Anaël Marit ENS Rennes

PERMUTATIONS ALÉATOIRES

- 105, 190, 264 –

—

On va dans ce développement établir certaines propriétés moyennes d'une permutation prise au hasard dans $\mathfrak{S}_n$. Outre que ce sujet semble beaucoup plaire au jury au vu du nombre de fois qu'ils l'évoquent dans le rapport, il donne lieu à de jolies démonstrations combinatoires et trouve des applications en informatique, permettant par exemple d'établir s'il est raisonnable de chercher à générer une permutation ayant certaines propriétés voulues par méthode de rejet.

On retrouvera ce développement éparpillé dans les questions d'un problème de probabilités dans [1]

On considère dans tout ce développement un entier non nul n et une variable aléatoire suivant une loi uniforme sur $\mathfrak{S}_n$. Posons C_n la variable aléatoire qui compte le nombre de cycles apparaissant dans sa décomposition en cycles à supports disjoints, avec la convention que tout point fixe compte pour un 1-cycle (par exemple, l'identité est considérée comme composée de n-cycles). L'objectif est d'obtenir la loi et l'espérance de C_n. Pour cela, on va calculer sa fonction génératrice en établissant une relation de récurrence double sur les probabilités atomiques.

Une formule de récurrence

Introduisons les ensembles suivants :

$$\mathfrak{S}_{n,k} := \{\sigma \in \mathfrak{S}_n \mid \sigma \text{ se décompose en } k \text{ cycles à supports disjoints}\} \tag{1}$$

Il est alors clair, par probabilités uniformes, que :

$$\mathbb{P}(C_n = k) = \frac{|\mathfrak{S}_{n,k}|}{n!} \tag{2}$$

On va établir une formule de récurrence sur n et k qui lie les cardinaux des $\mathfrak{S}_{n,k}$.

Tout d'abord, notons que la seule permutation de $[\![1,n]\!]$ étant produit de n-cycles à supports disjoints est l'identité, tandis qu'aucune permutation n'est produit de zéro cycles. D'où :

$$\forall n \in \mathbb{N}^*,\ |\mathfrak{S}_{n,n}| = 1 \wedge |\mathfrak{S}_{n,0}| = 0 \tag{3}$$

Notons, pour $l \in [\![1,n]\!]$:

$$\mathfrak{S}_{n+1,k+1}(l) := \{\sigma \in \mathfrak{S}_{n+1,k+1} \mid \sigma(n+1) = l\} \tag{4}$$

On alors la partition :

$$\mathfrak{S}_{n+1,k+1} = \bigsqcup_{l=1}^{n} \mathfrak{S}_{n+1,k+1}(l) \tag{5}$$

On va dénombrer selon la valeur de l.

Pour $l = n+1$, on considère l'application :

$$\begin{aligned} \mathfrak{S}_{n+1,k+1}(n+1) &\to \mathfrak{S}_{n,k} \\ \sigma &\mapsto \sigma_{|[\![1,n]\!]} \end{aligned}$$

Cette application est bien définie car $n+1$ est un point fixe pour toute les permutations de $\mathfrak{S}_{n+1,k}(n+1)$. C'est une bijection dont on donne explicitement l'inverse :

$$\begin{aligned} \mathfrak{S}_{n,k} &\to \mathfrak{S}_{n+1,k+1}(n+1) \\ \sigma &\mapsto \left(i \mapsto \begin{cases} \sigma(k) \text{ si } k < n+1 \\ n+1 \text{ sinon} \end{cases} \right) \end{aligned}$$

Ainsi :

$$|\mathfrak{S}_{n+1,k+1}(n+1) = |\mathfrak{S}_{n,k}| \tag{6}$$

Pour $l \leqslant n$, on considère la transposition $\tau = (l\ n+1)$. Alors :

$$\forall \sigma \in \mathfrak{S}_{n+1,k+1}(l),\ \tau\sigma \in \mathfrak{S}_{n+1,k+2}(n+1)\ ^{(\mathrm{i})} \tag{7}$$

Par ailleurs, la multiplication par τ est une bijection. Ainsi :

$$|\mathfrak{S}_{n+1,k+1}(l)| = |\mathfrak{S}_{n+1,k+2}(n+1)| = |\mathfrak{S}_{n,k+1}| \tag{8}$$

Finalement, il vient :

$$\begin{aligned} |\mathfrak{S}_{n+1,k+1}| &= \left| \bigsqcup_{l=1}^{n=1} \mathfrak{S}_{n+1,k+1}(l) \right| \qquad (9) \\ &= \sum_{l=1}^{n+1} |\mathfrak{S}_{n+1,k+1}(l)| \qquad (10) \\ &= |\mathfrak{S}_{n,k}| + n|\mathfrak{S}_{n,k+1}| \qquad (11) \end{aligned}$$

Factorielle croissante

Grâce à cette relation de récurrence, on va pouvoir déterminer la fonction génératrice de C_n. Considérons le polynôme suivant :

Définition 1 (Factorielle croissante). *Pour $n \in \mathbb{N}$, on appelle* factorielle croissante *le polynôme à coefficients entiers :*

$$X^{\overline{n}} := \prod_{k=0}^{n-1} (X+k) \tag{12}$$

(i). On a bien $k+2 \leqslant n+1$ car l étant différent de $n+1$, $n+1$ n'est pas un point fixe de σ et donc σ est différente de l'identité. De plus, on a augmenté le nombre de cycles dans la décompostion de σ d'exactement 1 en multipliant par τ, car cycle contenant auparavant $n+1$ a été divisé d'un côté en $\{n+1\}$, de l'autre en un cycle identique dont on a retiré $n+1$.

Notons sous forme développée :

$$X^{\overline{n}} = \sum_{k=0}^{n} s(n,k) X^k \tag{13}$$

On va montrer que $s(n,k) = |\mathfrak{S}_{n,k}|$ en montrant que ces deux suites doubles satisfont la même relation de récurrence.

Puisque $|s(m,m)|$ est le coefficient dominant de la factorielle croissante, qui est un polynôme unitaire, ce nombre est égal à 1. Par ailleurs, $s(m,0)$ est le produit des racines de la factorielle croissante, parmi lesquelles on compte 0 : c'est donc 0. De plus :

$$\begin{aligned} X^{\overline{m+1}} &= (X+m)X^{\overline{m}} && (14)\\ &= (X+m)\sum_{k=0}^{m} s(m,k)X^k && (15)\\ &= X^{m+1} + \sum_{k=0}^{m} (\underbrace{s(m,k) + ms(m,k+1)}_{=|s(k+1,m+1)|})X^k && (16) \end{aligned}$$

Finalement, on trouve bien la même relation de récurrence.

On déduit donc :

Proposition 2. *La fonction génératrice de C_n est donnée par :*

$$G_{C_n}(t) = \frac{1}{n!} t^{\overline{n}} \tag{17}$$

Calcul de l'espérance

Terminons cette petite étude en calculant l'espérance de C_n. Puisqu'on connaît sa fonction génératrice, on dispose de la formule suivante :

$$\mathbb{E}[C_n] = G'_{C_n}(1) = \frac{1}{n!}(X^{\overline{n}})'(1) \tag{18}$$

Pour calculer ce terme, on va utiliser la petite astuce suivante :

$$\frac{(X^{\overline{n}})'}{X^{\overline{n}}} = \sum_{k=0}^{n-1} \frac{1}{X+k} \tag{19}$$

Comme par ailleurs $1^{\overline{n}} = n!$, on trouve :

$$\mathbb{E}[C_n] = \sum_{k=1}^{n} \frac{1}{k} = H_n \tag{20}$$

où H_n est le n-ième nombre harmonique. En particulier :

$$\mathbb{E}[C_n] \sim \log(n) \tag{21}$$

lorsque n tend vers l'infini.

Références

[1] Xavier GOURDON. *Algèbre et probabilités*. Ellipses.