JOURNAL OF COMBINATORIAL THEORY **8**, 361–375 (1970)

Réarrangements de Fonctions et Dénombrement

DOMINIQUE FOATA ET AIMÉ FUCHS

Université de Montréal, Canada et Institut de Recherche Mathématique Avancée, Université de Strasbourg, France

Communicated by Gian-Carlo Rota

Received October, 1968

RÉSUMÉ

On donne l'énoncé d'un théorème sur les réarrangements d'applications d'un ensemble fini dans lui-même, qui généralise un résultat connu sur les permutations, et qui permet de retrouver le dénombrement des classes d'applications ultimement idempotentes et indécomposables, ainsi que celui des arbres de n sommets et des graphes connexes de n arêtes et n sommets.

1. INTRODUCTION

L'objet de cet article est de démontrer le théorème 1.1 suivant ainsi que les propriétés (1.5) à (1.8) ci-dessous, et d'en donner des applications combinatoires et probabilistes.

(1.1) THÉORÈME. *Soient* $[n] = \{1, 2, \ldots, n\}$ *et* F_n *l'ensemble de toutes les applications de* $[n]$ *dans lui-même; pour* $x, y \in [n]$ *et* $f \in F_n$, *on pose*

$$\begin{aligned} \nu_{x,y}(f) &= 1 \text{ si } f(x) = y \text{ et} \\ &\qquad x \in f([n]) \\ &= 0 \text{ sinon.} \end{aligned} \tag{1.2}$$

De même,

$$\begin{aligned} \xi_{x,y}(f) &= 1 \text{ s'il existe } z \in [n-1] \text{ tel que } f(z) = y, \\ &\qquad f(z+1) = x \text{ et} \\ &\qquad f(w) \neq x, \text{ pour tout } w = 1, 2, \ldots, z \\ &= 0 \text{ sinon.} \end{aligned} \tag{1.3}$$

Alors, on peut construire une permutation ϕ de F_n telle que

1) $v_{x,y} = \xi_{x,y} \circ \phi$ *pour* $1 \leqslant x < y \leqslant n$,

2) *si* $\phi(f) = g$, *la suite* $(g(1), g(2), \ldots, g(n))$ *est un réarrangement de la suite* $(f(1), f(2), \ldots, f(n))$.

La propriété 2) ci-dessus implique que ϕ envoie le groupe S_n des permutations de $[n]$ sur lui-même. Or si f est dans S_n, les conditions (1.2) et (1.3) sont toujours remplies (en désignant par z l'unique entier tel que $1 \leqslant z < n$ et $f(z+1) = x$) et en ne prenant que la restriction de ϕ à S_n, on retrouve un résultat connu sur les permutations (voir [2, Théorème 4.11]).

Maintenant si f est dans F_n, désignons par $m(f)$ le plus grand entier m tel que tous les termes de la suite $(f(1), f(2), \ldots, f(m))$ soient distincts. On a évidemment $1 \leqslant m(f) \leqslant n$ et l'on pose

$$\sigma_f = (f(1), f(2), \ldots, f(m(f))). \tag{1.4}$$

De même, notons R_f l'ensemble des éléments $x \in [n]$ tels que $f^j(x) = x$ pour un certain entier $j \geqslant 1$ et $\beta(R_f)$ la suite croissante formée par les éléments de R_f.

Considérons de plus les classes $A_n = \{f \in F_n : f^n = f^{n-1}\}$ des fonctions *ultimement idempotentes* et B_n des fonctions *indécomposables* (cf. [4]), c'est-à-dire des fonctions $f \in F_n$ telle que la restriction de f à R_f soit une permutation circulaire. On aura aussi les propriétés suivantes:

(1.5) *La suite* $\sigma_{\phi(f)}$ *est un réarrangement de la suite* $\beta(R_f)$, *donc en particulier*

$$m(\phi(f)) = \text{card } R_f . \tag{1.6}$$

(1.7) *On a* $\sigma_{\phi(f)} = \beta(R_f)$ *si et seulement si* f *est ultimement idempotente.*

(1.8) *La suite* $\sigma_{\phi(f)}$ *débute par son plus grand terme si et seulement si* f *est indécomposable.*

Ces propriétés permettent de retrouver le dénombrement des ensembles A_n, B_n et de l'ensemble $G_{n,d}$ des graphes connexes de n sommets et d arêtes pour $d = n - 1$ et $d = n$. L'ensemble $G_{n,n-1}$ est l'ensemble des *arbres* de n sommets (voir [1, p. 149]). Le dénombrement de $G_{n,n-1}$ remonte à Cayley [3]. On a card $G_{n,n-1} = n^{n-2}$. Notons $H_{n-2,n}$ l'ensemble des suites de longueur $(n-2)$ dont les termes sont pris dans $[n]$. On connait jusqu'alors la construction de deux bijections $\psi : G_{n,n-1} \to H_{n-2,n}$, celle de Prüfer [6], et de Neville [5]. Les propriétés ci-dessus nous fourniront la construction d'une nouvelle bijection $\psi : G_{n,n-1} \to H_{n-2,n}$. De même, on

retrouvera les résultats de Katz [4], et Rényi [7], sur le dénombrement des ensembles B_n et $G_{n,n}$.

Enfin, le théorème 1.1 a l'interprétation probabiliste que voici et que nous décrirons en termes de jeu de dé. Supposons que l'on jette six fois un dé et que l'on désigne par $Y_1, Y_2, \ldots, Y_6$ la suite des numéros sortis. Pour $1 \leqslant i \leqslant 6$, notons T_i le premier instant où l'on observe la face i; si celle-ci ne sort pas au cours des six jets, on pose $T_i = 7$. Le théorème 1.1 nous permet alors de dire

(1.9) *Le nombre aléatoire v^* d'indices i tels que $1 \leqslant T_i \leqslant 6$ et $Y_i > i$, ainsi que le nombre aléatoire ξ^* d'indices i tels que $1 < T_i \leqslant 6$ et et $Y_{T_i - 1} > i$ ont même distribution.*

La section 2 est un bref rappel sur les cycles des fonctions f de F_n et leurs propriétés. Dans la section 3, nous introduisons la Z-décomposition, utile pour démontrer la bijectivité de ϕ. Dans la section 4, nous donnons la construction de la restriction de ϕ à S_n et dans la section 5, la construction de ϕ dans le cas général. La section 6 est consacrée aux diverses applications combinatoires et probabilistes signalées plus haut.

2. Cycles d'Une Fonction

Si f est dans F_n, on pose $f^0(x) = x$ et $f^k(x) = f(f^{k-1}(x))$ pour $k > 0$ et $x \in [n]$. Un *cycle* de f est une suite d'éléments distincts de la forme $(x, f(x), \ldots, f^{j-1}(x))$ où $j \geqslant 1$ et $f^j(x) = x$. L'ensemble R_f a été précédemment défini (après la formule (1.4)); en empruntant la terminologie à la théorie des chaînes de Markov, on dit que R_f est l'ensemble des éléments *récurrents* (pour f). Soit $x \in [n]$; la suite des $(n+1)$ termes $(x, f(x), \ldots, f^n(x))$ contient nécessairement deux termes égaux, donc une sous-suite $(f^i(x), f^{i+1}(x), \ldots, f^{i+j-1}(x))$ qui soit un cycle avec $0 \leqslant i < n$ et $0 < j \leqslant n - i$. Ceci implique que l'on a

$$f^{n-1}([n]) = R_f \tag{2.1}$$

et que R_f n'est jamais vide. Il est clair que x est élément d'un cycle si et seulement s'il est récurrent et si tel est le cas, $f(x)$ est aussi récurrent et il existe un élément récurrent y tel que $f(y) = x$. Par conséquent, la restriction de f à l'ensemble R_f est une permutation de R_f notée π_f. Les cycles de f sont les cycles (au sens de la théorie élémentaire du groupe des permutations) de π_f. Deux cycles sont ainsi, ou confondus, ou disjoints. On dit qu'un cycle $(x, f(x), \ldots, f^{k-1}(x))$ est *isolé* si $f(y) = f^l(x)$ entraîne $l \geqslant 1$ et $y = f^{l-1}(x)$. L'ensemble $[n] \setminus f([n])$ des *valeurs non prises* par f

est noté Z_f. Notons que l'on a $R_f \cap Z_f = \emptyset$ et que si Z_f est vide, f est une permutation de $[n]$ et l'on écrit $f \in S_n$. Le lemme suivant sera utilisé pour la construction de la permutation ϕ.

(2.2) LEMME. *Soient $x \in [n]$ et $f \in F_n \setminus S_n$; si x n'est pas élément d'un cycle isolé de f, on a $f^m(z) = x$ pour un certain $m \geqslant 0$ et $z \in Z_f$.*

PREUVE: Supposons d'abord x non récurrent. S'il n'est pas dans Z_f, il existe $x_1 \neq x$ tel que $f(x_1) = x$. De plus, comme x est non récurrent, x_1 l'est aussi. Par ce procédé, on peut donc construire une suite $(x_0, x_1, x_2, \ldots)$ d'éléments non récurrents tels que $x_0 = x$ et $f(x_i) = x_{i-1}$ pour tout $i \geqslant 1$. Ces éléments étant tous distincts, la suite est nécessairement finie et il existe un indice $m \geqslant 0$ tel que $f(y) \neq x_m$ pour tout $y \in [n]$, c'est-à-dire $x_m \in Z_f$ et $f^m(x_m) = x_0$.

Maintenant si x est récurrent, il existe $x_0 \in [n]$ et un entier $k \geqslant 1$ tels que $f(x_0) = f^k(x)$ et $x_0 \neq f^{k-1}(x)$. Comme les suites $(x, f(x), \ldots)$ et $(x_0, f(x_0), \ldots)$ ont un élément en commun et que x_0 n'appartient pas à la première, x_0 est non récurrent. Comme on a $x = f^i(x_0)$ pour un certain entier $i \geqslant 1$, on est ramené au cas précédent. Ce qui achève la preuve du lemme.

3. LA Z-DÉCOMPOSITION DES MOTS

Nous allons définir dans cette section la Z-décomposition des mots qui nous servira à prouver dans la section 5 le caractère bijectif de ϕ. Soit X un ensemble non-vide; un *mot* est une suite $\sigma = (x_1, x_2, \ldots, x_t)$ qu'on notera plus volontiers $\sigma = x_1 x_2 \cdots x_t$ $(t \geqslant 1)$ où $x_1, x_2, \ldots, x_t$ appartiennent à X et sont les *lettres* du mot σ. L'entier t est la *longueur* du mot notée $l(\sigma)$. On suppose l'existence d'un *mot vide*, noté ϵ, de longueur 0 et ne contenant aucune lettre. Si $\sigma = x_1 x_2 \cdots x_t$ et $\sigma' = x_1' x_2' \cdots x_{t'}'$, sont deux mots non-vides, leurs produit $\sigma'' = \sigma\sigma'$ est obtenu par juxtaposition de σ et σ', c'est-à-dire que l'on a $\sigma'' = x_1'' x_2'' \cdots x_{t+t'}''$ avec $x_i'' = x_i$ pour $1 \leqslant i \leqslant t$ et $x_i'' = x_i'$ pour $t+1 \leqslant i \leqslant t+t'$. L'ensemble de tous les mots muni de ce produit est le *monoïde libre engendré par X* et noté $Mo(x)$. Si l'on a $\sigma_1\sigma_2\sigma_3 = \sigma$ où $\sigma, \sigma_1, \sigma_2, \sigma_3 \in Mo(X)$, on dit que σ_i est un *facteur* de σ s'il n'est pas vide $(i = 1, 2, 3)$ et que σ_1 et σ_3 sont respectivement des facteurs *gauche* et *droit* de σ. Un mot non-vide est *multilinéaire* si toutes ses lettres sont distinctes.

On dit que $\sigma' = x_1' x_2' \cdots x_t'$ est un *réarrangement* du mot $\sigma = x_1 x_2 \cdots x_t$ si $t = t'$ et s'il existe une permutation $k \to i_k$ de $[t]$ telle que $x_k' = x_{i_k}$ pour $1 \leqslant k \leqslant t$. Enfin, on désigne par $P\sigma$ la *première lettre* du mot σ.

On appelle *décomposition* d'un mot $\sigma \in Mo(X)$ toute suite finie $(\sigma_0, \sigma_1, \ldots, \sigma_p)$ de mots non-vides tels que $p \geqslant 0$ et $\sigma_0\sigma_1 \cdots \sigma_p = \sigma$.

L'entier $p+1$ est le *degré* de la décomposition. Soient enfin $x, y \in X$ et $\sigma = x_1 x_2 \cdots x_t$ un mot non-vide; on pose $\xi_{x,y}(\sigma) = 1$ s'il existe un indice i tel que $1 < i \leqslant t$, $x_{i-1} = y$, $x_i = x$ et $x_j \neq x$ pour tout $j = 1, 2, \ldots, i-1$. Dans le cas contraire, on pose $\xi_{x,y}(\sigma) = 0$. On pose en plus

$$\xi_x(\sigma) = \sum_{y \in X} \xi_{x,y}(\sigma) \qquad et \qquad \xi(\sigma) = \sum_{x \in X} \xi_x(\sigma).$$

On a évidemment

$$0 \leqslant \xi_x(\sigma) \leqslant 1 \tag{3.1}$$

et $\xi_{x,x}(\sigma) = 0$ pour tout $x \in X$. On dit que l'indice i est un indice *multiple* (de σ), si $i = 1$ ou s'il existe j tel que $1 \leqslant j < i$ et $x_j = x_i$.

(3.2) PROPOSITION. *Tout mot $\sigma = x_1 x_2 \cdots x_t$ non-vide admet une décomposition unique $(\sigma_0, \sigma_1, \ldots, \sigma_p)$, dite sa Z-décomposition, ayant les propriétés suivantes:*

(i) *$\sigma_0, \sigma_1, \ldots, \sigma_p$ sont multilinéaires,*

$$\text{(ii)} \quad \sum_{k'=0}^{k} \xi_{x,y}(\sigma_{k'}) = \xi_{x,y}(\sigma_0 \sigma_1 \cdots \sigma_k) \tag{3.3}$$

pour tout $(x, y) \in X^2$ et tout $k = 0, 1, \ldots, p$.

Si $(i_0, i_1, \ldots, i_p)$ est la suite croissante des indices multiples de σ et si l'on pose $i_{p+1} = t+1$, la Z-décomposition de σ est donnée par $(\sigma_0, \sigma_1, \ldots, \sigma_p)$ où

$$\sigma_k = x_{i_k} x_{i_k+1} \cdots x_{i_{k+1}-1} \tag{3.4}$$

pour $0 \leqslant k \leqslant p$.

PREUVE: Montrons d'abord que la suite $(\sigma_0, \sigma_1, \ldots, \sigma_p)$ où les σ_k sont donnés par les formules (3.4) satisfont aux propriétés (i) et (ii). Tout d'abord, les mots $\sigma_0, \sigma_1, \ldots, \sigma_k$ sont multilinéaires par définition même des indices multiples. Ensuite, si l'on a $\xi_x(\sigma_k) = 1$, pour un certain $x \in X$ et un certain k, alors x ne peut apparaître dans les mots $\sigma_{k+1}, \ldots, \sigma_p$ que comme première lettre, d'où $\xi_x(\sigma_{k'}) = 0$ pour $k' > k$ et d'autre part, les mots $\sigma_0, \ldots, \sigma_{k-1}$ n'ont aucune lettre égale à x; d'où $\xi_x(\sigma_{k'}) = 0$ pour $k' < k$. Le premier membre de (3.3) est donc égal à 0 ou à 1. S'il est nul, on a, ou bien $x_1 = x$, ou bien le mot $\sigma_0 \sigma_1 \cdots \sigma_k$ n'a aucune lettre égale à x; dans les deux cas, le second membre est aussi nul. S'il est égal à 1, on a $\xi_{x,y}(\sigma_{k'}) = 1$ pour un certain k' tel que $0 \leqslant k' \leqslant k$, donc $\sigma_{k'}$ s'écrit $\sigma_{k'} = \sigma' y x \sigma''$ avec $\sigma', \sigma'' \in Mo(X)$ et d'après ce qui-précède, le mot $\sigma_0 \cdots \sigma_{k'-1} \sigma' y$ ne contient aucune lettre égale à x. On a alors $\xi_{x,y}(\sigma_0 \sigma_1 \cdots \sigma_k) = 1$ et les relations (3.3) sont ainsi vérifiées.

Pour démontrer maintenant l'unicité de la Z-décomposition, on montre que si $(\sigma_0, \sigma_1, \ldots, \sigma_p)$ est une Z-décomposition de σ, alors les indices $i_0 = 1$, $i_1 = l(\sigma_0) + 1, \ldots, i_p = l(\sigma_0 \cdots \sigma_{p-1}) + 1$ sont les seuls indices multiples de σ. En effet, soit k un indice tel que $0 < k \leqslant p$; si l'indice i_k n'est pas multiple, le mot $\sigma_0\sigma_1 \cdots \sigma_{k-1}$ ne contient pas la lettre $x = x_{i_k}$, d'où $\xi_x(\sigma_0\sigma_1 \cdots \sigma_{k-1}) = 0$ et par suite

$$\sum_{k'=0}^{k-1} \xi_x(\sigma_{k'}) = 0 \tag{3.5}$$

d'après (3.3) et d'autre part, on a

$$\xi_{x,y}(\sigma_0\sigma_1 \cdots \sigma_k) = 1 \tag{3.6}$$

avec $x = x_{i_k}$ et $y = x_{i_k-1}$. Les relations (3.4), (3.5) et (3.6) entraînent alors que l'on a $\xi_{x,y}(\sigma_k) = 1$, ce qui contredit le fait que la première lettre de σ_k est x. D'où tous les indices $i_0, i_1, \ldots, i_p$ sont multiples. Soit enfin i un indice tel que $i_k < i < i_{k+1}$ où $0 \leqslant k \leqslant p$. Comme σ_k est multilinéaire, on a $\xi_x(\sigma_k) = 1$ avec $x = x_i$ d'où

$$\xi_x(\sigma_{k'}) = 0 \qquad \text{pour} \qquad 0 \leqslant k' < k \tag{3.7}$$

et

$$\xi_x(\sigma_0\sigma_1 \cdots \sigma_k) = 1 \tag{3.8}$$

d'après (3.3). Si i est multiple, désignons par j le plus petit indice tel que $x_j = x_i$. Si $j = 1$, on a $\xi_x(\sigma_0\sigma_1 \cdots \sigma_k) = 0$ ce qui contredit (3.8). Si $j > 1$, l'indice j n'est pas multiple et on a $i_{k'} < j < i_{k'+1}$ pour un certain k' tel que $0 \leqslant k' < k$. Comme σ_k est multilinéaire, on a $\xi_x(\sigma_{k'}) = 1$ ce qui contredit (3.7). Ainsi, les seuls indices multiples de σ sont $i_0, i_1, \ldots, i_p$. Ce qui achève la preuve de la proposition.

Dans la suite, il sera commode de noter $P_Z(\sigma)$ *le premier facteur de la Z-décomposition de* σ. D'autre part, l'une des relations (3.3) utile plus loin est la suivante:

$$\sum_{k=0}^{p} \xi_{x,y}(\sigma_k) = \xi_{x,y}(\sigma) \tag{3.9}$$

valable pour tout couple $(x, y) \in X^2$.

4. La Décomposition Croissante des Mots

Dans ce qui suit, R étant un sous-ensemble non vide de $[n]$, on désigne par $\beta(R)$ le mot *croissant* dont les lettres sont tous les éléments de R, par S_R

le groupe des permutations de R et enfin par H_R l'ensemble de tous les réarrangements du mot $\beta(R)$.

L'objet de cette section est d'exhiber une bijection $q : S_R \to H_R$ satisfaisant à

$$\nu_{x,y}(\pi) = \xi_{x,y}(q(\pi)) \tag{4.1}$$

pour $\pi \in S_R$ et $1 \leqslant x < y \leqslant n$. La construction de cette bijection n'est pas nouvelle (voir par exemple [2, théorème 4.11]), mais nous préférons la reproduire ici car elle est donnée dans la référence [2] dans un cadre tout à fait différent.

Soit $\pi \in S_R$ et γ un cycle de la permutation π. Le cycle γ est une permutation circulaire d'un sous-ensemble C de R, disons de cardinal j où $1 \leqslant j \leqslant b$ ($b = \text{card } R$). Posons $c = \max\{x : x \in C\}$ et notons $q(\gamma)$ le mot

$$q(\gamma) = \pi^j(c)\, \pi^{j-1}(c) \cdots \pi(c).$$

On a $\pi^j(c) = c$ et les j lettres du mot $q(\gamma)$ sont les j éléments (distincts) de C. Soit D_C l'ensemble de tous les réarrangements *dominés* (c'est-à-dire dont la première lettre est c) du mot $\beta(C)$. Il est clair que q est une bijection de l'ensemble des permutations circulaires de C sur D_C et que pour $1 \leqslant x < y \leqslant n$, on a

$$\nu_{x,y}(\gamma) = \xi_{x,y}(q(\gamma)). \tag{4.2}$$

Supposons que π soit le produit des cycles disjoints $\gamma_1, \gamma_2, \ldots, \gamma_s$ opérant sur les ensembles $C_1, C_2, \ldots, C_s$ (de réunion R) dont les plus grands éléments sont désignés par $c_1, c_2, \ldots, c_s$. Avec une numérotation appropriée, on peut supposer que la suite $c_1, c_2, \ldots, c_s$ est *croissante*. On désigne alors par $q(\pi)$ le produit de juxtaposition

$$q(\gamma) = q(\gamma_1)\, q(\gamma_2) \cdots q(\gamma_s). \tag{4.3}$$

Le mot appartient évidemment à H_R. Montrons que l'application $q : S_R \to H_R$ est *bijective*. Soit $\rho = x_1 x_2 \cdots x_b$ un mot de H_R. Posons $i_1 = 1$ et soit $(i_2, \ldots, i_s)$ la suite croissante des indices i tels que $1 < i \leqslant b$ et $x_i > x_j$ pour $1 \leqslant j < i$. Posons de plus $i_{s+1} = b + 1$ puis

$$\rho_k = x_{i_k} x_{i_k+1} \cdots x_{i_{k+1}-1}$$

et désignons par C_k l'ensemble des lettres du mot ρ_k ($1 \leqslant k \leqslant s$). On dit que la suite $(\rho_1, \rho_2, \ldots, \rho_s)$ ainsi définie est la *décomposition croissante* du mot ρ. Il est facile de vérifier que c'est l'unique décomposition de ρ satisfaisant aux deux propriétés:

(i) $\rho_1, \rho_2, \ldots, \rho_s$ sont dominés,

(ii) $P\rho_1 \leqslant P\rho_2 \leqslant \cdots \leqslant P\rho_s$

(voir [2, proposition 4.8]). La suite formée par les ensembles $C_1, C_2, \ldots, C_s$ est une partition de R et par définition des indices i_k, chaque mot ρ_k appartient à D_{C_k} $(1 \leqslant k \leqslant s)$ et la suite $x_{i_1}, x_{i_2}, \ldots, x_{i_s}$ est croissante. D'après ce qui précède, il correspond à chacun des ρ_k une et une seule permutation circulaire γ_k de l'ensemble C_k ; par conséquent, il existe un et un seul cycle γ_k tel que $q(\gamma_k) = \rho_k$ $(1 \leqslant k \leqslant s)$. Soit π la permutation $\pi = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s$. Il est alors immédiat que l'on a $q(\pi) = \rho$ et ainsi $q : S_R \to H_R$ est bijectif puisque S_R et H_R ont même cardinal.

Enfin, si l'on a $\pi \in S_R$ et $\nu_{x,y}(\pi) = 1$ pour $1 \leqslant x < y \leqslant n$ alors $\pi(x) = y$ et de plus x et y appartiennent à un même cycle de la permutation π. D'après (4.2), on a donc $\nu_{x,y}(\pi) = \xi_{x,y}(q(\pi)) = 1$. Réciproquement, si l'on a $1 \leqslant x < y \leqslant n$ et $\xi_{x,y}(q(\pi)) = 1$, le mot $q(\pi)$ contient le facteur yx. Soit $(\rho_1, \rho_2, \ldots, \rho_s)$ la décomposition croissante du mot $q(\pi)$. Comme y est supérieur à x, aucun des mots $\rho_1, \rho_2, \ldots, \rho_s$ ne peut se terminer par y et par conséquent on a $\xi_{x,y}(\rho_k) = 1$ pour un certain k tel que $1 \leqslant k \leqslant s$. D'où d'après (4.2), $\nu_{x,y}(q^{-1}(\rho_k)) = 1$ et par suite $\nu_{x,y}(\pi) = 1$. La propriété (4.1) est donc vérifiée.

5. Construction de la Bijection

$$\phi : F_n \to H_n$$

Soient $\omega = \beta([n]) = 1\,2 \cdots n$ le mot croissant dont toutes les lettres sont les entiers de 1 à n et H_n l'ensemble des mots de $Mo(\mathbf{N})$ de longueur n. Soit $f \in F_n$; si f est une *permutation* de $[n]$, on pose

$$\phi(f) = q(f) \tag{5.1}$$

où q est la bijection définie en (4.3). Si f n'est pas dans S_n, nous posons $\beta(Z_f) = z_1 z_2 \cdots z_p$ et $\beta(R_f) = r_1 r_2 \cdots r_b$, puis on définit par récurrence une suite de $(p+1)$ mots $\sigma_0, \sigma_1, \ldots, \sigma_p$ de $Mo(\mathbf{N})$. On pose d'abord

$$\sigma_0 = q(\pi_f). \tag{5.2}$$

D'après la section 4, σ_0 est un réarrangement de $r_1 r_2 \cdots r_b$. Supposons définis les mots $\sigma_0, \sigma_1, \ldots, \sigma_{k-1}$ pour un certain k tel que $1 \leqslant k \leqslant p$. Nous posons alors

$$m_k = \min\{m > 0 : \xi(\sigma_0 \sigma_1 \cdots \sigma_{k-1} f^m(z_k)) = \xi(\sigma_0 \sigma_1 \cdots \sigma_{k-1})\}, \tag{5.3}$$

puis

$$\sigma_k = f^{m_k}(z_k) f^{m_k-1}(z_k) \cdots f(z_k). \tag{5.4}$$

Autrement dit, m_k est le plus petit entier $m > 0$ tel que $f^m(z_k)$ soit égal à une lettre du mot $\sigma_0\sigma_1 \cdots \sigma_{k-1}$. Cette définition a bien un sens car $f^{n-1}(z_k)$ est dans R_f d'après (2.1), donc égal à une lettre du mot σ_0. On continue jusqu'à ce que σ_p soit défini et l'on pose

$$\phi(f) = \sigma_0\sigma_1 \cdots \sigma_p . \tag{5.5}$$

En conservant les mêmes notations que dans les formules (5.2) à (5.5), nous avons

(5.6) LEMME. *Soit x un élément de $[n]$ non récurrent et soit z_k le plus petit élément de Z_f satisfaisant $x = f^m(z_k)$ pour un certain $m \geqslant 0$. Alors*

$$0 \leqslant m < m_k = l(\sigma_k).$$

PREUVE: Notons d'abord que l'élément z_k dans l'énoncé ci-dessus est parfaitement défini d'après le lemme 2.2. Si l'on avait $m \geqslant m_k$, on aurait $x = f^i(y)$ avec $i = m - m_k$ et $y = f^{m_k}(z_k)$. Par définition de m_k, l'élément y apparaîtrait dans le mot $\sigma_0\sigma_1 \cdots \sigma_{k-1}$. De plus, l'hypothèse $x \notin R_f$ entraîne que y est également non récurrent et par conséquent y apparaîtrait en fait dans $\sigma_1 \cdots \sigma_{k-1}$. On aurait donc $y = f^{m'}(z_{k'})$ avec $1 \leqslant k' < k$ et $1 \leqslant m' \leqslant m_{k'}$, d'où $x = f^{i+m'}(z_{k'})$; ce qui contredirait la définition de z_k. On a donc $0 \leqslant m < m_k$ et le lemme 5.6 est démontré.

(5.7) COROLLAIRE. *Le mot $\phi(f)$ est un réarrangement du mot $f(1)f(2) \cdots f(n)$ et la suite $(\sigma_0, \sigma_1, ..., \sigma_p)$ est la Z-décomposition du mot $\phi(f)$.*

PREUVE: En effet, le mot $\tau_1\tau_2 \cdots \tau_p$ où

$$\tau_k = f^{m_k-1}(z_k) \cdots f(z_k)\, z_k \qquad (1 \leqslant k \leqslant p)$$

est d'une part multilinéaire (par définition des m_k) et d'autre part a pour lettres tous les éléments non récurrents d'après le précédent lemme et la définition des m_k. Par suite, le mot $\sigma_0\tau_1 \cdots \tau_p$ est un réarrangement de ω, ce qui implique pour $\phi(f)$ d'être un réarrangement de $f(1)f(2) \cdots f(n)$. Enfin, les mots $\sigma_1, ..., \sigma_p$ sont multilinéaires car autrement certaines de leurs lettres seraient des éléments récurrents. La définition (5.3) des m_k entraîne alors que $1, m_0 + 1, ..., m_{p-1} + 1$ sont les seuls indices multiples de $\phi(f)$. Ce qui prouve le corollaire d'après la proposition 3.2.

Dans l'énoncé du théorème combinatoire 5.9, nous reprenons les notations introduites au début de la section 4. En plus, nous poserons pour $\pi_0 \in S_R$ et $\sigma_0 \in H_R$

$$\begin{aligned} F_n(R, \pi_0) &= \{f \in F_n : R_f = R, \quad \pi_f = \pi_0\}, \\ H_n(R, \sigma_0) &= \{\sigma \in H_n : P_Z(\sigma) = \sigma_0\}. \end{aligned} \tag{5.8}$$

Il vient alors

(5.9) THÉORÈME. *L'application $\phi : F_n \to H_n$ est une bijection qui satisfait aux propriétés suivantes*:

1) *Le mot $\phi(f)$ est un réarrangement du mot $f(1)f(2)\cdots f(n)$ pour tout $f \in F_n$.*
2) *Si R est un sous-ensemble non vide de $[n]$ et si π_0 est une permutation de R, alors*

$$\phi(F_n(R, \pi_0)) = H_n(R, \sigma_0) \qquad \text{où} \qquad \sigma_0 = q(\pi_0).$$

3) *On a*

$$\nu_{x,y}(f) = \xi_{x,y}(\phi(f)) \qquad \text{pour} \qquad 1 \leqslant x < y \leqslant n \tag{5.10}$$

et tout $f \in F_n$.

PREUVE: La partie 1) a été prouvée (cf. corollaire 5.7). Comme les familles

$$\{F_n(R, \pi_0) : \pi_0 \in S_R, \emptyset \neq R \subset [n]\}$$

et

$$\{H_n(R, \sigma_0) : \sigma_0 \in H_R, \emptyset \neq R \subset [n]\}$$

sont des partitions de F_n et H_n respectivement et que $q : S_R \to H_R$ est bijectif pour tout sous-ensemble R non-vide de $[n]$, il nous suffit de prouver que $\phi : F_n(R, \pi_0) \to H_n(R, q(\pi_0))$ est une bijection satisfaisant à (5.10) pour tout $f \in F_n(R, \pi_0)$ ($\emptyset \neq R \subset [n]$, $\pi_0 \in S_R$). Ce résultat à déjà été démontré lorsque l'on a $R = [n]$ et $\pi_0 \in S_n$, dans la section 4. Dans la suite, on supposera donc R et π_0 fixés avec $R \neq [n]$ et l'on posera $\sigma_0 = q(\pi_0)$, $F_n(R, \pi_0) = F_{\pi_0}$ et $H_n(R, \sigma_0) = H_{\sigma_0}$.

Si f est dans F_{π_0}, on a bien $\phi(f) \in H_{\sigma_0}$ d'après (5.2) et le corollaire 5.7. Montrons alors que $\phi : F_{\pi_0} \to H_{\sigma_0}$ a la propriété (5.10). En effet, si l'on a $f \in F_{\pi_0}$, $1 \leqslant x < y \leqslant n$ et $x \in R_f$, il vient

$$\nu_{x,y}(f) = \nu_{x,y}(\pi_0) = \xi_{x,y}(\sigma_0) = \xi_{x,y}(\phi(f))$$

d'après (4.1) et le fait que σ_0 contient nécessairement la lettre x. Supposons ensuite $x \notin R_f$. Si l'on a $x \notin f([n])$, aucun des deux mots $f(1)f(2)\cdots f(n)$

et $\phi(f)$ ne contient la lettre x; d'où $\nu_{x,y}(f) = \xi_{x,y}(\phi(f)) = 0$ pour tout $y \in [n]$. Enfin si $x \in f([n])$, on a

$$\nu_{x,y}(f) = 1 \quad \text{si} \quad y = f(x) \quad \text{et}$$
$$= 0 \quad \text{si} \quad y \neq f(x).$$

Soit k le plus petit indice tel que $x = f^m(z_k)$ pour un certain $m > 0$. D'après le lemme 5.6, le mot σ_k contient le facteur $f(x)x$ et les mots $\sigma_0, \ldots, \sigma_{k-1}$ n'ont aucune lettre égale à x. Il en résulte l'identité

$$\nu_{x,y}(f) = \xi_{x,y}(\phi(f)) \quad \text{pour} \quad x \notin R_f \quad \text{et} \quad y \in [n]. \tag{5.11}$$

Montrons ensuite que $\phi : F_{\pi_0} \to H_{\sigma_0}$ est *injective*. Soient $f, f' \in F_{\pi_0}$; si l'on a $Z_f \neq Z_{f'}$, le mot $f(1) \cdots f(n)$ n'est pas un réarrangement du mot $f'(1) \cdots f'(n)$ et l'on a forcément $\phi(f) \neq \phi(f')$. Si maintenant $Z_f = Z_{f'}$, désignons par $(\sigma_0, \sigma_1, \ldots, \sigma_p)$ et $(\sigma_0', \sigma_1', \ldots, \sigma_p')$ les Z-décompositions de $\phi(f)$ et de $\phi(f')$ et par $(z_1, z_2, \ldots, z_p)$ la suite croissante des éléments de $Z_f = Z_{f'}$.

Si l'on a $y = f(x) \neq f'(x) = y'$, alors $x \notin R_f = R_{f'}$ et deux cas sont à considérer:

a) $x = z_k \in Z_f$ pour un certain k tel que $1 \leqslant k \leqslant p$. Les deux dernières lettres $f(z_k)$ et $f'(z_k)$ de σ_k et σ_k' sont alors distinctes, d'où $\sigma_k \neq \sigma_k'$ et par suite $\phi(f) \neq \phi(f')$ en vertu de l'unicité de la Z-décomposition.

b) $x \notin Z_f = Z_{f'}$. D'après (5.11) on a alors $\xi_{x,y}(\phi(f)) = \nu_{x,y}(f) = 1$ donc $\xi_{x,y'}(\phi(f)) = 0$ puisque $y \neq y'$ tandis que $\xi_{x,y'}(\phi(f')) = \nu_{x,y'}(f') = 1$. D'où encore $\phi(f) \neq \phi(f')$.

Montrons enfin que $\phi : F_{\pi_0} \to H_{\sigma_0}$ est *surjective*. Soient $\sigma = x_1 x_2 \cdots x_n$ un mot de H_{σ_0} et $x_{1,0}, x_{2,0}, \ldots, x_{p,0}$ la suite croissante des entiers $z \in [n]$ qui ne sont pas des lettres du mot σ. La Z-décomposition de σ est alors de degré $p + 1$; nous la notons $(\theta_0, \theta_1, \ldots, \theta_p)$ et nous posons

$$\theta_k = x_{k,m_k} x_{k,m_k-1} \cdots x_{k,1} \qquad (1 \leqslant k \leqslant p).$$

D'après les propriétés de la Z-décomposition, x_{k,m_k} est la seule lettre du mot θ_k qui soit égale à une lettre du mot $\theta_0\theta_1 \cdots \theta_{k-1}$ pour $1 \leqslant k \leqslant p$. Par conséquent, le mot $\theta_0\tau_1 \cdots \tau_p$ où $\tau_k = x_{k,m_k-1} \cdots x_{k,1}x_{k,0}$ $(1 \leqslant k \leqslant p)$ est un réarrangement du mot ω. D'autre part, l'application $\pi_0 = q^{-1}(\theta_0)$ est une permutation du sous-ensemble R formé par les lettres (distinctes) de θ_0. On définit donc une application $f \in F_{\pi_0}$ en posant

$$f(x_{k,m}) = x_{k,m+1} \qquad \text{pour} \qquad 1 \leqslant k \leqslant p \qquad \text{et} \qquad 0 \leqslant m < m_k$$

et

$$f(x) = \pi_0(x) \qquad \text{pour} \qquad x \in R.$$

Il est alors clair que l'on a $\phi(f) = \sigma$. Ce qui achève la preuve du théorème.

6. Applications Combinatoires et probabilistes

Avec les mêmes notations que dans l'énoncé du théorème 5.9, et en posant card $R = b$, on a

$$\text{card } F_n(R, \pi_0) = \text{card } H_n(R, \sigma_0) = bn^{n-b-1}. \tag{6.1}$$

Posons maintenant

$$A_n = \{f \in F_n : f^n = f^{n-1}\}$$

puis, pour $1 \leqslant b < n$

$$A_{n,b} = \{f \in A_n : \text{card } R_f = b\}.$$

L'ensemble A_n est l'ensemble des fonctions *ultimement idempotentes*, c'est-à-dire des fonctions f telles que π_f soit l'application identique de R_f. L'ensemble $A_{n,1}$ est l'ensemble des *arborescences*, [8, p. 157]. Pour $1 \leqslant b < n$, notons $K_{n,b}$ l'ensemble des mots $\sigma \in H_n$ tels que $P_Z(\sigma)$ soit *croissant* et $l(P_Z(\sigma)) = b$. D'après le théorème 5.9,

(6.2) *pour* $1 \leqslant b < n$, *l'application* ϕ *envoie bijectivement* $A_{n,b}$ *sur* $K_{n,b}$.

On a donc

$$\text{card } A_{n,b} = \text{card } K_{n,b} = \binom{n}{b} b\, n^{n-b-1} \tag{6.3}$$

et on retrouve le résultat bien connu

$$\text{card } A_n = \sum_{b=1}^{n} \binom{n}{b} b\, n^{n-b-1} = (n+1)^{n-1}. \tag{6.4}$$

L'ensemble $K_{n,1}$ est formé des mots $\sigma \in H_n$ de la forme $xx\sigma'$ où $x \in [n]$ et $\sigma' \in Mo(\mathbf{N})$. Si f est dans $A_{n,1}$ et si l'on a $\sigma(f) = xx\sigma'$, l'élément x est l'unique point fixe de $f(f(x) = x)$ et

(6.5) *l'application* $f \to x\sigma'$ *est une bijection de l'ensemble des arborescences sur l'ensemble* $H_{n-1,n}$ *des mots de longueur* $(n-1)$ *dont les lettres sont dans* $[n]$.

En particulier, on retrouve (voir [8, p. 157]):

$$\text{card } A_{n,1} = \text{card } H_{n-1,n} = n^{n-1}. \tag{6.6}$$

Pour $1 \leqslant n - 1 \leqslant d$, notons $G_{n,d}$ l'ensemble des graphes connexes de d arcs dont les sommets sont les entiers 1, 2,..., n. Les éléments de $G_{n,n-1}$ sont les *arbres* de n sommets. Il existe une bijection naturelle $\psi : G_{n,n-1} \times [n] \to A_{n,1}$, dite "enracinement." Soient en effet $T \in G_{n,n-1}$ et $r \in [n]$; la fonction $f = \psi(T, r)$ est ainsi définie. On pose d'abord $f(r) = r$ et si $x \in [n] \setminus \{r\}$, on pose $f(x) = y$ si et seulement si l'arbre T contient l'arête (x, y) et si les deux premiers sommets de l'unique chaîne joignant x à r sont x, y (dans cet ordre). On a ainsi $\phi(\psi(T, n)) = nn\sigma'$ où $\sigma' \in Mo(\mathbf{N})$ et

(6.7) *l'application $T \to \sigma'$ est une bijection de l'ensemble des arbres de n sommets sur l'ensemble $H_{n-2,n}$ des mots de longueur $(n - 2)$ dont les lettres sont dans $[n]$.*

En particulier, on retrouve le résultat de Cayley

$$\text{card } G_{n,n-1} = \text{card } H_{n-2,n} = n^{n-2}. \tag{6.8}$$

Intéressons-nous enfin à l'ensemble

$$B_n = \{f \in F_n : \pi_f \text{ est une permutation circulaire}\},$$

puis posons pour $1 \leqslant b \leqslant n$:

$$B_{n,b} = \{f \in B_n : \text{card } R_f = b\}.$$

On a $A_{n,1} = B_{n,1}$ et B_n est l'ensemble des *fonctions indécomposables*. Soit $L_{n,b}$ l'ensemble des mots $\sigma \in H_n$ tels que $P_Z(\sigma)$ soit *dominé* (voir section 4), et $l(P_Z(\sigma)) = b$ $(1 \leqslant b \leqslant n)$. D'après (5.2) et le théorème 5.9,

(6.9) *pour $1 \leqslant b \leqslant n$ l'application ϕ envoie bijectivement $B_{n,b}$ sur $L_{n,b}$.*

D'où

$$\text{card } B_{n,b} = \text{card } L_{n,b} = \binom{n}{b} (b - 1)!\, b\, n^{n-b-1},$$

soit

$$\text{card } B_{n,b} = (n - 1)!\, n^{n-b}/(n - b)!, \tag{6.10}$$

d'où l'on déduit le résultat de Katz [4]:

$$\text{card } B_n = \sum_{b=1}^{n} (n - 1)!\, n^{n-b}/(n - b)!.$$

Maintenant si T est un graphe connexe de n arêtes et n sommets, il contient un et un seul cercle C dont le nombre de sommets b est au moins

égal à 3 (voir [7]). Soient $c = \max\{x : x \in C\}$, c' et c'' les deux sommets de C indicents à c. Au graphe T correspond biunivoquement une paire $\{f, g\}$ de fonctions à un seul cycle, telle que $\pi_g = \pi_f^{-1}$: on pose $f(x) = y$ (resp. $g(x) = y$) si et seulement si le graphe T contient une chaîne dont les deux premiers sommets sont x, y et les deux derniers c', c (resp. c'', c).

Soit $G_{n,n,b}$ l'ensemble des graphes de n arêtes et n sommets, contenant un seul cercle de b sommets ($3 \leqslant b \leqslant n$). Alors

(6.11) *l'application $T \to \{f, g\}$ est une bijection de $G_{n,n,b}$ sur l'ensemble des paires $\{f, g\}$ de fonctions de $B_{n,b}$ telles que $\pi_g = \pi_f^{-1}$.*

D'après (6.10) on a

$$\text{card } G_{n,n,b} = (n-1)!\, n^{n-b}/(2(n-b)!) \tag{6.12}$$

et on retrouve le résultat connu (voir [7]):

$$\text{card } G_{n,n} = (n!/2) \sum_{b=3}^{n} n^{n-b-1}/(n-b)!. \tag{6.13}$$

Dans la dernière application que nous donnons, nous allons identifier toute fonction $f \in F_n$ au mot $\sigma = x_1 x_2 \cdots x_n$ où $f(i) = x_i$ pour tout $i \in [n]$. On remarque que $\nu_{i,j}(\sigma)$ est nul si $1 \leqslant i \leqslant n$ et $j \neq x_i$; de même $\xi_{j,k}(\sigma)$ est égal à 1 si et seulement s'il existe un indice i tel que l'on ait $1 \leqslant i < n$, $i+1$ non multiple, $x_i = k$ et $x_{i+1} = j$. On posera donc pour $1 \leqslant i < n$, $\eta_i(\sigma) = \nu_{i,x_i}(\sigma)$, c'est-à-dire que $\eta_i(\sigma)$ est égal à 1 ou à 0 suivant qu'il existe ou non un indice j tel que $1 \leqslant j \leqslant n$ et $x_j = i$; puis $\zeta_i(\sigma) = 0$ ou 1 suivant que l'indice $i+1$ est multiple ou non. De plus, si $g : \mathbf{R}^2 \to \mathbf{R}$ est une fonction arbitraire telle que $g(x, y) = 0$ si $x \leqslant y$, on désignera par $\Gamma_g(\sigma)$ et $\Delta_g(\sigma)$ les vecteurs à $(n-1)$ dimensions

$$\Gamma_g(\sigma) = (\eta_1(\sigma) \cdot g(x_1, 1), \eta_2(\sigma) \cdot g(x_2, 2), \ldots, \eta_{n-1}(\sigma) \cdot g(x_{n-1}, n-1)),$$

$$\Delta_g(\sigma) = (\zeta_1(\sigma) \cdot g(x_2, x_1), \zeta_2(\sigma) \cdot g(x_3, x_2), \ldots, \zeta_{n-1}(\sigma) \cdot g(x_n, x_{n-1})).$$

Le théorème 5.9 nous dit alors

(6.14) *qu'il existe une permutation ϕ de H_n telle que pour tout $\sigma \in H_n$, les vecteurs $\Gamma_g(\sigma)$ et $\Delta_g(\phi(\sigma))$ ne diffèrent que par un réarrangement de leurs coordonnées.*

Soit maintenant Y une variable aléatoire réelle dont la distribution est uniformément répartie sur les entiers $1, 2, \ldots, n$. Soient d'autre part, $Y_1, Y_2, \ldots, Y_n$ une suite de n variables aléatoires mutuellement indépendantes, ayant chacune même distribution que Y. On peut considérer tout $\sigma \in H_n$ comme une réalisation du vecteur aléatoire $(Y_1, Y_2, \ldots, Y_n)$. Soit

alors $h : \mathbf{R}^{n-1} \to \mathbf{R}$ une fonction mesurable *symétrique* de ses $(n-1)$ variables et supposons la fonction g mesurable. La propriété (6.14) entraîne alors que

(6.15) *les variables aléatoires* $h \circ \Gamma_g$ *et* $h \circ \Delta_g$ *ont même distribution.*

Une application de ce résultat en termes du jeu de dés, nous semble intéressante à donner. Supposons que $Y_1, Y_2, \ldots, Y_6$ soient les numéros des faces d'un dé qui apparaissent au cours de 6 jets successifs. Pour $1 \leqslant i \leqslant 5$, nous notons U_i l'évènement "la face i apparaît au cours de ces six jets et l'on a $Y_i > i$," puis V_i l'évènement "la face i apparaît et lorsqu'elle apparaît pour la première fois, on a observé au coup précédent une face supérieure à i." Il est facile de voir que U_i et V_i ont la même probabilité et par conséquent leurs indicatrices I_{U_i} et I_{V_i} ont même distribution pour $1 \leqslant i \leqslant 5$. La propriété (6.15) permet en plus d'affirmer que les variables

$$\nu^* = \sum_{i=1}^{5} I_{U_i} \qquad \text{et} \qquad \xi^* = \sum_{i=1}^{5} I_{V_i},$$

sommes de variables aléatoires *dépendantes*, ont elles aussi même distribution. Il suffit en effet dans l'énoncé (6.15) de prendre

$$h(x_1, \ldots, x_5) = x_1 + \cdots + x_5$$

et

$$g(x, y) = 1$$

si $x > y$ et $g(x, y) = 0$ si $x \leqslant y$.

RÉFÉRENCES

1. C. BERGE, *Théorie des Graphes et ses Applications*, Dunod, Paris, 1958.
2. P. CARTIER ET D. FOATA, *Problèmes Combinatoires de Commutation et Réarrangements* (Lecture Notes in Mathematics, No. 85), Springer-Verlag, Berlin, 1969.
3. A. CAYLEY, A Theorem on Trees, *Quart. J. Pure Appl. Math.* **23** (1889), 376–378.
4. L. KATZ, Probability of Indecomposability of a Random Mapping Function, *Ann. Math. Statist.* **26** (1955), 512–517.
5. E. H. NEVILLE, The Codifying of Tree-Structure, *Proc. Cambridge Philos. Soc.* **49** (1953), 381–385.
6. H. PRÜFER, Neuer Beweis eines Satzes über Permutationen, *Arch. Math. Phys.* **27** (1918), 142–144.
7. A. RÉNYI, On Connected Graphs, *Magyar Tud. Akad. Mat. Kutató Int. Közl.* **4** (1959), 385–387.
8. J. RIORDAN, *An Introduction to Combinatorial Analysis*, Wiley, New York, 1958.