Rota [1970] s'expliquent en termes de variation. Un article ultérieur traitera des "complexes d'André" qui permettent de retrouver certaines propriétés fondamentales de symétrie.

Il est clair que la plupart de nos énoncés pourraient aussi bien être présentés dans le langage statistique qui fut celui d'une grande partie de notre carrière. Notre choix d'une formulation moins spéciale est un hommage à notre Maître Bose dont l'oeuvre a tant illustré les enrichissements mutuels de la mathématique et de ses applications.

Nous remercions notre ami John Riordan de nous avoir signalé l'article de Kermack et McKendrick [1938] et d'avoir bien voulu relire et commenter une première version de cet article.

2. Les polynômes d'André

2.1. Définition et propriétés élémentaires

Soit D une fonction réelle de la variable u, analytique à l'origine et satisfaisant l'équation différentielle

$$D'' = t \exp D, \tag{2.1}$$

avec les conditions initiales

$$0 = D(0), \qquad s = D'(0), \tag{2.2}$$

où s et t sont des constantes. En raison de $0 = D(0)$, la relation (2.1) est équivalente à

$$D''' = D'D''. \tag{2.3}$$

Nous posons

$$D = \sum_{0 \leqslant n} (u^n/n!) D_n,$$

où, d'après (2.1) et (2.2), $D_0 = 0$, $D_1 = s$, $D_2 = t$. Considérant s et t comme des paramètres, les relations (2.1) et (2.3) déterminent de façon univoque par récurrence sur n les D_n comme polynômes en s et t. Ce sont eux que nous appellerons *polynômes d'André* et que nous désignerons dans cette section par $D_n = D_n(s, t)$ $(n \geqslant 0)$. La liste des premiers d'entre eux est la suivante:

$$D_0 = 0, \quad D_1 = s, \quad D_2 = t, \quad D_3 = st,$$
$$D_4 = s^2t + t^2, \quad D_5 = s^3t + 4st^2,$$
$$D_6 = s^4t + 11s^2t^2 + 4t^3, \quad D_7 = s^5t + 26s^3t^2 + 34st^3.$$

Les valeurs $D_n(1, 1)$ sont entières et sont bien les coefficients de la fonction

$D(u)$ présentée dans l'introduction puisque celle-ci était définie par l'équation différentielle

$$D'' = \exp D$$

avec les valeurs initiales

$$D(0) = 0, \qquad D'(0) = 1(= s)$$

et que l'on avait donc

$$D''(0) = \exp 0 = 1(= t).$$

Soit maintenant l'opérateur

$$\Delta = st\frac{\partial}{\partial t} + t\frac{\partial}{\partial s}.$$

On a

$$\Delta D_1 = t = D_2 \qquad \text{et} \qquad \Delta D_2 = st = D_3.$$

Observant que (2.3) équivaut à l'identité binomiale

$$D_{n+3} = \sum_{0 \leqslant j \leqslant n} [{}^{n}_{j}] D_{j+1} D_{n+2-j} \qquad (n \geqslant 0), \tag{2.4}$$

on en conclut que

$$D_{n+1} = \Delta D_n \qquad (n \geqslant 1), \tag{2.5}$$

soit encore, en tenant compte de la valeur initiale $D_1 = s$,

$$s + \Delta D = \frac{\partial}{\partial u} D. \tag{2.6}$$

Ces relations montrent que les polynômes d'André ont les propriétés élémentaires suivantes:

Propriété 2.1. *Les polynômes D_n sont homogènes de degré total n en les variables s et $\sqrt{t}$. Ils sont divisibles par t pour $n \geqslant 2$ et leurs coefficients sont des entiers positifs.*

On a donc pour chaque $n \geqslant 2$,

$$D_n = \sum_{1 \leqslant k \leqslant n/2} s^{n-2k} t_k \, \mathrm{d}_{n,k},$$

où les coefficients $d_{n,k}$ sont des entiers naturels et la relation (2.5) livre immédiatement la propriété suivante.

Propriété 2.2. *Pour $n \geqslant 2$, on a $d_{n,1} = 1$, et pour $2 \leqslant k \leqslant \frac{1}{2}n$, on a*

$$d_{n+1,k} = k\, d_{n,k} + (n+2-2k)\, d_{n,k-1}. \tag{2.7}$$

Par conséquent, tous les $d_{n,k}$ $(1 \leqslant k \leqslant \frac{1}{2}n)$ sont positifs. Posant maintenant

$$\bar{D}_n = \sum_{1 \leqslant k \leqslant n/2} \bar{t}^k \, d_{n,k},$$

la même relation (2.5) donne la formule de récurrence

$$\bar{D}_{n+1} = n\bar{t}\bar{D}_n + (\bar{t} - 2\bar{t}^2)\frac{\partial}{\partial \bar{t}} \bar{D}_n \qquad (n \geqslant 2) \tag{2.8a}$$

qui est équivalente à

$$\bar{\bar{D}}_{n+1} = \bar{t}(1-2\bar{t})^{\frac{1}{2}} \frac{\partial}{\partial \bar{t}} \bar{\bar{D}}_n, \tag{2.8b}$$

où

$$\bar{\bar{D}}_n = (1-2\bar{t})^{-n/2} \, \bar{D}_n.$$

On notera qu'en raison de (2.7) le polynôme D_n est divisible par s ssi n est impair.

2.2. Une relation différentielle

Nous établissons maintenant la généralisation naturelle de la deuxième égalité dans la relation (1.1).

Propriété 2.3. *On a l'identité*

$$2D'' = 2t - s^2 + D'^2. \tag{2.9}$$

Preuve. D'après (2.4) et (2.5), on a pour tout $n \in \mathbf{N}$

$$D_{n+3} = \Delta D_{n+2} = \sum_{0 \leqslant j \leqslant n} [{}^{n}_{j}](\Delta D_j) D_{n+2-j}.$$

Tenant compte de la symétrie des indices et de $[{}^{n}_{j}] = [{}^{n}_{n-j}]$, ceci donne

$$2\Delta D_{n+2} = \sum_{0 \leqslant j \leqslant n} [{}^{n}_{j}]\Delta(D_{j+1} D_{n+1-j}),$$

d'où

$$2D_{n+2} = \sum_{0 \leqslant j \leqslant n} [{}^{n}_{j}] D_{j+1} D_{n+1-j} + K_n, \tag{2.10}$$

où K_n est une fonction de s et t telle que $\Delta K_n = 0$. Comme les D_j sont des polynômes, K_n est un polynôme. D'autre part, comme

$$\Delta(t^p s^q) = p t^p s^{q+1} + q t^{p+1} s^{q-1} \qquad (p, q \in N),$$

on voit que le terme de plus bas degré de K_n en t ne peut s'annuler que si ce degré est zéro. Comme, d'après la propriété 2.1, on a $D_{n+2}(s, 0) = 0$ pour tout $n \geqslant 0$, le polynôme K_n est nul pour $n \geqslant 1$. Enfin, on vérifie directement que $K_0 = 2t - s^2$. Ceci fait, la formule (2.9) s'obtient par sommation.

On notera que pour $n+2 = 2m+1$ impair, l'expression (2.10), avec $K_n = 0$, est symétrique et peut par conséquent s'écrire sous la forme (1.7) de l'introduction, soit de façon équivalente

$$D_{2m+1}/(2m-1)! = \sum_{0 \leqslant j \leqslant m-1} (D_{2j+1}/(2j)!)(D_{m-2j}/(2m-2j-1)!);$$

c'est-à-dire

$$D_{(1)''} = D_{(1)'} D_{(2)'}, \tag{2.11}$$

avec les notations déjà introduites dans le cas particulier de $s = t = 1$,

$$D_{(2)} = \sum_{0 \leqslant m} (u^{2m}/(2m)!) D_{2m}(s, t),$$

$$D_{(1)} = D - D_{(2)}.$$

Nous en déduisons la formule suivante qui est la contre-partie polynomiale de (1.4).

Propriété 2.4. *On a*

$$D_{(1)'} = s \exp D_{(2)}. \tag{2.12}$$

7

Preuve. La formule (2.11) peut s'écrire

$$\frac{\partial}{\partial u}\log D_{(1)'} = \frac{\partial}{\partial u} D_{(2)'}.$$

D'où

$$D_{(1)'} = K(s, t)\exp D_{(2)},$$

où $K(s, t)$ est une fonction de s et t qui est déterminée en faisant $u = 0$ et en constatant que $D_2(u = 0) = 0$ et $D_{(1)'}(u = 0) = s$.

2.3. Fonction génératrice des polynômes d'André

Nous donnons maintenant des formules explicites pour D, D' et D''.

Propriété 2.5. *Posant* $r = (s^2-2t)^{\frac{1}{2}}$, $w = (s-r)/(s+r)$ *et* $E = \exp ru$, *on a les formules*

$$D = ru+2\log((1-w)/(1-wE)); \tag{2.13}$$

$$D' = r(1+wE)/(1-wE); \tag{2.14}$$

$$D'' = wr^2E/(1-wE)^2. \tag{2.15}$$

Preuve. L'équation (2.9) peut s'écrire

$$r = D''((D'-r)^{-1}-(D'+r)^{-1}),$$

d'où par intégration

$$ru = \log((D'-r)/(D'+r))+K(s, t),$$

où la fonction $K(s, t)$ est déterminée en faisant $u = 0$ et se trouve par conséquent égale à $-\log w$. Donc $(D'-r)/(D'+r) = w\exp ru$, ce qui est équivalent à (2.14). Maintenant le membre de droite de cette dernière équation peut s'écrire sous la forme

$$r(1+(2w\exp ru)/(1-w\exp ru)),$$

d'où par une nouvelle intégration

$$D = ru-2\log(1-w\exp ru)+K(s, t).$$

Faisant de nouveau $u = 0$, on trouve

$$K(s, t) = 2\log(1-w).$$

On obtient ainsi la formule (2.13). Enfin, la formule (2.15) s'obtient par simple dérivation.

Désignons par $D_{(0)'}$ la valeur du membre de droite de (2.14) pour $s = 0$. Posant $v = (2t)^{\frac{1}{2}}u$ et observant que $w = -1$ pour $s = 0$, on trouve

$$D_{(0)'} = (2t)^{\frac{1}{2}}\cdot \mathrm{i}(1-\exp \mathrm{i}v)/(1+\exp \mathrm{i}v),$$

soit

$$D_{(0)'} = (2t)^{\frac{1}{2}}\operatorname{tg}\tfrac{1}{2}v. \tag{2.16}$$

Ce résultat a la conséquence très remarquable suivante:

Propriété 2.6. *Pour tout* k *positif, les coefficients* $d_{2k-1,k-1}$ *et* $d_{2k,k}$ *sont égaux a* $2^{1-k}[D_{2k}]_{s=t=1}$, *c'est-a-dire a* 2^{1-k} *fois le* k*-ème nombre d'Euler.*

Preuve. Prenant $n = 2k-1$, la récurrence (2.8) donne

$$d_{2k,k} = k\, d_{n,k} + (2k-1+2-2k)\, d_{n,k-1} = d_{2k-1,k-1}$$

puisque $d_{n,k} = 0$ en vertu de $n < 2k$. Les deux coefficients d mentionnés dans l'énoncé sont donc égaux.

Maintenant pour vérifier leur égalité avec le nombre $2^{1-k}[D_{2k}]_{s=t=1}$, il suffit d'observer que pour $s = 0$, tous les polynômes D_{2k-1} sont nuls et chacun des polynômes D_{2k} se réduit à $d_{2k,k}t^k$. Par conséquent,

$$D_{(0)'} = \sum_{1 \leqslant k} (u^{2k-1}/(2k-1)!)\, d_{2k,k} t^k.$$

On peut alors appliquer la formule (2.16) qui s'écrit

$$D_{(0)'} = (2t)^{\frac{1}{2}} \sum_{1 \leqslant k} (u^{2k-1}/(2k-1)!)(\tfrac{1}{2}t)^{(2k-1)/2} D_{2k},$$

soit

$$D_{(0)'} = \sum_{1 \leqslant k} (u^{2k-1}/(2k-1)!) 2^{1-k} D_{2k} t^k.$$

Nous donnons enfin la formule binomiale

$$2d_{2n+2,n+1} = \sum_{0 \leqslant i \leqslant n-1} \left[\begin{smallmatrix} 2n \\ 2i+1 \end{smallmatrix}\right] d_{2i+2,i+1} d_{2n-2i,n-i} \qquad (n \geqslant 1), \quad (2.17)$$

qui se déduit immédiatement de la formule (2.9) lorsqu'on y fait $s = 0$ et $t = 1$, grâce à la propriété 2.6.

2.4. Relations avec les polynômes eulériens

Nous terminons cette section en établissant une relation entre les polynômes d'André et les polynômes eulériens. Pour la définition de ces derniers, nous renvoyons le lecteur à l'ouvrage de Riordan [1958], pp. 213–216, ou à notre précédent mémoire (Foata et Schützenberger [1970]).

Propriété 2.7. *Pour tout entier $n > 0$, le n-ème polynôme eulérien $A_n(x)$ est égal à*

$$\sum_{1 \leqslant k \leqslant (n+1)/2} d_{n+1,k} (2x)^{k-1} (1+x)^{n+1-2k},$$

où les $d_{n+1,k}$ sont les coefficients du $(n+1)$-ème polynôme d'André.

Preuve. Faisons la substitution

$$s = 1, \qquad t = 2x/(1+x)^2, \qquad u = (1+x)v$$

dans l'expression de $(D'-s)/t$ donnée par (2.14). Notant que la substitution envoie r sur $(1-x)/(1+x)$ et w sur x, on trouve

$$\frac{(1+x)\{\exp[(1-x)v]-1\}}{1-x\exp[(1-x)v]}.$$

Divisant par $1+x$, et ajoutant 1, on obtient

$$\frac{(1-x)\exp[(1-x)v]}{1-x\exp[(1-x)v]},$$

qui est l'expression classique de la fonction génératrice exponentielle des polynômes eulériens. Donc, pour $n > 0$, $A_n(x)$ est le polynôme obtenu en

faisant la substitution $s = 1$, $t = 2x/(1+x)^2$ dans $(1+x)^{n-1}t^{-1}D_{n+1}$, ce qui est précisément le résultat annoncé.

On pourra noter que la relation de symétrie $x^n A_n(x^{-1}) = A_n(x)$ correspond à l'invariance $t = 2x^{-1}/(1+x^{-1})^2$.

3. Les permutations d'André

3.1. Quelques notions générales

Nous commençons par décrire en détail quelques notions de base.

Soit X un ensemble totalement ordonné ayant un nombre fini n d'éléments. Une *permutation* de X est une bijection $f: [n] \to X$ où $[n]$ désigne l'ensemble ordonné $\{1, 2, \ldots, n\}$ ($= \emptyset$ si $n = 0$). Nous l'identifierons au *mot* $1f\,.\,2f\,.\,\ldots\,.\,nf$ en les lettres de X. Puisque f est une bijection, chaque élément de X figurera exactement une fois dans ce mot. Pour abréger, nous écrirons $f \in X^1$ pour indiquer que f est une permutation de X ou son mot associé.

Soient maintenant $n \geqslant 2$ et $f \in X^1$; la *variation* de f est le mot $fV = v_1 v_2 \ldots v_{n-1}$ de longueur $n-1$ en les symboles $v_j = (+)$ et $(-)$ qui est défini pour chaque $j \leqslant n-1$ par

$$\begin{aligned} v_j &= + \text{ si } jf < (j+1)f, \\ &= - \text{ si } jf > (j+1)f. \end{aligned}$$

Il est classique de dire que $[j, j+1]$ est une *montée* (resp. *descente*) ssi $v_j = +$ (resp. $= -$).

Soit maintenant $1 < j < n$:

$-[j-1, j+1]$ est une *double descente* ssi $[j-1, j]$ et $[j, j+1]$ sont deux descentes;

$-j$ est un *creux* ssi $[j-1, j]$ est une descente et $[j, j+1]$ une montée.

De façon analogue, la *variation circulaire* $f\mathring{V}$ est le mot de longueur n défini par $f\mathring{V} = fV\,.\,v_n$, où $v_n = +$ ou $-$ selon que $nf < 1f$ ou $nf > 1f$; autrement dit, v_n est défini pour $[n, 1]$ de la même manière que v_j était défini pour $[j, j+1]$.

D'une manière générale, une notion sera dite *circulaire* ssi dans sa définition il est convenu que "$n+1$" signifie "1". Par exemple pour $X = [8]$ et $f: [8] \to X$ identifié à 5 8 1 6 9 2 3 4 7 on a $fV = +-++-+++$ $(\in\{+, -\}^8)$, 1 et 2 sont les deux creux et f n'a pas de double descente. Comme $7 > 5$ on a $v_n = -$ et $f\mathring{V} = +-++-+++-$ $(\in\{+, -\}^9)$; enfin comme $7 > 5$, mais $5 < 8$, la permutation f est sans *double descente circulaire*, donc aussi sans double descente.

Nous introduisons maintenant une notion plus spéciale et nous définissons la *variation réduite* de f comme le mot fU de longueur $\leqslant n-1$ en les symboles t et s qui est obtenu à partir de la variation fV en remplaçant d'abord toutes les paires $v_i v_{i+1}$ telles que $v_i = -$, $v_{i+1} = +$ par t, ensuite en remplaçant par

s les v_i restants. Par construction, $fU = s$ ssi $n = 2$. Dans notre exemple $fU = ststss$ puisque $fV = +(-+)+(-+)++$.

Rappelons la notation standard $|f|_x$ pour désigner le nombre d'occurrences d'une lettre x dans un mot f.

Propriété 3.1. *Le nombre des creux de f est $|fU|_t$, celui des montées est $\leqslant |fU|_t + |fU|_s$ avec égalité ssi f est sans double descente et se termine par une montée* (*c'est-à-dire* $v_{n-1} = +$).

La preuve est immédiate.

On définit de la même manière la *variation réduite circulaire* $f\mathring{U}$ en convenant d'écrire la lettre t à la fin du mot fU quand n est un creux circulaire (c'est-à-dire quand $v_{n-1} = -$ et $v_n = +$) et au début quand 1 est un *creux circulaire* (c'est-à-dire quand $v_n = -$ et $V_1 = +$). C'est ce second cas qui se produit dans notre exemple et l'on a donc

$$f\mathring{U} = t\,t\,s\,t\,s\,s,$$

puisque $f\mathring{V} = +)(-+) + (-+) ++ (-$.

On notera que si $n = 2$, $f\mathring{U}$ est toujours t.

On *conviendra* pour $n = 1$, $f\mathring{U} = s$ et $fU = e$ (c'est-à-dire le mot vide du monoide libre $\{s, t\}^*$).

3.2. Définition des permutations d'André

Nous appellerons *permutation d'André* sur X ($0 \leqslant \text{card}\ (X) = n < \infty$) toute permutation $f\colon [n] \to X$ *sans double descente* satisfaisant la condition caractéristique suivante:

(A) Soient $j, j' \in [n]$ tels que $1 < j < j'$ et

$$(j-1)f = \max\{(j-1)f, jf, (j'-1)f, j'f\},$$
$$j'f = \min\{(j-1)f, jf, (j'-1)f, j'f\}.$$

Il existe un j'' tel que $j < j'' < j'$ et que $j''f < j'f$.

De façon intuitive, en tenant compte de ce que f n'a pas de double descente, la condition peut être reformulée ainsi.

Si j et $j' > j$ sont deux creux tels que $jf > j'f$ et $(j-1)f > (j'-1)f$, il existe un creux j'' entre j et j' ($j < j'' < j'$) tel que $j''f < j'f$ et la même condition vaut quand $j' = n$ et que $[j'-1, j']$ est une descente.

Il résulte immédiatement de la définition que toute permutation ayant 0 ou 1 descente est une permutation d'André, car elle n'a pas de double descente et la deuxième condition est trivialement vérifiée.

Une permutation f ayant exactement deux descentes $[j, j+1]$ et $[j', j'+1]$ ($j < j'$) est une permutation d'André ssi les deux conditions suivantes sont réalisées

(i) $j+1$ et $j'+1$ sont des creux ou bien $j+1$ est un creux et $[j', j'+1]$ est une descente finale;

(ii) l'on a $jf < j'f$ ou bien $jf > j'f$ et $(j-1)f < (j'-1)f$.

Pour avoir une idée concrète de cette condition, le lecteur pourra vérifier que parmi les six permutations de [6] qui sont de la forme $x\,2\,y\,3\,z\,1$ ($\{x, y, z\} = \{4, 5, 6\}$) et qui sont donc sans double descente puisqu'alternées, les permutations d'André sont les deux pour lesquelles $z = 6$.

En effet, puisque $2 = 2f < 3 = 4f$, la condition caractéristique ne s'applique qu'aux paires de creux $j = 2$ ou 4 et $j' = 6 > j$. Comme $jf = 2$ ou $4 > j'f = 1$ et comme il n'existe aucun creux j'' entre j et j' tel que $j''f < jf$ (puisque $4f = 3 > 6f = 1$), on doit avoir $(j-1)f < (j'-1)f$, c'est-à-dire $x < z$ et $y < z$.

Nous noterons D_n^* $(0 \leqslant n)$ l'ensemble des permutations d'André sur $[n]$ et $D^* = \bigcup_{0 \leqslant n} D_n^*$, en faisant comme d'usage la convention naturelle que pour $n = 0$, D_0^* est un singleton. Voici une table des D_n^* pour $n = 0, 1, 2, 3, 4$:

$$D_0^* = \{e\}, \quad D_1^* = \{1\}, \quad D_2^* = \{12, 21\},$$
$$D_3^* = \{123, 132, 213, 231, 312\},$$
$$D_4^* = \{1234, 1243, 1324, 1342, 1423,$$
$$2134, 2143, 2314, 2341, 2413,$$
$$3124, 3142, 3241, 3412,$$
$$4123, 4132\}.$$

On notera que $1 = \text{Card } D_0^* = \text{Card } D_1^*$; $2 = \text{Card } D_2^*$; $5 = \text{Card } D_3^*$; $16 = \text{Card } D_4^*$.

Par abus de notation, si $I = \{n'+1, \ldots, n'+m\}$ est un intervalle de $[n]$ et $f: [n] \to X$ une permutation, nous identifierons la restriction $f|I$ à la permutation $f': [m] \to If$ $(If \subset X)$ telle que $jf' = (n'+j)f$ identiquement.

Lemme 3.2. *Soit $f: [n] \to X$ une permutation d'André. Pour tout intervalle I de $[n]$, la restriction $f' = f | I$ de f à I est une permutation d'André.*

Preuve. Ceci découle de la structure des conditions "être sans double descente" et (A) qui ne font intervenir que les éléments d'un intervalle.

Nous introduisons maintenant deux familles spéciales de permutations d'André que nous appellerons respectivement (par abus de langage) *circulaires* et *augmentées*. Soit X un ensemble fini de cardinal n $(n \geqslant 0)$; une permutation d'André f sur X est dite *circulaire* (resp. *augmentée*) ssi son dernier élément nf est égal à $\min f$ (resp. $\max X$). On note D (resp. A) l'ensemble des permutations d'André appartenant à D qui sont circulaires (resp. augmentées); on pose $D_n = D \cap D_n^*$ et $A_n = A \cap D_n^*$ $(n > 0)$ et l'on convient que D_0 est vide et que $A_0 = D_0^* = \{e\}$. On voit sur la liste ci-dessus que $\text{Card } D_j = \text{Card } A_j = 1$ pour $j = 1, 2$; $\text{Card } D_3 = 1$; $\text{Card } A_3 = 2$; $\text{Card } D_4 = 2$; $\text{Card } A_4 = 5$.

Propriété 3.3. *Soient $n \in \mathbf{N}$ et $f: [n+2] \to X$ une permutation quelconque telle que*

(i) $$(n+2)f = \min X.$$

Les trois conditions suivantes sont équivalentes:

(1) *La permutation f est une permutation d'André (qui est nécessairement circulaire).*

(2) *La restriction $f' = f \mid [n+1]$ est une permutation d'André augmentée.*

(3) *La restriction $f'' = f \mid [n] = f' \mid [n]$ est une permutation d'André et*

(ii) $$j \in [n] \Rightarrow jf'' < (n+1)f'.$$

Preuve. Le lemme 3.2 donne immédiatement les implications

$$f \in D^* \Rightarrow f' \in D^* \Rightarrow f'' \in D^*.$$

Supposons (1) et prenons $j' = n+2$. D'après (i), d'une part $[j'-1, j']$ est une descente, d'autre part on ne peut pas avoir $j''f < j'f$ pour $j'' < j'$. Donc d'après (A) on aura $(j-1)f < (j'-1)f$ pour tout $j < j'$ tel que $[(j-1), j]$ soit une descente.

Considérons $\bar{\jmath}$ tel que $(\bar{\jmath}-1)f = \max X$; le couple $[\bar{\jmath}-1, \bar{\jmath}]$ est une descente et par conséquent $\bar{\jmath} = j'$, c'est-à-dire $(n+1)f = \max X$. La condition (1) implique donc (2).

Réciproquement supposons (3), c'est-à-dire que la restriction $f \mid [n]$ est une permutation d'André et que l'on a $(n+1)f = \max X$, $(n+2)f = \min X$. Il est clair que f n'a pas de double descente. D'autre part, prenant encore $j' = n+2$, la condition (A) est toujours satisfaite car il ne peut pas exister de creux $j < j'$ pour lequel $(j-1)f > (j'-1)f$. Donc (3) $\Rightarrow$ (1) et comme (2) $\Rightarrow$ (3) trivialement d'après $f' \in D^* \Rightarrow f'' \in D^*$, le résultat est établi.

Corollaire 3.4. *Pour tout $n \geqslant 0$, les ensembles D_{n+2}, A_{n+1} et D_n^* ont même cardinalité.*

3.3. Polynômes d'André en variables non commutatives

Pour simplifier, on appellera *polynômes d'André non commutatifs* les polynômes

$$A_n U = \sum \{fU : f \in A_n\},$$
$$D_n \mathring{U} = \sum \{f\mathring{U} : f \in D_n\} \qquad (n \geqslant 0)$$

en les variables non commutatives s et t. Dans la propriété 3.10 ci-après, on trouvera deux relations de récurrence sur ces polynômes. Enfin, la liste des polynômes pour les premières valeurs de n est donnée à la fin de cette section.

Lemme 3.5. *Soit f: $[n+1] \to X$ une permutation d'André. Il existe exactement une valeur $m \leqslant n$ telle que*

(i) $f \mid [m] \in D$;

(ii) $m' \geqslant m, f \mid [m'] \in D \Rightarrow m' = m$.

Preuve. Il suffit de prendre $m = (\min X)f^{-1}$ et d'observer que $m = (\min ([m']f))f^{-1}$ pour tout $m' \geqslant m$.

On notera $f^{(1)}$ la restriction $f \mid [m]$ ($m = (\min X)f^{-1}$) et on appellera $f^{(1)}$ le *premier facteur* de f. La restriction $f \mid [n] \setminus [m]$ sera le *cofacteur de* $f^{(1)}$ dans f et on utilisera souvent pour abréger la notation $f^{(1)-1}$ pour désigner $[m]$. L'importance de ce lemme est dans sa réciproque.

Propriété 3.6. *Une permutation* $f\colon [n+1] \to X$ *est une permutation d'André ssi posant* $m = (\min X)f^{-1}$, *les deux restrictions* $f^{(1)} = f \mid [m]$ *et* $f' = f \mid [n] \setminus [m]$ *sont des permutations d'André. Si ces hypothèses sont vérifiées et* $n \geqslant 1$, f *est augmentée si et seulement s'il en est de même de* f'.

Preuve. La partie directe résulte des lemmes 3.5 et 3.2. Supposons donc $f^{(1)}$, $f' \in D^*$ et sans perte de généralité $m < n$. Comme $mf = \min X$, $[m, m+1]$ est une montée. Donc f n'a pas de double descente puisque ni $f^{(1)}$ ni f' n'en ont.

Soit maintenant j et j' deux valeurs justiciables de la condition (A). Si $j, j' \in [m]$ ou $\in [n] \setminus [m]$, la condition (A) est satisfaite par f d'après l'hypothèse $f^{(1)}, f' \in D^*$. Si au contraire $j > m > j'$, la condition (A) est satisfaite par l'existence du creux $j'' = m$ entre j et j'.

Lemme 3.7. *Soit* $f\colon [n+1] \to X$ *une permutation d'André circulaire. Si* $n = 0$, $f\mathring{U} = s$ *et si* $n > 0$, $f\mathring{U} = (f'U)t$ *où* $f' = f \mid [n]$. *Par conséquent,*

$$D_{n+1}\mathring{U} = (A_n U)t \qquad \text{pour } n > 0.$$

Preuve. Le cas de $n = 0$ résulte de la définition même de $\mathring{U}$. Si $n \geqslant 1$, la variation de f se termine par une descente puisque $nf = \max X$, $(n+1)f = \min X$. Comme $(n+1)f < 1f$, la formule est encore une conséquence de la définition de $\mathring{U}$.

Lemme 3.8. *Soit* $f\colon [n+3] \to X$ *une permutation d'André circulaire. On a*

$$f\mathring{U} = g^{(1)}\mathring{U} \,.\, \bar{f}\mathring{U},$$

où $g^{(1)}$ *est le premier facteur de* $g = f \mid [n+1]$ *et* $\bar{f}$ *le cofacteur de* $g^{(1)}$ *dans* f.

Preuve. Le facteur $g^{(1)}$ est la restriction de f à $[m']$ où $m'f$ est le minimum de X privé de $\min X = (n+3)f$ et de $\max X = (n+2)f$. Donc $[m', m'+1]$ est toujours une montée de f.

Distinguons maintenant deux cas:

(i) $m' = 1$. On a $fV = +\bar{f}V$. Comme $\bar{f}\mathring{U}$ se termine par t puisque $n+3-m' \geqslant 2$, on a donc $f\mathring{U} = s \,.\, \bar{f}\mathring{U}$ et le résultat est établi.

(ii) $m' > 1$. Comme $g^{(1)} \in D$, $g^{(1)}$ se termine par la descente $[m'-1, m']$. Donc $fU = (g^{(1)}U)'\, t\, (\bar{f}U)$, où $(g^{(1)}U)'$ désigne le mot obtenu en supprimant le dernier s de $g^{(1)}U$. De façon équivalente, $fU = g^{(1)}\mathring{U} \,.\, \bar{f}U$, d'où encore $f\mathring{U} = g^{(1)}\mathring{U} \,.\, \bar{f}\mathring{U}$.

Corollaire 3.9. *Soit* $f\colon [n+2] \to X$ *une permutation d'André augmentée. On a*

$$fU = f^{(1)}\mathring{U} \,.\, f'U$$

où $f^{(1)}$ *est le premier facteur de* f *et* f' *son cofacteur.*

Preuve. Définissons la permutation $g : [n+3] \to X'$ par $g \mid [n+2] = f$ et $(n+3)g = \min X'$. Il est clair que g est une permutation d'André circulaire. Soient $g^{(1)}$ le premier facteur de $g \mid [n+1]$ et $\bar{g}$ le cofacteur de $g^{(1)}$ dans g. On a $g\mathring{U} = (fU)t$ (d'après le lemme 3.7), $f^{(1)} = g^{(1)}$, et enfin $\bar{g}\mathring{U} = (f'U)t$. Le lemme précédent donne d'autre part l'identité

$$g\mathring{U} = g^{(1)}\mathring{U} \,.\, \bar{g}\mathring{U},$$

c'est-à-dire

$$(fU)t = f^{(1)}\mathring{U} \,.\, (f'U)t.$$

Le corollaire est donc établi en supprimant la dernière lettre t de l'identité précédente.

Propriété 3.10. *Pour tout $n \geqslant 0$, on a les identités*

$$A_{n+2}U = \sum [{}^{n}_{j}] D_{j+1}\mathring{U} \,.\, A_{n+1-j}U, \tag{3.1}$$

$$D_{n+3}\mathring{U} = \sum [{}^{n}_{j}] D_{j+1}\mathring{U} \,.\, D_{n+2-j}\mathring{U}. \tag{3.2}$$

Preuve. La propriété 3.6 donne une bijection entre A_{n+2} et les triplés $(X' \cup X'', f^{(1)}, f')$, où $X' \cup X''$ est une partition de $X \setminus \{\min X, \max X\}$, $f^{(1)}$ une permutation circulaire d'André sur $X' \cup \{\min X\}$ et f' une permutation augmentée sur $X'' \cup \{\max X\}$. La première formule découle alors du corollaire 3.9 et la deuxième de la première et du lemme 3.7.

Tables 3.11. Pour terminer ce chapitre, nous donnons la liste des polynômes A_nU et $D_n\mathring{U}$ pour les premières valeurs de n. Ces polynômes peuvent être évidemment calculés à partir des formules de récurrence (3.1) et (3.2):

$$\begin{aligned}
A_1U &= 1,\\
A_2U &= s,\\
A_3U &= s^2+t,\\
A_4U &= s^3+2st+2ts,\\
A_5U &= s^4+3s^2t+5sts+3ts^2+4t^2,\\
A_6U &= s^5+4s^3t+9s^2ts+9sts^2+4ts^3+12st^2+10tst+12t^2s;\\
D_1\mathring{U} &= s,\\
D_{n+1}\mathring{U} &= (A_nU)t \text{ pour } n > 0.
\end{aligned}$$

4. Remarques

Comme il n'a pas été possible d'inclure dans le même article tous les résultats sur les polynômes d'André en variables non commutatives, nous renvoyons le lecteur à un prochain mémoire. Quelques ultimes remarques nous semblent cependant nécessaires.

Remarque 4.1. On a $D_1\mathring{U} = s$ et $D_2\mathring{U} = t$. D'autre part, la formule de récurrence (3.2) a la même structure formelle que la relation binomiale sur les polynômes *commutatifs* D_n qui s'écrivait en effet (voir formule (2.4))

$$D_{n+3} = \sum [{}^{n}_{j}] D_{j+1}D_{n+2-j} \qquad (n \geqslant 0). \tag{4.1}$$

Ceci montre que les polynômes $D_n\mathring{U}$ constituent bien une *version non commutative* des polynômes d'André $D_n(s, t)$.

Remarque 4.2. Lorsque les variables s et t commutent, on a aussi la *formule exponentielle*

$$\sum_{0\leqslant n} (u^n/n!)D_{n+2} = t \exp\left[\sum_{0\leqslant n} (u^n/n!)\, D_n\right]$$

(voir formule (2.1)). En fait, les formules (4.1) et (4.2) sont *équivalentes*. On peut s'en convaincre par l'argument suivant: La série formelle égale à t fois l'exponentielle de $\sum_{0<n} (u^n/n!)D_n$ est unique. Ceci résulte du fait que l'exponentielle est une bijection de l'ensemble des séries formelles sans terme constant sur l'ensemble des séries formelles de terme constant égal à 1. Or par dérivation de (4.2) par rapport à u, et identification des termes de même puissance en u, on obtient justement les formules (4.1).

Cette équivalence n'est *plus* valable lorsqu'on suppose s et t non commutatifs. Plus exactement, on n'a *pas* de formule exponentielle ayant même structure formelle que (4.2) avec les polynômes $D_n\mathring{U}$. Seule subsiste la formule (3.2), qui doit donc être regardée comme la *généralisation non commutative de la formule exponentielle*.

Remarque 4.3. Une autre façon d'établir directement la formule exponentielle (4.2) sans recourir aux arguments analytiques de la section 2 est de faire appel aux techniques purement combinatoires du *composé partitionnel*, développées dans notre précédent mémoire (Foata et Schützenberger [1970]). L'ensemble D^* est, en effet, le composé partitionnel de l'ensemble D des permutations d'André circulaires. Indiquons rapidement comment on peut le démontrer. Soit $f = 1f\,.\,2f\,.\,\ldots\,.\,nf$ $(n > 0)$ une permutation d'André. Elle admet une factorisation unique $(g^{(1)}, g^{(2)}, \ldots, g^{(k)})$ telle que

(1) le produit de juxtaposition $g^{(1)}g^{(2)}\ldots g^{(k)}$ soit égal à f;
(2) chaque $g^{(j)}$ est une permutation d'André circulaire;
(3) la suite formée par les dernières lettres des mots $g^{(j)}$ est croissante.

Par exemple, la factorisation de

$$f = 8\ 6\ 9\ 7\ 12\ 13\ 1\ 2\ 4\ 11\ 14\ 15\ 3\ 10\ 5$$

est donnée par

$$(8\ 6\ 9\ 7\ 12\ 13\ 1,\quad 2,\quad 4\ 11\ 14\ 15\ 3,\quad 10\ 5).$$

L'existence et l'unicité de cette factorisation peuvent être démontrées en utilisant le lemme 3.8. Supposant s et t commutatifs, on pose pour tout $f \in D_n^*$ $(n > 0)$

$$f\mu\,.\,t = (f\,.\,\overline{n+1}\,.\,0)\mathring{U}.$$

Là encore, à l'aide du lemme 3.8, on peut vérifier que μ est *multiplicative*. D'après la proposition 3.12 de la référence citée plus haut, on en déduit l'identité

$$1 + \sum_{0<n} (u^n/n!)D_n^*\mu = \exp\left[\sum_{0<n} (u^n/n!)A_n\mu\right].$$

L'identité (4.2) en résulte en observant que

$$D_n^*\mu \,.\, t = D_{n+2}(s,t) \quad \text{et} \quad A_n\mu = D_n(s,t) \quad \text{pour} \quad n > 0.$$

Remarque 4.4. Nous avons vu dans la propriété 2.3 que l'identité

$$2D_{n+2} = \sum_{0\leqslant j\leqslant n} [{}^n_j] D_{j+1} D_{n+1-j} \qquad (n \geqslant 1) \tag{4.3}$$

sur les polynômes *commutatifs* $D_n(s,t)$ se déduisait facilement de l'identité

$$D_{n+3} = \sum_{0\leqslant j\leqslant n} [{}^n_j] D_{j+1} D_{n+2-j} \qquad (n \geqslant 0).$$

Dans le cas des polynômes d'André *non commutatifs*, on peut établir également l'identité

$$2D_{n+3}\mathring{U} = s \,.\, D_{n+2}\mathring{U} + \sum_{1\leqslant j\leqslant n} [{}^{n+1}_{j}] D_{j+1}\mathring{U} \,.\, D_{n+2-j}\mathring{U} + D_{n+2}\mathring{U} \,.\, t^{-1}st \qquad (n \geqslant 0) \tag{4.4}$$

qui est l'équivalent non commutatif de (4.3). Comparant (3.2) et (4.4), on voit que pour obtenir (4.4), il suffit d'établir les formules

$$D_{n+3}\mathring{U} = \sum_{1\leqslant j\leqslant n} [{}^n_{j-1}] D_{j+1}\mathring{U} \,.\, D_{n+2-j}\mathring{U} + D_{n+2}\mathring{U} \,.\, t^{-1}st \qquad (n \geqslant 0). \tag{4.5}$$

Soit $w = u_1 \ldots u_k$ un mot en les lettres s et t; le mot *retourné* $\tilde{w}$ est défini par $\tilde{w} = u_k \ldots u_1$. Les formules (4.5) se déduisent alors de (3.2) et de la *propriété de symétrie* suivante: pour tout mot w en s et t, il y a dans l'ensemble A_n des permutations d'André augmentées autant d'éléments f tels que $fU = w$ que d'éléments g tels que $gU = \tilde{w}$. Cette propriété remarquable sera démontrée dans un article ultérieur. Nous y introduirons la notion abstraite de *complexe d'André*, qui nous permettra, en outre, de construire une bijection naturelle entre l'ensemble des permutations d'André et celui des permutations alternantes.

Références

D. André, 1879, Développements de sec x et de tang x, *C.R. Acad. Sci. Paris* **88**, 965–967.

D. André, 1881, Sur les permutations alternées, *J. Math. Pures Appl.* **7**, 167–184.

T. J. Buckholtz et D. E. Knuth, 1967, Computation of tangent, Euler and Bernoulli numbers, *Math. Comp.* **21**, 663–688.

F. N. David et D. E. Barton, 1962, *Combinatorial Chance* (Griffin, London).

D. Foata and M.-P. Schützenberger, 1970, *Théorie géométrique des polynômes euleriéns* (Springer, Berlin).

W. O. Kermack et A. G. McKendrick, 1938, Some properties of points arranged on a Möbius surface, *Math. Gaz.* **22**, 66–72.

R. Mullin et G.-C. Rota, 1970, On the foundations of combinatorial theory, III: Theory of binomial enumeration, *Graph Theory and its Applications* (B. Harris, ed.; Academic Press, New York) 167–213.

N. Nielsen, 1923, *Traité élémentaire des nombres de Bernoulli* (Gauthier-Villars, Paris).

J. Riordan, 1958, *An Introduction to Combinatorial Analysis* (Wiley, New York).

A PROPOS DU RELATION RATIONELLES FONCTIONNELLES

M. SCHUTZENBERGER
IRIA - Université - Paris 7
FRANCE

1. - INTRODUCTION

Le théorème de Mc Naughton ([2]) est une généralisation à l'ensemble X^{ω} des mots infinis sur un alphabet X du théorème de Kleene sur le monoïde libre X^*. Nous nous proposons d'en simplifier un peu la preuve originale grâce à l'idée due à Büchi ([1]) d'utiliser un cas particulier du Théorème de Ramsey.

Nous employons les notations standards de Eilenberg : $X^+ = XX^* = X^* \setminus \{1\}$, et $|f|$ = la longueur du mot f de X^* . Une partie A de X^* est reconnaissable ($A \in Rec$) ssi il existe un morphisme φ de X^* dans un monoïde fini qui satisfait $A\varphi\varphi^{-1} = A$ (qui "reconnaît" A).

L'écriture $s \in \omega(A)$ servira pour exprimer que le mot infini $s \in X^{\omega}$ possède une infinité de facteurs gauches dans la partie A de X^* .

Ceci permet de définir $\overset{\omega}{\mathrm{Rec}}$ comme la plus petite famille R de parties de X^{ω} qui satisfasse les deux conditions :

(i) Pour tout $A \in \mathrm{Rec}$, R contient l'ensemble $\{s \in X^{\omega} = s \in \omega(A)\}$

(ii) R est fermée par rapport aux opérations booléennes, c'est à dire que si $P, Q \in R$, la famille R contient $P \cup Q$, $P \setminus Q$ et $P \cap Q$.

Nous chercherons à établir l'identité de $\overset{\omega}{\mathrm{Rec}}$ et de la famille $\overset{\omega}{\mathrm{Rat}}$ définie comme la plus petite famille R' satisfaisant les deux conditions :

(iii) $c\, B^{\omega} \in R'$ pour tout c, $B \in \mathrm{Rat}$ tel que $1 \notin B$, $\emptyset \neq B$.

(iiii) $P, Q \in R' \Rightarrow P \cup Q \in R'$.

La preuve repose sur le théorème suivant :

THEOREME 1 (Ramsey, Büchi).

Soient φ un morphisme de X^* dans un monoïde fini M et $s = a_0\, a_1 \ldots a_n \ldots$ une factorisation d'un mot infini s de X^{ω}. $(a_0, a_1, \ldots, a_n, \ldots \in X^{+})$.

Il existe un élément m, un idempotent u et une factorisation $s = c_0\, c_1 \ldots c_n$ obtenue en regroupant les termes de la factorisation précédente qui satisfait les conditions :

$c_0\varphi = m = m\,u$; et pour tout $n \in \mathbb{N}$ $c_{n+1}\varphi = u = u^2$;

PREUVE - Soit A l'ensemble des facteurs de s de la forme $a_n\, a_{n+1} \ldots a_{n'}$ $(1 \leqslant n \leqslant n')$ et $k = \mathrm{Card}\,(A\varphi)$.

Si $k = 1$, $A\varphi$ se réduit à un idempotent u et le résultat est trivialement vérifié

en remplaçant a_0 par $a_0\ a_1$ et en prenant $m = (a_0\ a_1)\varphi = a_0\varphi\ u = a_0\varphi\ u\ u = m\ u$

Nous pouvons donc procéder par induction sur k.

Prenons $m \in A\varphi$ quelconque et notons $P = \{p_1 < p_2 < \ldots\}$ l'ensemble des indices $p \in \mathbb{N}$ tels qu'aucun des facteurs $a_p\ a_{p+1} \ldots a_{p'}$ $(1 \leqslant p \leqslant p')$ n'appartienne à $m\bar{\varphi}^1$.

Si P est infini, on peut, en regroupant les termes, obtenir la factorisation $a'_0\ a'_1 \ldots a'_n$ de s où chaque a'_n $(n \geqslant 1)$ est égal au produit $a_p\ a_{p+1} \ldots a_{p'-1}$ avec $p = p_n$, $p' = p_{n+1}$. L'ensemble A' des produits $a'_n\ a'_{n+1} \ldots a'_{n'}$ $(1 \leqslant n \leqslant n')$ a son image par φ contenue dans $A\varphi \setminus \{m\}$ et le résultat découle de l'hypothèse d'induction.

Considérons donc, maintenant, le cas où P est fini. Il existe un $q \in \mathbb{N}$ tel que pour tout $n \geqslant q$, au moins un des produits $a_n\ a_{n+1} \ldots a_{n'}$ $(n' \geqslant n)$ appartiennent $m\varphi^{-1}$.

Ceci permet de trouver une factorisation $s = a'_0\ a'_1 \ldots a'_n \ldots$ où $a'_n\varphi = m$ pour tout n positif.

Maintenant comme M est fini m a une puissance positive m^r qui est un idempotent. Regroupant les termes r par r on est ramené au cas de $k = 1$. Q.E.D.

Nous dirons que la factorisation $c_0\ c_1 \ldots c_n \ldots$ décrit dans l'énoncé une mu-factorisation de s subordonnée à $a_0\ a_1 \ldots a_n$.

Nous désignerons par $\Pi(s)$ l'ensemble des paires $(m = m\ u,\ u = u^2) \in M \times M$

tel que s admette au moins une mu-factorisation subordonnée à la factorisation $s = x_0 x_1 \ldots x_n \ldots$ où $x_0, x_1, \ldots, x_n, \ldots \in X$(donc à n'importe quelle autre factorisation).

2. - UNE CONSTRUCTION

Nous considérons deux parties reconnaissables non vides B, C $\in X^*$, où $1 \notin B$, et d'après le Théorème de Kleene il existe des morphismes φ' et φ de X^* dans des monoïdes finis M' et M et une application $[\ ]$ de M dans M' × M' qui satisfont les conditions suivantes :

(1) φ' reconnaît CB^* et B^+;

(2) Pour tout mot f de X^* , $[f\varphi]$ est l'ensemble des paires $(f'\varphi', f''\varphi')$ où $f', f'' \in X^*$, $f = f' f''$.

Il sera commode (et toujours possible) de supposer $1\varphi'\varphi'^{-1} = 1\varphi\varphi^{-1} = 1$. Désignons maintenant par V l'ensemble des paires $(m = m\,u, u = u^2) \in M \times M$ tel qu'il existe q, r, s $\in$ M' satisfaisant les conditions :

$q \in C\,B^*\varphi'$; $r\,s \in B^+\varphi'$;

$(q, r) \in [m]$; $(s, r) \in [u]$.

PROPRIETE 1- Soient $s \in X^\omega$ et $(m, u) \in U(s)$. On a $s \in C\,B^\omega$ ssi $(m, u) \in V$.

PREUVE : Supposons d'abord $(m, u) \in V$ et considérons une mu-factorisation $a_0\,a_1 \ldots a_n \ldots$ de s.

Notre hypothèse implique l'existence de factorisations $a_n = a'_n\,a''_n$ telles que l'on ait identiquement $a'_0\varphi' = q \in (C\,B^*)\varphi'$; $a''_n\varphi' = r$; $a'_{n+1}\varphi' = s$ où $r\,s \in B^+\varphi'$ et où, par conséquent :

$a'_0 \in C\,B^*$, $a''_n\,a'_{n+1} \in B^+$ ce qui établit $s \in C\,B^\omega$.

Réciproquement soit $s \in C\,B^\omega$, c'est-à-dire $s = c\,b_0\,b_1 \ldots b_n \ldots$ où $c \in C\,B^*$, $b_n \in B^+$.

Nous pouvons choisir une mu-factorisation $s = a_0\, a_1 \ldots a_n \ldots$ de telle sorte que les conditions suivantes soient vérifiées :

$a_0 = c\, b_0 \ldots b_n\, f \qquad (n \geqslant 0)$;

$b_{n+1} = f\, g$;

$a_1 = g\, b_{n+2} \ldots b_{n'}\, f' \qquad (n' \geqslant n+2)$;

$b_{n'+1} = f'\, g'$;

$f\, \varphi' = f'\, \varphi' \quad (= r)$.

Posant $q = (c\, b_0 \ldots b_n)\, \varphi'$

et $s = g\, b_{n+2} \ldots b_{n'}$, on en déduit immédiatement que $(m, u) \in V$.

Q.E.D.

Soit maintenant $u \neq 1$ un idempotent de M. D'après l'hypothèse $1\varphi\varphi^{-1} = 1$ on a $1 \notin u\varphi^{-1}$. Nous notons E_u la plus petite partie de X^+ telle que $u\varphi^{-1} = E_u^+ X^*$ et nous posons :

$E'_u = E_u \setminus E_u X^+$ ce qui entraine que tout mot de $u\varphi^{-1}$ ait exactement un facteur gauche dans E'_u.

Nous aurons besoin de la :

REMARQUE 2. La relation $a, b, abc \in u\varphi^{-1}$ $(a, b, c \in X^+)$ implique $b\, c \in u\varphi^{-1}$.

PREUVE - Soit $m = c\varphi \in M$. les hypothèses équivalent à $u\, u\, m = u$.

Donc (bc) $\varphi \cdot u\, m = u$. Q.E.D.

Soit enfin :

$K_u = U \setminus X^* E'_{u'} : u' \in W_u \}$ où, par commodité,

$W_u = \{u' = u'^2 \in M : u \notin M\, u'\, M\}$;

La propriété suivante traduit en termes de monoïdes la méthode de Mc Naughton.

On pourrait (au prix d'une légère complication) remplacer K_u par R_u^* où $R_u = R'_u \setminus R'_u X^+$ avec R'_u = l'ensemble des mots $f \in X^+$ tels que $u \notin M.f\varphi.M$.

PROPRIETE 3 - Soit $(m,u) \in V$.

La partie $A = m\varphi^{-1}(u\varphi^{-1})^\omega$ de X^ω est l'ensemble des mots infinis tels que l'on ait :

(1) $s \in \omega(F)$ où $F = m\varphi^{-1}.E_u.E'^{-1}_u$;

(2) $s \notin \omega(K_u)$.

PREUVE. Soit d'abord $s \in C\,B^\omega$ et $(m, u) \in U(s)$. On peut trouver une mu-factorisation $s = a_0 a_1 \ldots a_n \ldots$ dans laquelle tous les a_{n+1} appartiennent à E_u. Comme $(a_0 a_1 \ldots a_n)\varphi = m$, identiquement, ceci montre que $s \in \omega(F)$.

Supposons maintenant $u' \in W_u$, $h \in E'_u$, et que $g\,h$ soit un facteur gauche de s. Comme $u \in M.b\varphi.M$ pour tout facteur b de $a_1 \ldots a_n \ldots$, on a que g est un facteur gauche de a_0, donc que $s \notin \omega(K_u)$ puisque tout mot a au plus un facteur gauche dans chacun des E'_u, $(u' \in W_u)$.

Réciproquement soit s un mot infini ayant une infinité de facteurs gauches $f_n = g_n e_n e'_n$ dans F ($g_n \in m\varphi^{-1}$; $e_n \in E_u$; $e'_n \in E'_u$).

Supposons d'abord qu'il existe un mot g tel que $g_n = g$ pour une suite infinie de f_n. Comme aucun mot n'a plus de un facteur gauche dans E'_u, nous pouvons prendre une sous suite de la précédente telle que chaque $e_n e'_n$ soit un facteur gauche

de e_{n+1}. La conclusion $s \in A$ résulte alors immédiatement de la Remarque 2

Supposons maintenant qu'un tel mot g n'existe pas. Nous pouvons prendre une sous suite telle que chaque g_{n+1} ait la forme $f_n h_n$ ($h_n \in X^+$), ce qui donne une factorisation $s = a_0 a_1 \dots a_n$ où $a_0 = g_0 e_0$ et, identiquement, $a_{n+1} = e'_n h_{n+1} e_{n+1}$. Utilisant le théorème 1, il existe un idempotent $\bar{u}$ et une $\bar{m}\,\bar{u}$-factorisation subordonnée à la précédente $s = b_0 b_1 \dots b_n \dots$ où $b_0 = f_p$ pour un certain $p \in \mathbb{N}$ et où par conséquent $\bar{m} = m$.

Comme $b_{n+1} \in E'_u X^* E_u$, par construction, nous avons :

(i) $\bar{u} = \bar{u}^2 \in u M \cap M u$.

Introduisons alors l'hypothèse $s \notin \omega(K_u)$. Comme s a une infinité de facteurs dans $\bar{u}\,\varphi^{-1}$, on a $s \in \omega(X^* E'_{\bar{u}})$ et, par conséquent, $\bar{u} \notin W_u$, c'est à dire :

(ii) $u = u^2 \in M \bar{u} M$.

Comme M est fini, les deux relations : $\bar{u} \in u M \cap M u$ et $u \in M \bar{u} M$ entrainent que u et $\bar{u}$ appartiennent à la même $\mathcal{H}$ classe de M, donc qu'ils soient égaux puisque $u = u^2$, $\bar{u} = \bar{u}^2$. Ceci achève la preuve de $s \in A$.

COROLLAIRE. Le monôme CB^ω appartient à Rec^ω.

PREUVE. Ceci résulte immédiatement des propriétés 1. et 3.

Q.E.D.

3. - FIN DE LA DEMONSTRATION

THEOREME DE BUCHI. La famille $\overset{\omega}{\mathrm{Rat}}$ est fermée par rapport aux opérations booléennes.

PREUVE - Comme X^{ω} appartient à $\overset{\omega}{\mathrm{Rat}}$, et comme cette famille est fermée par union, il suffit de montrer qu'elle contient $D = X^{\omega} \setminus C\ B^{\omega}$, avec $C\ B^{\omega}$ comme dans la section précédente. Or ceci est trivial d'après le théorème de Ramsey-Büchi et le corollaire 4 puisque celui-ci montre que D est l'ensemble des $s \in X^{\omega}$ tels que $U(s) \cap V = \emptyset$ ou, de façon équivalente, $U(s) \not\subset V$.

Q.E.D.

THEOREME DE MC NAUGHTON - Les familles $R' = \overset{\omega}{\mathrm{Rat}}$ et $R = \overset{\omega}{\mathrm{Rec}}$ sont identiques.

PREUVE - L'inclusion de R' dans R résulte immédiatement de la Propriété 3 et des définitions de R et de R' puisque F et K_u sont certainement des parties reconnaissables de X^*.

Comme R' est fermée par les opérations booléennes d'après le théorème précédent, il suffit pour établir l'inclusion opposée de considérer un élément m d'un monoïde fini M et un morphisme $\varphi : X^* \to M$ et de prouver $A \in \overset{\omega}{\mathrm{Rat}}$ où $A = \{s \in X^{\omega} : s \in \omega(m\,\varphi^{-1})\}$.

Or de nouveau ceci est trivial puisque l'on peut écrire $A = m\,\varphi^{-1}.\ B^{+}$ où $B = \{f \in X^{+} : m.\ f\,\varphi = m\}$.

Q.E.D.

OBSERVATION. Pour tout morphisme de semi groupe $\varphi : X^+ \to M$ notons $\bar{\varphi}^{-1}$ l'application envoyant chaque $(m, u) \in M \times M$ sur $m\varphi^{-1}(u\varphi^{-1})^\omega \in X^\omega$ et $\bar{\varphi}$ l'application réciproque telle que pour chaque $s \in X^\omega$ on ait $(m, u) \in s\,\bar{\varphi}$ ssi $s \in (m, u)\,\bar{\varphi}^{-1}$.

On dira que φ reconnaît une partie A de X^ω ssi $A = A\,\bar{\varphi}\,\bar{\varphi}^{-1}$

(donc $V\,\bar{\varphi}^{-1}\,\bar{\varphi} = V$ où $V = A\,\bar{\varphi}$).

D'autre part appelons semi-groupe syntactique de la partie A de X^ω le semi groupe quotient $S = X^+\sigma$, où pout tout f, $f' \in X^+$ on pose comme dans le cas fini habituel :

$f\,\sigma = f'\,\sigma$ ssi

$g\,f\,s, g\,f'\,s \in A$ ou $g\,f\,s, g\,f'\,s \notin A$ pour chaque $(g, s) \in X^* \times X^\omega$.

Ces notations permettent de formuler de la façon suivante le Théorème de Buchi.

PROPRIETE. Le monoïde syntactique S de A est fini ssi $A \in \overset{\omega}{\text{Rat}}$. De plus dans ce cas :

le morphisme σ reconnaît A et S est image homomorphe de tout monoïde $X^+\varphi$ où le morphisme φ reconnaît A.

PREUVE. Supposons S fini et $(m, u) \in A\,\bar{\sigma}$. Il existe des mots $a_j \in X^+$ tels que $a_0\,\sigma = m$; $a_{j+1}\,\sigma = u$ $(j \in \mathbb{N})$ et $s = a_0\,a_1 \ldots a_n \ldots \in A$.
Soit $s' \in (m, u)\,\bar{\sigma}^{-1}$, c'est-à-dire $s' = b_0\,b_1 \ldots b_n \ldots$ où $b_j\,\sigma = a_j\,\sigma$ identiquement. D'après la définition de σ on a $h_0\,h_1 \ldots h_n\,a_{n+1} \ldots a_{n+h} \ldots \in A$ pour tout $n \in \mathbb{N}$, donc $s' \in A$.

Ceci montre que quand S est fini, le morphisme σ reconnaît A et que par conséquent $A \in \overset{\omega}{\text{Rat}}$.

Supposons maintenant $A \in \overset{\omega}{Rat}$. On déduit facilement de la Propriété 2 l'existence d'un semi-groupe fini M et d'un morphisme surjectif $\varphi : X^+ \to M$ qui reconnaît A. Pour prouver que S est image homomorphe de M, et par conséquent que S est fini, il suffit de considérer deux mots f, $f' \in X^+$ tels que $f\sigma \neq f'\sigma$ et de montrer $f\varphi \neq f'\varphi$.

L'hypothèse implique qu'il existe $(g, s) \in X^* \times X^\omega$ tels que par exemple $gfs \in A$ et $gf's \notin A$. De plus comme M est fini, on a $s \in (m, u)\bar{\varphi}^{-1}$ pour au moins une paire $(m, u) \in M \times M$. Maintenant comme φ reconnaît A, on a $(gf\varphi m, u) \in A\bar{\varphi}$ et $(gf'\varphi m, u) \notin A\bar{\varphi}$, donc $f\varphi \neq \varphi'\varphi$ Q.E.D.

REFERENCES

[1] BUCHI, J.R. (1962) - On a decision Methode ...
Proc. 1960 Int. Congress. Logic Methodology and Phil. of Science.
p. 1 - 11.

[2] R. Mc. NAUGHTON (1966) - Testing and generating Infinite sequences by finite automata.
Inf. and Control 9 - P. 521 - 530.

Séminaire Dubreil.
Algèbre

Marcel P. Schützenberger

Sur une construction de Gilbert de B. Robinson

Séminaire Dubreil. Algèbre, tome 25, n° 1 (1971-1972), exp. n° 8, p. 1-4.
<http://www.numdam.org/item?id=SD_1971-1972__25_1_A8_0>

Séminaire DUBREIL
(Algèbre)
25e année, 1971/72, n° 8, 4 p.

8-01

28 février 1972

SUR UNE CONSTRUCTION DE Gilbert de B. ROBINSON [1]

par Marcel P. SCHÜTZENBERGER

1. Introduction.

La théorie de la représentation linéaire des groupes classiques utilise toute une série de constructions portant sur les tableaux standards de Young. La plus notable est peut-être celle de Gilbert de B. ROBINSON qui livre une bijection entre les permutations et les paires de tableaux standards de même forme, puisqu'elle donne une manière commode d'exprimer les "rising and lowering operators" de Young. Je me propose ici d'indiquer les grandes lignes de la preuve d'un résultat assez simple dont on peut déduire la plupart des autres propriétés sans devoir recourir de nouveau à des raisonnements combinatoires.

Dans ce qui suit, la forme d'un tableau (gauche) de Young est un intervalle fini A du plan entier $\underset{\sim}{Z} \times \underset{\sim}{Z}$ ordonné de façon naturelle $((x , y) \leq (x' , y')$ si et seulement si $x \leq x'$ et $y \leq y')$, et un tableau est un morphisme bijectif φ (d'ensemble ordonné) d'un tel intervalle sur un intervalle de $\underset{\sim}{Z}$, ou plus exactement une classe d'équivalence de semblables morphismes par rapport aux translations de leur domaine. Un tableau est dit rectangulaire, si et seulement si sa forme est le produit direct $[p] \times [q]$ de deux chaînes $[p]$ $(= \{1 < 2 < \ldots < p\})$ et $[q]$. Il est principal si et seulement si l'intervalle de $\underset{\sim}{Z} \times \underset{\sim}{Z}$, qui est sa forme, a un élément minimum unique.

Par exemple,

$$\begin{array}{cccc} 8 & 11 & 13 & 14 \\ 6 & 9 & 10 & 12 \\ 3 & 4 & 5 & 7 \end{array}$$

est un tableau rectangulaire,

$$\begin{array}{cccc} 8 & 11 & & \\ 6 & 9 & 10 & \\ 3 & 4 & 5 & 7 \end{array}$$

est un tableau principal,

$$\begin{array}{cccc} 8 & 11 & & \\ 6 & 9 & 10 & \\ & & 5 & 7 \end{array}$$

est un tableau.

Dans tous les cas, la condition que φ soit un morphisme bijectif exprime simplement que les valeurs inscrites dans le tableau croissent (strictement) le long

des lignes et des colonnes.

2. Rappel de quelques propriétés des tableaux.

Si $I = \{z , z + 1 , \dots , z + r - 1\}$ est un intervalle de $\underset{\sim}{Z}$, nous noterons $I + 1$, l'intervalle $\{z + 1 , \dots , z + r\}$ obtenu en translatant l'image I d'une unité.

L'énoncé connu suivant sert à définir une bijection $\varphi \longmapsto \varphi\partial$ (appelée promotion) sur l'ensemble des tableaux ayant pour forme un intervalle donné A de $\underset{\sim}{Z} \times \underset{\sim}{Z}$.

2.1. Soit $\varphi : A \to I$ un tableau. Il existe un, et un seul tableau,

$$\varphi' = \varphi\partial : A \to I + 1$$

tel que l'on ait $z\varphi'^{-1} \leqslant z\varphi^{-1}$ pour chaque $z \in I \cap (I + 1)$.

De façon algorithmique, $\varphi\partial$ est obtenu à partir de φ en retirant la plus petite valeur, min (I), du tableau φ ; en "déplaçant" chacune des autres valeurs en bas ou à gauche comme dans le jeu du taquin, et en ajoutant enfin la valeur $1 + \max(I)$ à la dernière place restée libre. Ceci est illustré par l'exemple ci-dessous où sont utilisées plusieurs applications de l'opérateur de promotion ∂.

$$\varphi = \begin{matrix} 8 & 11 & 13 & 14 \\ 6 & 9 & 10 & 12 \\ 3 & 4 & 5 & 7 \end{matrix} \to \varphi\partial = \begin{matrix} 8 & 11 & 13 & 15 \\ 6 & 9 & 10 & 14 \\ 4 & 5 & 7 & 12 \end{matrix}$$

$$\to \varphi\partial^2 = \begin{matrix} 8 & 11 & 15 & 16 \\ 6 & 9 & 13 & 14 \\ 5 & 7 & 10 & 12 \end{matrix} \to \varphi\partial^4 = \begin{matrix} 11 & 15 & 16 & 17 \\ 8 & 9 & 13 & 14 \\ 6 & 7 & 10 & 12 \end{matrix} \to \text{etc.}$$

On voit facilement que l'opération inverse ∂^{-1} est simplement la conjuguée de ∂ par rapport à l'involution $\varphi \to \overline{\varphi}$ consistant à remplacer à la fois l'ordre sur $\underset{\sim}{Z} \times \underset{\sim}{Z}$ et l'ordre sur $\underset{\sim}{Z}$ par leurs ordres opposés

$$(\overline{\varphi} = \begin{matrix} -7 & -5 & -4 & -3 \\ -12 & -10 & -9 & -6 \\ -14 & -13 & -11 & -8 \end{matrix}, \text{ par exemple pour } \varphi \text{ comme ci-dessus}).$$

L'opération de promotion ∂ permet de définir une involution remarquable $\varphi \longmapsto \varphi\#$ appelée contraire. Pour abréger, nous nous bornons à décrire l'algorithme qui en fournit la construction et pour cela, nous considérons un tableau $\varphi : A \to I$ et la suite $\{\varphi\partial^p ; p \geqslant 0\}$ des tableaux qui s'en déduisent par itération de ∂. Soit $n = \text{Card}(I)$. Pour chaque $p = 0 , \dots , n - 1$, il existe exactement une case du tableau, disons a_p, telle que $a_p \varphi\partial^p \in I$ et $a_p \varphi\partial^{p+1} \notin I$. Nous définissons $\varphi\#$ par la condition que $-(a_p \varphi\#)$ soit égal à la p-ième plus petite valeur de l'intervalle initial I. Par conséquent, $\varphi\#$ a pour domaine A et pour image $-I$.

8-03

Par exemple, si φ est le tableau principal

$$\begin{array}{cccccccc} & & & & 6 & & & \\ & & & 3 & & 5 & & \\ 1 & & 2 & & 4 & & 7 & \end{array},$$

la suite $(\varphi\partial^p\ ,\ 0 \leqslant p \leqslant 7)$ est constituée par φ ; $\varphi\partial = \begin{array}{cccccccc} & & & & 6 & & & \\ 2 & & 4 & & 7 & & 8 & \end{array}$;

$\varphi\partial^2 = \begin{array}{cccccccc} & & & 6 & & & & \\ 3 & & 4 & & 7 & & 8 & \end{array}$; $\varphi\partial^3 = \begin{array}{cccccccc} & & & 6 & & & & \\ 4 & & 7 & & 8 & & 10 & \end{array}$; $\varphi\partial^4 = \begin{array}{cccccccc} & & & 11 & & & & \\ 5 & & 7 & & 8 & & 10 & \end{array}$; $\varphi\partial^5 = \begin{array}{cccccccc} & & & 11 & & & & \\ 6 & & 7 & & 8 & & 10 & \end{array}$;

$\varphi\partial^6 = \begin{array}{cccccccc} & & & 11 & & & & \\ 7 & & 8 & & 10 & & 13 & \end{array}$; $\varphi\partial^7 = \begin{array}{cccccccc} & & & 11 & & & & \\ 8 & & 10 & & 13 & & 14 & \end{array}$,

et l'on en déduit que le contraire $\varphi\#$ est le tableau

$$\begin{array}{cccccccc} & & & & -4 & & & \\ & & & -5 & & -2 & & \\ -7 & & -6 & & -3 & & -1 & \end{array}.$$

On démontre que $\varphi\#\# = \varphi$ et que pour chaque entier r (positif ou négatif), on a identiquement $\varphi\partial^r\,\# = \varphi\#\,\partial^{-r}$. Ces relations n'utilisent pas l'hypothèse que φ est un tableau, et elles resteraient vraies si φ était un morphisme bijectif d'un ensemble partiellement ordonné fini quelconque sur un intervalle de $\underset{\sim}{Z}$.

Le phénomène remarquable est que, quand φ est un tableau rectangulaire, le contraire $\varphi\#$ de φ est précisément égal à l'opposé $\overline{\varphi}$ de φ défini plus haut.

Ceci ne serait plus vrai pour les morphismes bijectifs dans $\underset{\sim}{Z}$ d'un produit direct de trois chaînes ou plus, et la preuve de ce résultat nécessite que nous introduisions quelques notions propres au plan $\underset{\sim}{Z} \times \underset{\sim}{Z}$.

3. Ordre croisé.

Nous définissons dans $\underset{\sim}{Z} \times \underset{\sim}{Z}$ un nouvel ordre, dit croisé, distinct de l'ordre naturel $\leqslant$, en posant $a \searrow a'$ si, et seulement si, les deux points

$$a = (x\ ,\ y)\ ,\quad a' = (x'\ ,\ y')$$

satisfont l'une des deux relations

$$(a = a')\quad \text{ou}\quad (x < x'\quad \text{et}\quad y \geqslant y')\ .$$

De façon duale, (par rapport à l'échange des deux coordonnées), nous poserons $a \nwarrow a'$ si, et seulement si,

$$(a = a')\quad \text{ou}\quad (x \leqslant x'\quad \text{et}\quad y > y')\ .$$

Il résulte de ces définitions que toute paire de points de $\underset{\sim}{Z} \times \underset{\sim}{Z}$ est comparable pour au moins une des relations $\leqslant$, $\searrow$ ou $\nwarrow$, et que l'on a

$$(a \searrow a'\quad \text{et}\quad a' \nwarrow a)\quad \text{si, et seulement si,}\quad a = a'\ .$$

Considérons en particulier un tableau $\varphi : A \longrightarrow I$ et deux éléments consécutifs

i et $i' = i + 1$ de son image I. En raison du fait que les valeurs $a\varphi$ $(a \in A)$ sont croissantes selon les lignes et selon les colonnes, on s'aperçoit que les points $a = i\varphi^{-1}$ et $a' = i'\varphi^{-1}$ sont nécessairement dans l'une des relations $a \searrow a'$ ou $a' \nwarrow a$. Sinon ils seraient dans la relation $a < a'$, et l'on aurait

$$a = (x , y) , \quad a' = (x' , y') \quad \text{avec} \quad (x < x' \quad \text{et} \quad y < y') ,$$

ce qui entrainerait que les points $b = (x + 1 , y)$ et $b' = (x , y + 1)$ satisfassent

$$i = a\varphi < b\varphi , \qquad b'\varphi < a'\varphi = i + 1 ,$$

ce qui est impossible puisque i et $i + 1$ sont consécutifs dans l'image $I = A\varphi$ de φ. L'essentiel de la démonstration de l'identité $\varphi\# = \overline{\varphi}$ repose sur la remarque (facile à vérifier) que si i appartient encore à l'image de $\varphi\partial$ (c'est-à-dire si $i \neq \min (I)$) les deux points $b = i(\varphi\partial)^{-1}$ et $b' = i'(\varphi\partial)^{-1}$ sont dans la même relation $\searrow$ ou $\nwarrow$ que les points $a = i\varphi^{-1}$ et $a' = i'\varphi^{-1}$. Autrement dit, les relations d'ordre croisé entre valeurs consécutives de l'image sont invariantes par promotion.

Un raisonnement un peu plus long permet d'établir que, dans les mêmes conditions, chaque relation $i\varphi^{-1} \searrow i'\varphi^{-1}$ équivaut à $-i(\varphi\#)^{-1} \searrow -i'(\varphi\#)^{-1}$ quand φ est un tableau rectangulaire.

4. Un résultat combinatoire.

Nous considérons maintenant trois valeurs consécutives i, $i' = i + 1$ et $i'' = i + 2$ de l'image d'un tableau φ, et la transposition $\theta_i = (i' , i'')$: $\underset{\sim}{Z} \to \underset{\sim}{Z}$. Cette transposition sera dite admissible pour φ si, et seulement si, les points $a = i\varphi^{-1}$, $a' = i'\varphi^{-1}$, $a'' = i''\varphi^{-1}$ satisfont

$$(a' \nwarrow a \quad \text{et} \quad a \searrow a'') \quad \text{ou} \quad (a'' \nwarrow a \quad \text{et} \quad a \searrow a') ,$$

(ce qui implique en particulier que a' et a'' ne soient pas comparables pour l'ordre naturel $\leq$). Il est clair que si θ_i est admissible pour le tableau φ : $A \to I$, la bijection $\varphi\theta_i$: $A \to I$ est encore un tableau et, dans ce cas, on peut vérifier sans difficulté que $\varphi\partial\theta_i = \varphi\theta_i\partial$ quand $i \neq \min (I)$. La situation est un peu plus compliquée quand $i = \min (I)$, et le résultat combinatoire que nous avions en vue peut s'énoncer de la façon suivante :

Propriété. - Soient φ : $A \to I$ un tableau rectangulaire, $i = \min (I)$ et θ_i admissible pour φ. On a $\varphi\theta_i\partial^3 = \varphi\partial^3$ et $\varphi\theta_i\# = \varphi\#\overline{\theta}_i$, où $\overline{\theta}_i$ désigne la transposition de $\underset{\sim}{Z}$ échangeant $-i'$ et $-i''$.

BIBLIOGRAPHIE

[1] ROBINSON (G. de B.). - On the representations of the symmetric group, Amer. J. of Math., t. 60, 1938, p. 745-760.

Marcel P. SCHÜTZENBERGER
97 rue du Ranelagh
75016 PARIS

LOGIC, METHODOLOGY AND PHILOSOPHY OF SCIENCE IV

PROCEEDINGS OF THE FOURTH INTERNATIONAL CONGRESS FOR LOGIC, METHODOLOGY AND PHILOSOPHY OF SCIENCE, BUCHAREST, 1971

Edited by

PATRICK SUPPES
Stanford University, Stanford, USA
LEON HENKIN
University of California, Berkeley, USA
ATHANASE JOJA
Académie Roumaine, Bucarest, Roumaine
GR. C. MOISIL
Université de Bucarest, Bucarest, Roumaine

1973

NORTH-HOLLAND PUBLISHING COMPANY
AMSTERDAM • LONDON

AMERICAN ELSEVIER PUBLISHING COMPANY, INC.
NEW YORK

SUR UN LANGAGE EQUIVALENT AU LANGAGE DE DYCK

M. P. SCHÜTZENBERGER

Faculté des Sciences, Paris, France

1. Introduction

Le langage de Dyck D_2 sur *deux* paires de lettres $\{\bar{y}, y, \bar{y}', y'\}$ est comme on sait, défini de façon équivalente, comme la solution de l'équation

$$\xi = 1 + \bar{y}\xi y\xi + \bar{y}'\xi y'\xi$$

ou comme la classe de 1 pour la congruence

$$1 \equiv \bar{y}y \equiv \bar{y}'y'$$

sur le monoïde libre $\{\bar{y}, y, \bar{y}', y'\}^*$.

Appelant suivant Eilenberg *cône* $\mathscr{C}(L)$ d'un langage L, la famille des langages qui peuvent être déduits de L par une relation rationnelle, on sait que le cône $\mathscr{C}(D_2)$ est l'ensemble des langages algébriques.

Cette propriété n'est pas partagée par le langage de Dyck $D_1 = D_2 \cap \{\bar{y}, y\}^*$ sur une seule paire de lettres.

On se propose de montrer qu'au contraire la même propriété est possédée par le langage $L \subset \{\bar{y}, y\}^*$ défini de façon équivalente comme :

— le quotient de $\{\bar{y}, y\}^* = Y^*$ par la congruence définie par :

$$\bar{y}y \equiv \bar{y}\bar{y}y\bar{y}yy\,;$$

— la solution de l'équation

$$\xi = \bar{y}y + \bar{y}\xi\xi y\,;$$

— la partie L de $D_1\backslash 1$ formée des mots $d \in D_1\backslash 1$ tels que pour chaque factorisation $d = a\bar{y}b$ $(a, b \in Y^*)$ le mot $\bar{y}b$ ait exactement un facteur gauche dans $D_1\backslash 1$ ssi $a \in 1 \cup Y^*y$.

On observera enfin que *l'équivalence rationnelle* de D_2 et L $(\mathscr{C}(D_2) = \mathscr{C}(L))$ entraîne celle de D_2 et de tout langage défini par une équation de la forme $\xi = a + b\xi c\xi d$ où cette fois a, b, c et d sont quatre mots vérifiant des conditions assez peu restrictives (par exemple que $\{a, b, c\}$ engendre

librement le monoïde $\{a, b, c\}^*$). En raison de sa simplicité cette dernière équation peut présenter des avantages techniques dans certains problèmes d'équivalence rationnelle avec D_2.

2. Les différentes définitions de L

Nous considérons $L \subset Y^*$ comme étant défini par l'équation

$$\xi = \bar{y}y + \bar{y}\xi\xi y.$$

Posant $X = \{\xi, \bar{y}, y\}$ ceci équivaut à $L = M \cap Y^*$, où M est la plus petite partie de X^* contenant ξ qui soit telle que

$$f, g \in X^*, \quad f\xi g \in M \Rightarrow f\bar{y}yg, \quad f\bar{y}\xi\xi yg \in M.$$

De façon équivalente, M peut être considéré comme le langage obtenu en remplaçant x par ξ dans la solution de l'équation

$$\xi = x + \bar{y}y + \bar{y}\xi\xi y.$$

Notant comme d'usage $|h|_z$ le nombre d'occurrences de la lettre z dans le mot h, nous déduisons immédiatement de la définition de M les deux propriétés suivantes :

2.1. $e \in M \Rightarrow e \in \{\xi\} \cup X^*(\bar{y}y + \bar{y}\xi\xi y)X^*$

2.2. $e \in M \Rightarrow |e|_{\bar{y}} = |e|_y$

et, si $e = fg$ où $f, g \in X^* \backslash \xi^*$, alors

$$|f|_{\bar{y}} > |f|_y.$$

PREUVE: En effet ces assertions sont trivialement vraies pour $e = \xi$ et si elles sont vraies pour un mot $e \in X^*$ elles le demeurent pour tout mot e' obtenu en remplaçant dans e une occurrence de ξ par $\bar{y}y$ ou par $\bar{y}\xi\xi y$.

Ecrivons $h' \in h\delta_i^{-1}$ $(i = 0, 1)$ ssi réciproquement il existe des mots $f, g \in X^*$ tels que $h = fu_i g$, $h' = f\xi g$ où $u_0 = \bar{y}y$, $u_1 = \bar{y}\xi\xi y$.

Rappelons que deux mots $a, b \in X^*$ *ne chevauchent pas* ssi il n'y a aucun mot $c \in XX^*$ tel que :

$$a \in X^*Xc, \quad \text{et} \quad b \in cXX^* \quad \text{ou}$$

$$a \in cXX^*, \quad \text{et} \quad b \in X^*Xc.$$

Cette condition est satisfaite ssi pour toute relation $fag = f'bg'$ $(f, f', g, g' \in X^*)$ l'on a l'une des quatre éventualités suivantes :

— $f'b$ un facteur gauche de f;

— $f'b$ un facteur gauche de fa et f un facteur gauche f' ;
— fa un facteur gauche de $f'b$ et f' un facteur gauche de f;
— fa un facteur gauche f'.

2.3. $h \in X^* \Rightarrow h\delta_0^{-1}\delta_1^{-1} = h\delta_1^{-1}\delta_0^{-1}$.

PREUVE: Ceci résulte immédiatement de ce que deux mots (éventuellement égaux) de $\{u_0, u_1\}$ ne chevauchent pas et que, de plus, aucun d'eux n'est facteur de l'autre quand ils sont différents.

Soit maintenant $\equiv$ la plus petite congruence sur X^* telle que

$$\xi \equiv \bar{y}y \equiv \bar{y}\xi\xi y.$$

2.4. *M est la classe de ξ pour $\equiv$ et L est la classe de $\bar{y}y$ pour la congruence ($\equiv$) sur Y^* définie par $\bar{y}y$ ($\equiv$) $\bar{y}\bar{y}y\bar{y}yy$.*

PREUVE: Supposant $e \in M$ tel que $e\delta_0^{-1} \cup e\delta_1^{-1} \subset M$, et $e = f\xi g$ ($f, g \in Y^*$), il résulte de 2.3 que l'on a encore $e'\delta_0^{-1} \cup e'\delta_1^{-1} \subset M$ pour $e' = fu_i g$ ($i = 0, 1$). Par induction ceci implique $M = \{h \in X^* : h(\delta_0^{-1} \cup \delta_1^{-1})^* = \xi\}$, donc

$$M = \{h \in X^* : h \equiv \xi\}.$$

Comme $\bar{y}\xi\xi y \in \bar{y}\bar{y}y\bar{y}yy\delta_0^{-1}\delta_0^{-1}$, la deuxième partie de l'énoncé résulte de la première.

COROLLAIRE 2.5: *Le langage L est rationnellement équivalent au langage N solution de l'équation*

$$\xi = x + \bar{y}\xi\xi y.$$

PREUVE: Soit φ le morphisme de $\{x, \bar{y}, y\}^*$ sur Y^* tel que $x\varphi = \bar{y}y$, $\bar{y}\varphi = \bar{y}$, $y\varphi = y$.

Il est clair que la restriction $\varphi|N$ est une bijection sur L.

Réciproquement, si $e = f\bar{y}zg \in L$ ($z = \bar{y}$ ou y) il résulte de 2.5 que l'on a $f\xi g \in M$ ssi $z = y$. De même si $fzyg \in L$ $z = \bar{y}$ ou y on a $f\xi g \in M$ ssi $z = \bar{y}$. Il en résulte que $N = L\bar{\varphi}$ (avec $\varphi\bar{\varphi} = 1$) où $\bar{\varphi} : Y^* \to \{\bar{y}, y, x\}^*$ est la relation rationnelle remplaçant par x tout $\bar{y}$ suivi d'un y, et par 1 tout y précédé d'un $\bar{y}$ et laissant inchangées les autres lettres.

2.6. *Soit $e = f\bar{y}g \in M$. On a $\bar{y}g = mg'$ où $g' \in yY^*$ et où $m \in M$ ou $\in M^2$ selon que $f \in Y^*(y + \xi)$ ou $\in 1 \cup Y^*\bar{y}$.*

PREUVE: L'énoncé est vrai pour $e = \xi$ et s'il est vrai pour $e = f'\xi g'$, il est encore vrai pour $f'u_i g'$.

Rappelons maintenant que le langage de Dyck D_1 est le sous-monoïde D^* de Y^* librement engendré par l'ensemble D des mots $d \in YY^*$ tels que :

— $|d|_{\bar{y}} = |d|_y$;

— $d = fg$, $f, g \in YY^* \Rightarrow |f|_{\bar{y}} > |f|_y$.

Cette condition implique que deux mots de D ne se chevauchent pas et que tout mot de Y^* ait au plus un facteur gauche (et droit) dans D. On sait aussi que :

Pour toute factorisation $f\bar{y}g$ d'un mot de D_1 ($f, g \in Y^*$), on a $\bar{y}g = d'g'$ où $g' \in 1 \cup yY^*$ et $d' \in D_1\backslash 1$, cette factorisation étant unique. On a alors $fg' \in D_1$.

2.7. *Les deux conditions suivantes* (D) *et* $(D)'$ *sur un mot* $d \in D_1\backslash 1$ *sont équivalentes* :

Pour toute factorisation $d = f\bar{y}g$ $(f, g \in Y^*)$,

(D) $\bar{y}g$ *a exactement un facteur gauche dans* $D_1\backslash 1$ *ssi* $f \in 1 \cup Y^*y$;

$(D)'$ $\bar{y}g = d'g'$ *où* $g' \in 1 \cup yY^*$ *et où* $d' \in D$ *ou* $\in D^2$ *selon que* $f \in Y^*\bar{y}$ *ou* $\in 1 \cup Y^*y$.

PREUVE: En vertu de $D_1 = D^*$ on peut écrire $\bar{y}g = d_1d_2 \ldots d_pg'$ où $p \geqslant 1$, $d_1, d_2, \ldots, d_p \in D$, $g' \notin DY^*$, donc $g' \in 1 \cup yY^*$. Comme $D \subset D_1\backslash 1$ p est le nombre de facteurs gauche dans $D_1\backslash 1$ de $\bar{y}g$.

Maintenant, comme $D \subset Y^*\bar{y}$, la condition (D) équivaut à la condition que $p \leqslant 2$ avec égalité ssi $f \in Y^*\bar{y}$, c'est-à-dire a $(D)'$.

PROPRIÉTÉ 2.8.: *L est la partie de $D_1\backslash 1$ définie par (D).*

PREUVE: La remarque 2.2 montre que $L \subset D \subset D_1\backslash 1$ et le fait que L satisfait (D) résulte de 2.6 et 2.7.

Réciproquement, on a $\bar{y}y \in D \cap L$. Supposons que l'implication $(D)' \Rightarrow L$ soit établie pour tous les mots plus courts que le mot $d \in D_1\backslash(1+\bar{y}y)$ satisfaisant $(D)'$.

On peut écrire $d = f\bar{y}g$ avec $f = 1$. Donc, $d \in D$, d'après $(D)'$ et plus précisément, $d = \bar{y}d_1d_2y$ où $d_1, d_2 \in D$.

Comme la condition (D) sur un mot, implique la même condition sur tous les facteurs dans $D_1\backslash 1$ de ce mot, l'hypothèse d'induction donne $d_1, d_2 \in L$, d'où évidemment,

$$d = \bar{y}d_1d_2y \in L.$$

3. Equivalence rationnelle de D_2 et de L

Comme L est algébrique et que par conséquent $L \in \mathscr{C}(D_2)$, il suffit de montrer que réciproquement $D_2 \in \mathscr{C}(L)$. Pour simplifier les calculs on établira plutôt $D_2' \in \mathscr{C}(N)$ où $D_2' \subset Y'^*$ $(Y' = \{\bar{y}, y, \bar{y}', y', y'', x\})$ est défini par l'équation

$$\xi = x + \bar{y}\xi y\xi y'' + \bar{y}'\xi y'\xi y''$$

et M par l'équation

$$\xi = x + \bar{y}\xi\xi y.$$

Comme $\mathscr{C}(L) = \mathscr{C}(N)$ ainsi qu'on l'a vu en 2.6 et comme $D_2' \in \mathscr{C}(D_2)$ puisque D_2' est algébrique, l'équivalence des inclusions $D_2 \in \mathscr{C}(L)$ et $D_2' \in \mathscr{C}(N)$ résulte immédiatement de la relation $D_2 = D_2'\varphi$ où φ est le morphisme de Y'^* dans lui-même envoyant y'' et x sur 1 et laissant inchangées les autres lettres.

De façon inverse, l'inclusion $D_2' \in \mathscr{C}(N)$ sera vérifiée en prouvant l'existence d'un morphisme $\psi : (\xi \cup Y')^* \to (\xi \cup X')^*$ $(X' = \{x, \bar{y}, y\})$ tel qu'en posant $a = \bar{y}\psi$, $a' = \bar{y}'\psi$, $b = y\psi$, $b' = y'\psi$, $c = y''\psi$, $d = x\psi$ les deux conditions suivantes soient satisfaites :

(1) $\xi\psi = \xi$ et ψ est injectif.

(2) Il existe un langage rationnel $R \subset Y'^*$ tel que $D_2' \subset R$ et que $R\psi \cap N$ soit la solution P de l'équation

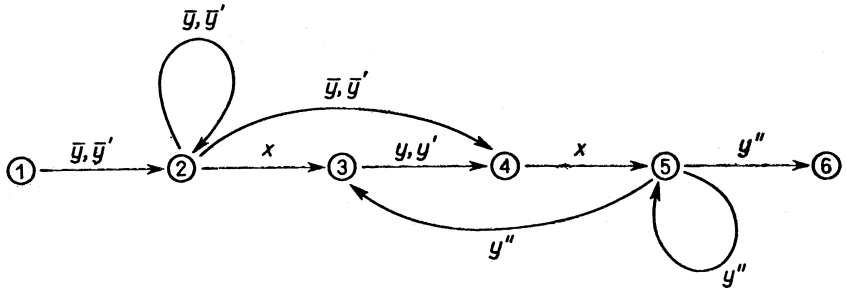
$$\xi = d + a\xi b\xi c + a'\xi b'\xi c.$$

En effet sous ces conditions on aura :

$$D_2' = (N \cap R\psi)^{-1}\psi, \text{ puisque } D_2'\psi \subset P, \text{ par construction.}$$

Nous commençons par la construction de R.

3.1. *$D_1'\backslash x$ est contenu dans le langage R' accepté par l'automate à 6 états avec 1 et 6 comme état initial et final respectivement.*



PREUVE: Soit $R_0 = (\bar{y}+\bar{y}')x(y+y')xy''$. On a $R_0 \subset R'$ et on voit sur le graphe que $fxg \in R' \Rightarrow fR_0g \subset R'$. Donc, par induction $\Rightarrow fR'g \subset R'$ ce qui établit $D_2'\backslash x \subset R'$.

Soit maintenant $X'' = \{\xi, x, \bar{y}, y\}$, et soit $\equiv$ la congruence sur X''^* définie par :

$$\xi \equiv x \equiv \bar{y}y \equiv \bar{y}\xi\xi y.$$

Sa restriction à X est la congruence étudiée plus haut et notant M' la classe de ξ on voit d'après 2.4 que $N = M'\backslash X''^*(\xi+\bar{y}y)X''^*$.

Nous choisissons maintenant le morphisme ψ et nous posons :

$$a = \bar{y}\psi = \bar{y}\bar{y}x\bar{y}\bar{y}; \quad b = y\psi = wyxyy$$
$$a' = \bar{y}'\psi = \bar{y}\bar{y}\bar{y}x\bar{y}; \quad b' = y'\psi = wyyxy$$
$$c = y, \quad d = x$$

où $w = \bar{y}xxy$.

Ce morphisme est injectif puisqu'aucun mot de $A = Y'\psi$ n'est facteur gauche d'un autre mot de A.

3.2. *P est contenu dans N et axb' et $a'xb$ appartiennent à $0 = \{h \in M' : X''^*hX''^* \cap M' = \emptyset\}$.*

PREUVE: La première assertion résulte de $a\xi b\xi c$, $a'\xi b'\xi c \in M'$ qui découle elle-même du parenthésage :

$$a\xi b\xi c = \bar{y}\left(\bar{y}x\left(\bar{y}\left(\bar{y}\xi(w)y\right)(xy)y\right)\xi y\right) \in M'$$
$$a'\xi b'\xi c = \bar{y}\left(\bar{y}\left(\bar{y}x\left(\bar{y}\xi(w)y\right)y\right)xy\right)\xi y \in M'.$$

Pour vérifier la seconde assertion, nous notons que d'après 2.6, on a $\bar{y}\xi y$, $\xi\xi\xi \in 0$. Par conséquent,

$$axb' \equiv a\xi b' = \bar{y}\bar{y}x\bar{y}\left(\bar{y}\xi(w)y\right)yxy \equiv \bar{y}\bar{y}x\bar{y}\xi yxy \in 0$$

et

$$a'xb \equiv a'\xi b = \bar{y}\bar{y}\bar{y}x(\bar{y}\xi wy)xyy \equiv \bar{y}\bar{y}\bar{y}\xi\xi\xi yy \in 0.$$

Fin de la preuve de $D_2 \in \mathscr{C}(L)$.

Il ne nous reste plus qu'à vérifier :

$$sx \in (x \cup S) \cap N \Rightarrow s \in P$$

où $S = R'\psi$. Comme le résultat est vrai pour $s = x$, $axbc$ et $a'xbx'c$ où les deux derniers sont les mots les plus courts de S, nous pouvons, par induction sur la longueur, nous borner à vérifier que tout mot $s \in S \cap N \backslash \{axbxc + a'xb'xc\}$ admet une factorisation $s = s_1vs'$ telle que $v = axbxc$ ou $a'xb'xc$ et que $s_1xs' \in S \cap N_1 + x$.

Soit donc un tel mot s. Considérant l'automate qui définit R', l'hypothèse $s \in S$ implique l'existence d'une factorisation $s = s_1 a s_2$ où $s = s_1 a' s_2$ avec $s_1 \in A^*$ et $s_2 \in A^* \backslash A^*(a+a')A^*$. De plus, la même hypothèse entraîne $s_2 \in x(b+b')x \subset s'$ où $s_1 x s' \in x \cup S$.

On a donc $s = s_1 r s'$ où $r \in (a+a')x(b+b')xc$. Comme $r \in P$ si $r = axbxc$ ou $r = a'xb'xc$ il n'y a donc qu'à vérifier $r \neq axb'xc, a'xbxc$, ce qui résulte immédiatement de 3.2 puisque $s \in N$.

Note bibliographique. Le langage défini par l'équation $\xi = d+a\xi b\xi c$ a été introduit par M. Nivat (*Thèse*, Paris, 1967) qui l'appele „langage de expressions arithmétiques". Un élève de M. Nivat, Y. Cochet a traité de façon approfondie dans sa *Thèse* (Rennes, 1971) les langages qui sont classe d'une congurence. Enfin une théorie complète des langages rationellement équivalents à D_2 est en cours de publication sous les signatures conjoints de L. Boasson et M. Nivat.

Nous avons fait dans le présent travail de nombreux emprunts aux recherches de ces auteurs.

Année 1974

Bibliographie

[1] Marcel-Paul Schützenberger. Une propriété des monoïdes libres. *C. R. Acad. Sci. Paris Sér. A*, 278 :833–834, 1974.

[2] Marcel-Paul Schützenberger. Sur les monoides finis dont les groupes sont commutatifs. *Rev. Française Automat. Informat. Recherche Opérationnelle Sér. Rouge*, 8(R-1) :55–61, 1974.

[3] Marcel-Paul Schützenberger. Sur certaines pseudo-variétés de monoïdes finis. In *Comptes Rendus des Journées Mathématiques de la Société Mathématique de France (Univ. Sci. Tech. Languedoc, Montpellier, 1974)*, pages 317–327. Cahiers Math. Montpellier, No. 3. U.E.R. de Math., Univ. Sci. Tech. Languedoc, Montpellier, 1974.

[4] Marcel-Paul Schützenberger. Sur une propriété syntactique des relations rationnelles. In *Automata, languages and programming (Second Colloq., Univ. Saarbrücken, Saarbrücken, 1974)*, volume 14 of *Lecture Notes in Comput. Sci.*, pages 612–619. Springer-Verlag, Berlin, 1974.

C. R. Acad. Sc. Paris, t. 278 (18 mars 1974) **Série A — 833**

ALGÈBRE. — *Une propriété des monoïdes libres.*

Note (*) de M. **Marcel Paul Schützenberger**, présentée par M. André Lichnerowicz.

On énonce sans démonstration une propriété de monoide libre A* engendré par un ensemble A et deux applications de celle-ci au monoide syntactique d'un sous-monoide finiment engendré et à la théorie de A. Lentin (1) des équations dans X*.

A chaque mot $a \in A^*$ correspond au plus grand entier p, sa *périodicité a* π, tel que l'on ait $b^p A^* \subset a A^* \subset b^{p+1} A^*$ pour au moins un mot $b \in A^*$; le mot b de longueur $|b|$ minimale satisfaisant ces relations est la *période* $\sqrt{a}$ du mot a [*cf.* (2), (3)].

Soit maintenant α un morphisme fixe d'un monoïde libre X* dans A*. Une α-*factorisation* de *multiplicité* d d'un mot $f \in A^*$ est un système de d triples $(f_i', y_i, f_i) \in A^* \times X^* \times A^*$ tels que l'on ait identiquement $f = f_i' . y_i \alpha . f_i$. Elle est *maximale* ssi pour chaque indice i, il existe des lettres $x, x' \in X$ pour lesquelles $x\alpha \in f_i AA^*$ et $x'\alpha \in AA^* f_i'$; *disjointe* ssi, pour chaque paire d'indices distinctes $i \neq j$ et de facteurs droits y_i' et y_j' de y_i et de y_j, on a

$$y_i' \alpha . f_i \neq y_j' \alpha . f_j.$$

Soit $|X| = \text{Card}(X)$, fini.

PROPRIÉTÉ. — *Tout mot* $f \in A^*$ *de longueur au moins égale à* $\text{Max}\{|x\alpha| : x \in X\}$ *admettant une* α*-factorisation maximale disjointe de multiplicité* $d \geqq 2|X|+1$ *a une périodicité au moins égale à* 2.

La preuve est trop longue pour être donnée ici. On commence par montrer que l'hypothèse sur d entraîne qu'à chaque factorisation $f = f'' a f'$ $(f'', f' \in A^*, a \in A)$ correspondre au moins une lettre $x \in X$ et trois indices distincts j_1, j_2, j_3 tels que les mots y_j aient des factorisations $y_j = y_j'' x y_j'$ pour lesquelles

$$|y_j' \alpha . f_j| \leqq |f'| < |x y_j' \alpha . f_j| \qquad (j = j_1, j_2, j_3).$$

Ceci implique que la périodicité de mot $x\alpha$ soit au moins 2 et que f ait un facteur de période $\sqrt{x\alpha}$ de périodicité au moins 3. Choisissant la lettre a de telle sorte que cette période soit la plus longue possible, on peut montrer que cette période se « propage » à tout le mot f.

APPLICATIONS. — L'hypothèse que X est fini entraîne l'existence d'un morphisme σ de A* dans un monoïde fini S tel que $(X^*\alpha)\sigma\sigma^{-1} = X^*\alpha$. S est le monoïde syntactique du sous-monoïde $X^*\alpha = (X\alpha)^*$ de A*. A chaque groupe maximal $G \subset S$ de degré d correspond un ensemble infini de mots f admettant des α-factorisations maximales disjointes de multiplicité d. La propriété précédente montre que G est un groupe cyclique quand $d \geqq 2|X|+1$, c'est-à-dire que, inversement, quand G n'est pas cyclique, il est image homomorphe d'un sous-groupe du groupe symétrique $\mathfrak{S}_{2|X|}$. Une autre application est que le nombre des $\mathscr{D}$-classes idempotentes de S est borné en fonction de $|X|$ (indépendamment de α), ce qui n'est vrai, ni du nombre total des $\mathscr{D}$-classes, ni de celui des groupes maximaux dans S. La preuve se fait en passant par la théorie de Lentin (1).

834 — Série A **C. R. Acad. Sc. Paris, t. 278 (18 mars 1974)**

Rappelons qu'une *équation* dans X^* est une paire $e = (y, y')$ de mots et que [supposant Card (A) $\geqq |X|$] sa *solution* est l'ensemble Φ_e des morphismes $\varphi : X^v \to A^*$ tels que $y\varphi = y'\varphi$.

Nous dirons qu'elle est *décomposable* ssi à chaque $\varphi \in \Phi_e$, correspond une factorisation $y = y_1 y_0 y_2 \neq y_1 y_2$, $y' = y'_1 y'_0 y'_2 \neq y'_1 y'_2$ telle que l'on ait encore $(y_1 y_2)\varphi = (y'_1 y'_2)\varphi$. La propriété énoncée plus haut donne divers cas de décomposabilité dont le plus simple est l'existence d'un nombre $\bar{d} \in \mathbf{N}$ fonction de $|X|$ tel que soit décomposable toute équation (y, y') pour laquelle chaque lettre $x \in X$ apparaît au moins $\bar{d}$ fois dans le mot yy'. Ceci livre le résultat relatif aux $\mathscr{D}$-classes en imposant des conditions assez strictes sur le mot le plus court de l'image inverse $u\sigma^{-1}\alpha^{-1}$ de chaque idempotent $u \in X^* \alpha \cap S$.

Je mentionne enfin que la valeur $d \geqq 2|X|+1$ de la propriété principale est probablement trop grande et qu'il est possible que l'énoncé subsiste pour $d \geqq |X|+1$, ce que je ne suis pas parvenu à établir.

(*) Séance du 28 janvier 1974.

(1) A. Lentin, *Équations dans les monoïdes libres*, Gauthier-Villars, Paris, 1972.

(2) N. J. Fine et H. S. Wilf, *Proc. Amer. Math. Soc.*, 16, 1965, p. 109-114.

(3) A. Lentin et M.-P. Schützenberger, *A combinatorial problem in the theory of free monoids, in Combinatorial Mathematics and its Applications* (*Proc. Chapel Hill Conf.*, 1969. R. C. Bose et T. A. Dowlina Ed.,) p. 128-144.

Institut de Recherche
d'Informatique et d'Automatique,
Domaine de Voluceau,
Rocquencourt,
78150 *Le Chesnay.*

R.A.I.R.O.
(8e année, R-1, 1974, p. 55-61)

SUR LES MONOIDES FINIS DONT LES GROUPES SONT COMMUTATIFS

par M. P. SCHÜTZENBERGER (1)

Communiqué par J.-F. PERROT

Résumés. — *On examine une caractérisation des parties reconnaissables dont les groupes dans le monoïde syntactique sont commutatifs.*

1. INTRODUCTION

Appelons *groupe latent* $Gp(F)$ d'une partie quelconque F d'un semi-groupe S, le plus petit groupe que divisent tous les groupes dans le semi-groupe syntactique de F. Nous nous proposons ici d'appliquer la théorie de la décomposition de Krohn et Rhodes pour examiner la famille $\mathcal{C}$ des parties reconnaissables au sens de Eilenberg ([1], c'est-à-dire des parties dont le monoïde syntactique est fini) d'un monoïde libre A^* dont le groupe latent appartient à une variété donnée Γ de groupes commutatifs finis.

Le cas où A^* est remplacé par un monoïde commutatif libre a été traité par J.-F. Perrot en 1965 ([2]).

La famille $\mathcal{C}$ elle-même a été introduite par McNaughton en 1960 ([3]) à l'intérieur d'une problématique différente.

Pour alléger les énoncés, nous dirons qu'une famille $\mathcal{F}$ de parties est *fermée par les opérations polynomiales* ssi elle contient la partie vide, la partie $\{1\}$ et toutes les parties de l'alphabet et si elle contient en outre l'union et le produit de deux quelconques de ses membres.

Étant donnés deux alphabets B et A et une famille $\mathcal{F}$ de parties de A^*, une *$\mathcal{F}$-substitution élémentaire* α est un morphisme de B^* dans le monoïde des parties de A^* qui satisfait les conditions suivantes :

(1) α est injectif en ce sens que les images par α de deux lettres distinctes de B sont disjointes ;

(1) Groupe d'Informatique théorique, UER de Mathématiques Université de Paris-VII.

Revue Française d'Automatique, Informatique et Recherche Opérationnelle n° mars 1974, R-1.

(2) Il existe une partie A' de A telle que $B\alpha$ soit contenue dans $(A/A')^* A'$;

(3) $b\alpha$ appartient à la famille $\mathcal{F}$ pour chaque lettre b.

Pour simplifier, nous supposerons toujours A infini dénombrable et nous nous limiterons aux substitutions élémentaires $\alpha : A^* \to A^*$ telles que $a\alpha$ soit non vide pour un nombre *fini* de lettres de A.

Enfin, une partie préfixe ayant un délai de synchronisation fini est une partie P du semi-groupe libre $A^+ = AA^*$ qui est préfixe ($P \cap PA^+ = \varnothing$) et pour laquelle il existe un entier fini d (le délai de synchronisation) tel que l'on ait la relation :

$$a \in A^*, p \in P^d, apA^* \cap P^* \neq \varnothing \Rightarrow ap \in P^*.$$

Cette notion, sous une forme ou une autre a été souvent considérée (cf. [4], [5], [6]). En particulier quand α est une substitution élémentaire, l'image par α de l'alphabet A est préfixe avec un délai de synchronisation un (ou zéro si $A\alpha = A$).

Première caractérisation. La famille $\mathfrak{C}$ est la plus petite famille $\mathfrak{C}'$ fermée par les opérations polynomiales et les $\mathfrak{C}'$-substitutions élémentaires qui contienne tous les noyaux $1\gamma^{-1}$ où γ est un morphisme dans un groupe de Γ d'un monoïde libre $A'^*(A' \subset A$, fini).

Notons $N(F)$ l'ensemble des entiers qui sont l'ordre d'au moins un groupe cyclique appartenant à Γ. Comme Γ est une variété de groupes commutatifs finis, elle est définie de façon unique par la donnée de $N(\Gamma)$.

Deuxième caractérisation. La famille $\mathfrak{C}$ est la plus petite famille $\bar{\mathfrak{C}}$ fermée par les opérations polynomiales qui contienne toutes les intersections finies $\cap \{ (P_i^{n_i})^* : 1 \leqslant i \leqslant m \}$ où les n_i appartiennent à $N(\Gamma)$ et où les P_i sont des parties préfixes ayant un délai de synchronisation fini et appartenant à $\bar{\mathfrak{C}}$.

II. DELAI DE SYNCHRONISATION FINI

Observons d'abord que si P est une partie préfixe ayant un délai de synchronisation d, toute relation $apa' \in P^*$, où $a, a' \in A^*$ et $p \in P^d P^*$ implique $ap, a' \in P^*$. En effet, on peut écrire $p = p'p''$ où $p' \in P^d$ et $p'' \in P^*$ et la relation $ap'p''a' \in P^*$ entraîne d'abord $ap' \in P^*$, d'après l'hypothèse de synchronisation, ensuite $p''a', a' \in P^*$ d'après l'hypothèse que P est préfixe.

Rappelons maintenant l'énoncé suivant dans lequel B est un alphabet quelconque, Q une partie préfixe dans B^+ ayant un délai de synchronisation fini d' et α un morphisme injectif de B^* dans A^* tel que $B\alpha$ soit contenue dans une partie préfixe P ayant un délai de synchronisation fini d.

II.1. La partie $R = Q\alpha$ est préfixe et a un délai de synchronisation $d + d'$.

Preuve : Il est trivial que R soit préfixe. Considérons un élément de $R^{d+d'}$. On peut l'écrire comme un produit rr' où $r \in R^d$ et $r' \in R^{d'}$. Supposons que $a, a' \in A^*$ satisfassent $arr'a' \in R^*$. Comme R est contenu dans P^+ ceci entraîne que $arr'a'$ soit dans P^* et que r soit dans P^dP^*, donc, comme on l'a vu ci-dessus, que ar, r' et a' appartiennent tous à P^*. Leurs images inverses par α sont donc des mots b, q' et b' de B^* où $q' = r'\alpha^{-1}$ est dans $Q^{d'}$ et l'on a $bq'b' \in Q^*$. D'après notre hypothèse sur Q, on en conclut que bq' et b' sont dans Q^* et enfin que $arr' = bq'\alpha$ et $a' = b'\alpha$ sont dans R^*.

Q.E.D.

Corollaire II.2. : Soient $\{\alpha_i : 1 \leqslant i \leqslant \kappa\}$ un ensemble fini de substitutions élémentaires $\alpha_i : A^* \to A^*$. L'image P de A par la substitution produit $\alpha_1\alpha_2 \ldots \alpha_k$ est préfixe et a un délai de synchronisation κ.

Preuve : Ceci résulte immédiatement de l'énoncé précédent et de ce que pour toute partie A' de A, l'ensemble $(A/A')^*A'$ est une partie préfixe ayant délai un.

Q.E.D.

REMARQUE : Les mêmes techniques permettent sans peine de vérifier que P est contenue dans une partie préfixe Q ayant un délai de synchronisation fini et satisfaisant les conditions supplémentaires suivantes :

(1) $a \in A^* \Rightarrow aA^* \cap A^* \neq \varnothing$;

(2) Il existe un entier fini κ tel que :

$$a_1, a_2, \ldots, a_k \in A^*,$$
$$a_1a_2, a_2a_3, \ldots, a_ja_{j+1}, \ldots, a_{k-1}a_k \in Q^* \Rightarrow a_k \in Q^*,$$

(3) Si X est une partie de A^* non contenue dans Q^*, il existe au moins un $x \in X$ tel que $X^*x \cap Q^* = \varnothing$.

Nous considérons maintenant une partie préfixe P ayant un délai de synchronisation fini d et une application γ de P dans un groupe G. Celle-ci se prolonge en un morphisme de P^* dans G. On sait que le noyau $1\gamma^{-1}$ est un sous-monoïde de P^* engendré par une partie préfixe R de P^+. Nous nous proposons d'examiner le groupe latent de R^* au moyen de la méthode des produits en couronne de Krohn et Rhodes.

Pour cela, nous considérons d'abord l'automate minimal reconnaissant les parties $P_g = P \cap g^{-1}\gamma (g \in G)$. Soient Q son ensemble d'états, q_1 son état initial et Q_+ l'ensemble de ses états finaux.

n° mars 1974, R-1.

Comme P est préfixe, l'état q_1 n'est pas contenu dans Q_+ et l'on a $Q_+a = \varnothing$ pour tout mot $a \neq 1$. De plus, il existe une bijection entre les parties $P_g(g \in G)$ et les états finaux qui permet de définir pour chaque $q \in Q_+$, l'élément $q\gamma$ de G égal à l'image par γ des mots de $q_1^{-1}q$ $(= \{a \in A^* : q_1 a = q\})$.

Posons $\bar{Q} = (G \times Q/Q_+)$ et définissons une action de A^* sur $\bar{Q}$ en posant pour chaque lettre a et chaque état $(g, q) \in \bar{Q}$:

$$\begin{aligned}(g, q)a &= (g \cdot q\gamma, q_1) && \text{si} \quad qa \in Q_+ \\ &= (g, qa) && \text{si} \quad qa \in Q/Q_+ \\ &= \varnothing && \text{si} \quad qa = \varnothing.\end{aligned}$$

Il est facile de voir que cette définition entraîne que pour tout mot a, on ait :

$(g, q)a = (g \cdot p\gamma, q_1)a''$ si $a = a'pa''$ où $a' \in q^{-1}Q_+$, p est le plus long facteur dans P^* de $a'^{-1}a$ et $a'' = (a'p)^{-1}a$.

$(g, q)a = (g, qa)$ ou $\varnothing$ si a n'a aucun facteur gauche dans $q^{-1}Q_+$.

En particulier, quels que soient $g \in G$ et $a \in A^*$, l'état $(g, q_1)a$ appartient à (G, q_1) ssi a est dans P^*. On en conclut que l'automate ainsi défini (avec $(1, q_1)$ comme état initial et final) reconnaît R^* et on vérifie facilement qu'il est minimal.

II.3. Tout groupe maximal dans le monoïde syntactique $A^*\sigma$ de R est isomorphe à G ou à un groupe dans le monoïde syntactique M dans $P_g(g \in G)$.

Preuve : Soient $H \subset A^*$ l'image inverse d'un groupe maximal $H\sigma$ dans $A^*\sigma$ et $\bar{Q}_H = Q(H \cap A^+)$.

Supposons d'abord que pour tout $(g, q) \in \bar{Q}_H$ et tout $h \in H$ on ait $qh \neq \varnothing$. D'après notre définition de l'action de A^* sur $\bar{Q}$ ceci implique que l'on ait $(g, q)h = (g, qh)$ identiquement pour tout $h \in H$ et $(g, q) \in \bar{Q}_H$ et par conséquent que $H\sigma$ soit isomorphe à un groupe dans le monoïde M.

Dans le cas contraire il existe un facteur gauche $a \neq 1$ d'un mot $ab \in H$ et un état (g, q) de $\bar{Q}_H$ tels que $qa = q_+$. Prenons un mot $c \in H$ tel que $(abc)\sigma$ soit idempotent. Les relations

$$(g, q)a = (g', q_1) = (g, q)abca = (g', q_1)bca$$

montrent que $bca \in P^+$.

Il existe donc des mots f, g tels que $gf \in P^dP^*$, $fg \in H$, et que les images par σ de fg et gf soient idempotents. Comme $(fgHfg)\sigma = H\sigma$ l'image par σ du monoïde $H' = gHf$ est un groupe isomorphe à $H\sigma$ et il existe un $p \in P^dP^*$

tel que son image par σ soit l'idempotent de ce groupe. Nous pouvons donc supposer pour simplifier que $H' = H$, c'est-à-dire que $H \cap P^d P^*$ contient un mot p tel que $p\sigma = pp\sigma$.

De nouveau, $H\sigma = Hp\sigma$ et par conséquent $\bar{Q}_H$ est contenu dans $\bar{Q}_p$. Soit $(g, q) \in \bar{Q}_H$. Il existe des mots a, a' tels que $q_1 a = q$, $qa' = q_+$. D'après $(g, q)p = (g, q)$ on a $apa' \in P^*$ et comme $p \in P^d P^*$ où d est le délai de synchronisation de P, on en conclut que $ap \in P^*$ c'est-à-dire que $q = q_1$. Donc $\bar{Q}_H$ est contenu dans (G, q_1), ce qui entraîne que H soit contenu dans P^*.

Q.E.D.

Corollaire II.4. : Si P préfixe a un délai de synchronisation borné, le groupe latent de $(P^r)^*$ divise le produit direct du groupe latent de P par le groupe cyclique $\mathbf{Z}_{(r)}$.

Preuve : Immédiate.

Corollaire II.5. : Les familles $\mathcal{C}'$ et $\bar{\mathcal{C}}$ de l'Introduction sont contenues dans $\mathcal{C}$.

Preuve : Compte tenu de II.2 et de II.4, ceci résulte immédiatement de la fermeture de $\mathcal{C}$ par rapports aux opérations polynomiales et aux opérations booléennes.

Q.E.D.

III. FIN DE LA VERIFICATION

Pour achever la preuve, il nous suffit de considérer une partie $F \in \mathcal{C}$ et de montrer qu'elle appartient aux familles $\mathcal{C}'$ et $\bar{\mathcal{C}}$. Nous notons σ le morphisme syntactique de F et comme les familles $\mathcal{C}$, $\mathcal{C}'$ et $\bar{\mathcal{C}}$ sont fermées par rapport à l'union, nous supposons que $F\sigma$ est un singleton.

III.1. Si $F\sigma$ est un groupe G, la partie F appartient à $\mathcal{C}'$ et $\bar{\mathcal{C}}$.

Preuve : Soit $K = 1^{-1}\sigma$ le noyau de σ. Tout mot b admet une factorisation $b = \kappa_1 a_1 \kappa_2 a_2 \dots \kappa_n a_n \kappa_{n+1}$ où $a_1, a_2, \dots, a_n \in A$; $\kappa_1, \kappa_2, \dots, \kappa_{n+1} \in K$ et où chaque κ_i est défini comme le plus long facteur dans K du mot b_i tel que $\kappa_1 a_1 \dots a_{i-1} b_i = b = b_1$.

Cette condition implique que pour chaque $m \leqslant n$ tous les produits $(a_i a_{i+1} \dots a_m)\sigma\ (1 \leqslant i \leqslant m)$ soient différents. Donc $n < \text{Card } G$ établissant que F est dans la fermeture polynomiale de K, et, par définition, l'inclusion $F \in \mathcal{C}'$. En ce qui concerne $\bar{\mathcal{C}}$, l'hypothèse que G est un groupe commutatif fini implique que G soit groupe quotient d'un groupe $G' \in \Gamma$ dont le noyau K'

est défini par une partition $\{A_i\}$ de A, des entiers $n_i \in N(\Gamma)$ et la condition qu'un mot a appartienne à K' ssi le nombre $|a|_i$ de lettres de A_i figurant dans a est pour chaque i un multiple de n_i. On peut donc supposer que $G = G'$ et $K = K'$ et posant $P_i = (A/A_i)^* A_i$, on obtient K comme l'intersection des monoïdes $(P_i^{n_i})^*$.

Corollaire III.2. : Si $1 \in F$ on a $F \in \mathcal{C}' \cap \bar{\mathcal{C}}$.

Preuve : Comme $F\sigma$ est un singleton, l'hypothèse $1 \in F\sigma$ entraîne $F\sigma = 1$. Il existe donc une partie A' de A telle que F soit contenue dans A'^* et que la restriction de σ à A'^* soit un morphisme dans un groupe.

Q.E.D.

Nous pouvons désormais supposer que F ne contient pas 1 ce qui entraîne que son monoïde syntactique soit l'union disjointe d'un élément neutre et d'un semi-groupe S image de A^+ par σ.

III.3. Si $A\sigma$ est un singleton ou si S est un semi-groupe $\mathfrak{L}$-simple on a $F \in \mathcal{C}' \cap \bar{\mathcal{C}}$.

Preuve : Si $A\sigma$ est un singleton, F est de la forme $A^k (k \in \mathbf{N})$ ou $A^k (A')^* (r \in \mathbf{N}(\Gamma))$ et le résultat est établi puisque A est une partie préfixe ayant un délai de synchronisation zéro.

Si S est $\mathfrak{L}$-simple, il existe un morphisme γ de A^+ dans un groupe G de Γ et une partition $\{A_i\}$ de A tels que F soit une union finie de termes de la forme $A_i(g\gamma^{-1})(g \in G)$.

Q.E.D.

Nous faisons maintenant intervenir le lemme classique de Krohn et Rhodes. Il affirme qu'en dehors des trois cas traités dans III.1, III.2 et III.3 il existe une partie A' de l'alphabet A ayant les propriétés suivantes :

(1) Posant $B = (A/A')^* A'$, on a $B^+\sigma \neq S$;

(2) Si $(A/A')\sigma$ n'est pas un singleton on a $(A/A')^+\sigma \neq S$.

Comme tout mot de A^* admet exactement une factorisation comme produit d'un mot de B^* par un mot de $(A/A')^*$, il en résulte que F est une union finie disjointe de produits non ambigus de la forme GF' où $G \subset B^*$, $F' \subset (A/A')^*$ et où $G\sigma$ et $F'\sigma$ sont des singletons.

Procédant par induction sur Card $(A^*\sigma)$, nous en concluons que compte tenu du premier cas de III.3, la partie F' appartient à $\mathcal{C}'$ et $\bar{\mathcal{C}}$.

Montrons qu'il en est de même pour G. Pour ce faire, prenons une partie A_1 de A en correspondance bi-univoque (par β) avec les paires dans

$((A/A')^*\sigma, A'\sigma)$. Pour chaque $a \in A_1$ nous définissons $a\alpha$ comme le produit de $s\sigma^{-1} \cap (A/A')^*$ par $s'\sigma^{-1} \cap A'$ si $a\beta = (s, s')$. Comme on vient de le voir, $a\alpha$ appartient à $\mathcal{C}' \cap \bar{\mathcal{C}}$ et par conséquent α peut être considérée comme une $\mathcal{C}' \cap \bar{\mathcal{C}}$-substitution élémentaire. Par définition, il existe une partie $G_1 \subset A_1^*$ telle que $G_1\alpha = G$. D'après l'hypothèse d'induction et $B^+\sigma \neq S$, on a $G_1 \in \mathcal{C}' \cap \bar{\mathcal{C}}$ ce qui établit directement $G \in \mathcal{C}'$ et qui donne $G \in \bar{\mathcal{C}}$ moyennant le corollaire II.2.

Q.E.D.

REMARQUE : La technique de factorisation de III.1 empêche (hormis certains cas particuliers) que les parties obtenues le soient de manière non ambiguë. Il serait évidemment possible d'obtenir ce résultat en admettant comme données dans la deuxième caractérisation toutes les intersections finies de parties de la forme

$$(P_i^{n_i})^* P_i^{m_i} (0 \leqslant m_i < n_i, n_i \in \mathbf{N}(\Gamma),$$

$P_i \in \bar{\mathcal{C}}$, préfixe ayant un délai de synchronisation fini). Inversement, on pourrait (en perdant la non-ambiguïté) remplacer les intersections par des « produits de mélange ». On notera que la deuxième caractérisation n'utilise pas le fait que l'alphabet A soit de cardinalité non bornée.

REFERENCES

[1] EILENBERG S., Livre sous presse, vol. 1.

[2] PERROT J.-F., *Sur quelques familles de parties des monoïdes abéliens libres*, C.R. Acad. Sc. Paris, 1965, *261*, 3008-3011.

[3] MCNAUGHTON R., *Symbolic Logic for automata*. Wright Air Dept. Div. Tech. Note. 60-244. Cincinnati. Ohio 1960.

[4] NEUMAN P. G., *On error limiting Codes*. IRE Trans. IT, 1963, *9*, 209-212.

[5] WINOGRAD S., *Input error limiting Automata*. IBM Research Report. RC 966, 1963.

[6] GOLOMB S. W. et GORDON B., *Codes with bounded synchronization delay*. Information and Control, 1965, *8*, 355-372.

n° mars 1974, R-1.

CAHIERS MATHÉMATIQUES

MONTPELLIER

3

COMPTES RENDUS

DES JOURNÉES MATHÉMATIQUES S. M. F.

UNIVERSITÉ DES SCIENCES
ET TECHNIQUES
DU LANGUEDOC
U. E. R. DE MATHÉMATIQUES
Place Eugène Bataillon
34060 MONTPELLIER CEDEX

1974

- I -

JOURNEES MATHEMATIQUES S.M.F.

MONTPELLIER 16-20 Avril 1974

INTRODUCTION

L'idée initiale pour ces Journées était de sortir des sentiers battus, comme en porte témoignage, le choix des thèmes. On a voulu exposer un certain nombre de sujets d'actualité en mathématiques ainsi que de leurs applications [on serait tenté de parler de mathématiques pures et appliquées, mais nous nous garderons bien de le faire]. Voici le programme de ces Journées :

P R O G R A M M E

* Les conférences ont lieu en Salle 102 A (1er étage du Bâtiment de Mathématiques) de 9h. à 12h. et de 14h. à 18h. Début des conférences : Mardi à 14h.

Mardi 16 Avril

MODELES

C.F. PICARD - Un aspect paradoxal de l'information

R. THOM - L'optimisation simultanée et la théorie des jeux en topologie différentielle.

K. MOUNT - Information size of Message Spaces and the regularity of the Pareto Correspondence

- II -

M. FLIESS - Une approche nouvelle de certains systèmes dynamiques utilisés en ingéniérie.

Mercredi 17 Avril

ASPECTS ALGEBRIQUES DE LA COMBINATOIRE

D. FOATA - Réarrangements d'applications associées aux nombres de Genocchi.

G. VIENNOT - Factorisations des monoïdes libres et bases des algèbres de Lie libres.

J.P. SOUBLIN - Problèmes de Burnside.

AUTOMATES ET LANGAGES

E. SPANIER - Mathematical Properties of languages.

J. PERROT - Monoïdes syntactiques des langages rationnels.

D. PERRIN - Sur les groupes de permutations associés aux codes biprefixes.

S. TERMINI - A. RESTIVO - An algorithm for deciding whether a strictly localy testable submonoïd is free.

- III -

Jeudi 18 Avril — COMPUTATIONAL PROBLEMS IN ALGEBRA

L. GERHARDS - On the construction of the automorphism group of a finite group.

D. LAZARD - Algèbre linéaire sur les anneaux de polynômes.

A. MICALI - Nombres et séries de Betti

11h. 30 — Départ pour Saint-Guilhem-Le-Désert.

Vendredi 19 Avril — ASPECTS ALGEBRIQUES DE LA COMBINATOIRE

P. HILTON - Localization of nilpotent groups ; homological and and combinatorial methods.

M. BROUE - Codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux éléments et Formes Formes quadratiques entières définies positives à discriminant +1.

S. FAKIR - Monoïdes et anneaux algébriquement clos.

- IV -

CALCUL ET PROGRAMMATION

L. NOLIN - Programmation et logique combinatoire.

M. NIVAT - Pour une sémantique algébrique

J. VUILLEMIN - Deux problèmes liés à l'analyse d'algorithmes.

G. WERNER - Sous-classes récursivement énumérables d'une classe de complexité.

Samedi 20 Avril

AUTOMATES ET LANGAGES

A. LENTIN - Equations dans les monoïdes libres (quelques problèmes actuels).

M. MORCRETTE - Catégories de systèmes algébriques suscitées par la théorie des équations dans le monoïde libre.

M. FONTET - π-systèmes involutifs.

AUTOMATES ET LANGAGES

M.P. SCHUTZENBERGER - Sur certaines pseudo-variétés de monoïdes finis.

- V -

G. JACOB - Séries formelles en variables non commutatives. Transductions rationnelles.

Réunion de clôture.

——— : ———

Ce fascicule contient les textes de presque toutes les conférences tenues lors de ces Journées. Nous regrettons que les textes de certaines conférences qui avaient intéressé beaucoup les participants ne nous soient pas parvenus. Nous pensons tout particulièrement aux conférences faites dans le cadre du thème CALCUL et PROGRAMMATION.

D'autre part, les papiers de N. ROBY et D. ALLOUCH n'ont pas été exposés, faute de temps.

Malgré la difficulté de classer tous ces articles sous les cinq thèmes des Journées, ce fascicule a la composition suivante :

MODELES

J.L. CHABERT : Systèmes dynamiques linéaires et extensions de Fatou.

M. FLIESS : Une approche nouvelle de certains systèmes dynamiques utilisés en ingéniérie.

K. MOUNT : Information size of Message Spaces and the regularity of the Pareto Correspondence.

C.F. PICARD : Un aspect paradoxal de l'information.

R. THOM : L'optimisation simultanée et la théorie des jeux en topologie différentielle.

- VI -

ASPECTS ALGEBRIQUES DE LA COMBINATOIRE

M. BROUE : Codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux éléments et Formes quadratiques entières définies positives à discriminant +1.

S. FAKIR : Monoïdes et nneaux algébriquement clos.

D. FOATA : Réarrangements d'applications associées aux nombres de Genocchi.

P. HILTON : Localization of Nilpotent Groups ; homological and combinatorial methods.

N. ROBY : Méthodes probabilistes et problèmes de densité en théorie des nombres.

J.P. SOUBLIN : Problèmes de Burnside.

G. VIENNOT : Factorisations des monoïdes libres et bases des algèbres de Lie libres.

AUTOMATES ET LANGAGES

D. ALLOUCH : R-ensemble maximal de fractions.

G. JACOB : Séries formelles en variables non commutatives. Transductions rationnelles.

A. LENTIN : Equations dans les monoïdes libres.

M. FONTET : π-systèmes involutifs.

M. MORCRETTE : Catégories de systèmes algébriques suscitées par la théorie des équations dans le monoïde libre.

D. PERRIN : Sur les groupes de permutations associés aux codes biprefixes.

J.F. PERROT : Monoïdes syntactiques des langages rationnels.

A. RESTIVO et S. TERMINI : An algorithm for deciding whether a strictly localy testable submonoïd is free.

- VII -

E. SPANIER : Mathematical properties of languages.

M.P. SCHUTZENBERGER : Sur certaines pseudo-variétés de monoïdes finis.

COMPUTATIONAL PROBLEMS IN ALGEBRA

J.B. CASTILLON et A. MICALI : Nombres et séries de Betti.

L. GERHARDS : On the construction of the automorphism group of a finite group.

D. LAZARD : Algèbre linéaire sur les anneaux de polynômes.

CALCUL et PROGRAMMATION

G. WERNER : Sous-classes récursivement énumérables d'une classe de complexité.

Nous sommes tenus à donner quelques explications complémentaires au lecteur. Les textes de A. LENTIN, M. FONTET et M. MORCRETTE sont disposés dans l'ordre où ils doivent être lus.

Par ailleurs, notre conditionnement scientifique est tel qu'il nous est impossible d'échapper au franglais ou directement, à l'anglais en tant que langue scientifique. Il nous a semblé qu'il n'y avait pas de titre français pouvant rendre compte de la situation en aussi peu de mots, raison pour laquelle nous avons conservé directement le titre anglais : COMPUTATIONAL PROBLEMS IN ALGEBRA.

Finalement, nous tenons à rendre publique la liste des organismes qui nous ont aidé financièrement dans la réalisation de ces Journées :

SOCIETE MATHEMATIQUE DE FRANCE-CNRS

UER de Mathématiques Appliquées aux Sciences Humaines, Université Paul Valéry (Université de Montpellier III)

Conseil Scientifique de l'USTL (Université de Montpellier II).

MIAGE (Maîtrise Informatique Appliquée à la Gestion des Entreprises)
de l'USTL.

IUT (Institut Universitaire de Technologie) de Montpellier.

UER de Mathématiques de l'USTL.

Ce fascicule n'a pu voir le jour que grâce aux moyens matériels de notre UER de Mathématiques et aux actions heroïques de Madame C. MORI qui a assuré la frappe et de Monsieur Meyran, pour la pagination. Qu'il leur soit rendu grâce ainsi qu'à tous ceux qui nous ont aidé et dont les noms nous échappent en ce moment.

———— : ————

Nous implorons finalement la clémence des Dieux pour avoir dépensé tant de papier et par conséquent, avoir contribué à abattre tant d'arbres....

Montpellier le 23 Janvier 1975

Yves CESARI

Artibano MICALI

SUR CERTAINES PSEUDO-VARIETES DE MONOIDES FINIS

par

M.P. SCHUTZENBERGER

I. Selon la théorie de S. Eilenberg, une pseudo-vairété de semi-groupes (ou monoïdes, ou groupes) est une famille de telles structures contenant toute image homomorphe du produit sous direct de deux de ses membres. En particulier, étant donnée une pseudo-variété de groupes $\mathcal{V}$ on peut définir la pseudo-variété $\bar{\mathcal{V}}$ de monoïdes finis par la condition que $M \in \bar{\mathcal{V}}$ ssi chaque groupe dans M appartient à $\mathcal{V}$ et pour chaque alphabet Σ la famille $\bar{\mathcal{V}}$-Rec des parties P de monoïde libre Σ^* telles que leur monoïde syntactique appartienne à $\bar{\mathcal{V}}$.

On sait d'autre part que la pseudo-variété (de groupes) $\mathcal{V}$ associe à chaque groupe G un plus petit sous-groupe normal V_G (= le $\mathcal{V}$-noyau de G) tel que $G/V_G \in \mathcal{V}$. L'hypothèse que $\mathcal{V}$ est une pseudo-variété, équivaut à la condition que pour tout morphisme $\phi : G \to H$, on ait $V_{G\phi} \subset V_H$ si ϕ est injectif et $V_H \subset V_{G\phi}$ si ϕ est surjectif.

Le résultat principal de ce travail est la

Propriété I.1.

Soit $A \in \bar{\mathcal{V}}$-Rec. On a $A^* \in \bar{\mathcal{V}}$-Rec ssi l'image $B = A^*\rho_{A^*}$ de A^* dans son monoïde syntactique $S = \Sigma^*\rho_{A^*}$ satisfait la condition :

($\mathcal{V}$). B contient le $\mathcal{V}$-noyau de chacun des groupes qu'elle rencontre.

Il est trivial que cette condition est nécessaire : en effet, comme B est un sous semi groupe du monoïde fini : son intersection avec chaque groupe G dans S contient l'idempotent e de ce dernier qui est lui-même précisément le $\mathcal{V}$-noyau de G ssi $G \in \mathcal{V}$.

Nous ne nous occuperons donc plus désormais que de l'implication inverse. Dans la section III nous utilisons la propriété précédente pour retrouver divers résultats connus.

Nous terminons cette introduction en rappelant quelques propriétés du monoïde syntactique, elles aussi connues depuis les travaux de R. Croisot (Equivalences Principales Bilatères définies dans un demi-groupe. J. de Math. Pures et Appl. 36 (1957). pp. 373-417).

Proposition I.2

Soit $M' = M\rho_E$ le monoïde syntactique de la partie E de M. Le morphisme syntactique ρ_E, de la partie $E' = E\rho_E$ de M' est l'identité.

Preuve : Par définition M' est le plus petit quotient de M pour lequel le morphisme correspondant ϕ de M satisfasse $E = E\phi\phi^{-1}$. L'énoncé en découle en vérifiant que cette dernière relation est satisfaite par $\phi = \rho_E\rho_{E'}$.

Q.E.D.

Pour chaque $m_1 \in M$ nous posons

$E :: m_1 = \{(m,m') \in MxM : mm_1m' \in E\}$.

Proposition I.3

Pour tout $m_1, m_2 \in M$ on a $m_1\rho_E = m_2\rho_E$ ssi $E : m_1 = E : : m_2$.

Preuve : Il est clair que la relation $E :: m_1 = E : : m_2$ définit une équivalence $\equiv$ sur M. Comme $E ::(m_1m_3) = \{(m,m') \in E ::m_1 : m' \in m_3M\} = (E ::m_1) \cap (M,m_3M)$ pour tout $m_1, m_3 \in M$ puisque M contient un élément neutre 1, et comme une relation semblable vaut pour m_3m_1, on voit que de fait, $\equiv$ est une congruence. Puisque $(1,1)$ appartient à $E::m_1$ ssi $m_1 \in E$,

elle sature E et elle contient toutes les congruences ayant cette propriété puisque $m_1 \not\equiv m_2$ implique l'existence d'une paire $(m_1 m')$ pour laquelle un seul des éléments mm_1m' et mm_2m' appartient à E.

Q.E.D.

Nous appliquons ceci au groupe G dans $S = \Sigma^*\rho$ en désignant désormais par ρ le morphisme syntactique ρ_{A^*}. Comme ci-dessus, e et V sont l'idempotent et le $\mathcal{V}$-noyau de G.

Lemme I.4. Soit $b \in e\,\rho^{-1}$. Supposons que pour tout $f, f' \in \Sigma^*$ tels que $fbb^*f' \subset A^*$ et chaque $v \in V$ il existe un $c \in v\,\rho^{-1}$ pour lequel on ait

(X) $\quad fb^*cb^*f' \cap A^* \neq \phi$

Alors $\quad V = \{e\}$.

Preuve Comme $b\rho = e = e^2$ on a $bb^*\rho = e$, et par conséquent $fbb^*f' \subset A^*$ implique $(f\rho)e(f'\rho) \in A^*\rho$. De même, comme $v = ev = ve = eve$ puisque $v \in V \subset G$, la relation (X) implique $(f\rho)v(f'\rho) \in A^*$.

Maintenant d'après I.2 et I.3 ci-dessus avec $M = S$ et $E = A^*$ on a $e = v$ ssi $A^*\rho::e = A^*\rho::v$.

L'hypothèse du lemme équivaut à l'assertion que chaque $(s,s') \in A^*\rho::e$ appartient à tous les $A^*\rho::v$ $(v \in V)$. En effet la première relation implique $(s\rho^{-1})(e\rho^{-1})(s'\rho^{-1}) \subset A^*\rho\rho^{-1} = A^*$ donc $fbb^*f' \subset A^*$ pour tout $f \in s\rho^{-1}$, $f' \in s\,\rho^{-1}$ et la relation (X). Ceci suffit pour entrainer l'égalité de $A^*\rho::e$ et de chacun des $A^*\rho::v$ car si (s,s') est dans ce dernier ensemble on a $(s,s'') \in A^*\rho::e$ pour $s'' = vs'$ donc $(s,s'') \in A^*\rho::v^{-1}$, ce qui équivaut à $(s,s') \in A^*\rho::e$ puisque $sv^{-1}s'' = sv^{-1}v's' = ses'$.

Q.E.D.

II. Vérification de la proposition I.1.

Nous gardons les mêmes notations que dans le lemme I.4. Dans le premier énoncé ci-dessous, nous choisissons un mot $b \in ep^{-1}$. Dans les suivants nous véridions que (X) est vraie dans tous les cas. Dans les deux derniers, seul intervient le fait que Σ^* est un monoïde libre et plus exactement que chaque mot $s \in \Sigma^*$ a une longueur $|s| \in N$, (avec $|s| > 0$ ssi $s \neq 1$). Dans les trois premiers on exploite l'hypothèse $T \in \bar{\mathcal{U}}$ où pour abréger $\tau : \Sigma^* \to T$ désigne le morphisme syntactique de A.

II.1. Sous l'hypothèse $T \in \bar{\mathcal{U}}$, il existe un sous-ensemble fini C de Σ^* tel que $C\rho = G$ et $C\tau = u$ où u est un idempotent de T.

Preuve : Comme $G\rho^{-1}$ est un semi groupe et T un ensemble fini, l'ensemble $G\rho^{-1}\tau$ est un semi groupe fini. D'après un théorème classique de Clifford (Am. J. of Math. 70 (1948) pp. 521-526) il contient un groupe H tel que $H = H(G\rho^{-1}\tau)H$. Cette relation entraine que $P\rho = G$ et $P_\tau = H$ où P désigne l'intersection de $G\rho^{-1}$ et $H\tau^{-1}$. Suit e l'idempotent de G. Posons $g\lambda = (g\rho^{-1} \cap P)\tau$ pour chaque $g \in G$. On a identiquement

(2.1.) $(g_1\lambda)(g_2\lambda) \subset (g_1 g_2)\lambda$

puisqu'une relation semblable vaut pour ρ^{-1}. Prenant en particulier $g_1 = g_2 = e$, on en déduit en utilisant la finitude de H que $e\lambda$ est un sous groupe K de H. Prenant successivement $g_1 = e$ et $g_1 = g_2^{-1}$, la même relation (2.1.) montre que K est un sous groupe normal et que λ induit un morphisme de G sur H/K. De façon symétrique, on trouve que le noyeau L de λ est l'ensemble $C'\rho$ où $C' = P \cap u\,\tau^{-1}$ $(u = u^2 \in H)$. Faisons intervenir l'hypothèse $T \in \bar{\mathcal{U}}$. Comme $\mathcal{U}$ est une pseudo variété de groupes elle entraine que H et H/K appartiennent à $\mathcal{U}$ et nous

en concluons que L contient le $\mathfrak{V}$-noyau V de G en raison de l'isomorphie de G/L et H/K et du caractère minimal de V. L'énoncé en résulte en prenant pour G une partie convenable de $C' \cap V\rho^{-1}$.

Q.E.D.

Corollaire II.2.

Soient $b, c \in C$. On a $xbcx' \in A$ pour tout $x, x' \in \Sigma^*$ tels que $xbx' \in A$.

Preuve : Ceci résulte immédiatement de $C\tau = u = u^2$ et de la définition de τ comme morphisme syntactique de A.

Q.E.D.

Dorénavant b sera un mot fixe de $C \cap e\rho^{-1}$ et f, f' une paire de mots telle que $fbb^*f' \subset A^*$.

II.3. Supposons $fb^n f' \in (A \setminus 1)^k$ pour une paire d'entiers n,k telle que $n \geq k+1$. Pour chaque $c \in C$ on a la relation

(X) $fb^*cb^*f' \cap A \neq \phi$

Preuve : Soit $fb^n f' = a_1 a_2 \ldots a_k$ où chaque $a_i \in A$.

On associe à chaque $m \leq n$ le plus grand entier $i = i_m$ pour lequel $a_1 \ldots a_i$ est un facteur gauche de fb^m. Comme $n \geq k+1$ il existe un m pour lequel $i_m = i_{m+1}$. Ceci permet de trouver des mots $a', a'' \in A^*$; $a \in A$, $x, x' \in \Sigma^*$ satisfaisant les relations $fb^m = a'x$; $xbx' = a$; $b^{m'} f = x'a''$. Celles ci entrainent que pour tout mot d le mot $w = fb^m d b^{m'} f'$ soit égal à $a'd'a''$ où $d' = xbdx'$. D'après le corollaire II.2. et $xbx' \in A$, on a donc $w \in A^*$ quand $d = c \in C$.

Q.E.D.

Nous n'utiliserons plus désormais l'hypothèse $T \in \bar{\mathfrak{V}}$ mais nous supposerons toujours que la condition $(\mathfrak{V})$ est satisfaite.

II.4. Soient $t,t' \in S$ tels que $tt' = e$ et $t'et \in A^*\rho$. La condition $(\mathfrak{V})$ entraîne que V soit contenu dans $t(A^*\rho)t'$.

Preuve : Soit $g\theta = t'gt$ pour chaque $g \in G$. On a $t(g\theta)t' = tt'gt't' = ege = g$ et $(g\theta)(g'\theta) = tgt'tg't' = tgeg't = tgg't' = (gg')\theta$ pour tout $g' \in G$. Par conséquent θ est un morphisme sur un groupe G' et $V = tV_{G'}t'$. Maintenant nous avons $e\theta = t'et \in A^*\rho$ par hypothèse, donc $V_{G'} \subset A^*\rho$ d'après $(\mathfrak{V})$.

Q.E.D.

II.5 Supposons que l'hypothèse de II.3 ne soit pas satisfaite par b,f,f'. Pour chaque $v \in V$, on peut trouver un $c \in v\rho^{-1}$ pour lequel (X) est vérifiée.

Preuve : Soit $w = fb^n f'$ où $n = |f| + |f'| + 2|b|^2$. Par l'hypothèse, w est un produit $a_1a_2\ldots a_k$ de mots de $A \setminus 1$ où $k \geq n$. Soit d le plus petit indice pour lequel $p_0 = a_1\ldots a_d$ ait f comme facteur gauche et soit d' le plus grand indice pour lequel $p_{|b|+1} = a_{d'+1}\ldots a_k$ ait f' comme facteur droit. Comme tous les a_i ont une longueur positive, le on a $d \leq |f|$ et $k-d' \leq |f'|$ et par conséquent $w = p_0 p p_{|b|+1}$ ou p est le produit d'au moins $2|b|^2$ mots de $A \setminus 1$. On peut donc écrire $p = \bar{p}_1\bar{p}_2\ldots\bar{p}_{|b|}$ où chaque $p_i \in A^*$ à une longueur au moins égale à $2|b|$. Ceci définit pour chaque $j = 0,1,\ldots,|b|$ un facteur gauche $b_j \neq b$ de b tel que $\bar{p}_0\bar{p}_1\ldots\bar{p}_j \in fb^*b_j$.

Comme b a évidemment $|b|$ facteurs gauches propres, on a $b_{j'} = b_j$ pour au moins une paire $0 \leq j' < j \leq |b|$. Définissant b' par

$b = b_j$, $b' = b_j b'$.

$\bar{a}_1 = \bar{p}_0 \cdots \bar{p}_j$, $= f b^m b_j$,

$\bar{a}_2 = \bar{p}_{j'+1} \cdots \bar{p}_j = b' b^q b_j$

$\bar{a}_3 = \bar{p}_{j+1} \cdots \bar{p}_{|b|+1} = b' b^{m'} f'$.

où $q \geq 1$ en raison de $|\bar{p}_{j'+1}| \geq 2|b|$.

Les hypothèses de II.4 sont satisfaites par $t = b_j \rho = b_{j'} \rho$ et $t' = b' \rho$ et nous pouvons donc trouver pour chaque $v \in V$ un mot $a \in A^*$ tel que $c = b_j a b' \in v\rho^{-1}$. Considérons maintenant le mot $w' = \bar{a}_1 \bar{a}_1 a \bar{a}_3 \in A^*$. Il est égal au mot $f b^{m+1} b j a b' b^{m'} f'$ qui appartient à $fb^* c b^* f'$.

Q.E.D.

Ceci achève de montrer que les hypothèses du lemme I.4. sont satisfaites dans tous les cas et conclut la preuve de la proposition I.1.

III. Exemples.

Dans ce qui suit, nous utiliserons le théorème suivant qui ne rassemble que des faits connus.

Théorème III.1. Soit s un élément d'un monoïde S ayant au plus $m < \infty$ éléments et soit $p \geq 1$ le plus petit commun multiple des entiers $\leq m$.

(i) Soit $q \geq 0$ le plus petit entier tel que $s^q \in Ss^{q+1}S$. L'ensemble $s^q s^*$ est un groupe cyclique C_s dont l'ordre $\pi(s)$ divise p.

(ii) Pour chaque multiple $p' \geq q$ de $\pi(s)$, $s^{p'}$ est l'idempotent de C_s;

(iii) $s^{p-1} \in C_s$.

Nous examinons maintenant le cas particulier d'une pseudo-variété de groupes $\mathfrak{V}(H)$ définie par un ensemble non vide Π d'entiers positifs

et la condition que l'ordre $\pi(g)$ de tout élément g d'un groupe de $\mathfrak{V}$ soit dans Π. Comme $\mathfrak{V}$ contient tous les sous groupes de ses membres, Π doit contenir les diviseurs de ses éléments et comme $\mathfrak{V}$ est fermée par produit direct, Π doit l'être par rapport au p.p.c.m. Réciproquement, il est clair que tout Π satisfaisant ces deux conditions définit une pseudo-variété. Le cas où Π est formé de toutes les puissances d'un nombre premier donné a été étudié par Bret Tilson ("On the p-Length of p-solvable semi groups" in "Semi groups", K.W. Folley Ed. 1969). Le cas où Π se réduit à $\{1\}$ donne la pseudo-variété des monoïdes finis dont tous les groupes sont triviaux qui sert dans la théorie des "Counter Free Automata" de R.Mc Naughton et S. Pappert (MII Press 1971).
Nous considérons maintenant une pseudo-variété $\mathfrak{V} = \mathfrak{V}(\Pi)$ fixe.

Exemple III.2. Soit $A \in \mathfrak{V}(\Pi)$-Rec ; A^* appartient à la meme famille ssi pour chaque mot $h \in \Sigma^*$ et tout $n \in N$ assez grand on a l'implication : $h^n \in A^* \Rightarrow h^{n+m} \in A^*$ où
$m = n \wedge \Pi$ désigne le plus grand diviseur de n qui appartienne à Π.

Preuve : Supposons $h^n \in A^*$ pour un $n \geq 1$. D'après le Théorème III.1, il existe un entier $q \in N$ tel $(h^q h^*)\rho$ soit un groupe cyclique C et comme A^* est un monoïde, $(h^q h^* \cap A^*)\rho$ est un sous groupe C' de C. Posant $r = \mathrm{Card}(C)$, $r' = \mathrm{Card}(C')$ on a que le $\mathfrak{V}$-noyau V de C est formé des éléments de la forme $C\rho$ $(c \in C)$ où $p = r \wedge \Pi$ et que pour chaque $n \geq q$ on a $h^n \in A^*$ ssi $n \in r'N$. Par conséquent, la condition énoncée équivaut à $V \subset C'$ et le résultat découle de la Prop. III.1.

Q.E.D.

Une formulation plus élégante due aussi à S.Eilenberg est la suivante :

Pour chaque $h \in \Sigma^*$, et $n \in N$ tels que $(h^n)^* \setminus A^*$ est fini on a $(h^m)^* \setminus A^*$ fini, où $m = n \wedge \Pi$.

Nous laissons au lecteur d'en vérifier l'équivalence avec la précédente.

On notera que comme $\mathrm{Card}(A^*\rho)$ peut être borné à priori en fonction de $k = \mathrm{Card}(A\rho)$, il suffit de vérifier l'implication pour tous les mots h de longueur inférieure à une certaine fonction de k et tous les n appartenant à un interval fini qui est aussi fonction de k.

Nous revenons maintenant à des pseudo-variétés plus générales. Elles requièrent une construction assez pesante pour obtenir des ensembles d'éléments contenus dans un groupe.

Nous commençons par introduire un résultat technique en utilisant les théorèmes classiques de Miller et Clifford (Regular D-classes in Semi groups ; Trans Am. Math. Soc. 82 1956. 270-280).

Dans tous ce qui suit Ω_m désigne le segment initial $\{\omega_1, \ldots \omega_m\}$ de l'alphabet infini $\Omega = \{\omega_j : j \geq 1\}$.

Définition : Soit α_m l'endomorphisme de Ω^* défini par :

$$\omega_j \alpha_m = \omega_1^p \omega_2^p \ldots \omega_{j-1}^p \omega_j^{p+1} \omega_{j+1}^p \ldots \omega_m^p$$

(où $p \geq 1$ est le p.p.c.m des entiers $\geq m$) pour $1 \leq j \leq m$;

$\omega_j \alpha_m = 1$ pour $j \geq m + 1$.

Nous considérons maintenant les endomorphismes α_m^k $(k \in N)$ obtenus en itérant α_m et pour abréger nous écrivons α au lieu de α_m.

III.3. Soit ϕ un morphisme de Ω_m^* dans un monoïde S ayant au plus m éléments.

(i) $\alpha^k\phi = \alpha^{k'}\phi$ pour tout $k' \geq k$ quand $S_k = \Omega_m\alpha^k\phi$ est contenu dans un groupe ;

(ii) Cette dernière condition est satisfaite par au moins un $k \leq m$.

Preuve : Nous posons $s_{j,k} = \omega_j\alpha^k\phi$ et $e_{j,k} = (s_{j,k})p = \omega_j^p\alpha^k\phi$. Donc

$$s_{j,0} = \omega_j\phi \quad \text{et} \quad s_{j,k+1} = e_{1,k}e_{2,k}\cdots e_{j,k}s_{j,k}e_{j+1,k}\cdots e_{m,k},$$

identiquement.

D'après le théorème III.1. et notre choix de p, tous les $e_{j,k}$ sont des idempotents. Donc quand $S_k = \Omega_m\alpha^k\phi = \{s_{j,k} : 1 \leq j \leq m\}$ est contenu dans un groupe, tous ces éléments sont égaux à l'idempotent e de ce dernier et l'on a identiquement $s_{j,k+1} = es_{j,k}e = s_{j,k}$ ce qui établit(i). Soit maintenant pour chaque $k \geq 0$, J_k l'union des idéaux $Se_{j,k}S(1\leq j\leq m)$. Il est clair que chacun de ces derniers contient tous les $s_{i,k+1}$ $(1\leq i\leq m)$ et que par conséquent $J_k \supset J_{k+1}$. Si ℓ est la longueur maximum d'une chaine décroissante d'idéaux (non vides) de S, il existe donc un plus petit $k \leq \ell$ pour lequel $J_k = J_{k+1}$. Or, comme on vient de le dire, J_{k+1} est contenu dans l'intersection des idéqux $Se_{j,k}S(1\leq j\leq m)$ et l'on a la relation $J_{k+1} = J_k = J_{j,k}(1\leq j\leq m)$ qui montre que J_k est un idéal principal. Soit $D = \{s \in S : S\,s\,S = J_k\}$. La relation précédente équivaut à l'assertion que D contient tous les $e_{j,k}(1\leq j\leq m)$ et au poins un $e_{i,k+1}$.

Posons $P = G_1G_2\ldots G_m$, où chaque G_j est la $\mathcal{H}$-classe de $e_{j,k}$. Tous les $s_{j,k+1}(1\leq j\leq m)$ sont contenus dans P. Par conséquent, l'existence d'au moins un $e_{i,k+1} \in D$ montre que $P \cap D \neq \phi$. Comme P est par construction un produit de $\mathcal{H}$-classes contenues dans la $\mathcal{H}$-classe D, les résultats de Clifford et Miller impliquent P soit elle une $\mathcal{H}$-classe contenue dans D et enfin que P soit un groupe ssi $PP^+ \cap D \neq \phi$.

Or cette dernière relation résulte immédiatement de l'existence de $e_{i,k+1} \in D$ et nous avons donc établi que S_{k+1} est contenu dans un groupe.

Pour justifier que $k \leq m$, il suffit enfin d'observer que $\ell = m$ ssi $S = \{1, s, s^2, \ldots, s^m = s^{+1}\}$ où $s^j \neq s^m$ pour $j < m$ et que dans ce cas particulier, l'on a soit $S_0 = S_1 = \ldots = \{1\}$, soit $S_1 = \{s^m\}$.

Q.E.D.

On notera que si l'on suppose $S_k = S_{k+1}$ au lieu de $J_k = J_{k+1}$, la première partie de l'argument montre que chaque $S_{j,k}$ est contenu dans le groupe G_j et que $S_{k+1} \subset p =$ une $\mathcal{R}$-classe dans D. On en conclut de même que P est un groupe d'après $G_j \subset P$ $(1 \leq j \leq m)$.

Université Paris VII
et IRIA
domaine de Voluceau
78150 Rocquencourt

SUR UNE PROPRIETE SYNTACTIQUE DES RELATIONS RATIONNELLES

M. P. SCHUTZENBERGER

(IRIA, Paris)

Résumé: On examine dans un cas particulier l'effet d'une relation rationnelle sur les monoïdes syntactiques.

Abstract: One studies in a special case connections between rational relations and syntactic monoids.

I - Introduction:

Une relation rationnelle $\theta : A^* \to B^*$ entre monoïdes libre associe à chaque partie reconnaissable F de B^* la partie reconnaissable $F\theta^{-1}$ de A^*.

Le problème des invariants syntactiques de θ, c'est à dire des propriétés du monoïde syntactique $Synt(F\theta^{-1})$ qui sont fonction de celles de Synt(F) a été posé par S. Eilenberg qui l'a complètement résolu dans les cas fondamentaux où θ est fonctionnelle ($Card(a\theta)\leq 1$ pour chaque $a \in A^*$) et en particulier quand θ est un morphisme. Nous nous proposons ici d'appliquer la théorie générale de la factorisation des morphismes et des cascades de produits en couronne de J.P. Rhodes et BR. Tilson (dont un bon exposé se trouve dans 'Algebraic Theory of Machines, Languages and Semi-groups, M.A. Arbib. Ed(1968))pour borner supérieurement pour certaines parties F les groupes dans $Synt(F\theta^{-1})$ au moyen de ce qu'après M. Nivat nous appelerons un transducteur pour θ.

Dans cette définition, nous notons 2^{B^*} le semi-anneau des parties du monoïde libre B^* (plus généralement 2^S sera le semi-anneau des parties de tout semi-groupe S).

Définition: μ est un transducteur pour θ ssi il existe un ensemble fini Q et deux éléments $q_0, q_+ \in Q$ tel que μ soit un morphisme de A^* dans le semi-anneau Γ_B des QxQ matrices à entrées dans 2^{B^*} satisfaisant la condition que $a\theta$ soit, pour chaque mot $a \in A^*$, l'entrée (q_0, q_+) de la matrice $a\mu$.

La donnée de θ comme partie rationnelle de $A^* \times B^*$ implique celle d'au moins un de ses transducteurs.

Soient maintenant Γ le semi-anneau des relations dans QxQ, Γ_B celui des QxQ matrices à entrées dans 2^G et enfin β le morphisme de Γ_B dans Γ envoyant chaque matrice m sur son support

$$m\beta = \{(q,q') \in QxQ : m_{q,q'} \neq \emptyset\}.$$

Nous appelerons monoïde des supports du transducteur μ le monoïde (nécessairement fini) $M_\mu = A^*\mu\beta$ formé des supports de toutes les matrices a_μ $(a \in A^*)$.

Le résultat principal de ce travail est la propriété ci-dessous dans laquelle la partie F de B^* est supposée être reconnaissable dans un groupe G, c'est à dire satisfaire $F = F\rho\rho^{-1}$ où ρ est un morphisme de B^* dans un groupe fini G.

Dans la section III on donne une application de cette propriété.

Propriété: Soient $\theta : A^* \to B^*$ une relation rationnelle et $F \subset B^*$ une partie reconnaissable dans un groupe fini G. Quelque soit le transducteur μ pour θ, tout groupe dans $Synt(F\theta^{-1})$ divise un produit en couronne $G \circ G'$ où G' est un groupe dans le monoide M_μ des supports du transducteur.

Montrons pour terminer comment la vérification de cet énoncé se ramène à l'application d'un lemme qui sera établi dans la section II.

Etant donnés Q et le morphisme $\rho: B^* \to G$, nous pouvons prolonger ce dernier à un morphisme (de semi-anneau) de 2^{B^*} dans 2^G puis à un morphisme de Γ_B dans le semi-anneau Γ_G des QxQ matrices à entrées dans G.

Gardant la notation β pour les supports de tous les semi-anneaux considérés, il est clair que $m\rho\beta = m\beta$ pour toute matrice m. Donc si $M' = A^*\mu\rho \subset \Gamma_G$, on a $M'\beta = M_\mu = A^*\mu\beta$. Comme $F\theta^{-1}$ est par définition l'ensemble des mots $a \in A^*$ tels que $a\theta \cap F \neq \emptyset$, nous avons la relation $F\theta^{-1} = \{a \in A^* : (a\mu\rho)_{q_0,q_+} \cap F\rho \neq \emptyset\}$, qui montre que $F' = F\theta^{-1}$ satisfait $F'(\mu\rho)(\mu\rho)^{-1}$. Ceci équivaut à ce que le monoide syntactique de $F\theta^{-1}$ soit une image homomorphe du monoïde fini $M' = A^*\mu\rho$.

Il suffit donc d'établir le lemme énoncé ci-dessous.

II. Un lemme technique:

Nous gardons les mêmes notations.

Lemme: Soit M' un monoïde de QxQ matrices à entrées dans 2^G où G est un groupe fini. Tout groupe H dans M' divise un produit en couronne $G \circ H\beta$ où $H\beta$ est un groupe dans $M'\beta$.

Nous désignons par u l'idempotent de H et nous montrons que la preuve se ramène par des méthodes standard (c'est à dire sans utiliser l'hypothèse que G est un groupe) au cas que nous appelerons positif c'est à dire à celui où le support de u est une classe d'équivalence Q'xQ' (Q'⊂Q).

II.1. Le groupe H divise le produit en couronne N Hβ où Hβ est un groupe et où : N = {h∈H : hβ = uβ}.

Preuve: Hβ est un groupe puisque H est un groupe et β un morphisme. De plus N est le noyau de β et la formule est un cas particulier des théorèmes de base des produits en couronne.

Q.E.D.

Etant données une relation quelconque r⊂QxQ et une matrice m∈M', nous designons par m∧r la matrice $m' \in \Gamma_G$ telle que l'on ait identiquement $m'_{q,q'} = m_{q,q'}$ ou = Ø selon que (q,q') ∈ r ou non.

II.2. Il existe une famille $\{\varepsilon_i : i \in I\}$ de morphismes de N tels que d'une part chaque $N\varepsilon_i$ soit positif, d'autre part N soit un sous-groupe du produit direct des groupes $N\varepsilon_i$.

Preuve: Comme le support de u est une relation idempotente, il existe une famille de parties de Q non vides disjointes, Q_i (i∈I) et une relation v telles que uβ soit l'union disjointe de $e = \sum_i Q_i x Q_i$ et de v et que $v = ev + ve + v^2$. Ceci entraîne que $\varepsilon_i : h \to h \cap (Q_i x Q_i)$ soit un morphisme de N pour chaque i ∈ I et que $\varepsilon : h \to \sum_i h\varepsilon_i$ soit un morphisme de N sur un sous-groupe Nε du produit direct des groupes positifs $N\varepsilon_i$. Il suffit donc de montrer que le noyeau E = {h∈N : hε=uε} de ε est réduit à {u} puisque N divise E∘Nε.
Ceci est trivial quand uβ=QxQ. Comme ce cas couvre celui où Q est un singleton, nous pouvons donc procéder par induction sur Card(Q)≥2 en supposant e≠QxQ. Cette dernière hypothèse implique l'existence d'une partition propre Q=Q'+Q" telle que h∩(Q"xQ') = Ø pour chaque h∈ N et que, par conséquent $h \to h \cap (Q'xQ' + Q"xQ")$ soit un morphisme de N. Ceci permet d'écrire $u = \begin{pmatrix} a & c \\ \emptyset & b \end{pmatrix}$ où a et b sont respectivement une Q'xQ' et une Q"xQ" matrice idempotente. Soit h ∈ E. D'après l'hypothèse d'induction $h = \begin{pmatrix} a & x \\ \emptyset & b \end{pmatrix}$, $h^{-1} = \begin{pmatrix} a & y \\ \emptyset & b \end{pmatrix}$.

Les identités $u = u^2 = uhh^{-1}$ et $h = uhu$ donnent les relations:

$c = ac + cb = axb + ay + cb$ et

$x = axb + ax + bc$.

Donc $x = axb + c = axb + ay + cb = c$ montrant que $h = u$ et $E = \{u\}$.

Q.E.D.

Il suffit donc maintenant de vérifier le lemme dans le cas particulier où $H = N$ est positif et l'on peut même supposer pour simplifier $u\beta = QxQ$.

II.3. Tout groupe H dans M' tel que $h\beta = QxQ$ pour chaque $h \in H$ divise le groupe G.

Preuve: D'après la relation $u^2 = u$ on a $(u_{q,q})^2 \subset u_{q,q}$ pour chaque $q \in Q$, donc $u_{q,q}$ est un sous semi-groupe de G. Comme il est non vide et que G est un groupe fini, c'est un sous-groupe G_q de G.

Soit $h \in H$. La relation $uh = h$ montre que $G_q h_{q,q'} = u_{q,q} h_{q,q'} \subset h_{q,q'}$ pour chaque $q' \in Q$, c'est à dire que $h_{q,q'}$ est une union des cosets de G_q. La même chose vaut pour les entrées $h^{-1}_{q',q}$ de h^{-1} et la relation $hh^{-1} = u$ qui implique $h_{q,q'} h^{-1}_{q',q} \subset u_{q,q} = G_q$ montre que de fait chacune de ces entrées de h et de h^{-1} est un coset unique (non vide) de G_q.

Ceci s'applique en particulier à la matrice u elle-même et à chacune de ses entrées, $u_{q',q''}$ qui est donc à la fois un coset à droite de $G_{q'}$ et un coset à gauche de $G_{q''}$. $(q',q'' \in Q)$.

Prenons maintenant un $q_0 \in Q$ fixe et posons pour chaque $h \in H$, $h_0 = h \wedge (\{q_0\}, \{q_0\})$ = la matrice obtenue en remplaçant toutes les entrées par $\emptyset$, sauf h_{q_0,q_0}. L'identité $h = uhu$ et les relations précédentes montrent que l'on a identiquement $h = uh_0u$.

Comme $\emptyset \neq h_0 h'_0 \subset (hh')_0$ pour tout $h,h' \in H$, l'application $h \to h_0$ est un morphisme injectif. Donc, enfin, H est isomorphe au groupe G'_{q_0}/G_{q_0} où le sous-groupe G'_{q_0} de G est l'union des cosets $H_0 (h \in H)$ de G_{q_0}.

Q.E.D.

Ceci achève la preuve du lemme, donc aussi de la propriété.
Les techniques restent appliquables quand H est un groupe de matrices à entrées dans 2^S où S est un semi-groupe sans idéaux propres (G est alors son groupe de Suschkewitsch). Ceci donnerait une généralisation assez immédiate de la propriété au cas où F est reconnaissable dans S à condition de considérer seulement les semi-groupes libres A^+ et B^+.

Dans le cas général, les groupes dans $Synt(F\theta^{-1})$ sont soumis à des contraintes (assez peu strictes, et de nature quasiment numérique) que je

n'ai pas réussi à formuler de façon raisonnablement simple (ou non triviale). Par exemple, si S est le monoïde booleen {1,0} (qui est union de groupes!), le monoide des QxQ matrices positives à entrées dans 2^S contient le groupe symétrique sur Q : il suffit pour cela de représenter ce dernier par le monoïde des bijections et de remplacer chaque entrée vide par {0} et chaque entrée non vide par {1,0}.

III. Une application

Revenant aux notation de l'introduction, nous considérons désormais le cas où la relation θ est l'inverse d'une subtitution (rationnelle) $\theta^{-1} : B^* \to A^*$, c'est à dire d'un morphisme de B^* dans 2^{A^*}, donné par les parties reconnaissables $b\theta^{-1} \subset A^*$ ($b \in B$ où l'alphabet B est évidemment supposé fini). Pour simplifier nous ferons l'hypothèse supplémentaire que $B\theta^{-1}$ est contenu dans le semi-groupe $A^+ (= A^* \setminus \{1\})$, c'est à dire que $1 = 1\theta = 1\theta^{-1}$.

Nous désignerons par $M_2 = A^*\tau_2$ le monoïde syntactique simultané des parties $b\theta^{-1}$ ($b \in B$), par $M_1 = A^*\tau_1$ celui de $B^*\theta^{-1}$, et par M_3 le produit direct $M_1 \times 2^{M_1 \times M_2} \times M_2$.

D'après la théorie générale des produits en couronne, il est possible de munir M_3 d'une structure de monoïde ayant les deux propriétés suivantes:

(i) Tout groupe dans M_3 est produit sous-direct d'un groupe dans M_1 et d'un groupe dans M_2;

(ii) Si σ_3' est l'application envoyant chaque mot $a \in A^*$ sur $a\sigma_3' = \{(a'\sigma_1, a''\sigma_2) \in M_1 \times M_2 : a', a'' \in A^*, a'a'' = a\}$, l'application $\sigma_3 : a \to (a\sigma_1, a\sigma_3', a\sigma_2)$ est un morphisme (de semi-groupe) de A^* dans M_3.

Rappelant que F est une partie de B reconnaissable dans le groupe fini G, nous nous proposons d'établir:

III.1. Tout groupe dans le monoïde syntactique de $F\theta^{-1}$ divise le produit en couronne de G dans un groupe dans M_3.

Nous construisons d'abord en application immédiate de la théorie générale des relations rationnelles, un transducteur (standard) μ pour θ et, d'après la propriété, il suffira de vérifier que son monoide des supports M_μ divise M_3.

Contruction du transducteur.

La donnée des parties $b\theta^{-1}$ ($b \in B$) implique celle d'un ensemble minimal fini Q', d'une action $Q' \times A^* \to Q'$, de parties Q_b de Q' ($b \in B$) et d'un élément distingué $q_o \in Q'$ tels que pour chaque lettre b de B on ait

$$b\theta^{-1} = q_o^{-1} Q_b \quad (=\{a \in A^* : q_o a \in Q_b\}).$$

Nous adjoignons un nouvel élément q_+ à Q' et nous étendons l'action précédente à $Q = \{q_+\} \cup Q'$ en posant $q_+ a = \emptyset$ pour chaque $a \in A^+$.

Nous définissons maintenant pour chaque lettre a deux QxQ matrices $a\mu'$ et $a\mu''$ (à entrées dans le semi-anneau des parties de B*) par les conditions suivantes :

Pour tout $q, q' \in Q$:

$a\mu'_{q',q} = 1$ ou $\emptyset$ selon que $q'a = q$ ou non;

$a\mu''_{q',q} = \emptyset$ pour $q \neq q_o, q_+$ et, sinon,

$= b$ si $q = q_o$ ou q_+ et $q'a \in Q_b$.

De plus nous définissons les deux matrices $1\mu'$ et $1\mu''$ par les conditions :

$1\mu'_{q',q} = 1$ si $q' = q \neq q_+$;

$= \emptyset$ sinon.

$1\mu''_{q',q} = 1$ si $q' = q_o, q = q_+$;

$= \emptyset$ sinon.

L'application $\mu = \mu' + \mu''$ s'étend à un morphisme (de semi-groupe) de A* dans le semi-anneau Γ_B.

III.2 μ est un transducteur pour θ.

Preuve: Notons av le Q-vecteur égal à la ligne q_o de $a\mu$ ($a \in A^*$). Pour $a = 1$, toutes ces coordonnées sont $\emptyset$ sauf la dernière, c'est à dire qui est égale à $1 = 1\theta^{-1}$ d'après l'hypothèse $B\theta^{-1} \subset A^+$.

Ceci permet de procéder par induction sur la longueur des mots et il suffit de vérifier les deux formules suivantes pour $a'a$ où $a' \in A^+$, $a \in A$ en les supposant établis pour a':

(21). Pour tout $q \in Q$:

$$a'av_q = \Sigma\{b \in B^* : a'a \in b\theta^{-1}q_0^{-1}q\};$$

(22). $$a'av_{q_+} = \Sigma\{b \in B^* : a'a \in b\theta^{-1}\} = a\theta.$$

Nous utilisons le fait que par construction, la ligne q_+ de $a\mu$ est vide et nous observons que les mots $b \in B^*$ qui apparaissent dans (21) le font d'au moins l'une des deux manières suivantes:

(i) Il existe un $q' \in Q'$ et une factorisation $a = a_1a_2 (a_1, a_2 \in A^*)$ tels que

$$a_1 \in b\theta^{-1} \; ; \; q_0a_2 = q' \; ; \; q'a = q.$$

On vérifie directement que la contribution de ces mots est pour $q \in Q'$, la coordonnée q du produit $a'v.a\mu'$ et pour $q = q_+$ celle de $a'v.a\mu"$.

(ii) On a $aa' \in b\theta^{-1}$ et $q = q_0$. Comme $b\theta^{-1} \subset A^+$, il existe un $q' \in Q'$ et des factorisations $b = b_1b'$ $(b_1 \in B^*, b \in B)$ $a = a_1a_2 (a_1, a_2 \in A^*)$ tels que:

$$a_1 \in b_1\theta^{-1} \; ; \; q_0a_2 = q' \; ; \; q'a \in Q_{b'}.$$

Comme ci-dessus la contribution correspondante est la coordonnée q_0 du produit $a'v.a\mu"$.

La formule (21) résulte immédiatement de ce deuxième cas et de la définition de $\mu"$.

Q.E.D.

III.3. Le monoïde $M_\mu = A^*{}_{\mu\beta}$ est une image homomorphe de M_3.

Preuve: Il suffit de vérifier que pour deux mots a et a' quelconques, $a\mu\beta \neq a'\mu\beta$ implique $a\sigma_3 \neq a'\sigma_3$.

La première relation signifie que les entrées (q',q) des deux matrices sont différentes pour au moins une paire $q',q \in Q$. On peut prendre $a" \in q_0^{-1}q'$ et, posant $a_1 = a"a$, $a_1' = a"a_1'$, on a que les coordonnées q des supports des vecteurs a_1v et $a_1'v$ sont différentes. Ceci entraîne $a_1\sigma_3 \neq a_1'\sigma_3$ (donc le résultat cherché) d'après la formule (21) et la définition de $\sigma_3' : A^* \to 2^{M_1 \times M_2}$ si $q \neq q_+$ et d'après la formule (22) et $\sigma_3 = \sigma_1 \times \sigma_3' \times \sigma_2$ si $q = q_+$.

Q.E.D.

Ceci conclut la preuve de II.1. A titre d'exemple, nous considérons le cas particulier suivant.

III.4. Soient $r \geq 1$ et P l'ensemble générateur minimum d'un sous-monoide de $P^* \in Rat(A^*)$ de A^*. Tout groupe dans le monoide syntactique de $(P^r)^*$ divise le produit en couronne du groupe cyclique $Z_{(r)}$ dans un produit direct de groupes dans le monoïde syntactique de P^*.

Preuve: Prenons $B = \{b\}$ et $\rho : B^* \to G = Z_{(r)}$ tel que b_ρ soit un générateur de ce groupe. Si θ^{-1} est la substitution telle que $b\theta^{-1} = P$, on a $(P^r)^* = 1\rho^{-1}\theta^{-1}$ et le résultat est encore une conséquence de la théorie des produits en couronne puisque d'après celle-ci chaque groupe dans le monoïde syntactique de P divise un groupe dans Synt(P*) quand P est l'ensemble générateur minimum.

Q.E.D.

En particulier tout groupe dans $Synt(P^r)^*$ est résoluble quand ceci est vrai pour Synt(P*).

Année 1975

Bibliographie

[1] Marcel-Paul Schützenberger. Solution non commutative d'une équation différentielle classique. In E. R. Caianiello, editor, *New concepts and technologies in parallel information processing (Proc. NATO Adv. Study Inst., Capri, 1973)*, pages 381–401. NATO Adv. Study Inst. Ser. E : Appl. Sci., Vol. 9. Noordhoff, Leiden, 1975.

[2] Marcel-Paul Schützenberger. Sur les relations rationnelles. In *Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975)*, pages 209–213. Lecture Notes in Comput. Sci., Vol. 33. Springer, Berlin, 1975.

[3] Marcel-Paul Schützenberger. Sur certaines opérations de fermeture dans les langages rationnels. In *Symposia Mathematica, Vol. XV (Convegno di Informatica Teorica, INDAM, Roma, 1973)*, pages 245–253. Academic Press, 1975.

[4] Dominique Foata and Marcel-Paul Schützenberger. Quelques remarques sur une propriété d'équidistribution des permutations. In J. C. Bermond and R. Cori, editors, *Journés de combinatoire et informatique, 4, 5, 6 juin 1975*, pages 121–124. Université de Bordeaux 1, 1975.

OFFPRINT FROM

NEW CONCEPTS AND TECHNOLOGIES IN PARALLEL INFORMATION PROCESSING

edited by

E. R. CAIANIELLO

Director of the Laboratory
of Cybernetics, CNR
Arco Felice, Italy

NATO ADVANCED STUDY INSTITUTES SERIES

Series E: Applied Sciences
Volume 9. New Concepts and Technologies in
Parallel Information Processing

NOORDHOFF – LEYDEN – 1975

SOLUTION NON COMMUTATIVE D'UNE EQUATION DIFFERENTIELLE CLASSIQUE

M.P. SCHÜTZENBERGER

(Fac. Sci. Paris et Laboratorio di Cibernetica del CNR, Arco Felice)

INTRODUCTION

Cette communication fait partie d'une série de recherches poursuivies depuis plusieurs années avec mon ami le Professeur D. Foata sur les nombres d'Euler, c'est à dire sur les coefficients de Hurwitz de la fonction $\mathrm{tgt} + 1/\mathrm{cost}$.

Les rapports que peuvent avoir de semblables questions arithmétiques avec certains aspects de la cybernétique ont été brillament illustrés par les deux conférenciers qui m'ont précédé et je me bornerai donc à discuter un problème de nature purement technique, à savoir la solution de l'équation différentielle classique $y'' = y\,y'$ dans le cas non commutatif, c'est à dire, par exemple, dans le cas où la fonction inconnue y et ses dérivées y' et y'' appartiennent à un anneau de matrices dont les entrées sont des fonctions de la variable indépendante t.

Dans le cas commutatif, la solution de cette équation qui satisfait les conditions initiales $y(0) = y'(0) = 1$ est précisément la fonction génératrice exponentielle $\mathrm{tgt} + 1/\mathrm{cost}$ des nombres

d'Euler. (Cf (1), (4), (5)). Il me parait assez remarquable que l'on puisse en exprimer la solution dans le cas général au moyen d'une famille infinie de polynomes en les variables (non commutatives) $y(0)$ et $y'(0)$ dont les coefficients numériques dépendent assez simplement des nombres d'Euler.

Dans un premier chapitre nous rappelons quelques éléments du formalisme de la théorie des équations différentielles et, dans les deux suivants, nous appliquons ces notions au cas de $y'' = y\,y'$. Dans le dernier chapitre nous présentons une autre propriété remarquable de l'opérateur associé à cette équation.

I. GENERALITES

I.1. Pour simplifier au maximum ce rappel de notions connues nous nous bornons à considérer une équation différentielle du second ordre.

(1) $y'' = H(t, y, y')$

où H est un polynôme dont les coefficients appartiennent à un anneau donné $\mathcal{A}$ de caractéristique zéro. Formellement nous introduisons l'anneau $\bar{\mathcal{A}} = \mathcal{A}[y, y']$ des polynomes à coefficients dans $\mathcal{A}$ en les variables (non commutatives) y et y' et l'anneau $\bar{\mathcal{A}}(t)$ n'ayant qu'un nombre fini de termes non nuls. Par définition, une solution formelle de (1) est un élément

$$Y = \sum_{0\leq n} \frac{t^n}{n!}\, a_n \quad \text{de} \quad \bar{\mathcal{A}}(t)$$

satisfaisant les deux conditions suivantes :

(2) $a_0 = y \;;\; a_1 = y' \;;\; a_{n+2} \in \bar{\mathcal{A}}$ pour chaque $n \in \mathbb{N}$;

(3) $Y'' = H(t, Y, Y')$ où Y' et Y'' sont définies par

(4) $Y' = \sum_{0\leq n} \frac{t^n}{n!}\, a_{n+1} \;;\; Y'' = \sum_{0\leq n} \frac{t^n}{n!}\, a_{n+2}$.

Comme H est un polynome, le coefficient de t^n dans le membre de droite de (3) est pour chaque n un polynome en $a_0, a_1, \ldots, a_{n+1}$ cependant que le coefficient de t^n dans Y" est égal à $(n+2)\,a_{n+2}$. Il en résulte immédiatement que a_{n+2} est déterminé de façon unique par les a_i d'indices inférieurs, d'où par induction, que tous les a_n appartiennent à $\bar{\mathcal{A}}$. Autrement dit, l'équation (1) admet une et une seule solution formelle satisfaisant $Y(0) = y$, $Y'(0) = y'$.

Soit maintenant φ un morphisme de $\bar{\mathcal{A}}$ dans une algèbre normée. On peut montrer que pour chaque ε positif il existe un ε', positif lui aussi, tel que l'on ait identiquement $||a_n \varphi|| \leq n!\,\varepsilon^n$ quand $||y\varphi||$ et $||y'\varphi||$ sont inférieurs à ε'. Ceci entraine que la série $Y\varphi = \Sigma \frac{t^n}{n!} (a_n\varphi)$ converge absolument au voisinage de l'origine et montre que la solution formelle est bien <u>la</u> solution de (1).

I.2. Nous en venons maintenant au calcul effectif des polynomes a_n et pour cela nous rappelons qu'une <u>dérivation</u> d'un anneau $\mathcal{B}$ quelconque est une application β de $\mathcal{B}$ dans lui même, satisfaisant l'identité :

(5) $(ab)\,\beta = (a\,\beta)\,.\,b + a\,.\,(b\,\beta)$ pour tout $a, b \in \mathcal{B}$.

$\mathcal{A}(t)$ des séries formelles en la variable t dont les coefficients sont dans $\mathcal{A}$. Par définition, une solution formelle de (1) est un élément de l'anneau

Nous considérons désormais le cas où $\mathcal{B} = \bar{\mathcal{A}}_{(t)}$ et nous notons ∂ la dérivation de noyau $\bar{\mathcal{A}}$ envoyant t sur 1. On a identiquement $t^n\partial = nt^{n-1}$.

Ceci entraine évidemment que β soit définie par la donnée de son action sur les générateurs de $\mathcal{B}$ et que $\beta\,\mu$ et $\mu\,\beta$ soient aussi des dérivations pour tout morphisme μ de $\mathcal{B}$ dans lui même.

Par conséquent si

$$X = \Sigma \frac{t^n}{n!} b_n$$

est une série formelle (dont les coefficients b_n sont dans $\bar{\mathcal{A}}$) nous aurons la formule habituelle

(6) $X \partial^p = \Sigma \frac{t^n}{n!} b_{n+p} \quad (p \in \mathbb{N})$

d'où l'on déduit que $b_n = X \partial^n \theta$ où θ est le morphisme de $\bar{\mathcal{A}}(t)$ sur son sous-anneau $\bar{\mathcal{A}}$, laissant ce dernier invariant et envoyant t sur 0.

En particulier notre équation différentielle peut s'écrire sous la forme $Y \partial^2 = H(t, Y, Y \partial)$ et les calculs d'identification des coefficients a_n de $\frac{t^n}{n!}$ dans Y effectués plus haut sont équivalents à l'ensemble des équations :

(7) $Y \theta = y \; ; \; y \partial \theta = y' \; ; \; Y \partial^{n+2} \theta = H \partial^n \theta$.

Nous nous proposons de mettre ces relations sous une forme plus compacte. Pour cela nous considérons une suite de nouvelles variables non commutatives $\{x_j\}$ $(j \in \mathbb{N})$, l'algèbre large $\mathcal{A}(t, \{x_j\})$, une dérivation χ de cette algèbre définie par la condition que $a\chi = 0$ pour chaque $a \in \mathcal{A}$, $t\chi = 1$ et $x_j \chi = x_{j+1}$ pour chaque $j \in \mathbb{N}$ et enfin le morphisme ξ laissant $\mathcal{A}(t)$ invariant et envoyant chaque x_j sur $X\partial^j$ où $X = \Sigma \frac{t^n}{n!} b_n$ $(b_n \in \mathcal{A})$.

Comme on l'a mentionné plus haut, $\xi\partial$ et $\chi\partial$ sont deux dérivations et par définition elles coincident sur $\mathcal{A}(t)$. En outre pour chaque $j \in \mathbb{N}$ on a $x_j \xi\partial = x_{j+1}\xi = x_j \chi\xi$.

Par conséquent on a

(8) $K\xi\partial = K\chi\xi$

quelque soit la série formelle K en t et les x_j .

Posons maintenant $x_0 = y$, $x_1 = y'$ et définissons une dérivation η de $\mathcal{A}(t)$ par les conditions $a\eta = 0$ pour $a \in \mathcal{A}$, $t\eta = 1$; $y\eta = y'$, $y'\eta = H(t, y, y')$.

Si $X = Y$ est la solution formelle de notre équation, nous avons l'identité

$$Y\partial^{n+2} = H(t, x_0, x_1)\,\xi\,\partial^n = H(t, x_0, x_1)\,\chi^n\,\xi$$

d'où en particulier $x_2\,\xi = Y\partial^2 = H(t, x_0, x_1)\,\xi$ puis par induction sur n $x_{n+2}\,\xi = Y\partial^{n+2} = H\eta^n\,\xi = y\,\eta^{n+2}\,\xi$ ce qui donne enfin d'après (7) la formule cherchée :

$a_n = Y\partial^n\theta = y\,\eta^n\,\theta$ c'est à dire

$$(9)\quad Y = \sum_{o\le n} \frac{t^n}{n!}\,(y\,\eta^n\,\theta)\ .$$

I.3. Considérons à titre d'exemple l'équation classique

$$y' = ay - yb + c \quad (a, b, c \in \mathcal{A})$$

dont la solution remonte à Wedderburn. En raison de sa forme particulière la dérivation η se réduit au morphisme de $\mathcal{A}(t)$ laissant $\mathcal{A}(t)$ invariant et envoyant y sur $ay - yb + c$. En outre θ se réduit à l'identité. La solution Y est donc égale à

$$y + \frac{t}{1!}\,(ay - by + c) + \ldots + \frac{t^n}{n!}\,(y\,\eta^n) + \ldots$$

Par induction sur n on pourrait d'ailleurs vérifier que le coefficient $a_n = y\,\eta^n$ peut s'expliciter de la façon suivante :

$$a_n = \sum_{o\le j\le n} (-1)^j \begin{bmatrix} n \\ j \end{bmatrix} a^{n-j}\,y\,b^j + \sum_{o\le j\le n-1} (-1)^j \begin{bmatrix} n-1 \\ j \end{bmatrix} a^{n-1-j}c\,b^j$$

Un autre exemple est fourni par l'équation $y'' = y\,y'$ qui nous interessera plus particulièrement ici. La dérivation η laisse $\mathcal{A}(t)$ invariant et elle envoye y sur y' et y' sur $y\,y' = H$. Les premiers termes du développement de la solution Y sont $Y = y + \frac{t}{1!}\,y' + \frac{t^2}{2!}\,(y\,y') + \ldots$ et on calcule :

386

$$a_3 = (y\,y')\,\eta = y'\,y' + y\,y\,y'$$
$$a_4 = (y'^2 + y^2\,y')\,\eta = y\,y'\,y' + y'\,y\,y' + y'\,y\,y' + y\,y'\,y' + y^2\,y\,y' = (y^3 + 2\,y\,y' + 2\,y'\,y)\,y'$$
$$a_5 = a_4\,\eta = (y^4 + 3\,y^2\,y' + 5\,y\,y'\,y + 3\,y'\,y^2 + 4\,y'^2)\,y'$$
$$a_6 = a_5\,\eta = (y^5 + 4\,y^2\,y'\,y + 9\,y^2\,y'\,y + 9\,y\,y'\,y^2 + 4\,y'\,y^2 + 12\,y\,y'^2 + 10\,y'\,y\,y' + 12\,y'^2\,y)\,y'$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

L'expression des coefficients est passablement compliquée et sera donnée (de façon indirecte) dans la section suivante.Les polynomes a_n ont été définis dans un tout autre contexte (où ils sont dénotés par D_{n+1}). Leurs valeurs pour $y = y' = 1$ sont les nombres d'Euler.

II. L'EQUATION $y'' = y\,y'$

II.1. Nous gardons les notations utilisées dans l'exemple ci-dessus et nous nous proposons d'expliciter les polynomes $a_n = y\,\eta^n \in \overline{\mathcal{A}} = \mathcal{A}[y, y']$ au moyen d'un changement de variable. Pour cela nous considérons deux nouvelles variables x et z et l'anneau $\overline{\mathcal{B}} = \mathcal{A}[x, z]$ de leurs polynomes non commutatifs. Nous définissons le morphisme φ, l'anneau de polynomes et la dérivation σ de $\overline{\mathcal{B}}$ par les conditions suivantes :

(10.1) $x\varphi = y$; $z\varphi = -y^2 + 2y'$;

(10.2) $x\sigma = x^2 + z$; $z\sigma = 0$.

Nous établissons d'abord la remarque (11) :

Pour chaque $\eta \in \mathbb{N}$ on a $a_{n+1} = b_n\,\varphi\,y'\,2^{-n}$ où les b_n sont des polynomes de $\overline{\mathcal{B}}$ définis par la récurrence

$$b_o = 1 \quad ; \quad b_{n+1} = b_n\,\sigma + x\,b_n + b_n\,x \;(= b_n\,\lambda).$$

Preuve : On a $a_o = y$ et d'après $y\,\eta = y'$ $y'\,\eta = y\,y'$, il existe pour chaque $\eta \in \mathbb{N}$ un polynome a'_n tel que $a_{n+1} = a'_n y'$.

Comme $a'_{n+1}\, y' = a_{n+1} = a_n\, \eta = a'_n\, y'\, \eta = a'_n\, \eta\, y' + a'_n\, (y'\, \eta)$ $= a'_n\, \eta\, y' - a'_n\, yy'$, on a la récurrence $a'_{n+1} = a'_n\, \eta + a'_n\, y$ avec $a'_o = 1$.

Notons maintenant que φ est un isomorphisme dont l'inverse ψ est définie par $y\, \psi = x$ et $y'\, \psi = \frac{1}{2}\, (x^2 + z)$.
Posant $b_n = a'_n\, \psi\, .\, 2^n$ nous aurons donc $b_o = 1$ et $a_n = b_n\, \varphi\, .\, y'$ pour chaque n positif. De plus les b_n satisferont la relation de récurrence

$$b_{n+1} = a'_{n+1}\, \psi\, .\, 2^{n+1} = 2\, (a'_n\, \eta\, \psi\, .\, 2^n + a'_n\, .\, y\, \psi\, .\, 2^n)$$
$$= 2\, (b_n\, \varphi\, \eta\, \psi + b_n\, x)\ .$$

Maintenant, comme φ est un isomorphisme l'application linéaire $\bar{\eta} = \varphi\, \eta\, \psi$ est une dérivation de $\mathfrak{B}$ dont l'action sur les générateurs x et z est donnée par le calcul

$$x\, \bar{\eta} = y\, \eta\, \psi = y'\, \psi = \frac{1}{2}\, (x^2 + z) = \frac{1}{2}\, x\, \sigma \ ;$$
$$z\, \bar{\eta} = (2\, y' - y^2)\, \eta\, \psi = (2\, y\, y' - y\, y' - y'\, y)\, \psi$$
$$= (y\, y' - y'\, y)\, \psi = x\, \frac{1}{2}\, (x^2 + z) - \frac{1}{2}\, (x^2 + z)\, x$$
$$= \frac{1}{2}\, (x\, z - z\, x)\ .$$

Ceci permet d'écrire $\bar{\eta} = \frac{1}{2}\, (\sigma + \rho)$ où ρ est la dérivation envoyant x sur 0 et z sur $x\, z - z\, x$, et nous avons donc $b_{n+1} = b_n\, \sigma + b_n\, \rho + 2\, b_n\, x$.

Il suffit désormais de montrer que pour tout monôme u en x et z on a identiquement $u\, \rho + 2\, u\, x = x\, u + u\, x$. Or ceci est trivial quand $u = x^n$ puisque $x^n\, \rho = 0$ et $x^n\, x = \frac{1}{2}\, (x\, x^n + x^n\, x)$.

Supposons donc ce résultat établi pour le monome v et prenons $u = v\, z\, x^n$. On a :

388

$$u\rho + 2ux = v\rho \cdot z x^n + v(xz - zx)x^n + 2vzx^{n+1}$$
$$= xvzx^n - vxzx^n + vxzx^n - vzx^{n+1} + 2vzx^{n+1}$$
$$= xu + ux \qquad \text{Q.E.D.}$$

Dans ce qui suit nous nous bornerons au calcul des polynômes $b_n = 1\lambda^n$ dont les premiers sont

$b_o = 1$; $b_1 = b_o\lambda = x1 + 1x = 2x$;

$b_2 = 2x\lambda = 2(x^2 + z) + x \cdot 2x + 2x \cdot x = 6x^2 + 2z$;

$b_3 = 24x^3 + 8(xz + zx)$;

$b_4 = 120x^4 + 40(x^2z + xzx + zx^2) + 16z^2$;

Notre résultat principal est résumé par les formules 17 et 22 ci-dessous. Notant M le monoïde libre engendré par $\{x, z\}$, c'est à dire l'ensemble des monômes en x et z nous écrirons chaque polynôme b de B comme une somme finie $\Sigma\{\langle b, m\rangle m : m \in M\}$ dont les coefficients $\langle b, m\rangle$ appartiennent à $\mathcal{A}$. L'application $\langle , \rangle$ sera étendue de façon naturelle à une application bilinéaire de $\mathcal{B} \times \mathcal{B}$ dans $\mathcal{A}$.

Le degré $|m|$ d'un mot $m \in M$ sera par définition $|m|_x + 2|m|_z$ où, comme d'usage, $|m|_x$ (resp. $|m|_z$) dénote le nombre d'occurence de x (resp. z) dans m.

On vérifie sans difficulté que chacun des termes d'un polynôme $m\lambda$ $(m \in M)$ est de degré $|m| + 1$.

Comme $b_o = 1$ est homogène de degré zéro, il en résulte que chaque $b_n = 1\lambda^n$ est homogène de degré n. Ceci entraine en particulier que chaque mot m ait le même coefficient dans $b_{|m|}$ et dans la série formelle $B = \Sigma_{o\le n} b_n$. Ceci nous permettra d'utiliser la notation $\langle B, m\rangle$ au lieu de $\langle b_{|m|}, m\rangle$.

III. CALCUL DES POLYNOMES b_n

III.1. Nous désignerons par μ la transposée de $\lambda\dagger$ de λ, c'est à dire l'application linéaire de $\mathcal{B}$ telle que pour chaque paire $m, m' \in M$ le coefficient de m dans $m'\mu$ soit égal au coefficient de m' dans $m\lambda$. On vérifie facilement que chaque $m'\mu$ est un polynôme. Par définition on a la formule

(12) $b\lambda = \Sigma \langle b, m\mu \rangle m$

pour tout polynôme (ou série formelle) b. En particulier

(13) $\langle B, m \rangle = \langle b, m\mu \rangle$ identiquement.

Comme λ est rationnelle au sens de Eilenberg, un théorème de cet auteur que nous nous bornerons à appliquer donne une technique générale pour calculer M. Pour cela nous écrivons $\sigma = \sigma_x + \sigma_z$ où σ_x est la dérivation envoyant x sur x^2 et σ_z la dérivation envoyant x sur z, les noyaux de ces deux dérivations étant les polynômes qui ne contiennent pas la variable x. La transposée μ de λ est la somme des transposées des applications linéaires σ_x, σ_z, $m \longrightarrow m\,x$ et $m \longrightarrow x\,m$.

En ce qui concerne ces deux dernières, ce sont les applications $m \longrightarrow m\,x^{-1}$ et $m \longrightarrow x^{-1}\,m$ où, comme d'usage, la notation $m\,x^{-1}$ (resp. $x^{-1}\,m$) désigne le monome m' tel que $m'\,x = m$ (resp. $x\,m' = m$) s'il en éxiste un et 0 autrement. En ce qui concerne $\sigma_z\dagger$ c'est l'application envoyant chaque $m \in M$ sur la somme des produits $m_1 \times m_2$ où $m_1, m_2 \in M$ satisfont $m_1\,z\,m_2 = m$.

Enfin $m\,\sigma_x\dagger$ est la somme des monômes $m_1 \times m_2$ étendue à toutes les paires $m_1, m_2 \in M$ telles que $m_1 \times x \times m_2 = m$. On voit sans peine que $x^{-1}\,m + m\,x^{-1} + m\,\sigma_z\dagger$ a tous ses coefficients 0 ou 1 et qu'aucun mot du support de $m\,\sigma_z\dagger$ (c'est à

390

dire de l'ensemble des mots ayant un coefficient non nul dans ce polynôme) n'appartient au support de m $m\,\sigma_x^{-1}$.

Par contre, si $m = m_1\, x^n\, m_2$ où $n \geq 2$ et où les mots m_1 et m_2 satisfont la condition $m_1 \notin M_x$, $m_2 \notin x\,M$ (c'est à dire, pour abréger si x^n est un x^*– facteur maximal de m), le mot $m' = m_1\, x^{n-1}\, m_2$ apparait dans $m\,\sigma_x\dagger$ avec la multiplicité $n-2$. Si en outre $m_1 = 1$, le même mot m' apparait dans $x^{-1}\, m$ ce qui fait que son coefficient dans $m\mu$ devient $n-1$. La même remarque vaut quand $m_2 = 1$.

A titre d'application nous calculons

(14) Pour chaque $n \in \mathbb{N}$, le coefficient $\langle B, x^n \rangle$ est égal à $(n+1)!$.

Preuve : Ceci est vrai pour $n = 0$, puisque $b_o = 1 = (0+1)!$. Soit donc n positif. On a $x^n\,\sigma_z\dagger = 0$ et par conséquent

$$x^n\,\mu = x^n\,\sigma_x\dagger + x^{-1}\,x^n + x^n\,x^{-1} = (n-1)\,x^{n-1} + x^{n-1} + x^{n-1}$$
$$= (n+1)\,x^{n-1} .$$

Comme $\langle B, x^n \rangle = \langle B, x^n\,\mu \rangle$ d'après (13) le résultat en découle par induction. Q.E.D.

Nous établissons maintenant un énoncé technique essentiel pour la suite. Pour abréger nous notons $\mathcal{M}$ la relation dans $M \times M$ telle que $(m', m) \in \mathcal{M}$ ssi m appartient au support de $m'\,\sigma_x + x\,m' + m'\,x$ et nous étendons $\mathcal{M}$ à une relation $\overline{\mathcal{M}}$ dans $\mathcal{B} \times \mathcal{B}$ en posant $(b', b) \in \overline{\mathcal{M}}$ ssi il existe une bijection α entre les supports des polynômes b' et b telle que pour tout monôme m' ou ait d'une part $(m', m'\alpha) \in \mathcal{M}$ et d'autre part $\langle b', m' \rangle = \langle b, m'\alpha \rangle$.

Propriété 15 : Soient $(m', m) \in \mathcal{M}$. On a $(m'\mu, m\mu - m') \in \overline{\mathcal{M}}$

Preuve : La vérification que $(m' \sigma_z\dagger, m \sigma_z\dagger) \in \overline{\mathcal{M}}$ est facile. Pour le reste, nous distinguons trois cas, et comme le résultat résulte immédiatement de (14) quand m et m' sont des puissances de x nous pouvons supposer que $|m|_z$ est positif.

Cas i : $m = x\, m'$.
Nous pouvons écrire $m' = x^n z\, m''$ $(n \in \mathbb{N}, m'' \in M)$ et comme $m' = x^{-1} m$ il nous suffira de vérifier d'une part $(m' x^{-1}, m x^{-1}) \in \overline{\mathcal{M}}$ ce qui est trivial et d'autre part $(m' \sigma_x\dagger + x^{-1} m', m \sigma_x\dagger) \in \mathcal{M}$.

Soit S l'ensemble des paires (m_1, m_2) telles que $m_1 x x\, m_2 = m$. Le sous ensemble S_1 de celles pour lesquelles $|m_1|_z$ est positif, est en correspondance biunivoque par $m_1 \longrightarrow x^{-1} m_1$ avec l'ensemble correspondant pour m'. En outre l'ensemble $S \setminus S_1$ est formé de n paires $(x^i, x^{n-i-1} z\, m'')$ $(o \leq i \leq n-1)$ ce qui fait que $x^n z\, m''$ a le coefficient n dans $m \sigma_x\dagger$.

On peut donc se limiter au cas de n positif et on vérifie de même que $x^{n-1} z\, m''$ a le coefficient $(n-1) + 1$ dans $m' \sigma_x\dagger + x^{-1} m'$ ce qui établit le résultat dans ce cas.

Cas ii : $m = m' x$.
Le même raisonnement s'applique par symétrie.

Cas iii : $m \neq m' x, x\, m'$.
On peut écrire $m' = m'' z\, x^n z\, m'''$ où z est positif et l'on a $m = m'' z\, x^{n+1} z\, m'''$. Il est clair que $(x^{-1} m' + m' x^{-1}, x^{-1} m + m x^{-1})$ est dans $\overline{\mathcal{M}}$. Comme ci-dessus le sous ensemble $S_1 \subset S$ des paires (m_1, m_2) telles que $m_1 x x\, m_2 = m$ qui satisfont la condition supplémentaire que $|m_1|_z \neq |m''|_z$ est en correspondance biunivoque avec le sous ensemble correspondant pour m'. En ce

392

qui concerne les autres paires elles produisent le mot m' avec la multiplicité n et par conséquent le coefficient de m' dans $m\,\sigma_x\dagger - m'$ est $n-1$. Le mot correspondant $m''\,z\,x^{n-1}\,z\,m''$ a le coefficient $n-1$ dans $m'\,\sigma_x\dagger$ et le résultat est donc établi dans tous les cas. Q.E.D.

(16) Corollaire : Soit $(m', m) \in \mathcal{M}$. On a
$< B, m > = < B, m' > . (|m| + 1)$.

Preuve : Si $|m| = 1$, on a $m = x$ et il existe un seul m' , à savoir 1 tel que $(m', m) \in \mathcal{M}$. Comme $< B, x > = 2$ ainsi qu'on l'a vu dans (14), la formule vérifiée dans ce cas et nous pouvons procéder par induction sur le degré de m .
D'après (13) nous avons
$< B, m> = < B, m\mu >$ et $< B, m' > = < B, m' \mu >$.

De plus d'après (15) $m\,\mu$ est la somme de m' et d'un polynôme b tel que $(m'\,\mu, b) \in \mathcal{M}$. Comme b est homogène de degré $|m|-1$, il en résulte par l'hypothèse d'induction que
$< B, b > = < B, m'\mu > . |m|$. Par conséquent
$< B, m > = < B, m' > + < B, m' \mu > |m|$ où
$< B, m'> = < B, m'\mu >$ ce qui est le résultat cherché. Q.E.D.

Considérons maintenant un mot quelconque $m \in M$. On peut l'écrire sous la forme

$$m = x^{n_o} z^{p_1} x^{1+n_1} z^{p_2} \ldots x^{1+n_{k-1}} z^{p_k} x^{n_k}$$

où les p_i sont positifs et où k et les n_i sont non négatifs.

Désignons par $\hat{m}$ le mot $z^{p_1} x z^{p_2} \ldots x z^{p_k}$ (et par conséquent $\hat{m} = 1$ ssi $m = x^{n_o}$).

(17) Pour tout $m \in M$, on a $< B, m > = < B, \hat{m}> \dfrac{(1 + |m|)!}{(1 + |\hat{m}|)!}$

Preuve : Par induction sur $|m| - |\hat{m}|$ en observant que si $m \neq \hat{m}$, il existe au moins un m_1 tel que $(m_1, m) \in \mathcal{M}$ et que pour tout m_i satisfaisant cette dernière relation on a $\hat{m}_i = \hat{m}$.

Q.E.D.

(18) Quelques soient l'entier n et le polynome homogène a on a $< B, a\, x^n > = < B, a > \dfrac{(|a| + n + 1)!}{(|a| + 1)!} = < B, x^n\, a >$.

Preuve : Ceci résulte immédiatement de (17) et de ce que $\hat{m}_1 = \hat{m}$ pour chaque m_1 de la forme $m\, x^n$ ou $x^n\, m$. Q.E.D.

III.2. Le résultat principal

Définissons d'abord une suite infinie de nombres rationnels (d_k) par la récurrence

(20) $d_o = 1$; $d_{k+1} = (2k+3)^{-1} \sum_{o \leq j \leq k} d_j\, d_{k-j}$.

Nous vérifions d'abord

(21) pour chaque entier positif k et chaque mot $g \in \{1\} \cup M\, x$ on a $< B, g\, z^k > = < B, g\, x^{2k} > d_k$.

Preuve : Le résultat est facilement vérifié pour $|g\, z^k| \leq 2$ et nous pouvons procéder par induction sur le degré.

Considérons d'abord le cas de $g = 1$. On a

$$z^{k+1}\, \mu = z^{k+1}\, \sigma_z \dagger = \sum_{o \leq j \leq k} z^{k-j}\, x\, z^j \quad .$$

D'après l'hypothèse d'induction et (17) on a

$$< B, z^{k-j}\, x\, z^j > = < B, z^{k-j}\, x^{2j+1} > d_j$$

$$= < B, z^{j-j} > d_j\, \frac{(2k+2)!}{(2k-2j+1)!}$$

$$= < B, x^{2k-2j} > d_j\, \frac{(2k+2)!}{(2k-2j+1)!}$$

394

$$= d_{k-j} \cdot d_j\ (2k+2) = (2k+3)^{-1} < B, x^{2k+2} > .$$

Par conséquent nous avons bien

$$< B, z^{k+1} > = <B, x^{2k+2}> \cdot (2k+3)^{-1} \sum_{o \le j \le k} d_j\, d_{k-j} .$$

Supposons maintenant que g soit différent de 1, c'est à dire que $g = f\,x$ $(f \in M)$. On vérifie facilement que $g\,z^{k+1}\,\mu$ est la somme de $b = g\,(z^{k+1}\,\mu)$ et d'un autre polynôme c qui est égal à z^{k+1} si $f = 1$ et à $(f\,\mu)\,x\,z^{k+1}$ si $f \neq 1$.

D'après l'hypothèse d'induction, on trouve que

$$b = < B, g\,x^{2k+1} > \sum_{o \le j \le k} d_j\, d_{k-j}$$

$$= < B, g\,x^{2k+1} > (2k+3)\, d_{k+1} \quad ;$$

D'autre part $c = d_{k+1}$ si $f = 1$ et sinon, utilisant l'hypothèse d'induction et (17), on trouve

$$c = < B, g\,x^{2k+1} > (\,|f| + 1)\, d_{k+1} .$$

Par conséquent dans tous les cas

$$< B, g\,z^{k+1} > = < B, b > + < B, c >$$

$$= < B, g\,x^{2k+1} > (|g| + 2k + 3)\, d_{k+1}$$

ce qui est bien égal à $< B, g\,x^{2k+2} > d_{k+1}$. Q.E.D.

Nous sommes maintenant à même d'énoncer notre résultat principal :

(22) Si $m = x^{n_o} z^{p_1} x^{n+n_1} \ldots z^{p_k} x^{n_k}$

$(p_1, p_2, \ldots, p_k \ge 1)$ on a

$$< B, m > = (1 + |m|.)!\, d_{p_1}\, , d_{p_2} \ldots d_{p_k}$$

Preuve : Pour $k = 0$ ceci est la formule (14). Le cas général s'en déduit par induction sur k au moyen de (22) et (17) . Q.E.D.

On notera que comme tous les coefficients intervenant dans λ sont des entiers non négatifs, il en est de même des coefficients $< B, m >$ des polynômes $b_n = 1\,\lambda^n$ $(n \in \mathbb{N})$ bien que les d_k soient des nombres fractionnaires.

III.3. Relations avec les nombres d'Euler.

Soit Y_o la solution de $y'' = y\,y'$ telle que $Y_o = 0$ pour $t = 0$. Elle est obtenue en faisant $y = 0$ dans les polynômes a_n décrits dans la première section de ce chapitre. Nous noterons a_{on} ces polynômes qui sont donc des polynômes en y'.

En particulier $a_{oo} = 0$ et $a_{o1} = y'$.

Rappelant la formule $a_{n+1} = b_n \varphi \,.\, y'\, 2^{-n}$ utilisée pour définir les polynômes b_n au moyen du morphisme φ envoyant x sur y et z sur $-y^2 + 2y'$, nous aurons $a_{o,n+1} = b_{on} \varphi \,.\, y'\, 2^{-n}$ où $b_{o,n}$ est le polynôme obtenu en faisant $x = 0$ dans b_n. Comme b_n est homogène de degré n et que les degrés de x et z sont respectivement 1 et 2 nous savons que b_{on} est nul pour n impair et qu'il se réduit à $< B, z^k > z^k$ pour $n = 2k$ $(k \in \mathbb{N})$.

De plus, d'après (22) et (17) nous savons que $< B, z^k >$ est égal à $(2k + 1)!\, d_k$.

Il en résulte que $a_{o,n} = 0$ pour n pair et que pour $n = 2k + 1$ on a $a_{o,2k+1} = 2^{-k}\,(2k + 1)!\, d_k\, y'^{k+1}$ et

$$Y_o = \sum_{o \le k} \frac{t^{2k+1}}{(2k+1)!}\, a_{o,2k+1} \quad .$$

Faisons maintenant $y' = 1$ dans Y_o. La série obtenue est la solution de l'équation différentielle (ordinaire) $y'' = y\,y'$

396

qui, pour $t = 0$, prend la valeur 0 cependant que sa dérivée prend la valeur 1, c'est à dire comme il est bien connu, la fonction $tg(t)$. Les nombres $2^{-k}(2k+1)!\, d_k$ en sont les coefficients de Hurwitz; ce sont donc les nombres d'Euler d'indice impair.

IV. UNE AUTRE APPLICATION

IV.1. Nous commençons par un complément aux généralités de I. Considérons un anneau de polynomes (non commutatifs) $\mathcal{A}[u, v, w, \ldots]$ en les variables $u, v, w, \ldots$, son quotient $\mathcal{C}$ par la congruence $u v \equiv v u \equiv 1$ et une dérivation ζ telle que :

(23) $v \zeta = - v (u \zeta) v$.

Remarque : ζ est une dérivation de $\mathcal{C}$.

Preuve : Il suffit de montrer que pour tout $a, b \in \mathcal{A}[u, v, \ldots]$ on a $a u v b \zeta \equiv a v u b \zeta \equiv a b \zeta$.
Calculons $a u v b \zeta$. On a
$a u v b \zeta = (a \zeta) u v b + a u v (b \zeta) + a (u \zeta) v b + a u (v \zeta) b$.

La somme des deux premiers termes est congrue à $(a \zeta) b + a (b\zeta)$ c'est à dire à $a b \zeta$. La somme des deux derniers termes est congrue à 0 puisque
$a u (v \zeta) b = - a u v (u \zeta) v b \equiv - a (u \zeta) b v$.
Un calcul analogue vaut pour $a v u b \zeta$. Q.E.D.

Il résulte de ceci que $(u v) \zeta = (v u) \zeta = 1 \zeta = 0$, donc que $(u v) \zeta^n = (v u) \zeta^n = 0$ pour tout n positif. Or, comme ζ est une dérivation, on a identiquement
$(a b) \zeta^n = \sum_{o \le j \le n} (a \zeta^j) (b \zeta^{n-j}) \begin{bmatrix} n \\ j \end{bmatrix}$ quelque soient a, b et $n \ge 0$.

Divisant par $n!$ on en déduit l'identité

(24) $\sum_{o\le j\le n} \frac{u\,\zeta^j}{j!} \cdot \frac{v\,\zeta^{n-j}}{(n-j)!} = 0$ pour chaque n positif.

Introduisant une nouvelle variable t commutant avec u et v et posant

$$U = \sum_{o\le n} \frac{t^n}{n!} \cdot u\,\zeta^n \quad ; \quad V = \sum_{o\le n} \frac{t^n}{n!} \cdot v\,\zeta^n$$

il en résulte finalement la relation

(25) $U\,V = V\,U = 1$

par identification des coefficients de t^n et (24) .

IV.2. Nous revenons aux notations de II.1. et nous adjoignons à $\bar{\mathcal{A}}(t)$ une nouvelle variable v satisfaisant $y'\,v = v\,y' = 1$ (ce qui entraine $v\,t = t\,v$ puisque $t\,y' = y'\,t$)

En conformité avec (23), nous étendons la dérivation η (définie par $y\,\eta = y'$, $y'\,\eta = y\,y'$) en posant $v\,\eta = -\,v\,(y'\,\eta)\,v$ ce qui donne $v\,\eta = -\,v\,y\,y'\,v = -\,v\,y$.

D'après (25) les deux séries formelles

$$Y' = \sum_{o\le n} \frac{t^n}{n!}\,(y'\,\eta^n) \quad \text{et} \quad V = \sum_{o\le n} \frac{t^n}{n!}\,(v\,\eta^n)$$

sont inverses l'une de l'autre et nous proposons de calculer directement les coefficients $v\,\eta^n$ de V .

Remarque 26 : Pour chaque $n \in \mathbb{N}$ on a

$$2\,v\,\eta^n = v\,(C_n\,\varphi)$$

où les C_n sont des polynomes dans $\bar{\mathcal{B}}$ définis par la récurrence

$$C_o = 2 \quad ; \quad C_{n+1} = \frac{1}{2}\,(C_n\,\sigma - x\,C_n - C_n\,x) = C_n\,\nu.$$

Preuve : C'est essentiellement la même que celle de la remarque 11 dont nous utilisons les notations.

398

Nous avons $v\,\eta^0 = v$ et par conséquent nous pouvons prendre $C_0 = 2 \in \bar{\mathcal{B}}$

Supposons maintenant que $2\,v\,\eta^n = v\,(C_n\,\varphi)$ où $C_n \in \bar{\mathcal{B}}$.

Nous avons :

$$\begin{aligned} 2\,v\,\eta^{n+1} &= (v\,(C_n\,\varphi))\,\eta = v\,\eta\,.\,(C_n\,\varphi) + v\,(C_n\,\varphi\,\eta) \\ &= -\,v\,y\,(C_n\,\varphi) + v\,(C_n\,\varphi\,\psi\,\bar{\eta}\,\varphi) \\ &= -\,v\,x\,\varphi\,(C_n\,\varphi) + v\,(C_n\,\bar{\eta}\,\varphi)\,. \end{aligned}$$

Mettant v en facteur nous obtenons donc $2\,v\,\eta^{n+1} = v\,C_{n+1}$ où $C_{n+1} = -\,x\,C_n + C_n\,\bar{\eta}$ appartient à $\bar{\mathcal{B}}$ par induction.

Il ne reste plus qu'à vérifier que cette équation peut se mettre sous la forme plus simple

$$C_{n+1} = \frac{1}{2}\,(C_n\,\sigma - x\,C_n - C_n\,x) = C_n\,\nu$$

ce qui est facile compte tenu de $\bar{\eta} = \sigma + \rho$ et des propriétés de ρ établies dans la preuve de la remarque 11; Q.E.D.

On trouve pour les premiers termes

$$C_0 = 2\ ;\ C_1 = -\,2\,x\ ;\ C_2 = x^2 - z\ ;\ C_3 = x\,z + z\,x\ ;$$

On a les formules suivantes :

(27) $C_{2k} = (-1)^k\,(z^k - x\,z^{k-1}\,x)$ pour $k \geq 1$;

$C_{2k+1} = (-1)^{k+1}\,(x\,z^k + z^k\,x)$ pour $k \geq 0$.

Preuve : On vérifie directement que $C_1 = -\,2\,x$.

Supposant maintenant que C_{2k+1} a la forme (27), on trouve :

$$\begin{aligned} &2\,(-1)^{k+1}\,C_{2k+2} = 2\,(-1)^{k+1}\,C_{2k+1}\,\nu \\ &= (x^2 + z)\,z^k + z^k\,(x^2 + z) - x^2\,z^k - x\,z^k\,x - x\,z^k\,x - z^k\,x^2 \\ &= 2\,(z^{k+1} - x\,z^k\,x)\,. \end{aligned}$$

De même supposant que C_{2k} $(k \geq 1)$ a la forme (27) on obtient

$$2\,(-1)^k\, C_{2k+1} = 2\,(-1)^k\, C_{2k}\,\nu = -\,(x^2 + z)\, z^{k-1}\, x$$
$$- x\, z^{k-1}\,(x^2 + z) - x\, z^k + x^2\, z^{k-1}\, x - z^k x + x\, z^{k-1}\, x^2$$
$$= -\,2\,(x\, z^k + z^k\, x) \quad .$$

Q.E.D.

Posant $C = \sum_{o \leq n} t^n\, C_n$ les formules précédentes peuvent être résumées par la formule unique

(28) $C = 1 + (t - t\,x)\,(1 + t\,z)^{-1}\,(1 - t\,x)$

où, comme d'usage, $(1 + t\,z)^{-1}$ est une abréviation pour $\sum_{o \leq n} (-1)^n\, t^n\, z^n$ ce qui donnerait facilement l'expression de $\sum_{o \leq n} t^n\,(v\,\eta^n)$ en appliquant le morphisme φ . Il me parait très remarquable que cette dernière fonction se trouve ainsi être une fonction rationnelle en tous ses arguments.

IV.3. Nous terminons en montrant que la fonction V de t est la solution de l'équation différentielle

(29) $V'' = V'\, V^{-1}\, V' - 1$

où $V' = V\,\partial$, $V'' = V'\partial$

et où ∂ est la dérivation de noyau $\overline{\mathcal{B}}$ envoyant t sur 1 qui a été définie et utilisée dans le chapitre I .

Tout d'abord, nous avons par hypothèse $Y'' = Y\,Y'$ d'où $Y''' = Y\,Y'' + Y'^2$ ce qui donne $Y = Y''\,Y'^{-1}$ et $Y''' = Y''\,Y'^{-1}Y'' + Y'^2$ ce qui peut se réécrire

$$Y'^{-1}\,Y'''Y'^{-1} = Y'^{-1}\,Y''\,Y'^{-1}\,Y''\,Y'^{-1} + 1 \ .$$

Maintenant d'après (25) nous avons $V = Y'^{-1}$ d'où d'après (23)

$V' = -\,V\,Y''\,V$ puis $V'' = -\,V'\,Y''\,V - V\,Y'''\,V - V\,Y''\,V'$

$= 2\,V\,Y''\,V\,Y''\,V - V\,Y'''\,V$ ce qui est égal à $V\,Y''\,V\,Y''\,V - 1$ d'après l'expression trouvée plus haut pour

400

$$Y'^{-1}\, Y'''\, Y'^{-1} = V\, Y'''\, V$$

et le résultat s'en déduit en utilisant la relation

$$V\, Y''\, V = -\, V' \quad .$$

Q.E.D.

REFERENCES

[1] D. André. Developpements de Sec x et tang x . C.R. Acad. Sc. Paris 88 (1879) - 965 - 967 .

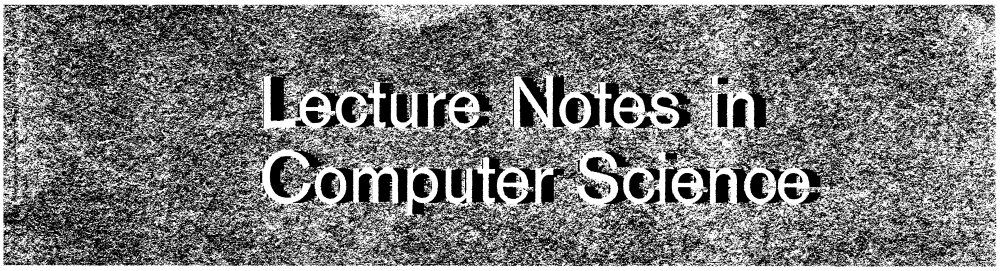
[2] S. Eilenberg. Theory of Automata. (Sous presse)

[3] D. Foata et M. P. Schützenberger. Nombres d'Euler et permutations alternantes. In a Survey of Combinatorial Theory (J. N. Stivastaver Ed) Amsterdam 1973 .

[4] N. Nielsen. Traite élementaire des nombres de Bernovilli. Paris 1923 .

[5] I. Riordan. Combinatorial Identites. N. Y. 1970 .

[6] Wedderburn. Lectures on Matrices. Am. Math. Soc. Colloq. Publi. 17 1934 .



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

33

Automata Theory and Formal Languages 2nd GI Conference

Kaiserslautern, May 1975

Springer-Verlag
Berlin · Heidelberg · New York

SUR LES RELATIONS RATIONNELLES

M.P. Schutzenberger
IRIA

I. Introduction

Nous faisons référence aux chapitres IX et XI du traité de S. Eilenberg ([1]) pour les résultats de base concernant les relations rationnelles $\rho : A^* \to B^*$ entre monoïdes libres et nous appelons une telle relation *fonctionnelle* ssi l'image $a\rho$ de chaque mot a de A^* est vide (=0) ou un singleton. Nous nous proposons d'établir la propriété suivante qui peut être considérée comme une modification d'un résultat banal concernant les séries rationnelles.

Propriété : Si la relation rationnelle $\rho : A^* \to B^*$ n'est pas une somme finie de relations rationnelles fonctionnelles il existe trois mots $a,a',h \in A^*$ tels que $\mathrm{Card}\,((ah^n a')\rho) \geq n+1$ pour chaque $n \in N$.

Dans ce qui suit nous supposerons d'abord la relation ρ donnée par un transducteur au sens de Nivat ([2]), c'est à dire par un morphisme μ de A^* dans le semi-anneau des QxQ matrices à entrées dans Rat(B), où Q est un ensemble d'indice fini, et la règle que pour chaque mot a, la partie $a\rho$ de B^* est certaine entrée fixe(disons, l'entrée (q_-,q_+)) de la matrice $a\mu$. En outre, on peut supposer que cette représentation est *réduite* en ce sens que pour chaque q de Q il existe des mots a,a' de A^* tels que $a\mu\,(q_-,q)$ et $a'\mu\,(q_-,q_+)$ soient non nuls. En effet s'il n'en était pas ainsi on pourrait, sans changer la valeur de ρ, remplacer par 0 les entrées des lignes et colonnes "q" dans toutes les matrices, et par conséquent, omettre q.

Sous cette hypothèse qui sera toujours faite désormais, il est clair que la propriété serait triviale si l'une des entrées de l'une des matrices génératrices $a\mu$ ($a \in A$) était une partie infinie du B^*. Nous supposerons donc aussi que toutes ces

entrées sont des parties *finies* de B^*. Une autre simplification peut encore être faite : comme l'énoncé ne dépend pas du nombre d'éléments de 1ρ (où 1 est comme d'usage l'élément neutre) nous supposerons toujours que $1\rho = 0$ ou $= 1$, ces deux cas correspondant respectivement aux hypothèses que les états distingués q_- et q_+ sont distincts ou confondus.

II. Preuve de la propriété

Nous notons $||X||$ le nombre d'éléments d'un ensemble X quelconque et en particulier nous posons $||Q|| = d$.

Lemme 1. La relation ρ est fonctionnelle ssi $||a\rho|| \leq 1$ pour tous les mots a de longueur $|a|$ du plus égal à $L = 1+2\,d(\,d-1\,)$.

Preuve : Soit a un mot de longueur minimum $|a| = n$ parmi ceux pour lesquels $||a\rho|| \geq 2$. Si l'une des matrices $a'\mu$ ($a' \in A$) a une entrée qui n'est ni vide ni un singleton, l'hypothèse que μ est un transducteur *réduit* implique que $n \leq 1+2(\,d-1\,)$, et le résultat est vérifié dans ce cas. Dans le cas contraire où chaque entrée de chacune des matrices génératrices $a'\mu$ ($a' \in A$) est au plus un singleton, soit $a = a_1 a_2 \ldots a_n$ ($a_i \in A$). Il existe une suite de n-1 paires $(\,q_j, q'_j\,)$ d'indices $(\,1 \leq j \leq n-1, q_j \neq q'_j\,)$ tels que posant $q_0 = q'_0 = q_-$, $q_n = q'_n = q_+$ et $b_j = a_j\mu(\,q_{j-1}, q_j\,)$, $b'_j = a_j\mu(\,q'_{j-1}, q'_j\,)$ $(\,1 \leq j \leq n\,)$ les mots $b = b_1 \ldots b_n$ et $b' = b'_1 \ldots b'_n$ soient deux éléments *distincts* de $a\rho$. Supposons que $n > L$ et montrons que l'hypothèse de minimalité sur $|a| = n$ conduit à une contradiction.

D'après $L = 1 + 2d(\,d-1\,)$ il existe trois indices $i<j<k$ pour lesquels $(\,q_i, q'_i\,) = (\,q_j, q'_j\,) = (\,q_k, q'_k\,)$, ce qui détermine une factorisation $a = f_1 f_2 f_3 f_4$ où $f_1 = a_1 \ldots a_i$; $f_2 = a_{i+1} \ldots a_j$; $f_3 = a_{j+1} \ldots a_k$; $f_4 = a_k \ldots a_n$ et induit de façon évidente les factorisations correspondantes $b = g_1 g_2 g_3 g_4$ et $b' = g'_1 g'_2 g'_3 g'_4$. Par construction on a les inclusions $g_1 g_4, g'_1 g'_4 \in (\,f_1 f_4\,)\rho$ et $g_1 g_x g_4, g'_1 g'_x g'_4 \in (\,f_1 f_x f_4\,)\rho$ (x = 2 ou 3).

En raison du caractère minimal de a, les membres de droite sont des singletons et on a donc les trois équations $g_1 g_4 = g'$ et $g_1 g_x g_4 = g'_1 g'_x g'_4$.

Supposant, par exemple, que $|g_1| \leq |g'_1|$ il en résulte l'existence d'un mot h tel que $g'_1 = g_1 h$ et $g_4 = h g'_4$, d'où en reportant dans les autres équations et en simplifiant, les deux équations $h g_2 = g'_2 h$ et $h g_3 = g'_3 h$.

Il en résulte que

$$b = g_1 g_2 g_3 g_4 = g_1 g_2 g_3 h g'_4 = g_1 g_2 h g'_3 g'_4 = g_1 h g'_2 g'_3 g'_4 = h\, g'_1 g'_2 g'_3 g'_4 = b'$$

en contradiction avec l'hypothèse que b et b' étaient distincts.

Par conséquent $n \leq L$.

Q.E.D.

Nous rappelons maintenant que le *support* $m\beta$ d'une QxQ matrice m est la relation binaire sur Q définie par l'ensemble de ses entrées non vides. Autrement dit, β est un morphisme du monoïde $A^*\mu$ dans un monoïde de relations binaires sur Q. On dit que μ est *irréductible* ssi l'union des relations $a\mu\beta$ ($a \in A^*$) est égale à QxQ lui-même. Nous avons donc le

Corollaire 2. Quand μ est irréductible et que ρ n'est pas fonctionnelle, il existe trois mots a,h,a' tels que $\|(ah^n a')\rho\| \geq n+1$ ($n \in N$).

Preuve : Supposons que $\|a\rho\| \geq 2$, c'est à dire que $\|a\mu(q_-,q_+)\| \geq 2$.

Puisque μ est irréductible il existe un mot a" tel que (q_+,q_-) appartienne au support de la matrice $a"\mu$. Posant $h = a"a$ on a donc que l'entrée (q_-,q_+) de $h\mu$ contient au moins deux mots distincts. Il est trivial que la même entrée de $h^n\mu$ contient donc au moins n+1 mots distincts pour chaque $n \in N$ et l'on a par conséquent $\|(ah^n)\rho\| = \| (ah^n)\mu(q_-,q_+)\| \geq n+1$ identiquement.

Q.E.D.

Par conséquent la propriété est déjà établie dans le cas particulier où le transducteur μ est irréductible. Comme elle l'est trivialement quand le domaine de ρ est fini nous pouvons désormais procéder par induction sur $\|Q\|$ ou plus exactement, sur le nombre total des entrées non nulles des matrices génératrices $a\mu$ ($a \in A$) du monoïde $A^*\mu$.

Avant de passer au cas général nous rappelons que le produit (de concaténation) de deux relations $\rho,\sigma : A^* \to B^*$ est la relation $\pi = \rho\sigma$ telle que pour chaque mot a on ait :

$$a\pi = \Sigma \{ (a'\rho)(a"\rho) : a',a" \in A^* ; a = a'a" \}.$$

Supposons maintenant que μ ne soit pas irréductible. Il existe une partition $Q = Q' \cup Q"$ tel qu'aucun des supports $a\mu\beta$ ne rencontre Q" x Q'. Nous définissons un morphisme μ' par la condition que pour tout $a \in A$, $q,q' \in Q$ on ait :

$$a\mu'(q,q') = a\mu(q,q') \text{ si } q,q' \in Q' ;$$
$$= 0 \text{ sinon ;}$$

et un autre morphisme $\mu"$ par la condition que $\mu = \mu' + \mu"$ et que le support des $a\mu"$ ne rencontre pas Q' x Q'. On vérifie facilement que ρ est la somme étendue à tous les $q \in Q'$ des produits $\rho'_q\rho"_q$ où $\rho'_q = \mu'(q_-,q)$ et $\rho"_q = \mu"(q,q_+)$.

Ces relations sont rationnelles et on peut leur appliquer l'hypothèse d'induction. Donc pour conclure la preuve de la propriété il nous suffit de vérifier le

Lemme 3 : Si le produit $\pi = \rho\rho'$ de deux relations rationnelles fonctionnelles n'est pas une somme finie de telles relations, il existe trois mots pour lesquels $\|(ah^n a')\pi\| \geq n+1$ ($n \in N$).

Preuve : Nous utilisons les bimachines de Eilenberg ([1], chap XI), c'est à dire que nous associons à ρ un morphisme ϕ de A^* dans un monoïde fini M et une application

partielle θ : $M \times A \times M \to B^*$ telle que pour chaque mot $a = a_1 \dots a_n$ ($a_i \in A$) on ait que $a\rho$ est le produit de $i = 1$ à $i = n$ de termes $(m'_i, a_i, m''_i)\theta$ où m'_i (resp. m''_i) est l'image par ϕ du facteur gauche (resp. droit) de longueur $i-1$ (resp. $n-i$) de a. Une construction semblable avec $\phi' : A^* \to M'$ et θ' vaut pour ρ'. De fait, on peut remplacer M et M' par leur produit direct et, ceci fait, supposer simplement que $\phi = \phi'$, les deux bimachines ne diffèrant alors que par leurs fonctions θ et θ'. On peut de plus exprimer ρ comme la somme sur tous les $s \in S$ des relations ρ_s qui sont définies comme la restriction de ρ à $s\phi^{-1}$. Il en est de même pour ρ' et il suffit donc d'établir le lemme sous l'hypothèse supplémentaire que le domaine de ρ est $s\phi^{-1} = D$ et que celui de ρ' est $s'\phi^{-1} = D'$.

Le domaine de $\pi = \rho\rho'$ est donc DD' et l'on a que π est fonctionnelle quand chaque mot de A^* admet au plus une factorisation comme produit d'un mot de D par un mot de D'. Dans le cas contraire, l'ensemble des mots $p \neq 1$ satisfaisant les conditions $s'.p\phi = s'$ et $p\phi.s'' = s''$ est un sous semi groupe non vide P^+ de A^* (engendré par la base P) et chaque mot a de DD' admettant plusieurs factorisations admet une factorisation maximale unique $dp_1p_2 \dots p_nd'$ où $n \geq 1$, $d \in D$, $d' \in D'$ et $p_i, \dots, p_n \in P$.

Nous étendons θ (et θ') à des fonctions de $M \times A^* \times M$ dans B^* par les identités :

$$(t,xy,t')\theta'' = (t,x,y\phi.t')\theta''. (t.x\phi,y,t')\theta''$$

$$(x,y \in A^*, t,t' \in S , \theta'' = \theta \text{ ou } = \theta').$$

Nous notons σ et σ' les relations rationnelles fonctionnelles de domaine P^+ envoyant respectivement chaque $p_i \in P^+$ sur $g_i = (s,p_i,s')\theta$ et $g'_i = (s,p_i,s')\theta'$.

On vérifie alors que $a\rho$ est l'union pour $i = 0,1,\dots,n$ des produits $bg_1g_2\dots g_ig'_{i+1}\dots g'_nb'$ où $b = (1,d,s')\theta$ et $b' = (s,d',1)\theta'$. Ces $n+1$ mots sont les mêmes ssi $g_i = g'_i$ identiquement. Si au contraire $g = p\sigma \neq g' = p\sigma$ (pour un $p \in P$) on voit que les $n+1$ mots de $(ap^na')\rho$, c'est à dire les mots $d\, g^i g'^{n-i}\, d'$, $(0 \leq i \leq n)$ sont tous distincts. Par conséquent les deux alternatives énoncées dans la propriété correspondent respectivement aux deux cas possibles selon que $\sigma \neq \sigma'$ ou $\sigma = \sigma'$. Nous observons maintenant que comme σ et σ' sont fonctionnelles, on a $\sigma = \sigma'$ ssi la relation rationnelle $\sigma + \sigma'$ l'est aussi, ce que l'on peut vérifier au moyen du lemme 1.

Q.E.D.

Remarque : Un examen plus détaillé des morphismes irréductibles permet de trouver des mots (s'il en existe) tels que Card $((ah^na')\rho) \geq 2^n$ ($n \in \mathbb{N}$) et, de vérifier que, sinon, Card $(a\rho)$ est au plus égal à une fonction polynomiale de la longueur des mots a. ("cas polynomial").

Quand $\|a\rho\|$ est bornée, on peut montrer que ρ est la somme d'une relation ayant un domaine fini et de d relations rationnelles fonctionnelles où d est le plus petit entier tel que $a\rho$ contienne d mots distincts de B^* pour une infinité de mots a de A^*.

Donc pour deux relations de ce type, ρ et ρ', on peut décider si l'on a ou non identiquement $a\rho \subset a\rho'$, et même si cette inclusion est vérifiée dans le complément d'une partie finie de A^*. Je présume qu'il en est de même dans le "cas polymial" mais je ne suis pas parvenu à la démontrer.

Références :

[1] S. Eilenberg. Automata languages and Machins vol. A
Academic Press N.Y. 1974.

[2] M. Nivat (1968) Transductions des langages de Chomsky
Annales. Inst. Fourier. XVIII. pp. 335 - 455.

ISTITUTO NAZIONALE DI ALTA MATEMATICA

SYMPOSIA MATHEMATICA

VOLUME XV

(Estratto)

M. P. Schützenberger

SUR CERTAINES OPÉRATIONS DE FERMETURE DANS LES LANGAGES RATIONNELS

"MONOGRAF"
BOLOGNA - 1975

Istituto Nazionale di Alta Matematica
Symposia Mathematica
Volume XV (1975)

SUR CERTAINES OPÉRATIONS DE FERMETURE DANS LES LANGAGES RATIONNELS

M. P. Schützenberger

1. Introduction.

Nous nous proposons d'examiner la possibilité d'engendrer les langages rationnels au sens d'Eilenberg dans un monoïde libre au moyen de diverses opérations plus restreintes que celles qui interviennent dans la théorie classique de Kleene.

Nous dirons qu'une famille de parties d'un semi-groupe S est fermée par les *opérations polynomiales* si elle contient tous les singletons ainsi que l'union et le produit de deux quelconques de ses membres. Ainsi la famille des *parties rationnelles* de S est la plus petite famille de parties de S fermée par les opérations polynomiales et par l'opération unaire $P \to P^+$ envoyant une partie P sur le semi-groupe P^+ qu'elle engendre.

Considérons d'autre part une partie P du semi-groupe S. Il existe un plus petit semi-groupe quotient de S, le *semi-groupe syntactique* Synt (P) de P tel que $P = P\sigma\sigma^{-1}$ où σ est le morphisme de S sur Synt (P). Si Q est une autre partie de S satisfaisant aussi $Q\sigma\sigma^{-1}$, on voit facilement que l'union $P \cup Q$, le complément $P \setminus Q$ de Q dans P et les parties $PQ^{-1} = \{s \in S : Qs \cap P \neq \emptyset\}$ et $Q^{-1}P = \{s \in S : sQ \cap P \, N \, \emptyset\}$ sont les images inverses par σ^{-1} des parties obtenues par les mêmes opérations dans $S\sigma$ à partir de $P\sigma$ et de $Q\sigma$. Réciproquement, quand P est *reconnaissable*, c'est-à-dire, par définition, quand son monoïde syntactique est fini, toute partie P' de S satisfaisant $P'\sigma\sigma^{-1} = P'$ peut être obtenu par les opérations booléennes et les opérations « $^{-1}$ » à partir de P lui-même et des singletons. Comme enfin, les monoïdes syntactiques de $P \cup Q$, $P \setminus Q$ ou PQ se déduisent facilement de ceux de P et de Q, ces remarques motivent la définition d'une famille fermée

(*) I risultati conseguiti in questo lavoro sono stati esposti nella conferenza tenuta il 9 febbraio 1973.

par les *opérations reconnaissables* comme une famille fermée par les opérations polynomiales, la complémentation et les deux opérations « $^{-1}$ ».

La plus petite famille de parties d'un monoïde libre fermée par les opérations reconnaissables est la famille ***Ap*** des langages « counter-free » de McNaughton, appelés ici *apériodiques*. Notre résultat principal (Corollaire IV.3) consiste à faire apparaître ***Ap*** comme la plus petite famille fermée par les opérations polynomiales et contenant le sous-semigroupe P^+ engendré par chacun de ses membres P, sous réserve que P ait la propriété (définie dans les Sections II et III) d'être préfixe et d'avoir un délai de synchronisation *fini*. Cette dernière condition entraîne réciproquement la propriété remarquable que le semigroupe P^+ soit contenu dans la plus petite famille Rec (P) qui contienne P lui-même et qui soit fermée par les opérations reconnaissables (Énoncé II.3).

En outre, une certaine sous-famille de parties préfixes ayant un délai de synchronisation fini permet d'obtenir toutes les parties rationnelles au moyen des opérations polynomiales et d'une opération de substitution dans les parties dont le monoïde syntactique est un groupe. C'est l'opération de G-fermeture qui est l'objet de l'énoncé IV.2.

2. **Constantes.**

Soit T une partie donnée d'un monoïde M. Un élément u de M sera appelé une *constante* pour T ssi l'on a l'implication

$$(C) \qquad m_1 u m_2,\ m_3 u m_4 \in T \Rightarrow m_1 u m_4 \in T$$

quelque soient les éléments m_i $(i = 1, 2, 3, 4)$ de M. Donc en particulier l'ensemble $U(T)$ des constantes pour T contient le *zéro* $W(T)$ de T, c'est-à-dire l'ensemble des éléments w de M pour lesquels l'intersection de T et de MwM est vide. Cette terminologie est expliquée par le fait que u est une constante ssi Qu est au plus un singleton où Q désigne l'ensemble des états de l'automate (déterministe) minimal reconnaissant T. En effet, supposons que Qu contienne deux états distincts q et q'. Ceci équivaut à l'hypothèse qu'il existe deux mots m_1 et m_3 de M tels que les ensembles $(m_1 u)^{-1}T$ et $(m_3 u)^{-1}T$ sont non vides et différents. On peut donc, par exemple, trouver un élément m_4 dans le complément de $(m_2 u)^{-1}T$ dans $(m_1 u)^{-1}T$ et, prenant m_2 quelconque dans $(m_1 u)^{-1}T$, on obtient $m_1 u m_2,\ m_3 u m_4 \in T,\ m_1 u m_4 \notin T$. Dans l'autre direction, supposons que Qu soit un singleton $\{q\}$: D'après la définition des états de l'automate minimal, ceci équivaut

à l'existence d'une partie M_1 non vide de M telle que pour tout $m \in M$ l'ensemble $(mu)^{-1}T$ soit vide ou égal à M_1, ce qui implique finalement que u soit une constante. Q.E.D.

Il résulte immédiatement de cette remarque (ou de la définition) que l'ensemble $U = U(T)$ des constantes est un idéal de M. Une autre observation utile est que quand une constante t appartient à l'ensemble T lui-même toute relation $mtm' \in T$ entraîne que mt et tm' soient dans T: ceci résulte immédiatement de la définition en prenant $m_3 = m$, $m_4 = m'$ et $m_1 = m_2 = 1$ (= l'unité de M) et en observant que la condition (C) est symétrique en les deux paires (m_1, m_2) et (m_3, m_4). Finalement, en posant $S = U \cap T$, et $W = W(T)$, nous notons la formule

$$(SM \cap MS) \setminus W \subset T \,. \tag{1}$$

PREUVE: Soient $s, s' \in T \cap U = S$ et $h, h' \in M$ tels que les produits sh et $h's'$ soient égaux et ne soient pas contenues dans W. Cette dernière condition entraîne l'existence de $m, m' \in M$ tels que $mshm' \in T$. Comme s est une constante, nous déduisons de l'observation faite plus haut que shm' est dans T. Maintenant, $shm' = h's'm'$ où de nouveau s' est une constante. Par la même raison on a $h's' \in T$, ce qui est le résultat cherché. Q.E.D.

Nous considérons maintenant le cas particulier où M est le monoïde libre engendré par l'alphabet A et où $T = P^+$ est le sous-semigroupe engendré par une partie P de A^+ ayant la propriété qu'il existe un entier naturel $\varkappa$ tel que $P^\varkappa$ soit contenu dans U. Le plus petit entier pour lequel ceci est vrai sera appelé le *délai de synchronisation de* P et sera noté $\delta(P)$. Il est naturel de considérer $\delta(P)$ comme infini s'il n'existe aucun entier naturel $\varkappa$ pour lequel $P^\varkappa$ soit contenu dans l'ensemble des constantes pour P^+.

Dans le reste de cette section, nous supposons toujours $T = P^+$ où $\delta(P) = \varkappa$ est fini. Il est clair que l'on pourrait aussi bien prendre $T = P^*$, c'est-à-dire que les constantes pour P^+ ou P^* sont les mêmes.

II.2. L'idéal W de A^* est engendré par l'ensemble V des mots v de $A^* \setminus A^* P^{\varkappa+1} A^*$ tels que $A^* v A^* \cap P^{\varkappa+1}$ est vide.

PREUVE: L'idéal W est engendré en tant que tel d'une part par une partie A_0 de l'alphabet A, qui est certainement contenue dans V et d'autre part, par l'ensemble V' des mots de W de longueur au moins deux dont aucun facteur propre n'est dans W.

Soit ahb $(a, b \in A,\ h \in A^*)$ un tel mot. L'hypothèse $ah, hb \notin W$ équivaut à l'existence de mots m_i tels que $m_1 a h m_2$ et $m_3 h b m_4$ soient

dans T. Donc h n'est pas une constante puisque sinon on aurait $m_1 ahb m_4 \in T$ contrairement à l'hypothèse $ahb \in W$. Il en résulte que h n'a pas de facteur dans P^x. Supposons que ahb appartienne à l'idéal engendré par P^{x+1}, c'est-à-dire que l'on puisse écrire

$$ahb = fprqg \quad \text{où} \quad f, g \in A^*, \quad p, q \in P \quad \text{et} \quad r \in P^*.$$

Comme ahb n'est pas dans $T = P^+$, l'un au moins des deux mots f et g est différent de 1, disons $= g'b$, ce qui entraîne $ah = fprqg'$.

Puisque h n'a pas de facteur (propre ou non) dans P^x, le mot a doit admettre fp comme facteur gauche *propre*. Or ceci est impossible puisque a est une lettre et que p appartient à la partie P de A^+.

Nous avons donc établi que chacun des générateurs $v' = ahb$ de W est contenu dans le complément de $A^*P^{x+1}A^*$.

Comme en outre $A^*v'A^*$ a une intersection vide avec P^{x+1} puisque v' est contenu dans l'idéal W, on a bien vérifié que V est l'union de V' et de la partie A_0 de A. Q.E.D.

Corollaire II.3: Pour toute partie reconnaissable P de A^* ayant un délai de synchronisation fini, le semi-groupe P^+ et le monoïde P^* appartiennent à la plus petite famille $\mathcal{A}$ fermée par les opérations reconnaissables et contenant P.

Preuve: Le semi-groupe P^+ est l'union de $P \cup P^2 \cup \ldots \cup P^{x-1}$ et de P^xP^*. Le premier de ces ensembles est contenu dans $\mathcal{A}$. Il en est de même de $P^xA^* \cap A^*P^x$ et, ainsi qu'on vient de le voir de zéro W de P^+. Par conséquent $\mathcal{A}$ contient $Q = (P^xA^* \cap A^*P^x) \backslash\backslash W$. Comme Q est contenu dans P^+ d'après la formule (1) et que trivialement P^xP^* est contenu dans Q, le résultat est établi. Q.E.D.

Corollaire II.4: Soit P une partie apériodique ayant un délai de synchronisation fini. La partie P^+ est aussi apériodique.

Preuve: Ceci résulte immédiatement du corollaire précédent et de ce que la famille $\mathcal{A}p$ est fermée par les opérations reconnaissables. Q.E.D.

3. Parties et substitutions préfixes.

Rappelons qu'un sous-monoïde P^* d'un monoïde M est dit *unitaire* ssi P^* contient $M^{-1}P^*$, c'est-à-dire, de façon équivalente, ssi P^* est le stabilisateur d'un état dans une représentation de M par des applications d'un ensemble dans lui-même. Pour les sous-monoïdes unitaires, la notion de constante a la propriété remarquable suivante:

III.1. Soit P^* un sous-monoïde unitaire de M. Un élément p de P^* est une constante pour P^* ssi pour tout $m, m' \in M$ la relation $mpm' \in P^*$ entraîne que mp et m' soient dans P^*.

PREUVE: Si $p \in P^*$ est une constante, on a vu que l'inclusion de mpm' dans P^* implique $mp \in P^*$ (et $pm' \in P^*$). L'hypothèse que P^* est unitaire permet alors de déduire $m' \in P^*$ de ce que mpm' et mp sont dans P^*.

Réciproquement, supposons que l'élément p de P^* soit tel que $mpm' \in P^*$ entraîne mp, $m' \in P^*$ et que les éléments m_i de M satisfont $m_1 p m_2$, $m_3 p m_4 \in P^*$. On a $m_1 p$, $m_4 \in P^*$ et la relation désirée $m_1 p m_4 \in P^*$ résulte de ce que P^* est un semi-groupe. Q.E.D.

Quand M est un monoïde libre A^*, on sait qu'un sous-monoïde est unitaire ssi son ensemble générateur minimum P est *préfixe*, c'est-à-dire satisfait la condition $P \cap PA^+ = \emptyset$.

Les parties préfixes ayant un délai de synchronisation fini sont très voisines des « locally parsable codes » de McNaughton et Papper et, des résultats intéressants ont été obtenus récemment à leur sujet par A. Restivo. Nous nous bornons ici à quelques énoncés très simples.

III.2. Pour tout sous-ensemble Q d'une partie préfixe P, on a $\delta(Q) \leqslant \delta(P)$.

PREUVE: Il suffit de montrer que tout mot p qui est une constante pour P^+ et qui appartient à Q^* est une constante pour Q^+.

Supposons que mpm' soit dans Q^*. Comme Q^* est contenu dans P^*, on déduit de III.1 que mp et m' sont dans P^*. Maintenant, comme P est préfixe, chaque mot de A^* admet au plus une factorisation en produit de mots de P. Donc, puisque Q est un sous-ensemble de P, l'hypothèse $mpm' \in Q^*$ implique que tous les facteurs dans P de la factorisation de mpm' soient en réalité des mots de Q et par conséquent que les mots mp et m' soient dans Q^*, ce qui achève la preuve d'après (III.1) et le fait que Q est préfixe en tant que sous-ensemble de la partie préfixe P. Q.E.D.

EXEMPLE III.3: Soit B une partie d'un alphabet A et Q une partie de $P = B^*(A \setminus B)$. Q est une partie préfixe telle que $\delta(Q) \leqslant 1$ et l'on a $\delta(Q) = 0$ quand Q est contenu dans $A \setminus B$.

PREUVE: Il est clair que le semi-groupe P^+ est égal à l'idéal à gauche $A^*(A \setminus B)$ de A^*. Donc $\delta(P) = 1$. Comme P est préfixe, Q est préfixe en tant que partie de P et $\delta(Q) \leqslant 1$ résulte de III.2.

Quand $Q = A \setminus B$, on a $\delta(Q) = 0$ puisque, trivialement, tout mot m de A^* appartient à $(A \setminus B)^*$ ssi il ne contient aucune lettre dans B, ce qui est équivalent à $mA^* \cap (A \setminus B)^* \neq \emptyset$. Q.E.D.

Rappelons qu'une *substitution* α d'un monoïde M dans un autre, M' est simplement un morphisme de M dans le monoïde des parties de M'. Une substitution α sera dite *complète* ssi le zéro $W(M\alpha)$ dans M' de l'image par α de M est vide.

Dans le cas où $M = A^*$ et $M' = B^*$ sont deux monoïdes libres, nous dirons que α est *injective* ssi, d'une part, les images par α de deux lettres distinctes de l'alphabet A sont des parties disjointes de B^* et, d'autre part, l'ensemble $A\alpha$ engendre librement le sous-monoïde $A^*\alpha$.

On vérifie facilement que si $\alpha: A^* \to B^*$ et $\beta: B^* \to C^*$ sont deux substitutions complètes ou injectives, il en est encore de même de la substitution produit $\alpha\beta: A^* \to C^*$.

Reprenant les notations de l'exemple précédent, on voit sans peine que si X est un ensemble et ξ une surjection de P sur X, l'application inverse ξ^{-1} de X dans les parties de A^* se prolonge de façon unique en une substitution dans A^* du monoïde libre X^* et que cette dernière est à la fois *complète* et *non ambigue*.

Appelons, pour abréger, substitution *préfixe* (resp. ayant un délai de synchronisation fini) toute substitution non ambigue, telle que l'image de l'alphabet soit une partie préfixe (resp. ayant un délai de synchronisation fini).

III.4. Le produit (de composition) de deux substitutions préfixes ayant un délai de synchronisation fini est encore une substitution du même type.

Preuve: Il suffit de considérer une substitution préfixe $\alpha: A^* \to B^*$ telle que $\delta(A\alpha) = \varkappa$ soit fini et de montrer que si P est une partie préfixe de A^* et p une constante pour P^+, tout mot de la forme qr où $q \in (A\alpha)^\varkappa$ et $r \in p\alpha$ est encore une constante pour $R^+ = P^+\alpha$.

Supposons donc que $mqrm' \in R^*$. Comme R^* est contenu dans $A^*\alpha$ et que q est une constante pour le monoïde unitaire, on a $mq, rm' \in A^*\alpha$. Utilisant une deuxième fois de caractère unitaire de $A^*\alpha$, on déduit $m' \in A^*\alpha$ de $r, rm' \in A^*\alpha$. On peut donc trouver des mots $a = mq\alpha^{-1}$ et $a' = m'\alpha^{-1}$ et l'on a $(mqrm')\alpha^{-1} = apa' \in P^*$, puisque α est injectif et que $R^* = P^*\alpha$.

Maintenant comme p est une constante et P^* unitaire, les deux mots ap et a' sont dans P^* et prenant leurs images par α on obtient le résultat désiré que $m \in ap\alpha$ et $m' \in a'\alpha$ sont dans R^*. Q.E.D.

On a donc dans les conditions de l'énoncé $\delta(P\alpha) \leqslant \delta(P) + \delta(A\alpha)$. Quand on ne suppose pas que la substitution non ambigue α est préfixe, on obtient une inégalité semblable avec $2\delta(A\alpha)$ au lieu de $\delta(A\alpha)$.

4. Fin de la preuve.

Nous obtiendrons le résultat annoncé comme corollaire d'une propriété plus générale qui utilise une nouvelle opération de fermeture. Cette dernière serait triviale dans le cas apériodique.

Soit maintenant un groupe fini G et un alphabet fini A. Nous appelons *G-fermeture élémentaire* la plus petite famille $\mathcal{F}_A$ de parties de A^* qui soit fermée par les opérations polynomiales et qui contienne toutes les parties de la forme $g\gamma^{-1}$ où $g \in G$ et où γ est un morphisme dans G du monoïde libre engendré par une partie de l'alphabet A.

Ceci fait, la *G-fermeture* $\mathcal{F}$ est obtenu en fermant $\mathcal{F}_A$ par rapport aux substitutions $\alpha: X^* \to A^*$ où X est un alphabet fini et où il existe une partition $A = B \dot{+} C$ telle que α soit une substitution complète non ambigue pour laquelle l'image de chaque lettre x est de la forme Pc avec $c \in C$ et $P \in \mathcal{F}_B$.

En utilisant par exemple la théorie de la décomposition de J. Rhodes, on peut montrer que tout groupe dans le monoïde syntactique d'un membre de la G-fermeture est diviseur d'un produit direct de copies de G. Nous n'aurons pas besoin de ce résultat. Nous établirons par contre un énoncé fondamental dû à Krohn et Rhodes. Dans celui-ci F est une partie reconnaissable F de A^*. Nous désignons par σ le morphisme de A^* sur le monoïde syntactique $\bar{S}$ de F et par S l'image par σ du semi-groupe A^+. Par conséquent, le monoïde syntactique $\bar{S}$ est égal à S ou à $1 \dot{+} S$, selon que 1 est ou non dans S.

Lemme de Krohn et Rhodes.

Trois cas seulement sont possibles:

(1) S est un semi-groupe £-simple;

(2) S est cyclique;

(3) Il existe une partition $A = B \dot{+} C$ de l'alphabet telle que les semigroupes $(B^*C)^+\sigma$ et $B^+\sigma$ soient des parties propres de S.

PREUVE: Supposons d'abord que le sous-ensemble D des lettres d de A pour lesquelles 1 est contenu dans $(A^*dA^*)\sigma$. Puisque S est fini, $D^+\sigma$ est un groupe et nous sommes dans le cas (1) quand $D = A$, puisque tout groupe est £-simple en tant que semi-groupe. Quand D

est différent de A, nous sommes dans le cas (3) en prenant $B =: D$, $C =: A \setminus D$ puisque l'idéal $(A^*CA^*)\sigma$ ne contient pas l'élément 1 qui était contenu dans S. On peut donc supposer désormais que D est vide, c'est-à-dire que 1 n'appartient pas à S.

Puisque S est fini, il existe au moins une lettre b_1 de A telle que l'idéal à gauche $K =: (A^*b_1)\sigma =: \bar{S}(b_1\sigma)$ de $\bar{S}$ soit maximal parmi les idéaux de la même forme. Notons L l'ensemble des éléments de S qui engendrent K et posons $B =: A \cap L\alpha^{-1}$. Si $B^+\alpha$ est différent de S, nous sommes dans le cas (3) puisque d'après le caractère maximal de K, L n'est pas contenu dans l'idéal $A^*(A \setminus B)A^*$.

On peut donc supposer désormais que $B^+\alpha$ est égal à S. Si L se réduit à un singleton s, nous avons a fortiori $B\sigma =: s$ et S est le semi-groupe cyclique s^+, c'est-à-dire que nous sommes dans le cas (2). Nous pouvons donc supposer que L contient deux éléments distincts s et s'. Comme L est une $\mathfrak{L}$-classe, il existe au moins un $t \in \bar{S}$ tel que $ts =: s'$ et l'on a $t \neq 1$ puisque $s \neq s'$. En raison de l'hypothèse $S =: B^+\alpha = L^+$, nous avons donc $t \in L^+$.

Maintenant, *puisque S est fini*, t ne peut pas appartenir à l'idéal bilatère de $\bar{S}$ complément de L dans S, et par conséquent il appartient à L qui satisfait donc la condition

$$s, s' \in L \Rightarrow s' \in sL$$

qui définit les semi-groupes $\mathfrak{L}$-simples. On en conclut que $L =: L^+$ et enfin que $S =: L^+$ est $\mathfrak{L}$-simple. Q.E.D.

IV.2. Soit F une partie reconnaissable de A^* et soit $\bar{G}$ le plus petit groupe dont tous les groupes dans le monoïde syntactique de F sont des diviseurs. Alors F appartient à la $\bar{G}$-famille $\mathfrak{F}$ de A.

Preuve: L'énoncé est trivial si $F =: \{1\}$. Comme les groupes dans les monoïdes syntactiques de F et de $F \cap A^+$ sont les mêmes on peut désormais supposer que F est contenue dans le semi-groupe A^+.

Nous considérons successivement chacun des cas du lemme de Krohn et Rhodes. Comme $\mathfrak{F}$ est fermée par union, il suffit à chaque fois détablir le résultat quand F est l'image inverse d'un singleton $\{s\}$.

(1) S est union disjointe de groupes G_i tous isomorphes à $\bar{G}$ et satisfaisant identiquement $G_iG_i =: G_i$. Donc $s\sigma^{-1}$ est union finie de termes de la forme $a(g\varrho^{-1})$ où a est une lettre, g est un élément de $\bar{G}$ et ϱ un morphisme de A^* dans $\bar{G}$. Comme $\mathfrak{F}$ contient les parties de A et est fermée par produit, il suffit de vérifier, ce qui est facile, que chacun des $g\varrho^{-1}$ appartient à $\mathfrak{F}$.

(2) Il existe un élément t de S et des entiers positifs tels que $S = \{t^j : 1 \leqslant j \leqslant p + q - 1\}$ avec en outre $t^j = t^j(t^p)^*$ pour tout j au moins égal à $q-1$. Le groupe $\bar{G}$ est le groupe cyclique d'ordre p. Notant A_u l'intersection avec l'alphabet A de l'image inverse d'un élément quelconque u de S, on vérifie facilement que $s\sigma^{-1}$ est soit un polynôme en les A_u si $s = t^j$ et $j \leqslant q-1$, soit le produit d'un polynôme de ce type par le monoïde $(A^p)^*$. Dans ce dernier cas, on a encore que $(A^p)^*$ appartient à $\mathcal{F}$. Comme cette famille est fermée par les opérations polynomiales, le résultat est encore vérifié.

Comme le cas (1) couvre celui où S est réduit à un singleton, nous pouvons désormais procéder par induction sur le nombre des éléments de S.

(3) En raison de l'identité $A^* = (B^*C)^*B^*$, l'image inverse de chaque élément de S est une union finie disjointe des produits (non ambigus) de la forme $F'F''$ où F' et F'' sont soit 1 soit respectivement de la forme $(B^*C)^+ \cap s\sigma^{-1}$ ou $B^+ \cap s\sigma^{-1}$ avec s dans $(B^*C)^+\sigma = S'$ ou dans $B^+\sigma = S''$. D'après l'hypothèse d'induction on a $F'' \in \mathcal{F}$. Introduisons maintenant un alphabet fini X et une bijections σ' de X sur $(B^*C)\sigma$. Celle-ci s'étend à un morphisme σ' de X^+ sur $(B^*C)^+$.

Définissons une substitution α de X^* dans A^* en posant $x\alpha = x\sigma'\sigma^{-1} \cap B^*C$ pour chaque lettre x de X. Par construction $x\alpha$ est une union finie disjointe de termes de la forme $F''c$ où $c \in C$ et où F'' est 1 ou l'intersection avec B^+ de l'image inverse par σ^{-1} d'un élément de S''. On vient de voir que ces parties sont dans $\mathcal{F}$. La substitution α est du type voulu et d'après l'hypothèse d'induction, F' est l'image par α d'une partie appartenant à la G-famille de X. Q.E.D.

Corollaire IV.3: La famille $\boldsymbol{Ap}$ des parties apériodiques est la plus petite famille $\mathcal{A}$ fermée par les opérations polynomiales et par l'opération unaire $P \to P^+$ restreinte aux parties préfixes $P \in \mathcal{A}$ ayant un délai de synchronisation fini.

Preuve: L'inclusion de $\mathcal{A}$ dans $\boldsymbol{Ap}$ résulte immédiatement du dernier corollaire de la Section II. L'inclusion opposée résulte de l'énoncé précédent. Q.E.D.

Testo pervenuto il 23 marzo 1973.
Bozze licenziate il 2 dicembre 1974.

analyse appliquée et informatique

journées de combinatoire et informatique

4, 5, 6 juin 1975

jean-claude bermond et **robert cori** éditeurs

bordeaux 1

uer de mathématique & informatique

cnrs

équipe du laboratoire associé 226

QUELQUES REMARQUES SUR UNE PROPRIETE D'EQUIDISTRIBUTION DES PERMUTATION

Dominique FOATA
Université de Strasbourg(1)

Marcel Paul SCHUTZENBERGER
Université de Paris VII(2)

Cette brève communication a pour but de signaler un phénomène assez curieux concernant la distributions de certains éléments remarquables sur l'ensemble S des permutations d'une chaîne standard $[n] = \{1<2<\ldots<n\}$ fixée.

(1) Département de Mathématiques - 7, rue René Descartes - 67084 Strasbourg

(2) Département de Mathématiques - 2, Place Jussieu , Tour 45 p. 518, 75005 Paris.

1. Pour décrire ceux ci nous notons chaque application f de $[n]$ comme le mot $1f.\ 2f.\ \ldots\ nf$ et nous appelons <u>forme</u> de f la suite des relations $\geq$ ou $<$ satisfaites par les valeurs successives. Par exemple la forme de $f = 4122652$ est $(\geq < \geq < \geq\geq)$. Les pics de f sont les positions $j \geq 2$ telle s que $(j-1)f < jf \geq (j+1)f$ pour $j \leq n-1$ et la position $j = n$ si $(n-1)f < nf$. Dans l'exemple ci-dessus les pics sont 3 et 5. Enfin chaque forme définit une partition ordonnée unique $I = \{I_i, \ldots, I_h\}$ de $[n]$ en intervalles consécutifs par la condition que les pics soient les premiers éléments de chaque composant I_i $(i \geq 2)$. Pour la forme de f ci-dessus cette partition est $\{1,2\}$, $\{3,4\}$ $\{5,6,7\}$; pour la forme (sur $[9]$) définie par $(< \geq \geq \geq < \geq <)$ la partition serait $(\{13\},\{2,3,4,5,6\},\{7,8\},\{9\})$ tout comme pour la forme définie par $(< \geq < < < < \geq <)$.

D'autre part nous appelons <u>avance</u> d'une permutation toute position i telle que $i < (i\ s + 1)\ s^{-1}$, c'est-à-dire toute position telle que le successeur (immédiat) de la valeur qu'elle porte soit à sa droite. Par exemple les avances des permutations $s = \underline{5}\ 9\ \underline{3}\ 2\ 1\ \underline{4}\ \underline{7}\ 6\ 8$ et $s' = \underline{7}\ \underline{8}\ \underline{4}\ 3\ \underline{1}\ 9\ 2\ 5$ sont les positions soulignées, c'est-à-dire respectivement $Av\ (s) = \{1,3,5\}$ et $Av\ (s') = \{1,2,3,5\}$.

Nous noterons $Av^{-1}(X)$ l'ensemble des permutations dont l'ensemble des avances est une partie donnée X de $[n]$.

Enfin, étant donné l'ensemble F des permutations ayant une forme donnée et $I = I(F) = \{I_i, \ldots, I_h\}$, la partition associée de $[n]$ définie par les pics, nous noterons $|I \cap X|$ pour chaque partie X de $[n]$ le vecteur $(m_1, m_2, \ldots, m_h)$ où $m_j = |I_j \cap X|$ $(= \text{Card}\ (I_j \cap X))$ pour $j = 1,2,\ldots h$.

THEOREME 1 : Soit F l'ensemble des permutations de S ayant une forme donnée. Si deux parties X et Y de $[n]$ sont telles que $|I \cap X| = |I \cap Y|$ on a $\text{Card}\ \{F \cap Av^{-1}X\} = \text{Card}\ \{F \cap Av^{-1}\ Y\}$.

Autrement dit, le nombre des permutations (de la forme donnée) dont l'ensemble des avances est une partie quelconque X de $[n]$ <u>ne dépend que</u> du vecteur $|I \cap X|$. Pour prendre un exemple simple, considérons la forme sur $[5]$ définie par $(< \geq < \geq)$. La partition correspondante est $(\{1\},\{2,3\},\{4,5\})$.

Il existe 2 permutations pour lesquelles Av s se réduit à $\{1\}$, 6 pour lesquelles Av s = $\{1,2\}$, 6 aussi pour lesquelles Av (x) = $\{1,3\}$ et enfin 2 pour lesquelles A (x) = $\{1,2,3\}$. Ce qui correspond aux trois vecteurs $|I \cap X|$ = (1, 0, 0), (1, 1, 0), et (1, 2, 0) qui sont les seuls ici dont l'ensemble de permutations correspondant ne soit pas vide.

Notre preuve est passablement compliquée. Pour en donner une idée, appelons codage de Lehmer l'application L associant à chaque permutation s l'applications t = sL de $[n]$ dans $\mathbb{N}$ telle que pour chaque $j = 1, 2, \ldots, n$ on ait $j\,t = \text{Card}\{i < j : is < js\}$. Par construction t = sL est non décroissante et a la même forme que s.

Soit I M A (s) l'ensemble des valeurs positives distinctes de sL. D. Dumont auquel revient le mérite d'avoir songé a considérer ce paramètre, a montré que $|I\,M\,A\,(s)|$ est distribué (sur S) comme le nombre des descentes. Indépendamment de ce résultat, on peut vérifier de façon assez simple que pour une forme donnée les ensembles I M A (s) suivent les mêmes loi déquipartition que celle formulée dans le Théorème 1 pour les ensembles Av (s). Ceci dit il ne reste plus qu'à trouver une bijection V de F sur lui même telle que I M A (sV) = Av (s) identiquement. Ce qui est faisable mais plutôt long.

De fait le Théorème 1 ne semble dire toute la vérité. A chaque permutation $s = s_1\, s_2 \ldots s_n$ on peut associer son dual $\bar{s} = \bar{s}_n\, \bar{s}_{n-1} \ldots \bar{s}_2\, \bar{s}_1$ où $\bar{s}_i = n+1 - s_i$ $(i = 1, 2, \ldots n)$ dont la forme est la forme duale de celle de s. On voit aisément que si j est une avance de s, c'est-à-dire si $j < (j\,s+1)\,s^{-1} = j'$, la positions $\bar{j}' = n+1 - j'$ est une avance de $\bar{s}$.

Par exemple prenant $s = \underline{5}\ 9\ \underline{3}\ 2\ 1\ \bar{\underline{4}}\ \underline{7}\ \bar{6}\ \bar{8}$ on obtient $\bar{s} = \underline{2}\ \underline{4}\ \bar{\underline{3}}\ \underline{6}\ 9\ 8\ \bar{\underline{7}}\ 1\ \bar{5}$ dont les avances sont (1, 2, 4) = (10-9, 10-8, 10-6).

On a donc une dualité complète entre s et $\bar{s}$ par rapport à la forme et aux avances. Nous avons observé sans avoir pu jusqu'ici le prouver que si $\bar{I}$ est la partition de $[n]$ définie par la forme duale de F on a la propriété suivante

Conjecture 2 : Soit F l'ensemble des permutations ayant une forme données.

Si les parties X, X', Y, Y' de $[n]$ sont telles que $|I \cap X| = |I \cap Y|$ et $|\bar{I} \cap X'| = |\bar{I} \cap Y'|$ on a

$$\text{Card}\{s \in F : \text{Av}\, s = X, \text{Av}\, \bar{s} = X'\} = \text{Card}\{s \in F : \text{Av}\, s = Y, \text{Av}\, \bar{s} = Y'\}.$$

Si ceci est vrai, comme nous en sommes persuadés, on aurait ce résultat remarquables que les avances de s et de $\bar{s}$ sont en un certain sens distribués de façon indépendantes. Nous comptons revenir ultérieurement sur cette conjecture.

Table des matières

Tome VIII

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 8 : 1971 – 1975

Ce tome contient de nombreux articles consacrés à des problèmes combinatoires. L'article « On the principle of equivalence of Sparre Andersen » se veut une algébrisation dudit principe, bien connu dans l'étude probabiliste des fluctuations de variables aléatoires.
On trouve dans ce tome, à la fois l'article « Nombres d'Euler et permutations alternantes » et le mémoire complet. Les deux notes « Sur un théorème de G. de B. Robinson » et « Sur une construction de Gilbert de B. Robinson » constituent la genèse d'une longue étude sur l'algèbre des tableaux de Young, déjà abordée dans l'article antérieur « Quelques remarques sur une construction de Schensted » (voir tome 5). Dans ces deux notes, on trouve une première formulation des propriétés de l'opération « évacuation » des tableaux, une opération qui s'avèrera fondamentale dans le traitement du monoïde plaxique (voir les articles « Evacuations » et « La correspondance de Robinson », tome 9).
On trouve aussi, dans ce tome, des travaux sur les langages formels. L'article « Sur les monoïdes finis dont les groupes sont commutatifs » donne deux caractérisations de la variété des ensembles dont le monoïde syntaxique ne contient que des groupes commutatifs. Cet article, ainsi que plusieurs autres de cette période, fut écrit pendant le séjour que Schützenberger fit à Naples en 1972–73 sur invitation d'Eduardo Caianiello, au Laboratorio di Cibernetica.