« Le problème des rencontres »

E. Kowalski
ETH Zürich

Andrew Granville's 60th BirthDay

CRM - Montréal
Septembre 2022

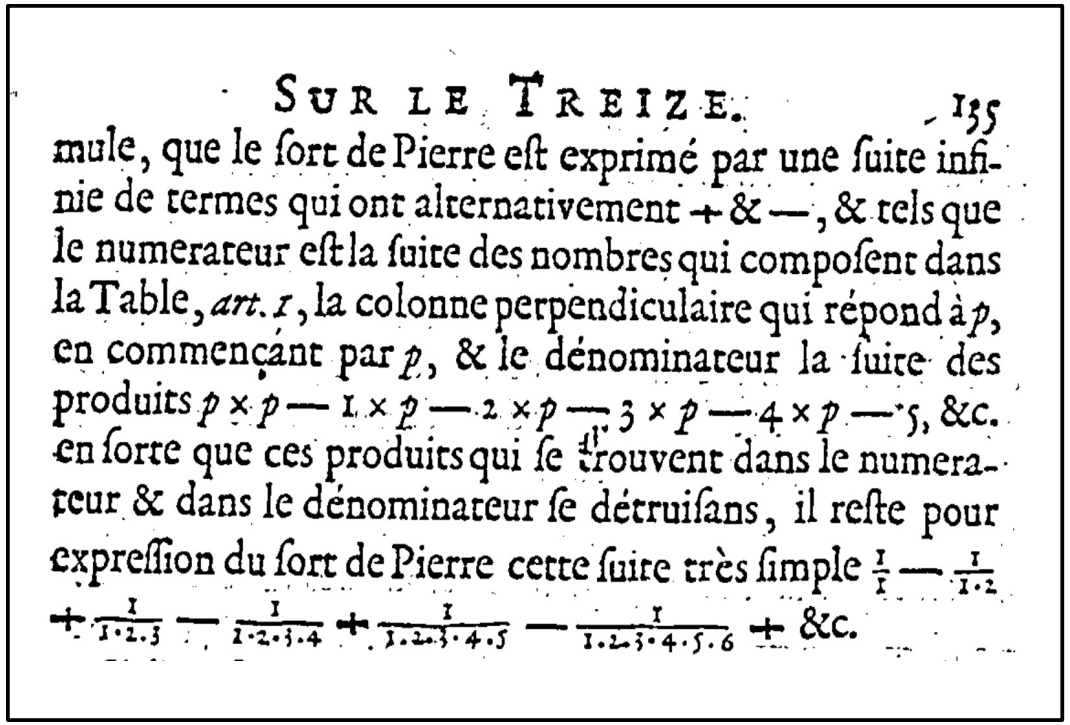
(Version anglaise:
https://www.math.ethz.ch/~kowalski/granville.pdf)

« Le problème des rencontres »

(1708 — 1750 ;
P. de Montmort
N. Bernoulli I
A. de Moivre)

(1) Un des premiers problèmes concernant les permutations aléatoires

(2) Première apparition de la loi de Poisson



SUR LE TREIZE. 135

mule, que le ſort de Pierre eſt exprimé par une ſuite infinie de termes qui ont alternativement + & —, & tels que le numerateur eſt la ſuite des nombres qui compoſent dans la Table, *art.* 1, la colonne perpendiculaire qui répond à p, en commençant par p, & le dénominateur la ſuite des produits $p \times p - 1 \times p - 2 \times p - 3 \times p - 4 \times p -$ 5, &c. en ſorte que ces produits qui ſe trouvent dans le numerateur & dans le dénominateur ſe détruiſans, il reſte pour expreſſion du ſort de Pierre cette ſuite très ſimple $\frac{1}{1} - \frac{1}{1 \cdot 2} + \frac{1}{1 \cdot 2 \cdot 3} - \frac{1}{1 \cdot 2 \cdot 3 \cdot 4} + \frac{1}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} - \frac{1}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6}$ + &c.

Th. X_n uniforme sur $\mathfrak{S}_n$

$\mathrm{Fix}(\sigma) = \{\text{pts fixes de } \sigma\}$

$|\mathrm{Fix}(X_n)| \xrightarrow[n \to \infty]{\text{loi}} P_1$.

P_1 : loi de Poisson de paramètre 1

« Le problème des rencontres »

(1708 — 1750 ;
P. de Montmort
N. Bernoulli I
A. de Moivre)

(1) Un des premiers problèmes concernant les permutations aléatoires

(2) Première apparition de la loi de Poisson

Th. X_n uniforme sur $\mathfrak{S}_n$

$$\mathrm{Fix}(\sigma) = \{\text{pts fixes de } \sigma\}$$

$$|\mathrm{Fix}(X_n)| \xrightarrow[n\to\infty]{\text{loi}} P_1.$$

P_1 : loi de Poisson de paramètre 1

PROBLEM XXXV.

Any number of Letters a, b, c, d, e, f, &c. *all of them different, being taken promiſcuouſly as it happens : to find the Probability that ſome of them ſhall be found in their places according to the rank they obtain in the Alphabet ; and that others of them ſhall at the ſame time be diſplaced.*

SOLUTION.

Let the number of all the Letters be $= n$; let the number of thoſe that are to be in their places be $= p$, and the number of thoſe that are to be out of their places $= q$. Suppoſe for brevity's ſake $\frac{1}{n} = r$, $\frac{1}{n \cdot n-1} = s$, $\frac{1}{n \cdot n-1 \cdot n-2} = t$, $\frac{1}{n \cdot n-1 \cdot n-2 \cdot n-3} = v$, &c. then let all the quantities 1, r, s, t, v, &c. be written down with Signs alternately poſitive and negative, beginning at 1, if p be $= 0$; at r, if p be $= 1$: at s, if p be $= 2$, &c. Prefix to theſe Quantities the Coefficients of a Binomial Power, whoſe index is $= q$; this being done, thoſe Quantities taken all together will expreſs the Probability required. Thus the Probability that in 6 Letters

Autrement dit : pour tout entier $k \geq 0$, on a :

$$\lim_{n\to\infty} \frac{1}{n!} \left| \{ \sigma \in \mathfrak{S}_n \mid |\mathrm{Fix}(\sigma)| = k \} \right| = \frac{1}{e} \frac{1}{k!}.$$

Preuve – Par comptage explicite : pour $k \geq 0$, le nombre de $\sigma \in S_n$ avec $|\mathrm{Fix}(\sigma)| = k$ est

$$\binom{n}{k} D_{n-k}, \qquad D_n = |\{ \sigma \in S_n \mid \mathrm{Fix}(\sigma) = \emptyset \}|.$$

Mais $D_n = n! - n \cdot (n-1)! + \frac{n(n-1)}{2} (n-2)! - \dots$

par inclusion – exclusion, donc la probabilité d'avoir $|\mathrm{Fix}(\sigma)| = k$ est $\frac{1}{\cancel{n!}} \frac{\cancel{n!}}{k! \cancel{(n-k)!}} \cdot \cancel{(n-k)!} \left(1 - 1 + \frac{1}{2} - \frac{1}{6} + \dots\right) \longrightarrow \frac{1}{e} \frac{1}{k!}$.

CQFD

Une preuve ... festive

(extrait de travaux en cours avec A. Forey et J. Fresán)

Étape 1 - (Interprétation)

$n \geq 1$, $\sigma \in \mathfrak{S}_n$

$$|\mathrm{Fix}(\sigma)| = \mathrm{Tr}(u_\sigma),$$ u_σ matrice de permutation $n \times n$

Étape 2 - (Test de convergence)

D'après la méthode des moments il suffit de démontrer :

Prop. $k \geq 0$ entier

$$\frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} |\mathrm{Fix}(\sigma)|^k \xrightarrow[n \to +\infty]{} \mathbb{E}\left(P_1^k\right).$$

Étape 3 - (Algèbre / représentations linéaires)

On sait que

$$\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}|\mathrm{Fix}(\sigma)| = \text{dimension du sous-espace de } \mathbb{C}^n \text{ invariant par } \{u_\sigma\}$$

Mieux :

$$\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}|\mathrm{Fix}(\sigma)|^k = \text{dimension du sous-espace de } \mathbb{C}^{n^k} \text{ invariant par } \{u_\sigma^{\otimes k}\}$$

(σ permute les $\{1,\dots,k\}\to\{1,\dots,n\}$, et on regarde la matrice de permutation de taille n^k)

« Then felt I like some watcher of the skies
When a new planet swims into his ken »

(J. Keats)

Étape 4 -

Pour t une indéterminée, Deligne[2004] / Knop[2007]

ont défini « le groupe symétrique $\mathfrak{S}_t$ »

⟶ « matrices de permutation de taille t »

⟶ dimension du « sous-espace invariant »

au sens usuel !

Propriété 1 : on peut « spécialiser » t en n, et la dimension **diminue** :

$$\dim\left(\text{ss-espace de } \mathbb{C}^{n^k} \text{ invariant}\right) \leq \dim\left(\text{ss-espace de } \mathbb{C}^{t^k} \text{ invariant}\right)$$

avec **égalité** si (et seulement si)

$$k \leq n.$$

Propriété 2 : il y a une base canonique du sous-espace invariant de $\mathbb{C}^{t^k}$ formé par l'ensemble des partitions de $\{1, \ldots, k\}$.

Par conséquent :

$$\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}|Fix(\sigma)|^k \xrightarrow{n\to\infty} b_k$$

$$(= \text{si } n\geq k)$$

où b_k est ce nombre de partitions.

Mais $b_k = \mathbb{E}(P_1^k)$

d'où le théorème.

[par exemple, ces deux suites vérifient la récurrence

$$a_{k+1} = \sum_{j=0}^{k}\binom{k}{j}a_j \;]$$

(Coïncidence des moments : observée par Diaconis et Shahshahani en 1994).

Cette preuve est-elle honnête ?

(+ε)

(1) Elle se généralise « mutatis mutandis » à beaucoup d'autres situations. Par exemple : Forey - Fresán - K.

Th. (Fulman, 1997 ; Fulman - Stanton, 2016)

E corps fini

Y_n uniforme sur $GL_n(E)$ (resp. sur $Aff_n(E)$)

$|\mathrm{Ker}(1_n - Y_n)| \xrightarrow[\text{loi}]{n\to\infty} F_E$, où F_E est caractérisée par (resp. $|\mathrm{Fix}(Y_n)|$)

$\mathbb{E}(F_E^k) =$ nb. de sous-espaces de E^k. (resp. ss-espaces affines)

$(k \geq 0)$

(2) La preuve donne une idée d'où vient la limite (« image par la trace de la mesure de proba. uniforme sur $\mathcal{C}_t$ »)

(3) Mais il reste des questions...

(i) Quid de $Sp_{2n}(E)$?

(ii) Quid du nombre de 2-cycles dans σ ? de 3-cycles ?

(4) Et pour conclure...

Spéculations arithmétiques...

Th. (Frobenius ; Chebotarev) —

$g \in \mathbb{Z}[X]$, $\deg(g) = n$, $Gal(g) \simeq \mathfrak{S}_n$

$|\{ x \bmod p \mid g(x) = 0 \}| \longrightarrow |Fix(\sigma)|$, $\sigma \in \mathfrak{S}_n$

moyenne sur $p \leq x$, $x \to +\infty$

$Sg(p)$

(**Raison :** $Z_p = \{$racines de g dans $\overline{\mathbb{F}_p}\}$, $|Z_p| = n$

$x \longmapsto x^p$ permute $Z_p \rightsquigarrow \sigma_p \in \mathfrak{S}_n$

$\{\sigma_p \mid p \leq x\} \xrightarrow[x \to \infty]{}$ σ uniforme)

Gageure : Faire apparaître $\mathfrak{S}_t$ à la place...

Pseudopolynôme

Soit $f(n) = \lfloor en! \rfloor = 1 + n + n(n-1) + \cdots$

La fonction f est un «pseudo-polynôme»:

$f \bmod q : \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z}$ a un sens ($q \geq 1$ entier).

Conjecture (K. – Sound):

$$\left| \{ x \bmod p \mid f(x) = 0 \bmod p \} \right| \longrightarrow P_1 \left(= |\mathrm{Fix}(\sigma)|, \sigma \in G_t \right)$$

Numériquement : $p \leq 10^6$

k	1	2	3	4
moment	0,99671	1,9964	5,0034	15,054