



**HAL**  
open science

# Cycles of random permutations with restricted cycle lengths

Florent Benaych-Georges

► **To cite this version:**

Florent Benaych-Georges. Cycles of random permutations with restricted cycle lengths. 2007. hal-00196123v5

**HAL Id: hal-00196123**

**<https://hal.science/hal-00196123v5>**

Preprint submitted on 18 Jun 2008 (v5), last revised 16 Jan 2009 (v6)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# 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 whose distribution is invariant under conjugation. These results were first established to be applied in a forthcoming paper ([BG]), where 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 the permutations of  $\{1, \dots, n\}$  which have all their cycle lengths in  $A$ , and then let  $n$  tend to infinity. Improving slightly a recent result of Yakymiv ([Y07]), we prove that under a general hypothesis on  $A$ , the numbers of cycles with different fixed 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  $n$ ,  $\sigma_n$  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  $\sigma_n$  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

$$\text{Pois}(1/1) \otimes \text{Pois}(1/2) \otimes \dots \otimes \text{Pois}(1/l),$$

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

The proof of this result is rather simple (see, e.g. [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 "small cycles", i.e. 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 distributed according to measures which are invariant under conjugation (Theorem 1.5). This result will play a key roll in a forthcoming paper ([BG]) where we prove results about cycles of random permutations which can be written as free words in several independent random permutations with

---

*Date:* June 18, 2008.

*MSC 2000 subject classifications.* primary 20B30, 60B15, secondary 60C05.

*Key words.* Random permutations, cycles of random permutations, random permutations with restricted cycle lengths.

restricted cycle length. More precisely, in [BG], Corollary 2.19 (thus also, indirectly, Theorems 3.5 and 3.6) and Theorem 3.10 are consequences of Theorem 1.5 of the present paper (or of its Corollary 1.7).

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  $\sigma_n$  chosen uniformly in  $\mathfrak{S}_n^{(A)}$ .

We first prove, as an application of our general result mentioned above, that under certain hypothesis on an infinite set  $A$ , 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  $l \notin A$ ,  $N_l(\sigma_n)$  is almost surely null): for all  $l \geq 1$ , the distribution of the random vector

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

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

$$(2) \quad \bigotimes_{1 \leq k \leq l, k \in A} \text{Pois}(1/k).$$

Here, we shall mention that as the author published this work on arxiv, it was pointed out to him that proving this result under some slightly stronger hypothesis was exactly the purpose of a very recent paper ([Y07]). However, the method used in this article is different from the one we use here: it relies on an identity in law between the random vector of (1) and a vector with law (2) conditioned to belong to a certain set and on some estimations provided by asymptotic behavior of generating functions. It is the approach of analytic combinatorics, which provides a powerful machinery for the analysis of random combinatorial objects. The book [FS08] offers synthetic presentation of these tools. It is possible that the result presented in this paragraph can be deduced from chapter IX of this book, but our proof is very short, and the object of the present paper is overall to prove the general result presented above about random permutations which distributions are invariant under conjugation.

Note that the result presented in the previous paragraph implies that the number of cycles of any given length "stays finite" even though  $n$  goes to infinity, i.e. takes large values with a very small probability. 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  $\sigma_n$  of random permutations to have the weak convergence of the distribution of  $(N_1(\sigma_n), \dots, N_l(\sigma_n))$  to  $\text{Pois}(1/1) \otimes \text{Pois}(1/2) \otimes \dots \otimes \text{Pois}(1/l)$  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. It seems possible that analytic combinatorics, as presented in [FS08], will show a way to answer this question.

**0.3. Notation.** In this text, for  $n$  an 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  $[n]$  all of whose 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  $\sigma$  as a product of cycles with disjoint supports. For  $\lambda > 0$ ,  $\text{Poiss}(\lambda)$  will denote the Poisson distribution with parameter  $\lambda$ .  $\mathbb{N}$  will denote the set of non negative integers.

**Acknowledgments.** The author would like to thank Professor Vatutin for having mentioned to him the works of Yakymiv and Pavlov, and Professor Yakymiv for his support and some interesting remarks about a draft of this work.

## 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

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

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*

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

*for any family  $A_1, \dots, A_N$  of events in any probability space  $(\Omega, \Sigma, \mathbb{P})$ , it suffices to prove it under the additional hypothesis that each of the  $A_i$ 's is either  $\emptyset$  or  $\Omega$ .*

**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 any family  $A_1, \dots, A_N$  of events in a probability space  $(\Omega, \Sigma, \mathbb{P})$ ,

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

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

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

where we choose every  $A_i$  to be either  $\Omega$  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  $(\Omega, \Sigma, \mathbb{P})$ ,  $q \geq 1$ , and for all  $i = 1, \dots, q$ ,  $(A_{i,j})_{j \in I_i}$  a finite family of events. Let us define the random vector  $C = (C_1, \dots, C_q)$  by, 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  $k = (k_1, \dots, k_q) \in \mathbb{N}^q \setminus \{0\}$ ,

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

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

$$(3) \quad \mathbb{P}(C = r) = \sum_{k_1=r_1}^{|I_1|} \cdots \sum_{k_q=r_q}^{|I_q|} (-1)^{k_1-r_1+\dots+k_q-r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1, \dots, k_q)}.$$

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

$$(4) \quad \mathbb{P}(C = r) \geq \sum_{\substack{k_1=r_1, \dots, |I_1| \\ \vdots \\ k_q=r_q, \dots, |I_q| \\ k_1-r_1+\dots+k_q-r_q \leq m}} (-1)^{k_1-r_1+\dots+k_q-r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1, \dots, k_q)} \quad (\text{resp. } \leq).$$

**Proof.** First note that the alternating inequalities, used for  $m$  large enough, imply (3). So we are only going to prove the alternating inequalities.

Then, let us suppose that for all  $i = 1, \dots, q$ ,  $I_i = [n_i]$ , with  $n_i \geq 1$ . As an application of the previous theorem, one can suppose every  $A_{i,j}$  to be either  $\emptyset$  or  $\Omega$ . In this case, for all  $i = 1, \dots, q$ , 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  $k = (k_1, \dots, k_q) \in \mathbb{N}^q$ ,

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

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

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

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

Now consider  $(r_1, \dots, r_q) \neq (c_1, \dots, c_q)$ . Then  $\mathbb{P}(C = r) = 0$  and we have to prove that the right-hand-side term in equation (4) is either non negative or non positive according to  $m$  is even or odd. For all  $m \geq 0$ ,

$$\begin{aligned}
& \sum_{\substack{k_1=r_1, \dots, n_1 \\ \vdots \\ k_q=r_q, \dots, n_q \\ k_1-r_1+\dots+k_q-r_q \leq m}} (-1)^{k_1-r_1+\dots+k_q-r_q} \binom{k_1}{r_1} \dots \binom{k_q}{r_q} \mathcal{S}_{(k_1, \dots, k_q)} \\
&= \sum_{\substack{k_1=r_1, \dots, n_1 \\ \vdots \\ k_q=r_q, \dots, n_q \\ k_1-r_1+\dots+k_q-r_q \leq m}} (-1)^{k_1-r_1+\dots+k_q-r_q} \binom{k_1}{r_1} \dots \binom{k_q}{r_q} \binom{c_1}{k_1} \dots \binom{c_q}{k_q} \\
&= \sum_{\substack{k_1=r_1, \dots, c_1 \\ \vdots \\ k_q=r_q, \dots, c_q \\ k_1-r_1+\dots+k_q-r_q \leq m}} (-1)^{k_1-r_1+\dots+k_q-r_q} \binom{k_1}{r_1} \dots \binom{k_q}{r_q} \binom{c_1}{k_1} \dots \binom{c_q}{k_q}.
\end{aligned}$$

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

$$\begin{aligned}
& \binom{c_1}{r_1} \dots \binom{c_q}{r_q} \sum_{\substack{l_1=0, \dots, c_1-r_1 \\ \vdots \\ l_q=0, \dots, c_q-r_q \\ l_1+\dots+l_q \leq m}} (-1)^{l_1+\dots+l_q} \binom{c_1-r_1}{l_1} \dots \binom{c_q-r_q}{l_q}.
\end{aligned}$$

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

$$\begin{aligned}
Z(m, d) &:= (-1)^m \sum_{\substack{l_1=0, \dots, d_1 \\ \vdots \\ l_q=0, \dots, d_q \\ l_1+\dots+l_q \leq m}} (-1)^{l_1+\dots+l_q} \binom{d_1}{l_1} \dots \binom{d_q}{l_q}
\end{aligned}$$

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

If  $d_1 + \dots + d_q = 1$ , 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  $d_1 + \dots + d_q - 1 \geq 1$ . First note that if  $m = 0$ , then  $Z(m, d) = 1$ , so the result holds. So let us suppose that  $m \geq 1$ . Since  $d_1 + \dots + d_q \geq 2$ , there exists  $i_0$  such that  $d_{i_0} \neq 0$ . 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

$$\begin{aligned}
Z(m, d) &= (-1)^m \sum_{\substack{l_1=0, \dots, d_1 \\ \vdots \\ l_q=0, \dots, d_q \\ l_1+\dots+l_q \leq m}} (-1)^{l_1+\dots+l_q} \binom{d_1}{l_1} \dots \binom{d_{q-1}}{l_{q-1}} \left[ \binom{d_q-1}{l_q} + \binom{d_q-1}{l_q-1} \right] \\
&= (-1)^m \sum_{\substack{l_1=0, \dots, d_1 \\ \vdots \\ l_{q-1}=0, \dots, d_{q-1} \\ l_q=0, \dots, d_q-1 \\ l_1+\dots+l_q \leq m}} (-1)^{l_1+\dots+l_q} \binom{d_1}{l_1} \dots \binom{d_{q-1}}{l_{q-1}} \binom{d_q-1}{l_q} \\
&\quad + (-1)^{m-1} \sum_{\substack{l_1=0, \dots, d_1 \\ \vdots \\ l_{q-1}=0, \dots, d_{q-1} \\ l_q=0, \dots, d_q-1 \\ l_1+\dots+l_q \leq m-1}} (-1)^{l_1+\dots+l_q} \binom{d_1}{l_1} \dots \binom{d_{q-1}}{l_{q-1}} \binom{d_q-1}{l_q} \\
&= Z(m, (d_1, \dots, d_{q-1}, d_q - 1)) + Z(m-1, (d_1, \dots, d_{q-1}, d_q - 1)) \geq 0,
\end{aligned}$$

which closes the proof of the induction, and of the corollary.  $\square$

**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

$$(5) \quad S_{(r_1, \dots, r_q)} = \sum_{k_1=r_1}^{|I_1|} \dots \sum_{k_q=r_q}^{|I_q|} \binom{k_1}{r_1} \dots \binom{k_q}{r_q} \mathbb{P}(C_1 = k_1, \dots, C_q = k_q).$$

**1.2. Number of cycles of a given length of random permutations.** The main results of section 1 are Theorem 1.5 and Corollary 1.7. Both of them play a key roll in a forthcoming paper ([BG]). Recall that for all  $n$  integer, a probability measure  $\mathbb{P}$  on  $\mathfrak{S}_n$  is said to be *invariant under conjugation* if for all  $\sigma, \tau \in \mathfrak{S}_n$ ,  $\mathbb{P}(\{\sigma \circ \tau \circ \sigma^{-1}\}) = \mathbb{P}(\{\tau\})$ .

**Theorem 1.5.** For a positive integer  $q$ , let  $l_1 < \dots < l_q$  be positive integers. Let  $\mu_1, \dots, \mu_q$  be a collection of probability measures on the nonnegative integers. Let, for for each  $n$  in a certain infinite set of positive integers,  $\mathbb{P}_n$  be probability measure on  $\mathfrak{S}_n$  which is invariant under conjugation. Suppose that for all  $k = (k_1, \dots, k_q) \in \mathbb{N}^q$ , denoting  $k_1 l_1 + \dots + k_q l_q$  by  $p$ , for all  $\sigma \in \mathfrak{S}_p$  which has  $k_1$  cycles of length  $l_1, \dots, k_q$  cycles of length  $l_q$ , the sequence

$$\frac{n^p}{l_1^{k_1} \dots l_q^{k_q} k_1! \dots k_q!} \mathbb{P}_n(\{\tau \in \mathfrak{S}_n; \forall i = 1, \dots, p, \tau(i) = \sigma(i)\})$$

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

$$(6) \quad \sum_{k_1 \geq r_1} \dots \sum_{k_q \geq r_q} (-1)^{k_1 - r_1 + \dots + k_q - r_q} \binom{k_1}{r_1} \dots \binom{k_q}{r_q} S_{(k_1, \dots, k_q)}$$

is equal to

$$(7) \quad \prod_{1 \leq i \leq q} \mu_i(r_i).$$

Then if for all  $n$ ,  $\sigma_n$  is a random variable distributed according to  $\mathbb{P}_n$ , the law of  $(N_{l_1}(\sigma_n), \dots, N_{l_q}(\sigma_n))$  converges, as  $n$  goes to infinity, to  $\mu_1 \otimes \dots \otimes \mu_q$ .

**Remark 1.6.** Note that the series of (6) are not asked to converge absolutely. We only ask the sequence

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

to have the limit (7) 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,  $\sigma_n$  be a random element of  $\mathfrak{S}_n$  distributed according to a probability measure which is invariant under conjugation. 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 any finite subset  $K$  of  $A$ , the law of  $(N_l(\sigma_n))_{l \in K}$  converges, as  $n$  goes to infinity, to  $\otimes_{l \in K} \text{Poiss}(1/l)$ .

**Proof of the corollary.** The proof is immediate, since clearly, if one fixes a finite family  $l_1 < \dots < l_q$  of elements of  $A$ , then Theorem 1.5 can be applied with  $\mathbb{P}_n = \text{Law}(\sigma_n)$  for all  $n$ , with  $\mu_1 = \text{Poiss}(1/l_1), \dots, \mu_q = \text{Poiss}(1/l_q)$  and with the  $S_k$ 's given by

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

□

**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  $\sigma_n$  under conjugation, let us suppose that for all  $q \geq 1$ , the law of  $(N_1(\sigma_n), \dots, N_q(\sigma_n))$  converges, as  $n$  goes to infinity, to  $\otimes_{1 \leq l \leq q} \text{Poiss}(1/l)$ . Is it true that for all  $p \geq 1$ , for all  $\sigma \in \mathfrak{S}_p$ , 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? The main difficulty, to prove it, is the fact that no alternating inequality seems to hold in (5). 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 some notation. Let  $\mathfrak{C}_l(n)$  be the set of cycles of  $[n]$  with length  $l$ . Let, for all cycle  $c$  of  $[n]$ ,

$$E_c(n) = \{\sigma \in \mathfrak{S}_n; c \text{ appears in the cycle decomposition of } \sigma\}.$$

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

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



converges, as  $n$  goes to infinity, to

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

i.e. to

$$(8) \quad \sum_{k_1 \geq r_1} \cdots \sum_{k_q \geq r_q} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1, \dots, k_q)}.$$

With the notations introduced above, we have to prove that

$$(9) \quad \mathbb{P}_n(\forall i = 1, \dots, q, \text{ exactly } r_i \text{ of the events of the family } (E_c(n))_{c \in \mathfrak{C}_{i_i}(n)} \text{ occur})$$

converges, as  $n$  goes to infinity, to (8).

By (3), for all  $n$ , the probability of (9) is

$$(10) \quad \sum_{k_1 = r_1, \dots, |\mathfrak{C}_{i_1}(n)|} \cdots \sum_{k_q = r_q, \dots, |\mathfrak{C}_{i_q}(n)|} (-1)^{k_1 - r_1 + \cdots + k_q - r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1, \dots, k_q)}(n),$$

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

$$(11) \quad S_k(n) := \sum_{i \in [q]} \mathbb{P}_n(\bigcap_{c \in J_i} E_c(n)),$$

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

*Step II.* Let us fix  $k = (k_1, \dots, k_q) \in \mathbb{N}^q \setminus \{0\}$  and compute  $\lim_{n \rightarrow \infty} S_k(n)$ . 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  $\sigma$  contains  $k_1$  cycles of length  $l_1$ ,  $k_2$  cycles of length  $l_2$ ,  $\dots$ ,  $k_q$  cycles of length  $l_q$ . Then the invariance of  $\mathbb{P}_n$  by conjugation allows us to claim that  $S_k(n)$  is equal to

$$\mathbb{P}_n(\{\sigma \in \mathfrak{S}_n; \forall i = 1, \dots, p, \sigma_n(i) = \sigma(i)\})$$

times the number of sets  $J$  of cycles of  $[n]$  which consist exactly in  $k_1$  cycles of length  $l_1$ ,  $k_2$  cycles of length  $l_2$ ,  $\dots$ ,  $k_q$  cycles of length  $l_q$  such that these cycles are pairwise disjoint. Such a set  $J$  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  $l_2$ ,  $\dots$ ,  $k_q$  subsets of cardinality  $l_q$ , and for every of these subsets, by the choice of a cycle having the subset for support. Hence there are exactly

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

such sets  $J$ . So

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

Hence by hypothesis,

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

*Step III.* Now, let us prove that the probability of the event of (9) converges to (8). Fix  $\varepsilon > 0$ . Choose  $m_0 \geq 0$  such that for all  $m \geq m_0$ , the absolute value of

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

is less than  $\varepsilon/2$ .

By (4) for all  $m, m' \geq m_0$  such that  $m$  is odd and  $m'$  is even, the probability of the event of (9) is minored by

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

and majored by

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

Hence for  $n$  large enough, the probability of the event of (9) is minored by

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

and majored by

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

hence is  $\varepsilon$ -close to the sum of (8). It closes the proof of the theorem.  $\square$

## 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  $A$  (see Lemma 2.3 of [Ne07] for example).

**2.1. Case where  $A$  is infinite.** The following proposition is the analog 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  $k \notin A$ ,  $N_k(\sigma_n)$  is almost surely null).

**Proposition 2.1.** *Suppose that  $A$  is a set of positive integers such that if one denotes by  $q$  the greatest common divisor of  $A$  and by  $u_n$  the quotient  $|\mathfrak{S}_{qn}^{(A)}|/(qn)!$ , one has*

$$(12) \quad \frac{u_n}{u_{n-1}} \xrightarrow{n \rightarrow \infty} 1.$$

We consider, for  $n$  large enough, a random permutation  $\sigma_n$  which has the uniform distribution on  $\mathfrak{S}_{qn}^{(A)}$ . 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, to

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

Note also that this result implies that for all  $l$ , 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  $\{\forall m = 1, \dots, p, \sigma_n(m) = \sigma(m)\}$  is equivalent to  $n^{-p}$  as  $n$  goes to infinity. This probability is equal to

$$\frac{|\{s \in \mathfrak{S}_{qn}^{(A)}; \forall m = 1, \dots, p, s(m) = \sigma(m)\}|}{|\mathfrak{S}_{qn}^{(A)}|} = \frac{|\mathfrak{S}_{qn-p}^{(A)}|}{|\mathfrak{S}_{qn}^{(A)}|},$$

hence the proposition follows from (12).  $\square$

**Remark 2.2.** 1. *Note that this result improves Theorem 1 of [Y07], which states the same result under the slightly stronger hypothesis that  $(u_n)$  is a sequence with regular variation with exponent in  $(-1, 0]$ . However, the author did not find any example where the hypothesis of this result are satisfied but the hypothesis of Theorem 1 of [Y07] are not. We also didn't find any example where the hypothesis of this result is satisfied but the greatest common divisor of  $A$  is not 1.*

2. *A number of examples of classes of sets  $A$  for which the hypothesis of this proposition holds can be found in the list of examples following Theorem 2 of [Y05a]. It holds for example if  $|A \cap [n]|/n \xrightarrow{n \rightarrow \infty} 1$ . More details are given in Theorem 3.3.1 of the book [Y05b].*

**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  $\sigma_n$  which has the 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*

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

**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. One can suppose that for all such  $n$ , the probability space where  $\sigma_n$  is defined is  $\mathfrak{S}_n^{(A)}$ . Then  $\mathbb{P}_n$  denote the uniform probability measure on  $\mathfrak{S}_n^{(A)}$  and  $\mathbb{E}_n$  denote the expectation with respect to  $\mathbb{P}_n$ .

So let us fix  $l \in A$  and  $m \geq 1$ . Since  $N_l(\sigma_n) = \frac{1}{l} \sum_{k=1}^n 1_{\{k \text{ belongs to a cycle of length } l\}}$ , one has

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

But  $\mathbb{P}_n$  is invariant by conjugation, so for all  $m_1, \dots, m_n \geq 0$ ,

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

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

$$\begin{aligned} \mathbb{E}_n [N_l(\sigma_n)^m] &= \frac{1}{l^m} \sum_{j=1}^m \sum_{\substack{m_1, \dots, m_n \geq 0 \\ |\{k \in [n]; m_k \neq 0\}| = j \\ m_1 + \dots + m_n = m}} \binom{m}{m_1, \dots, m_n} \mathbb{P}_n (1, \dots, j \text{ belong to cycles of length } l) \\ (13) \quad &= \frac{1}{l^m} \sum_{j=1}^m \left[ \binom{n}{j} \mathbb{P}_n (1, \dots, j \text{ belong to cycles of length } l) \sum_{\substack{m_1, \dots, m_j \geq 1 \\ m_1 + \dots + m_j = m}} \binom{m}{m_1, \dots, m_j} \right]. \end{aligned}$$

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

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

Let  $p$  be the greatest common divisor of  $A$ . We know that for all positive integer  $n$ ,  $\mathfrak{S}_n^{(A)} \neq \emptyset \implies p|n$ , 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

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

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

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

So by Lemma 2.5, as  $n$  goes to infinity, one has

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

(note that in the case where the greatest common divisor of  $A$  is 1, this result can be deduced from the main theorem of [P95]). It follows by induction on positive integers  $k$  divisible by  $p$  that, as  $n$  goes to infinity in such a way that  $p$  divides  $n$ ,

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

Hence in (14), for each partition  $\pi$ , the corresponding term is equivalent to

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

thus in (14), the leading term is the one of the singletons partition, and

$$(15) \quad \mathbb{P}_n(1, \dots, j \text{ belong to cycles of length } l) \sim n^{(l/d-1)j}.$$

Combining (13) and (15), one gets  $\mathbb{E}_n[N_l(\sigma_n)^m] \sim \frac{n^{lm/d}}{l^m}$ , which completes the proof of the theorem.  $\square$

## 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
- [FS08] Flajolet, P, Sedgewick, *Analytic combinatorics*, Cambridge University Press, Coming in 2008, now available on the web.
- [Ne07] Neagu, M. *Asymptotic freeness of random permutation matrices with restricted cycles lengths*. Indiana Univ. Math. J. 56 (2007) 2017 - 2049
- [P95] Pavlov, A. I. *On the number of permutations with a finite set of cycle lengths*. (Russian) Trudy Mat. Inst. Steklov. 207 (1994), 256–267; translation in Proc. Steklov Inst. Math. 1995, no. 6 (207), 233–242
- [Y05a] A. L. Yakymiv, *The distribution of lengths of the  $m$ -th maximal cycle in a random  $A$  permutation*. Translated from russian in Discrete Math. Appl. 15 (5), 527-546 (2005).
- [Y05b] A. L. Yakymiv, *Probabilistic applications of Tauberian theorems*. Translated by Andrei V. Kolchin. (English) Modern Probability and Statistics. Leiden: VSP.
- [Y07] A. L. Yakymiv, *Random  $A$ -Permutations: Convergence to a Poisson Process*. Translated from russian in Mathematical Notes, 2007, Vol. 81, No. 6, pp. 840-846.

FLORENT BENAYCH-GEORGES, LPMA, UPMC UNIV PARIS 6, CASE COURIER 188, 4, PLACE JUSSIEU, 75252 PARIS CEDEX 05, FRANCE.

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