Paire génératrice de sous-groupes de $\mathfrak{S}_n$

Antoine Dequay

14 septembre 2022

Notes

- Prof : .
- Leçons : 101, 104, 105, 108, 190.
- Références :
  - *131 DVP*, Lesesvre.

Théorème 1 Soit $n \in \mathbb{N}^*$ et t_n la proportion de paires $(x, y) \in \mathfrak{S}_n^2$ qui engendre un sous-groupe transitif de $\mathfrak{S}_n$. Alors :

$$t_n = 1 - \frac{1}{n} + O\left(\frac{1}{n^2}\right)$$

Preuve.

Lemme 2 Soit $n \in \mathbb{N}^*$, on a :

$$n = \sum_{k=1}^{n} \binom{n}{k}^{-1} k t_k$$

Preuve. On considère la décomposition

$$[\![1, n]\!] = \bigsqcup_{i=1}^{n} A_i$$

avec les A_i éventuellement vides. Soit $(n_i)_{i \in [\![1,n]\!]} \in \mathbb{N}^n$ tel que $\sum_{i=1}^{n} i n_i = n$. Commençons par calculer le cardinal de

$$A = \left\{ (A_i)_{i \in [\![1,n]\!]}, [\![1, n]\!] = \bigsqcup_{i=1}^{n} A_i, \forall i \in [\![1, n]\!], \# \{A_j, \# A_j = i\} = n_i \right\}$$

Pour cela, on découpe $[\![1, n]\!]$ en n blocs de taille croissante, de sorte qu'on ait exactement n_i blocs de taille i pour tout $i \in [\![1, n]\!]$.

A dire à l'oral en écrivant la formule : Dénombrer A revient à dénombrer le nombre de façons de "remplir" ces blocs par les éléments de $[\![1, n]\!]$, c'est à dire dénombrer des permutations (d'où le $n!$) de $\mathfrak{S}_n$ qui stabilisent chaque bloc (d'où le $\prod_{i=1}^{n} (i!)^{n_i}$) sans ce soucier de leur ordre (d'où le $\prod_{i=1}^{n} n_i!$), ce qui donne :

$$\# A = \frac{n!}{\prod_{i=1}^{n} (i!)^{n_i} n_i!}$$

Calculons maintenant le cardinal de :

$$B = \left\{ (x, y) \in \mathfrak{S}_n^2, \forall i \in [\![1, n]\!], (A_i \neq \emptyset \Longrightarrow \exists z \in \langle x, y \rangle, orb(z) = A_i) \right\}$$

A dire à l'oral en écrivant la formule : Pour chaque $i \in [\![1, n]\!]$, on peut choisir librement les restrictions $x|_{A_i}$ et $y|_{A_i}$ au sein de leur orbite A_i. $\langle x|_{A_i}, y|_{A_i} \rangle$ est bien un sous-groupe de

$\mathfrak{S}_{\#A_i}$ agissant transitivement sur A_i, d'où, avec la convention $t_0 = 1$:

$$\#B = \prod_{i=1}^{n} (\#A_i!)^2 \, t_{\#A_i} = \prod_{i=1}^{n} \left((i!)^2 \, t_i\right)^{n_i}$$

On obtient donc, en énumérant l'ensemble des décompositions possibles de $[\![1, n]\!]$, l'ensemble des paires de $\mathfrak{S}_n^2$ via ce qui précède, d'où :

$$n!^2 = \sum_{\substack{(n_i)_{i\in[\![1,n]\!]}\in\mathbb{N}^n \\ \sum_{i=1}^n in_i=n}} \frac{n!}{\displaystyle\prod_{i=1}^{n}(i!)^{n_i} n_i!} \prod_{i=1}^{n} \left((i!)^2 \, t_i\right)^{n_i} = n! \sum_{\substack{(n_i)_{i\in[\![1,n]\!]}\in\mathbb{N}^n \\ \sum_{i=1}^n in_i=n}} \prod_{i=1}^{n} \frac{(i!t_i)^{n_i}}{n_i!}$$

On peut donc écrire l'égalité entre séries formelles :

$$\begin{aligned}\sum_{n=1}^{+\infty} n!X^n &= \sum_{n=1}^{+\infty} \left(\sum_{\substack{(n_i)_{i\in[\![1,n]\!]}\in\mathbb{N}^n \\ \sum_{i=1}^n in_i=n}} \prod_{i=1}^{n} \frac{(i!t_i)^{n_i}}{n_i!} \right) X^n = \sum_{n=1}^{+\infty} \left(\sum_{\substack{(n_i)_{i\in[\![1,n]\!]}\in\mathbb{N}^n \\ \sum_{i=1}^n in_i=n}} \prod_{i=1}^{n} \frac{(i!t_iX^i)^{n_i}}{n_i!} \right) \\ &= \prod_{i=1}^{+\infty} \sum_{j=0}^{+\infty} \frac{(i!t_iX^i)^j}{j!} = \prod_{i=1}^{+\infty} \exp\left(i!t_iX^i\right) = \exp\left(\sum_{i=1}^{+\infty} i!t_iX^i\right)\end{aligned}$$

Une dérivée formelle permet alors d'avoir :

$$\sum_{n=1}^{+\infty} n \cdot n!X^{n-1} = \sum_{j=1}^{+\infty} j \cdot j!t_jX^{j-1} \exp\left(\sum_{i=1}^{+\infty} i!t_iX^i\right) = \sum_{j=1}^{+\infty} j \cdot j!t_jX^{j-1} \sum_{k=1}^{+\infty} k!X^k$$

En particulier, l'égalité des coefficients d'ordre $n - 1$ donne bien :

$$n = \frac{1}{n!} \sum_{i=1}^{n} i \cdot i!t_i(n-i)! = \sum_{i=1}^{n} \binom{n}{i}^{-1} it_i$$

□

On pose, pour $n \in \mathbb{N}^*$, $r_n = n(1 - t_n)$ et $c_n = \displaystyle\sum_{i=1}^{n-1} \binom{n}{i}^{-1} i$. On cherche donc à prouver que $r_n = 1 + O\left(\dfrac{1}{n}\right)$. Par le lemme, on a, pour $n \in \mathbb{N}^*$ fixé :

$$\begin{aligned} r_n = n - nt_n &= \sum_{i=1}^{n} \binom{n}{i}^{-1} it_i - nt_n = \sum_{i=1}^{n-1} \binom{n}{i}^{-1} it_i \\ &= \sum_{i=1}^{n-1} \binom{n}{i}^{-1} i - \sum_{i=1}^{n-1} \binom{n}{i}^{-1} r_i = c_n - \sum_{i=1}^{n-1} \binom{n}{i}^{-1} r_i \end{aligned}$$

Comme les t_i sont des proportions, $\forall i \in \mathbb{N}^*$, $t_i \leq 1$, et donc $0 \leq r_n \leq c_n$. Étudions $(c_n)_{n\in\mathbb{N}^*}$.

Par changement de variables et symétrie des coefficients binomiaux, on a :

$$c_n = \sum_{i=1}^{n-1} \binom{n}{i}^{-1} i = \sum_{i=1}^{n-1} \binom{n}{i}^{-1} (n-i) = n \sum_{i=1}^{n-1} \binom{n}{i}^{-1} - c_n$$

Ainsi, pour $n \geq 6$, on peut écrire :

$$c_n = \frac{n}{2} \sum_{i=1}^{n-1} \binom{n}{i}^{-1} = 1 + \frac{2}{n-1} + \frac{n}{2} \sum_{i=1}^{n-1} \binom{n}{i}^{-1}$$

On a, pour $i \in [\![3, n-3]\!]$, $\binom{n}{3} \leq \binom{n}{i}$, d'où :

$$\frac{n}{2} \sum_{i=1}^{n-3} \binom{n}{i}^{-1} \leq \frac{n^2}{2} \binom{n}{3}^{-1} = O\left(\frac{1}{n}\right)$$

et

$$c_n = 1 + O\left(\frac{1}{n}\right)$$

La suite $(c_n)_{n\in\mathbb{N}^*}$ est donc bornée, donc $(r_n)_{n\in\mathbb{N}^*}$ aussi. Il existe donc $M > 0$, tel que :

$$\sum_{i=1}^{n-1} \binom{n}{i}^{-1} r_i \leq M \sum_{i=1}^{n-1} \binom{n}{i}^{-1} = 2M \frac{c_n}{n} = O\left(\frac{1}{n}\right)$$

d'où

$$r_n = c_n - O\left(\frac{1}{n}\right) = 1 + O\left(\frac{1}{n}\right)$$

□