Statistiques du nombre de cycles d'une permutation

Xavier Caruso* et Igor Kortchemski†

Mai 2010

Résumé

Le but de ce texte est d'étudier certaines propriétés statistiques du nombre de cycles d'une permutation de $\{1,\dots,n\}$. Typiquement, nous nous demandons combien de cycles en moyenne possède une telle permutation, ou comment quantifier l'écart à cette moyenne.

Mots-clés : permutations, cycles, records, statistiques

Introduction

Dans tout cet article, on fixe un nombre entier n et on note $\mathfrak{S}_n$ le groupe des permutations de l'ensemble $\{1,\dots,n\}$. Rappelons que toute permutation σ se décompose de façon unique comme un produit de cycles à supports disjoints. Notons $\mathrm{cyc}(\sigma)$ le nombre de cycles de σ ainsi que $c_n(k)$ le nombre de permutations de $\mathfrak{S}_n$ qui ont exactement k cycles. Notre but est d'obtenir des résultats concernant la fonction cyc et les entiers $c_n(k)$.

Dans la première partie, nous nous intéressons à la fonction génératrice du nombre de cycles, c'est-à-dire au polynôme P_n dont le k-ième coefficient est égal au nombre de permutations de $\mathfrak{S}_n$ ayant exactement k cycles. Un certain nombre de propriétés peuvent s'en déduire (voir [2] pour un compte-rendu exhaustif). Par exemple, il en résultera directement des formules pour la moyenne et la variance (le carré de l'écart type) de cyc à partir desquelles on déduira notamment que, lorsque n tend vers l'infini, ces deux quantités sont de l'ordre de $\ln n$. Nous allons présenter trois manières différentes pour réaliser ce calcul, chacune d'entre elles présentant ses avantages. Les deux premières peuvent être trouvées dans [9], mais la dernière est originale.

Avec la deuxième partie, commence une étude plus fine de la répartition du nombre de cycles. Plus précisément, nous obtenons une estimée quantitative du comportement asymptotique de $c_n(k)$ lorsque n tend vers l'infini, qui est un résultat récent. Finalement, nous étudions le nombre moyen de cycles d'une permutation aléatoire uniforme de longueur n en démontrant un théorème de type « central limite ».

1 La fonction génératrice du nombre de cycles

Rappelons que $c_n(k)$ désigne le nombre de permutations de $\mathfrak{S}_n$ qui ont k cycles, et définissons comme dans l'introduction le polynôme P_n par

$$P_n(q) = \sum_{k=1}^{n} c_n(k) q^k = \sum_{\sigma \in \mathfrak{S}_n} q^{\mathrm{cyc}(\sigma)}.$$

Le but de cette première partie est de démontrer le théorème suivant, qui est bien connu (voir par exemple [9]).

Théorème 1. *Avec les notations précédentes, on a* $P_n(q) = q(q+1)(q+2)\cdots(q+n-1)$.

Nous proposons ci-après trois démonstrations différentes de ce théorème. La première d'entre elles est certainement la plus directe (et la plus courte). Elle a donc l'avantage de l'économie mais, en contrepartie, elle ne met pas clairement en évidence les structures sous-jacentes, et ne permettra pas par la suite d'aller plus loin dans l'étude des statistiques de nombres de cycles. À l'opposé, la portée de deux autres preuves, qui établissent un lien profond entre cycles et records (voir définition 2) d'une permutation, dépasse largement l'assertion du théorème 1.

*Chercheur au CNRS affecté au laboratoire Poncelet à Moscou (Russie)
†Élève à l'École Normale Supérieure de Paris

Avant de poursuivre, mentionnons que l'on peut déjà déduire du théorème 1 le nombre moyen de cycles d'une permutation de $\mathfrak{S}_n$. En effet, il est par définition égal à $\frac{P_n'(1)}{n!} = \frac{P_n'(1)}{P_n(1)}$, c'est-à-dire la valeur de la dérivée logarithmique de P_n en 1. Un calcul direct à partir de l'expression du théorème 1 montre que celle-ci vaut :

$$H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}. \tag{1}$$

En particulier, lorsque n tend vers l'infini, ce nombre est équivalent à $\ln n$. De même, en considérant la dérivée seconde de P_n, on peut déterminer la variance du nombre de cycles d'une permutation de $\mathfrak{S}_n$. On trouve :

$$\left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right) - \left(1 + \frac{1}{2^2} + \cdots + \frac{1}{n^2}\right)$$

ce qui est encore de l'ordre de $\ln n$; l'écart type est donc de l'ordre de $\sqrt{\ln n}$.

1.1 Première démonstration *via* une formule de récurrence

La première méthode consiste simplement à établir une relation de récurrence sur les $c_n(k)$. Nous allons, pour cela, dénombrer les permutations $\sigma \in \mathfrak{S}_n$ telles que $\mathrm{cyc}(\sigma) = k$ en les comptant séparément selon la valeur de $\sigma(n)$. Si $\sigma(n) = n$, on remarque que se donner une telle permutation revient simplement à se donner une permutation de $\{1, \ldots, n-1\}$ ayant $(k-1)$ cycles (puisque n est tout seul dans son cycle). Il y a donc $c_{n-1}(k-1)$ permutations qui relèvent de ce cas.

Examinons maintenant le cas où $\sigma(n)$ est un entier m fixé strictement inférieur à n. L'entier n apparaît alors dans un cycle de σ qui est de longueur au moins 2 (puisqu'il contient au moins n et m) et on peut construire une permutation τ de $\{1, \ldots, n-1\}$ simplement en retirant n de ce cycle et en laissant les autres cycles inchangés. Par construction, il est évident que τ a encore k cycles. Par ailleurs, on peut reconstruire σ à partir de τ et l'entier m comme suit : on regarde le cycle de τ qui contient m et, dans ce cycle, on insère l'entier n juste avant m. On déduit de cela qu'il y a $c_{n-1}(k)$ permutations à k cycles telles $\sigma(n)$ est égal à un entier $m < n$ fixé.

On aboutit à $c_n(k) = c_{n-1}(k-1) + (n-1)c_{n-1}(k)$. En tenant compte du fait que $c_{n-1}(0) = c_{n-1}(n) = 0$ trivialement, et en sommant l'égalité précédente pour k variant de 1 à n, il vient :

$$P_n(q) = \sum_{k=1}^{n} c_n(k) q^k = \sum_{k=1}^{n-1} c_{n-1}(k) q^{k+1} + (n-1) \cdot \sum_{k=1}^{n-1} c_{n-1}(k) q^k = (q+n-1) \cdot P_{n-1}(q).$$

Le théorème 1 s'ensuit par récurrence après avoir remarqué que $P_1(q) = q$.

1.2 Deuxième démonstration *via* la notion de record

Si n est un entier, posons $[n] = \{0, \ldots, n-1\}$ et $S_n = [1] \times [2] \times \cdots \times [n]$. Il est clair que $[n]$ est de cardinal n et, par voie de conséquence, que S_n est de cardinal $n!$. Le principe de la deuxième démonstration est de construire une bijection

$$F : \mathfrak{S}_n \to S_n, \quad \sigma \mapsto (F_1(\sigma), F_2(\sigma), \ldots, F_n(\sigma))$$

telle que pour tout $\sigma \in \mathfrak{S}_n$, on ait :

$$\mathrm{cyc}(\sigma) = \mathrm{Card}\left\{ i \in \{1, \ldots, n\} \mid F_i(\sigma) = 0 \right\} = \delta_0(F_1(\sigma)) + \cdots + \delta_0(F_n(\sigma)) \tag{2}$$

où δ_0 est la fonction qui vaut 1 en 0 et 0 ailleurs. Le théorème 1 en découlera facilement. En effet, connaissant F, on peut écrire :

$$P_n(q) = \sum_{(k_i) \in S_n} q^{\delta_0(k_1) + \cdots + \delta_0(k_n)} = \prod_{i=1}^{n} \left(\sum_{k=0}^{i-1} q^{\delta_0(k)} \right) = q(q+1)\cdots(q+n-1).$$

Reste donc à construire F. Nous procédons en deux étapes : nous construisons tout d'abord une bijection $\mathcal{B} : \mathfrak{S}_n \to \mathfrak{S}_n$ qui transforme « nombre de cycles » en « nombre de records[1] » puis une bijection $\mathrm{inv} : \mathfrak{S}_n \to S_n$ qui vérifie une propriété analogue à (2) sauf que le nombre de cycles est remplacé par le nombre de records. Il suffira finalement de poser $F = \mathrm{inv} \circ \mathcal{B}$.

[1] Nous définirons également ce qu'est un record.

1.2.1 Records d'une permutation : construction de $\mathcal{B}$

Définition 2. Un *record* d'une permutation $\sigma \in \mathfrak{S}_n$ est un entier $\sigma(i)$ tel que $\sigma(j) < \sigma(i)$ pour tout $j < i$. Si $\sigma(i)$ est un record de σ, l'entier i est appelé sa *position*.

Il est commode pour bien comprendre la définition précédente d'imaginer que les entiers de 1 à n sont des candidats prenant part à une compétition dans l'ordre indiqué par la permutation σ, et dont la performance est fonction de leur grandeur. Dans ces conditions, le notion de record correpond au sens usuel du terme.

Construisons à présent la bijection $\mathcal{B}$, en commençant par sa réciproque $\mathcal{B}^{-1}$ qui est légèrement plus facile. Considérons σ une permutation de $\mathfrak{S}_n$ que l'on écrit en ligne : cela signifie que l'on écrit sur une même ligne de la gauche vers la droite les nombres $\sigma(1), \sigma(2), \ldots, \sigma(n)$ dans cet ordre. Plaçons ensuite des barres verticales à la gauche de chacun des records. Comme $\sigma(1)$ est toujours un record, on a nécessairement placé une barre tout à gauche. Rajoutons également une barre tout à droite. Ce faisant, on est en train de regrouper les nombres de 1 à n en k paquets, chaque paquet étant délimité par deux barres consécutives. Par exemple, si σ est la permutation 3-2-4-1-7-9-8-5-6, on dessine :

$$\big|\ 3 \quad 2\ \big|\ 4 \quad 1\ \big|\ 7\ \big|\ 9 \quad 8 \quad 5 \quad 6\ \big|$$

et les paquets sont $(3,2)$, $(4,1)$, *etc.* On définit alors $\mathcal{B}^{-1}(\sigma)$ en convenant que ses cycles sont exactement les paquets précédents et que $\mathcal{B}^{-1}(\sigma)$ agit à l'intérieur d'un cycle donné en envoyant un entier qui n'est pas le dernier du cycle sur celui qui vient juste après dans l'écriture en ligne de σ. Dans notre exemple, la permutation $\mathcal{B}^{-1}(\sigma)$ échange 3 et 2 (c'est le premier paquet), échange 4 et 1 (c'est le deuxième paquet), *etc.* Il est évident que $\mathcal{B}^{-1}(\sigma)$ a autant de cycles que σ n'a de records. Il reste à démontrer que $\mathcal{B}^{-1}$ est une bijection et pour cela, il suffit de construire son inverse $\mathcal{B}$. Pour cela, partant d'une permutation $\tau \in \mathfrak{S}_n$,

1. on écrit τ comme un produit de cycles à supports disjoints ;
2. pour chaque cycle, on écrit son élément maximal et à la suite les itérés successifs de cet élément jusqu'à avoir parcouru tout le cycle ;
3. on met finalement bout à bout les écritures précédentes en prenant soin de trier les cycles par ordre croissant de leurs éléments maximaux ;

Il est alors facile de vérifier que si l'on obtient comme ceci l'écriture en ligne d'une permutation σ telle que $\mathcal{B}^{-1}(\sigma) = \tau$. On démontre enfin également que la composée dans l'autre sens $\mathcal{B} \circ \mathcal{B}^{-1}$ est l'identité. En conclusion :

Théorème 3. *L'application $\mathcal{B} : \mathfrak{S}_n \to \mathfrak{S}_n$ est une bijection qui transforme une permutation à k cycles en permutation à k records.*

1.2.2 Nombre d'inversions : construction de inv

Nous en arrivons à présent à la construction de l'application inv que nous avons évoquée en introduction du §1.2. Elle est définie comme suit :

$$\mathrm{inv} : \mathfrak{S}_n \to S_n, \quad \sigma \mapsto (\mathrm{inv}_1(\sigma), \mathrm{inv}_2(\sigma), \ldots, \mathrm{inv}_n(\sigma))$$

où $\mathrm{inv}_i(\sigma)$ est le nombre d'entiers $j < i$ tels que $\sigma(j) > \sigma(i)$. Il est évident que $\sigma(i)$ est un record de σ si, et seulement si $\mathrm{inv}_i(\sigma) = 0$. Ainsi si on note $\mathrm{rec}(\sigma)$ le nombre de records de σ, on a

$$\mathrm{rec}(\sigma) = \mathrm{Card}\left\{ i \in \{1, \ldots, n\} \mid \mathrm{inv}_i(\sigma) = 0 \right\} = \delta_0(\mathrm{inv}_1(\sigma)) + \cdots + \delta_0(\mathrm{inv}_n(\sigma))$$

c'est-à-dire l'équivalent de la formule (2) que nous voulions. Le théorème classique suivant, laissé en exercice au lecteur, permet de conclure notre démonstration.

Théorème 4. *L'application* inv $: \mathfrak{S}_n \to S_n$ *est une bijection.*

À nouveau, à titre d'exercice, le lecteur pourra également chercher à décrire la bijection inverse de inv.

Signalons enfin que a somme $\mathrm{inv}(\sigma) = \mathrm{inv}_1(\sigma) + \cdots + \mathrm{inv}_n(\sigma)$ est un invariant classique de la permutation σ qui s'appelle son *nombre d'inversions*. Il est relié à la signature $\varepsilon(\sigma)$ par $\varepsilon(\sigma) = (-1)^{\mathrm{inv}(\sigma)}$. Des méthodes semblables à celles que nous avons utilisées pour démontrer le théorème 1 permettent d'obtenir des formules plus générales — que nous laissons à nouveau en exercice au lecteur — comme par exemple :

$$\sum_{\sigma \in \mathfrak{S}_n} x^{\mathrm{inv}(\sigma)} y^{\mathrm{rec}(\sigma)} = \prod_{i=1}^{n} (y + x + x^2 + \cdots + x^{i-1}).$$

En particulier, pour $x = y = 2$, cette formule implique $\sum_{\sigma \in \mathfrak{S}_n} 2^{\mathrm{inv}(\sigma) + \mathrm{rec}(\sigma)} = 2^{n(n+1)/2}$.

1.3 Troisième démonstration *via* la permutation des perdants

La dernière démonstration que nous souhaitons présenter — qui est très proche de la précédente — fait partie de la famille des preuves dites bijectives que les combinatoriciens apprécient en général pour leur élégance. Dans son sens le plus strict, une preuve bijective d'une identité combinatoire $a = b$ est une démonstration de cette identité dans laquelle on construit un ensemble A de cardinal a, un ensemble B de cardinal b et une bijection entre A et B ; il est alors clair que l'on a montré $a = b$.

Dans notre cas, nous allons faire quelque chose de très légèrement différent : étant donné un entier q strictement positif[2], nous allons construire un ensemble $A_{q,n}$ de cardinal $q(q+1)\cdots(q+n-1)$, ainsi qu'une application $G'_{q,n} : A_{q,n} \to \mathfrak{S}_n$ telle que :

$$\text{pour tout } \sigma \in \mathfrak{S}_n, \quad \operatorname{Card}(G'_{q,n})^{-1}(\sigma) = q^{\operatorname{cyc}(\sigma)}.$$

Il est clair que l'identité du théorème 1 en résultera. En fait, plutôt que de construire $G'_{q,n}$ comme nous venons de le dire, nous allons construire une application $G_{q,n} : A_{q,n} \to \mathfrak{S}_n$ vérifiant :

$$\text{pour tout } \sigma \in \mathfrak{S}_n, \quad \operatorname{Card} G_{q,n}^{-1}(\sigma) = q^{\operatorname{rec}(\sigma)}. \tag{3}$$

Bien entendu, on passe de $G'_{q,n}$ à $G_{q,n}$ et réciproquement en composant dans le bon sens par la bijection $\mathcal{B}$ ou son inverse. Notons enfin avant de nous lancer dans la construction que, pour $q = 1$, il suffit de prendre $A_{q,n} = \mathfrak{S}_n$ et $G_{q,n} = \mathrm{id}$; nous oublierons donc ce cas dans la suite.

1.3.1 Le cas $q = 2$: la permutation des perdants

On suppose pour commencer $q = 2$. Dans ce cas, l'ensemble $A_{2,n}$ doit être de cardinal $(n+1)!$; un candidat raisonnable est donc $A_{2,n} = \mathfrak{S}_{n+1}$. Il nous reste à définir l'application $G_{2,n}$. On introduit pour cela la définition suivante.

Définition 5. Soit $\sigma \in \mathfrak{S}_{n+1}$. La *permutation des perdants* de σ est la permutation $\sigma' \in \mathfrak{S}_n$ définie par récurrence en décrétant que $\sigma'(i)$ est le plus petit élément de l'ensemble différence

$$\big\{\, \sigma(1), \sigma(2), \ldots, \sigma(i+1) \,\big\} \setminus \big\{\, \sigma'(1), \ldots, \sigma'(i-1) \,\big\}. \tag{4}$$

On montre immédiatement par récurrence que l'ensemble (4) est toujours de cardinal 2 (*i.e.* que l'ensemble que l'on ôte est toujours inclus dans le premier), et plus précisément qu'il contient exactement l'élément $\sigma(i+1)$, et le dernier record de σ apparaissant avant i. Ainsi si $\sigma(i+1)$ n'est pas un record de σ, on a $\sigma'(i) = \sigma(i+1)$, tandis que dans le cas contraire, $\sigma'(i)$ est le record précédent de σ. Ainsi, si l'on reprend la métaphore de la compétition, la permutation des perdants n'est autre que la liste ordonnée des candidats qui n'ont pas décroché le record ou à qui celui-ci a été volé.

Ainsi, la permutation des perdants se calcule simplement par la méthode suivante :

1. on écrit σ en ligne (ce qui, rappelons-le, signifie que l'on écrit les nombres $\sigma(1)$, $\sigma(2)$, *etc.* les uns à la suite des autres) ;
2. on entoure les records de σ ;
3. on effectue une permutation circulaire de la gauche vers la droite des entiers entourés (et uniquement ceux-ci) ;
4. on efface le premier entier (qui est nécessairement entouré et égal à $n+1$).

Ce qu'il reste après ces manipulations est l'écriture en ligne de σ', la permutation des perdants de σ (on conseille au lecteur de traiter un exemple par lui-même). En fait, on obtient même un peu plus puisque certains entiers sont entourés ; ce sont par construction les records de σ auxquels on a retiré $n+1$. On peut reformuler ce qui précède de façon plus formelle comme suit : si $\mathcal{P}(X)$ désigne l'ensemble des parties d'un ensemble X, la construction est donnée par l'application

$$f : \mathfrak{S}_{n+1} \to \mathfrak{S}_n \times \mathcal{P}(\{1, \ldots, n\}), \quad \sigma \mapsto (\sigma', \operatorname{Rec}(\sigma) \backslash \{n+1\})$$

où $\operatorname{Rec}(\sigma)$ désigne l'ensemble des records de σ.

[2] L'argument que nous allons donner ne permet de démontrer l'égalité du théorème 1 que sous cette hypothèse supplémentaire. Toutefois, il résulte facilement de là, le théorème dans toute sa généralité étant donné que polynômes qui coïncident sur $\mathbb{N}^\star$ sont égaux.

Proposition 6. *L'application f est injective et son image est exactement formée des couples (τ, A) pour lesquels A est un sous-ensemble de* $\mathrm{Rec}(\tau)$.

Démonstration. Il est clair que tout record de σ différent de $n+1$ est un encore record de σ'. Ainsi l'image de f est bien incluse dans le sous-ensemble défini dans la proposition. Par ailleurs, étant donné un couple (τ, A) vérifiant $A \subset \mathrm{Rec}(\tau)$, on construit facilement son unique antécédent par f en « défaisant » une par une les étapes de la construction de f comme suit :

1. on écrit τ en ligne ;
2. on entoure les éléments de A ;
3. on ajoute l'entier $n+1$ tout à gauche et on l'entoure ;
4. on effectue une permutation circulaire de la droite vers la gauche des entiers entourés (et uniquement ceux-ci).

La lecture des entiers obtenus donne alors l'unique permutation de $\mathfrak{S}_n$ qui s'envoie sur (τ, A). En effet, il suffit de démontrer que les entiers entourés sont exactement les records de cette permutation. Or, si l'entier k est entouré, c'est un record car il était déjà un record de τ et il s'est déplacé vers la gauche (*i.e.* il a joué plus tôt), tandis que si k n'est pas entouré, l'entier entouré qui le suit est plus grand et passe devant après la manipulation (s'il n'y a aucun tel entier, c'est $n+1$ qui passe devant), il subtilise donc le record à k dans le cas où celui-ci le détenait. □

Il résulte directement de la proposition que si l'application $G_{2,n} : \mathfrak{S}_{n+1} \to \mathfrak{S}_n$, $\sigma \mapsto \sigma'$ vérifie la condition (3). Nous avons donc achevé la troisième démonstration du théorème 1 lorsque $q = 2$.

1.3.2 Le cas général : itération de la permutation des perdants

On en vient maintenant au cas général. Posons $m = q-1$ et notons $\mathfrak{S}_{[n+1,n+m]}$ le sous-groupe de $\mathfrak{S}_{n+m}$ formé par les permutations qui fixent point par point les entiers $1, 2, \ldots, n$. Un élément de $\mathfrak{S}_{[n+1,n+m]}$ peut donc être vu comme une permutation de l'ensemble $\{n+1, \ldots, n+m\}$ de cardinal m. L'ensemble $A_{q,n}$ que nous considérons est le quotient $\mathfrak{S}_{[n+1,n+m]} \backslash \mathfrak{S}_{n+m}$: c'est, par définition, l'ensemble des classes à *droite* de $\mathfrak{S}_{n+m}$ selon le sous-groupe $\mathfrak{S}_{[n+1,n+m]}$, c'est-à-dire les sous-ensembles de $\mathfrak{S}_{n+m}$ de la forme $\mathfrak{S}_{[n+1,n+m]} \cdot \sigma$ pour $\sigma \in \mathfrak{S}_{n+m}$. Son cardinal s'obtient en divisant celui de $\mathfrak{S}_{n+m}$ par celui de $\mathfrak{S}_{[n+1,n+m]}$ et donc vaut $\frac{(m+n)!}{m!} = (m+1)(m+2)\cdots(m+n) = q(q+1)\cdots(q+n-1)$, comme souhaité.

L'application $G_{q,n} : A_{q,n} \to \mathfrak{S}_n$, quant à elle, se définit à partir de la m-ième itérée de la construction « permutation des perdants ». Plus précisément, pour $\sigma \in \mathfrak{S}_{n+m}$, définissons les $\sigma^{(i)}$ $(0 \leqslant i < n+m)$ par récurrence en convenant que $\sigma^{(0)} = \sigma$ et $\sigma^{(i+1)}$ est la permutation des perdants de $\sigma^{(i)}$. On a $\sigma^{(i)} \in \mathfrak{S}_{n+m-i}$, et donc en particulier $\sigma^{(m)} \in \mathfrak{S}_n$. Par ailleurs, à partir de la définition de la permutation des perdants, on démontre facilement par récurrence que[3] :

$$\forall \sigma \in \mathfrak{S}_{n+m}, \forall \tau \in \mathfrak{S}_{[n+1,n+m]}, \quad (\tau \circ \sigma)^{(m)} = \sigma^{(m)}.$$

Il en résulte que l'application $\sigma \mapsto \sigma^{(m)}$ définit par passage au quotient une application $G_{q,n} : A_{q,n} \to \mathfrak{S}_n$. Pour terminer la démonstration, il reste donc à montrer qu'un élément $\tau \in \mathfrak{S}_n$ a exactement $q^{\mathrm{rec}(\tau)}$ antécédents par $G_{q,n}$. Pour cela, on considère l'application f_m qui à une permutation $\sigma \in \mathfrak{S}_{n+m}$ associe le couple $f_m(\sigma) = (\sigma^{(m)}, g_m(\sigma))$ où $g_m(\sigma) : \mathrm{Rec}(\sigma^{(m)}) \to [q] = \{0, 1, \ldots, m\}$ est la fonction qui, à un record r de $\sigma^{(m)}$, associe le plus petit entier i tel que r soit aussi un record de $\sigma^{(i)}$. On construit comme ceci une application $f_m : \mathfrak{S}_{n+m} \to E_{q,n}$ où, par définition, $E_{q,n}$ est formé des couples (τ, g) où $\tau \in \mathfrak{S}_n$ et g est une fonction quelconque définie sur $\mathrm{Rec}(\tau)$ et à valeurs dans $[q] = \{0, \ldots, m\}$. La proposition suivante, finalement, conclut la preuve.

Proposition 7. *Pour tout $\sigma \in \mathfrak{S}_{n+m}$ et tout $\tau \in \mathfrak{S}_{[n+1,n+m]}$, on a $f_m(\tau \circ \sigma) = f_m(\sigma)$. De plus, l'application $A_{q,n} \to E_{q,n}$ déduite de f_m par passage au quotient est une bijection.*

Démonstration. Exercice. □

Remarque 8. Il est intéressant de faire le lien entre les constructions des deuxième et troisième démonstrations. Voici ce que l'on peut démontrer à ce sujet (et que nous laissons à nouveau en exercice au lecteur).

1. l'application $\mathrm{inv}_{\leqslant n} : \mathfrak{S}_{[n+1,n+m]} \backslash \mathfrak{S}_{n+m} \to [m+1] \times \cdots \times [m+n]$, $\sigma \mapsto (\mathrm{inv}_{k_1}(\sigma), \ldots, \mathrm{inv}_{k_n}(\sigma))$, où $k_1 < k_2 < \cdots < k_n$ sont les entiers tels que $\sigma(k_i) \leqslant n$, est bien définie et elle réalise une bijection ;

[3] En fait, l'égalité est encore vraie pour $\tau \in \mathfrak{S}_{[n,n+m]}$, mais cela ne sera pas utile dans la suite.

2. la composée $\mathrm{inv} \circ G_{q,n} \circ (\mathrm{inv}_{\leqslant n})^{-1} : [m+1] \times \cdots \times [m+n] \to [1] \times \cdots \times [n]$ est donnée par la formule $(k_1, \ldots, k_n) \mapsto (\max(0, k_1 - m), \ldots, \max(0, k_n - m))$.

À partir de là, on peut combiner les deuxième et troisième démonstrations que nous avons données pour obtenir une nouvelle preuve bijective du théorème 1 basée sur l'étude de l'application $[m+1] \times \cdots \times [m+n] \to \mathfrak{S}_n$, $(k_1, \ldots, k_n) \mapsto \mathcal{B}^{-1} \circ \mathrm{inv}^{-1}(\max(0, k_1 - m), \ldots, \max(0, k_n - m))$.

Exercice. Reprendre la démonstration qui précède en remplaçant le quotient $\mathfrak{S}_{[n+1,n+m]} \backslash \mathfrak{S}_{n+m}$ par $\mathfrak{S}_{n+m}/\mathfrak{S}_m$ (ensemble des classes à gauche) où $\mathfrak{S}_m$ est plongé de façon habituelle dans $\mathfrak{S}_{n+m}$ (un élément de $\mathfrak{S}_m$ permute les m premiers entiers).

2 Interprétation probabiliste des records et applications

Nous interprétons ici de manière probabiliste le théorème 4 en remarquant que pour une permutation aléatoire, choisie uniformément parmi celles de longueur n, les records apparaissent de manière indépendante (ceci sera rigoureusement défini un plus plus loin, voir théorème 14). Ceci nous servira pour étudier le nombre de cycles d'une grande permutation. Avant de continuer, précisons rapidement le langage probabiliste que nous utilisons. Insistons sur le fait que les notions introduites le sont dans des cas très particuliers et que, dans une certaine mesure, ceci peut être généralisé (nous renvoyons le lecteur intéressé à [4, 5]).

2.1 Introduction du langage probabiliste

Définition 9. Nous noterons $\Omega = \mathfrak{S}_n$, que nous appellerons *espace probabilisé*. Une permutation $\omega \in \Omega$ sera appelée *aléa* et une partie de Ω sera appelée *événement*. Une *variable aléatoire* (sous-entendue réelle ou complexe) est une application $X : \Omega \to \mathbb{R}$ ou $\mathbb{C}$. La moyenne, ou espérance, d'une variable aléatoire X, notée $\mathbb{E}[X]$, est définie par[4] :

$$\mathbb{E}[X] = \frac{1}{n!} \sum_{\omega \in \Omega} X(\omega).$$

Pour une partie $A \subset \Omega$, la *probabilité* de l'événement A est l'espérance de la fonction indicatrice de A, $\mathbb{P}[A] = \mathbb{E}[1_A]$, qui est donc égale au nombre de permutations de longueur n appartenant à A, divisé par $n!$, qui est le nombre total de permutations de longueur n.

Les fonctions cyc et rec qui donnent respectivement le nombre de cycles et de records sont des exemples de variables aléatoires définies sur $\Omega = \mathfrak{S}_n$. Pour éviter les confusions, nous les noterons dans la suite cyc_n et rec_n en précisant en indice l'entier n qui détermine leur ensemble de définition. Dans un autre registre, soulignons qu'intuitivement, $\mathbb{P}[A]$ représente la probabilité qu'une permutation aléatoire, choisie uniformément parmi celles de longueur n, appartienne à la partie A.

Remarque 10. D'une part, pour des variables aléatoires $X_1, \ldots, X_k : \Omega \to \mathbb{R}$, la définition de l'espérance implique que $\mathbb{E}[X_1 + \cdots + X_n] = \mathbb{E}[X_1] + \cdots + \mathbb{E}[X_n]$ et, d'autre part, Si Ω est l'union disjointe de deux ensembles A et B, alors la définition précédente nous fournit $1 = \mathbb{P}[A] + \mathbb{P}[B]$.

Définition 11. Pour des variables aléatoires $X_1, X_2, \ldots, X_k$ et des intervalles $I_1, \ldots, I_k$, on note :

$$\mathbb{P}\left[X_1 \in I_1, \ldots, \ldots, X_k \in I_k\right]$$

la probabilité de l'événement $\{\omega \in \Omega;\ X_1(\omega) \in I_1, \ldots, X_k(\omega) \in I_k\}$. Ceci est juste une commodité de notation, qui permet d'écrire des formules plus simplement.

La propriété clé intervenant dans l'étude des records est l'indépendance, que nous définissions maintenant.

Définition 12. Soient $X_1, X_2 \ldots, X_k$ des variables aléatoires à valeurs dans $\mathbb{N}$. On dit que ces variables aléatoires sont *indépendantes* si pour tous entiers $u_1, \ldots, u_k$:

$$\mathbb{P}[X_1 = u_1, X_2 = u_2, \ldots, X_k = u_k] = \mathbb{P}[X_1 = u_1]\mathbb{P}[X_2 = u_2] \cdots \mathbb{P}[X_k = u_k].$$

Un des intérêts de l'indépendance réside dans la faculté de pouvoir calculer des espérances faisant intervenir n'importe quelles fonctions de nos variables aléatoires indépendantes, comme l'illustre la propriété suivante.

[4] Il est sous-entendu que nous travaillons avec la mesure uniforme, c'est-à-dire que deux permutations différentes de même longueur ont autant de chance d'apparaître.

Proposition 13. *Soient $X_1, X_2 \dots, X_k$ des variables aléatoires à valeurs dans $\mathbb{N}$ et $f_1, \dots, f_k$ des applications de $\mathbb{N}$ dans $\mathbb{C}$. Alors :* $\mathbb{E}[f_1(X_1)f_2(X_2)\cdots f_k(X_k)] = \mathbb{E}[f_1(X_1)]\mathbb{E}[f_2(X_2)]\cdots\mathbb{E}[f_k(X_k)]$.

Démonstration. On écrit :

$$\begin{aligned}
\mathbb{E}[f_1(X_1)f_2(X_2)\cdots f_k(X_k)] &= \frac{1}{n!}\sum_{\omega\in\Omega} f_1(X_1(\omega))f_2(X_2(\omega))\cdots f_k(X_k(\omega)) \\
&= \sum_{u_1,\dots,u_k\geqslant 0} f_1(u_1)f_2(u_2)\cdots f_k(u_k)\frac{1}{n!}\sum_{\omega\in\Omega} 1_{X_1(\omega)=u_1, X_2(\omega)=u_2,\dots,X_k(\omega)=u_k} \\
&= \sum_{u_1,\dots,u_k\geqslant 0} f_1(u_1)f_2(u_2)\cdots f_k(u_k)\mathbb{P}[X_1=u_1,\dots,X_k=u_k] \\
&= \sum_{u_1,\dots,u_k\geqslant 0} f_1(u_1)f_2(u_2)\cdots f_k(u_k)\mathbb{P}[X_1=u_1]\cdots\mathbb{P}[X_k=u_k] \text{ par indépendance} \\
&= \mathbb{E}[f_1(X_1)]\mathbb{E}[f_2(X_2)]\cdots\mathbb{E}[f_k(X_k)].
\end{aligned}$$

□

2.2 Interprétation probabiliste du théorème 4

Rappelons qu'on note $\Omega = \mathfrak{S}_n$. Le théorème suivant, obtenu par Rényi [7], formalise l'idée que les records apparaissent indépendamment au sein d'une permutation aléatoire uniforme, et sera crucial.

Théorème 14. *Pour $1 \leqslant i \leqslant n$, on définit la variable aléatoire $X_i : \Omega \to \{0,1\}$ de la manière suivante :*

$$X_i(\omega) = \begin{cases} 1 \text{ si } i \text{ est une position de record de } \omega \\ 0 \text{ sinon,} \end{cases}$$

de sorte que pour tous $\omega \in \Omega$, $\mathrm{rec}(\omega) = X_1(\omega) + \cdots + X_n(\omega)$. Alors $X_1, X_2, \dots, X_n$ sont indépendantes, $\mathbb{P}[X_i = 1] = \frac{1}{i}$ et $\mathbb{P}[X_i = 0] = 1 - \frac{1}{i}$.

Démonstration. Fixons un entier $1 \leqslant i \leqslant n$ et calculons $\mathbb{P}[X_i = 1]$ en remarquant que i est une position de record d'une permutation ω si, et seulement si $\mathrm{inv}_i(\sigma) = 0$. On a :

$$\begin{aligned}
\mathbb{P}[X_i = 1] &= \frac{1}{n!}\mathrm{Card}\big(\{\omega\in\Omega;\, X_i(\omega)=1\}\big) = \frac{1}{n!}\mathrm{Card}\big(\{\omega\in\Omega;\, \mathrm{inv}_i(\omega)=0\}\big) \\
&= \frac{1}{n!}\mathrm{Card}\big(\{(u_1,\dots,u_n)\in[1]\times[2]\times\cdots\times[n];\, u_i=0\}\big) \text{ d'après le théorème 4} \\
&= \frac{1}{n!}\frac{n!}{i} = \frac{1}{i}.
\end{aligned}$$

La remarque 10 nous fournit alors $\mathbb{P}[X_i = 0] = 1 - \frac{1}{i}$. Montrons maintenant l'indépendance des variables aléatoires $X_1, \dots, X_n$ en établissant d'abord que, pour des entiers $1 \leqslant i_1 < \cdots < i_k \leqslant n$, $\mathbb{P}[X_{i_1} = 1, X_{i_2} = 1, \dots, X_{i_k} = 1] = \mathbb{P}[X_{i_1} = 1]\mathbb{P}[X_{i_2} = 1]\cdots\mathbb{P}[X_{i_k} = 1]$. Comme ci-dessus, le théorème 4 permet d'écrire :

$$\begin{aligned}
\mathbb{P}[X_{i_1}=1, X_{i_2}=1,\dots,X_{i_k}=1] &= \frac{1}{n!}\mathrm{Card}\big(\{(u_1,\dots,u_n)\in[1]\times[2]\times\cdots\times[n];\, u_{i_1}=0,\dots,u_{i_k}=0\}\big) \\
&= \frac{1}{n!}\frac{n!}{i_1\cdots i_k} = \frac{1}{i_1}\frac{1}{i_2}\cdots\frac{1}{i_k} = \mathbb{P}[X_{i_2}=1]\cdots\mathbb{P}[X_{i_k}=1].
\end{aligned}$$

On en déduit, en utilisant la remarque 10, que $X_1, \dots X_n$ sont indépendantes (exercice laissé au lecteur). □

À titre d'illustration, re-démontrons le théorème 1. On a :

$$\begin{aligned}
\sum_{\omega\in\Omega} q^{\mathrm{cyc}(\omega)} &= \sum_{\omega\in\Omega} q^{\mathrm{rec}(\omega)} \quad \text{d'après le théorème 3} \\
&= \sum_{\omega\in\Omega} q^{X_1(\omega)+\cdots+X_n(\omega)} = n!\,\mathbb{E}\left[q^{X_1+\cdots+X_n}\right] = n!\,\mathbb{E}\left[q^{X_1}\right]\cdots\mathbb{E}\left[q^{X_n}\right] \quad \text{d'après la proposition 13} \\
&= n!\left(1-\frac{1}{1}+\frac{1}{1}q\right)\left(1-\frac{1}{2}+\frac{1}{2}q\right)\cdots\left(1-\frac{1}{n}+\frac{1}{n}q\right) = q(q+1)\cdots(q+n-1).
\end{aligned}$$

En regardant ceci de plus près, on voit qu'on n'a fait que paraphraser la deuxième démonstration du théorème 1. Cependant, cette méthode de calcul sera utilisée dans les deux prochaines sections.

Exercice. Pour $\sigma \in \mathfrak{S}_n$, on note $\mathrm{srec}(\sigma)$ la somme des positions des records de σ. Calculer $\sum_{\sigma\in\mathfrak{S}_n} q^{\mathrm{srec}(\sigma)}$.

2.3 Étude asymptotique du nombre de cycles d'une permutation

Nous nous intéressons ici au comportement asymptotique de $c_n(k)$ lorsque n tend vers l'infini. Lorsque k est fixé, on voit que dans cette limite, $c_n(k)$ tend vers l'infini. Nous voudrions avoir une estimée quantitative de ce phénomène, autrement dit, nous voudrions trouver un équivalent de $c_n(k)$ lorsque n tend vers l'infini, valable *pour tout* k. Remarquons que k prend un nombre variable de valeurs possibles en fonction de n. Pour pallier cette difficulté, nous effectuons un changement de variable afin de ramener la plage des valeurs possibles à un intervalle qui ne dépend pas de n en introduisant la variable $x = k/n$. Plus précisément définissons, pour $0 \leqslant x \leqslant 1$, l'application $f_n(x)$ comme suit :

$$f_n(x) = \begin{cases} c_n\left([nx]\right) & \text{si } x \geqslant \frac{1}{n}, \\ c_n(1) & \text{sinon} \end{cases}, \tag{5}$$

où $[x]$ désigne la partie entière de x. Nous allons démontrer le théorème suivant, qui régit le comportement asymptotique de la suite de fonctions f_n et donc des entiers $c_n(k)$.

Théorème 15 ([3])**.** *Lorsque n tend vers l'infini, la suite de fonctions $\{\frac{\ln(f_n)}{n\ln(n)}; n \in \mathbb{N}^+\}$ converge uniformément par rapport à x sur l'intervalle $[0,1]$ vers l'application $x \mapsto 1-x$, avec une précision $\mathcal{O}\left(\frac{1}{\ln n}\right)$. En d'autres termes, il existe une constante C telle que pour tout entier $n \geqslant 2$:*

$$\sup_{x\in[0,1]} \left| \frac{\ln(f_n(x))}{n\ln n} - (1-x) \right| \leqslant \frac{C}{\ln n}\,.$$

Insistons sur le fait que le théorème est de nature purement combinatoire et déterministe faisant intervenir les cycles, alors que sa preuve utilise la bijection avec les records et des idées probabilistes qui en découlent. Plus précisément, la preuve de ce théorème passe par une interprétation probabiliste des coefficients $c_n(k)$ *via* le théorème 14, constituant notre premier lemme. Dans la suite, $k, n \in \mathbb{N}^*$ sont des entiers tels que $k \leqslant n$.

Lemme 16. *On a :*

$$\mathbb{P}(\mathrm{cyc}_n = k) = \sum_{\substack{v_1<v_2<\cdots<v_k\leqslant n \\ v_1=1}} \frac{1}{v_1 v_2 \cdots v_k}\left(1-\frac{1}{v_{k+1}}\right)\cdots\left(1-\frac{1}{v_n}\right) \tag{6}$$

où, par définition, les v_i pour $i > k$ sont les éléments de l'ensemble $\{1,\ldots,n\}\backslash\{v_1,\ldots,v_k\}$ triés par ordre croissant.

Démonstration. D'après le théorème 3, on a $\mathbb{P}(\mathrm{cyc}_n = k) = \mathbb{P}(\mathrm{rec}_n = k)$. En comptant les permutations de longueur n suivant la position de leurs records, on trouve, en reprenant les notations et résultats du théorème 14 :

$$\begin{aligned}
\mathbb{P}(\mathrm{rec}_n = k) &= \sum_{\substack{v_1<v_2<\cdots<v_k\leqslant n \\ v_1=1}} \mathbb{P}[v_1,\ldots,v_k \text{ sont des positions de record et } v_{k+1},\ldots,v_n \text{ n'en sont pas}] \\
&= \sum_{\substack{v_1<v_2<\cdots<v_k\leqslant n \\ v_1=1}} \mathbb{P}[X_{v_1} = X_{v_2} = \cdots = X_{v_k} = 1, X_{v_{k+1}} = \cdots = X_{v_n} = 0] \\
&= \sum_{\substack{v_1<v_2<\cdots<v_k\leqslant n \\ v_1=1}} \mathbb{P}[X_{v_1}=1]\cdots\mathbb{P}[X_{v_k}=1]\mathbb{P}[X_{v_{k+1}}=0]\cdots\mathbb{P}[X_{v_n}=0] \qquad \text{par indépendance} \\
&= \sum_{\substack{v_1<v_2<\cdots<v_k\leqslant n \\ v_1=1}} \frac{1}{v_1 v_2 \cdots v_k}\left(1-\frac{1}{v_{k+1}}\right)\cdots\left(1-\frac{1}{v_n}\right).
\end{aligned}$$

□

Exercice. Démontrer le lemme 16 à partir de la formule $P_n(q) = q(q+1)\cdots(q+n-1)$.

L'idée de la preuve du théorème 15 consiste à remarquer que dans la somme précédente, dans la limite considérée, un seul terme est prépondérant. Le contrôle des autres termes se fait grâce à notre deuxième lemme ci-dessous. Remarquons que le plus grand terme de cette somme est inférieur à $1/k!$. En admettant que la somme soit du même ordre que cette quantité, on a $c_n([nx]) \approx n!/[nx]!$, et donc, grâce à la formule de Stirling, $\frac{\ln(c_n([nx]))}{n\ln n} \approx 1-x$ lorsque n est grand, expliquant la provenance de la quantité $1-x$. Ceci est expliqué dans ce qui suit.

Lemme 17. *Soient $x \in [\frac{1}{n}, 1]$ et $k = [nx]$. La double inégalité suivante est vérifiée :*

$$\frac{(n-[nx])!}{n!} \leqslant \mathbb{P}(\mathrm{rec}_n = k) \leqslant 2^n \frac{1}{[nx]!}$$

Démonstration. La minoration est une conséquence du fait que $\mathbb{P}(\mathrm{rec}_n = k) = c_n(k)/n!$ et que $c_n(k) \geqslant (n-k)!$ (exercice). La majoration est une conséquence du lemme 16 après avoir pris en compte les faits suivants :

(i) le nombre de n-uplets $(v_1, \ldots, v_n)$ tels que $v_1 < v_2 < \cdots < v_k \leqslant n$, $v_1 = 1$, $v_i \neq v_j$ pour $i \neq j$ et $v_{k+1} < \cdots < v_n \leqslant n$ est inférieur à 2^n,

(ii) on a $\left(1 - \frac{1}{v_{k+1}}\right) \cdots \left(1 - \frac{1}{v_n}\right) \leqslant 1$,

(iii) et, pour des entiers $1 = v_1 < v_2 < \cdots < v_k \leqslant n$, on a l'inégalité $k! \leqslant v_1 v_2 \cdots v_k$.

□

Nos deux lemmes préparatoires ayant été démontrés, tournons-nous vers la preuve du théorème 15.

Idée de la démonstration du théorème 15. Rappelons que $\mathbb{P}(\mathrm{rec}_n = k) = \frac{c_n(k)}{n!}$. En utilisant les mêmes notations que dans le lemme 17 et la fonction f_n définie en (5), on obtient :

$$\frac{\ln\left((n-[nx])!\right)}{n \ln n} \leqslant \frac{\ln(f_n(x))}{n \ln(n)} \leqslant \frac{\ln 2}{\ln n} + \frac{\ln n!}{n \ln n} - \frac{\ln([nx]!)}{n \ln n}. \tag{7}$$

Définissons $M_n(x) = \ln n \left| \frac{\ln(f_n(x))}{n \ln(n)} - (1-x) \right|$. Rappelons que nous souhaitons montrer que ceci est borné, uniformément en x, lorsque n tend vers l'infini. On commence par écrire :

$$\sup_{x \in [0,1]} M_n(x) \leqslant \sup_{x \in [0, \frac{1}{n}]} M_n(x) + \sup_{x \in [\frac{1}{n}, 1]} M_n(x)$$

L'égalité $c_n(1) = (n-1)!$ (voir par exemple le théorème 1) et le lemme 17 fournissent :

$$\sup_{x \in [0,1]} M_n(x) \leqslant \sup_{x \in [0, \frac{1}{n}]} \ln n \left| \frac{\ln(n-1)!}{n \ln n} - (1-x) \right| + \sup_{x \in [\frac{1}{n}, 1]} \ln n \left| \frac{\ln(f_n(x))}{n \ln(n)} - (1-x) \right|$$

La formule de Stirling (ou plutôt une version moins forte, à savoir $\ln n! = n \ln n + \mathcal{O}(n)$) permet d'affirmer que le premier terme est borné lorsque n tend vers l'infini.

Appelons maintenant B_n le second terme apparaissant dans le terme de droite de l'inégalité précédente. D'après l'équation (7), il existe des constantes C_1 et C_2 telles que :

$$B_n \leqslant C_1 + \sup_{x \in [\frac{1}{n}, 1]} \left| \frac{\ln n!}{n} - \frac{\ln([nx]!)}{n} - (1-x) \ln n \right| + \sup_{x \in [\frac{1}{n}, 1]} \left| \frac{\ln\left((n-[nx])!\right)}{n} - (1-x) \ln n \right| \leqslant C_2,$$

où la formule de Stirling a encore été utilisée pour écrire la deuxième inégalité. Ceci conclut la preuve. □

Exercice (difficile)**.** Obtenir un résultat similaire à celui du théorème 15 avec srec à la place du nombre de cycles (rappelons que pour $\sigma \in \mathfrak{S}_n$, on note $\mathrm{srec}(\sigma)$ la somme des positions des records de σ). Pour le lecteur intrigué, la solution se trouve dans [3].

2.4 Théorème central limite pour les cycles

Les fonctions f_n, que nous venons d'étudier, s'interprètent en termes probabilistes en disant que $\frac{f_n(x)}{n!} = \mathbb{P}[x \leqslant \frac{\mathrm{cyc}_n}{n} < x + \frac{1}{n}]$. Ainsi, le théorème 15 donne une certaine information sur le comportement des variables aléatoires $\frac{\mathrm{cyc}_n}{n}$ lorsque n tend vers l'infini. Toutefois, un petit instant de réflexion montre que la normalisation consistant à diviser par n, bien que très naturelle, n'est pas forcément la seule envisageable, ni même peut-être la plus intéressante. En effet, demandons-nous ce qu'est le nombre moyen de cycles d'une permutation de longueur n. Celui-ci a déjà été calculé grâce à la fonction génératrice P_n (voir formule (1)) et on a vu qu'il valait $1 + \frac{1}{2} + \cdots + \frac{1}{n}$. Notons au passage que cette formule se retrouve directement, à partir du théorème 14 avec des arguments probabilistes, puisque ce nombre moyen n'est autre que $\mathbb{E}[\mathrm{cyc}_n] = \mathbb{E}[\mathrm{rec}_n] = \mathbb{E}[X_1] + \cdots + \mathbb{E}[X_n]$ avec $\mathbb{E}[X_i] = \frac{1}{i}$ pour tout i. Dans tous les cas, cette moyenne est de l'ordre de $\ln n$. De même, nous avons déjà

calculé l'écart type de rec_n et vu qu'il était de l'ordre de $\sqrt{\ln n}$. Concernant la variable aléatoire cyc_n, cela signifie qu'elle se concentre autour de $\ln n$ avec un écart moyen environ égal à $\sqrt{\ln n}$. Ainsi, la normalisation $\frac{\mathrm{cyc}_n - \ln n}{\sqrt{\ln n}}$ apparaît, elle aussi, comme un bon candidat à considérer pouvant donner lieu à une convergence intéressante. C'est exactement là l'idée du théorème central limite, classique en probabilité, dont l'objectif en définitive est d'étudier les fluctuations d'une variable aléatoire autour de sa moyenne au « second ordre » (ceci sera explicité ultérieurement).

Afin de préciser la convergence qui va intervenir, nous introduisons la notion de convergence en loi.

Définition 18. Soient $X_1, X_2, \ldots$ des variables aléatoires (qui ne sont pas nécessairement définies sur le même espace de probabilité). Soit $f : \mathbb{R} \to \mathbb{R}^+$ une application continue d'intégrale 1. On dit que la suite de variables aléatoires $X_1, X_2, \ldots$ *converge en loi vers la densité* f [5] si pour tous réels $a < b$, on a :

$$\lim_{i \to +\infty} \mathbb{P}\left[X_i \in]a, b[\right] = \int_a^b f(x)dx.$$

Ainsi, intuitivement, la convergence en loi signifie que la « répartition » des valeurs de X_n, lorsque n tend vers l'infini, se « rapproche » de la répartition d'une certaine quantité[6].

Théorème 19. *La suite de variables aléatoires* $\frac{\mathrm{cyc}_n - \ln n}{\sqrt{\ln n}}$ *converge en loi vers la densité* $t \mapsto \frac{1}{\sqrt{2\pi}} e^{-t^2/2}$ *(qu'on appelle densité gaussienne, centrée, réduite). En d'autres mots, on a pour tous réels* $a < b$ *:*

$$\lim_{n \to +\infty} \mathbb{P}\left[a < \frac{\mathrm{cyc}_n - \ln n}{\sqrt{\ln n}} < b\right] = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-\frac{x^2}{2}} dx.$$

Notre ingrédient principal sera pour démontrer ce théorème[7] sur le théorème de Lévy, que nous admettrons.

Théorème 20 (de convergence de Lévy)**.** *Pour une variable aléatoire* X*, on note* ϕ_X *sa* fonction caractéristique*, qui est une application de* $\mathbb{R}$ *dans* $\mathbb{C}$ *définie par :*

$$\phi_X(t) = \mathbb{E}[e^{itX}].$$

Soient $X_1, X_2, \ldots$ *des variables aléatoires (qui ne sont pas nécessairement définies sur le même espace de probabilité) et* $f : \mathbb{R} \to \mathbb{R}^+$ *une application continue d'intégrale* 1*. Alors* $X_1, X_2, \ldots$ *converge en loi vers la densité* f *si, et seulement si, on a pour tout réel* t *:*

$$\lim_{n \to +\infty} \phi_{X_n}(t) = \int_{-\infty}^{+\infty} e^{itu} f(u)du.$$

On commence par un lemme technique mais utile.

Lemme 21. *Soit* $u \in \mathbb{C}$ *tel que* $|u| \leqslant 1/2$*. Alors* $|\ln(1+u) - u| \leqslant |u^2|$*, où* ln *désigne ici (et dans toute la suite) la détermination principale du logarithme.*

Démonstration. Laissée en exercice (on pourra par exemple utiliser un développement en série entière). □

Démonstration du théorème 19. Soit $\theta \in \mathbb{R}$ tel que $|e^{i\theta} - 1| \leqslant 1/2$. On calcule d'abord $\phi_{\mathrm{cyc}_n}(\theta)$ grâce au théorème 14 et à la partie 1.2.1 :

$$\begin{aligned}
\phi_{\mathrm{cyc}_n}(\theta) &= \mathbb{E}[e^{i\theta \mathrm{cyc}_n}] = \mathbb{E}[e^{i\theta X_1} e^{i\theta X_2} \cdots e^{i\theta X_n}] = \mathbb{E}[e^{i\theta X_1}]\mathbb{E}[e^{i\theta X_2}] \cdots \mathbb{E}[e^{i\theta X_n}] \\
&= \prod_{j=1}^{n} \left(1 - \frac{1}{j} + \frac{1}{j} e^{i\theta}\right) = \prod_{j=1}^{n} \left(1 + \frac{1}{j}(e^{i\theta} - 1)\right) \\
&= \prod_{j=1}^{n} \exp\left(\ln\left(1 + \frac{1}{j}(e^{i\theta} - 1)\right)\right) = \exp\left(\sum_{j=1}^{n} \ln\left(1 + \frac{1}{j}(e^{i\theta} - 1)\right)\right)
\end{aligned}$$

[5] Cette terminologie est imprécise, mais suffit à notre propos : en toute rigueur, il faudrait dire « converge en loi vers une variable aléatoire de densité f », mais ceci demanderait à étendre notre définition de « variable aléatoire ».

[6] qui est celle d'une variable aléatoire de densité f.

[7] Précisons qu'ici nos variables aléatoires ne suivent pas la même loi ; il s'agit d'une version plus générale que le théorème central limite usuel, cas particulier du théorème de Lindeberg-Feller (voir par exemple [1], section 3.4).

Posons $\epsilon(u) = \frac{\ln(1+u)-u}{u^2}$ pour $u \in \mathbb{C}^*$ tel que $|u| \leqslant 1/2$, avec ϵ prolongé par continuité en 0. Ainsi, $\ln(1+u) = u + u^2\epsilon(u)$. Alors :

$$\begin{aligned}\phi_{\mathrm{cyc}_n}(\theta) &= \exp\left(\sum_{j=1}^{n}\left(\frac{1}{j}(e^{i\theta}-1) + \left(\frac{1}{j}(e^{i\theta}-1)\right)^2 \epsilon\left(\frac{1}{j}(e^{i\theta}-1)\right)\right)\right) \\ &= \exp\left((\ln n + \mathcal{O}(1))(e^{i\theta}-1) + (e^{i\theta}-1)^2\mathcal{O}(1)\right),\end{aligned}$$

où $\mathcal{O}(1)$ indique une quantité bornée dépendant de n et θ. Ainsi :

$$\phi_{\mathrm{cyc}_n}(\theta) = \exp((\ln n)(e^{i\theta}-1) + \mathcal{O}(1)(e^{i\theta}-1) + (e^{i\theta}-1)^2\mathcal{O}(1)).$$

Soit $t \in \mathbb{R}$ fixé et calculons $\phi_{\frac{\mathrm{cyc}_n - \ln n}{\sqrt{\ln n}}}(t)$. Pour n suffisamment grand pour que $|e^{it/\sqrt{\ln n}} - 1| < 1/2$, on a :

$$\begin{aligned}\phi_{\frac{\mathrm{cyc}_n - \ln n}{\sqrt{\ln n}}}(t) &= \mathbb{E}\left[e^{it\frac{\mathrm{cyc}_n - \ln n}{\sqrt{\ln n}}}\right] = e^{-it\sqrt{\ln n}}\mathbb{E}\left[e^{i\frac{t}{\sqrt{\ln n}}\mathrm{cyc}_n}\right] = \exp(-it\sqrt{\ln n})\exp\left(\ln n\left(e^{it/\sqrt{\ln n}} - 1\right) + o(1)\right) \\ &= \exp(-it\sqrt{\ln n})\exp\left(\ln n\left(it\frac{1}{\sqrt{\ln n}} - \frac{t^2}{2\ln n} + \mathcal{O}\left(\frac{1}{(\ln n)^{3/2}}\right)\right) + o(1)\right) \\ &= \exp(-t^2/2 + o(1)),\end{aligned}$$

où $o(1)$ indique une quantité tendant vers 0 lorsque n tend vers l'infini. On conclut grâce au théorème de convergence de Lévy, car l'application $t \mapsto e^{\frac{-t^2}{2}}$ est la fonction caractéristique de la densité gaussienne, centrée, réduite (c'est-à-dire que $\int_{-\infty}^{+\infty} e^{itu}\frac{1}{\sqrt{2\pi}}e^{-u^2/2}du = e^{\frac{-t^2}{2}}$, voir par exemple [4, 5] pour une preuve). □

Conclusion

Ainsi, nous avons étudié les statistiques du nombre de cycles de différentes manières. Cependant, hormis le premier calcul de $P_n(q)$, le théorème 3, construisant une bijection $\mathcal{B}$ de $\mathfrak{S}_n$ dans $\mathfrak{S}_n$ envoyant une permutation avec k cycles sur une permutation à k records, a été fondamental pour tout notre propos. En effet, nous avons pu étudier les records, d'une part via la « permutation des perdants » (partie 1.3) et d'autre part via une interprétation probabiliste des records (théorème 14), puis nous avons transporté ces résultats sur les cycles via $\mathcal{B}$.

Références

[1] R. Durrett, *Probability : Theory and Examples*, 4th edition, Cambridge U. Press, 2010.

[2] P. Flajolet and R. Sedgewick, *Analytic combinatorics*, Cambridge University Press, Cambridge, 2009.

[3] I. Kortchemski, Asymptotic behavior of permutation records, *Journal of Combinatorial Theory Series A* **116(6)** : 1154-1166, 2009.

[4] J.-F. Le Gall, *Intégration, Probabilités et Processus Aléatoires*, disponible sur son site web, non publié, 2006.

[5] J.-Y. Ouvrard, *Probabilités : Tome II, Master - Agrégation*, Cassini, 2004.

[6] D. Perrin, *Cours d'algèbre*, Éditions de l'École Normale Supérieure de Jeunes Filles, 1981.

[7] A. Rényi, Théorie des éléments saillants d'une suite d'observations , *Ann. Fac. Sci. Univ. Clermont-Ferrand* No. **8** 1962 7-13.

[8] B. E. Sagan, *The Symmetric Group : Representations, Combinatorial Algorithms, and Symmetric Functions*, Graduate Texts in Mathematics 203 (Springer-Verlag, 2000).

[9] R. P. Stanley, *Enumerative Combinatorics, vol. 1*, Cambridge, England : Cambridge University Press, 1999.