

3.3 Quelques résultats sur les permutations aléatoires suivant la loi uniforme sur \mathfrak{S}_n (101, 105, 190, 262, 264) [19], [21], [34]

Définition 3.13 (Factorielles croissante et décroissante). Soit $x \in \mathbb{R}$. On définit la n -ième factorielle décroissante et la n -ième factorielle croissante de x , notées respectivement $x^{\underline{n}}$ et $x^{\overline{n}}$ par les formules de récurrence suivantes :

$$\begin{cases} x^{\underline{0}} = x^{\overline{0}} = 1, \\ x^{\underline{n+1}} = (x-n)x^{\underline{n}}, \quad \forall n \in \mathbb{N}, \\ x^{\overline{n+1}} = (x+n)x^{\overline{n}}, \quad \forall n \in \mathbb{N}. \end{cases}$$

On peut alors définir les *nombre de Stirling de première espèce* :

Définition 3.14 (Nombres de Stirling de première espèce). Soient $x \in \mathbb{R}$, $n \in \mathbb{N}$, $k \in \llbracket 0, n \rrbracket$. Le nombre $x^{\underline{n}}$ est un polynôme en x et on note $s(n, k)$ les nombres entiers tels que :

$$x^{\underline{n}} = \sum_{k=0}^n s(n, k)x^k.$$

Théorème 3.15 (Loi et espérance du nombre de cycles à supports disjoints d'une permutation tirée uniformément dans \mathfrak{S}_n). Soit Σ_n une variable aléatoire suivant la loi $\mathcal{U}(\mathfrak{S}_n)$, et notons C_n la variable aléatoire comptant le nombre de cycles à supports disjoints apparaissant dans la décomposition de Σ_n . Alors, on a :

$$\forall t \in \mathbb{R}, \quad G_{C_n}(t) = \frac{t^{\overline{n}}}{n!},$$

plus précisément :

$$\forall k \in \llbracket 1, n \rrbracket, \quad \mathbb{P}(C_n = k) = \frac{|s(n, k)|}{n!}$$

et :

$$\mathbb{E}(C_n) = \sum_{k=1}^n \frac{1}{k}.$$

De plus (à mettre pour la leçon 262) on a le théorème limite central suivant :

$$\frac{C_n - \ln(n)}{\sqrt{\ln(n)}} \xrightarrow[n \rightarrow +\infty]{\mathcal{L}} \mathcal{N}(0, 1).$$

Démonstration. Étape 1 : $\sum_{k=0}^n |s(n, k)|x^k = x^{\overline{n}}$:

En développant l'écriture de $x^{\underline{n}}$ et $x^{\overline{n}}$, on obtient :

$$x^{\underline{n}} = x(x-1)\dots(x-n+1), \quad x^{\overline{n}} = x(x+1)\dots(x+n-1).$$

Ainsi :

$$\forall x \in \mathbb{R}, \quad (-x)^{\underline{n}} = (-1)^n x^{\overline{n}}.$$

Ainsi, on obtient :

$$\forall x \in \mathbb{R}, \quad x^{\overline{n}} = \sum_{k=0}^n (-1)^{n-k} s(n, k)x^k.$$

Or, en notant $\tilde{s}(n, k)$ les entiers tels que :

$$x^{\bar{n}} = \sum_{k=0}^n \tilde{s}(n, k)x^k$$

on a :

$$\forall k \in \llbracket 0, n \rrbracket, \quad \tilde{s}(n, k) \geq 0$$

par somme et produits d'entiers positifs. On a donc :

$$\forall k \in \llbracket 0, n \rrbracket, \quad (-1)^{n-k} s(n, k) \geq 0$$

et donc :

$$x^{\bar{n}} = \sum_{k=0}^n |s(n, k)|x^k.$$

Étape 2 : Une relation de récurrence sur les $|s(n, k)|$:

On va utiliser la relation de récurrence sur la factorielle croissante afin de déduire une relation de récurrence sur les $|s(n, k)|$:

$$\sum_{k=0}^{n+1} |s(n+1, k)|x^k = x^{\overline{n+1}} = (x+n) \sum_{k=0}^n |s(n, k)|x^k = \sum_{k=1}^n (|s(n, k-1)| + n|s(n, k)|)x^k + |s(n, n)|x^{n+1}.$$

On en déduit donc :

$$\forall n \in \mathbb{N}^*, \quad \begin{cases} |s(n, 0)| = 0 \\ |s(n, n)| = 1 \\ |s(n+1, k)| = |s(n, k-1)| + n|s(n, k)|, \quad \forall k \in \llbracket 1, n \rrbracket. \end{cases}$$

Étape 3 : Le nombre de permutations de \mathfrak{S}_n s'écrivant comme produit de k cycles à supports disjoints vérifie la même relation de récurrence :

Disclaimer : Attention ! Ici, l'identité sera considérée comme étant un produit de n cycles à supports disjoints ! (on considère les 1-cycles comme étant des cycles à part entière).

Notons $\mathfrak{S}_{n,k}$ l'ensemble des permutations de \mathfrak{S}_n s'écrivant comme produits de k cycles à supports disjoints et $C(n, k)$ son cardinal. On a :

$$C(n, 0) = 0, \text{ et } C(n, n) = 1$$

car si $n \geq 1$, une permutation possède au moins 1 cycle dans sa décomposition et $id_{\llbracket 1, n \rrbracket}$ est la seule permutation de \mathfrak{S}_n s'écrivant comme produit de n cycles à supports disjoints. Pour passer du cran n au cran $n+1$, il faut distinguer les cas selon la présence de $n+1$ dans un cycle de longueur plus grande que 1 ou non. On écrit alors $\mathfrak{S}_{n+1,k}$ grâce à la partition suivante :

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

où on a noté :

$$\mathfrak{S}_{n+1,k}(m) = \{ \sigma \in \mathfrak{S}_{n,k} \mid \sigma(n+1) = m \}$$

Cas $m = n+1$: Si $\sigma(n+1) = n+1$, alors l'application de restriction à $\llbracket 1, n \rrbracket$ devient une bijection entre $\mathfrak{S}_{n+1,k}(n+1)$ et $\mathfrak{S}_{n,k-1}$. En effet, si $\sigma \in \mathfrak{S}_{n+1,k}(n+1)$, alors sa restriction à $\llbracket 1, n \rrbracket$ est une permutation et s'écrit nécessairement comme un produit de $k-1$ cycles à supports disjoints (puisque σ possède déjà le cycle $(n+1)$). Réciproquement, une permutation de $\llbracket 1, n \rrbracket$ s'écrivant comme un produit de $k-1$ cycles à supports disjoints se voit

naturellement comme un élément de \mathfrak{S}_{n+1} s'écrivant comme produit de k cycles à supports disjoints. D'où :

$$|\mathfrak{S}_{n+1,k}(n+1)| = C(n, k-1).$$

Cas $m \leq n$: Si $\sigma \in \mathfrak{S}_{n+1,k}(m)$, alors, il s'écrit :

$$\sigma = c \circ c_2 \circ \dots \circ c_k$$

où $c = (n+1 \ m \ i_3 \ \dots \ i_r)$ désigne le cycle de σ dans sa décomposition contenant $n+1$. On a alors, en notant :

$$\sigma' = (n+1 \ m) \circ \sigma,$$

que $\sigma' \in \mathfrak{S}_{n+1,k}(n+1)$. Ainsi, $\sigma'_{[[1,n]]} \in \mathfrak{S}_n$. Notons cette restriction $f(\sigma)$. On a alors défini une application :

$$f : \mathfrak{S}_{n+1,k}(m) \longrightarrow \mathfrak{S}_n$$

Montrons qu'en réalité, $f(\sigma) \in \mathfrak{S}_{n,k}$ et que f est bijective (comme application à valeurs dans $\mathfrak{S}_{n,k}$). Premièrement, on observe que le cycle c de σ est transformé en le cycle $c' = (m \ i_3 \ \dots \ i_r)$ dans la décomposition de σ' . Plus concrètement, on a :

$$\sigma' = c' \circ c_2 \circ \dots \circ c_k$$

et, étant donné que tous les entiers apparaissant dans le support de σ' sont entre 1 et n , $f(\sigma)$ s'écrit exactement :

$$f(\sigma) = c' \circ c_2 \circ \dots \circ c_k.$$

Ainsi, $f(\sigma)$ possède exactement k cycles dans sa décomposition. Donc :

$$f(\sigma) \in \mathfrak{S}_{n,k}.$$

Enfin, f est bijective. En effet, si $\sigma' \in \mathfrak{S}_{n,k}$, alors en posant :

$$\sigma' = c_1 \circ c_2 \circ \dots \circ c_k$$

avec $m \in \text{supp}(c_1)$ et :

$$\sigma = (n+1 \ m) \circ c_1 \circ c_2 \circ \dots \circ c_k \in \mathfrak{S}_{n+1},$$

on a :

$$\sigma \in \mathfrak{S}_{n+1,k}(m)$$

car $(n+1 \ m) \circ c_1$ est un cycle dont le support est $\{n+1\} \cup \text{supp}(c_1)$, et donc son support est disjoint de celui des cycles c_2, \dots, c_k . Enfin, on a bien que $\sigma(n+1) = m$ (car $n+1$ n'apparaît pas dans le support des c_i). On a donc construit la bijection réciproque de f ! Il s'agit donc d'une bijection entre $\mathfrak{S}_{n+1,k}(m)$ et $\mathfrak{S}_{n,k}$ pour tout $m \in [[1, n]]$. On a donc :

$$C(n+1, k) = |\mathfrak{S}_{n+1,k}| = \sum_{m=1}^{n+1} |\mathfrak{S}_{n+1,k}(m)| = C(n, k-1) + \sum_{m=1}^n C(n, k) = C(n, k-1) + nC(n, k).$$

On montre alors par récurrence sur $n \in \mathbb{N}^*$ que pour tout $k \in [[0, n]]$, $C(n, k) = |s(n, k)|$.

Étape 4 : Conclusion

Si Σ est une variable aléatoire suivant la loi $\mathcal{U}(\mathfrak{S}_n)$, et si C_n désigne son nombre de cycles à supports disjoints

apparaissant dans sa décomposition, on a :

$$\mathbb{P}(C_n = k) = \frac{C(n, k)}{n!} = \frac{|s(n, k)|}{n!}.$$

On peut alors en déduire sa série génératrice :

$$\forall t \in \mathbb{R}, \quad G_{C_n}(t) = \sum_{k=0}^{+\infty} \mathbb{P}(C_n = k) t^k = \sum_{k=0}^n \frac{|s(n, k)|}{n!} t^k = \frac{t^{\bar{n}}}{n!}.$$

On en déduit donc :

$$\mathbb{E}(C_n) = G'_{C_n}(1) = \underbrace{G_{C_n}(t)}_{=1} \times \frac{d}{dt} (\ln(t^{\bar{n}}))|_{t=1}$$

Or, pour tout $t > 0$, on a :

$$\ln(t^{\bar{n}}) = \sum_{i=0}^{n-1} \ln(t+i).$$

D'où :

$$\frac{d}{dt} (\ln(t^{\bar{n}})) = \sum_{i=0}^{n-1} \frac{1}{t+i}.$$

On conclut donc que :

$$\mathbb{E}(C_n) = \sum_{i=0}^{n-1} \frac{1}{i+1}$$

ce qui termine la preuve!

Étape 5 : Le théorème limite central pour les cycles (en bonus pour la leçon 262)

On a pu déterminer la fonction génératrice de notre nombre de cycles C_n . On peut donc en déduire sa fonction caractéristique! En effet :

$$\forall t \in \mathbb{R}, \quad \varphi_{C_n}(t) = G_{C_n}(e^{it}) = \prod_{k=1}^n \left(\frac{e^{it} + k - 1}{k} \right).$$

Ainsi, pour tout $n \in \mathbb{N}^*$, on a :

$$\varphi_{\frac{C_n - \ln(n)}{\sqrt{\ln(n)}}}(t) = e^{-it\sqrt{\ln(n)}} \varphi_{C_n} \left(\frac{t}{\sqrt{\ln(n)}} \right) = e^{-it\sqrt{\ln(n)}} \prod_{k=1}^n \left(1 + \frac{\exp\left(\frac{it}{\sqrt{\ln(n)}}\right) - 1}{k} \right).$$

Or, $\exp\left(\frac{it}{\sqrt{\ln(n)}}\right) - 1 \underset{n \rightarrow +\infty}{\sim} \frac{it}{\sqrt{\ln(n)}}$. Ainsi, il existe un rang à partir duquel $\exp\left(\frac{it}{\sqrt{\ln(n)}}\right) - 1$ soit de module strictement inférieur à $\frac{1}{2}$, de sorte qu'on puisse appliquer la branche principale du logarithme :

$$\varphi_{\frac{C_n - \ln(n)}{\sqrt{\ln(n)}}}(t) = \exp \left(-it\sqrt{\ln(n)} + \sum_{k=1}^n \log \left(1 + \frac{\exp\left(\frac{it}{\sqrt{\ln(n)}}\right) - 1}{k} \right) \right).$$

Or, il existe une fonction h holomorphe sur le disque $\mathbb{D}\left(0, \frac{1}{2}\right)$ telle que $h(z) \xrightarrow{z \rightarrow 0} \frac{1}{2}$ et :

$$\forall z \in \mathbb{D}\left(0, \frac{1}{2}\right), \quad \log(1+z) = z + z^2 h(z).$$

Ainsi, on obtient l'expression suivante pour $\varphi_{\frac{C_n - \ln(n)}{\sqrt{\ln(n)}}}(t)$:

$$\exp \left(-it\sqrt{\ln(n)} + \sum_{k=1}^n \left(\frac{\exp\left(\frac{it}{\sqrt{\ln(n)}}\right) - 1}{k} + \frac{\left(\exp\left(\frac{it}{\sqrt{\ln(n)}}\right) - 1\right)^2}{k^2} h \left(\frac{\exp\left(\frac{it}{\sqrt{\ln(n)}}\right) - 1}{k} \right) \right) \right).$$

On a alors le développement limité suivant :

$$\begin{aligned} \varphi_{\frac{C_n - \ln(n)}{\sqrt{\ln(n)}}}(t) &= \exp \left(-it\sqrt{\ln(n)} + \underbrace{(\ln(n) + O(1))}_{\text{DL de la série harmonique}} \left(\frac{it}{\sqrt{\ln(n)}} - \frac{t^2}{2\ln(n)} + o\left(\frac{1}{\ln(n)}\right) \right) + o(1) \right) \\ &= \exp \left(-it\sqrt{\ln(n)} + it\sqrt{\ln(n)} - \frac{t^2}{2} + o(1) \right) \\ &= \exp \left(-\frac{t^2}{2} + o(1) \right). \end{aligned}$$

□

Ce développement serait un petit peu court si on s'arrêtait là non ? Alors vous reprendrez bien un petit résultat pour la route !

Définition 3.16 (Nombres de Stirling de deuxième espèce). Pour $n \in \mathbb{N}$ et $k \in \llbracket 0, n \rrbracket$, on définit les *nombre de Stirling de deuxième espèce*, notés $S(n, k)$ comme les entiers vérifiant :

$$\forall x \in \mathbb{R}, \quad x^n = \sum_{k=0}^n S(n, k)x^k.$$

Proposition 3.17. $S(n, k)$ est le nombre de façons de partitionner $\llbracket 1, n \rrbracket$ en exactement k sous-ensembles. En particulier, on a :

$$\forall n \in \mathbb{N}, \quad \sum_{k=0}^n S(n, k) = B_n$$

où B_n désigne le n -ième nombre de Bell, comptant le nombre de façons de partitionner $\llbracket 1, n \rrbracket$.

Démonstration. Déjà, les nombres $S(n, k)$ sont bien définis car la famille $(1, X, \dots, X(X-1) \dots (X-n+1))$ est échelonnée en degré et possède $n+1$ éléments. Ainsi, elle forme une base de $\mathbb{Q}_n[X]$. Ensuite, on vérifie les faits suivants :

$$S(0, 0) = 1 \quad \text{et} \quad \forall n \in \mathbb{N}^*, \quad \begin{cases} S(n, 0) = 0 \\ S(n, n) = 1 \\ S(n+1, k) = S(n, k-1) + kS(n, k), \quad \forall k \in \llbracket 1, n \rrbracket. \end{cases}$$

En effet, $S(0, 0)$ est bien égal à 1 car $x^0 = 1$ et pour $n \geq 1$, en identifiant les coefficients devant x^0 et x^n des deux côtés de l'égalité, on obtient :

$$S(n, 0) = 0 \quad \text{et} \quad S(n, n) = 1.$$

Enfin, en calculant x^{n+1} de deux façons différentes, on obtient :

$$\sum_{k=0}^{n+1} S(n+1, k)x^k = \sum_{k=0}^n S(n, k)xx^k.$$

Or, on a :

$$xx^k = (x - k)x^k + kx^k = x^{k+1} + kx^k.$$

Ainsi, on obtient :

$$\sum_{k=0}^{n+1} S(n+1, k)x^k = \sum_{k=1}^{n+1} S(n, k-1)x^k + \sum_{k=0}^n kS(n, k)x^k.$$

Ainsi, en identifiant les coefficients devant x^k pour $k \in \llbracket 1, n \rrbracket$, on obtient :

$$\forall k \in \llbracket 1, n \rrbracket, \quad S(n+1, k) = S(n, k-1) + kS(n, k).$$

Enfin, vérifions que le nombre $P(n, k)$ de façons de partitionner $\llbracket 1, n \rrbracket$ en k sous-ensembles non-vides vérifie la même relation de récurrence que $S(n, k)$ et les mêmes conditions initiales. Notons $\mathcal{P}_{n,k}$ l'ensemble des partitions de $\llbracket 1, n \rrbracket$ en exactement k sous-ensembles non-vides. Pour $P \in \mathcal{P}_{n+1,k}$, on numérote les éléments p_1, \dots, p_k de P de sorte que :

$$\min p_1 < \dots < \min p_k,$$

et on définit $m(P)$ l'entier tel que $n+1 \in p_{m(P)}$. On va donc partitionner $\mathcal{P}_{n+1,k}$ selon si $n+1$ est le seul élément de $p_{m(P)}$ ou pas. Définissons donc $p'(P) = p_{m(P)} \setminus \{n+1\}$ de sorte qu'on ait la partition :

$$\mathcal{P}_{n+1,k} = \mathcal{P}_{n+1,k}^* \sqcup \left(\bigsqcup_{m=1}^k \mathcal{P}_{n+1,k}(m) \right)$$

avec :

$$\mathcal{P}_{n+1,k}^* = \{P \in \mathcal{P}_{n+1,k} \mid p'(P) = \emptyset\}$$

et :

$$\mathcal{P}_{n+1,k}(m) = \{P \in \mathcal{P}_{n+1,k} \mid m(P) = m, p'(P) \neq \emptyset\}.$$

Les applications :

$$\begin{aligned} \mathcal{P}_{n+1,k}^* &\longrightarrow \mathcal{P}_{n,k-1} \\ P &\longmapsto \{p_i \mid i \in \llbracket 1, k \rrbracket \setminus \{m(P)\}\} \end{aligned}$$

et :

$$\begin{aligned} \mathcal{P}_{n+1,k}(m) &\longrightarrow \mathcal{P}_{n,k} \\ P &\longmapsto \{p_i \mid i \in \llbracket 1, k \rrbracket \setminus \{m(P)\}\} \cup \{p'(P)\} \end{aligned}$$

sont alors des bijections. On a donc :

$$P(n+1, k) = P(n, k-1) + kP(n, k),$$

et il est clair que $P(n, 0) = 0$ et $P(n, n) = 1$, ce qui conclut. □

Théorème 3.18 (Moments du nombre de points fixes d'une permutation tirée uniformément dans \mathfrak{S}_n). Si Σ est une variable aléatoire suivant la loi $\mathcal{U}(\mathfrak{S}_n)$, alors, en notant F la variable aléatoire comptant le nombre de points fixes de Σ , alors on a :

$$\forall k \in \mathbb{N}, \quad \mathbb{E}(F^k) = \sum_{i=0}^n S(k, i).$$

(avec, pour tout $k > n$, $S(n, k) = 0$). En particulier, on a :

$$\forall k \leq n, \quad \mathbb{E}(F^k) = B_k$$

et donc, F a les mêmes n premiers moments que la loi de Poisson $\mathcal{P}(1)$. En

Démonstration. Pour tout $k \in \mathbb{N}$, on a, par définition de F :

$$\mathbb{E}(F^k) = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} |\text{Fix}(\sigma)|^k$$

où $\text{Fix}(\sigma)$ désigne l'ensemble des points fixes d'une permutation σ . Si $k = 0$, on a $\mathbb{E}(F^k) = 1$ et $B_0 = 1$ par convention. Si $k = 1$, on reconnaît un des deux membres de l'égalité dans la formule de Burnside lorsqu'un groupe G agit sur un ensemble X :

$$\left| \frac{X}{G} \right| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|.$$

Ici, $G = \mathfrak{S}_n$ et $X = \llbracket 1, n \rrbracket$. L'action de \mathfrak{S}_n sur $\llbracket 1, n \rrbracket$ étant transitive, le nombre d'orbites est 1. Ainsi :

$$\mathbb{E}(F) = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} |\text{Fix}(\sigma)| = 1.$$

On a également $B_1 = 1$. La clef de ce résultat est donc la formule de Burnside. On va donc considérer l'action de \mathfrak{S}_n sur $\llbracket 1, n \rrbracket^k$:

$$\forall \sigma \in \mathfrak{S}_n, \forall (i_1, \dots, i_k) \in \llbracket 1, n \rrbracket^k, \quad \sigma \cdot (i_1, \dots, i_k) = (\sigma(i_1), \dots, \sigma(i_k)).$$

On l'appelle *action diagonale*. Si $\text{Fix}^k(\sigma)$ désigne l'ensemble des points fixes de la permutation σ pour cette action, alors, on a :

$$\text{Fix}^k(\sigma) = \text{Fix}(\sigma)^k.$$

Ainsi :

$$\mathbb{E}(F^k) = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} |\text{Fix}^k(\sigma)| = \left| \frac{\llbracket 1, n \rrbracket^k}{\mathfrak{S}_n} \right|.$$

En notant $\mathcal{P}_{k,j}$ l'ensemble des partitions de $\llbracket 1, k \rrbracket$ en exactement j sous-ensembles non-vides, considérons l'application :

$$f : \begin{array}{ccc} \frac{\llbracket 1, n \rrbracket^k}{\mathfrak{S}_n} & \longrightarrow & \bigsqcup_{j=1}^n \mathcal{P}_{k,j} \\ \mathfrak{S}_n \cdot (i_1, \dots, i_k) & \longmapsto & P_{(i_1, \dots, i_k)} \end{array}$$

où $P_{(i_1, \dots, i_k)}$ désigne la partition de $\llbracket 1, k \rrbracket$ donnée par la relation d'équivalence $\mathcal{R}_{(i_1, \dots, i_k)}$:

$$\forall m, l \in \llbracket 1, k \rrbracket, \quad m \mathcal{R}_{(i_1, \dots, i_k)} l \iff i_m = i_l.$$

c'est-à-dire que $P_{(i_1, \dots, i_k)}$ est la partition $\{I_1, \dots, I_r\}$ de $\llbracket 1, k \rrbracket$ regroupant les indices de sorte que les valeurs de la

liste en ces indices soient identiques. Plus concrètement :

$$\begin{aligned} \forall s \in \llbracket 1, r \rrbracket, \forall m, l \in I_s, \quad i_l = i_m, \\ \forall s, t \in \llbracket 1, r \rrbracket, s \neq t, \forall (l, m) \in I_s \times I_t \quad i_l \neq i_m. \end{aligned}$$

Par exemple, si $k = 7$ et $n = 5$, alors $P_{(1,3,2,3,1,5,1)} = \{\{1, 5, 7\}, \{2, 4\}, \{3\}, \{6\}\} \in \mathcal{P}_{7,4}$.

f est bien définie à la source car si $(i_1, \dots, i_k) \in \llbracket 1, n \rrbracket^k$ et $\sigma \in \mathfrak{S}_n$, alors $\mathcal{R}_{(i_1, \dots, i_k)} = \mathcal{R}_{(\sigma(i_1), \dots, \sigma(i_k))}$ et f est bien définie au but car, si $k \leq n$, alors il y a forcément moins de n éléments dans une partition $P_{(i_1, \dots, i_k)}$ et si $k > n$, alors dans toute liste $(i_1, \dots, i_k) \in \llbracket 1, n \rrbracket^k$, il y a au plus n éléments distincts, et donc au plus n éléments dans la partition $P_{(i_1, \dots, i_k)}$. De plus, f est bijective par définition de la relation $\mathcal{R}_{(i_1, \dots, i_k)}$ et par le fait que \mathfrak{S}_n agit n -transitivement sur $\llbracket 1, n \rrbracket$. En effet, on a la caractérisation suivante de $\mathfrak{S}_n \cdot (i_1, \dots, i_k)$:

$$\mathfrak{S}_n \cdot (i_1, \dots, i_k) := \{(\sigma(i_1), \dots, \sigma(i_k)) \mid \sigma \in \mathfrak{S}_n\} = \{(m_1, \dots, m_k) \in \llbracket 1, n \rrbracket^k \mid P_{(m_1, \dots, m_k)} = P_{(i_1, \dots, i_k)}\}.$$

Si on reprend l'exemple précédent,

$$\begin{aligned} \mathfrak{S}_5 \cdot (1, 3, 2, 3, 1, 5, 1) &= \{(\sigma(1), \sigma(3), \sigma(2), \sigma(3), \sigma(1), \sigma(5), \sigma(1)) \mid \sigma \in \mathfrak{S}_5\} \\ &= \{(a, b, c, b, a, d, a) \mid a, b, c, d \in \llbracket 1, 5 \rrbracket \text{ distincts } 2 \text{ à } 2\}, \end{aligned}$$

et on a bien que $P_{(a,b,c,b,a,d,a)} = P_{(1,2,3,2,1,5,1)}$.

Ainsi, on a :

$$\left| \frac{\llbracket 1, n \rrbracket^k}{\mathfrak{S}_n} \right| = \sum_{j=1}^n |\mathcal{P}_{k,j}| = \sum_{j=1}^n S(k, j).$$

Vérifions pour finir que les moments de la loi de Poisson $\mathcal{P}(1)$ sont égaux aux nombres de Bell.

$$\forall k \in \mathbb{N}, \quad e^{-1} \sum_{i=0}^{+\infty} \frac{i^k}{i!} = e^{-1} \sum_{i=0}^{+\infty} \sum_{j=0}^k S(k, j) i^j \frac{1}{i!}.$$

Or, pour $i \leq j$, $i^j = 0$. Donc :

$$e^{-1} \sum_{i=0}^{+\infty} \frac{i^k}{i!} = e^{-1} \sum_{j=0}^k \sum_{i=j}^{+\infty} S(k, j) \frac{i^j}{i!} = e^{-1} \sum_{j=0}^k S(k, j) \sum_{i=j}^{+\infty} \frac{1}{(i-j)!} = \sum_{j=0}^k S(k, j) = B_k.$$

Cela termine la preuve! □