The problem of coincidences

E. Kowalski

ETH Zürich

Andrew Granville's 60th birthday
CRM-Montréal, September 2022

“The problem of coincidences”

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

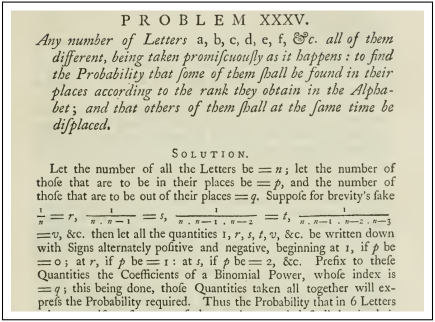
(1) One of the first problems concerning random permutations.

(2) First appearance of the Poisson distribution.

Theorem. X_n uniform on $\mathfrak{S}_n$.
Fix$(\sigma) = \{$fixed points of $\sigma\}$

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

where P_1 is a Poisson distribution with parameter 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

In other words: for any integer $k \geqslant 0$, we have

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

Proof. By explicit counting: for $k \geqslant 0$, the number of $\sigma \in \mathfrak{S}_n$ with $|\mathrm{Fix}(\sigma)| = k$ is $\binom{n}{k} D_{n-k}$, $D_n = |\{\sigma \in \mathfrak{S}_n \mid \mathrm{Fix}(\sigma) = \emptyset\}$.

But

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

by inclusion-exclusion, so the probability that $|\mathrm{Fix}(\sigma)| = k$ is

$$\frac{1}{n!} \cdot \frac{n!}{k!(n-k)!} \cdot (n-k)! \cdot \Big(1 - 1 + \frac{1}{2} - \frac{1}{6} + \cdots\Big) \to \frac{1}{e}\frac{1}{k!}.$$

A... “festive” proof

(From ongoing joint work with A. Forey and J. Fresán)

Step 1. (Interpretation)

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

$$|\mathrm{Fix}(\sigma)| = \mathrm{Tr}(u_\sigma)$$

where u_σ is the $n \times n$ permutation matrix.

Step 2. (Convergence criterion)

According to the *method of moments*, it is enough to prove:

Proposition. $k \geqslant 0$ integer

$$\frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} |\mathrm{Fix}(\sigma)|^k \longrightarrow \mathbf{E}(P_1^k).$$

Step 3. (Linear algebra/representation theory)

It is known that

$$\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}|\mathrm{Fix}(\sigma)| = \text{dimension of the subspace of } \mathbf{C}^n \text{ invariant under } \{u_\sigma\}$$

Better:

$$\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}|\mathrm{Fix}(\sigma)|^k = \text{dimension of the subspace of } \mathbf{C}^{n^k} \text{ invariant under } \{u_\sigma^{\otimes k}\}$$

where σ permutes the $\{1,\dots,k\} \to \{1,\dots,n\}$, and $u_\sigma^{\otimes k}$ is the permutation matrix of size n^k.

“Then felt I like some watcher of the skies
When a new planet swims into his ken” (J. Keats)

Step 4.
For a **variable** t, Deligne (2004) and Knop (2007) have defined “the symmetric group $\mathfrak{S}_t$”,

$\longrightarrow$ “permutation matrices of size t

$\longrightarrow$ dimension[1] of the “invariant subspace”

[1] in the usual sense!

Property 1: one can “specialize” t to n, and the dimension **decreases**:

$$\dim\begin{pmatrix} \text{subspace of } \mathbf{C}^{n^k} \\ \text{invariant} \end{pmatrix} \leqslant \dim\begin{pmatrix} \text{subspace of } \mathbf{C}^{t^k} \\ \text{invariant} \end{pmatrix}$$

with **equality** if (and only if)

$$k \leqslant n.$$

Property 2: there is a canonical basis of the invariant subspace of $\mathbf{C}^{t^k}$ whose elements are the partitions of the finite set $\{1, \ldots, k\}$.

Consequently

$$\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} |\mathrm{Fix}(\sigma)|^k \xrightarrow[n\to+\infty]{=\text{ if } n\geqslant k} b_k$$

where b_k is this number of partitions.

But $b_k = \mathbf{E}(P_1^k)$ [e.g. because both sequences satisfy the recursive relation $a_{k+1} = \sum_{j=0}^{k} \binom{k}{j} a_j$], hence the theorem.

(The coincidence of the moments was observed by Diaconis and Shahshahani in 1994.)

Is this an honest proof?

(1) It can be generalized *mutatis mutandis* ($+\varepsilon$) to many other situations. For instance:

Theorem (Fulman, 1997; Fulman–Stanton, 2016; F-F-K).
E finite field.
Y_n uniform on $\mathrm{GL}_n(E)$ (on $\mathrm{Aff}_n(E)$)

$$\begin{array}{c}|\mathrm{Ker}(1_n - Y_n)| \\ |\mathrm{Fix}(Y_n)|\end{array} \xrightarrow[n\to+\infty]{\text{law}} F_E$$

where F_E is characterized by

$$\mathbf{E}(F_E^k) = \text{number of subspaces of } E^k$$
(number of affine subspaces of E^k)

(2) The proof gives an idea of the origin of the Poisson limit (image under the trace of the uniform probability measure on $\mathfrak{S}_t$)

(3) But there remain questions...

(i) What about $\mathrm{Sp}_{2n}(E)$?

(ii) What about the number of 2-cycles in σ? Of 3-cycles?

(4) But now, to conclude...

Arithmetic speculations...

Theorem (Frobenius; Chebotarev).
$g \in \mathbf{Z}[X]$, $\deg(g) = n$, $\mathrm{Gal}(g) = \mathfrak{S}_n$

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

(average of the number of roots over $p \leqslant x$, $x \to +\infty$).

(Reason: $Z_p = \{\text{roots of } g \text{ in } \overline{\mathbf{F}}_p\}$, $|Z_p| = n$, $x \mapsto x^p$ permutes Z_p, giving a $\sigma_p \in \mathfrak{S}_n$,

$$\{\sigma_p \mid p \leqslant x\} \xrightarrow{x \to +\infty} \sigma \ \text{ uniform.}$$

Challenge: Have $\mathfrak{S}_t$ appear instead of $\mathfrak{S}_n$...

Pseudo-polynomial

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

The function f is a *pseudo-polynomial*: the function $f \bmod q\colon \mathbf{Z}/q\mathbf{Z} \to \mathbf{Z}/q\mathbf{Z}$ has a sense ($q \geqslant 1$ integer).

Conjecture (K.–Soundararajan)

$$|\{x \bmod p \mid f(x) = 0 \bmod p\}| \longrightarrow \quad P_1$$

$$(= |\mathrm{Fix}(\sigma)|,\ \sigma \in \mathfrak{S}_t)$$

Numerically: $p \leqslant 10^6$

k	1	2	3	4
Moment	0.99671	1.9964	5.0034	15.054