Acta Math. Hung.
45(1—2) (1985), 69—84.

DISTRIBUTION STATISTIQUE DE L'ORDRE D'UN ELEMENT DU GROUPE SYMETRIQUE

J. L. NICOLAS (Limoges)

I. Introduction

Soit S_n le groupe des permutations de n objets. P. Erdős et P. Turán ont démontré: (cf. [5])

$$\lim_{n\to\infty} \text{Prob}\left\{\frac{\log(\text{ordre de } \sigma)-(1/2)\log^2 n}{(1/\sqrt{3})\log^{3/2} n} < x\right\} = \Phi(x) \tag{1}$$

avec

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2}\, dt$$

en mettant sur S_n la mesure d'équiprobabilité. P. Erdős et P. Turán annoncent qu'il est possible d'obtenir un terme d'erreur dans la formule (1).

Pour chaque permutation $\sigma \in S_n$, nous désignerons par

$$n_1 < n_2 < \ldots < n_k$$

les différentes longueurs de cycles de σ, et par $m_1, \ldots, m_k$ leur multiplicité, de telle sorte que

$$\sum_{1\leqq i\leqq k} m_i n_i = n.$$

La démonstration de (1) est basée d'abord sur le résultat (cf. [4]): excepté $o(n!)$ permutations, tous les éléments $\sigma \in S_n$ vérifient:

$$\exp\left(-3\log n\,(\log\log n)^4\right) \leqq \frac{\text{ordre de } \sigma}{n_1 n_2 \ldots n_k} \leqq 1 \tag{2}$$

et ensuite sur la distribution des valeurs de la fonction

$$f(\sigma) = \sum_{1\leqq i\leqq k} \log n_i$$

à l'aide de sa fonction caractéristique.

Par la suite, M. R. Best [1] et J. D. Bovey [2] ont redémontré la loi limite vérifiée par f, par des méthodes plus élémentaires.

Nous allons démontrer le théorème suivant, qui améliore (2):

THÉORÈME 1. *Si l'on enlève de S_n un ensemble de $O\left(n!/\sqrt{\log n}\right)$ permutations, celles qui restent vérifient:*

$$\log(\text{ordre de } \sigma) = f(\sigma) - \log n \log\log n + O(\log n \log\log\log n).$$

La démonstration du théorème 1 repose sur l'idée suivante, fournie par P. Erdős: dans une permutation aléatoire, la moitié des cycles est de longueur paire, un tiers des cycles est de longueur multiple de 3, etc... et le nombre de cycles étant environ $\log n$, la contribution des nombres premiers $p \leqq \log n$ dans la différence $f(\sigma) - \log(\text{ordre de } \sigma)$ est approximativement:

$$\sum_{p \leqq \log n} \log p \frac{\log n}{p} = \log n (\log\log n + O(1)).$$

La contribution des nombres premiers $p > \log n$ est négligeable. La proposition 1 permet d'évaluer très précisement le nombre de $\sigma \in S_n$ qui ont exactement j cycles de longueur multiple de α, et je remercie M. Szalay, qui m'a signalé la référence [11]. La proposition 2, qui m'a été suggérée par A. Odlyzko, majore le nombre de $\sigma \in S_n$ pour lesquelles $n_1 n_2 \ldots n_k$ est divisible par une puissance assez grande d'un produit de nombres premiers.

Nous montrerons ensuite:

THÉORÈME 2. *On a uniformément en* $x \in \mathbf{R}$:

$$\text{Prob}\left\{\frac{f(\sigma) - (1/2)\log^2 n}{(1/\sqrt{3})\log^{3/2} n} < x\right\} = \Phi(x) + O\left(1/\sqrt{\log n}\right).$$

La démonstration du théorème 2 reprend les calculs originaux de P. Erdős et P. Turán. En fait un calcul similaire a été fait dans [10], pour étudier une fonction voisine de f, définie sur l'ensemble $\mathbf{F}_q^{(n)}[X]$ des polynômes unitaires de degré n sur un corps fini.

On déduit immédiatement des théorèmes 1 et 2:

THÉORÈME 3. *On a uniformément en* $x \in \mathbf{R}$:

$$\text{Prob}\left\{\frac{\log(\text{ordre de } \sigma) - (1/2)\log^2 n + \log n \log\log n}{(1/\sqrt{3})\log^{3/2} n} < x\right\} = \Phi(x) + O\left(\frac{\log\log\log n}{\sqrt{\log n}}\right).$$

Nous conjecturons que l'on peut supprimer le $\log\log\log n$ dans le reste du théorème 1, et du théorème 3.

NOTATIONS. Nous écrirons, pour simplifier

$$l = \log n; \quad l_2 = \log\log n; \quad l_3 = \log\log\log n.$$

Pour $1 \leqq v \leqq n$, et pour $\sigma \in S_n$ fixé, nous poserons: $N(v) = \sum_{\substack{i=1 \\ v \mid n_i}}^{k} 1$, le nombre de longueurs distinctes de cycles de σ multiples de v. La lettre p, indicée ou non désignera toujours un nombre premier. Enfin nous noterons $[x]$ la partie entière de x.

II. Démonstration du théorème 1

Enonçons d'abord quelques lemmes:

LEMME 1. *Soit* $x>0$. *On a:*
pour $u\geqq x$:

$$\sum_{m\geqq u}\frac{x^m}{m!}\leqq\left(\frac{ex}{u}\right)^u$$

et pour $0<v\leqq x$:

$$\sum_{0\leqq m\leqq v}\frac{x^m}{m!}\leqq\left(\frac{ex}{v}\right)^v.$$

DÉMONSTRATION. Elle est facile (cf. [8], p. 149).

LEMME 2. *Soit* $1\leqq v_1<v_2<\ldots<v_r$ *avec* $\sum_{i=1}^{r}v_i\leqq n$. *Le nombre de permutations de* S_n *ayant au moins un cycle de longueur* v_1, *un cycle de longueur* $v_2, \ldots,$ *un cycle de longueur* v_r *est* $\leqq n!/(v_1v_2\ldots v_r)$.

DÉMONSTRATION. Il y a

$$\frac{n!}{v_1!v_2!\ldots v_r!(n-v_1-v_2-\ldots-v_r)!}$$

façons de choisir r parties de $\{1, 2, \ldots, n\}$ de cardinal $v_1, \ldots, v_r$. Dans chacune de ces parties on doit avoir une permutation circulaire ce qui donne $(v_1-1)!\ldots(v_r-1)!$ choix possibles. Dans ce qui reste, n'importe quelle permutation marche, il y en a $(n-v_1-\ldots-v_r)!$. Cette démonstration est voisine de celle de la formule de Cauchy (cf [3], t.2, p. 75).

LEMME 3. *Soit* λ *réel vérifiant* $0<\lambda<1$. *On a:*

$$\sum_{p\leqq x}\frac{\log p}{p^\lambda}=O\left(\frac{x^{1-\lambda}}{1-\lambda}\right);\quad\sum_{p^m\leqq x}\frac{\log p}{p^{\lambda m}}=O\left(\frac{x^{1-\lambda}}{1-\lambda}\right);$$

$$\sum_{p\leqq x}\frac{\log p}{p}=\log x+O(1);\quad\sum_{p^m\leqq x}\frac{\log p}{p^m}=\log x+O(1).$$

Si $x\geqq 2$ *et si* $\lambda\geqq 2$, *on a:*

$$\sum_{p\geqq x}\frac{1}{p^\lambda}\leqq\frac{3}{(\log x)x^{\lambda-1}}.$$

DÉMONSTRATION. Soit $\theta(x)=\sum_{p\leqq x}\log p$ la fonction de Čebyšev. On a, par l'intégrale de Stieltjes

$$\sum_{p\leqq x}\frac{\log p}{p^\lambda}=\int_{2^-}^{x}\frac{d[\theta(t)]}{t^\lambda}=\frac{\theta(x)}{x^\lambda}+\int_2^x\frac{\lambda\theta(t)}{t^{\lambda+1}}dt$$

et comme $\theta(t)=O(t)$, cette quantité est:

$$O\left(x^{1-\lambda}+\int_0^x \lambda t^{-\lambda}dt\right)=O(x^{1-\lambda}/(1-\lambda)).$$

Pour évaluer $\sum_{p^m\leqq x}(\log p)p^{-\lambda m}$, on procède de même en remplaçant $\theta(x)$ par $\psi(x)=\sum_{p^m\leqq x}\log p$, la seconde fonction de Čebyšev. L'estimation de $\sum_{p\leqq x}(\log p)/p$ est classique (cf. [9], ch. 22).

De même, soit $\pi(x)=\sum_{p\leqq x}1$; on a:

$$\sum_{p\leqq x}p^{-\lambda}=\int_{x^-}^{+\infty}\frac{d[\pi(t)]}{t^\lambda}\leqq-\frac{\pi(x)-1}{x^\lambda}+\int_x^{+\infty}\frac{\lambda\pi(t)}{t^{\lambda+1}}dt.$$

Or on sait que $\pi(t)\leqq(3/2)(t/\log t)$ pour tout t, donc

$$\sum_{p\leqq x}p^{-\lambda}\leqq\frac{3/2}{\log x}\int_x^\infty\lambda t^{-\lambda}dt\leqq\frac{3}{(\log x)x^{\lambda-1}}.$$

LEMME 4. *Soit* $20\leqq\omega_1,\omega_2\leqq n$. *Si l'on enlève de* S_n *un nombre de permutations* $\leqq 3n!\left(\frac{1}{\omega_1}+\frac{1}{\omega_2!}\right)$, *les permulations restantes ont la propriété suivante: les cycles de longueur* $>\omega_1$ *sont uniques et les cycles de longueur* $\leqq\omega_1$, *ont une multiplicité* $\leqq\omega_2$.

DÉMONSTRATION. Ce lemme est le lemme III de [4].

PROPOSITION 1. *Soit:*

$$c_j=(1/n!)\,\mathrm{Card}\left\{\sigma\in S_n;\ \sum_{\substack{1\leqq i\leqq k\\ \alpha\mid n_i}}m_i=j\right\}$$

la probabilité qu'une permutation de S_n *ait exactement* j *cycles dont les longueurs sont multiples de* α. *Alors, si l'on pose* $r=[n/\alpha]$, *on a:*

$$c_j=\sum_{k=j}^{r}\frac{1}{r!}\frac{|s(r,k)|}{\alpha^k}\binom{k}{j}(\alpha-1)^{k-j}$$

où $s(r,k)$ *désigne le nombre de Stirling de* 1ère *espèce, et on a la majoration, pour* $r\geqq 2$

$$c_j\leqq e^\gamma r^{-1/\alpha}\frac{H^{j-1}}{j!\alpha^j}(j+H)$$

où γ *désigne la constante d'Euler, et* $H=1+\frac{1}{2}+\ldots+\frac{1}{r-1}$.

DÉMONSTRATION. D'après la formule 0.27, p. 183 de [11], on a:

$$\sum_{j=0}^{r}c_jx^j=\binom{(x-1)/\alpha+r}{r}$$

et d'après la définition des nombres de Stirling de première espèce, le deuxième membre ci-dessus est égal à: (cf. [3], t.2, p. 48)

$$\frac{1}{r!}\sum_{0\leqq k\leqq r}|s(r,k)|\frac{(x+\alpha-1)^k}{\alpha^k}=\frac{1}{r!}\sum_{0\leqq k\leqq r}\frac{|s(r,k)|}{\alpha^k}\sum_{j=0}^{k}\binom{k}{j}x^j(\alpha-1)^{k-j}=$$

$$=\sum_{j=0}^{r}x^j\sum_{k=j}^{r}\frac{1}{r!}\frac{|s(r,k)|}{\alpha^k}\binom{k}{j}(\alpha-1)^{k-j}.$$

Ce qui nous donne la première formule de la proposition.

On utilise ensuite la majoration:

$$|s(n,k)|\leqq\frac{(n-1)!}{(k-1)!}\left(1+\frac{1}{2}+\ldots+\frac{1}{n-1}\right)^{k-1}.$$

Cette majoration peut être démontrée par récurrence en utilisant la formule:

$$|s(n+1,k+1)|=|s(n,k)|+n|s(n,k+1)|.$$

On obtient alors:

$$c_j\leqq\sum_{k=j}^{r}\frac{1}{r!}\frac{(r-1)!}{(k-1)!}H^{k-1}\frac{k!}{j!(k-j)!}\frac{1}{(\alpha-1)^j}\left(1-\frac{1}{\alpha}\right)^k$$

et en posant $i=k-j$,

$$c_j\leqq\frac{H^{j-1}}{rj!\alpha^j}\sum_{i=0}^{r-j}\frac{H^i(1-1/\alpha)^i}{i!}(i+j).$$

La sommation est majorée par:

$$\sum_{i=0}^{\infty}\frac{(H(1-1/\alpha))^i}{i!}(i+j)=(H(1-1/\alpha)+j)\exp(H(1-1/\alpha)).$$

Compte tenu de ce que

$$H=1+\frac{1}{2}+\ldots+\frac{1}{r-1}\leqq\gamma+\log r$$

on obtient le résultat annoncé.

COROLLAIRE. *Si l'on enlève de S_n un nombre de permutations $O(n!/(\log n)^2)$, celles restantes ont la propriété: Pour tout $\alpha\leqq l/l_2^2$, le nombre de cycles dont la longueur est multiple de α est* $\dfrac{\log n}{\alpha}+O\left(\dfrac{\log n}{\alpha}\right)^{0,8}$.

DÉMONSTRATION. Fixons d'abord α. On pose, avec les notations de la proposition précédente, $x=H/\alpha$, $j_0=x-x^u$, $j_1=x+x^u+1$. On choisira $u=0{,}8$. Le nombre de permutations à enlever, c'est-à-dire celles qui ont moins de j_0 (ou plus de j_1) cycles dont la longueur est multiple de α, vaut:

$$S=\sum_{j\leqq j_0}c_j+\sum_{j\geqq j_1}c_j\leqq 2e^{\gamma}r^{-1/\alpha}\left(\sum_{j\leqq j_0}\frac{x^j}{j!}+\sum_{j\geqq j_1}\frac{x^{j-1}}{(j-1)!}\right)$$

et, par le lemme 1,

$$S \leqq 2e^{\gamma} r^{-1/\alpha}\left(\left(\frac{ex}{j_0}\right)^{j_0}+\left(\frac{ex}{j_1-1}\right)^{j_1-1}\right).$$

Or on a:

$$j_0 \log(ex/j_0) = x-\frac{1}{2}x^{2u-1}+O(x^{3u-2})$$

$$(j_1-1)\log\left(ex/(j_1-1)\right) = x-\frac{1}{2}x^{2u-1}+O(x^{3u-2}).$$

Ce qui nous donne:

$$S = O\left(r^{-1/\alpha}\exp\left(x-\delta x^{2u-1}\right)\right)$$

pour un certain $\delta>0$. On remarque ensuite que

$$H = 1+\frac{1}{2}+\ldots+\frac{1}{r-1} = \log r+O(1)$$

et donc $e^x = O(r^{1/\alpha})$. Enfin, comme $r=[n/\alpha]$, on a: $x=(1/\alpha)\left(l+O(l_2)\right)$; comme $\alpha\leqq l/l_2^2$, on voit que $x\geqq l_2^2/2$ pour n assez grand, et donc

$$S = O\left(\exp\left(-\delta_1 l_1^{1,2}\right)\right) = O(l^{-3})$$

en choisissant $u=0{,}8$.

En faisant le même raisonnement pour tous les $\alpha\leqq l/l_2^2$, on obtient qu'excepté $O(n!/l^2)$ permutations, le nombre de cycles dont la longueur est multiple de α est compris entre $x-x^u$ et $x+x^u+1$, ce qui achève la démonstration du corollaire.

Pour démontrer le théorème 1, nous allons construire des sous-ensembles $S_n^{(1)}\subset \subset S_n, \ldots, S_n^{(i+1)}\subset S_n^{(i)}$, tous tels que $\mathrm{Card}\,(S_n-S_n^{(i)})=O(n!/\sqrt{l})$.

Construction de $S_n^{(1)}$. On utilise le lemme 4 avec $\omega_1=[\sqrt{\log n}]$ et $\omega_2=l_2$. On a bien:

$$1/\omega_1+1/\omega_2! = O\left(1/\sqrt{l}\right)$$

et les $\sigma\in S_n^{(1)}$ ont la propriété

$$P_1\colon \left(n_i > \sqrt{l} \Rightarrow m_i = 1\right) \quad \text{et} \quad \left(n_i \leqq \sqrt{l} \Rightarrow m_i \leqq l_2\right).$$

On désignera par k_0 le nombre entier tel que $n_{k_0}\leqq\sqrt{l}<n_{k_0+1}$. La propriété P_1 s'écrit alors:

$$P_1\colon (1 \leqq i \leqq k_0 \Rightarrow m_i \leqq l_2) \quad \text{et} \quad (k_0 < i \leqq k \Rightarrow m_i = 1).$$

Construction de $S_n^{(2)}$. On utilise le corollaire de la proposition 1. Les $\sigma\in S_n^{(2)}$ auront la propriété P_1 et la propriété P_2:

$$P_2\colon \forall \alpha \leqq l/l_2^2, \quad \sum_{\substack{1\leqq i\leqq k\\ \alpha\mid n_i}} m_i = l/\alpha+O(l/\alpha)^{0,8}.$$

Minoration dans le théorème. 1. Nous allons montrer que pour $\sigma\in S_n^{(2)}$, on a:

$$f(\sigma)-\log(\text{ordre de }\sigma) \geqq ll_2+O(ll_3).$$

On remarque d'abord que, à cause de P_1,

$$\sum_{\substack{1\leqq i\leqq k\\ \alpha|n_i}} m_i = \sum_{\substack{1\leqq i\leqq k\\ \alpha|n_i}} 1 + \sum_{\substack{1\leqq i\leqq k_0\\ \alpha|n_i}} (m_i-1) = N(\alpha)+O\left(\frac{l_2\sqrt{l}}{\alpha}\right).$$

On a donc, par P_2, et si $\alpha\leqq l/l_2^2$:

$$N(\alpha) = (l/\alpha)+O(l/\alpha)^{0,8}. \tag{3}$$

On a ensuite:

$$f(\sigma)-\log(\text{ordre de }\sigma) = \log(n_1\ldots n_k)-\log(\text{p.p.c. } m(n_1,\ldots,n_k)) \geqq$$
$$\geqq \sum_{p\leqq l/l_2^2} \log p\big(N(p)-1\big).$$

Cette dernière somme vaut:

$$\sum_{p\leqq l/l_2^2} l\frac{\log p}{p}+O\left(l^{0,8}\frac{\log p}{p^{0,8}}\right) = ll_2+O(ll_3)$$

par le lemme 3.

Construction de $S_n^{(3)}$. On remarque d'abord, en faisant $\alpha=1$ dans la formule (3), que l'on a pour tout $\sigma\in S_n^{(2)}$ la propriété P_2':

$$P_2'\colon\ k = N(1) = \log n+O(\log n)^{0,8}.$$

En fait, on aurait pu obtenir P_2' à partir des résultats de Gončarov [7], comme l'ont fait P. Erdős et P. Turán [5].

On impose ensuite les propriétés suivantes:

$$P_3\colon\ \forall\alpha\geqq(\log n)^3,\quad N(\alpha)\leqq 1,$$
$$P_3'\colon\ \forall\alpha\geqq(\log n)^{3/2},\quad N(\alpha)\leqq 4,$$
$$P_3''\colon\ \forall y,\quad l/l_2^2\leqq y\leqq l,\quad \forall\alpha\geqq y,\quad N(\alpha)\leqq ll_2/y.$$

Fixons $\alpha\geqq l/l_2^2$ et $j_0\geqq l/\alpha$. Avec les notations de la proposition 1, on a $r\leqq n/2$,

$$H = 1+\ldots+\frac{1}{r-1}\leqq\gamma+\log r\leqq\log n$$

et le nombre de $\sigma\in S_n$ pour lesquelles $N(\alpha)\geqq j_0$ est majoré par:

$$n!\sum_{j\geqq j_0} c_j \leqq 2n!\sum_{j\geqq j_0}\left(\frac{(l/\alpha)^j}{j!}+\frac{(l/\alpha)^{j-1}}{\alpha(j-1)!}\right) = O\left(\frac{el}{\alpha j_0}\right)^{j_0} n!$$

par le lemme 1, à condition que $j_0\geqq 2$ et $j_0\leqq l$.

Pour P_3, on fait $j_0=2$. Le nombre de $\sigma\in S_n$ qui font exceptions à P_3 est majoré par

$$n!O\big(l^2\sum_{\alpha\geqq l^3}\alpha^{-2}\big) = O(n!/l).$$

Pour P_3' on raisonne de même avec $j_0=5$.

Pour P_3'', on fixe y, et α, avec $y\leqq\alpha\leqq l^{3/2}$. (Pour $\alpha>l^{3/2}$, on a par P_3', $N(\alpha)\leqq$ $\leqq 4\leqq ll_2/y$). On choisit $j_0=ll_2/y$. On a bien $l/\alpha\leqq j_0\leqq l$ et on remarque que $j_0\geqq l_2$.

Le nombre d'exceptions est donc:

$$O\left(\frac{ey}{\alpha l_2}\right)^{j_0} n! = O\left(\frac{e}{l_2}\right)^{l_2} n! = O(n!/l^4).$$

Comme il y a au plus l valeurs de y et $l^{3/2}$ valeurs de α, le nombre d'exceptions à P_3'' est négligeable.

PROPOSITION 2. *Soit n assez grand, $m\geqq 1$, $t\geqq 2$, $tm\leqq l/2$, $y\geqq\sqrt{l}$. Le nombre de $\sigma\in S_n^{(2)}$ pour lesquelles il existe m nombres premiers $p_1<p_2<\ldots<p_m$, avec $y\leqq p_1$ tels que $N(p_1)\geqq t, \ldots, N(p_m)\geqq t$ est majoré par:*

$$n!\left(\left(\frac{30\log n}{yt}\right)^t \frac{9y}{m\log y}\right)^m.$$

DÉMONSTRATION. Fixons d'abord $p_1, \ldots, p_m$. Comme $tm\leqq(1/2)\log n$, par la propriété P_2' si σ est telle que chacun de ces p_i divisent au moins la longueur de t cycles distincts, on peut trouver μ cycles de σ, de longueurs $\nu_1<\nu_2<\ldots<\nu_\mu$ avec $t\leqq\mu\leqq tm$ et $\nu_1\geqq\sqrt{\log n}$ tels que $P=p_1^t\ldots p_m^t$ divise $\nu_1\ldots\nu_\mu$. Le nombre de telles σ est donc majoré d'après le lemme 2, par:

$$Q \leqq \sum_{\mu=t}^{tm} \sum_{\substack{\sqrt{\log n}\leqq\nu_1<\nu_2<\ldots<\nu_\mu\leqq n \\ P\mid\nu_1\nu_2\ldots\nu_\mu}} \frac{n!}{\nu_1\ldots\nu_\mu} \leqq \sum_{\mu=t}^{tm} \frac{n!}{(\mu)!} \sum_{\substack{\nu_1=1 \\ \vdots \\ \nu_\mu=1 \\ P\mid\nu_1\ldots\nu_\mu}}^{n} \frac{1}{\nu_1\ldots\nu_\mu}$$

On peut mettre $1/P$ en facteurs dans la dernière somme, à condition de multiplier par $\tau_\mu(P)=\binom{\mu+t-1}{t}^m$. La fonction $\tau_r(n)$ est définie par:

$$\tau_2(n) = \sum_{d\mid n} 1$$

pour $r\geqq 3$,

$$\tau_r(n) = \sum_{d\mid n} \tau_{r-1}(d).$$

Il s'ensuit que:

$$Q \leqq \sum_{\mu=t}^{tm} \frac{n!}{(\mu)!P} \left(\sum_{\substack{\nu_1'=1 \\ \vdots \\ \nu_\mu'=1}}^{n} \frac{1}{\nu_1'\ldots\nu_\mu'}\right)\binom{\mu+t-1}{t}^m \leqq$$

$$\leqq \sum_{\mu=t}^{tm} \frac{n!}{(\mu)!P} (2\log n)^\mu \frac{(\mu+t)^{tm}}{(t!)^m} \leqq \frac{n!}{P}\left(\frac{4e^2\log n}{t}\right)^{tm} \frac{\sum_{\mu=t}^{tm}\left(\frac{\mu}{\log n}\right)^{tm-\mu}}{(\sqrt{2\pi t})^{m+1}} \leqq$$

$$\leqq \frac{n!}{P}\left(\frac{4e^2\log n}{t}\right)^{tm} \frac{tm}{(\sqrt{2\pi t})^{m+1}} \leqq \frac{n!}{p_1^t\ldots p_m^t}\left(\frac{30\log n}{t}\right)^{tm}$$

en minorant $u!$ par $\sqrt{2\pi u}\,u^u e^{-u}$, et en majorant $\mu+t$ par 2μ et $4e^2$ par 30.

Maintenant, on fait varier les nombres premiers $p_1, \ldots, p_m$. On a:

$$\sum_{y \leqq p_1 < \ldots < p_m} \frac{1}{p_1^t \cdots p_m^t} \leqq \frac{1}{m!}\left(\sum_{p \geqq y} \frac{1}{p^t}\right)^m \leqq \left(\frac{e}{m} \sum_{p \geqq y} \frac{1}{p^t}\right)^m \leqq \left(\frac{9}{m y^{t-1} \log y}\right)^m$$

d'après le lemme 3, ce qui achève la démonstration.

Construction de $S_n^{(4)}$. On va imposer aux $\sigma \in S_n^{(3)}$ la condition suivante; avec $c_0 = 18 \exp(60/e)$

$$P_4\colon \forall t, \quad 2 \leqq t \leqq l_2, \quad m_t = \operatorname{Card}\{p \geqq l;\ N(p \geqq t\} \leqq c_0 2^{-t} l/l_2.$$

Fixons d'abord t; on applique la proposition 2, avec $y = \log n$, $m = [c_0 2^{-t} l/l_2] + 1$. Le nombre d'exceptions est allors majoré par:

$$n! 2^{-c_0 2^{-l_2} l/l_2} = O(n! l^{-2})$$

et on fait ensuite varier t.

Construction de $S_n^{(5)}$. La condition supplémentaire imposée est

$$P_5\colon \forall y, \quad l/l_2^2 \leqq y \leqq l, \quad \forall s, \quad 2 \leqq s \leqq l_2,$$

$$m_s' = \operatorname{Card}\{p \geqq y;\ N(p) > 60 ls/y\} \leqq 36 \cdot 2^{-s} y/l_2.$$

On fixe d'abord y et s, on applique la proposition 2 avec $t = [60\, ls/y] + 1$ et $m = [36 \cdot 2^{-s} y/l_2] + 1$, et on termine comme précédemment.

Démonstration de la majoration dans le théorème. Soit $\sigma \in S_n^{(5)}$, nous devons majorer $f(\sigma) - \log$ (ordre de σ). Cette quantité est d'abord majorée par:

$$\sum_{\substack{p,a \\ N(p^a) \geqq 2}} (\log p) N(p^a) = \sum_{i=1}^{7} T_i$$

où les sommes partielles T_i portent sur les couples (p, a), p premier, $a \geqq 1$ vérifiant $N(p^a) \geqq 2$ et:

$$i = 1 \quad p^a > l^3$$

$$i = 2 \quad p^a \leqq l/l_2^2$$

$$i = 3 \quad a = 1 \quad \text{et} \quad l/l_2^2 < p \leqq l$$

$$i = 4 \quad a = 1 \quad \text{et} \quad l < p \leqq l^3$$

$$i = 5 \quad a \geqq 2 \quad \text{et} \quad l/l_2^2 < p \leqq l^{3/2}$$

$$i = 6 \quad a \geqq 2, \quad p \leqq l \quad \text{et} \quad l^{3/2} < p^a \leqq l^3$$

$$i = 7 \quad a \geqq 2, \quad p > l \quad \text{et} \quad l^{3/2} < p^a \leqq l^3.$$

Par la propriété P_3, la somme T_1 est vide.

Par P_2, on a:

$$T_2 \leqq \sum_{p^a \leqq l/l_2^2} l \frac{\log p}{p} + O\left(l^{0,8} \frac{\log p}{p^{0,8a}}\right) \leqq l l_2 + O(l l_3),$$

par le lemme 3.

Dans T_5 le nombre de termes est $O(l^{3/4})$, et par P_3'', on a:

$$T_5 = O(l^{3/4} l_2^4).$$

Dans T_6, en utilisant P_3', on a:

$$T_6 \leqq \sum_{p \leqq l} \log p \sum_{a \leqq 3l_2/\log p} 4 \leqq 12 l_2 \pi(l) = O(l).$$

Dans T_7, on remarque que a vaut exactement 2 et comme $N(p^a) \leqq N(p)$, on constate que $T_7 \leqq T_4$. On a ensuite:

$$T_4 = \sum_{\substack{l < p \leqq l^3 \\ N(p) \geqq 2}} (\log p) N(p) \leqq 3 l_2 \sum_{\substack{l < p \leqq l^3 \\ N(p) \geqq 2}} N(p).$$

D'après P_3'', $N(p) \leqq l_2$ et par la propriété P_4,

$$T_4 \leqq 3 l_2 \sum_{t=2}^{l_2} t m_t = O(l).$$

Pour évaluer T_3, choisissons y, $l/l_2^2 \leqq y \leqq l/2$ et considérons

$$W_y = \sum_{y < p \leqq 2y} (\log p) N(p) \leqq l_2 \sum_{y < p \leqq 2y} N(p).$$

Nous allons montrer que pour tout y, $W_y = O(l)$. Il en résultera que $T_3 = O(l l_3)$ ce qui achèvera la démonstration du thèoreme. Par la propriété P_3'', on a $N(p) \leqq l l_2 / y$. Ensuite, par P_5,

$$\sum_{y < p \leqq 2y} N(p) \leqq \frac{120 l}{y} \Big(\sum_{y < p \leqq 2y} 1 \Big) + \sum_{s=2}^{[l_2]} \frac{60 l (s+1)}{y} m_s' = O(l/l_2).$$

Pour supprimer le «l_3» dans le reste du théorème 1, il faudrait pouvoir montrer que:

$$T_3 = 2 l l_3 + O(l).$$

III. Démonstration du théorème 2

Nous utiliserons la notation suivante pour les séries entières:

$$\sum_{n=0}^{\infty} a_n z^n \ll \sum_{n=0}^{\infty} b_n z^n$$

signifie: pour tout $n \geqq 0$, $|a_n| \leqq b_n$.

LEMME 5. *On a:*

$$\sum_{m=2}^{\infty} \frac{\log m}{m} z^m - \frac{1}{2} \log^2 \frac{1}{1-z} \ll \log \frac{1}{1-z} = \sum_{m=1}^{\infty} \frac{z^m}{m}.$$

LEMME 6. *On a:*

$$\sum_{m=2}^{\infty} \frac{\log^2 m}{m} z^m - \frac{1}{3} \log^3 \frac{1}{1-z} \ll 2 \sum_{m=2}^{\infty} \frac{\log m}{m} z^m.$$

LEMME 7. *Soit* $a>0$ *et une suite de coefficients* a_k *vérifiant* $|a_k|\leqq a/k$ *pour* $1\leqq k\leqq n$. *On pose:*

$$\exp\Big(\sum_{k\geqq 1}\alpha_k z^k\Big) = 1+\sum_{k=1}^{\infty} b_k z^k.$$

Alors, on a, pour $1\leqq k\leqq n$

$$|b_k| \leqq a e^a k^{a-1}.$$

LEMME 8. *Soit* $n\geqq 3$ *et* $t\in\mathbf{R}$, *vérifiant* $|t|\leqq\sqrt{\log n}$. *On pose:*

$$h(z) = \frac{1}{1-z}\exp\left\{\frac{it}{2\log^{3/2} n}\log^2\frac{1}{1-z} - \frac{t^2}{6\log^3 n}\log^3\frac{1}{1-z}\right\} = \sum_{m=0}^{\infty} e_m z^m.$$

Alors on a, $e_0=e_1=1$, *et*

$$e_n = \exp\left\{\frac{it\sqrt{\log n}}{2} - \frac{t^2}{6}\right\} + O\left(e^{-t^2/6}\frac{|t|}{\sqrt{\log n}}\right) + O\left(\frac{1}{n}\right)$$

et pour $2\leqq m\leqq n$,

$$|e_m| = O\left(\exp\left\{-\frac{t^2}{6}\frac{\log^3 m}{\log^3 n}\right\}\right) + O(2^{-m})$$

où les O sous entendent des constantes explicites.

La démonstration des lemmes 5 à 8 se trouve dans [10]. Sous une forme un peu moins précise, ces lemmes figuraient dans [5].

LEMME 9. *On a pour tout x réel et m entier* $\geqq 1$,

$$\left|e^{ix} - 1 - ix - \ldots - \frac{(ix)^{m-1}}{(m-1)!}\right| \leqq \frac{|x|^m}{m!}.$$

La démonstration est facile, et se trouve par exemple dans [6], p. 512.

LEMME 10. *Soit a un nombre réel vérifiant* $0\leqq a\leqq 1/6$. *Soit* a_k *une suite de coefficients vérifiant* $|a_k|\leqq a/k^2$ *pour* $k\geqq 1$. *On pose:*

$$\exp\Big(\sum_{k\geqq 1} a_k z^k\Big) = 1+\sum_{k\geqq 1} b_k z^k.$$

Alors on a pour $k\geqq 1$:

$$|b_k| \leqq 2a/k^2.$$

DÉMONSTRATION. On pose:

$$y(z) = \exp\Big(\sum_{k\geqq 1} a z^k/k^2\Big) = 1+\sum_{k\geqq 1} u_k z^k.$$

On a évidemment $|b_k|\leqq u_k$ pour tout $k\geqq 1$. D'autre part, y vérifie l'équation différentielle:

$$y' = a y\Big(\sum_{k\geqq 1} z^{k-1}/k\Big)$$

d'où l'on déduit, pour $n\geqq 0$

$$(n+1)u_{n+1} = \frac{a}{n+1} + \sum_{j=1}^{n} a u_j/(n-j+1).$$

Montrons par récurrence sur n, que l'on a $u_n \leqq 2a/n^2$. La relation est vérifiée pour $n=1$, puisque $u_1=a$. Supposons la vérifiée jusqu'à n ($n \geqq 1$) et montrons la pour $n+1$. On a:

$$(n+1)u_{n+1} \leqq \frac{a}{n+1} + \sum_{j=1}^{n} \frac{2a^2}{j^2(n-j+1)} =$$

$$= \frac{a}{n+1} + 2a^2 \sum_{j=1}^{n} \left(\frac{1}{(n+1)j^2} + \frac{1}{(n+1)^2 j} + \frac{1}{(n+1)^2(n+1-j)} \right).$$

Or on a:

$$\frac{1}{n+1} \sum_{j=1}^{n} \frac{1}{j} \leqq \frac{1+\log n}{n+1} \leqq 0{,}6 \quad \text{et} \quad \sum_{j=1}^{n} 1/j^2 \leqq \pi^2/6 \leqq 5/3,$$

ce qui donne:

$$(n+1)^2 u_{n+1} \leqq a + \frac{10a^2}{3} + 2{,}4a^2 \leqq 2a \text{ lorsque } a \leqq 1/6.$$

REMARQUE. Cette condition $a \leqq 1/6$ n'est pas indispensable. En utilisant les méthodes de l'analyse complexe, *H.* Delange peut démontrer que pour tout a fixé, le coefficient u_k ci-dessus vérifie $u_k \sim ae^a/k^2$.

LEMME 11. *Soit* $n_1 < n_2 < \ldots < n_k$ *les longueurs distinctes des cycles de* $\sigma \in S_n$. *La valeur moyenne de* $f(\sigma) = \sum_{1 \leqq i \leqq k} \log n_i$ *vérifie:*

$$M_n = \frac{1}{n!} \sum_{\sigma \in S_n} f(\sigma) = \frac{1}{2} \log^2 n + O(1).$$

DÉMONSTRATION. Rappelons d'abord le résultat classique: soit k, $1 \leqq k \leqq n$; le nombre de permutations de S_n qui n'ont aucun cycle de longueur j est:

$$n! \sum_{j=0}^{[n/k]} (-1)^j/(j!\, k^j).$$

Lorsque $k=1$, c'est le problème des chapeaux (cf. [3], p. 10). Il s'ensuit que, le nombre $d(n, k)$ de permutations qui ont au moins un cycle de longueur k vérifie:

$$\frac{n!}{k}\left(1 - \frac{1}{2k}\right) \leqq d(n, k) \leqq n!/k.$$

On remarque ensuite que l'on a:

$$M_n = \frac{1}{n!} \sum_{1 \leqq k \leqq n} (\log k) d(n, k) = \sum_{1 \leqq k \leqq n} \frac{\log k}{k} + O(1) =$$

$$= \int_1^n \frac{\log x}{x}\, dx + O(1) = \frac{1}{2} \log^2 n + O(1).$$

1ère *étape*. Avec la notation du lemme 11, on pose:

$$F_n(x) = \text{Prob}\{f(\sigma) - M_n < x \log^{3/2} n\}.$$

On associe à la distribution de probabilités F_n sa fonction caractéristique, définie par l'intégrale de Stieltjes:

$$\varphi_n(t) = \int_{-\infty}^{+\infty} e^{itx} dF_n(x).$$

On a, d'après [5], p. 313:

$$\varphi_n(t) = \exp\left\{\frac{-itM_n}{\log^{3/2} n}\right\} \cdot \text{Coeff. de } z^n \text{ dans } \frac{1}{1-z} \exp D_n(z, \tau) \tag{4}$$

avec

$$\tau = t(\log n)^{-3/2}$$

et

$$D_n(z, \tau) = \sum_{j=2}^{n} \log\{1+(j^{i\tau}-1)(1-e^{-z^j/j})\}.$$

2ème *étape*. P. Erdős et P. Turán ont montré que pour t fixé,

$$\lim \varphi_n(t) = \exp(-t^2/6). \tag{5}$$

En vue d'une estimation du terme d'erreur dans (5), nous supposerons que $|t| \leqq \leqq \beta\sqrt{\log n}$, où β est une constante assez petite. Les majorations qui suivent, y compris les «O» seront valides pour $|t| \leqq \beta\sqrt{\log n}$ et $n \geqq n_0$, où n_0 est une constante absolue.

On écrit comme dans [5]:

$$D_n(z, \tau) = h_1(z)+h_2(z)+h_3(z)+h_4(z)$$

avec

$$h_1(z) = \sum_{j=2}^{n} \left\{i\tau \frac{\log j}{j} - \frac{\tau^2}{2} \frac{\log^2 j}{j}\right\} z^j,$$

$$h_2(z) = \sum_{j=2}^{n} \left\{\frac{j^{i\tau}-1}{j} - i\tau \frac{\log j}{j} + \frac{\tau^2}{2} \frac{\log^2 j}{j}\right\} z^j,$$

$$h_3(z) = \sum_{j=2}^{n} (j^{i\tau}-1)(1-e^{-z^j/j} - z^j/j),$$

$$h_4(z) = \sum_{j=2}^{n} \sum_{r=2}^{\infty} \frac{(-1)^{r-1}}{r} (j^{i\tau}-1)^r (1-e^{-z^j/j})^r.$$

On a, par le lemme 9, avec la notation $\ll$:

$$h_2(z) \ll \sum_{j=2}^{n} \frac{|\tau|^3 \log^3 j}{6j} z^j \ll \sum_{j=2}^{n} \frac{|t|^3}{6(\log n)^{3/2}} \frac{z^j}{j}.$$

Et, P. Erdős et P. Turán donnent:

$$h_4(z) \ll c_4 \frac{t^2}{\log n} \sum_{j=4}^{\infty} \frac{z^j}{j^2}$$

et

$$h_3(z) \ll c_3 \frac{|t|}{\sqrt{\log n}} \sum_{j=4}^{\infty} \frac{z^j}{j^2}.$$

On remarque que la condition: $n>\exp(10^4 t^2)$ est assurée en choisissant $\beta<10^{-2}$. On peut donc écrire:

$$D_n(z,\tau) = h_1(z) + \sum_{j=2}^{\infty} a_j^{(1)} z^j \tag{6}$$

avec

$$|a_j^{(1)}| \leqq c^{(1)} \frac{|t|}{\sqrt{\log n}} \left(\frac{1}{j^2} + \frac{t^2}{j \log n}\right). \tag{7}$$

3ème *étape.* Compte tenu de (6), et en observant que les puissances de z d'exposant $>n$ n'interviennent pas, (4) devient:

$$\varphi_n(t) = \exp\left\{-\frac{itM_n}{\log^{3/2} n}\right\} \cdot \text{Coeff. de } z^n \text{ dans}$$

$$\frac{1}{1-z} \exp\left\{i\tau \sum_{j=2}^{\infty} \frac{\log j}{j} z^j - \frac{\tau^2}{2} \sum_{j=2}^{\infty} \frac{\log^2 j}{j} z^j\right\} \exp\left\{\sum_{j=2}^{\infty} a_j^{(1)} z^j\right\}.$$

On utilise alors les lemmes 5 et 6, et avec la définition de la fonction h dans le lemme 8, on obtient:

$$\varphi_n(t) = \exp\left\{\frac{-itM_n}{\log^{3/2} n}\right\} \cdot \text{Coeff. de } z^n \text{ dans } h(z) \exp\left\{\sum_{j=2}^{\infty} a_j^{(2)} z^j\right\} \tag{8}$$

avec

$$|a_j^{(2)}| \leqq c^{(2)} \left(\frac{|t|}{j^2 \sqrt{\log n}} + \frac{|t^3|+|t|}{j \log^{3/2} n}\right),$$

pour $2 \leqq j \leqq n$.

4ème *étape.* On pose:

$$\begin{cases} \exp\left(\sum_{j=2}^{\infty} a_j^{(2)} z^j\right) = 1 + \sum_{j=2}^{\infty} a_j^{(3)} z^j, \\ \exp\left(\sum_{j=2}^{\infty} \frac{c^{(2)}|t|}{j^2 \sqrt{\log n}} z^j\right) = 1 + \sum_{j=2}^{\infty} b_j^{(1)} z^j, \\ a = a(t,n) = \frac{c^{(2)}(|t|+|t^3|)}{\log^{3/2} n}. \end{cases} \tag{9}$$

(On impose à β d'être assez petit de façon à avoir $a \leqq 1/3$)

$$\exp\left(\sum_{j=2}^{\infty} a(t,n) \frac{z^j}{j}\right) = 1 + \sum_{j=2}^{\infty} b_j^{(2)} z^j,$$

$$\left(1 + \sum_{j=2}^{\infty} b_j^{(1)} z^j\right)\left(1 + \sum_{j=2}^{\infty} b_j^{(2)} z^j\right) = 1 + \sum_{j=2}^{\infty} b_j z^j.$$

On aura alors, pour $2 \leqq j \leqq n$,

$$|a_j^{(3)}| \leqq b_j.$$

Il reste à estimer b_j. D'après le lemme 7, on aura:

$$b_j^{(2)} \leqq e^{1/3} a j^{a-1} \leqq 2a j^{a-1}$$

et d'après le lemme 10, en choisissant $\beta<1/6c^{(2)}$,

$$b_j^{(1)} \leqq \frac{2c^{(2)}|t|}{\sqrt{\log n}\, j^2}.$$

Il s'ensuit que:

$$b_j \leqq b_j^{(1)} + b_j^{(2)} + \sum_{r=2}^{j-2} 4c^{(2)} \frac{|t|}{\sqrt{\log n}\, r^2} \frac{a}{(j-r)^{1-a}}.$$

On coupe la somme en deux, suivant que $r \leqq j/2$ ou non. On a:

$$\sum_{2 \leqq r \leqq j/2} \frac{a}{r^2(j-r)^{1-a}} = O(aj^{a-1})$$

et

$$\sum_{j/2 < r \leqq j-2} \frac{a}{r^2(j-r)^{1-a}} \leqq \frac{4}{j^2} \sum_{r=2}^{[j/2]} a r^{a-1} = O(j^{-5/3}).$$

On a donc, pour $2 \leqq j \leqq n$:

$$a_j^{(3)} = O\left(\frac{|t|}{\sqrt{\log n}}\, j^{-5/3} + a j^{-1+a}\right)$$

d'où l'on déduit:

(10) $$a_j^{(3)} = O(j^{-2/3}) \quad (2 \leqq j \leqq n)$$

et

(11) $$\sum_{j=2}^{n} |a_j^{(3)}| = O\left(\frac{|t|}{\sqrt{\log n}} + \exp\left\{c^{(2)} \frac{|t|+|t^3|}{\sqrt{\log n}}\right\} - 1\right).$$

5e *étape.* Compte tenu de (9), et avec les notations du lemme 8, (8) devient:

$$\varphi_n(t) = \exp\left\{\frac{-itM_n}{\log^{3/2} n}\right\}\left(e_n + \sum_{j=2}^{n-1} a_j^{(3)} e_{n-j} + a_n^{(3)}\right).$$

Le même calcul que dans [10] donne, en tenant compte du lemme 8, de (10) et de (11):

(12)

$$\varphi_n(t) = \exp(-t^2/6) + (\exp(-t^2/48))O\left(\frac{|t|}{\sqrt{\log n}} + \exp\left(c^{(2)} \frac{|t|+|t^3|}{\sqrt{\log n}}\right) - 1\right) + O(n^{-1/6}).$$

6e *étape.* On pose:

$$F(x) = \sqrt{\frac{3}{2\pi}} \int_{-\infty}^{x} e^{-(3/2)u^2}\, du.$$

Sa fonction caractéristique vaut:

$$\varphi(t) = \int_{-\infty}^{+\infty} e^{itx}\, dF(x) = e^{-t^2/6}$$

et l'on a la formule (cf. [Fel], p. 538):

(13) $$|F_n(x) - F(x)| \leqq \frac{1}{\pi} \int_{-T}^{T} \left|\frac{\varphi_n(t) - \varphi(t)}{t}\right| dt + \frac{24F'(0)}{\pi T}$$

valable pour tout x réel et tout $T>0$. On choisit $T=\beta\sqrt{\log n}$ avec β assez petit. Le même calcul que dans [10] permet de déduire des formules (12) et (13) que l'on a, uniformément en x:

$$F_n(x)-F(x)=O\left(1/\sqrt{\log n}\right). \tag{14}$$

La démonstration du théorème 2 découle alors de (14), puisque l'on a:

$$\text{Prob}\left\{\frac{f(\sigma)-(1/2)\log^2 n}{(1/\sqrt{3})\log^{3/2} n}<x\right\}=F_n(y)$$

avec

$$y=x/\sqrt{3}+\left((1/2)\log^2 n-M_n\right)/\log^{3/2} n=x/\sqrt{3}+O\left(\log^{-3/2} n\right)$$

par le lemme 11.

References

[1] M. R. Best, The distribution of some variables on symmetric groups, *Indag. Math.*, **32** (1970), 385—402.
[2] J. D. Bovey, An approximate probability distribution for the order of elements of the symmetric group, *Bull. London Math. Soc.*, **12** (1980), 41—46.
[3] L. Comtet, *Analyse combinatoire*, Presses Universitaires de France (Paris, 1970), collection SUP.
[4] P. Erdős and P. Turán, On some problems of a statistical grouptheory I, *Zeitschr. für Wahrscheinlichkeitstheorie und verw. Gebiete*, **4** (1965), 175—186.
[5] P. Erdős and P. Turán, On some problems of a statistical grouptheory. III, *Acta Math. Acad. Sci. Hungar.*, **18** (1967), 309—320.
[6] W. Feller, *An introduction to probability theory and its applications*, vol II, 2nd edition, J. Wiley and sons (1966—1971).
[7] V. L. Gončarov, On the field of combinatory analysis, *Izvestija Akad. Nauk SSSR, Ser. mat.* **8** (1944), 3—48 et *Translations of the Amer. Math. Soc.*, Ser. 2, **19** (1962), 1—46.
[8] H. Halberstam and K. F. Roth, *Sequences*, Clarendon Press (Oxford, 1966).
[9] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4 th. edition, Clarendon Press (Oxford, 1960).
[10] J. L. Nicolas, *A Gaussian law on* $\mathbf{F}_q[X]$, Coll. Math. Soc. János Bolyai 34, Topics in classical number theory, ed: G. Halász, Elsevier/North Holland, 1127—1162.
[11] V. N. Sačkov, *Probability methods in Combinatorial analysis*, (en russe), Nauka (Moscow, 1978).

(Reçu le 12. octobre 1982.)

U. E. R. DES SCIENCES DE LIMOGES
DÉPARTEMENT DE MATHÉMATIQUES
123 RUE ALBERT-THOMAS
F-87 060 LIMOGES CEDEX
FRANCE