Etude statistique des éléments de $\mathfrak{S}_n$

Christopher-Lloyd SIMON

TIPE 2014-2015

Résumé

Ce document présente mes Travaux d'Initiative Personnelle Encadrés concernant diverses propriétés statistiques et asymptotiques au sujet des ordres et des cycles des éléments des groupes symétriques.

Préambule : Bob dispose d'une image $n \times m$ comme par exemple celle en niveau de gris croissant figure 1 et d'une transformation bijective (c'est à dire d'une permutation de l'emplacement des pixels). Il sait qu'en appliquant sa transformation à l'image d'origine et en la réitérant suffisamment de fois, il retrouvera cette première car le nombre de configurations totales est au nombre de $(n \cdot m)!$ et la transformation est bijective. Les questions que Bob se pose sont les suivantes :

- Q1 Combien d'itérations peut-il espérer avoir à effectuer afin de retomber sur la configuration de départ ?
- Q2 Pourra-t-il reconnaitre tout ou partie de son image, au cours des transformatons successives, avant de la récupérer identique à l'état initial ?

Dans la suite, la première partie adresse Q1 et la deuxième introduit des notions abstraites utiles à l'étude de Q2 menée dans la troisième partie. La figure 1 illustre la configuration de départ en haut à gauche ainsi que trois autres grilles correspondant toutes à l'application d'une permutation à l'état initial avec indiqué pour chacune d'elles, le nombre minimal d'itérations idoine.

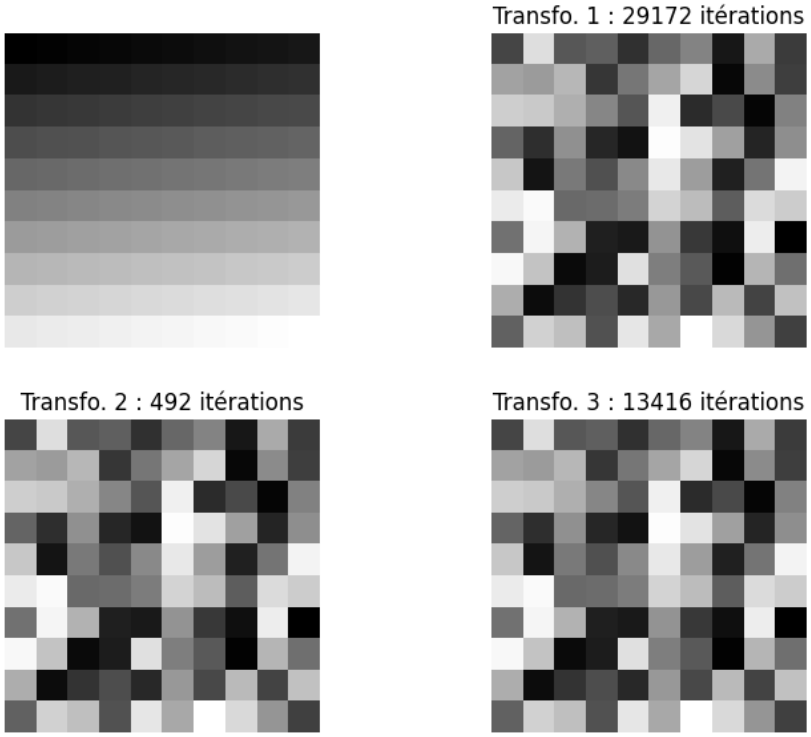


FIGURE 1 – Image initiale et sa transformation après trois permutations

Table des matières

Notations

On utilisera fréquemment l'abréviation dcsd pour décomposition en cycles à support disjoint, en se référant à une permutation.

Si $f(x) = \sum_{i \in \mathbb{N}} f_i \cdot x^i$ est une série formelle, alors on note $\langle x^n \rangle \{f(x)\} = f_n$, le coefficient de x^n dans $f(x)$.

$\mathfrak{S}_n$ **:** groupe symmétrique d'ordre n.

$|I|$ **:** cardinal de l'ensemble I.

$\mathbb{P}$ **:** ensemble des nombres premiers.

$ord(\sigma)$ l'ordre d'une permutation $\sigma \in \mathfrak{S}_n$.

$ppcm(a_i)_{i \in I}$ **:** le ppcm d'une suite finie d'entiers $(a_i)_{i \in I}$.

$\sum a$ **:** la somme des termes d'une suite presque nulle a.

$\mathcal{P}_a(n)$ **:** l'ensemble des partitions de n. On les associera aux suites d'entiers décroissantes a vérifiant $\sum a = n$.

$c(\sigma)$ **:** la suite $(a_1, a_2, ...)$ où a_i est le nombre de i-cycles dans la dcsd de σ. Par exemple, $c(\sigma) = (2, 3, 5)$ signifie que sa dcsd contient 2 points fixes, 3 2-cycles et 5 3-cycles (ainsi $\sigma \in \mathfrak{S}_{23}$). On l'appellera le vecteur caractéristique des cycles de σ.

$\widetilde{c}(\sigma)$ **:** la suite $(x_1, ..., x_1, x_2, ..., x_2, ...)$ des longueurs des cycles présents dans la dcsd de σ par ordre décroissant. Par exemple, $\widetilde{c}(\sigma) = (3, 3, 3, 3, 3, 2, 2, 2, 1, 1)$ signifie que sa dcsd contient 5 3-cycles, 3 2-cycles et 2 points fixes.

$\gamma_n((a_1, a_2, ...))$: le nombre de permutations $\sigma \in \mathfrak{S}_n$ telles que $c(\sigma) = (a_1, a_2, ...)$.

α_n **:** Ordre le plus représenté dans $\mathfrak{S}_n$, c'est à dire l'élément réalisant le maximum de w_n définie ci-dessous.

$\pi_n(k)$ **:** Probabilité que $\sigma \in \mathfrak{S}_n$ ait k cycles dans sa dcsd.

$\binom{\beta}{n} = \frac{\beta \cdot (\beta-1) \cdots (\beta-n+1)}{n!}$ pour tout entier naturel n et complexe β.

Pour $m \in \mathbb{N}^*$, on définit :

$\mathfrak{R}_n(m) = \{\sigma \in \mathfrak{S}_n,\ \sigma^m = Id\}$

$\mathfrak{W}_n(m) = \{\sigma \in \mathfrak{S}_n,\ ord(\sigma) = m\}$

$r_n(m) = |\mathfrak{R}_n(m)|$ (par convention $r_0(m) = 1$)

$w_n(m) = |\mathfrak{W}_n(m)|$ (par convention $w_0(m) = 1$)

$R_n(m) = \sum_{n \geq 0} r_n(m) \cdot \frac{x^n}{n!}$

$W_n(m) = \sum_{n \geq 0} w_n(m) \cdot \frac{x^n}{n!}$

$\theta_n = max\{ord(\sigma),\ \sigma \in \mathfrak{S}_n\}$

1 Distribution des ordres dans $\mathfrak{S}_n$

1.1 Nombre d'éléments d'ordre premier

1.1.1 Analyse combinatoire

Formule sommatoire : Calculons $w_n(p)$ lorsque $p \in \mathbb{P}$. Pour cela on remarque que si $\sigma \in \mathfrak{W}_n(p)$, alors sa dcsd ne comporte que des cycles de longueur p puisque son ordre est le ppcm de la longueur de ses cycles. On va donc partitionner $\mathfrak{W}_n(p)$ selon le nombre de cycles que comportent ses éléments. Un fois cet entier k choisi, il y a $\binom{n}{kp}$ supports possibles. Il ne reste qu'à agencer les éléments du support dans les k p-cycles. Comme les cycles commutent (ils sont à support disjoint), leur ordre n'a pas d'importance ; de plus, l'écriture d'un p-cycle est unique à permutation circulaire près de ses éléments. Ainsi, il faut diviser les $(kp)!$ configurations possibles par $p^k k!$ ce qui donne en regroupant tout :

$$w_n(p) = \sum_{k=1}^{\left\lfloor \frac{n}{p} \right\rfloor} \binom{n}{kp} \cdot \frac{(kp)!}{p^k k!}$$

Formule de récurrence : Avec un autre aperçu combinatoire, il n'est pas difficile de dériver une formule de récurrence portant sur l'indice n pour les suites $(w_n(p))_{n\in\mathbb{N}^*}$ pour tout $p \in \mathbb{P}$ fixé. Pour cela nous allons à nouveau partitionner $\mathfrak{W}_n(p)$. Considérons l'image de n par un élément σ de cet ensemble. Deux possibilités se présentent : soit il est laissé fixe, soit il appartient à un p-cycle dans la dscd de σ. Il y a $w_{n-1}(p)$ éléments correspondant au premier cas. Dans le second, il suffit de sélectionner $p-1$ entiers de $[1, n-1]$ pour compléter le cycle, d'ordonner les éléments dans le cycle selon l'un des $(p-1)!$ ordres possibles, puis d'y juxtaposer une permutation d'ordre p ou l'identité sur les $n-p$ éléments restants (le p-cycle déjà formé assure l'ordre de σ c'est pourquoi l'identité convient aussi). D'autre part, si $n < p$ on ne peut former de p-cycle donc $w_n(p) = 0$. On peut donc entièrement définir nos suites par récurrence à l'aide de l'équation valable pour $n \geq p$.

$$w_n(p) = w_{n-1}(p) + \frac{(n-1)!}{(n-p)!} \cdot (w_{n-p}(p) + 1)$$

1.1.2 Simulation informatique

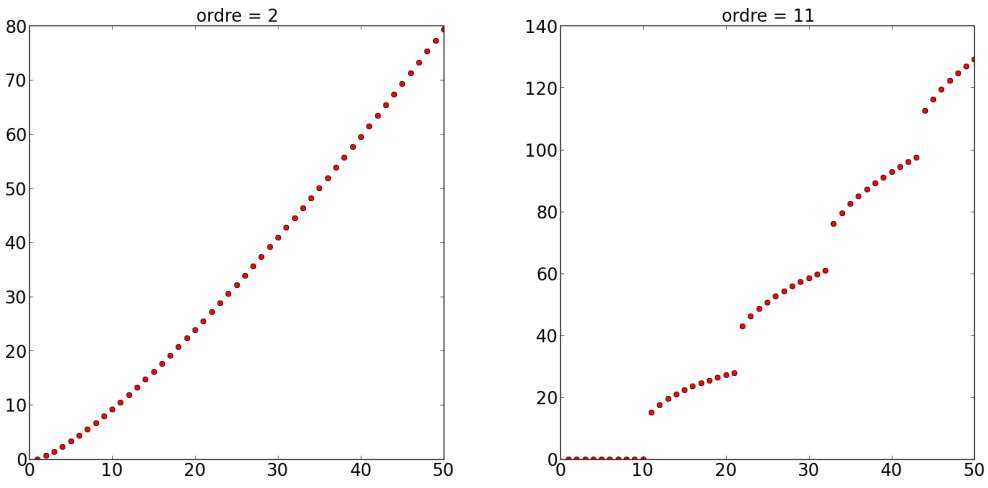


FIGURE 2 – Evolution de $\ln(w_n(p))$ en fonction de n pour deux valeurs (2 et 11) de l'ordre premier p

Les paliers successifs du graphe pour $p = 11$ corroborent que la relation de récurrence fait intervenir le terme précédent mais aussi celui dont l'indice a été retranché de p. Ils s'interprètent aussi dans la partie fractionnaire apparaissant dans les bornes de la formule sommatoire. Ce même type de graphe est représenté en annexe A.1.1 pour d'autres valeur de $p \in \mathbb{P}$.

1.1.3 Trouver un équivalent

Bob s'interroge : peut-on trouver un équivalent pour $w_n(p)$ lorsque $p \in \mathbb{P}$? Ce n'est pas une mince affaire à cause de la présence du terme n dans la borne supérieure ainsi que dans l'expression de la somme et il est difficile de l'isoler convenablement. Chowla, Herstein et Moore l'ont traité au fil de [4] dans le cas $p = 2$ et Moser et Wyman ont généralisé le résultat dans [6] pour les premiers supérieurs à 2. Avant de trouver ces références j'ai montré l'encadrement suivant dont la preuve est en B.1.

Proposition 1. *Pour tout $p \in \mathbb{P}$ il existe deux suites $mino_n(p)$ et $majo_n(p)$ telles que sur les n multiples de p :*

$$mino_n(p) \leq w_n(p) \leq majo_n(p)$$

$$mino_n(p) \sim \frac{1}{\sqrt{p}} \cdot \left(\frac{n}{e}\right)^{n\left(1-\frac{1}{p}\right)} \qquad majo_n(p) \sim \sqrt{\frac{2n\pi}{p}}^{p} \cdot \left(1 + \frac{1}{p^{p-1}}\right)^{\frac{n}{p}} \cdot \left(\frac{n}{e}\right)^{n\left(1-\frac{1}{p}\right)}$$

On peut constater l'écart entre le logarithme de ces équivalents et la suite $\ln(w_n(p))$ en annexe A.2 et les comparer à l'expression donnée par Moser et Wyman :

Proposition 2. *Pour p premier supérieur à 2, $w_n(p) \sim \frac{1}{\sqrt{p}} \cdot \exp\left(n^{1/p}\right) \cdot \left(\frac{n}{e}\right)^{n\left(1-\frac{1}{p}\right)}$*

1.2 Nombre d'éléments d'ordre quelconque

1.2.1 Analyse combinatoire et formule sommatoire

On cherche une formule (non nécessairement close mais calculable informatiquement) pour les quantités $w_n(m)$. Si le cas où $m \in \mathbb{P}$ est plus simple, c'est parce que les éléments de $\mathfrak{W}_n(m)$ sont des produits de m cycles à supports disjoints. Dans le cas général, il s'agit de trouver toutes les permutations $\sigma \in \mathfrak{S}_n$ telles que $ppcm(\widetilde{c}(\sigma)) = m$ et donc toutes les suites finies u telles que $\sum u = n$ et $ppcm(u) = m$:

$$w_n(m) = \sum_{\substack{\sigma \in \mathfrak{S}_n \\ ppcm(\widetilde{c}(\sigma))=m}} 1 \quad = \sum_{\substack{P \in \mathcal{P}_a(n) \\ ppcm(P)=m}} |\{\sigma \in \mathfrak{S}_n,\ \widetilde{c}(\sigma) = P\}| = \sum_{\substack{P \in \mathcal{P}_a(n) \\ ppcm(P)=m}} \gamma_n(P)$$

Cette dernière formule est très pratique lorsqu'il s'agit de calculer informatiquement $w_n(m)$ puisqu'il est facile, comme nous le verrons plus loin, de générer les partitions de n et d'en calculer le *ppcm*. Il suffit donc de calculer l'expression dans cette dernière somme. En nottant $P = (\underbrace{x_1, ..., x_1}_{l_1}, ..., \underbrace{x_j, ..., x_j}_{l_j})$, on obtient par un raisonnement identique à celui effectué en 1.1.1 la formule : $\gamma_n(P) = n! \cdot \left(\prod_{k=1}^{j} \left(x_k^{l_k} \cdot l_k!\right)\right)^{-1}$. En combinant les deux dernières égalités on obtient une formule générale certes complexe mais calculable informatiquement pour les quantités $w_n(m)$.

1.2.2 Simulation informatique

J'ai procédé en deux temps lors de la mise en oeuvre de mes modélisations informatiques. Je me suis tout d'abord servi de Caml afin de vérifier mes résultats et mes raisonnements sur le plan théorique puis j'ai réécrit toutes mes fonctions avec Python afin de pouvoir bénéficier à la fois de sa "puissance de calcul" (Caml compte modulo $2^{64} - 1$ tandis que Python n'a aucun mal pour calculer 170!) ainsi que des disponibilités graphiques pourvues par la bibliothèque matplotlib.

Algorithme et code Python : Voici l'un des algorithmes que j'ai écrit sous Python afin de générer toutes les partitions d'un entier n :

```
def partitions_gen_rec(n):
    if n == 0:
        yield []
        return
    for p in partitions_gen_rec(n-1):
        yield [1] + p
        if p and (len(p) <= 1 or p[1] > p[0]):
            yield [p[0] + 1] + p[1:]
```

Cet algorithme récursif repose sur la simple constatation que chaque partition de n s'obtient canoniquement d'une partition de $n+1$ en soustrayant un unité à la plus petite des parties. Par exemple $1+5+7$ donne $5+7$ et $3+5+5$ donne $2+5+5$. On remonte ici le processus. Pour chaque partition de $n-1$, on concatène la partie [1] à la liste des parties ou on ajoute 1 à la plus petite des parties. On remarquera que l'invariant suivant est conservé au cours des appels récursifs de la fonction : les partitions sont triées dans l'ordre lexicographique décroissant et dans toute partition, les parties sont triées par ordre croissant. Une fois l'itérateur des partitions d'un entier n généré, il suffit de le parcourir et de calculer pour chaque partition son ppcm i ainsi que le nombre de permutations de $\mathfrak{S}_n$ correspondantes j par la formule décrite plus haut. Dans un tableau créé en amont, incrémenter la case $i-1$ de cette quantité j.

Images Python : J'ai représenté figure 3 $w_n(m)$ en fonction de m pour deux valeurs fixées de n afin d'avoir une brève intuition de la convergence de la loi de distribution des ordres dans $\mathfrak{S}_n$.

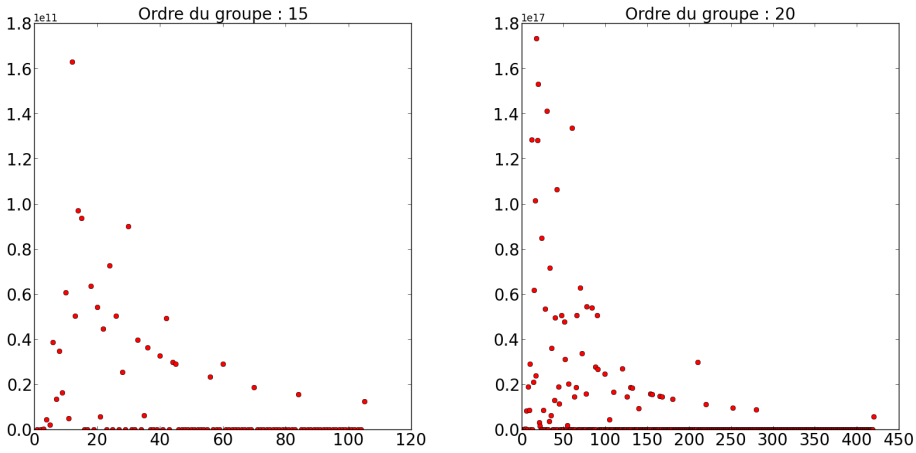


FIGURE 3 – Evolution de $w_n(m)$ en fonction de m pour deux valeurs de n (15 et 20)

Ces deux graphiques sont loin d'être suffisants pour se persuader de la convergence en question, c'est pourquoi j'en représenté d'un autre type en A.3 afin de s'en faire une idée plus précise.

1.3 Questions et éléments de réponse

Diverses interrogations émergent des graphes précédents. J'en évoquerai deux d'entre-elles précisant Q1 :

Q1.1 Y-a-t-il effectivement convergence lorsque n tend vers l'infini de la distribution probabiliste des ordres dans $\mathfrak{S}_n$, et le cas échéant quelle est la loi limite ?

Q1.2 Quel est, asymptotiquement, l'ordre maximal atteint dans $\mathfrak{S}_n$?

1.3.1 La distribution asymptotique des ordres dans $\mathfrak{S}_n$

Afin de reformuler Q1.1, on considère l'espace probabilisé $(\mathfrak{S}_n, \mathfrak{P}(\mathfrak{S}_n), \mathcal{P})$ où $\mathcal{P}$ suit la loi uniforme. Pour tout $n \in \mathbb{N}^*$ on définit la variable aléatoire :

$$X_n : \left\{ \begin{array}{ccc} \mathfrak{S}_n & \to & \mathbb{N}^* \\ \sigma & \mapsto & ord(\sigma) \end{array} \right.$$

La question posée revient à déterminer la loi de $\ln(X_n)$ (c'est la plus intéressante) lorsque $n \to +\infty$. Celle-ci n'est pas triviale et je me contenterai de citer les résultats que j'ai rencontré au fil de mes recherches bibliographiques (voir [5]) puis d'en vérifier informatiquement la cohérence.

Théorème 1 (ERDOS et TURAN)**.** $\ln X_n$ *suit asymptotiquement une distribution normale de moyenne* $\mu_n = \frac{1}{2} \cdot \ln(n)^2$ *et de variance* $\nu_n^2 = \frac{1}{3} \cdot \ln(n)^3$. *Plus précisément :*

$$\lim_{n \to +\infty} \mathcal{P}\left(\frac{\ln X_n - \mu_n}{\nu_n} \leq x \right) = \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^{x} e^{-\frac{y^2}{2}} dy$$

Ce théorème assure une stabilité dans la distribution des ordres dans $\mathfrak{S}_n$ pour de grandes valeurs de n qui est frappante à la vue du graphe en A.3. La figure 4 suivante permet de vérifier expérimentalement ces faits.

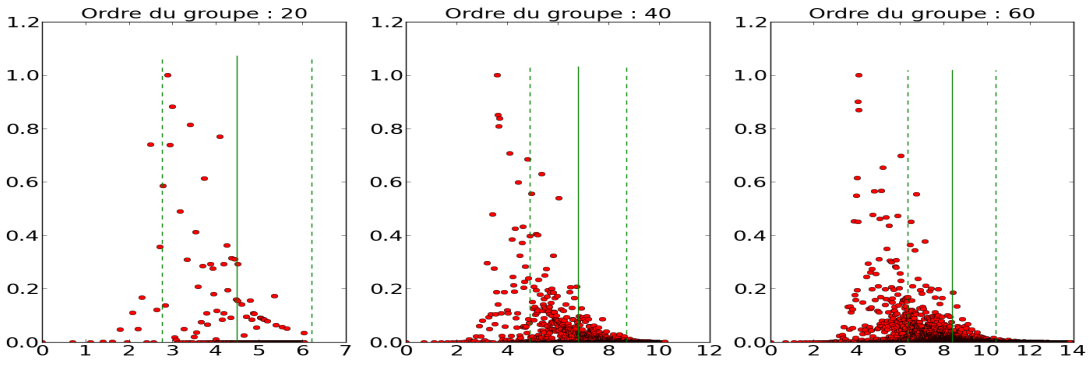


FIGURE 4 – Pour $n \in 20, 40, 60$: $\frac{w_n(m)}{w_n(\alpha_n)}$ en fonction de $\ln(m)$ pour $1 \leq m \leq \theta_n$ et $\mu_n \pm \nu_n$

On observe en effet que la densité de probabilité de $\ln X_n$ tend vers une gaussienne. Un détail à ne pas omettre : le fait que l'enveloppe semble ne pas converger vers une gaussienne n'est pas contradictoire avec le théorème car il faut prendre en compte le nombre de points à une abscisse donnée puisqu'une forte probabilité peut compenser de faibles valeurs. Bien que les valeurs données pour les équivalents de la moyenne et de l'écart-type semblent plutôt s'éloigner des valeurs réelles selon le graphe en A.4 ce n'est pas contradictoire avec la notion d'équivalent. Finalement, il faut prendre garde au fait que les ordres prennent pour une valeur de n donnée des valeurs positives bornées dans $\mathbb{N}$ ce qui rend le théorème de convergence d'autant plus remarquable.

1.3.2 L'ordre maximal dans Sn

Q1.2 concerne θ_n. Avec quelques considérations plutôt simples on peut se donner un encardrement assez large mais qui donne une idée approximative de θ_n. On cherche $\sigma \in \mathfrak{S}_n$ tel que *ppcm* $\widetilde{c}(\sigma)$ soit maximal et donc un j-uplet $x = (x_1, ..., x_j)$ correspondant aux longueurs des cycles de σ vérifiant $\sum_{1 \leq i \leq j} x_i = n$ et *ppcm* $(x_i) = \theta_n$.

Comme *ppcm* $(x_i) \leq \prod_{1 \leq i \leq j} x_i$ on a immédiatement avec l'IAG : $\theta_n \leq \max_{j \leq n}(n/j)^j$. C'est un exercice facile de vérifier que ce maximum (si l'on autorise j à prendre des valeurs non entières) est atteint en $\frac{n}{e}$ et on obtient la majoration pour tout entier n :

$$\theta_n \leq \exp\left(\frac{n}{e}\right)$$

.

En admettant un lemme conjecturé sous Python et proche de celui de Felgner (1990) relatif aux nombres premiers cité dans [1], j'ai trouvé une minoration θ_n pour certaines valeurs de n dont la démonstration figure en B.2 :

Proposition 3. *Considérons* $(p_i)_{i \in \mathbb{N}^*}$ *la suite ordonnée des nombres premiers et les entiers* $I_n = \sum_{i=1}^{n} p_i$.

Alors, $\forall \epsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geq N,\ \sqrt[2+\epsilon]{2I_n}^{\,\sqrt[2+\epsilon]{2I_n}} \leq \theta_{I_n}$

L'article [5] énnonce le théorème suivant dû à Landau donnant un résulatat plus précis : $\ln(\theta_n) \sim \sqrt{n \ln(n)}$.

Qu'en pense Bob ? Bob dispose donc désormais d'une réponse quasi-complète à sa question Q1 à condition que son image soit suffisament grande : une approximation de la distribution asymptotique des ordres ainsi que de l'ordre maximal dans $\mathfrak{S}_n$. A n grand fixé, les temps d'attente moyen et dans le pire des cas sont nettement meilleurs que ce qu'il aurait pu espérer naïvement. Par exemple, pour $n = 1000000$ (nombre de pixels moyen d'un appareil photo contemporain) : le logarithme de l'ordre de sa permutation vaut en moyenne 95 et il y a 68% de chances pour qu'il se trouve entre 92 et 99. De plus il vaut au maximum 3700. Ces valeurs sont à comparer avec le logarithme de l'ordre du groupe qui vaut environ 13000000 (majorant à priori déduit du théorème de Lagrange).

2 Les groupes symétriques : des familles exponentielles

J'applique dans cette partie la théorie générale du calcul dans les familles exponentielles présenté dans [3] au cas particulier du groupe symétrique afin d'obtenir quelques résultats importants concernant les séries génératrices qui sont d'une part indispensables pour calculer les équivalents évoqués plus haut et qui serviront d'autre part dans la suite de l'étude.

2.1 Introduction du matériel nécessaire

Pour tout $i \in \mathbb{N}$ on considère $\hat{D}_i$ l'ensemble de tous les i-cycles de $\mathfrak{S}_i$ (avec $\mathfrak{S}_0 = \emptyset$), $E = \bigcup_{i\in\mathbb{N}} \hat{D}_i$, $D_i \subset \hat{D}_i$, $d_i = |D_i|$ et $F = \bigcup_{i\in\mathbb{N}} D_i$. On appelle réindéxation de tout élément $(a_1 \dots a_j) \in F$ par l'ensemble $S = \{b_1, \dots, b_j\}$, le j-cycle formé par les éléments de S rangés dans le même ordre (sur les naturels) que les x_k. Par exemple, la réindéxation de (3 4 2 1 5) par {7 11 13 17 19} donne (13 17 11 7 19). On note $h(n,k)$ le nombre de permutations de $\mathfrak{S}_n$ que l'on peut obtenir en faisant le produit de k éléments de F après réindéxation. Enfin, on considère les séries formelles : $D_F(x) = \sum_{i\in\mathbb{N}} d_i \cdot \frac{x^i}{i!}$, $H_F(x,y) = \sum_{(n,k)\in\mathbb{N}^2} h(n,k) \cdot \frac{x^n}{n!} \cdot y^k$.

Dans [3] Wilf explique que l'on peut manipuler toute série formelle selon une algèbre appropriée sans se soucier de la convergence de la série entière associée, ensuite si le rayon de convergence n'est pas nul, en déduire des propriétés sur ses coéfficients grâce à l'analyse.

2.2 Formule de dénombrement

L'objectif est désormais d'exprimer $H_F(x,y)$ en fonction de $D_F(x)$. L'essentiel est de remarquer que si $F_1 \cup F_2 = F$ et sont disjoints, alors $H_F(x,y) = H_{F_1}(x,y) \cdot H_{F_2}(x,y)$. Le preuve de ce lemme de fusion est en B.3. Fort de ce lemme, on peut donc construire notre ensemble F petit à petit en multipliant les séries formelles entre elles afin d'obtenir le résultat visé. Considérons donc pour commencer un ensemble F_1 très simple, constitué d'un seul cycle de longueur r. Dans ce cas, $h_1(n,k) = \delta_{n,kr} \cdot \frac{(kr)!}{k!r!^k}$ d'où : $H_{F_1}(x,y) = \exp\left(y \cdot \frac{x^r}{r!}\right)$. Si maintenant on considère F_2 constitué de d_r r-cycles, on n'a d'après le lemme qu'à élever H_{F_1} à la puissance d_r pour obtenir $H_{F_2} = \exp\left(y \cdot d_r \cdot \frac{x^r}{r!}\right)$. Finalement, en réappliquant le lemme, on obtient pour tout ensemble F décrit comme précédemment :

Proposition 4. $H_F(x,y) = \exp\left(y \cdot D_F(x)\right)$

Par ailleurs, notant $h(n)$ le nombre de permutations de $\mathfrak{S}_n$ que l'on peut obtenir en faisant le produit d'un nombre quelconque d'éléments de F après réindéxation, on a :

$$H_F(x) = \sum_{n\in\mathbb{N}} h(n) \cdot \frac{x^n}{n!} = H_F(x,1) = \exp\left(D_F(x)\right)$$

2.3 Conséquences pour certaines séries formelles relatives à $\mathfrak{S}_n$

Calcul de la série des $(w_n(m)+1)_{n\in\mathbb{N}}$: Fixons un entier m et choisissons pour F l'ensemble des cycles dont la longueur est un diviseur de m. Alors $d_r = \mathbf{1}_{r|m} \cdot (r-1)!$ et $D_F(x) = \sum_{d|m} (d-1)! \cdot \frac{x^d}{d!}$. Il s'en suit que la série génératrice associée aux nombres de solutions $sol_n(m)$ de $\sigma^m = Id$ dans $\mathfrak{S}_n$ vaut : $H_F(x) = \exp\left(\sum_{d|m} \frac{x^d}{d}\right)$. Lorsque $m = p$ est premier, on en déduit que : $w_n(p) = \langle x^n \rangle \left\{\exp\left(x^p/p + x\right)\right\} - 1$. Des théorèmes sophistiqués relevant de l'analyse complexe (comme celui de Hayman exposé dans [3]) permettent ensuite de dériver les équivalents de $w_n(p)$ présentés plus haut.

Nombre de permutations ayant k cycles : Prenons cette fois-ci $F = E$. Alors $d_i = (i-1)!$ donc $D_F(x) = \ln \frac{1}{1-x}$ et $H_F(x,y) = \frac{1}{(1-x)^y}$. Ainsi, les nombres $h(n,k)$ de permutations de $\mathfrak{S}_n$ ayant k cycles vérifient :

$$\sum_{k\in\mathbb{N}} h(n,k) \cdot y^k = \left\langle \frac{x^n}{n!} \right\rangle \left\{ \frac{1}{(1-x)^y} \right\} = n! \cdot \langle x^n \rangle \left\{ \frac{1}{(1-x)^y} \right\} = n! \cdot \binom{n+y-1}{n}$$

La prbabilité qu'une permutation de $\mathfrak{S}_n$ ait k cycles est donc le coefficient de y^k dans le polynôme en y : $\binom{n+y-1}{n}$.

3 Quelle forme a la dcsd d'une permutation

Interprétation mathématique de Q2 : Bob voulait savoir s'il ne pourrait pas reconnaitre son image au cours des transformations successives en partie ou en tout. Cela revient à étudier la dcsd de la permutation dont il dispose. En effet, si sa transformation possède de grands cycles, un nombre important de pixels sera à un moment donné correctement agencé de sorte qu'il pourra espérer reconnaitre la trame de son image si les pixels sont délocalisés ou un partie de celle-ci sinon. On va donc s'intéresser à la composition probabiliste de la dcsd d'une permutation.

3.1 Probabilité d'avoir exactement k cycles

Si n est fixé (taille de l'image de Bob), la probabilité d'avoir exactement k cycles renseigne Bob sur le nombre de groupes de pixels (et donc sur leur taille) qui vont se réaranger périodiquement lors des transformations successives. Si k est petit, Bob peut être sûr de reconnaître son image initiale avant d'en avoir récupéré la totalité. En appliquant les relations coéfficients racines au polynôme $\binom{n+y-1}{n}$, on obtient la :

Proposition 5. *Probabilité que $\sigma \in \mathfrak{S}_n$ ait k cycles dans sa dcsd :* $\pi_n(k) = \frac{(-1)^{n-k}}{n!} \cdot \sum_{R \in \mathfrak{P}_{n-k}([0,n-1]\cap\mathbb{N})} \prod_{r\in R} (-r)$

Les quantités $(s(n,k) = n! \cdot \pi_n(k))_{(n,k)\in(\mathbb{N}^*)^2}$ sont bien renseignées dans [2] : ce sont les nombres de Stirling de première espèce.

3.2 Composition asymptotique des dcsd

J'ai reformulé en B.4 la démonstration du théorème suivant apparaisant dans [3] et qui constitue la pierre angulaire en ce qui concerne l'étude probabiliste des cycles d'une permutation.

Théorème 2. *Soit $S \subset \mathbb{N}$ tel que la famille $\left(\frac{1}{s}\right)_{s\in S}$ soit sommable, et $a = (a_1, a_1, \cdots)$. La probabilité que le vecteur caractéristique des cycles d'une permutation $\sigma \in \mathfrak{S}_n$ corresponde avec a sur l'ensemble des indices $s \in S$ admet une limite lorsque $n \to \infty$ qui vaut :*

$$\prod_{s\in S} \left(e^{-\frac{1}{s}} \cdot \frac{(1/s)^{a_s}}{a_s!} \right)$$

Autrement dit, définissant pour tout $(n,s) \in \mathbb{N} \times S$ la variable aléatoire $Y_n(s) : \mathfrak{S}_n \to \mathbb{N}$ qui compte le nombre de s-cycles des $\sigma \in \mathfrak{S}_n$, alors lorsque $n \to \infty$, les variables $Y_n(s)$ sont indépendantes et suivent respectivement une loi de Poisson de paramètre $\frac{1}{s}$.

3.3 Applications

Donnons quelques exemples pour concrétiser le théorème et en montrer la portée.

Evènement : Structure de la dcsd	Ensemble S	Probabilité limite
a points fixes	$\{1\}$	$\frac{1}{e\cdot a!}$
a r-cycles	$\{r\}$	$\frac{1}{e^{\frac{1}{r}}\cdot r^a \cdot a!}$
a_r r-cycles et a_s s-cycles	$\{r,s\}$	$\frac{1}{e^{\frac{1}{r}}\cdot r^{a_r}\cdot a_r!} \cdot \frac{1}{e^{\frac{1}{s}}\cdot s^{a_s}\cdot a_s!}$
Aucun des cycles n'a pour longueur un carré	$\left\{x^2, x \in \mathbb{N}^*\right\}, \quad (a_i = 0)_{i\in S}$	$e^{-\frac{\pi^2}{6}}$
Aucun cycle de longueur un nombre premier	$\mathbb{P}, \quad (a_i = 0)_{i\in\mathbb{P}}$	0
Autant de 1-cycles que de 2-cycles	$\{1,2\}, \quad a_1 = a_2$	$\sum_{j=0}^{\infty} e^{-\frac{3}{2}} \cdot \frac{1}{2^j \cdot j!^2}$

On remarque que le premier cas qui est le plus simple, fournit déjà une généralisation du fameux problème des dérangements. De plus, le paramètre des lois de Poisson étant en $\frac{1}{s}$, on retrouve avec la linéarité de l'éspérance l'équivalent $\ln n$ bien connu pour le nombre de cycles moyens d'une permutation.

Un réponse à Q2 Si on admet le critère arbitraire selon lequel Bob peut reconnaitre son image si au moins la moitié des pixels est correctement agencée et que l'on suppose que Bob s'est fixé un entier maximal d'itérations réalisables m sur son image de n pixels ($m \ll n$ afin de pouvoir utiliser le théorème de manière approchée), alors la probabilité que Bob reconnaisse son image vaut approximativement :

$$\sum_{\substack{S\subset[1,n]\\ ppcm_{s\in S}(s)\leq m}} \left(\sum_{s_1\cdot a_{s_1}+\cdots+s_{|S|}\cdot a_{s_{|S|}}\geq \frac{n}{2}} \left(\prod_{s\in S} e^{-\frac{1}{s}} \frac{(1/s)^{a_s}}{a_s!} \right) \right)$$

Cette expression peut se calculer informatiquement pour de petites valeurs de m, ce faisant on remarque que les probabilités obtenues ne sont pas négligeables.

Conclusion

Afin de répondre aux problématiques Q1 et Q2 relatives aux images j'ai exploré certaines propriétés asymptotiques concernant la répartition des ordres et la composition des cycles dans les groupes symétriques. Cette étude m'a permis de développer ma curiosité et de vivre ma propre expérience de recherche : il fallait choisir l'orientation dans les phases de questionnement, de résolution et documentation. J'ai commencé par travailler seul pour voir ce que je pouvais tirer de mes propres connaissances puis afin de progresser davantage, j'ai alterné des phases de recherche bibliographiques (qui m'ont mené à la lecture de [3]) avec des périodes de recherches personnelles.

Dans cette étude les séries formelles permettent de relier diverses branches des mathématiques telles que les probabilités, la combinatoire, l'analyse asymptotique et la théorie des groupes ; de plus les méthodes employées peuvent être généralisées de façon très puissante (indice des cycles d'un groupe quelconque) permettant de résoudre des problèmes combinatoires comme ceux de Polya.

Les deux problèmes sont riches en applications notamment en informatique : en plus de l'interprétation donnée avec les images de Bob, les résultats fournissent des renseignements sur un aspect probabiliste des permutations qui a suscité mon questionnement lors de mes modélisations informatiques et qui concerne la génération aléatoire fidèle de permutations.

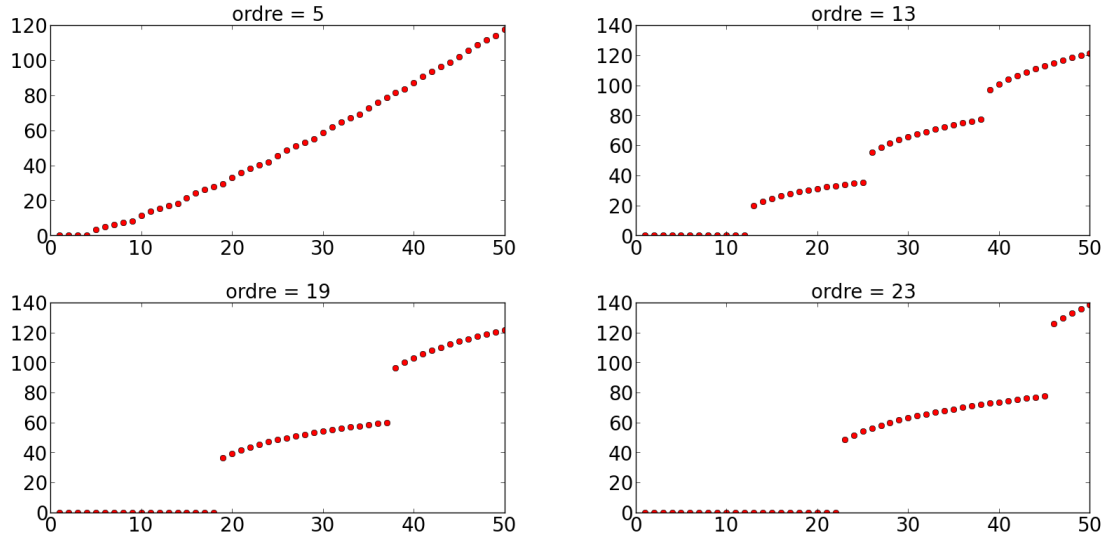
Enfin, j'ai relevé certaines curiosités dans l'annexe C que je n'ai pas approfondies et dont je n'ai trouvé aucune mention dans la littérature d'aujourd'hui.

A Représentations Graphiques

A.1 Variations de $\ln(w_n(m))$ en fonction de n

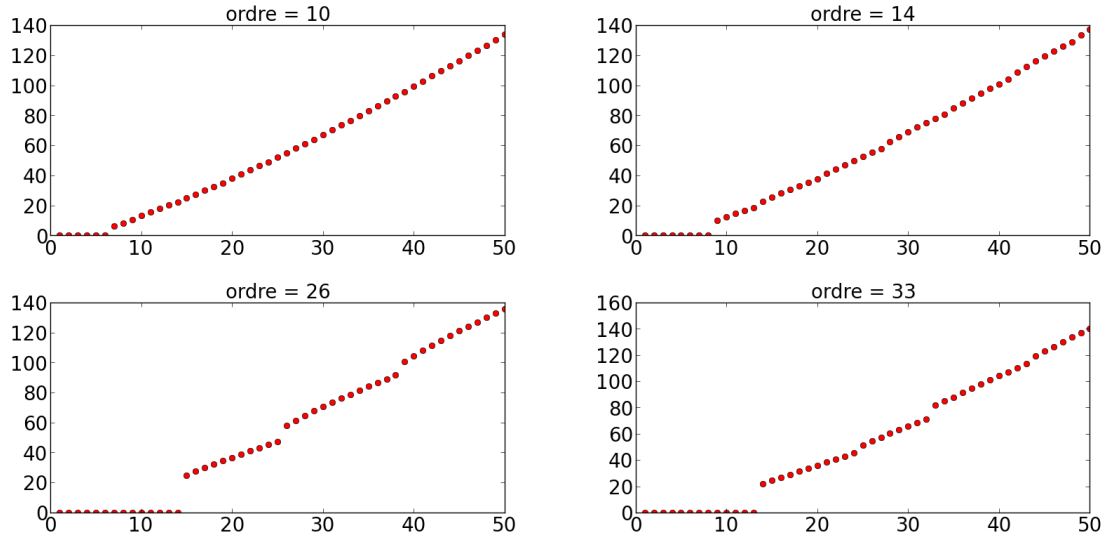
A.1.1 Lorsque l'ordre est premier

Evolution de $\ln(w_n(p))$ en fonction de n pour plusieurs valeurs $(5, 13, 19, 23)$ de l'ordre premier p



A.1.2 Pour des valeurs composées de l'ordre

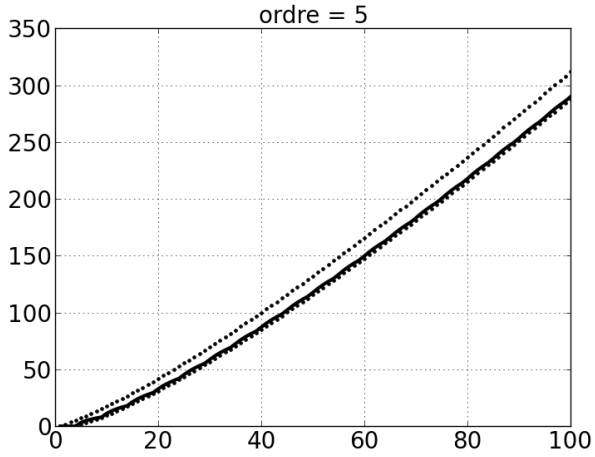
Evolution de $\ln(w_n(m))$ en fonction de n pour plusieurs valeurs $(10, 14, 26, 33)$ de l'ordre composé m



J'ai choisi pour l'ordre, des nombres composés comme multiples de deux nombres premiers $p < q$ distants l'un de l'autre afin de visualiser les "interférences" lors des accroissements de n : de p en p et de q en q.

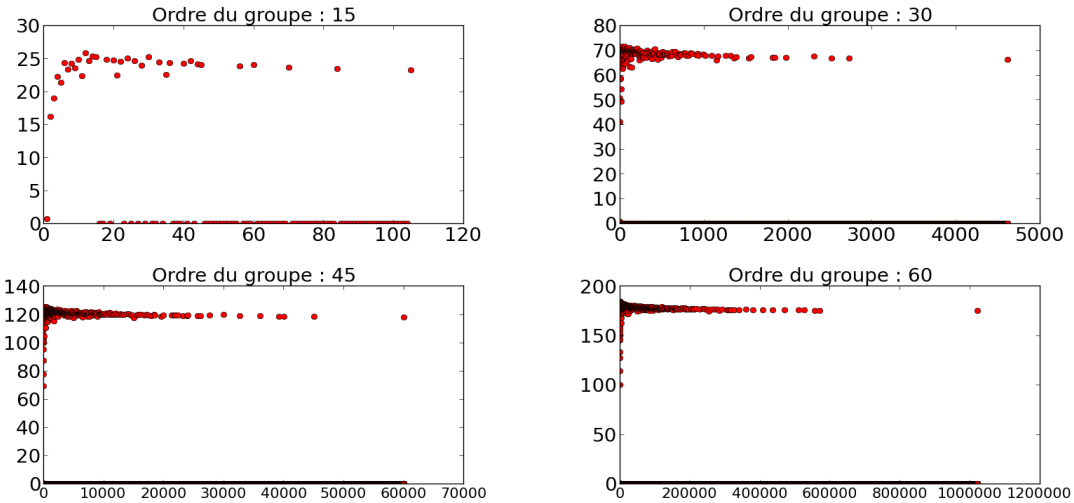
A.2 Précision de l'encadrement de $w_n(p)$

En fonction de n : $\ln(w_n(5))$ et les équivalents donnés pour $mino_n(5)$ et $majo_n(5)$ en pointillés



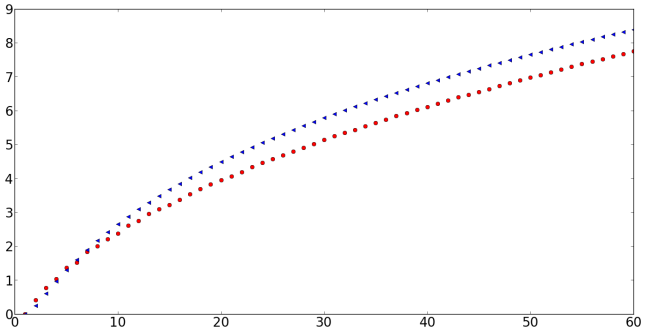
A.3 Distribution des ordres dans $\mathfrak{S}_n$

Tracé de la distribution $\ln(w_n(m))$ en fonction de m pour n prenant les valeurs 15, 30, 45 et 60



A.4 Ordres moyens dans $\mathfrak{S}_n$

Pour $1 \leq n \leq 60$, Rouge : espérance de $\ln X_n$ calculée informatiquement, Bleu : $\frac{1}{2} \cdot \ln(n)^2$



B Démonstrations

B.1 Encadrement de $w_n(p)$

On s'intéresse aux entiers n multiples de p premier et on démare de l'expression sommatoire de $w_n(p)$ en posant :

$$u_n(p,k) = \binom{n}{kp} \cdot \frac{(kp)!}{p^k k!}$$

Alors :

$$w_n(p) = u_n(p, \frac{n}{p}) \cdot \sum_{k=1}^{\frac{n}{p}} \binom{\frac{n}{p}}{k} \cdot p^{\frac{n}{p}-k} \cdot \frac{(\frac{n}{p}-k)!}{(n-kp)!}$$

Or la formule de Stirling permet de dire que :

$$u_n(p, \frac{n}{p}) \sim \frac{1}{\sqrt{p}} \cdot \left(\frac{n}{e}\right)^{n\left(1-\frac{1}{p}\right)}$$

Il faut désormais encadrer le facteur $\frac{(\frac{n}{p}-k)!}{(n-kp)!}$ pour k entre les bornes idoines. Il est toujours positif et vaut 1 lorsque $k = \frac{n}{p}$ ce qui permet d'obtenir la mioration.

D'autre part, on montre aisément par récurrence déscendante sur k allant de $\frac{n}{p}$ à 1 que :

$$\frac{(\frac{n}{p}-k)!}{(n-kp)!} \leq \frac{1}{\sqrt{p}} \cdot \left(\frac{\sqrt{2\frac{n}{p}\pi}}{p^{\frac{n}{p}-k}}\right)^p$$

Cette formule n'est pas aussi biscornue qu'elle en à l'air, elle s'intuite immédiatement en majorant l'équivalent trouvé grâce à la formule de Stirling. On obient donc en remplaçant et en remarquant un binôme de Newton dont on aurait tronqué le premier terme :

$$w_n(p) \leq u_n(p, \frac{n}{p}) \cdot \frac{\sqrt{2\frac{n}{p}\pi}}{\sqrt{p}} \cdot \left[\left(1 + \frac{1}{p^{p-1}}\right)^{\frac{n}{p}} - p^{\frac{n(p-1)}{p}}\right]$$

Finalement, on a l'encadrement voulu en éliminant simplement le deuxième terme du dernier facteur.

B.2 Minoration de θ_n

Soit $(p_j)_{j\in\mathbb{N}^*}$ la suite ordonnée des nombres premiers et posons $\forall n \in \mathbb{N}^*$, $I_n = \sum_{i=1}^{n} p_j$. Admettons le :

Lemme. $\forall j \in \mathbb{N}^*$, $j\ln(j) \leq p_j \leq j(\ln(j)+2)$

En faisant le produit de p_j-cycles à supports disjoints pour $1 \leq j \leq m$, on obtient une permutation dans $\mathfrak{S}_{I_m}$ dont l'ordre vaut $P_m = \prod_{j\leq m} p_j$ et donc une minoration de θ_{I_m}.

Or, d'après le Lemme, $\forall m \in \mathbb{N}^*$,

$$I_m \leq \sum_{j=1}^{m} j(\ln(j)+2) \leq \int_1^{m+1} t(\ln(t)+2)dt = \left[\frac{t^2}{2}\ln(t)\right]_1^{m+1} + \int_1^{m+1} \frac{3t}{2}dt \leq \frac{(m+1)^2}{2} \cdot (\ln(m+1) + \frac{3}{2})$$

Soit $\epsilon > 0$. On a donc par comparaison logarithme-puissance : $\exists N \in \mathbb{N}$, $\forall m \geq N$, $I_m \leq \frac{m^{2+\epsilon}}{2}$.

Considérons un tel entier N et $m \geq N$. Alors, en notant $Q_{I_m} = \prod_{j=1}^{\lfloor \sqrt[2+\epsilon]{2I_m} \rfloor} p_j$, on a $Q_{I_m} \leq P_m \leq \theta_{I_m}$.

Minorons désormais $\ln(Q_{I_m})$:

$$\ln(Q_{I_m}) \geq \ln(4\ln(2)) + \int_2^{\lfloor \sqrt[2+\epsilon]{2I_m} \rfloor} \ln(t\ln(t))dt \geq \ln(4\ln(2)) + [t\ln(t)-t]_2^{\lfloor \sqrt[2+\epsilon]{2I_m} \rfloor} + \int_2^{\lfloor \sqrt[2+\epsilon]{2I_m} \rfloor} \ln(\ln(t))dt \geq \sqrt[2+\epsilon]{2I_m} \cdot \ln(\sqrt[2+\epsilon]{2I_m})$$

On obtient ainsi la minoration souhaitée de θ_{I_m} pour $m \geq N$.

B.3 Lemme de fusion

Sachant la réunion disjointe : $F_1 \cup F_2 = F$, on veut montrer que $H_F(x,y) = H_{F_1}(x,y) \cdot H_{F_2}(x,y)$.

Il suffit pour cela d'identifier le coefficients de $x^n y^k$ de chacun des membres pour tous les entiers n et k et donc d'après le produit de Cauchy de montrer que :

$$h(n,k) = \sum_{\substack{n_1 \leq n \\ k_1 \leq k}} \binom{n}{n_1} \cdot h_1(n_1,k_1) \cdot h_2(n-n_1, k-k_1)$$

Or une permutation produit de k éléments de F après réindéxation sur les entiers dans $[1,n]$ est uniquement déterminée par le choix de deux entiers n_1 et k_1,puis d'un ensemble de n_1 indices parmis $[1,n]$, d'une permutation produit de k_1 éléments de F_1 après réindéxation sur l'ensemble choisi et d'une permutation produit de $k-k_1$ éléments de F_2 après réindéxation sur les indices restants. C'est exactement l'interprétation combinatoire (qui a une traduction ensembliste tout à fait rigoureuse) de la somme précédente.

B.4 Distribution de poisson

Cette preuve exalte l'efficacité des séries formelles dans la quête de renseignements concernant une suite d'origine combinatoire, cependant de manière générale, leur fécondité est d'autant plus surprenante lorsqu'elles sont couplées en aval aux outils d'analyse. On considère l'indice du groupe $\mathfrak{S}_n$ c'est à dire le polynôme en $x = (x_1, x_2, ...)$:

$$\phi_n(x) = \sum_{\substack{a_1+2a_2+\cdots=n \\ a_i \geq 0}} \gamma_n(a) \cdot x_1^{a_1} x_2^{a_2} \cdots$$

Si on définit la série génératrice : $\Psi(x,t) = \sum_{n=0}^{\infty} \phi_n(x) \cdot \frac{t^n}{n!}$, on s'apperçoit que la probabilité que $\sigma \in \mathfrak{S}_n$ ait une dcsd de la forme $a = (a_1, a_2, ...)$ vaut exactement : $Prob(a,n) = \langle x^a \cdot t^n \rangle \{\Psi(x,t)\}$. Or on a montré que $\gamma_n(a) = \frac{n!}{\prod_{k\geq 1}(k^{a_k} \cdot a_k!)}$ donc en remaniant la somme on a :

$$\begin{aligned} \Psi(x,t) &= \sum_{n\geq 0} \frac{t^n}{n!} \left(\sum_{a_1+2a_2+\cdots=n} \frac{n!}{\prod_{k\geq 1}(k^{a_k}\cdot a_k!)} \cdot x_1^{a_1} x_2^{a_2} \cdots \right) = \left(\sum_{a_1 \geq 0} \frac{(tx_1)^{a_1}}{1^{a_1}\cdot a_1!} \right) \cdot \left(\sum_{a_2 \geq 0} \frac{(tx_2)^{a_2}}{2^{a_2}\cdot a_2!} \right) \cdots \\ &= e^{tx_1} \cdot e^{t^2 x_2/2} \cdot e^{t^3 x_3/3} \cdots = \exp\left(\sum_{j\geq 1} \frac{x_j t^j}{j} \right) \end{aligned}$$

On considère désormais $S \subset \mathbb{N}^*$ l'ensemble des longueurs des cycles qui nous intéresse tel que $\left(\frac{1}{s}\right)_{s\in S}$ soit sommable, et on fixe $(x_i = 1)_{i \notin S}$ car on ne s'occupe pas des i-cycles correspondants. Alors :

$$\Psi(x,t) = \exp\left(\sum_{s\in S} x_s \cdot \frac{t^s}{s} + \sum_{i\notin S} \frac{t^i}{i} \right) = \exp\left(\sum_{s\in S} (x_s - 1) \cdot \frac{t^s}{s} + \ln\frac{1}{1-t} \right) = \frac{1}{1-t} \cdot \exp\left(\sum_{s\in S} (x_s-1) \cdot \frac{t^s}{s} \right)$$

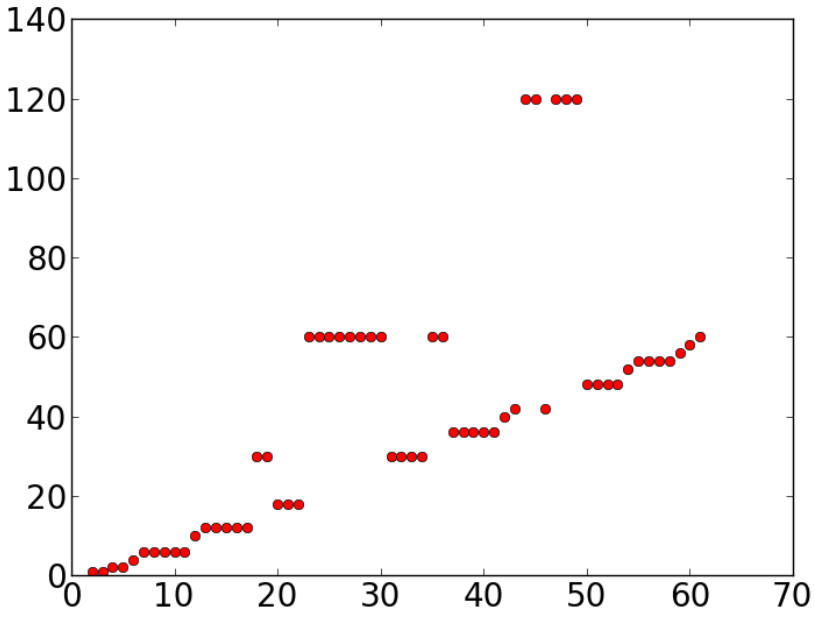
Ainsi, en reconnaissant un produit de Cauchy, on en identifie les coefficients :

$$\lim_{n\to+\infty} Prob(a,n) = \langle x^a \rangle \left\{ \exp\left(\sum_{s\in S} \frac{(x_s-1)}{s} \right) \right\} = \left(\prod_{s\in S} e^{-\frac{1}{s}} \right) \langle x_1^{a_1} x_1^{a_1} \cdots \rangle \left\{ \prod_{s\in S} e^{\frac{x_s}{s}} \right\} = \prod_{s\in S} e^{-\frac{1}{s}} \cdot \frac{(1/s)^{a_s}}{a_s!}$$

C Curiosités

C.1 Ordre le plus représenté dans Sn

Une notion qui a retenu mon attention mais que je n'ai pas investiguée suffisamment pour pouvoir présenter des résultats pertinents est le graphe des ordres les plus représentés dans $\mathfrak{S}_n$ lorsque n parcours $\mathbb{N}$. Le voici pour $n \leq 70$. Il semble intéressant de constater que la pluspart des points se situe proche de la droite $y = x$ et que parmis les valeurs atteintes on observe beaucoup de nombres ploutons. Voici les valeurs prises de 1 à 70 : 1, 1, 2, 2, 4, 6, 6, 6, 6, 10, 12, 12, 12, 12, 12, 30, 30, 18, 18, 18, 60, 60, 60, 60, 60, 60, 60, 60, 30, 30, 30, 30, 60, 60, 36, 36, 36, 36, 36, 40, 42, 120, 120, 42, 120, 120, 120, 48, 48, 48, 48, 52, 54, 54, 54, 54, 56, 58, 60, 60, 60, 60, 60, 60, 60, 60, 66, 66, 68.



C.2 Une analogie avec les racines de l'unité et la fonction ζ intervient

En se rappelant les notions introduites au début du document, on a :

$$\forall n \in \mathbb{N},\ \forall n \in \mathbb{N},\quad \coprod_{d|m} \mathfrak{W}_n(m) = \mathfrak{R}_n(m)$$

D'où : $\sum_{d|m} W_d(x) = R_m(x)$ et l'inversion de Mobiüs donne : $W_m(x) = \sum_{d|m} \mu(\frac{m}{d}) \cdot R_d(x)$.

En prenant le coefficient de $\frac{x^n}{n!}$, on obtient : $\forall n \in \mathbb{N}^*,\ w_n(m) = \sum_{d|m} \mu(\frac{m}{d}) \cdot r_n(d)$.

Ceci peut être utile car les quantités $r_n(d)$ sont plus faciles à calculer que $w_n(d)$ puisque sans tout redétailler ici, la théorie des séries génératrices exposée dans [3] permet de montrer que $R_m(x) = \exp\left(\sum_{d|m} \frac{x^d}{d}\right)$.

Il est au passage impressionnant de remarquer que si l'on définit les séries de Dirichlet suivantes :

$$\begin{cases} \omega(x,s) &= \sum_{m\geq 1} \frac{W_m(x)}{m^s} \\ \rho(x,s) &= \sum_{m\geq 1} \frac{R_m(x)}{m^s} \end{cases}$$

la relation précédente se traduit par : $\rho(x,s) = \zeta(s) \cdot \omega(x,s)$.

C.3 Nombre de sous groupes d'ordre $p \in \mathbb{P}$ dans $\mathfrak{S}_n$

C.3.1 Formule générale

Si p est premier, un sous-groupe de $\mathfrak{S}_n$ d'ordre p est cyclique (découle immédiatement du théorème de Lagrange). Il est donc engendré par une permutation σ d'ordre p qui est alors un produit de p-cycle. Les p-cycles sont à support disjoints et lorsque l'on considère les puissances de σ, elles sont toutes de la même forme tant que l'exposant est plus petit que p. Ce groupe contient donc $p-1$ telles permutations d'ordre p ainsi que l'identité. On obtient donc immédiatement de 1.1.1 le résultat qui suit.

$$w_n(p) = \sum_{k=1}^{\lfloor \frac{n}{p} \rfloor} \binom{n}{kp} \cdot \frac{(kp)!}{(p-1)p^k k!}$$

C.3.2 Le cas où $n = p$

En considérant les sous-groupes d'ordre $p \in \mathbb{P}$ dans $\mathfrak{S}_p$ on en déduit immédiatement de l'expression précédente le petit résultat qui suit.

Proposition 6. *Si $p \in \mathbb{P}$, le nombre de sous-groupes d'ordre p dans $\mathfrak{S}_p$ est $(n-2)!$.*

Références

[1] Jean-Paul Delahaye : *Merveilleux nombres premiers*, Belin, (2000).

[2] R. Graham, D. Knuth, O. Patashnik : *Concrete Mathematics*, Addison-Wesley, (1994).

[3] Herbert S. Wilf : *generatingfunctionology*, Academic Press, (1992).

[4] S. Chowla, I. N. Herstein et W. K. Moore : *On recursions connected with symmetric groups I*, Combinatorial Journal of Mathematics, **03**, (1951) 328-334

[5] P. Erdos et P. Turan : *On some problems of a statistical group-theory*, Acta Mathematica Academiae Scientiarum Hungaricae, **18**, (1967), 309-320.

[6] L. Moser et M. Wyman : *On solutions of $x^d = 1$ in symmetric groups*, Combinatorial Journal of Mathematics, **07**, (1955) 159-168