

# Table des matières

0.1	Ajout de nombres, et processus des retenues . . . . .	2
0.2	Mélange de cartes . . . . .	5
0.3	Connexion entre le mélange des cartes et les retenues . . . . .	9
0.4	Liens avec la combinatoire algébrique . . . . .	11



# Ajout de nombres, mélange de cartes et fonctions symétriques

Persi Diaconis

9 février 2010

2

Selon l'exposé en anglais de Persi Diaconis (Stanford University) intitulé « Adding numbers, shuffling cards and symmetric functions ». La leçon est basée sur un travail commun de Persi avec Jason Fulman [5] (University of Southern California).

C'est un exposé à propos de simples faits concernant l'ajout de nombres, le mélange des cartes (à jouer) et à propos du joli sujet des fonctions symétriques ; et vous allez voir que ces sujets vont se mélanger. Je commence avec l'ajout des nombres.

## 0.1 Ajout de nombres, et processus des retenues

Voici deux nombres de 50 chiffres que l'on ajoute à l'aide de la méthode traditionnelle. J'indique la retenue apparaissant dans le calcul sous la ligne.

		52564	72537	78954	12536	74561	54135	78932	87613	31518	71321
	+	76574	12365	74102	96542	00255	05081	71513	87412	33758	78925
retenues	1	01100	00111	11001	01000	00100	00101	11001	11000	01011	1100
résultat	1	29138	84903	59357	09078	74816	59217	50446	75025	65277	50246

On ajoute à partir de la droite. 1+5 donne 6, je retiens 0, 2+2 égal 4, je retiens 0, 3+9 donne 12, je retiens 1, 1+8+ma retenue 1 donne 10, je retiens 1, etc... Ainsi lorsque l'on ajoute des nombres, il y a un processus naturel de « retenues ». Dans cet exemple particulier, on a eu la retenue 1, 23 fois (sur 50 places possibles) et la retenue 0, 27 fois. Il est naturel de penser que si l'on prend de grands nombres aléatoires, on va avoir la retenue 0 dans 50 pour cent des cas, et bien sûr la retenue 1, dans 50 pour cent des cas aussi. Dans l'exemple ci-dessous, je n'ai pas écrit les nombres en entier. J'ajoute maintenant 3 nombres.

		08453	...	...	...	...	...	...	...	...	74321
	+	67711	...	...	...	...	...	...	...	...	19354
	+	76306	...	...	...	...	...	...	...	...	78125
retenues	1	21010	...	...	...	...	...	...	...	...	2011
résultat	1	52470	...	...	...	...	...	...	...	...	71800

Maintenant lorsque j'ajoute trois nombres, les retenues peuvent être 0, 1 ou 2. Et dans cet exemple (que je n'ai pas écrit en entier) 24 pour cent du temps un 0 est apparu en retenue, 62 % ce fût un 1, et 14 % un 2. Je pense qu'il n'est pas facile de comprendre ce qui arrive. Moi, je ne peux pas deviner... et en fait, c'est une véritable question de savoir ce qui arrive. Transformons là en une véritable question mathématique. On va définir le processus des retenues. Supposons que j'ai  $m$  nombres, de longueur  $r$  (avec  $r$  décimales). J'écris le développement décimal du premier nombre comme cela  $X_{1,r-1}X_{1,r-2} \cdots X_{1,1}X_{1,0}$ , le deuxième nombre  $X_{2,r-1}X_{2,r-2} \cdots X_{2,1}X_{2,0}$  ; je note  $S_r \dots S_0$  la somme et  $C_r \dots C_0$  le processus des retenues (avec  $C_0 = 0$ ) :

		$X_{1,r-1}$	$\cdots$	$X_{1,1}$	$X_{1,0}$
	+	$\vdots$	$\ddots$	$\vdots$	$\vdots$
	+	$X_{m,r-1}$	$\cdots$	$X_{m,1}$	$X_{m,0}$
retenues	$C_r$	$C_{r-1}$	$\cdots$	$C_1$	$C_0 = 0$
résultat	$S_r$	$S_{r-1}$	$\cdots$	$S_1$	$S_0$

Ainsi, si j'ajoute  $m$  nombres écrits en base  $b$ , j'ai un processus de retenue bien défini, à valeurs dans  $\{0, 1, \dots, b-1\}$ . La première chose à dire est la suivante. Supposons que l'on choisisse maintenant les nombres de manières aléatoires, indépendamment les uns des autres selon la loi suivante : les décimales sont indépendantes les unes des autres, et chaque décimale est choisie uniformément dans l'ensemble  $\{0, \dots, b-1\}$ . Autrement dit, la famille de décimales  $(X_{i,j})_{i=1..m, j=0..r-1}$  est une famille de variables aléatoires indépendantes et de loi uniforme dans  $\{0, \dots, b-1\}$ . On observe aisément dans ce cas que les retenues, les  $C_i$ , ne sont pas des variables indépendantes. Elles sont dépendantes de manière simple : la suite  $(C_i, i \in \{0, \dots, r-1\})$  forme une chaîne de Markov. C'est facile à voir. Si je m'intéresse à  $C_5$  par exemple. Il est facile de voir que parmi  $C_4, C_3, C_2, C_1, C_0$ , seul  $C_4$  me donne une information, puisque les nombres déterminant la valeur de  $C_5$  sont d'une part  $X_{1,5}, \dots, X_{m,5}$  (qui sont indépendants clairement de  $C_4, C_3, C_2, C_1, C_0$ ) et d'autre part  $C_4$ . Ainsi,  $C_0, C_1, \dots$  est une chaîne de Markov dont il est raisonnablement simple d'exprimer la probabilité de transition. Notons  $P_b\{i, j\}$  la probabilité que si une retenue est  $i$  la suivante soit  $j$  (autrement dit, la probabilité que  $C_k$  vaille  $j$  conditionnellement à l'événement  $\{C_{k-1} = i\}$ ). On trouve, pour  $i$  et  $j$  dans  $\{0, m-1\}$

$$P_b\{i, j\} = P_b\{jb \leq i + X_1 + \dots + X_m \leq (j+1)b - 1\} \quad (1)$$

$$= \frac{1}{b^m} \sum_{r=0}^{j-\lfloor i/b \rfloor} (-1)^r \binom{m+1}{r} \binom{n-1-i+(j+1-r)b}{m} \quad (2)$$

où les  $X_i$  sont des variables indépendantes et uniformes sur  $\{0, \dots, b-1\}$ , et où  $\lfloor x \rfloor$  désigne la partie entière de  $x$ . En effet, pour un  $k \geq 1$  quelconque une retenue  $R_k$  vaut  $j$  conditionnellement au cas où la retenue précédente  $R_{k-1}$  vaut  $i$ , si et seulement si  $i$  ajouté aux  $m$  variables indépendantes  $X_1, \dots, X_m$  contribuant au calcul de  $R_k$  vérifient  $jb \leq i + X_1 + \dots + X_m \leq (j+1)b - 1$  (notez bien que ceci ne dépend pas de  $k$ ). Maintenant, pour obtenir la deuxième formule indiquée, il s'agit d'un problème de dénombrement simple du nombre de chemins à  $m$  pas, dont les incréments sont dans  $\{0, \dots, b-1\}$ , et nous connaissons une formule pour faire cela. On obtient ainsi une matrice  $m$  par  $m$  définie à l'aide de (2), puisque rappelons-le, les retenues peuvent prendre toutes les valeurs dans  $\{0, \dots, m-1\}$ . On peut alors regarder ce que donne la formule pour les petites valeurs de  $b$  et  $m$ .

– Le cas le plus simple est le cas où on ajoute des nombres écrits en base  $b = 2$  où on arrive à obtenir une formule simple :

$$P_2\{i, j\} = \frac{1}{2^m} \binom{m+1}{2j+i-1}, \quad i, j \in \{0, \dots, m-1\}.$$

– Le deuxième cas où les choses se passent simplement est lorsque  $m = 3$ , autrement dit, on ajoute 3 nombres, dans une base  $b$  quelconque. La matrice  $\mathcal{P}_b = (P_b\{i, j\})_{i=0,1,2, j=0,1,2}$  que l'on obtient est

$$\mathcal{P}_b = \frac{1}{6b^2} \begin{pmatrix} b^2 + 3b + 2 & 4b^2 - 4 & b^2 - 3b + 2 \\ b^2 - 1 & 4b^2 + 2 & b^2 - 1 \\ b^2 - 3b + 2 & 4b^2 - 4 & b^2 + 3b + 2 \end{pmatrix}.$$

On peut remarquer que cette matrice possède une symétrie centrale. Si on écrit les matrices pour  $m = 4, m = 5$ ... on voit que ce sont aussi de très jolies matrices.

Alors, d'où sortent ces matrices? Je ne les ai pas inventées... Je perdais mon temps un jour, à lire « American math monthly » au lieu de travailler, d'arbitrer des articles, ou de faire quelque chose d'important... Je survolais un papier par John Holt [7], s'appelant « Carries,

combinatorics and an amazing matrix » (retenues, combinatoire, et une matrice étonnante). Il utilisait mathematica pour démontrer des théorèmes – au passage, je déteste mathematica – et voici l'un des théorèmes qu'il a prouvé.

Tout d'abord cette matrice n'est pas symétrique, et a priori il n'y a pas de raison que ces valeurs propres soient réelles ou positives... mais c'est le cas! Voici :

- Pour tout  $m$ ,  $\mathcal{P}_b$  a des valeurs propres réelles, qui sont  $1 = 1/b^0, 1/b^1, \dots, 1/b^{m-1}$ . (1 est valeur propre, puisqu'on a affaire à une matrice stochastique)
- les vecteurs propres sont réels, et on peut les écrire à l'aide de coefficients binomiaux, et chose étonnante, ils ne dépendent pas de  $b$ . Attention, ici, je m'intéresse aux vecteurs propres à gauche : un vecteur ligne  $V$  est vecteur propre à gauche de  $\mathcal{P}_b$  si  $V\mathcal{P}_b = \lambda V$  pour un certain  $\lambda$ . Par exemple, le premier vecteur propre (normalisé de sorte que la somme de ses coefficients vaille 1), celui correspondant à la valeur propre 1 est donné par  $\pi = (\pi(0), \dots, \pi(m-1))$  avec

$$\pi(j) = \frac{1}{m!} \left\langle \begin{matrix} m \\ j \end{matrix} \right\rangle \quad (3)$$

où  $\left\langle \begin{matrix} m \\ j \end{matrix} \right\rangle$  est le nombre de permutations de  $S_m$  (du groupe des permutations des  $m$  entiers  $\{1, 2, \dots, m\}$ ) possédant  $j$  descentes. Une descente étant simplement ce qu'on pense : Une permutation  $\sigma$  a une descente en  $i$ , si  $\sigma(i+1) < \sigma(i)$  (notion déjà vue dans la Section 0.3). Par exemple la permutation  $\sigma = (\underline{6}2\underline{5}3\underline{4}1)$  possède 3 descentes (soulignées). Le nombre de descente d'une permutation  $\sigma$  sera noté  $D(\sigma)$ . Ainsi,  $\left\langle \begin{matrix} m \\ j \end{matrix} \right\rangle = \#\{\sigma \in S_m, D(\sigma) = j\}$ ; ces nombres sont appelés nombres eulériens. Le vecteur propre  $\pi$  est important puisque il donne la mesure stationnaire de la chaîne de Markov, la mesure vers laquelle converge la loi de  $C_j$  lorsque  $j \rightarrow +\infty$  (correspondant donc à la somme de nombres dont la taille tend vers l'infini).<sup>(1)</sup>

Par exemple, lorsque  $m = 3$ , il y a 6 permutations une ayant 0 descente (123), 4 ayant 1 descente (231), (132), (312), (213) et 1 ayant deux descentes (321), ce qui donne, donc

$$\pi(0) = 1/6, \quad \pi(1) = 2/3, \quad \pi(2) = 1/6.$$

Ainsi, asymptotiquement si on ajoute de très grands nombres, un sixième des retenues seront des 0, quatre sixièmes des 1, et le reste des 2, indépendamment de la valeur de  $b$ . Pour  $m = 4$ , ça donne

$$\pi(0) = 1/24, \quad \pi(1) = 11/24, \quad \pi(2) = 11/24, \quad \pi(4) = 1/24.$$

- Une autre chose intéressante à remarquer et que ces matrices, notées  $\mathcal{P}_b$  plus haut, font intervenir uniquement la base  $b$ ; on peut prouver que pour tout  $a, b \geq 2$  (deux matrices de taille  $m \times m$  correspondant à l'ajout de  $m$  nombres), on a

$$\mathcal{P}_a \mathcal{P}_b = \mathcal{P}_{ab}. \quad (4)$$

---

<sup>1</sup>ndlr : Lorsqu'une chaîne de Markov sur un ensemble fini  $E$  a de bonnes propriétés (apériodicité, irréductibilité), elle possède une loi stationnaire  $\mu$  unique. Cette loi est une mesure de probabilité sur  $E$ , invariante par la loi transition de la chaîne de Markov : c'est la seule loi  $\mu$  telle que si  $X_0$  suit la loi  $\mu$ ,  $X_1$  aussi. Puisque  $P(X_1 = j) = \sum_i P(X_1 = j | X_0 = i) P(X_0 = i)$ ,  $\mu$  satisfait  $\mu_j = \sum_i \mu_i Q_{i,j}$  pour  $Q_{i,j} = P(X_1 = j | X_0 = i)$ , le noyau de transition de la chaîne. Autrement dit,  $\mu$  est un vecteur propre à gauche pour la matrice  $Q$ , associé à la valeur propre 1 (normalisé de sorte que la somme de ses coordonnées fasse 1). Maintenant, si on suppose quelconque la loi de départ, c'est-à-dire la loi de  $X_0$ , il se trouve que sous les hypothèses d'apériodicité et d'irréductibilité,  $X_n$  converge en loi vers  $\mu$ , lorsque  $n \Rightarrow +\infty$ . On renvoie au livre de Brémaud [2] pour plus d'informations.

Ainsi ces deux matrices se combinent de cette manière. Notez que ça aurait pu être un vrai bazar, mais ce n'est pas le cas...

Donc, bref, je lisais cet article de Holt dans la revue en question... et si vous aviez été moi, votre réaction aurait été :

« eh! mais c'est pareil que de mélanger des cartes!! »

J'imagine que pour vous ce que je dis n'a pas trop de sens. Laissez moi vous parler un peu de mélange de cartes.

## 0.2 Mélange de cartes

Tout d'abord ce que j'entends par mélange de cartes, c'est la même chose que vous. Vous prenez un jeu de cartes, vous le coupez en deux, en prenez la moitié dans chaque main, et d'une manière ou d'une autre, vous mélangez<sup>(2)</sup>. Je vais alors vous parler d'un modèle mathématique qui a été introduit par Gilbert, Shannon, et Reeds.

Tout d'abord, on commence par prendre un jeu ordonné. On le coupe en deux paquets  $A$  et  $B$  : le paquet  $A$  sera de taille  $c$  dans le cas où j'ai  $m$  cartes en tout, avec probabilité

$$\binom{m}{c} / 2^m \quad \text{pour } c \in \{0, \dots, m\};$$

il s'agit de la loi binomiale. Les distributions de la taille de  $A$  et de  $B$  sont alors les mêmes. C'est cette distribution qui apparaît si on demande à chaque carte du paquet total de choisir un tas  $A$  ou  $B$  avec probabilité  $1/2$ , indépendamment des autres cartes. Seulement ici, les cartes sont numérotées de 1 à  $m$ , et on attribue au paquet  $A$  les  $c$  premières, et au paquet  $B$  les suivantes.

Maintenant que l'on a ces deux paquets de cartes, notés  $A$  et  $B$ , le processus de mélange se passe comme suit. On empile les cartes en les laissant tomber du paquet  $A$  ou du paquet  $B$ , de la manière suivante. Si à un certain moment le paquet  $A$  possède  $a$  cartes, le paquet  $B$ ,  $b$  cartes, alors on laisse tomber la carte du fond du paquet de  $A$  avec probabilité  $a/(a+b)$  et la carte du fond du paquet de  $B$  avec probabilité  $b/(a+b)$ . Ainsi si j'ai, à un certain moment donné, un gros paquet  $A$  et un petit paquet  $B$ , la prochaine carte à tomber a plus de chance d'être issue de  $A$ . La description de l'évolution des événements que je viens de faire décrit entièrement le processus probabiliste.

Considérons maintenant la permutation de  $S_m$  définie par l'ordre des cartes du jeu mélangé. Cette permutation est aléatoire et sa loi est notée  $\mathbb{Q}$ . Ainsi  $\mathbb{Q}(\sigma)$  est donc la probabilité d'observer le jeu en position  $\sigma$  après le mélange. Que se passe-t-il, si on itère cette manière de mélanger ?

Si on mélange deux fois, de manière indépendantes, la loi de la permutation aléatoire devient

$$\mathbb{Q}^{*2}(\sigma) = \sum_{\eta \in S_m} \mathbb{Q}(\eta) \mathbb{Q}(\sigma \eta^{-1});$$

en effet, pour être en position  $\sigma$  après deux mélanges, il faut que si le premier mélange me donne  $\eta$ , le deuxième me donne ce qu'il faut pour retomber sur  $\sigma$ , c'est-à-dire,  $\sigma \eta^{-1}$ . Il s'agit

---

<sup>2</sup>ndlr : il fait le geste de mettre les deux demi-jeux proches l'un de l'autre, et par une légère torsion, permet aux cartes des deux paquets de se mélanger, par insertion plus ou moins régulière des deux paquets de cartes, comme font les professionnels.

donc juste de la loi de la convolution sur le groupe... Avec le même argument on obtient

$$\mathbb{Q}^{\star k}(\sigma) = \sum_{\eta \in S_m} \mathbb{Q}(\eta) \mathbb{Q}^{\star k-1}(\sigma \eta^{-1}).$$

Ceci est notre modèle mathématique pour le mélange de cartes.

Une question que nous avons étudié avec Dave Bayer [1] de Colombia (New York) est la suivante :

« combien de fois doit-on mélanger un jeu de cartes pour qu'il soit bien mélangé ? »

La manière dont on traduit cela mathématiquement est la suivante : je définis une distance entre la loi  $\mathbb{Q}^{\star k}$  de la permutation obtenue en mélangeant le jeu  $k$  fois, et la mesure uniforme sur l'ensemble  $S_m$  de toutes les permutations possibles (il s'agit bien sûr de la loi donnant un poids  $1/m!$  à chacune des permutations de  $S_m$ ). La distance est donnée par cette formule :

$$\|\mathbb{Q}^{\star k} - \text{UNIF}\| = \max_{E \subset S_m} \left| \mathbb{Q}^{\star k}(E) - \frac{|E|}{m!} \right| = \frac{1}{2} \sum_{\sigma \in S_m} \left| \mathbb{Q}^{\star k}(\sigma) - \frac{1}{m!} \right|.$$

Cette distance est appelée distance en variation totale par les probabilistes. La dernière égalité est une identité classique. Ainsi, ma distance est facile à comprendre : vous prenez un sous ensemble  $E$  des permutations de taille  $k$ . Si le jeu était parfaitement mélangé après  $k$  étapes vous auriez  $\mathbb{Q}^{\star k}(E) = k/m!$ . Ici, on calcule  $|\mathbb{Q}^{\star k}(E) - k/m!|$  et on prend le supremum sur tous les ensembles  $E$ .

Maintenant que j'ai bien tout spécifié, ma distance et le mécanisme selon lequel je mélange, j'ai un problème de mathématique : si on se donne  $\varepsilon > 0$ , comment faut-il choisir  $k$  pour avoir  $\|\mathbb{Q}^{\star k} - \text{UNIF}\| < \varepsilon$  ? Avec Dave, nous avons résolu ce problème. Je vais vous énoncer le résultat ; d'abord, je vais vous dire ce qu'il se passe lorsque  $m = 52$ , car finalement c'est ce qui intéresse pas mal de gens. Enfin, les casinos sont intéressés par la réponse pour 6 jeux<sup>(3)</sup> de cartes...

La distance en variation est inférieure à 1, puisqu'elle est définie par des différences de probabilités, qui sont des nombres compris entre 0 et 1. Voici les distances que l'on obtient

$k$	1	2	3	4	5	6	7	8	9	...
$\ \mathbb{Q}^{\star k} - \text{UNIF}\ $	1,000	1,000	1,000	1,000	0,929	0,628	0,318	0,162	0,084	...

on voit qu'au début c'est collé à 1, en fait bien sûr, c'est un peu moins que 1, et à partir de 5, ça démarre, à 6 ça fait 0,628, puis ensuite c'est divisé en gros par deux à chaque fois, et ça continue comme ça, ensuite, pour les  $k$  plus grands... On voit qu'il y a une transition : au début ce n'est pas mélangé, puis ça devient exponentiellement bien mélangé. Où apparaît la transition ? Je dis que ça commence à partir de 7 mélanges... on pourrait en discuter. En fait, je sais ce que sont ces nombres précisément, on va le voir. Alors, voyons maintenant quelque chose qui ressemble plus à des maths :

**Théorème 0.2.1.** *Pour  $m$  général et  $k = \frac{3}{2} \log_2 m + c$*

$$\|\mathbb{Q}^{\star k} - \text{UNIF}\| = 1 - 2\Phi\left(\frac{2^{-c}}{4\sqrt{3}}\right) + O(1/\sqrt{m})$$

avec  $\Phi(x) = \int_{-\infty}^x \frac{e^{-t^2/2}}{\sqrt{2\pi}} dt$ , la fonction de répartition d'une variable gaussienne (en particulier elle tend vers 1/2 lorsque  $x$  tend vers 0).

<sup>3</sup>Il y a 6 jeux de cartes dans le sabot du Blackjack, au casino

Autrement dit : on a un jeu de  $m$  cartes que l'on mélange  $k$  fois. Si on me donne  $k$  et  $m$ , cela détermine  $c$ . Le théorème dit que la distance à la mesure stationnaire, qui est la loi uniforme ici, est à une petite quantité près, à savoir  $O(1/\sqrt{m})$  égale à  $1 - 2\Phi(\frac{2-c}{4\sqrt{3}})$ . Si on trace pour  $m$  grand la suite  $k \mapsto \|Q^{*k} - U\|$  on voit qu'elle passe de presque 1 à presque 0, aux alentours de  $(3/2)\log_2 m$ , et la chute est exponentiellement rapide. La courbe a ce qu'on appelle une transition "sharp" (abrupte) en  $(3/2)\log_2 m$ . Comme on connaît bien l'asymptotique de  $\Phi$  aux alentours de 0, on montre aisément que la descente de 1 vers 0 est exponentiellement rapide, et dans l'autre sens, en prenant la courbe à l'envers, le passage de 0 vers 1 est doublement exponentiel. Ainsi dans un tout petit domaine, la courbe passe de 1 à 0. Ainsi avec ce théorème, vous pouvez savoir combien de fois il faut mélanger 6 jeux de cartes, comme au casino, pour qu'il soient bien mélangés. Bien sûr, vous devez fournir  $\varepsilon$ , la distance entre la distribution du jeu mélangé et la loi uniforme, puisque bien sûr, le jeu ne sera jamais parfaitement mélangé, quel que soit le nombre de mélange que l'on fasse.

Le théorème 0.2.1 a été démontré avec Dave Bayer [1], il y a de cela 15 ans.

J'imagine que le point commun entre l'histoire du mélange d'un jeu de cartes et l'histoire des retenues n'est pas encore très clair pour l'audience. Je vais maintenant expliquer ce point. Voici une nouvelle description du mélange. Prenez  $m$  points  $U_1, \dots, U_m$  selon la loi uniforme et indépendamment dans l'intervalle  $[0, 1]$ , et numérotez les, par ordre croissant

$$x(1) < \dots < x(m).$$

Ainsi  $x(1)$  est le plus petit,  $x(m)$  le plus grand. Maintenant appliquons la transformation de Baker

$$x \mapsto \{2x\},$$

avec  $\{u\}$  donnant la partie fractionnaire de  $u$ . Cette transformation envoie l'intervalle  $[0, 1]$  sur lui-même, et conserve la mesure uniforme et l'indépendance : si  $U$  et  $V$  suivent la loi uniforme et sont indépendantes, leur image par la transformation de Baker ont la même propriété. Si j'applique la transformation à la suite  $x(1), \dots, x(m)$ , les images ne seront plus ordonnées.

- Que fait la transformation de Baker ?

- Elle prend l'intervalle  $[0, 1/2]$  et l'étire sur l'intervalle  $[0, 1]$ ; elle fait la même chose sur la deuxième partie  $[1/2, 1]$ . Pour voir l'ensemble des images des nombres  $x(i)$ , on prend les deux intervalles allongés et on les met l'un sur l'autre. Cela revient à mélanger les nombres  $x(1), \dots, x(m)$  : maintenant les nombres  $x(i)$  apparaissent dans un ordre généralement différent de ce qu'ils étaient avant : il existe une permutation  $\sigma$  telle que le nouvel ordre soit

$$x(\sigma(1)), \dots, x(\sigma(m)).$$

Combien de nombres  $x(i)$  avais-je au début dans l'intervalle  $[0, 1/2]$ ? Eh bien, un nombre aléatoire de loi binomiale  $B(m, 1/2)$  puisque chaque  $U_i$  au début avait 50% de chance d'être dans cet intervalle, indépendamment des autres  $x(i)$ . Il n'est pas difficile de voir et de démontrer que la loi de  $\sigma$  est la même que celle du mélange des cartes que j'ai présenté avant et que j'ai noté  $\mathbb{Q}$ .

De même, je peux définir avec ce modèle un  $b$  mélange : considérez pour  $b \geq 2$  la transformation

$$x \mapsto \{bx\},$$

et regardez la agir sur les  $x(1), \dots, x(m)$ . La permutation induite, la permutation  $\sigma$  telle que  $x(\sigma(1)) < \dots < x(\sigma(m))$  est ce que j'appelle un  $b$ -mélange. Par exemple lorsque  $b = 3$ , ça revient

à couper l'intervalle  $[0, 1]$  en trois,  $[0, 1/3]$ ,  $[1/3, 2/3]$  et  $[2/3, 1]$ , à les étirer sur  $[0, 1]$  et à observer l'ordre des  $x(i)$  obtenus après cette opération. Pour les jeux de cartes, ça revient à couper le jeu en trois parties selon la loi multinomiale de paramètre  $(m, 1/3, 1/3)$ . J'ai maintenant trois mains! Je fabrique un tas, en laissant tomber une carte d'une main, en choisissant cette main, proportionnellement au nombre de cartes qu'elle contient. Autre chose à signaler à propos du  $b$ -mélange; imaginons que vous ayez un gros jeu de cartes. Pour faire un 4-mélange, vous pouvez aussi, faire d'abord 4 tas; faire un mélange des deux premiers, puis des deux autres, et enfin, mélanger les deux paquets obtenus. On se convainc aisément que le résultat est le même qu'un 4-mélange, surtout en réfléchissant à l'aide de la représentation utilisant les applications  $x \mapsto \{bx\}$ . Je note maintenant  $\mathbb{Q}_b$  la loi d'un  $b$  mélange (la distribution  $\mathbb{Q}$  introduite plus haut s'écrit maintenant  $\mathbb{Q}_2$ ).

Le principal résultat que nous avons obtenu avec Dave Bayer est une expression simple de la probabilité d'obtenir une permutation  $\sigma$  donnée lors d'un  $b$ -mélange :

**Théorème 0.2.2.** *La probabilité que le jeu soit dans la position  $\sigma$  après un  $b$ -mélange est*

$$\mathbb{Q}_b(\sigma) = \frac{\binom{m+b-r}{m}}{b^m}$$

où  $r = r(\sigma)$  est le nombre de suites croissantes dans  $\sigma$  (ou de manière équivalente, 1 plus le nombre de suites décroissantes dans  $\sigma^{-1}$ ).

Alors je dois dire maintenant ce qu'est le nombre de suites croissantes dans une permutation. Je vais vous dire cela en terme de jeu de cartes. Votre jeu de cartes est mélangé et disons que vous voyez la suite

$$4, 5, 1, 8, 7, 2, 3, 6.$$

Localisez 1, puis en partant de 1, on voit 2 à droite de 1, puis 3 à droite de 2... mais pas 4. La première suite croissante est 1,2,3. Je la retire, et obtient 4,5,8,7,6; la deuxième suite croissante est 4,5,6; la troisième 7, et la quatrième 8. J'ai ici donc 4 suites croissantes; on peut alors démontrer la deuxième assertion du théorème, à savoir que le nombre de suites croissantes dans  $\sigma$  est, à un près, égale au nombre de suites décroissantes dans  $\sigma^{-1}$ .

Je voudrais maintenant vous donner quelques informations concernant le mélange de cartes.

- Je note  $\mathcal{Q}_b$  la matrice de transition de la chaîne de Markov sur le groupe  $S_m$ , correspondant au mélange; ainsi  $\mathcal{Q}_b(\sigma, \tau)$  est la probabilité, partant de  $\sigma$  d'obtenir  $\tau$  après un  $b$ -mélange<sup>(4)</sup>. La matrice  $\mathcal{Q}_b$  est la matrice de transition d'une chaîne de Markov sur  $S_m$ , qui est un ensemble à  $m!$  éléments, donc  $\mathcal{Q}_b$  est une matrice  $m! \times m!$ . On sait que 1 est valeur propre car c'est une matrice stochastique; eh bien, les valeurs propres de  $\mathcal{Q}_b$  sont  $1, 1/b, 1/b^2, \dots, 1/b^{m-1}$ . D'autre part, ces valeurs propres ont des multiplicités que l'on sait calculer.
- Les vecteurs propres de  $\mathcal{Q}_b$  ne dépendent pas de  $b$
- On a  $\mathcal{Q}_b \star \mathcal{Q}_a = \mathcal{Q}_{ab}$ . C'est-à-dire, si vous faites un  $a$ -mélange suivi d'un  $b$ -mélange, eh bien, c'est comme si vous faisiez directement un  $ab$ -mélange. C'est facile à voir, car il s'agit juste de voir que la composition de  $x \mapsto \{ax\}$  et de  $x \mapsto \{bx\}$  donne  $x \mapsto \{abx\}$ , et d'ailleurs c'est encore plus clair si vous réfléchissez en terme d'intervalle étiré, comme je le disais avant.

---

<sup>4</sup>ndlr : la loi  $\mathbb{Q}_b$  est la loi de la chaîne au temps 1, en partant au temps 0 de permutation identité  $\sigma = (123 \dots m)$

Evidemment, ce dernier point est crucial pour l'analyse de mélanges successifs. Car bien sûr,  $\mathbb{Q}_2^{*k}$  donnant la loi après  $k$ -mélanges, c'est la même chose que  $\mathbb{Q}_2^k$ . Donc si vous connaissez bien les  $a$ -mélanges, vous connaissez tout. C'est crucial.

Eh bien, donc, si vous étiez moi, et que vous sachiez cela, eh bien, vous vous diriez... il doit y avoir un lien, une connexion entre le problème du mélange des cartes, et le problèmes des retenues...

### 0.3 Connexion entre le mélange des cartes et les retenues

Vous vous souvenez, dans la première partie, j'ai appelé  $C_1, \dots, C_k$  le processus des retenues, lorsque j'ajoutais  $m$ -nombres, de décimales (en base  $b$ ) indépendantes. Notons ces variables sous la forme  $C_k^b$  pour faire apparaître la base. Pour décrire la connexion entre les deux problèmes, je pars de  $\sigma_0$  la permutation identité de  $S_m$  et je considère des  $b$ -mélanges successifs de  $\sigma_0$ . J'appelle  $\sigma_1$  un  $b$ -mélange de  $\sigma_0$ ,  $\sigma_2$  un  $b$ -mélange de  $\sigma_1$ , etc, ces  $b$  mélanges étant indépendants. Maintenant je note  $D_0^b = D(\sigma_0) = 0, D_1^b = D(\sigma_1), D_2^b = D(\sigma_2), \dots$  les variables aléatoires donnant les nombres de suites décroissantes dans  $\sigma_0, \sigma_1, \sigma_2, \dots$ . Voici un lien fondamental entre le problèmes du mélange des cartes et celui des retenues :

**Théorème 0.3.1.** (Avec Jason Fulman [5]) Pour tout  $n > 1$  et tout  $b \geq 2$ , les vecteurs  $(D_1^b, \dots, D_n^b)$  et  $(C_1^b, \dots, C_n^b)$  ont même loi (ou encore, les processus  $(D_i, i \geq 1)$  et  $(C_i, i \geq 1)$  ont même loi).

Un corollaire, bien sûr, est que la matrice de Holt donnée en (3) est liée au problème du mélange comme suit

$$P_b\{i, j\} = P(D_{n+1}^b = j \mid D_n^b = i), \quad (5)$$

c'est à dire la suite  $(D_k^b, k \geq 0)$  (donnant la liste des longueurs des suites décroissantes lors de  $b$ -mélanges successifs) est une chaîne de Markov dont la matrice de transitions est cette matrice  $\mathcal{P}_b$  ayant une symétrie centrale, dont j'ai parlé au début.

Il y a une question naturelle qui se pose maintenant :

« quel est le rapport avec le mélange de vraies cartes ? »

Laissez moi raconter cela sous la forme d'un tour de cartes. Voici, je retourne à Nice la semaine prochaine. Imaginez que je vous laisse un jeu de cartes, maintenant, et je vous donne une lettre, contenant un petit script à effectuer lorsque je serai à Nice... Il n'y a donc pas de trucs, vous serez tranquille chez vous, pour l'appliquer, sans surveillance. La lettre dit :

- retirer le jeu de sa boîte.
- couper le jeu, le mélanger.
- couper le jeu, le mélanger.
- couper le jeu, une fois, deux fois, autant que vous voulez.

Je suis sûr que vous ne savez pas ce qu'est la carte du dessus.

Prenez là, et rappelez vous ce qu'elle vaut... et remettez là au milieu du paquet.

- couper et mélanger une dernière fois... et envoyez moi le jeu dans sa boîte par la poste.

Et restez toute la soirée concentré sur votre carte... pour ne pas l'oublier. Et quelque jours après, je vous enverrai un message disant "c'est le 6 de carreau"... et c'était le 6 de carreau !

Alors parlons un peu de ce tour pendant quelques secondes : le jeu que je vous ai donné était arrangé. Je veux dire : disons que je l'ai mélangé, puis que j'ai noté sur un papier l'ordre des cartes... Donc disons, pour l'analyse, mais ça ne change rien, que les cartes soient classés et numérotées de 1 à 52. D'abord, le fait que vous coupiez ne change rien... en terme de permutation, vous appliquez une permutation circulaire... et en fait, vous pouvez imaginer que votre jeu est cyclique, et que finalement, vous ne changez rien. Maintenant, lorsque vous mélangez, le jeu se trouve avoir deux suites croissantes... que vous mélangez n'importe comment (euh... en fait, il peut même y en avoir qu'une, si au lieu de mélanger, vous mettez la deuxième moitié au dessus, comme c'est permis dans ma règle de mélange). Vous coupez encore... pas grave... et vous mélangez. Votre première moitié avait 2 suites croissantes, et la deuxième aussi. Après mélange vous avez maintenant au plus 4 suites croissantes. Trois mélanges vous donnent 8 suites croissantes. Lorsque vous prenez la carte du dessus et que vous la mettez au milieu, ça vous donne une 9ème suite croissante, de taille 1. Alors qu'est-ce que je fais quand je reçois le jeu par la poste ?

Je prends la première carte, disons le 5, je la pose. Si la suivante c'est le 6 je la mets dessus, si c'est le 9 je commence une nouvelle pile. Je continue. Si à un moment donné je prends une carte qui est juste supérieure de 1 à une pile existante, je mets la carte dessus, sinon, je commence une nouvelle pile. Lorsque vous faites cela, vous obtenez 8 piles de taille environ un huitième du jeu, et une pile de taille 1... C'est votre carte ! Vous pouvez essayer... enfin, il est bon de s'entraîner un peu avant, bien sûr...

La morale, bien sûr, c'est que trois mélanges ne sont pas suffisants pour mélanger proprement un jeu de cartes. De la même façon, avec 4 mélanges vous avez 16 suites croissantes, avec 5, 32 suites croissantes, ou plutôt, au plus 32 suites croissantes, et si vous faites le calcul, vous voyez que vous perdez un certain pourcentage des arrangements possibles d'un jeu de cartes, que vous mélangez n'importe comment. Je veux dire, quelle que soit la taille des deux parties que vous choisissiez... Donc 5 mélanges ne sont pas suffisants pour mélanger proprement 52 cartes. La distance avec la loi uniforme est toujours autour au mieux à distance 0,9. Si vous êtes intéressés par le bridge, vous pouvez me poser des questions... car il y a une très jolie illustration de ce que je viens de dire au bridge. <sup>(5)</sup>

---

Je viens juste de montrer qu'il y avait une connexion entre le mélange des cartes, et l'histoire des retenues. Voici maintenant ma contribution à l'étude de la connection entre les deux sujets. Voici quelques faits. Supposons que l'on ajoute  $m$  nombres aléatoires en base  $b$ , la valeur moyenne de la retenue dans la  $k^{\text{ème}}$  colonne est

$$\mathbb{E}(C_k) = \frac{m-1}{2}(1-b^{-k}), \quad \text{pour } k = 0, 1, 2, \dots$$

rappelons que l'on a posé  $C_0 = 0$ , par convention. L'asymptotique de la valeur de la  $k^{\text{ème}}$  retenue, lorsque  $k \rightarrow +\infty$  est donc aisée, ça donne  $(m-1)/2$ . Cela donne aussi le nombre moyen de retenues dans les  $k$  premières colonnes :

$$\frac{m-1}{2} \left( k - \frac{1}{b-1}(1-b^{-k}) \right).$$

Cette formule est obtenue par sommation de la précédente. On peut aussi calculer la variance. Il y a aussi un théorème de la limite centrale, qui dit que les fluctuations du nombre de retenues

---

<sup>5</sup>ndlr : s'adresser directement à l'orateur qui n'est pas revenu sur cette illustration...

suit la loi Gaussienne. On voit que la  $k^{\text{ème}}$  retenue a pour moyenne  $\frac{m-1}{2}(1 - b^{-k})$  et que petit à petit le comportement des retenues s'approche d'un comportement stationnaire.

Il y a en fait un contrôle très précis de la vitesse de convergence vers la loi stationnaire que l'on peut traduire par :

le processus des retenues est proche de la loi stationnaire après  $k = \log_b(m)$  pas.

Plus précisément, on peut prouver que

$$\frac{1}{2} \sum_{j=0}^{m-1} \left| P(C_k = j) - \frac{\langle \begin{smallmatrix} m \\ j \end{smallmatrix} \rangle}{m!} \right| \leq \frac{1}{2} \sqrt{e^{1/c^2} - 1} \sim \frac{1}{2c} \quad (6)$$

pour  $k = \lceil \log_b(cm) \rceil$ . Ceci donne un contrôle très précis de cette vitesse de convergence.

Pour notre contribution au lien entre l'étude des retenues et celui du mélange des cartes, on peut ajouter encore quelques mots. On a vu qu'il fallait mélanger  $\frac{3}{2} \log_2 m$  fois un paquet de  $m$  cartes pour le mélanger "correctement". On peut se demander que valent certaines caractéristiques du jeu de cartes à ce moment là, ou plutôt combien faut-il de temps pour que certaines caractéristiques ressemblent à celle d'un jeu sous la loi uniforme. Ainsi, on peut montrer que le nombre de descentes "à la bonne distribution" après  $\log_b m$  mélanges, que la longueur de la plus grande suite croissante a la bonne distribution après  $\frac{5}{6} \log_2 m$ ; si on s'intéresse maintenant à la structure de cycle de la permutation  $(a_1(\sigma), a_2(\sigma), \dots, a_m(\sigma))$  donnant le nombre de cycle de longueur 1, 2, ...,  $m$ , eh bien, n'importe qu'elle suite  $k_m$  de mélange,  $k_m \rightarrow \infty$  avec  $m$  convient : par exemple, si vous prenez un grand jeu de cartes, vous le mélangez  $\log \log \log m$  fois, et votre jeu a, en ce qui concerne la distribution de ses longueurs de cycle, la bonne distribution (il s'agit bien sûr, d'une propriété asymptotique). En fait, pour des raisons simples, si vous vous intéressez juste à la longueur du plus grand cycle, elle a la bonne distribution après un seul mélange. D'autre question, par exemple, combien de temps faut il pour que l'as de pique soit bien mélangé (ait une loi uniforme dans le paquet), pour mélanger les cartes rouges et noires, etc? Eh bien il faut mélanger  $\log_2 m$  fois le paquet.

## 0.4 Liens avec la combinatoire algébrique

On a parlé des liens entre l'étude des retenues et celui du problème du mélange des cartes. La chose que je veux faire maintenant et de parler de combinatoire algébrique; c'est le domaine dans lequel on trouvera les outils nécessaires pour faire les calculs. Voici donc un peu de combinatoire algébrique, on va parler de fonctions de Schur.

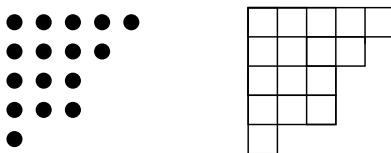


FIG. 1 – Représentations d'une partition de 16

Une partition  $\lambda$  de  $n$  est une liste décroissante d'entiers strictement positifs de somme  $n$ . On représente une telle partition  $\lambda$  souvent par un ensemble de points ou un ensemble de cases,

comme sur la Figure 1 ; on note  $\lambda \vdash n$ . Sur le dessin, on a la partition  $(5,4,3,3,1)$  et on note donc  $(5,4,3,3,1) \vdash 16$ . Le dessin constitué de cases et représentant la partition est appelé tableau, ou diagramme de Ferrer.

Un tableau de Young standard de forme  $\lambda$ , partition de  $n$ , est la donnée d'un remplissage des cases du tableaux  $\lambda$  par tous les entiers de 1 à  $n$ , tel que :

- sur chaque ligne (de gauche à droite) les entiers croissent,
- sur chaque colonne (de haut en bas) les entiers croissent.

En voici un exemple sur la figure 2. Le nombre de tableaux de Young standard de forme  $\lambda$  est

1	2	3	5	8
4	7	10	13	
6	9	14		
11	15	16		
12				

FIG. 2 – Exemple de tableau de Young standard

noté  $f(\lambda)$ .

Je dois aussi introduire la notion de tableau de Young semi-standard ; la différence est que cette fois, dans le remplissage on autorise les répétitions de nombres ; les conditions de croissance sur les lignes et colonnes changent aussi :

- sur chaque ligne (de gauche à droite) les entiers croissent au sens large,
- sur chaque colonne (de haut en bas) les entiers croissent strictement.

Par exemple, les tableaux semi-standards associés à la partition  $\lambda = (2, 1)$  sont

1	1	1	1	1	2	1	2	1	3	1	3	2	2	2	3
2		3		2		3		2		3		3		3	

On a le droit qu'aux nombres 1,2,3, ce qui garantit la finitude du nombre des tableaux de forme donnée. On note  $TYSS(\lambda)$  l'ensemble des tableaux de Young semi-standards de forme  $\lambda$ .

Voici maintenant la définition du polynôme (ou fonction) de Schur  $s_\lambda$  :

$$s_\lambda(x_1, \dots, x_n) = \sum_{T \in TYSS(\lambda)} x^T$$

où  $x^T = \prod_{i=1}^n x_i^{T_i}$ , où  $T_i$  est le nombre de fois où le nombre  $i$  apparaît dans le tableau  $T$  ; par exemple, en utilisant la liste donnée plus haut, on obtient

$$s_{2,1}(x_1, x_2, x_3) = x_1^2 x_2 + x_1^2 x_3 + x_1 x_2^2 + 2x_1 x_2 x_3 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2.$$

En fait, les polynômes de Schur sont des polynômes symétriques (ce qui n'apparaît pas clairement dans leur définition). L'ensemble des polynômes associés aux partitions de  $n$  forme une base de l'ensemble des polynômes symétriques sur  $n$  variables. Il y a beaucoup d'endroits où les polynômes de Schur jouent un rôle en mathématiques, en combinatoire, en théorie de représentation des groupes, dans l'étude des polynômes symétriques, bien sûr. Il s'avère, et cela peut paraître étonnant si on ne l'a pas vu avant, que les polynômes de Schur ont aussi à voir avec le processus des retenues et le mélange des cartes.

Voici un fait standard, que je vais illustrer sur un exemple et qui s'appelle la correspondance de Schensted. Elle associe à toute permutation  $\sigma$  de  $S_n$  un couple de tableaux de Young

standard, de même forme (associé à la même partition) et ce, de manière bijective. On va voir cela sur un exemple. Je prends la permutation

$$\sigma = (976851432).$$

Je vais d'abord construire ce qu'on appelle le tableau  $\mathbf{P}(\sigma)$ . Voyez ça comme l'arrangement d'un jeu de cartes, numérotées de 1 à 9. Maintenant on va jouer à une sorte de jeu de solitaire. Je retourne les cartes une à une. Et les règles sont les suivantes : je vais fabriquer des piles de cartes. Je peux mettre une petite carte sur une grosse, un 5 sur un 10 , par exemple. Mais si je retourne une carte qui est plus grosse que toutes les cartes du dessus, je dois créer une nouvelle pile.

D'abord, je mets le 9, ça donne

9
---

puis je mets le 7 sur le 9 ça donne

7
9

puis je mets le 6 sur le 7 ça donne

6
7
9

Le 8 arrive, on doit créer une nouvelle pile : on ne peut pas le mettre sur le 6, ça donne

6	8
7	
9	

Maintenant, le 5 ; l'objet du jeu est de créer le moins de pile possible. Il est facile de voir que la stratégie optimale est de mettre la carte sur la pile la plus à gauche possible. Donc, on le met sur le 6, ça donne

5	8
6	
7	
9	

On dit que le 5 pousse le 6 qui pousse le 7, puis le 9. Ensuite, le 1. On a

1	8
5	
6	
7	
9	

puis le 4

1	4
5	8
6	
7	
9	

Maintenant, si on fait pareil avec le 3, on va avoir

1	3
5	4
6	8
7	
9	

Ce n'est pas ce qu'on veut : on veut que ce soit croissant sur les lignes (c'est une règle supplémentaire). La règle générale est donc la suivante : une carte arrivant sur une ligne où elle est la plus grande se met tout à droite. Si elle n'est pas la plus grande, elle prend la place de la carte la plus petite qui lui soit supérieure. Cette carte est envoyée sur la ligne en dessous... et ça recommence en dessous, jusqu'au moment où tout le monde a trouvé une place. <sup>(6)</sup>.

Donc, ici, la carte 4 arrivant en deuxième ligne prend la place du 5, et l'éjecte sur la ligne suivante. Ça donne finalement

1	3
4	8
5	
6	
7	
9	

puis le 2 arrive, pousse le 3 qui doit prendre la place du 4, et ça donne

$$\mathbf{P}(\sigma) = \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & 8 \\ \hline 4 & \\ \hline 5 & \\ \hline 6 & \\ \hline 7 & \\ \hline 9 & \\ \hline \end{array}$$

(le 2 pousse le 3 qui doit éjecter le 4, celui ci en montant pousse le 5, qui pousse le 6...).

Le deuxième tableau associé à la permutation, est une sorte de tableau de « réservation ». C'est un tableau, nommé  $\mathbf{Q}(\sigma)$ , qui grossit en même temps que  $\mathbf{P}(\sigma)$ , de la même manière (à chaque instant il a la même forme), et qui est rempli par les nombres de 1 à 9, de sorte que la case ajoutée au temps  $i$ , contienne le nombre  $i$ .

Ici ça donne ça :

$$\boxed{1} \quad \text{puis} \quad \begin{array}{|c|} \hline 1 \\ \hline 2 \\ \hline \end{array} \quad \text{puis} \quad \begin{array}{|c|c|} \hline 1 & \\ \hline 2 & \\ \hline 3 & \\ \hline \end{array} \quad \text{puis} \quad \begin{array}{|c|c|} \hline 1 & 4 \\ \hline 2 & \\ \hline 3 & \\ \hline \end{array}$$

et finalement

$$\mathbf{Q}(\sigma) := \begin{array}{|c|c|} \hline 1 & 4 \\ \hline 2 & 7 \\ \hline 3 & \\ \hline 5 & \\ \hline 6 & \\ \hline 8 & \\ \hline 9 & \\ \hline \end{array} .$$

---

<sup>6</sup>ndlr : cette construction s'appelle le jeu de taquin en combinatoire ; voir [6] pour un aperçu de l'importance de cette construction en combinatoire algébrique

Ainsi, cette construction associe à chaque permutation une paire  $(\mathbf{P}(\sigma), \mathbf{Q}(\sigma))$  de tableaux de Young standard de même forme ; et cela est une bijection. Si vous me donnez une paire  $(\mathbf{P}, \mathbf{Q})$  de tableaux de Young standard de même forme, alors il existe une seule permutation  $\sigma$ , qui permet de les fabriquer par cette méthode, c'est-à-dire pour laquelle  $(\mathbf{P}(\sigma), \mathbf{Q}(\sigma)) = (\mathbf{P}, \mathbf{Q})$ . L'une des très nombreuses conséquences de cette bijection, est une formule liée aux représentations irréductibles du groupe des permutations, qui dit que

$$\sum_{\lambda: \lambda \vdash n} f(\lambda)^2 = n! \quad (7)$$

où  $f(\lambda)$  est le nombre de tableaux de Young de forme  $\lambda$ , la somme portant sur les partitions  $\lambda$  de  $n$ . La correspondance de Schensted a de très nombreuses propriétés magiques ; si vous êtes combinatoriste, un spécialiste de combinatoire algébrique, vous savez en particulier la chose suivante. Une permutation a une descente en  $i$ , si  $\sigma(i+1) < \sigma(i)$  (notion déjà vue dans la Section 0.3). Dans la permutation suivante, j'ai souligné là où il y avait des descentes :

$$\underline{9} \ \underline{7} \ 6 \ \underline{8} \ \underline{5} \ 1 \ \underline{4} \ \underline{3} \ 2.$$

Je dis maintenant qu'un tableau de Young a une descente en  $i$  si le nombre  $i+1$  se trouve dans une ligne plus basse que  $i$ . Voici avec une étoile les descentes en les nombres concernés dans  $\mathbf{Q}(\sigma)$ ,

$$\mathbf{Q}(\sigma) := \begin{array}{|c|c|} \hline 1^* & 4^* \\ \hline 2^* & 7^* \\ \hline 3 & \\ \hline 5^* & \\ \hline 6 & \\ \hline 8^* & \\ \hline 9 & \\ \hline \end{array} .$$

Une des propriétés de la bijection de Schensted est que le nombre de descentes dans la permutation  $\sigma$  et dans le tableau  $\mathbf{Q}(\sigma)$  sont égales :

$$D(\sigma) = \#\{\text{descentes de } \mathbf{Q}(\sigma)\}. \quad (8)$$

Une autre conséquence, moins familière, mais présente dans la littérature, lie la théorie du mélange des cartes à la théorie des fonctions symétriques. Une application de cela est la suivante : prenons un jeu de  $n$  cartes ordonnées, appliquons lui un  $b$ -mélange  $k$  fois, et observons la permutation correspondante  $\sigma$ , et plus précisément, le tableau de « réservation »  $\mathbf{Q}(\sigma)$ . On s'intéresse à  $\mathbb{Q}_{b^k}(\mathbf{Q}(\sigma) = T)$ , la probabilité que le tableau en question soit égal à un tableau  $T$  que l'on s'est donné à l'avance,  $T$  étant de forme  $\lambda$ . Eh bien, on a

$$\mathbb{Q}_{b^k}(\mathbf{Q}(\sigma) = T) = s_\lambda \left( \frac{1}{b^k}, \dots, \frac{1}{b^k} \right),$$

la fonction de Schur associée à  $\lambda$ , évaluée en les  $1/b^k$ . Ainsi, une autre conséquence est que les nombres Eulériens,  $\left\langle \begin{smallmatrix} m \\ j \end{smallmatrix} \right\rangle$  comptant les permutations de  $m$  éléments ayant  $j$  descentes, vérifient

$$\left\langle \begin{smallmatrix} m \\ j \end{smallmatrix} \right\rangle = \sum_{\lambda: \lambda \vdash m} f(\lambda) f_j(\lambda) \quad (9)$$

où  $f_j(\lambda)$  est le nombre de tableau standard de Young possédant  $j$  descentes. En fait, c'est une conséquence claire de la formule (8).

J'aimerais maintenant, en vous montrant quelques calculs (mais ce sont les seuls dans mon exposé), vous montrer comment, ce que je viens de dire, permet de montrer mon théorème.

Je regarde la distance en variation entre la loi des retenues, à la mesure de probabilité stationnaire. Rappelons que  $P_b(C_k = j)$  est la probabilité que la  $k^{\text{ème}}$  retenue est  $j$  quand j'ajoute des nombres. Retranchons la loi stationnaire (souvenez vous de (3)), et sommons sur  $j$  (ça donne le membre de gauche de la formule suivante). Or, je dis que ceci c'est exactement la même chose que la probabilité qu'un  $b^k$  mélange de  $m$  cartes possède  $j$  descentes. On obtient donc la formule suivante.

$$\sum_{j=0}^{m-1} \left| P_b(C_k = j) - \frac{\langle m \atop j \rangle}{m!} \right| = \sum_{j=0}^{m-1} \left| \mathbb{Q}_{b^k}(\#\text{descentes}(\mathbf{Q}(\sigma) = j) - \frac{\langle m \atop j \rangle}{m!}) \right|.$$

En utilisant une formule (9), ça donne

$$= \sum_{j=0}^{m-1} \left| \sum_{\lambda: \lambda \vdash n} f_j(\lambda) s_\lambda \left( \frac{1}{b^k}, \dots, \frac{1}{b^k} \right) - \frac{f(\lambda) f_j(\lambda)}{m!} \right|$$

Je rentre la valeur absolue sous la deuxième somme, factorise un peu, ça donne la borne supérieure suivante

$$\leq \sum_{\lambda: \lambda \vdash n} \left| s_\lambda \left( \frac{1}{b^k}, \dots, \frac{1}{b^k} \right) - \frac{f(\lambda)}{m!} \right| \sum_{j=0}^{m-1} f_j(\lambda)$$

Cette dernière somme, tout à droite fait  $f(\lambda)$ , ça donne

$$= \sum_{\lambda: \lambda \vdash n, |\lambda|=n} \left| f(\lambda) s_\lambda \left( \frac{1}{b^k}, \dots, \frac{1}{b^k} \right) - \frac{f^2(\lambda)}{m!} \right|.$$

On utilise alors l'inégalité de Cauchy-Schwarz,

$$\leq \left( \sum_{\lambda: \lambda \vdash n} \left| s_\lambda \left( \frac{1}{b^k}, \dots, \frac{1}{b^k} \right) - \frac{f(\lambda)}{m!} \right|^2 \sum_{\lambda, |\lambda|=n} f^2(\lambda) \right)^{1/2}.$$

ce qui par la formule (7) est égal à

$$\leq \left( \sum_{\lambda: \lambda \vdash n} \left| s_\lambda \left( \frac{1}{b^k}, \dots, \frac{1}{b^k} \right) - \frac{f(\lambda)}{m!} \right|^2 m! \right)^{1/2}.$$

Maintenant on utilise des choses qui sont connues sur les fonctions de Schur, et on obtient

$$= \left( \sum_{\lambda: \lambda \vdash n} s_\lambda^2 \left( \frac{1}{b^k}, \dots, \frac{1}{b^k} \right) - 1 \right)^{1/2} = \left( \prod_{i=1}^{m-1} \left( 1 + \frac{i}{b^{2k}} \right) - 1 \right)^{1/2} \quad (10)$$

$$\leq \left( e^{\binom{m}{2}/b^{2k}} - 1 \right)^{1/2} \quad (11)$$

Et voilà, ça démontre ce que je voulais sur la vitesse de convergence vers la loi stationnaire, à la fois pour les retenues et pour le nombre de descentes lors du mélange des cartes.

Voici aussi quelque chose que je voulais faire remarquer : en fait, tout cela n'utilise pas grand chose. Il n'y a pas là dedans d'invention particulière, juste l'utilisation de combinatoire bien connue. Ainsi, pour résoudre ce problème, il ne s'agissait pas de sortir une grande théorie, mais bien d'utiliser une théorie existante, connue par les combinatoristes. Aussi, je voudrais dire que je ne connais aucune autre approche à ce problème, en particulier, je ne connais aucune approche uniquement probabiliste. Je voudrais ajouter quelques petites choses, qui viennent de sortir, et dont on m'a parlé un jour où j'exposais ces résultats devant un parterre de combinatoristes. Prennez une suite de nombres réels  $(a_j, j \geq 0)$  tel que la série  $S(x) = \sum_{j \geq 0} a_j x^j$  soit rationnelle, et s'écrive sous la forme

$$S(x) = \frac{h(x)}{(1-x)^d};$$

on s'intéresse maintenant, pour un certain  $r$  fixé, à la série  $S_r(x)$  associée à la sous-suite  $(a_{jr}, j \geq 0) = (a_0, a_r, a_{2r}, a_{3r}, \dots)$ , autrement dit :

$$S_r(x) = \sum_{j \geq 0} a_{jr} x^j.$$

Eh bien, il s'avère que cette série est encore rationnelle, et s'écrit

$$S_r(x) = \frac{h^{<r>}(x)}{(1-x)^d}$$

avec comme vous le voyez le même dénominateur, et le numérateur  $h^{<r>}$  lui, est un autre polynôme, mais du même degré que  $h$  (cf. F. Brenti, V. Welker [3]). En fait, il s'avère que la fonction

$$h \rightarrow h^{<r>}$$

est linéaire (de l'espace des polynômes sur lui même). Il s'agit donc « d'une matrice ». C'est-à-dire, un polynôme est un vecteur (ses coefficients forment un vecteur), et notre application agissant linéairement sur iceux, agit bien sûr comme la multiplication par une matrice. Cette matrice, en fait, est essentiellement la matrice des retenues que l'on a vue plus haut (en fait, il faut effacer des lignes, mais c'est ça).

En conclusion – et cela peut-être sera-t-il intéressant pour les plus jeunes mathématiciens – je voudrais dire premièrement que l'on peut trouver des mathématiques partout : en ajoutant des nombres, en mélangeant des cartes. La deuxième chose que je souhaitais dire, concerne la manière d'apprendre les mathématiques, et ceci spécialement en France. Pour faire des mathématiques, on apprend des tas de choses, de l'algèbre, de l'analyse, de la topologie algébrique, de la combinatoire algébrique, etc. Il y a une autre manière de faire des mathématiques : trouver un problème qui vous intéresse, et y réfléchir. Ce n'est pas une manière très française de faire les choses. Bien sûr, la machinerie est importante : j'ai juste utilisé la machinerie de la combinatoire algébrique, mais vous voyez c'est le problème qui m'a amené à cela. Bien sûr, on peut faire des maths conceptuellement, en ne partant de rien, et faire des théories abstraites très intelligentes. Mais on peut aussi, comme Schensted l'a fait, partir d'un problème très simple. Je voudrais dire comment s'est passée la découverte de Schensted. Il travaillait dans le bureau à côté de celui de Don Knuth qui étudiait la combinatoire du jeu du solitaire. Schensted, qui essayait de comprendre la taille de la plus grande sous-suite croissante dans une permutation

a vu qu'un jeu similaire au solitaire, en l'occurrence, le jeu de taquin, donnait sous la forme du nombre de piles restantes, la longueur de cette suite.<sup>(7)</sup> Il a vu ensuite, qu'en faisant en même temps le tableau des réservations,  $\mathbf{Q}(\sigma)$ , on obtenait une bijection. C'est en se représentant un jeu de solitaire que Schensted a pensé à sa correspondance.

---

<sup>7</sup>ndlr : en fait la longueur de la plus grande sous-suite croissante dans une permutation  $\sigma$  est égale à la longueur de la première ligne (la plus longue) dans le tableau de Young  $\mathbf{P}(\sigma)$  associé.

# Bibliographie

- [1] D. BAYER, P. DIACONIS, *Trailing the Dovetail Shuffle to Its Lair*, Annals of Applied Probability, volume 2, p. 294-313, (1992).
- [2] P. Brémaud, *Markov chains. Gibbs fields, Monte Carlo simulation, and queues*, Texts in Applied Mathematics. New York, NY : Springer. xviii, 444 p.
- [3] F. BRENTI, V. WELKER, *The Veronese construction for formal power series and graded algebras*, Advances in Applied Mathematics, Volume 42, Issue 4, May 2009, Pages 545-556.
- [4] P. DIACONIS *Mathematical developments from the analysis of riffle shuffling*, [www-stat.stanford.edu/~cgates/PERSI/papers/Riffle.pdf](http://www-stat.stanford.edu/~cgates/PERSI/papers/Riffle.pdf)
- [5] P. DIACONIS, J. FULMAN, *Carries, shuffling, and symmetric functions*, <http://arxiv.org/abs/0902.0179> (2009)
- [6] W. Fulton, *Young tableaux*. Reprinted with corrections. - Cambridge University Press, 1999. - (London Mathematical Society Student Texts).
- [7] J. HOLT, *Carries, combinatorics and an amazing matrix*, Amer. Math. Monthly 104, p. 138-142, (1997).