Cycles of random permutations with restricted cycle lengths

Florent Benaych-Georges

CYCLES OF RANDOM PERMUTATIONS WITH RESTRICTED CYCLE LENGTHS

FLORENT BENAYCH-GEORGES

Abstract. We prove some general results about the asymptotics of the distribution of the number of cycles of given length of a random permutation which distribution is invariant under conjugation. These results were first established to be applied in a forthcoming paper ([BG]) were we prove results about cycles of random permutations which can be written as free words in several independent random permutations. However, we also apply them here to prove asymptotic results about random permutations with restricted cycle lengths. More specifically, for A set of positive integers, we consider a random permutation chosen uniformly among permutations of $\{1, \dots, n\}$ which have all their cycle lengths in A, and then let n tend to infinity. We prove that if A is infinite and large enough, then the number of cycles of different given cycle lengths of this random permutation are asymptotically independent and distributed according to Poisson distributions. In the case where A is finite, we prove that the behavior of these random variables is completely different: cycles with length $\max A$ are predominant.

Introduction

0.1. **Presentation of the results.** It is well known that if for all positive integer n, σ_n is a random permutation chosen uniformly among all permutations of $\{1, \dots, n\}$ and if for all positive integer l, $N_l(\sigma_n)$ denotes the number of cycles of length l in the decomposition of σ_n as a product of cycles with disjoint supports, then for all $l \geq 1$, the joint distribution of the random vector

$$(N_1(\sigma_n), \dots, N_l(\sigma_n))$$

converges weakly, as n goes to infinity, to

$$\mathrm{Poiss}(1/1) \otimes \mathrm{Poiss}(1/2) \otimes \cdots \otimes \mathrm{Poiss}(1/l),$$

where for all positive number λ, $\mathrm{Poiss}(\lambda)$ denotes the Poisson distribution with mean λ.

The proof of this result is rather simple (one can find it in [ABT05]) because the uniform distribution on the symmetric group is easy to handle. However, many other distributions on the symmetric group give rise to limit distributions for the number of cycles of given length. In the first section of this paper, we shall prove a general theorem about the convergence of the distributions of the number of cycles of given length of random permutations (theorem 1.5). This result will play a key roll in a forthcoming paper ([BG]) were we prove results about cycles of random permutations which can be written as free words in several independent random permutations with restricted cycle length.

Date: December 12, 2007.
MSC 2000 subject classifications. primary 20B30, 60B15, secondary 60C05.
Key words. Random permutation, cycle, random permutation with restricted cycle length.

In the second part of the paper, for A set of positive integers, we introduce $\mathfrak{S}_n^{(A)}$ to be the set of permutations of $\{1,\dots,n\}$ which have all their cycle lengths in A. For all n such that $\mathfrak{S}_n^{(A)} \neq \emptyset$, we consider a random permutation σ_n chosen uniformly in $\mathfrak{S}_n^{(A)}$.

We first prove, as an application of our general result mentioned above, that if A is infinite and satisfies

$$\sum_{\substack{j\geq 1\\ j\notin A}} \frac{1}{j} < \infty,$$

then the result presented in the first paragraph about uniform random permutations stays as true as it can (as long as we consider the fact that for all $l \notin A$, $N_l(\sigma_n) = 0$): for all $l \geq 1$, the distribution of the random vector

$$(N_k(\sigma_n))_{1\leq k\leq l, k\in A}$$

converges weakly, as n goes to infinity in such a way that $\mathfrak{S}_n^{(A)}$ is non empty, to

$$\bigotimes_{1\leq k\leq l, k\in A} \mathrm{Poiss}(1/k).$$

Note that it implies that the number of cycles of any given length takes large values with a very small probability even though n goes to infinity. Hence if A is finite, such a result cannot be expected. We also study this case here, and prove that if one denotes $\max A$ by d, for all $l \in A$, $N_l(\sigma_n)/n^{l/d}$ converges in every L^p space to $1/l$. As a consequence, the cycles with length d will be predominant: the cardinality of the subset of $\{1,\dots,n\}$ covered by the supports of cycles with length d in such a random permutation is equivalent to n, which means that the random permutation is not faraway from having order d. This remark will appear to be very helpful in the study of words in independent such random permutations.

0.2. **Comments on these results and open questions.** a) In corollary 1.7, we give a general sufficient condition on certain sequences σ_n of random permutations to have the weak convergence of the distribution of $(N_1(\sigma_n),\dots,N_l(\sigma_n))$ to $\mathrm{Poiss}(1/1)\otimes\mathrm{Poiss}(1/2)\otimes\cdots\otimes\mathrm{Poiss}(1/l)$ for all $l \geq 1$ as n goes to infinity. It would be interesting to know if this condition is sufficient. For more details, see remark 1.8.

b) There is another question the author would like to point at: in the case where A is finite, the convergence we prove for the (renormalised) sequence $N_l(\sigma_n))$ is to a constant limit: $N_l(\sigma_n)/n^{l/d}$ tends to $1/l$. It would be interesting to know if we have a dilation of the random variables of $N_l(\sigma_n)/n^{l/d} - 1/l$ which has a non degenerate weak limit as n goes to infinity.

0.3. **Notations.** In this text, for n integer, we shall denote $\{1,\dots,n\}$ by $[n]$ and the group of permutations of $[n]$ by $\mathfrak{S}_n$. For A set of positive integers, $\mathfrak{S}_n^{(A)}$ denotes the set of permutations of $[n]$ which cycles have length in A. For $\sigma \in \mathfrak{S}_n$ and $l \geq 1$, we shall denote by $N_l(\sigma)$ the number of cycles of length l in the decomposition of σ as a product of cycles with disjoint supports. For $\lambda > 0$, $\mathrm{Poiss}(\lambda)$ will denote the Poisson distribution with parameter λ. $\mathbb{N}$ will denote the set of non negative integers.

1. A general result about cycles of random permutations

1.1. **Technical preliminaries about boolean polynomials.** This section is devoted to the proof of corollary 1.3, that we did not find in the literature. Let us first introduce the terminology

of [B01]. A *boolean polynomial* $f(X_1,\dots,X_N)$ in the indeterminate sets $X_1,\dots,X_N$ is a formula of the type

$$f(X_1,\dots,X_N) = (\cap_{\in I} X_i) \cap \left(\cap_{j\in J} X_j^c\right),$$

where I, J are disjoint subsets of $[N]$ and where for all j, X_j^c designs the complementary set of X_j. It is said to be *complete* if J is the complementary set of I. A *disjoint sum of complete boolean polynomials* is a formula of the type

$$f(X_1,\dots,X_N) = \cup_{i=1}^{L} f_i(X_1,\dots,X_N),$$

where $L \geq 1$ and the f_i's are pairwise distinct complete boolean polynomials.

Remark 1.1. *Using the classical distributivity rules, it is easy to see that any boolean polynomial can be put under the form of a disjoint sum of complete boolean polynomials.*

The following theorem can be found in section 1.4 of [B01], but for the convenience of the reader, we give its proof.

Theorem 1.2. *Fix $n \geq 1$, $\lambda_1,\dots,\lambda_n \in \mathbb{R}$, $f_1,\dots,f_n$ boolean polynomials in the indeterminate sets $X_1,\dots,X_N$. Then in order to have*

$$\sum_{k=1}^{n} \lambda_k P(f_k(A_1,\dots,A_N)) \geq 0 \quad \textit{(resp. } = 0\textit{)}$$

for all family $A_1,\dots,A_N$ of events in any probability space (Ω,Σ,P), it suffices to prove it under the additional hypothesis that each of the A_i's is either $\emptyset$ or Ω.

Proof. We only prove the result for $\geq$ and the other one follows. Using remark 1.1, we can suppose that there exists a family $(C_I)_{I\subset[N]}$ of real numbers indexed by the set of subsets of $[N]$ such that for all family $A_1,\dots,A_N$ of events in a probability space (Ω,Σ,P),

$$\sum_{k=1}^{n} \lambda_k P(f_k(A_1,\dots,A_N)) = \sum_{I\subset[N]} C_I P\left[(\cap_{i\in I} X_i) \cap \left(\cap_{j\in I^c} X_j^c\right)\right].$$

It suffices to prove that for all $I_0 \subset [N]$, $C_{I_0} \geq 0$. It follows from the equation

$$\sum_{I\subset[N]} C_I P\left[(\cap_{in I} X_i) \cap \left(\cap_{j\in I^c} X_j^c\right)\right] = \sum_{k=1}^{n} \lambda_k P(f_k(A_1,\dots,A_N)) \geq 0$$

where we chose every A_i to be either Ω or $\emptyset$ according to $i \in I_0$ or not. $\square$

We shall use the following corollary to prove theorem 1.5.

Corollary 1.3. *Consider a probability space (Ω,Σ,P), $q \geq 1$, and for all $i = 1,\dots,q$, $(A_{i,j})_{j\in I_i}$ a finite family of events. Let us define, for $i = 1,\dots,q$ and $\omega \in \Omega$,*

$$C_i(\omega) = |\{j \in I_i\,;\, \omega \in A_{i,j}\}|.$$

Let us also define, for $k = (k_1,\dots,k_q) \in \mathbb{N}^q \backslash \{0\}$,

$$S_k = \sum_{\substack{J_1\subset I_1 \\ |J_1|=k_1}} \cdots \sum_{\substack{J_q\subset I_q \\ |J_q|=k_q}} P(\cap_{l=1}^{q} \cap_{j\in J_l} A_{i,j})$$

and $S_0 = 1$. Then for all $r = (r_1,\dots,r_q) \in \mathbb{N}^q$,

$$P(C = r) = \sum_{k_1=r_1}^{|I_1|} \cdots \sum_{k_q=r_q}^{|I_q|} (-1)^{k_1-r_1+\cdots+k_q-r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1,\dots,k_q)}. \tag{1}$$

Moreover, "alternating inequalities" are satisfied in the following way: for all $m \geq 0$ odd (resp. even),

$$P(C = r) \geq \sum_{\substack{k_1 = r_1, \ldots, |I_1| \\ \vdots \\ k_q = r_q, \ldots, |I_q| \\ k_1 - r_1 + \cdots + k_q - r_q \leq m}} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1, \ldots, k_q)} \quad \textit{(resp. } \leq \textit{)}. \tag{2}$$

Proof. First note that the alternating inequalities, used for m large enough, imply (1). So we are only going to prove the alternating inequalities.

Then, let us suppose that for all $i = 1, \ldots, q$, $I_i = [n_i]$, with $n_i \geq 1$. As an application of the previous theorem, one can suppose every $A_{i,j}$ to be either $\emptyset$ or Ω. In this case, for all $i = 1, \ldots, q$, the random variable C_i is constant, equal to the number c_i of j's such that $A_{i,j} = \Omega$, and for all $k = (k_1, \ldots, k_q) \in \mathbb{N}^q$,

$$S_k = \binom{c_1}{k_1} \cdots \binom{c_q}{k_q}.$$

Hence for $(r_1, \ldots, r_q) = (c_1, \ldots, c_q)$, for all $m \geq 0$,

$$\begin{aligned} &\sum_{\substack{k_1 = r_1, \ldots, n_1 \\ \vdots \\ k_q = r_q, \ldots, n_q \\ k_1 - r_1 + \cdots + k_q - r_q \leq m}} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1, \ldots, k_q)} \\ = &\sum_{\substack{k_1 = c_1, \ldots, n_1 \\ \vdots \\ k_q = c_q, \ldots, n_q \\ k_1 - r_1 + \cdots + k_q - r_q \leq m}} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{c_1} \cdots \binom{k_q}{c_q} \binom{c_1}{k_1} \cdots \binom{c_q}{k_q}, \end{aligned}$$

which is equal to 1, i.e. to $P(C = r)$.

Now consider $(r_1, \ldots, r_q) \neq (c_1, \ldots, c_q)$. Then $P(C = r) = 0$ and we have to prove that the right-hand-side term in equation (2) is either non negative or non positive according to m is even or odd. For all $m \geq 0$,

$$\begin{aligned} &\sum_{\substack{k_1 = r_1, \ldots, n_1 \\ \vdots \\ k_q = r_q, \ldots, n_q \\ k_1 - r_1 + \cdots + k_q - r_q \leq m}} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1, \ldots, k_q)} \\ = &\sum_{\substack{k_1 = r_1, \ldots, n_1 \\ \vdots \\ k_q = r_q, \ldots, n_q \\ k_1 - r_1 + \cdots + k_q - r_q \leq m}} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} \binom{c_1}{k_1} \cdots \binom{c_q}{k_q} \end{aligned}$$

$$= \sum_{\substack{k_1=r_1,\dots,c_1 \\ \vdots \\ k_q=r_q,\dots,c_q \\ k_1-r_1+\cdots+k_q-r_q\le m}} (-1)^{k_1-r_1+\cdots+k_q-r_q}\binom{k_1}{r_1}\cdots\binom{k_q}{r_q}\binom{c_1}{k_1}\cdots\binom{c_q}{k_q}.$$

If there exists i such that $r_i > c_i$, then the previous sum is zero. In the other case, since for all $0 \le r \le k \le c$, $\binom{k}{r}\binom{c}{k} = \binom{c}{r}\binom{c-r}{l}$ for $l = k-r$, the previous sum is equal to

$$\binom{c_1}{r_1}\cdots\binom{c_q}{r_q}\sum_{\substack{l_1=0,\dots,c_1-r_1 \\ \vdots \\ l_q=0,\dots,c_q-r_q \\ l_1+\cdots+l_q\le m}} (-1)^{l_1+\cdots+l_q}\binom{c_1-r_1}{l_1}\cdots\binom{c_q-r_q}{l_q}.$$

So we have to prove that for all $d = (d_1,\dots,d_q) \in \mathbb{N}^q\backslash\{0\}$ and for all $m \in \mathbb{N}$,

$$Z(m,d) := (-1)^m \sum_{\substack{l_1=0,\dots,d_1 \\ \vdots \\ l_q=0,\dots,d_q \\ l_1+\cdots+l_q\le m}} (-1)^{l_1+\cdots+l_q}\binom{d_1}{l_1}\cdots\binom{d_q}{l_q}$$

is non negative. Let us prove it by induction over $d_1+\cdots+d_q \ge 1$.

If $d_1+\cdots+d_q = 1$, then

$$Z(m,d) = \begin{cases} 1 & \text{if } m = 0, \\ 0 & \text{if } m > 0, \end{cases}$$

so the result holds.

Suppose the result to be proved to the rank $d_1+\cdots+d_q-1 \ge 1$. First note that if $m = 0$, then $Z(m,d) = 1$, so the result holds. So let us suppose that $m \ge 1$. Since $d_1+\cdots+d_q \ge 2$, there exists i_0 such that $d_{i_0} \ne 0$. One can suppose that $i_0 = q$. Using $\binom{d_q}{l_q} = \binom{d_q-1}{l_q} + \binom{d_q-1}{l_q-1}$, one has

$$Z(m,d) = (-1)^m \sum_{\substack{l_1=0,\dots,d_1 \\ \vdots \\ l_q=0,\dots,d_q \\ l_1+\cdots+l_q\le m}} (-1)^{l_1+\cdots+l_q}\binom{d_1}{l_1}\cdots\binom{d_{q-1}}{l_{q-1}}\left[\binom{d_q-1}{l_q}+\binom{d_q-1}{l_q-1}\right]$$

$$= (-1)^m \sum_{\substack{l_1=0,\dots,d_1 \\ \vdots \\ l_{q-1}=0,\dots,d_{q-1} \\ l_q=0,\dots,d_q-1 \\ l_1+\cdots+l_q\le m}} (-1)^{l_1+\cdots+l_q}\binom{d_1}{l_1}\cdots\binom{d_{q-1}}{l_{q-1}}\binom{d_q-1}{l_q}$$

$$+(-1)^{m-1} \sum_{\substack{l_1=0,\dots,d_1 \\ \vdots \\ l_{q-1}=0,\dots,d_{q-1} \\ l_q=0,\dots,d_q-1 \\ l_1+\cdots+l_q\le m-1}} (-1)^{l_1+\cdots+l_q}\binom{d_1}{l_1}\cdots\binom{d_{q-1}}{l_{q-1}}\binom{d_q-1}{l_q}$$

$$= Z(m,(d_1,\dots,d_{q-1},d_q-1)) + Z(m-1,(d_1,\dots,d_{q-1},d_q-1)) \geq 0,$$

which closes the proof of the induction, and of the corollary. □

Remark 1.4. *We use the same notations as in the previous corollary. One can easily prove, using theorem 1.2, that for all $r=(r_1,\dots,r_q)\in\mathbb{N}^q$, one has*

$$S_{(r_1,\dots,r_q)} = \sum_{k_1=r_1}^{|I_1|} \cdots \sum_{k_q=r_q}^{|I_q|} \binom{k_1}{r_1}\cdots\binom{k_q}{r_q} P(C_1=k_1,\dots,C_q=k_q). \tag{3}$$

1.2. **Number of cycles of a given length of random permutations.** The main results of section 1 are the following ones. Both of them play a key roll in a forthcoming paper ([BG]).

Theorem 1.5. *Consider a family of positive integers $q, l_1<\cdots<l_q$ and $\mu_1,\dots,\mu_q$ probability measures on the set of nonnegative integers. Let, for for each n in a certain infinite set of positive integers, σ_n be a random element of $\mathfrak{S}_n$ such that the law of σ_n is invariant under conjugation by any element of $\mathfrak{S}_n$. Suppose that for all $k=(k_1,\dots,k_q)\in\mathbb{N}^q$, denoting $k_1l_1+\cdots+k_ql_q$ by p, for all $\sigma\in\mathfrak{S}_p$ which has k_1 cycles of length l_1, …, k_q cycles of length l_q, the sequence*

$$\frac{n^p}{l_1^{k_1}\cdots l_q^{k_q}k_1!\cdots k_q!} P(\{\forall i=1,\dots,p, \sigma_n(i)=\sigma(i)\})$$

converges, as n goes to infinity, to a limit denoted by S_k such that for all $r_1,\dots,r_q\geq 0$, the series

$$\sum_{k_1\geq r_1} \cdots \sum_{k_q\geq r_q} (-1)^{k_1-r_1+\cdots+k_q-r_q} \binom{k_1}{r_1}\cdots\binom{k_q}{r_q} S_{(k_1,\dots,k_q)} \tag{4}$$

converges to

$$\prod_{1\leq i\leq q} \mu_i(r_i). \tag{5}$$

Then the law of $(N_{l_1}(\sigma_n),\dots,N_{l_q}(\sigma_n))$ converges, as n goes to infinity, to $\mu_1\otimes\cdots\otimes\mu_q$.

Remark 1.6. *Note that the series of (4) are not asked to converge absolutely. We only ask the sequence*

$$\sum_{\substack{k_1\geq r_1\\ \vdots \\ k_q\geq r_q \\ k_1-r_1+\cdots+k_q-r_q\leq n}} (-1)^{k_1-r_1+\cdots+k_q-r_q} \binom{k_1}{r_1}\cdots\binom{k_q}{r_q} S_{(k_1,\dots,k_q)},$$

to have a the limit of (5) as n goes to infinity.

Before the proof of the theorem, let us give its main corollary:

Corollary 1.7. *Let A be a set of positive integers and let, for each n in a certain infinite set of positive integers, σ_n be a random element of $\mathfrak{S}_n$ such that the law of σ_n is invariant under conjugation by any element of $\mathfrak{S}_n$. Suppose that for all $p\geq 1$, for all $\sigma\in\mathfrak{S}_p^{(A)}$, the probability of the event*

$$\{\forall m=1,\dots,p, \sigma_n(m)=\sigma(m)\}$$

is equivalent to n^{-p} as n goes to infinity. Then for all finite subset K of A, the law of $(N_l(\sigma_n))_{l\in K}$ converges, as n goes to infinity, to $\bigotimes_{l\in K}\mathrm{Poiss}(1/l)$.

Proof of the corollary. The proof is immediate, since clearly, if one fixes a finite family $l_1 < \cdots < l_q$ of elements of A, then theorem 1.5 can be applied with $\mu_1 = \text{Poiss}(1/l_1), \ldots,$ $\mu_q = \text{Poiss}(1/l_q)$ and with the S_k's given by

$$\forall k_1, \ldots, k_q, \quad S_{(k_1,\ldots,k_q)} = \frac{1}{l_1^{k_1} \cdots l_q^{k_q} k_1! \cdots k_q!}.$$

□

Remark 1.8. *It would be interesting to know if the inverse implication is true, at least when A is the set of all positive integers: with the same hypothesis of invariance of the distribution of σ_n under conjugation, let us suppose that for all $q \geq 1$, the law of $(N_1(\sigma_n), \ldots, N_q(\sigma_n))$ converges, as n goes to infinity, to $\bigotimes_{1 \leq l \leq q} \text{Poiss}(1/l)$. Is that true that for all $p \geq 1$, for all $\sigma \in \mathfrak{S}_p$, the probability of the event*

$$\{\forall m = 1, \ldots, p, \sigma_n(m) = \sigma(m)\}$$

is equivalent to n^{-p} as n goes to infinity ? The main difficulty, to prove it, is the fact that no alternating inequality seems to hold in (3). Such a result would be useful to prove the reciprocal implications of certain results proved in this paper.

Proof of theorem 1.5. Before the beginning of the proof, let us introduce a few notations. Let, for all n and for all $c \in \mathfrak{S}_n$ cycle, $E_c(n)$ be the event "c appears in the cycle decomposition of σ_n". Let, for all $l, n \geq 1$, $\mathfrak{C}_l(n)$ be the set of cycles of $\mathfrak{S}_n$ with length l.

Step I. In order to prove the theorem, we fix a family of non negative integers $(r_1, \ldots, r_q)$, and we prove that the probability of the event

$$\{\forall i = 1, \ldots, q, N_{l_i}(\sigma_n) = r_i\}$$

converges, as n goes to infinity, to

$$\prod_{1 \leq i \leq q} \mu_i(r_i),$$

i.e. to

$$\sum_{k_1 \geq r_1} \cdots \sum_{k_q \geq r_q} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1,\ldots,k_q)}. \tag{6}$$

With the notations introduced above, we have to prove that the probability of the event

$$\{\forall i = 1, \ldots, q, \text{ exactly } r_i \text{ of the events of the family } (E_c(n))_{c \in \mathfrak{C}_{l_i}(n)} \text{ occur}\} \tag{7}$$

converges, as n goes to infinity, to (6).

By (1), for all n, the probability of the event of (7) is

$$\sum_{k_1 = r_1, \ldots, |\mathfrak{C}_{l_1}(n)|} \cdots \sum_{k_q = r_q, \ldots, |\mathfrak{C}_{l_q}(n)|} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1,\ldots,k_q)}(n), \tag{8}$$

where we have defined $S_0(n) = 1$ and for all $k = (k_1, \ldots, k_q) \in \mathbb{N}^q \backslash \{0\}$,

$$S_k(n) := \sum P(\bigcap_{i \in [q]} \bigcap_{c \in J_i} E_c(n)), \tag{9}$$

the sum being taken on all families $(J_i)_{i \in [q]}$ such that for all i, $J_i \subset \mathfrak{C}_{l_i}(n)$ and $|J_i| = k_i$.

Step II. Let us fix $k = (k_1, \ldots, k_q) \in \mathbb{N}^q \backslash \{0\}$ and compute $\lim_{n \to \infty} S_k(n)$. Define $p = k_1 \cdot l_1 + \cdots + k_q \cdot l_q$ and consider $\sigma \in S_p$ such that the decomposition in cycles of σ contains k_1 cycles of

length l_1, k_2 cycles of length l_2, ..., k_q cycles of length l_q. Then the invariance by conjugation of the law of σ_n allows us to claim that $S_k(n)$ is equal to the probability of the event

$$\{\forall i = 1, \dots, p, \sigma_n(i) = \sigma(i)\}$$

times the number of subsets J of $\mathfrak{S}_n$ which consist exactly in k_1 cycles of length l_1, k_2 cycles of length l_2, ..., k_q cycles of length l_q such that these cycles are pairwise disjoint. Such a subset J is defined by a set of pairwise disjoint subsets of $[n]$ in which there are exactly k_1 subsets of cardinality l_1, k_2 subsets of cardinality l_2, ..., k_q subsets of cardinality l_q, and by the choice of a cycle build in every of these subsets. Hence there are exactly

$$\underbrace{\frac{n!}{(n-p)!l_1!^{k_1}l_2!^{k_2}\cdots l_q!^{k_q}}\frac{1}{k_1!k_2!\cdots k_q!}}_{\text{counting the sets of pairwise disjoint subsets of } [n]}\ \underbrace{(l_1-1)!^{k_1}(l_2-1)!^{k_2}(l_3-1)!^{k_3}\cdots(l_q-1)!^{k_q}}_{\text{choice of the cycles}}$$

such subsets J. So

$$S_k(n) = \frac{n!}{(n-p)!l_1^{k_1}l_2^{k_2}\dots l_q^{k_q}}\frac{1}{k_1!k_2!\cdots k_q!}P(\{\forall i = 1, \dots, p, \sigma_n(i) = \sigma(i)\}).$$

Hence by hypothesis,

$$\lim_{n\to\infty} S_k(n) = S_{(k_1,\dots,k_q)}.$$

Step III. Now, let us prove that the probability of the event of (7) converges to (6). Fix $\varepsilon > 0$. Choose $m_0 \geq 0$ such that for all $m \geq m_0$, the absolute value of

$$\sum_{\substack{k_1\geq r_1\\ \vdots\\ k_q\geq r_q\\ k_1-r_1+\cdots+k_q-r_q>m}} (-1)^{k_1-r_1+\cdots+k_q-r_q}\binom{k_1}{r_1}\cdots\binom{k_q}{r_q}S_{(k_1,\dots,k_q)},$$

is less than $\varepsilon/2$.

By (2) for all $m, m' \geq m_0$ such that m is odd and m' is even, the probability of the event of (7) is minored by

$$\sum_{\substack{k_1=r_1,\dots,|C_1(n)|\\ \vdots\\ k_q=r_q,\dots,|C_q(n)|\\ k_1-r_1+\cdots+k_q-r_q\leq m}} (-1)^{r_1+k_1+\cdots+r_q+k_q}\binom{k_1}{r_1}\cdots\binom{k_q}{r_q}S_{(k_1,\dots,k_q)}(n)$$

and majored by

$$\sum_{\substack{k_1=r_1,\dots,|C_1(n)|\\ \vdots\\ k_q=r_q,\dots,|C_q(n)|\\ k_1-r_1+\cdots+k_q-r_q\leq m'}} (-1)^{k_1-r_1+\cdots+k_q-r_q}\binom{k_1}{r_1}\cdots\binom{k_q}{r_q}S_{(k_1,\dots,k_q)}(n).$$

Hence for n large enough, the probability of the event of (7) is minored by

$$-\varepsilon/2 + \sum_{\substack{k_1\geq r_1\\ \vdots\\ k_q\geq r_q\\ k_1-r_1+\cdots+k_q-r_q\leq m}} (-1)^{k_1-r_1+\cdots+k_q-r_q}\binom{k_1}{r_1}\cdots\binom{k_q}{r_q}S_{(k_1,\ldots,k_q)}$$

and majored by

$$\varepsilon/2 + \sum_{\substack{k_1\geq r_1\\ \vdots\\ k_q\geq r_q\\ k_1-r_1+\cdots+k_q-r_q\leq m'}} (-1)^{k_1-r_1+\cdots+k_q-r_q}\binom{k_1}{r_1}\cdots\binom{k_q}{r_q}S_{(k_1,\ldots,k_q)},$$

hence is ε-closed to the sum of (6). It closes the proof of the theorem. □

2. Cycles of random permutations with restricted cycle lengths

First of all, let us recall that for n large enough, $\mathfrak{S}_n^{(A)}$ is non empty if and only if n is divided by the greatest common divisor of A (lemma 2.3 of [Ne07] for example).

2.1. Case where A is infinite.

Let us first give a lemma, which is a particular case of proposition 3.10 of [Ne07].

Lemma 2.1. *Suppose that A is a set of positive integers which satisfies $\sum_{\substack{j\geq 1\\ j\notin A}}\frac{1}{j}<\infty$. Consider $p\geq 1$ and an oriented graph Γ with vertex set $[p]$, which is a disjoint union of loops with length in A (i.e. of graphs of the type $v_1\to\cdots\to v_l\to v_1$, with $v_1,\ldots,v_l$ pairwise distinct and $l\in A$). Then as n goes to infinity in such a way that $\mathfrak{S}_n^{(A)}\neq\emptyset$, the probability that a uniform random permutation σ_n of $\mathfrak{S}_n^{(A)}$ satisfies*

$$\forall e \text{ edge of } \Gamma,\ \sigma_n(\text{beginning of } e) = \text{end of } e$$

is equivalent to n^{-p}.

The following proposition is the analogous of the result stated in the beginning of the introduction, in the case where the random permutation we consider is not anymore distributed uniformly on the symmetric group but on the set of permutations with cycle lengths in A (indeed, in this case, for all $k\notin A$, $N_k(\sigma_n)=0$).

Proposition 2.2. *Suppose that A is an infinite set of positive integers such that $\sum_{\substack{j\geq 1\\ j\notin A}}\frac{1}{j}<\infty$. We consider, for all n such that $\mathfrak{S}_n^{(A)}$ is non empty, a random permutation σ_n which has uniform distribution on $\mathfrak{S}_n^{(A)}$. Then for all $l\geq 1$, the distribution of the random vector*

$$(N_k(\sigma_n))_{1\leq k\leq l, k\in A}$$

converges weakly, as n goes to infinity in such a way that $\mathfrak{S}_n^{(A)}$ is non empty, to

$$\bigotimes_{1\leq k\leq l, k\in A}\mathrm{Poiss}(1/k).$$

Note also that this result implies that even for large values of n, every $N_l(\sigma_n)$ takes large values with a very small probability.

Proof. By corollary 1.7, it suffices to prove that for all $p \geq 1$, for all $\sigma \in \mathfrak{S}_p^{(A)}$, the probability of the event $\{\forall m = 1, \ldots, p, \sigma_n(m) = \sigma(m)\}$ is equivalent to n^{-p} as n goes to infinity, which follows directly from the application of lemma 2.1 to the graph Γ defined to be the union of the loops defined by the cycles of σ. □

2.2. **Case where A is finite.** We are going to prove the following result:

Theorem 2.3. *Suppose that A is a finite set of positive integers, and denote its maximum by d. We consider, for all n such that $\mathfrak{S}_n^{(A)}$ is non empty, a random permutation σ_n which has uniform distribution on $\mathfrak{S}_n^{(A)}$. Then for all $l \in A$, as n goes to infinity in such a way that $\mathfrak{S}_n^{(A)}$ is non empty, $\frac{N_l(\sigma_n)}{n^{l/d}}$ converges in all L^p spaces ($p \in [1, +\infty)$) to $1/l$.*

Note that it implies that for all $l \in A$, the distribution of $\frac{N_l(\sigma_n)}{n^{l/d}}$ converges weakly to the Dirac mass at $1/l$. Since constant random variables are always independent, this result also contains the asymptotic independence of the family $\left(\frac{N_l(\sigma_n)}{n^{l/d}}\right)_{l \in A}$.

To prove this theorem, we shall need the following lemmas. The first one is well known (see, for instance, Theorem 3.53 of [B04]). The second one is lemma 3.6 of [Ne07].

Lemma 2.4. *Let p be the greatest common divisor of A. Then for all complex number z, one has*

$$\sum_{n \geq 0} \frac{\left|\mathfrak{S}_{pn}^{(A)}\right|}{(pn)!} z^{pn} = \exp\left(\sum_{k \in A} \frac{z^k}{k}\right).$$

Lemma 2.5. *Let B be a finite set of positive integers. Let $(c_j)_{j \in B}$ be a finite family of positive numbers. Let $\sum_{n \geq 1} b_n w^n$ be the power expansion of $\exp\left(\sum_{j \in B} c_j w^j\right)$. Suppose that $b_n > 0$ for sufficiently large n. Then as n goes to infinity,*

$$\frac{b_{n-1}}{b_n} \sim \left(\frac{n}{bc_b}\right)^{1/b},$$

with $b = \max B$.

Proof of the theorem. First note that by Hölder formula, it suffices to prove that for all p positive integer, the expectation of the $2p$-th power of

$$\frac{N_l(\sigma_n)}{n^{l/d}} - \frac{1}{l}$$

tends to zero as n goes to infinity. Hence by the binomial identity, it suffices to prove that for all $l \in A$, for all $m \geq 1$, the expectation of the m-th power of $N_l(\sigma_n)$ is equivalent to $n^{ml/d}/l^m$ as n goes to infinity in such a way that $\mathfrak{S}_n^{(A)}$ is non empty.

So let us fix $l \in A$ and $m \geq 1$. We know that

$$N_l(\sigma_n) = \frac{1}{l} \sum_{k=1}^{n} 1_{\{k \text{ belongs to a cycle of length } l\}}.$$

Hence

$$\mathbb{E}[N_l(\sigma_n)^m] = \frac{1}{l^m} \sum_{\substack{m_1,\dots,m_n \geq 0 \\ m_1+\cdots+m_n=m}} \binom{m}{m_1,\dots,m_n} \mathbb{E}\left[\prod_{k=1}^{n} (1_{\{k \text{ belongs to a cycle of length } l\}})^{m_k}\right]$$

But the distribution of σ_n is invariant by conjugation, so for all $m_1, \dots, m_n \geq 0$,

$$\mathbb{E}\left[\prod_{k=1}^{n} (1_{\{k \text{ belongs to a cycle of length } l\}})^{m_k}\right]$$

depends only on the number j of k's such that $m_k \neq 0$. So

$$\begin{aligned}
\mathbb{E}[N_l(\sigma_n)^m] &= \frac{1}{l^m} \sum_{j=1}^{m} \sum_{\substack{m_1,\dots,m_n \geq 0 \\ |\{k \in [n]\,;\, m_k \neq 0\}|=j \\ m_1+\cdots+m_n=m}} \binom{m}{m_1,\dots,m_n} P\left(1,\dots,j \text{ belong to cycles of length } l\right) \\
&= \frac{1}{l^m} \sum_{j=1}^{m} \left[\binom{n}{j} P\left(1,\dots,j \text{ belong to cycles of length } l\right) \sum_{\substack{m_1,\dots,m_j \geq 1 \\ m_1+\dots+m_j=m}} \binom{m}{m_1,\dots,m_j} \right]. \qquad (10)
\end{aligned}$$

Now, let us compute, for $j \geq 1$, an equivalent of $P\left(1,\dots,j \text{ belong to cycles of length } l\right)$. Let us denote by $\mathrm{P}(j)$ the set of partitions of $[j]$. We have

$$\begin{aligned}
&P\left(1,\dots,j \text{ belong to cycles of length } l\right) \\
&= \sum_{\pi \in \mathrm{P}(j)} P(1,\dots,j \text{ are in cycles of length } l \\
&\text{and } \forall i,i' \in [j],\ [i,i' \text{ belong to the same cycle}] \Leftrightarrow [i = i' \mod \pi]) \\
&= \sum_{\substack{\pi \in \mathrm{P}(j) \\ \pi = \{V_1,\dots,V_{|\pi|}\}}} \binom{n-j}{l-|V_1|,\dots,l-|V_{|\pi|}|,n-l|\pi|} ((l-1)!)^{|\pi|} \frac{\left|\mathfrak{S}_{n-l|\pi|}^{(A)}\right|}{\left|\mathfrak{S}_n^{(A)}\right|} \\
&= \sum_{\pi \in \mathrm{P}(j)} \frac{1}{n(n-1)\cdots(n-j+1)} \frac{\left|\mathfrak{S}_{n-l|\pi|}^{(A)}\right| / (n-l|\pi|)!}{\left|\mathfrak{S}_n^{(A)}\right| / n!} \prod_{V \in \pi} \frac{(l-1)!}{(l-|V|)!}. \qquad (11)
\end{aligned}$$

Let p be the greatest common divisor of A. We know that for all positive integer n,

$$\mathfrak{S}_n^{(A)} \neq \emptyset \Longrightarrow p | n,$$

and that for sufficiently large n, the inverse implication is also true (lemma 2.3 of [Ne07]). Hence by lemma 2.4, for $z \in \mathbb{C}$, one has

$$\sum_{n \geq 0} \frac{\left|\mathfrak{S}_{pn}^{(A)}\right|}{(pn)!} (z^p)^n = \exp\left(\sum_{j \in \frac{1}{p}.A} \frac{(z^p)^j}{pj} \right).$$

Hence for $w \in \mathbb{C}$, one has

$$\sum_{n \geq 0} \frac{\left|\mathfrak{S}_{pn}^{(A)}\right|}{(pn)!} w^n = \exp\left(\sum_{j \in \frac{1}{p}.A} \frac{w^j}{pj} \right).$$

So by lemma 2.5, as n goes to infinity,

$$\frac{\left|\mathfrak{S}_{pn-p}^{(A)}\right|/(pn-p)!}{\left|\mathfrak{S}_{pn}^{(A)}\right|/(pn)!} \sim \left(\frac{n}{(d/p)1/d}\right)^{p/d} = (pn)^{p/d}.$$

Hence by induction on k positive integer divided by p, one can easily prove that, as n goes to infinity in such a way that p divides n,

$$\frac{\left|\mathfrak{S}_{n-k}^{(A)}\right|/(n-k)!}{\left|\mathfrak{S}_{n}^{(A)}\right|/(n)!} \sim n^{k/d}.$$

Hence in (11), for each partition π, the corresponding term is equivalent to

$$n^{l|\pi|/d-j} \prod_{V\in\pi} \frac{(l-1)!}{(l-|V|)!},$$

thus in (11), the leading term is the one of the singletons partition, and

$$P\,(1,\ldots,j \text{ belong to cycles of length } l) \sim n^{(l/d-1)j}. \tag{12}$$

Mixing (10) and (12), one gets $\mathbb{E}[N_l(\sigma_n)^m] \sim \dfrac{n^{lm/d}}{l^m}$, which closes the proof of the theorem. □

References

[ABT05] Arratia, Richard; Barbour, A. D.; Tavaré, Simon *Logarithmic combinatorial structures: a probabilistic approach* EMS Monographs in Mathematics. European Mathematical Society (EMS), Zürich, 2003.

[BG] Benaych-Georges, Florent *Cycles of free words in several random permutations with restricted cycles lengths.* Submitted, available on http://www.proba.jussieu.fr/∼benaych/

[B01] Bollobás, B. *Random Graphs*, second edition. 2001.

[B04] Bóna, M. *Combinatorics of permutations*, Chapman & Hall/CRC, Boca Raton, FL, 2004

[Ne07] Neagu, M. *Asymptotic freeness of random permutation matrices with restricted cycles lengths.* arxiv, to appear in Indiana University Math. Journal

Florent Benaych-Georges, LPMA, Université Paris VI, Case courier 188, 4, Place Jussieu, 75252 Paris Cedex 05, France

E-mail address: florent.benaych@gmail.com