Cycles of free words in several independent random permutations

Florent Benaych-Georges

CYCLES OF FREE WORDS IN SEVERAL INDEPENDENT RANDOM PERMUTATIONS

FLORENT BENAYCH-GEORGES

Abstract. In this text, extending results of [Ni94] and [Ne05], we study the asymptotics of the number of cycles of a given length of a word in several independent random permutations with restricted cycle lengths. Specifically, for $A_1, \ldots, A_k$ non empty sets of positive integers and for w word in the letters $g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}$, we consider, for all n such that it is possible, an independent family $s_1(n), \ldots, s_k(n)$ of random permutations chosen uniformly among the permutations of n objects which have all their cycle lengths in respectively $A_1, \ldots, A_k$, and for l positive integer, we are going to give asymptotics (as n goes to infinity) on the number $N_l(n)$ of cycles of length l of the permutation obtained by changing any letter g_i in w by $s_i(n)$. In many cases, we prove that the distribution of $N_l(n)$ converges to a Poisson law with parameter $1/l$ and that the family of random variables $(N_1(n), N_2(n), ...)$ is asymptotically independent. We notice the pretty surprising fact that from this point of view, many things happen like if we considered the number of cycles of given lengths of a single permutation with uniform distribution on the n-th symmetric group.

Contents

Date: November 16, 2006.
MSC 2000 subject classifications. primary 60B15, 20B30, 20P05, secondary 60C05.
Key words. Random permutation, cycle, free group.

1. Introduction

1.1. **General introduction.** In all this text, we shall consider a random element σ_n (whose distribution will be specified) of the group $\mathfrak{S}_n$ of the permutations of $\{1, \ldots, n\}$ and study the law of the family random variables $(N_l(\sigma_n))_{l\geq 1}$, where for all $l \geq 1$, $N_l(\sigma_n)$ is the number of cycles of length l in the decomposition of σ_n as a product of cycles with disjoint supports. It is well known (see, e.g., theorem 1.3 of [ABT05]), that if for all n, σ_n is uniformly distributed on $\mathfrak{S}_n$, then for all $l \geq 1$, the joint distribution of the random vector

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

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. In this paper, we are going to prove that this result (or part of it) stays true for random permutations σ_n with other distributions.

1.2. **Single random permutation with restricted cycle lengths.** We define, for A non empty set of positive integers, $\mathfrak{S}_n^{(A)}$ to be the set of permutations of $\mathfrak{S}_n$ with all cycle lengths in A. It is easy to see 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.

1.2.1. *Case where A is infinite.* We first prove, in section 3.3.1, that if for all n such that $\mathfrak{S}_n^{(A)}$ is non empty, σ_n is uniformly distributed on $\mathfrak{S}_n^{(A)}$, then under the additional hypothesis that $\sum_{\substack{j\geq 1 \\ j\notin A}} \frac{1}{j} < \infty$, from the previously mentioned result about the case where σ_n is uniformly distributed on $\mathfrak{S}_n$, it remains that 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 since for all $k \notin A$, $N_k(\sigma_n) = 0$, this result is the strongest one could keep from the previous one for such a random permutation.

1.2.2. *Case where A is finite.* Note also that the result exposed in section 1.2.1 implies that even for large values of n, every $N_l(\sigma_n)$ stays finite. Hence if A is finite, no such result can be expected. Specifically, denoting $\max A$ by d, we prove in section 3.4 that for all $l \in A$, $N_l(\sigma_n)/n^{l/d}$ converges in every L^p to $1/l$.

1.3. **Word in random permutations with restricted cycle lengths.**

1.3.1. *Exposition of the problem.* In a second time, we shall fix $k \geq 1$, consider $A_1, \ldots, A_k$ non empty sets of positive integers (non of them being $\{1\}$), each of them being either finite or satisfying $\sum_{\substack{j\geq 1\\ j\notin A}} \frac{1}{j} < \infty$, w a word in the letters $g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}$, and, for all n such that $\mathfrak{S}_n^{(A_1)}$, $\ldots$, $\mathfrak{S}_n^{(A_k)}$ are all non empty, an independent family $s_1(n), \ldots, s_k(n)$ of random permutations chosen uniformly in respectively $\mathfrak{S}_n^{(A_1)}$, $\ldots$, $\mathfrak{S}_n^{(A_k)}$. We are going to give asymptotics (as n goes to infinity) on the random variables $N_l(\sigma_n)$ when σ_n is the permutation obtained by changing any letter g_i in w by $s_i(n)$.

1.3.2. *Role played by a quotient of the free group generated by $g_1, \ldots, g_k$.* Note first that the result exposed just above in section 1.2.2, about random permutations of $\mathfrak{S}_n^{(A)}$ in the case where A is finite (with maximum d), states that in such random permutations, the cycles with length equal to d will be predominant: the cardinality of the subset of $\{1, \ldots, n\}$ covered by the support of such a random permutation will be equivalent to n. Hence its d-th power will be closed to one. Heuristically, one can say that for large n, this random permutation is not faraway from having order d. This is what has led us to introduce the group $F_k/[g_1^{d_1}, \ldots, g_k^{d_k}]$ generated by free elements $g_1, \ldots, g_k$ and quotiented by the relations $g_i^{d_i} = 1$ for $i \in [k]$, with $d_i = \sup A_i$ (when $d_i = +\infty$, the relation $g_i^{d_i} = 1$ counts for nothing). Any word in the letters $g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}$ represents an element of this group. It is natural to expect that the distribution of the permutation σ_n obtained by changing any letter g_i in w by $s_i(n)$ will depend especially, as n goes to infinity, on the element of this group represented by w. More specifically, since the functions N_l are constant on any conjugation class of the symmetric group, we are going to consider the conjugation class of the element of this group represented by w.

1.3.3. *Existence of cycles of most lengths.* The most general result we are going to prove about words in random permutations with restricted cycle length, theorem 5.1, is the following one. In the case where the element of $F_k/[g_1^{d_1}, \ldots, g_k^{d_k}]$ represented by w is not conjugated to an element represented by a word of the type g_i^{α} ($i \in [k]$, α integer), for all $l \geq 1$,

$$\liminf_{n\to\infty} \mathbb{E}(N_l(\sigma_n)) \geq \frac{1}{l}.$$

It means that the cycles of the letters of w are going to mix in a hieratic enough way to give birth to cycles of any length, at least as much as in a uniform random permutation, even when

the letters of w have very restricted cycle lengths. In the other case, we also have stronger lower bounds for this expectation, but not for any l.

1.3.4. *Weak limit of the distributions of the $N_l(\sigma_n)$.* Then, we are going to prove more precise results: under certain hypothesis on w and on the A_i's, for all $l \geq 1$, the joint distribution of the random vector

$$(N_1(n), \ldots, N_l(n))$$

converges weakly, as n goes to infinity, to

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

just like if the distribution of σ_n would have been uniform on $\mathfrak{S}_n$. Our hypothesis, for obtaining such a conclusion, are either (theorem 5.3) that all A_i's are infinite and that w is not a power of another word (note that this hypothesis on w, which is formulated in a slightly more precise way in the article, is not a real restriction, since the cycle lengths of a power of a permutation only depend on the cycle lengths of the permutation itself) , or (theorem 5.4) that $w = g_1 \cdots g_k$ (with the exception of the case $k = 2$ and $A_1 \cup A_2 \subset \{1, 2\}$, which means that our results do not apply to the product of two random involutions).

This results extend in one hand a result of A. Nica, who proved in [Ni94] that in the case where all A_i's are equal to the set of all positive integer and where w is not a power of another word, for all $l \geq 1$, the distribution of $N_l(\sigma_n)$ converges weakly to $\mathrm{Poiss}(1/l)$, and on the other hand a result of M. Neagu, who proved in [Ne05] that the matrices of independent random permutations with restricted cycle length are asymptotically free. Here, we shall mention that much of the methods we use in this paper are inspired by the ones invented in both of this papers, and that we use many of their results.

1.4. **Comments on this results and open questions.** Note first that all the random permutations σ_n we consider have a distribution which is invariant by conjugation. Hence their distributions are completely determined by the distribution of the random vector $(N_1(\sigma_n), \ldots, N_n(\sigma_n))$. In our results, we fix $l \geq 1$ and study $(N_1(\sigma_n), \ldots, N_l(\sigma_n))$ as n goes to infinity.

If σ_n is the permutation obtained by changing any letter g_i in a word w by $s_i(n)$, then under the pretty general hypothesis exposed in the section 1.3.4, we obtain an asymptotic distribution which is the same as the one we would have obtained if σ_n would have been uniform on $\mathfrak{S}_n$:

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

It leads to the question of the distance between the distribution of a word in independent random permutations and the uniform distribution: what are the functionals f of a permutation such that $f(\sigma_n)$ is asymptotically distributed as if σ_n would have been uniformly distributed on $\mathfrak{S}_n$?

Another pretty interesting question arising from the similarity between σ_n and a uniform random permutation on $\mathfrak{S}_n$ is the following one: do we have a characterization of the words w in the letters $g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}$ such that for n large enough, the random permutation obtained by replacing any letter g_i of the word w by $s_i(n)$, with $s_1(n), \ldots, s_k(n)$ independent family of uniform random permutations in $\mathfrak{S}_n$, is uniformly distributed ? This question has an analogue in any compact group, and it would also be interesting to compare the words convenient for different groups. One can find some sufficient conditions, like the fact that for some $i \in [k]$, g_i appears only once in w and g_i^{-1} doesn't appear, or, the (more general) fact that there is a sequence of words $w = w_0, w_1, \ldots, w_p$ such that w_p is a single letter and for all $i \in [p]$, w_i a simple reduction of w_{i-1}, where we call a *simple reduction* of a word w any word w' such that

there exists $a, b \in \{g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}\}$ which are distinct and not inverse one of each other such that in w, the letter a (resp. a^{-1}) always appears followed by b (resp. preceded by b^{-1}) and w' is the word obtained from w by replacing ab (resp. $b^{-1}a^{-1}$) everywhere it appears by a (resp. a^{-1}). As an example, $g_1g_2g_2g_3g_1g_2g_1^{-1}$ is a direct reduction of $g_1g_3g_2g_2g_3g_1g_3g_2g_3^{-1}g_1^{-1}$ for $a = g_1$, $b = g_3$. The author, despite the active and friendly help of Thierry Lévy, did not manage to prove that this condition is, or is not, necessary.

In theorem 2.5, we give a general sufficient condition on certain sequences σ_n of random permutations to have the weak convergence of the distribution of $(N_1(\sigma_n), \ldots, N_n(\sigma_n))$ to $\mathrm{Poiss}(1/1) \otimes \mathrm{Poiss}(1/2) \otimes \cdots \otimes \mathrm{Poiss}(1/l)$ as n goes to infinity. It would be interesting to know if this condition is sufficient. For more details, see remark 2.6.

Of course, the question of extension the results exposed in section 1.3.4 to some more general words when the A_i's are not all infinite is a natural continuation of this paper. For more details about it, we refer to remark 4.18.

There is a last open question the author would like to point at: do we have a dilation of the random variables of $N_l(\sigma_n)/n^{l/d} - 1/l$ of section 1.2.2 (which converge to zero) which has a non degenerate weak limit as n goes to infinity ?

1.5. **Notation.** In this text, for N integer, we shall denote $\{1, \ldots, N\}$ by $[N]$.

2. A general result about cycles of random permutations

2.1. **Technical preliminaries about boolean polynomials.** This section is devoted to the proof of corollary 2.3, that we did not find in the literature. Let us first introduce the terminology of [B01]. A *boolean polynomial* $f(X_1, \ldots, X_N)$ in the indeterminate sets $X_1, \ldots, X_N$ is a formula of the type

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

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

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

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

Remark 2.1. *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 2.2. *Fix $n \geq 1$, $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$, $f_1, \ldots, f_n$ boolean polynomials in the indeterminate sets $X_1, \ldots, X_N$. Then in order to have*

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

for all family $A_1, \ldots, A_N$ of events in a 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 2.1, 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. □

We shall use the following corollary to prove theorem 2.5.

Corollary 2.3. *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),

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

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 $i=1,\dots,q$, $I_i=[n_i]$, with $n_i\geq 1$. As an application of the previous theorem, one can suppose every $A_{i,j}$ to be either $\emptyset$ or Ω. 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 $m\geq 0$,

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

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

Now consider $(r_1,\dots,r_q)\neq(c_1,\dots,c_q)$. 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 $m\geq 0$,

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

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

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

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

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

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

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 $d_1 + \cdots + d_q - 1 \geq 1$. First note that if $m = 0$, then $Z(m,d) = 1$, so the result holds. So let us suppose that $m \geq 1$. Since $d_1 + \cdots + d_q \geq 2$, 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

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

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

Remark 2.4. *We use the same notations as in the previous corollary. One can easily prove, using theorem 2.2, that for all $r = (r_1,\ldots,r_q) \in \mathbb{N}^q$, one has*

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

2.2. **Number of cycles of a given length of random permutations.** The main theorem of section 2 is the following one. We shall use it in the following of the paper. Recall that we have defined, for A set of positive integers and $n \geq 1$, $\mathfrak{S}_n^{(A)}$ to be the set of permutations of $\mathfrak{S}_n$ with all cycle lengths in A.

Theorem 2.5. *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 $\mathfrak{S}_n$. Let, for all $l \geq 1$, $N_l(\sigma_n)$ denote the number of cycles of length l of σ_n. Suppose 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. 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

$$\bigotimes_{l\in K} \mathrm{Poiss}(1/l).$$

Remark 2.6. *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 $(N_1(\sigma_n), \dots, N_q(\sigma_n))$ converges, as n goes to infinity, to $\bigotimes_{1\leq l\leq q} Poiss(1/l)$. Is that true that for all $p \geq 1$, for all $\sigma \in \mathfrak{S}_p$, the probability of the event*

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

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 (3).

Proof. 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 positive integer q, a subset $\{l_1 < \dots < l_q\}$ of A, a family of non negative 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

$$\prod_{1\leq i\leq q} e^{-1/l_i} \frac{(1/l_i)^{r_i}}{r_i!}. \tag{4}$$

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

$$\{\forall i = 1, \dots, q, \text{ exactly } r_i \text{ of the events of the family } (E_c(n))_{c\in\mathfrak{C}_{l_i}(n)} \text{ occur}\} \tag{5}$$

converges, as n goes to infinity, to (4).

By (1), for all n, the probability of the event of (5) is

$$\sum_{k_1=r_1,\dots,|\mathfrak{C}_{l_1}(n)|} \cdots \sum_{k_q=r_q,\dots,|\mathfrak{C}_{l_q}(n)|} (-1)^{k_1-r_1+\dots+k_q-r_q} \binom{k_1}{r_1} \cdots \binom{k_q}{r_q} S_{(k_1,\dots,k_q)}(n), \tag{6}$$

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

$$S_k(n) := \sum P(\bigcap_{i\in[q]} \bigcap_{c\in J_i} E_c(n)), \tag{7}$$

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 first fix $k = (k_1, \dots, k_q) \in \mathbb{N}^q\backslash\{0\}$. We shall compute $\lim_{n\to\infty} S_k(n)$. Define $p = k_1 \cdot l_1 + \dots + k_q \cdot l_q$ 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

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

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 this 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 this 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

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

Hence by hypothesis,

$$\lim_{n\to\infty}S_k(n)=\frac{1}{l_1^{k_1}l_2^{k_2}\ldots l_q^{k_q}}\frac{1}{k_1!k_2!\cdots k_q!}.$$

We denote this limit by $S_{(k_1,\ldots,k_q)}$.

Step III. Now, let us prove that the probability of the event of (5) converges to

$$\sum_{\substack{k_1\geq r_1\\ \vdots\\ k_q\geq r_q}}(-1)^{k_1-r_1+\cdots+k_q-r_q}\binom{k_1}{r_1}\cdots\binom{k_q}{r_q}S_{(k_1,\ldots,k_q)}, \tag{8}$$

which is equal to

$$\sum_{\substack{k_1\geq r_1\\ \vdots\\ k_q\geq r_q}}(-1)^{k_1-r_1+\cdots+k_q-r_q}\frac{1}{(k_1-r_1)!r_1!}\cdots\frac{1}{(k_q-r_q)!r_q!}\frac{1}{l_1^{k_1}l_2^{k_2}\ldots l_q^{k_q}}, \tag{9}$$

(this shows that the series converges).

Fix $\varepsilon>0$. Choose $m_0\geq 0$ such that for all $m\geq m_0$, the absolute value of

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

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 (5) is minored by

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

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 (5) is minored by

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

and majored by

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

hence is ε-closed to the sum of (8).

Step IV. Now, let us write again the limit of the probability of the event of (5). By the previous step and by (9), it is equal to

$$\frac{1}{r_1!\cdots r_q!}\frac{1}{l_1^{r_1}\cdots l_q^{r_q}}\sum_{\substack{t_1\geq 0\\ \vdots\\ t_q\geq 0}}(-1)^{t_1+\cdots+t_q}\frac{1}{t_1!}\cdots\frac{1}{t_q!}\frac{1}{l_1^{t_1}\cdots l_q^{t_q}},$$

i.e. to the expected limit of (4). It closes the proof of the theorem. □

3. Number of cycles of a given length of random permutations with restricted cycle lengths

3.1. **Graph theoretic basic definitions.** In this text, we shall consider *oriented, edge-colored graphs with color set* $[k]$: these are families $G=(V;E_1,\dots,E_k)$, where V is a finite set (its elements are called the *vertices* of G) and for all $r\in[k]$, E_r is a subset of V^2 (the set of *edges with color* r of G). For $e=(u,v)$ edge of G, u (resp. v) is called the *beginning vertex* of e (resp. the *ending vertex* of e) and is denoted by $\mathrm{Beg}(e)$ (resp. $\mathrm{End}(e)$). e is often denoted by $u\to v$. Note that the E_r's are not supposed to be pairwise disjoint, hence for $u,v\in V$ there can be several edges (with pairwise distinct colors) beginning at u and ending at v. When the E_r's are pairwise disjoint, as it will be the case for the graphs $G(\sigma,w)$ that we shall introduce the section 4.2.2, one can define the graph by giving the set of vertices, the set of edges, and the color of every edge.

An *oriented graph* is an oriented, edge-colored graph where all edges have the same color.

A *loop* is an oriented graph of the type $(\{v_1,\dots,v_l\},\{v_1\to v_2\to\cdots\to v_l\to v_1\})$, with $v_1,\dots,v_l$ pairwise distinct. We define its *length* to be l.

A *string* is an oriented graph of the type $(\{v_1,\dots,v_l\},\{v_1\to v_2\to\cdots\to v_l\})$, with $v_1,\dots,v_l$ pairwise distinct. We define its *length* to be $l-1$.

A graph is said to be *connected* if for every two distinct vertices a,b, there exists a positive integer n and vertices $a=a_0,a_1,\dots,a_n=b$ such that for every $i\in[n]$, there is an edge (of any color and either direction) between a_{i-1} and a_i.

A *connected component* of a graph $(V;E_1,\dots,E_k)$ is a maximal *subgraph* (i.e. graph of the type $(V';E_1',\dots,E_k')$ with $V'\subset V$, $E_1'\subset E_1$, …, $E_k'\subset E_k$) which is connected.

We define, for G oriented, edge-colored with color set $[k]$ graph, for $r\in[k]$, $G[r]$ to be the graph obtained from G by erasing all edges which color is not r and all vertices which are not the beginning or the end of an edge of color r. A *string* (resp. a *loop*) *with color* r of G is a connected component of $G[r]$ which is a string (resp. a loop).

A graph is said to be *2-regular* if for all vertex v,

$$|\operatorname{Beg}^{-1}(\{v\})|+|\operatorname{End}^{-1}(\{v\})|=2.$$

3.2. **A preliminary result.** We fix a non empty set A of positive integers, different from $\{1\}$. 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.

Let us consider Γ an oriented graph which is a union of

- loops with lengths in A,
- strings with lengths $<\sup A$,

such that the union is disjoint, i.e. that non vertex of Γ belongs in the same time to two different loops, to two different strings or to a loop and a string.

Let us also consider γ an injective function from the vertex set of Γ to $[n]$, and let $p_n^{(A)}(\Gamma)$ be the probability that a random permutation s with uniform distribution on $\mathfrak{S}_n^{(A)}$ satisfies

$$\forall e \text{ edge of } \Gamma, s(\gamma(\operatorname{End}(e)))=\gamma(\operatorname{Beg}(e)).$$

Let us first note that this probability does not depend on the choice of γ. Indeed, let γ' be another injective function from the vertex set of Γ to $[n]$. Let B_γ (resp. $B_{\gamma'}$) be the set of s's in $\mathfrak{S}_n^{(A)}$ that satisfy

$$\forall e \text{ edge of } \Gamma, s(\gamma(\operatorname{End}(e)))=\gamma(\operatorname{Beg}(e)) \text{ (resp. } s(\gamma'(\operatorname{End}(e)))=\gamma'(\operatorname{Beg}(e))).$$

Since γ and γ' are both injective, there exists $\tau\in\mathfrak{S}_n$ such that $\gamma'=\tau\circ\gamma$. Then one has

$$\forall s\in\mathfrak{S}_n^{(A)}, s\in B_\gamma\iff \tau s\tau^{-1}\in B_{\gamma'},$$

from which it follows that the probability of the previously mentioned event does not depend on the choice of γ, since the uniform distribution on $\mathfrak{S}_n^{(A)}$ is invariant under conjugation.

The following result is proved in [Ne05].

Theorem 3.1. *Suppose that A is either finite or satisfies $\sum_{\substack{j\geq 1\\ j\notin A}} \frac{1}{j} < \infty$. Then as n goes to infinity in such a way that $\mathfrak{S}_n^{(A)} \neq \emptyset$,*

$$p_n^{(A)}(\Gamma) \sim n^{\left\{ -|\{edges\ of\ \Gamma\}| + \sum_{L\ loop\ of\ \Gamma} \frac{length\ of\ L}{d} \right\}}, \tag{10}$$

where $d = \sup A$ and with the convention $l/\infty = 0$ for all $l \geq 1$.

3.3. Cycles of a random permutation of $\mathfrak{S}_n^{(A)}$.

3.3.1. *Case where A is infinite.* As an application of theorem 3.1 and of theorem 2.5, we are going to prove the following result:

Proposition 3.2. *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 that for all $k \notin A$, $N_k(\sigma_n) = 0$.

Note also that this result implies that even for large values of n, every $N_l(\sigma_n)$ stays finite.

Proof. By theorem 2.5, it suffices to prove that for $p \geq 1$, for $\sigma \in \mathfrak{S}_p^{(A)}$, 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 is a direct application of theorem 3.1 for $\Gamma = ([p], \{i \to \sigma(i)\,;\, i \in [p]\})$. □

3.4. Case where A is finite.

We are going to prove the following result:

Theorem 3.3. *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's ($p \in [1, +\infty)$) 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 ransom 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 appears in [Ne05].

Lemma 3.4. *Let p be the greatest common divisor of A. Then for $|z| < 1$,*

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

Lemma 3.5. *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 around zero 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 $l^{-m} n^{ml/d}$ 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

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

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

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

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

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

i.e.

(11)

$$\mathbb{E}[N_l(\sigma_n)^m] = \frac{1}{l^m} \sum_{j=1}^{m} \left[\binom{n}{j} P\left(1,\ldots,j \text{ belong to cycles of length } l\right) \sum_{\substack{m_1,\ldots,m_j\geq 1 \\ m_1+\ldots+m_j=m}} \binom{m}{m_1,\ldots,m_j}\right].$$

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

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

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. Hence by lemma 3.4, for $|z| < 1$, 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 $|w| < 1$, 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 3.5, 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

$$P\left(1,\dots,j \text{ belong to cycles of length } l\right) \sim \frac{1}{n^j} \sum_{\pi\in\mathrm{P}(j)} n^{l|\pi|/d} \prod_{V\in\pi} \frac{(l-1)!}{(l-|V|)!} \sim n^{(l/d-1)j}. \tag{12}$$

Mixing equations (11) and (12), one gets

$$\mathbb{E}[N_l(\sigma_n)^m] \sim \frac{1}{l^m}\sum_{j=1}^{m}\left[\frac{n^{lj/d}}{j!}\sum_{\substack{m_1,\ldots,m_j\geq 1\\ m_1+\cdots+m_j=m}}\binom{m}{m_1,\ldots,m_j}\right] \sim \frac{n^{lm/d}}{l^m}.$$

□

4. Combinatorial preliminaries to the study of words in random permutations

4.1. **Words and groups generated by relations.**

4.1.1. *Words.* Let, for $k \geq 1$, M_k be the set of *words* in the letters $g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}$, i.e. the set of sequences $g_{i_1}^{\alpha_1}\cdots g_{i_n}^{\alpha_n}$, with $n \geq 0$, $i_1, \ldots, i_n \in [k]$, $\alpha_1, \ldots, \alpha_n = \pm 1$. A word $w \in M_k$ is said to be *reduced* if in its writing, no letter is followed by its inverse. It is said to be *cyclically reduced* if moreover, the first and the last letter are not the inverses one of each other. It is easy to prove that for all $w \in M_k$ reduced, there is $v \in M_k$ cyclically reduced, $m \geq 0$, $i_1, \ldots, i_m \in [k]$, $\alpha_1, \ldots, \alpha_m \in \{1, -1\}$ such that

$$w = g_{i_1}^{\alpha_1}\cdots g_{i_m}^{\alpha_m} v g_{i_m}^{-\alpha_m}\cdots g_{i_1}^{-\alpha_1}.$$

A cyclically reduced word is said to be *primitive* if it is not the concatenation of $d \geq 2$ times the same word. It can be proved that any cyclically reduced word is a power of a primitive word.

For $w = g_{i_1}^{\alpha_1}\cdots g_{i_{|w|}}^{\alpha_{|w|}} \in M_k$ and $s = (s_1, \ldots, s_k)$ family of elements of a group, $w(s)$ denotes $s_{i_1}^{\alpha_1}\cdots s_{i_{|w|}}^{\alpha_{|w|}}$.

4.1.2. *The quotient of the free group with k generators by the relations $g_1^{d_1} = 1, \ldots, g_k^{d_k} = 1$.* Let F_k be the free group generated by $g_1, \ldots, g_k$. It is the set of reduced words of M_k endowed with the operation of concatenation-reduction via the relations $g_i g_i^{-1} = 1, g_i^{-1} g_i = 1, i \in [k]$. For $w, w_0 \in M_k$ with w_0 reduced, w is said to *represent* or to be a *writing of* the element w_0 of F_k if one can reduce w to w_0 via the previous relations.

Consider $d_1, \ldots, d_k \in \{2, 3, 4, \ldots\} \cup \{\infty\}$. Let $F_k/[g_1^{d_1}, \ldots, g_k^{d_k}]$ be the group F_k quotiented by its normal subgroup generated by the set $\{g_i^{d_i}\,;\, i \in [k], d_i < \infty\}$. For $w \in M_k$, w is said to *represent* or to be a *writing of* a class $C \in F_k/[g_1^{d_1}, \ldots, g_k^{d_k}]$ if it is a writing of an element of C.

Theorem 1.4 of section 1.4 of [MKS66] states the following facts.

Theorem 4.1. *(a) Any element of $F_k/[g_1^{d_1}, \ldots, g_k^{d_k}]$ has a writing of the type $g_{i_1}^{\alpha_1}\cdots g_{i_n}^{\alpha_n}$ with $i_1 \neq i_2 \neq \cdots \neq i_n \in [k]$, $\alpha_1, \ldots, \alpha_n$ integer numbers such that $0 < |\alpha_1| < d_{i_1}, \ldots, 0 < |\alpha_n| < d_{i_n}$, and this writing is unique up to replacements of the type*

$$g_{i_j}^{\alpha_j} \to \begin{cases} g_{i_j}^{d_{i_j}+\alpha_j} & \text{if } \alpha_j < 0 \text{ and } d_{i_j} < \infty, \\ g_{i_j}^{-d_{i_j}+\alpha_j} & \text{if } \alpha_j > 0 \text{ and } d_{i_j} < \infty, \end{cases}$$

with $j \in [n]$.

(b) In any conjugation class of $F_k/[g_1^{d_1}, \ldots, g_k^{d_k}]$, there is an element represented by a word of the previous type such that moreover, $i_n \neq i_1$, and such a word is unique up to replacements of the previous type and to transformations of the type $g_{i_1}^{\alpha_1}\cdots g_{i_n}^{\alpha_n} \to g_{i_n}^{\alpha_n} g_{i_1}^{\alpha_1}\cdots g_{i_{n-1}}^{\alpha_{n-1}}$.

For (b), the existence (but not the uniqueness) will be proved again in lemma 4.3.

Let us define the $(d_1 \dots, d_k)$-*cyclically reduced words* to be the words of the type $g_{i_1}^{\alpha_1} \cdots g_{i_n}^{\alpha_n}$ with $n \geq 0$, $i_1 \neq i_2 \neq \cdots \neq i_n \neq i_1 \in [k]$, $\alpha_1, \dots, \alpha_n$ integers such that $0 < |\alpha_1| < d_{i_1}, \dots$, $0 < |\alpha_n| < d_{i_n}$. For $w \in M_k$, the set of $(d_1 \dots, d_k)$-cyclically reduced words which represent elements of the class of conjugation of the element of $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$ represented by w are called the $(d_1 \dots, d_k)$-*cyclic reductions* of w. In general, there are more than one $(d_1 \dots, d_k)$-cyclic reductions of w.

Remark 4.2. *1. Note that since in any group, if two elements are conjugated, then all their powers are, for all $l \geq 1$, the $(d_1 \dots, d_k)$-cyclic reductions of w^l are the $(d_1 \dots, d_k)$-cyclic reductions of the l-th power of any $(d_1 \dots, d_k)$-cyclic reduction of w.*
2. Note also that the l-th power of a $(d_1 \dots, d_k)$-cyclically reduced word is $(d_1 \dots, d_k)$-cyclically reduced whenever the word is not of the type g_i^α, with $i \in [k]$, $\alpha \neq 0$ such that $d_i \geq l|\alpha|$.

The following lemma gives a concrete way, from a word $w \in M_k$, to achieve one of its $(d_1 \dots, d_k)$-cyclic reductions.

A non empty word $w \in M_k$ is said *admit a reduction w' on the right* if there exists $w' \in M_k$ and $r \in [k]$ such that w is one of the following words

$$w' g_r g_r^{-1}, w' g_r^{-1} g_r, w' g_r^{d_r}, w' g_r^{-d_r}.$$

The *cyclic permutation* of a non empty word $w = g_{i_1}^{\varepsilon_1} \cdots g_{i_m}^{\varepsilon_m}$ with $n \geq 1$, $i_1, \dots, i_m \in [k]$, $\varepsilon_1, \dots, \varepsilon_m \in \{-1, 1\}$, is defined to be $c(w) := g_{i_m}^{\varepsilon_m} g_{i_1}^{\varepsilon_1} \cdots g_{i_{m-1}}^{\varepsilon_{m-1}}$.

Lemma 4.3. *Consider $w \in M_k$. Then there exists a unique $n \geq 0$, a unique sequence $w_0 = w, w_1, \dots, w_n \in M_k$ such that*

(i) *$w_1, \dots, w_{n-1}$ are not $(d_1 \dots, d_k)$-cyclically reduced,*
(ii) *w_n is $(d_1 \dots, d_k)$-cyclically reduced,*
(iii) *for all $i \in [n]$, w_i is the reduction on the right of w_{i-1} if w_{i-1} admits one, and its cyclic permutation in the other case.*

Note that w_n is one of the $(d_1 \dots, d_k)$-cyclic reductions of w. We shall call it its *canonical right $(d_1, \dots, d_k)$-cyclic reduction.*

Proof. We have an obvious notion of length for the elements of M_k. The lemma can easily be proved by induction on the length $|w|$ of w.

For $|w| = 0$, the result is obvious.

Suppose that w is non empty and that the result is proved for all words of length $< |w|$.
- If there is $p \geq 0$ such that the p-th cyclic permutation $c^p(w)$ admits a reduction on the right, then let p_0 be the smallest such integer and define $w_i = c^i(w)$ for $i = 0, \dots, p_0$ and w_{p_0+1} to be the reduction on the right of $c^{p_0}(w)$. Then the induction hypothesis allows to conclude.
- If there is no $p \geq 0$ such that $c^p(w)$ admits a reduction on the right, then there is $p \geq 0$ such that $c^p(w)$ is $(d_1 \dots, d_k)$-cyclically reduced. Let n be the smallest such integer. Then n, $w_0 = c^0(w)$, …, $w_n = c^n(w)$ are convenient. □

4.2. **Colored graphs associated to words and permutations. Congruences.**

4.2.1. *Partitions, graphs and congruences.* Recall that a *partition* Δ of a set X is a set of pairwise disjoint, non empty subsets of X which union is X. Since Δ is a set, $|\Delta|$ denotes the its cardinality, i.e. the number of *classes* of Δ.

For any function γ defined on a set X, we shall denote by $\mathrm{Part}(\gamma)$ the partition of X by the level sets of γ.

In the section 3.1, we introduced the notion of oriented, edge-colored with color set $[k]$ graph. Let us fix such a graph G, with vertices set V.

G is said to be *admissible* if two different edges with the same color cannot have the same beginning of the same end.

We call a *congruence of* G a partition Δ of V such that the beginnings of two edges with the same color are in the same class of Δ if and only if the ends are in the same class of Δ.

We are also going to use the notion of *quotient graph*, that we define now. Let us define, for Δ partition of V, G/Δ to be the oriented edge-colored (with color-set $[k]$) graph whose vertices are the classes of Δ and such that for all C, C' classes of Δ, for all $r \in [k]$, there is an edge with color r from C to C' in G/Δ when there is an edge with color r in G from a vertex of C to a vertex of C'.

Remark 4.4. *Note that Δ is a congruence of G if and only if G/Δ is admissible.*

4.2.2. *The graph $G(\sigma, w)$.* Fix $k, p \geq 1$, $\sigma \in \mathfrak{S}_p$ and $w = g_{i_1}^{\alpha_1} \cdots g_{i_{|w|}}^{\alpha_{|w|}} \in M_k$ a non empty word. In [Ni94], Nica defined $G(\sigma, w)$ (denoted by $\mathcal{H}_{\sigma^{-1}} \bigstar w$ in his paper) to be the directed, edge-colored with color set $[k]$, 2-regular graph with vertex set $V := [p] \times [|w|]$ and edge set

$$E := \underbrace{\{a_1, \ldots, a_p\}}_{\substack{\text{pairwise distinct elements which could} \\ \text{have been replaced by } 1, \ldots, p, \text{ but which are} \\ \text{called } a_i\text{'s in order to avoid confusions}}} \times [|w|],$$

where the color of any edge (a_m, l) is i_l, and the beginning and the end of any edge (a_m, l) are given by :

$$\mathrm{Beg}(a_m, l) = \begin{cases} (m, l) & \text{if } \alpha_l = 1 \\ (m, l+1) & \text{if } l \neq |w|, \alpha_l = -1 \\ (\sigma^{-1}(m), 1) & \text{if } l = |w|, \alpha_l = -1 \end{cases}$$

$$\mathrm{End}(a_m, l) = \begin{cases} (m, l+1) & \text{if } l \neq |w|, \alpha_l = 1 \\ (\sigma^{-1}(m), 1) & \text{if } l = |w|, \alpha_l = 1 \\ (m, l) & \text{if } \alpha_l = -1 \end{cases}$$

In the case where $p = 1$ and $\sigma = Id$, we shall denote $G(\sigma, w)$ by $G(w)$ and identify its vertex set and its edge set with $[|w|]$ by $(1, l) \simeq l$ and $(a_1, l) \simeq l$ for all $l \in [|w|]$. We will also use the convention that if w is the empty word, then $G(\sigma, w)$ is the empty graph.

Remark 4.5. *Note that this graph is admissible if and only if w is cyclically reduced.*

A graph $(V; E_1, \ldots, E_k)$ is said to be the *disjoint union* of the graphs $(V'; E_1', \ldots, E_k')$ and $(V''; E_1'', \ldots, E_k'')$ if $V = V' \cup V''$, $E_1 = E_1' \cup E_1''$, $\ldots$, $E_k = E_k' \cup E_k''$ and all this unions are disjoint.

An *isomorphism* between two oriented, edge-colored graphs $(V; E_1, \dots, E_k)$, $(V'; E'_1, \dots, E'_k)$ is a bijection $\varphi : V \to V'$ such that for all $u, v \in V$, for all $r \in [k]$, one has

$$u \to v \in E_r \iff \varphi(u) \to \varphi(v) \in E'_r.$$

The following lemma is going to give us a way to understand the graphs of the type $G(\sigma, w)$ by reducing them to disjoint unions of graphs isomorphic to graphs of the type $G(w)$.

Lemma 4.6. *$G(\sigma, w)$ is the disjoint union of $N_1(\sigma)$ graphs isomorphic to $G(w^1)$, $N_2(\sigma)$ graphs isomorphic to $G(w^2)$, ..., $N_p(\sigma)$ graphs isomorphic to $G(w^p)$.*

Proof. If I, J are disjoint subsets of $[p]$ stable by σ, then in $G(\sigma, w)$, there is no edge between elements of $I \times [|w|]$ and $J \times [|w|]$. Hence $G(\sigma, w)$ is the disjoint union of the graphs $(V(c), E_1(c), \dots, E_k(c))$, where c varies in the set of cycles of the cycle-decomposition of σ, and where for all such cycle c, with support $C \subset [p]$, $V(c) = C \times [|w|]$ and for all $i \in [k]$, $E_i(c) = E_i \cap (V(c)^2)$.

Hence it suffices to prove that for all $d \in [p]$, for all cycle $c = (m_1\, m_2 \cdots m_d)$ of σ of length d, there is an isomorphism between $(V(c), E_1(c), \dots, E_k(c))$ and $G(w^d)$. The function which maps $(m_i, l) \in \{m_1, m_2, \dots, m_d\} \times [|w|]$ to $(d-i)|w| + l \in [d|w|]$ is such an isomorphism. □

As an example, when $w = g_1 g_2 g_1^{-1} g_2^{-1}$, $p = 3$ and σ is the cycle (123), $G(\sigma, w)$ is the graph

$$\begin{array}{ccccccccc}
(1,1) & \underset{(a_1,1)}{\overset{1}{\to}} & (1,2) & \underset{(a_1,2)}{\overset{2}{\to}} & (1,3) & \underset{(a_1,3)}{\overset{1}{\leftarrow}} & (1,4) & \underset{(a_1,4)}{\overset{2}{\leftarrow}} & \\
(3,1) & \underset{(a_3,1)}{\overset{1}{\to}} & (3,2) & \underset{(a_3,2)}{\overset{2}{\to}} & (3,3) & \underset{(a_3,3)}{\overset{1}{\leftarrow}} & (3,4) & \underset{(a_3,4)}{\overset{2}{\leftarrow}} & \\
(2,1) & \underset{(a_2,1)}{\overset{1}{\to}} & (2,2) & \underset{(a_2,2)}{\overset{2}{\to}} & (2,3) & \underset{(a_2,3)}{\overset{1}{\leftarrow}} & (2,4) & \underset{(a_2,4)}{\overset{2}{\leftarrow}} & (1,1),
\end{array}$$

where the name and the color of every edge are written respectively below and above the edge, and where one has to read in a cyclic way (i.e. the last vertex of the last line is the same one as the first vertex of the first line).

When w is still $g_1 g_2 g_1^{-1} g_2^{-1}$, but $p = 5$ and σ is the product of disjoint cycles $(123)(45)$, $G(\sigma, w)$ is the disjoint union of the previous graph and of

$$\begin{array}{ccccccccc}
(4,1) & \underset{(a_4,1)}{\overset{1}{\to}} & (4,2) & \underset{(a_4,2)}{\overset{2}{\to}} & (4,3) & \underset{(a_4,3)}{\overset{1}{\leftarrow}} & (4,4) & \underset{(a_4,4)}{\overset{2}{\leftarrow}} & \\
(5,1) & \underset{(a_5,1)}{\overset{1}{\to}} & (5,2) & \underset{(a_5,2)}{\overset{2}{\to}} & (5,3) & \underset{(a_5,3)}{\overset{1}{\leftarrow}} & (5,4) & \underset{(a_5,4)}{\overset{2}{\leftarrow}} & (4,1).
\end{array}$$

4.2.3. *A result of Nica we are going to use.* In [Ni94], Nica proved the following theorem, involving quotients of the graph $G(\sigma, w)$ by congruences.

Theorem 4.7. *Consider $w \in M_k$ cyclically reduced. Then for all congruence Δ of $G(\sigma, w)$, the number of classes of Δ is less or equal than the number of edges of $G(\sigma, w)/\Delta$. Moreover, if w is primitive, then the singletons partition is the only congruence Δ of $G(\sigma, w)$ such that the number of classes of Δ is equal than the number of edges of $G(\sigma, w)/\Delta$ and for all $m \neq m' \in [p]$, $m \neq m' \mod \Delta$.*

4.2.4. *Admissible graphs with restricted loop and string lengths.* Let us fix $A_1, \dots, A_k$ non empty (finite or infinite) sets of positive integers, non of them being $\{1\}$. Let us denote $\sup A_1, \dots, \sup A_k$ by respectively $d_1, \dots, d_k$.

If an oriented, edge-colored graph G with color set $[k]$ is admissible and $r \in [k]$, it is easy to see, since two different edges of $G[r]$ cannot have the same beginning or the same end, that $G[r]$ is a disjoint union of strings and of loops (see section 3.1 for the definitions of strings and loops). If for each $r \in [k]$, all this strings have length $< \sup A_r$ and all this cycles have length in A_r (resp. length equal to d_r), G will be said to be $(A_1, \dots, A_k)$-*admissible* (resp. $(d_1, \dots, d_k)$-*strongly admissible*). Note that the empty graph is $(d_1, \dots, d_k)$-strongly admissible. A congruence Δ of an oriented, edge-colored graph G will be said to be an $(A_1, \dots, A_k)$-*congruence* (resp. an $(d_1, \dots, d_k)$-*strong congruence*) if G/Δ is $(A_1, \dots, A_k)$-admissible (resp. $(d_1, \dots, d_k)$-strongly admissible).

We define the *Neagu characteristic* of an admissible graph G to be

$$\chi(G) = |\{\text{vertices of } G\}| - \sum_{r=1}^{k} |\{\text{edges of } G \text{ with color } r\}| + \sum_{r=1}^{k} \sum_{\substack{L \text{ loop of } G \\ \text{with color } r}} \frac{\text{length of } L}{d_r},$$

with the convention $l/\infty = 0$ and that the Neagu characteristic of the empty graph is 1. Note that in the case where G is $(d_1, \dots, d_k)$-strongly admissible (and non empty), its Neagu characteristic is its number of vertices minus its number of edges plus its number of mono-colored cycles.

Now, consider an admissible graph $G = (V; E_1, \dots, E_k)$, consider $v \in V, w \notin V, r \in [k]$, and define

$$G' = (V \cup \{w\}; E_1, \dots, E_{r-1}, E_r \cup \{v \to w\}, E_{r+1}, \dots, E_k)$$
$$(\text{resp. } G' = (V \cup \{w\}; E_1, \dots, E_{r-1}, E_r \cup \{w \to v\}, E_{r+1}, \dots, E_k)).$$

Then G' is admissible if and only if no edge with color r of G begins at v (resp. ends at v), and is $(A_1, \dots, A_k)$-admissible if and only if moreover, G is $(A_1, \dots, A_k)$-admissible and v is not the ending (resp. beginning) vertex of a string of G with color r and length $d_r - 1$. When G is $(A_1, \dots, A_k)$-admissible, if G' is admissible but not $(A_1, \dots, A_k)$-admissible, then if one denotes by u the beginning (resp. ending) vertex of the string with color r ending (resp. beginning) at v, the graph

$$(V \cup \{w\}; E_1, \dots, E_{r-1}, E_r \cup \{v \to w, w \to u\}, E_{r+1}, \dots, E_k)$$
$$(\text{resp. } (V \cup \{w\}; E_1, \dots, E_{r-1}, E_r \cup \{u \to w, w \to v\}, E_{r+1}, \dots, E_k))$$

is $(A_1, \dots, A_k)$-admissible. Moreover, the previous graph is also $(d_1, \dots, d_k)$-strongly admissible if and only if G is $(d_1, \dots, d_k)$-strongly admissible.

Hence we can define a *direct* $(d_1, \dots, d_k)$-*strongly admissible extension* of an admissible non empty graph $G = (V; E_1, \dots, E_k)$ to be either a graph of the type

$$(V \cup \{w\}; E_1, \dots, E_{r-1}, E_r \cup \{v \to w\}, E_{r+1}, \dots, E_k)$$
$$(\text{resp. } (V \cup \{w\}; E_1, \dots, E_{r-1}, E_r \cup \{w \to v\}, E_{r+1}, \dots, E_k)),$$

with $r \in [k]$, $v \in V, w \notin V$ when no edge with color r of G begins (resp. ends) at v and v is not the ending (resp. beginning) vertex of a string of G with color r and length $d_r - 1$ or a graph of the type

$$(V \cup \{w\}; E_1, \dots, E_{r-1}, E_r \cup \{v \to w, w \to u\}, E_{r+1}, \dots, E_k)$$

with $r \in [k]$, $u, v \in V, w \notin V$ when u, v are the respective beginning and ending vertices of a string with length $d_r - 1$ and color r.

By convention, we say that a direct $(d_1, \dots, d_k)$-strongly admissible extension of the empty graph is any graph with two vertices linked by a single edge of any color.

Remark 4.8. *Note that a direct $(d_1, \dots, d_k)$-strongly admissible extension of an admissible graph G is $(A_1, \dots, A_k)$-admissible (resp. $(d_1, \dots, d_k)$-strongly admissible) if and only if G is, and it has the same Neagu characteristic as G.*

Now, we can define an $(d_1, \dots, d_k)$-*strongly admissible extension* of an admissible graph G to be a graph G' such that there exists $m \geq 0$ and $G_0 = G, G_1, \dots, G_m = G'$ such that for all $i \in [m]$, G_i is a direct $(A_1, \dots, A_k)$-admissible extension of G_{i-1}.

Remark 4.9. *The following results can easily be proved by induction on the m of the previous definition using remark 4.8.*
1. A $(d_1, \dots, d_k)$-strongly admissible extension of an admissible graph G is $(A_1, \dots, A_k)$-admissible (resp. $(d_1, \dots, d_k)$-strongly admissible) if and only if G is.
2. A $(d_1, \dots, d_k)$-strongly admissible extension of an admissible graph G has the same Neagu characteristic as G.

Using lemma 4.3 with an induction on the n of this lemma, one can easily prove the following theorem. Recall that $G(w)$ has been defined in section 4.2.2.

Theorem 4.10. *Consider $w = g_{i_1}^{\varepsilon_1} \cdots g_{i_{|w|}}^{\varepsilon_{|w|}} \in M_k$ and denote its canonical right $(d_1, \dots, d_k)$-cyclic reduction by w'. Let $\Delta_m(w)$ be the partition of the vertex set $[|w|]$ of $G(w)$ defined by*

$$\forall l, l' \in [|w|], \quad l = l' \mod \Delta_m(w) \iff \text{one of the two words } g_{i_l}^{\varepsilon_l} \cdots g_{i_{l'-1}}^{\varepsilon_{l'-1}},$$

$$g_{i_{l'}}^{\varepsilon_{l'}} \cdots g_{i_{|w|}}^{\varepsilon_{|w|}} g_{i_1}^{\varepsilon_1} \cdots g_{i_{l-1}}^{\varepsilon_{l-1}} \text{ has the empty word for } (d_1, \dots d_k)\text{-cyclic reduction.}$$

Then $G(w)/\Delta_m(w)$ is a $(d_1, \dots, d_k)$-strongly admissible extension of a graph isomorphic to $G(w')$.

Remark 4.11. *We are not going to use it in the following, but it is easy to see that if $G(w')$ is $(d_1, \dots, d_k)$-strongly admissible (i.e. if w' is not of the type g_i^α, with $i \in [k]$ and $\alpha \neq 0$), then $\Delta_m(w)$ is the minimum (with respect to the refinement order) of the set of $(d_1, \dots, d_k)$-strong congruences of $G(w)$, and that in the other case, there is no $(d_1, \dots, d_k)$-strong congruence of $G(w)$.*

We shall use the following corollary later. $(1 \cdots l)$ denotes the cyclic permutation of $[l]$ which maps 1 to 2,..., $l-1$ to l and l to 1.

Corollary 4.12. *Consider $w = g_{i_1}^{\varepsilon_1} \cdots g_{i_{|w|}}^{\varepsilon_{|w|}} \in M_k$ and denote its canonical right $(d_1, \dots, d_k)$-cyclic reduction by w'. Suppose that w' is not the empty word.*
(a) If w' is not of the type g_i^α, with $i \in [k]$ and $\alpha \neq 0$, then for all $l \geq 1$, there is an $(A_1, \dots, A_k)$-admissible congruence Δ of $G((1 \cdots l), w)$ such that $\chi(G((1 \cdots l), w)/\Delta) = 0$ and for all $m \neq m' \in [l]$, $(m, 1) \neq (m', 1) \mod \Delta$.
(b) If w' is of the type g_i^α, with $i \in [k]$ and $\alpha \neq 0$, then for all $l \geq 1$ such that $|\alpha| l \in A_i$, there is an $(A_1, \dots, A_k)$-admissible congruence Δ of $G((1 \cdots l), w)$ such that $\chi(G((1 \cdots l), w)/\Delta) = |\alpha| l / d_i$ and for all $m \neq m' \in [l]$, $(m, 1) \neq (m', 1) \mod \Delta$.

Proof. Note first that by lemma 4.6, for all $l \geq 1$, the function $(m, i) \in [l] \times [|w|] \mapsto (l-m)|w| + i \in [l|w|]$ realizes an isomorphism between $G((1 \cdots l), w)$ and $G(w^l)$, hence we are going to work with $G(w^l)$ instead of $G((1 \cdots l), w)$ (and the condition "for all $m \neq m' \in [l]$, $(m, 1) \neq (m', 1)$

mod Δ" gets "for all $m \neq m' \in [l]$, $(m-1)|w|+1 \neq (m'-1)|w|+1 \mod \Delta$"). Let us prove that in (a) and in (b), $\Delta := \Delta_m(w^l)$ is convenient.

Let w'' be the canonical right $(d_1, \ldots, d_k)$-cyclic reduction of w^l. Note first that by 1 of remark 4.2, the $(d_1, \ldots, d_k)$-cyclic reductions of w^l are the $(d_1, \ldots, d_k)$-cyclic reductions of w'^l. In the case (a), where w'^l is $(d_1, \ldots, d_k)$-cyclically reduced by 2 of remark 4.2, it implies that w'' can be obtained from w'^l by the replacements and transformations mentioned in (b) of theorem 4.1. In the case (b), it implies, by 2 of remark 4.2, that $w'' = g_i^{\alpha l}$ if $|\alpha| l < d_i$ (case which will be denoted by (b1)) and that w'' is the empty word if $|\alpha| l = d_i$ (case which will be denoted by (b2)).

In the case (a), by what precedes, $G(w'')$ is $(A_1, \ldots, A_k)$-admissible and has null Neagu characteristic. So, since by theorem 4.10, $G(w^l)/\Delta$ is a $(d_1, \ldots, d_k)$-strongly admissible extension of a graph isomorphic to $G(w'')$, by the remark 4.9, Δ is an $(A_1, \ldots, A_k)$-admissible congruence of $G(w^l)$ and $\chi(G(w^l)/\Delta) = 0$. Moreover, for $m < m' \in [l]$, $(m-1)|w|+1 = (m'-1)|w|+1 \mod \Delta$ would imply, by definition of Δ, that one of the words $w^{m'-m}, w^{l-(m'-m)}$ has the empty word for cyclic reduction, which is false by 1 of remark 4.2.

In the case (b1), since $|\alpha| l \in A_i$ and $|\alpha| l < d_i$, $G(w'')$ is $(A_1, \ldots, A_k)$-admissible and has $|\alpha| l / d_i$ for Neagu characteristic. So, since by theorem 4.10, $G(w^l)/\Delta$ is a $(d_1, \ldots, d_k)$-strongly admissible extension of a graph isomorphic to $G(w'')$, by the remark 4.9, Δ is an $(A_1, \ldots, A_k)$-admissible congruence of $G(w^l)$ and $\chi(G(w^l)/\Delta) = |\alpha| l / d_i$. Moreover, for $m < m' \in [l]$, $(m-1)|w|+1 = (m'-1)|w|+1 \mod \Delta$ would imply, by definition of Δ, that one of the words $w^{m'-m}, w^{l-m'+l}$ has the empty word for cyclic reduction, which is false by 1 of remark 4.2.

In the case (b2), $G(w'')$ is the empty graph, hence is $(A_1, \ldots, A_k)$-admissible and has 1 for Neagu characteristic. So, since by theorem 4.10, $G(w^l)/\Delta$ is a $(d_1, \ldots, d_k)$-strongly admissible extension of a graph isomorphic to $G(w'')$, by the remark 4.9, Δ is an $(A_1, \ldots, A_k)$-admissible congruence of $G(w^l)$ and $\chi(G(w^l)/\Delta) = 1$. Moreover, for $m < m' \in [l]$, $(m-1)|w|+1 = (m'-1)|w|+1 \mod \Delta$ would imply, by definition of Δ, that one of the words $w^{m'-m}, w^{l-(m'-m)}$ has the empty word for cyclic reduction, which is false by 1 of remark 4.2, since $|\alpha| l = d_i$ and $m'-m$ and $l-(m'-m)$ both belong to $[l-1]$. □

4.3. **Application to words in random permutations.**

4.3.1. *Congruences of $G(\sigma, w)$ and permutations.* We fix again, until the end of section 4.3.1, $k, p \geq 1$, $\sigma \in \mathfrak{S}_p$ and $w = g_{i_1}^{\alpha_1} \cdots g_{i_{|w|}}^{\alpha_{|w|}} \in M_k$, with $i_1, \ldots, i_{|w|} \in [k]$ and $\alpha_1, \ldots, \alpha_{|w|} \in \{-1, 1\}$.

Define, for any $s \in (\mathfrak{S}_n)^k$, the function

$$\gamma_s : (m, l) \in V \mapsto s_{i_l}^{\alpha_l} \cdots s_{i_{|w|}}^{\alpha_{|w|}}(m) \in [n].$$

Remark 4.13. *It is clear that for all $s \in (\mathfrak{S}_n)^k$, the partition* $\mathrm{Part}(\gamma_s)$ *of level sets of this function is a congruence of $G(\sigma, w)$. It is also clear, by a descending induction on l, that for all $m \neq m' \in [p]$, for all $l \in [|w|]$, $(m, l) \neq (m', l) \mod \mathrm{Part}(\gamma_s)$.*

Lemma 4.14. *Consider a function $\gamma : V \to [n]$ whose level sets partition is a congruence of $G(\sigma, w)$ and such that for all $m = 1, \ldots, p$, $\gamma(m, 1) = \sigma(m)$. For all $s = (s_1, \ldots, s_k) \in (\mathfrak{S}_n)^k$, $\gamma_s = \gamma$ if and only if for all $r = 1, \ldots, k$, for all edge e of $G(\sigma, w)$ with color r,*

$$s_r(\gamma(\mathrm{End}(e))) = \gamma(\mathrm{Beg}(e)). \tag{13}$$

Proof. ($\Rightarrow$) Consider an edge $e = (a_m, l)$ of $G(\sigma, w)$ (with $m \in [p], l \in [|w|]$). Its color is i_l.

- If $\alpha_l = 1$. Then
$$\mathrm{End}(e) = \begin{cases} (m, l+1) & \text{if } l \neq |w| \\ (\sigma^{-1}(m), 1) & \text{if } l = |w| \end{cases}$$
and $\mathrm{Beg}(e) = (m, l)$.
  - If $l = |w|$, then
$$s_{i_l}(\gamma(\mathrm{End}(e))) = s_{i_l}(\gamma(\sigma^{-1}(m), 1)) = s_{i_l}(\sigma(\sigma^{-1}(m))) = s_{i_{|w|}}(m) = \gamma_s(m, |w|) = \gamma(\mathrm{Beg}(e)).$$
  - If $l < |w|$, then
$$s_{i_l}(\gamma(\mathrm{End}(e))) = s_{i_l}(\gamma_s(m, l+1)) = s_{i_l}(s_{i_{l+1}}^{\alpha_{l+1}} \cdots s_{i_{|w|}}^{\alpha_{|w|}}(m))$$
$$= s_{i_l}^{\alpha_l} \cdots s_{i_{|w|}}^{\alpha_{|w|}}(m) = \gamma_s(\mathrm{Beg}(e)) = \gamma(\mathrm{Beg}(e)).$$
- If $\alpha_l = -1$. Then $\mathrm{End}(e) = (m, l)$ and
$$\mathrm{Beg}(e) = \begin{cases} (m, l+1) & \text{if } l \neq |w| \\ (\sigma^{-1}(m), 1) & \text{if } l = |w| \end{cases}$$
  - If $l = |w|$, then
$$s_{i_l}(\gamma(\mathrm{End}(e))) = s_{i_{|w|}}(\gamma_s(m, |w|)) = s_{i_{|w|}}(s_{i_{|w|}}^{-1}(m)) = m = \sigma(\sigma^{-1}(m)) = \gamma(\mathrm{Beg}(e)).$$
  - If $l < |w|$, then
$$s_{i_l}(\gamma(\mathrm{End}(e))) = s_{i_l}(\gamma_s(m, l)) = s_{i_l}(s_{i_l}^{-1} s_{i_{l+1}}^{\alpha_{l+1}} \cdots s_{i_{|w|}}^{\alpha_{|w|}}(m))$$
$$= s_{i_{l+1}}^{\alpha_{l+1}} \cdots s_{i_{|w|}}^{\alpha_{|w|}}(m) = \gamma_s(\mathrm{Beg}(e)) = \gamma(\mathrm{Beg}(e)).$$

($\Leftarrow$) We have to prove that for all $(m, l) \in [p] \times [|w|]$,
$$s_{i_l}^{\alpha_l} \cdots s_{i_{|w|}}^{\alpha_{|w|}}(m) = \gamma(m, l).$$
Let us prove it by descending induction on l.

- If $l = |w|$. We have to prove that
$$s_{i_{|w|}}^{\alpha_{|w|}}(m) = \gamma(m, |w|). \tag{14}$$
  - If $\alpha_{|w|} = 1$, then (14) follows from (13) for $e = (a_m, |w|)$. Indeed,
$$s_{i_{|w|}}^{\alpha_{|w|}}(m) = s_{i_{|w|}}(\sigma(\sigma^{-1}(m))) = s_{i_{|w|}}(\gamma(\sigma^{-1}(m), 1)) = s_{i_{|w|}}(\gamma(\mathrm{End}(e))) = \gamma(\mathrm{Beg}(e)) = \gamma(m, |w|).$$
  - If $\alpha_{|w|} = -1$, then (14) follows again from (13) for $e = (a_m, |w|)$. Indeed,
$$s_{i_{|w|}}^{\alpha_{|w|}}(m) = s_{i_{|w|}}^{-1}(\sigma(\sigma^{-1}(m))) = s_{i_{|w|}}^{-1}(\gamma(\sigma^{-1}(m), 1)) = s_{i_{|w|}}^{-1}(\gamma(\mathrm{Beg}(e))) = \gamma(\mathrm{End}(e)) = \gamma(m, |w|).$$
- Suppose the result to be proved to the rank $l+1 \leq |w|$, and let us prove it to the rank l. We have to prove that
$$s_{i_l}^{\alpha_l} \underbrace{s_{i_{l+1}}^{\alpha_{l+1}} \cdots s_{i_{|w|}}^{\alpha_{|w|}}(m)}_{=\gamma(m,l+1) \text{ by induct. hyp.}} = \gamma(m, l). \tag{15}$$
  - If $\alpha_l = 1$, then (15) follows from (13) for $e = (a_m, l)$.
  - If $\alpha_l = -1$, then for $e = (a_m, l)$,
$$s_{i_l}^{\alpha_l}(\gamma(m, l+1)) = s_{i_l}^{-1}(\gamma(\mathrm{Beg}(e))) = \gamma(\mathrm{End}(e)) = \gamma(m, l).$$

□

Lemma 4.15. *Consider two functions $\gamma, \gamma' : V \to [n]$ such that*

$$\forall m = 1, \dots, p,\ \gamma(m,1) = \gamma'(m,1) = \sigma(m),$$

and $\mathrm{Part}(\gamma) = \mathrm{Part}(\gamma')$*, which is a congruence of $G(\sigma, w)$. Then there is $\tau \in \mathfrak{S}_n$ such that for all $s = (s_1, \dots, s_k) \in (\mathfrak{S}_n)^k$,*

$$\gamma_s = \gamma \iff \gamma_{\tau s \tau^{-1}} = \gamma',$$

where $\tau s \tau^{-1} = (\tau s_1 \tau^{-1}, \dots, \tau s_k \tau^{-1})$.

Proof. Since $\mathrm{Part}(\gamma) = \mathrm{Part}(\gamma')$, we know that there is $\tau \in \mathfrak{S}_n$ such that $\gamma' = \tau \circ \gamma$. Consider first $s \in \mathfrak{S}_n^k$ such that $\gamma_s = \gamma$. We are going to prove that $\gamma_{\tau s \tau^{-1}} = \gamma'$ using the previous lemma. For $r = 1, \dots, k$ and e edge with color r,

$$\tau s_r \tau^{-1}(\gamma'(\mathrm{End}(e))) = \tau s_r(\gamma(\mathrm{End}(e)) = \tau(\gamma(\mathrm{Beg}(e)) = \gamma'(\mathrm{Beg}(e)).$$

So we have $\gamma_{\tau s \tau^{-1}} = \gamma'$. In the same way, one can prove that if $\gamma_{\tau s \tau^{-1}} = \gamma'$, then $\gamma_s = \gamma$. □

4.3.2. *Random permutations.* We fix again, until the end of the proof of proposition 4.16, $k, p \geq 1$, $\sigma \in \mathfrak{S}_p$ and $w \in M_k$. We shall use the notations of section 4.2. We also fix $A_1, \dots, A_k$ non empty sets of positive integers (non of them being $\{1\}$), such that for all i, A_i is either finite or satisfies $\sum_{\substack{j \geq 1 \\ j \notin A_i}} \frac{1}{j} < \infty$.

For all n such that $\mathfrak{S}_n^{(A_1)}, \dots, \mathfrak{S}_n^{(A_k)}$ are all non empty, we consider an independent family $s_1(n), \dots, s_k(n)$ of random permutations chosen uniformly in respectively $\mathfrak{S}_n^{(A_1)}, \dots, \mathfrak{S}_n^{(A_k)}$ and define $\sigma_n = w(s_1(n), \dots, s_k(n))$.

Proposition 4.16. *The probability of the event*

$$\{\forall m = 1, \dots, p, \sigma_n(m) = \sigma(m)\} \tag{16}$$

is equivalent, as n goes to infinity in such a way that $\mathfrak{S}_n^{(A_1)}, \dots, \mathfrak{S}_n^{(A_k)}$ are all non empty, to

$$\frac{1}{n^p} \sum_{\Delta \in C(\sigma, w, A_1, \dots, A_k)} n^{\chi(G(\sigma,w)/\Delta)}, \tag{17}$$

where $C(\sigma, w, A_1, \dots, A_k)$ is the set of $(A_1, \dots, A_r)$-congruences Δ of $G(\sigma, w)$ such that for all $m \neq m' \in [p]$, $(m,1) \neq (m',1) \mod \Delta$.

Proof. We have seen at remark 4.13 that for all $s \in (\mathfrak{S}_n)^k$, the partition $\mathrm{Part}(\gamma_s)$ of level sets of the function

$$\gamma_s : (m,l) \in V \mapsto s_{i_l}^{\alpha_l} \cdots s_{i_{|w|}}^{\alpha_{|w|}}(m) \in [n]$$

is a congruence of $G(\sigma, w)$. Moreover, for all $s \in (\mathfrak{S}_n)^k$, one has

$$\forall m = 1, \dots, p, \quad w(s)(m) = \sigma(m) \iff \gamma_s(m,1) = \sigma(m),$$

which implies that that for all $m \neq m' \in [p]$, $(m,1) \neq (m',1) \mod \mathrm{Part}(\gamma_s)$.

Hence the probability of the event

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

is the sum, over all functions $\gamma : V \to [n]$ whose level set partition is a congruence and who satisfy $\gamma(m,1) = \sigma(m)$ for all $m \in [p]$, of the probability that $\gamma_{s_1(n), \dots, s_k(n)} = \gamma$.

Now, note that for all $r = 1, \dots, k$, the distribution of $s_r(n)$ is invariant under conjugation by any permutation, hence since the distribution of $(s_1(n), \dots, s_k(n))$ is the tensor product of the distributions of the $s_r(n)$'s, for all $\tau \in \mathfrak{S}_n$, the distribution of $(s_1(n), \dots, s_k(n))$ is the same as the one of $(\tau s_1(n)\tau^{-1}, \dots, \tau s_k(n)\tau^{-1})$. Hence by lemma 4.15, for all function $\gamma : V \to [n]$ whose level set partition is a congruence and who satisfies $\gamma(m, 1) = \sigma(m)$ for all $m \in [p]$, the probability that $\gamma_{s_1(n),\dots,s_k(n)} = \gamma$ only depends on the partition of level sets of $\gamma_{s_1(n),\dots,s_k(n)}$.

Hence probability of the event

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

is the sum, over all congruences Δ of $C(\sigma, w)$, of the number of functions $\gamma : V \to [n]$ whose level set partition is Δ and who satisfy $\gamma(m, 1) = \sigma(m)$ for all $m \in [p]$, times the probability that $\gamma_{s_1(n),\dots,s_k(n)}$ is a certain (fixed, but the choice is irrelevant) of these functions. Note that for Δ congruence of $C(\sigma, w)$, the number of such functions is

$$\begin{cases} n(n-1)\cdots(n-|\Delta|+p+1) & \text{if } \forall m \neq m' \in [p], (m,1) \neq (m',1) \mod \Delta, \\ 0 & \text{in the other case,} \end{cases}$$

and that by lemma 4.14, the probability that $\gamma_{s_1(n),\dots,s_k(n)}$ is a certain (fixed) of these functions is

$$\begin{cases} \prod_{r=1}^{k} p_n^{(A_r)}((G(\sigma, w)/\Delta)[r]) & \text{if for all } r \in [k], \text{ all loops of } (G(\sigma, w)/\Delta)[r] \text{ have length in } A_r \text{ and} \\ & \text{all strings of } (G(\sigma, w)/\Delta)[r] \text{ have length} < \sup A_r, \\ 0 & \text{in the other case.} \end{cases}$$

So by definition of $C(\sigma, w, A_1, \dots, A_k)$, the probability of the event

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

is equal to

$$\sum_{\Delta \in C(\sigma, w, A_1, \dots, A_k)} n(n-1)\cdots(n-|\Delta|+p+1) \prod_{r=1}^{k} p_n^{(A_r)}((G(\sigma, w)/\Delta)[r]).$$

Theorem 3.1 allows us to claim that it is equivalent, as n goes to infinity, to

$$\frac{1}{n^p} \sum_{\Delta \in C(\sigma, w, A_1, \dots, A_k)} n^{|\Delta|} \prod_{r=1}^{k} n^{\left\{ -|\{\text{edges of } (V/\Delta)[r]\}| + \sum_{L \text{ loop of } (V/\Delta)[r]} \frac{\text{length of } L}{\sup A_r} \right\}}$$

□

The following result is a direct application of theorem 2.5 applied with A equal to the set of all positive integers and of proposition 4.16.

Corollary 4.17. *If w is such that for all $p \geq 1$, for all $\sigma \in \mathfrak{S}_p$, for all $\Delta \in C(\sigma, w, A_1, \dots, A_k)$, one has $\chi(G(\sigma, w)/\Delta) \leq 0$, with equality for exactly one $\Delta \in C(\sigma, w, A_1, \dots, A_k)$, then for all $l \geq 1$, the law of $(N_1(\sigma_n), \dots, N_l(\sigma_l))$ converges weakly, as n goes to infinity in such a way that $\mathfrak{S}_n^{(A_1)}$, …, $\mathfrak{S}_n^{(A_k)}$ are all non empty, to*

$$\text{Poiss}(1/1) \otimes \cdots \otimes \text{Poiss}(1/l).$$

Remark 4.18. *The hypothesis of this corollary do not always hold: as an example, suppose that* $w = g_1^4 g_2^5$*, with* $A_1 = \{4,5\}$*,* $A_2 = \{5,6\}$*. Then for* $p = 1$ *and* $\sigma = Id$*, in the graph* $G(w)$*, the partition which only links* 1 *and* 5 *has characteristic* $8 - 9 + 4/5 + 5/6 > 0$*. Since, as noticed in remark 2.6, we do not know if theorem 2.5 has an inverse implication, we cannot conclude that the conclusion of the corollary is false in this case. However, remark 5.2, applied for this word* w *and* $l = 1$*, allows us to claim that the expectation of the number of fixed points of* σ_n *tends to infinity as* n *goes to infinity.*

5. Main results about words in random permutations

We fix, until the end of section 5, $k \geq 1$ and $w \in M_k$. We also fix $A_1, \ldots, A_k$ non empty sets of positive integers (non of them being $\{1\}$), such that for all i, A_i is either finite or satisfies $\sum_{\substack{j \geq 1 \\ j \notin A_i}} \frac{1}{j} < \infty$. For all n such that $\mathfrak{S}_n^{(A_1)}, \ldots, \mathfrak{S}_n^{(A_k)}$ are all non empty, we consider an independent family $s_1(n), \ldots, s_k(n)$ of random permutations chosen uniformly in respectively $\mathfrak{S}_n^{(A_1)}, \ldots, \mathfrak{S}_n^{(A_k)}$ and define $\sigma_n = w(s_1(n), \ldots, s_k(n))$. We are going to study the limit behavior of the random variables $N_l(\sigma_n)$ as n goes to infinity (recall that $N_l(\sigma_n)$ denotes the number of cycles of length l in the cycle decomposition of σ_n).

5.1. **Existence of cycles of most lengths.** The first interesting fact is that even though the lengths of the cycles of the letters of $w(s_1(n), \ldots, s_k(n))$ are supposed to belong to the specific sets $A_1, \ldots, A_k$ of positive integers, in many cases, these cycles are going to mix enough to give birth to cycles of any length, at least as much as in a uniform random permutation. We are going to detail more this idea in the following, but we can give a first surprising result of this kind.

Theorem 5.1. *Suppose that the canonical right* $(d_1, \ldots, d_k)$*-cyclic reduction* w' *of* w *is not the empty word.*
(a) If w' *is not of the type* g_i^α*, with* $i \in [k]$*,* $\alpha \neq 0$*, then for all* $l \geq 1$*, as* n *goes to infinity in such a way that for all* $r = 1, \ldots, k$*,* $\mathfrak{S}_n^{(A_r)} \neq \emptyset$*,*

$$\liminf \mathbb{E}(N_l(\sigma_n)) \geq \frac{1}{l}.$$

(b) If w' *is of the type* g_i^α*, with* $i \in [k]$*,* $\alpha \neq 0$*, then for all* $l \geq 1$ *such that* $|\alpha| l \in A_i$*, as* n *goes to infinity in such a way that for all* $r = 1, \ldots, k$*,* $\mathfrak{S}_n^{(A_r)} \neq \emptyset$*,*

$$\liminf \frac{\mathbb{E}(N_l(\sigma_n))}{n^{|\alpha| l / d_i}} \geq \frac{1}{l}.$$

Remark 5.2. *In fact, we prove the more general result: for all* $\Delta \in C(c_l, w, A_1, \ldots, A_k)$*,*

$$\liminf \frac{\mathbb{E}(N_l(\sigma_n))}{n^{\chi(G(c_l, w)/\Delta)}} \geq \frac{1}{l},$$

with $c_l := (1 \cdots l)$*.*

Proof. We have

$$\mathbb{E}(N_l(\sigma_n)) = \frac{1}{l} \mathbb{E}\left(\sum_{i=1}^n 1_{i \text{ belongs to a cycle of length } l} \right) = \frac{1}{l} \sum_{i=1}^n P(\{i \text{ belongs to a cycle of length } l\}).$$

But in the last sum, all terms are equal, since the law of σ_n is invariant under conjugation. Moreover, by this invariance principle again, each term is equal to the number of cycles of length l containing 1 times the probability that σ_n contains the cycle $c_l := (1 \cdots l)$. So

$$\begin{aligned}\mathbb{E}(N_l(\sigma_n)) &= \frac{n}{l}\binom{n}{l-1}(l-1)!P(\{\forall m = 1,\dots,l-1, \sigma_n(m) = m+1, \sigma_n(l) = 1\}) \\ &\sim \frac{n^l}{l}P(\{\forall m = 1,\dots,l-1, \sigma_n(m) = m+1, \sigma_n(l) = 1\}).\end{aligned}$$

Now we are going to use proposition 4.16 for $p = l$ and $\sigma = c_l$. This proposition allows us to claim that for all $\Delta \in C(c_l, w, A_1, \dots, A_k)$,

$$\liminf \frac{\mathbb{E}(N_l(\sigma_n))}{n^{\chi(G(c_l,w)/\Delta)}} \geq \frac{1}{l}.$$

Then corollary 4.12 allows us to conclude. □

5.2. **Case when all A_i's are infinite.** Note first that the random variables $N_l(\sigma_n)$ do not change if w is replaced by its reduction (i.e. by the unique reduced word which represents the same element in the free group with generators $g_1, \dots, g_k$), hence one can suppose w to be reduced. Note also that the number of cycles of a given length of a permutation is the same as the one of any other permutation in the same conjugation class, so, by section 4.1.1, one can suppose w to be cyclically reduced. Note at moreover that the cycle decomposition of a power of a permutation can be deduced from the cycle decomposition of the permutation itself, so, since any cyclically reduced word is a power of a primitive word, we are also going to suppose that w is primitive. Note at last that the case where $|w| = 1$ has already been treated in section 3.3, so we are going to suppose that $|w| > 1$.

To sum up, in the following theorem, w is a primitive word with length > 1.

Theorem 5.3. *Suppose all A_i's to be infinite. Then as n goes to infinity in such a way that for all $r = 1, \dots, k$, $\mathfrak{S}_n^{(A_r)} \neq \emptyset$, for all $l \geq 1$, the law of $(N_1(\sigma_n), \dots, N_l(\sigma_l))$ converges weakly to*

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

Proof. This result is a direct consequence of corollary 4.17. Note first that since all A_i's are infinite, for all i, $d_i = \infty$. Hence for all $p \geq 1$, for all $\sigma \in \mathfrak{S}_p$, for all Δ congruence of $G(\sigma, w)$, $\chi(G(\sigma, w)/\Delta)$ is the number of classes of Δ minus the number of edges of $G(\sigma, w)/\Delta$, hence isn't positive by theorem 4.7. This theorem also says that there is only one congruence Δ of $G(\sigma, w)$ for which we have equality, it is the singletons partition. It remains only to prove that the singletons partition is in $C(\sigma, w, A_1, \dots, A_k)$, i.e. that for all $r \in [k]$, all loops of $G(\sigma, w)[r]$ have length in A_r. It is immediate since there is no loop in $G(\sigma, w)[r]$. Indeed, by lemma 4.6, $G(\sigma, w)[r]$ is a disjoint union of graphs of the type $G(w^d)[r]$ (with $d \geq 1$), and since $|w| > 1$ and w is cyclically reduced, the letters of w are not all the same and there is no loop in $G(w^d)[r]$. □

5.3. **Case where $w = g_1 \cdots g_k$.** Now, we are not going to make the hypothesis that all A_i's are infinite anymore, but we are going to suppose that w is a particular word: $w = g_1 \cdots g_k$, with $k \geq 2$. We have another little restriction: in the case where $k = 2$ (i.e. where we consider the product of an element of $\mathfrak{S}_n^{(A_1)}$ by an element of $\mathfrak{S}_n^{(A_2)}$), we are going to suppose that $A_1 \cup A_2$ is not contained in $\{1, 2\}$. It means that we do not consider the product of two involutions.

Theorem 5.4. *Under this hypothesis, as n goes to infinity in such a way that for all $r = 1, \dots, k$, $\mathfrak{S}_n^{(A_r)} \neq \emptyset$, for all $l \geq 1$, the law of $(N_1(\sigma_n), \dots, N_l(\sigma_l))$ converges weakly to*

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

In order to prove the theorem, we shall need the following lemmas.

Lemma 5.5. *Let $\mathcal{X}$ be a finite set, let $\mathcal{B}$ be a set of subsets of $\mathcal{X}$ which have all cardinality 2. Let Δ be a partition of $\mathcal{X}$ such that for all $\{x, y\} \in \mathcal{B}$, $x = y \mod \Delta$. Then we have $|\Delta| \leq |\mathcal{X}| - |\mathcal{B}|$.*

Proof. Let us define a partition Γ of $\mathcal{X}$ by

$$\Gamma = \mathcal{B} \cup \{\{z\}\,;\, z \in \mathcal{X}, z \notin \cup_{\{x,y\} \in \mathcal{B}} \{x, y\}\}.$$

By hypothesis, any class of Δ is a union of classes of Γ, so $|\Delta| \leq |\Gamma| = |\mathcal{X}| - |\mathcal{B}|$. □

Let us define, for Δ congruence of an oriented, edge-colored graph G, $\hat{\Delta}$ to be the partition of the set of edges of G defined by

$$\forall e, f \text{ edges of } G,\ [e = f \mod \hat{\Delta}] \Longleftrightarrow [e, f \text{ have the same color and } \mathrm{Beg}(e) = \mathrm{Beg}(f) \mod \Delta].$$

Note that since Δ is a congruence of G, we also have

$$\forall e, f \text{ edges of } G,\ [e = f \mod \hat{\Delta}] \Longleftrightarrow [e, f \text{ have the same color and } \mathrm{End}(e) = \mathrm{End}(f) \mod \Delta].$$

Remark 5.6. *Note also that there is a canonical bijection between the set of classes of $\hat{\Delta}$ and the set of edges of the graph G/Δ.*

Lemma 5.7. *Consider $w = g_1 \cdots g_k$, with $k \geq 2$, and $\sigma \in \mathfrak{S}_p$, with $p \geq 1$. Let Δ be a congruence of $G(\sigma, w)$ such that for all $i \neq j \in [p]$, $(i, 1) \neq (j, 1) \mod \Delta$. Then*

(i) *the partition $\hat{\Delta}$ of the set of edges of $G(\sigma, w)$ is the singletons partition,*
(ii) *the following inequalities hold:*
   (a) *if $k > 2$, then $|\Delta| \leq pk - \sum_{r=1}^{k} \sum_{\substack{L \text{ loop of} \\ (G(\sigma,w)/\Delta)[r]}} \text{length of } L$,*
   (b) *if $k = 2$, then for all $r = 1, 2$, $|\Delta| \leq pk - \sum_{\substack{L \text{ loop of} \\ (G(\sigma,w)/\Delta)[r]}} \text{length of } L$.*

Proof. Note first that since for all $i \neq j \in [p]$, $(i, 1) \neq (j, 1) \mod \Delta$, and by definition of a congruence, one has (by an obvious induction on l):

$$\forall i \neq j \in [p], \forall l \in [k],\ (i, l) \neq (j, l) \mod \Delta. \tag{18}$$

This implies that

$$\forall i \neq j \in [p], \forall l \in [k],\ (a_i, l) \neq (a_j, l) \mod \hat{\Delta}. \tag{19}$$

Since two edges of $G(\sigma, w)$ linked by $\hat{\Delta}$ must have the same color, it implies (i).

The proofs of both points of (ii) will be applications of the previous lemma. First, note that by the first part of the lemma and remark 5.6, the edges of $(G(\sigma, w))/\Delta$ can be identified with the ones of $G(\sigma, w)$. Let, for $r \in [k]$, $\mathcal{L}[r]$ be the set of edges of $G(\sigma, w)$ which belong to a loop of $(G(\sigma, w)/\Delta)[r]$. Define

$$\mathcal{L} := \cup_{r=1}^{k} \mathcal{L}[r].$$

Note that no edge of $\mathcal{L}$ can belong to more than one loop. Indeed, if it where the case, there would be $r \in [k]$, $e, e', e'' \in \mathcal{L}[r]$ such that e' and e'' both follow e in loops of $(G(\sigma, w)/\Delta)[r]$ and $e' \neq e''$. Since e' and e'' follow e in loops of $(G(\sigma, w)/\Delta)[r]$, we have

$$\mathrm{Beg}(e') = \mathrm{End}(e) = \mathrm{Beg}(e'') \mod \Delta.$$

But $\mathrm{Beg}(e') = \mathrm{Beg}(e'') \mod \Delta$, with the fact that e' and e'' are both of color r, implies that $e' = e'' \mod \Delta$, which implies $e' = e''$ by (i). Contradiction.

So one can define a permutation φ of $\mathcal{L}$ which maps any edge $e \in \mathcal{L}$ to the edge which follows e in the loop e belongs to. Let us define, for $e \in \mathcal{L}$,

$$S(e) := \{\mathrm{End}(e), \mathrm{Beg}(\varphi(e))\} \subset [p] \times [|w|].$$

Note that since $k \geq 2$, for all edge e of $G(\sigma, w)$, the color of e is not the same as has the one of the edge which beginning is the end of e. It allows us to claim that for all $e \in \mathcal{L}$, $|S(e)| = 2$.

For all $e \in \mathcal{L}$, since $\varphi(e)$ follows e in $G(\sigma, w)/\Delta$, we have

$$\mathrm{End}(e) = \mathrm{Beg}(\varphi(e)) \mod \Delta.$$

So, in order to apply the previous lemma, we have to minor the cardinality of

$$\mathcal{A} := \{S(e)\,;\, e \in \mathcal{L}\} \quad \text{(to prove (a))}$$

or, for $r \in [k]$, of

$$\mathcal{A}[r] := \{S(e)\,;\, e \in \mathcal{L},\ e \text{ has color } r\} \quad \text{(to prove (b))}.$$

Consider $e \neq f \in \mathcal{L}$ such that $S(e) = S(f)$. One has either

$$(\mathrm{End}(e), \mathrm{Beg}(\varphi(e))) = (\mathrm{End}(f), \mathrm{Beg}(\varphi(f)))$$

or

$$(\mathrm{End}(e), \mathrm{Beg}(\varphi(e))) = (\mathrm{Beg}(\varphi(f)), \mathrm{End}(f)).$$

But $(\mathrm{End}(e), \mathrm{Beg}(\varphi(e))) = (\mathrm{End}(f), \mathrm{Beg}(\varphi(f)))$ is impossible because two different edges of $G(\sigma, w)$ cannot have the same end, since no letter of w has the exponent -1. So one has $(\mathrm{End}(e), \mathrm{Beg}(\varphi(e))) = (\mathrm{Beg}(\varphi(f)), \mathrm{End}(f))$.

If $k > 2$: let us prove that $S(e) = S(f)$ with $e \neq f$ is impossible. We have $\mathrm{End}(e) = \mathrm{Beg}(\varphi(f))$, so the color following the one of e in the cyclic order $1, 2, \ldots, k, 1, \ldots$ is the one of $\varphi(f)$, i.e. of f. In the same way, the relation $\mathrm{End}(f) = \mathrm{Beg}(\varphi(e))$ implies that the color following the one of f in the same cyclic order is the one of e. To sum up, in this cyclic order, one has the following direct sequence:

$$\ldots, \text{color of } e, \text{color of } f, \text{color of } e, \ldots$$

which s impossible, since $k > 2$.

So the cardinality of $\mathcal{A}$ is the one of $\mathcal{L}$, and the result (a) is an immediate application of the previous lemma, for $\mathcal{X} = [p] \times [|w|]$ and $\mathcal{B} = \mathcal{A}$.

If $k = 2$: We have seen that for $e \neq f$ edges of $G(\sigma, w)$, $S(e) = S(f)$ implies that the end of the edge f is the beginning of the edge $\varphi(e)$. It implies that the color of f is different from the color of $\varphi(e)$, i.e. of e. So for all $r = 1, 2$, the cardinality of $\mathcal{A}[r]$ is the one of $\mathcal{L}[r]$, and the result (b) is an immediate application of the previous lemma, for $\mathcal{X} = [p] \times [|w|]$ and $\mathcal{B} = \mathcal{A}[r]$.

□

Now we are able to prove theorem 5.4.

Proof of the theorem. Again, we are going to apply corollary 4.17. Let us fix $p \geq 1$ and $\sigma \in \mathfrak{S}_p$.

Note that the singletons partition, denoted by Δ_s, is in $C(\sigma, w, A_1, \ldots, A_k)$. Indeed it is a congruence by remarks 4.4 and 4.5. It is an $(A_1, \ldots, A_k)$-congruence because for all $r \in [k]$, since g_r is not the only letter of w, no edge of color r of $G(\sigma, w)$ is followed by an edge of color r, hence there is no string with length > 1 and no loop in $G(\sigma, w)[r]$. At last, we clearly have for all $i \neq j \in [p]$, $(i, 1) \neq (j, 1) \mod \Delta$. Using lemma 4.6, one easily sees that the Neagu characteristic of $G(\sigma, w)$ is 0.

Hence it suffices to prove that for all $\Delta \in C(\sigma, w, A_1, \ldots, A_k)\backslash\{\Delta_s\}$, the Neagu characteristic of $G(\sigma, w)/\Delta$ is negative. Let us fix such a partition Δ. By remark 5.6, we have to prove that

$$|\Delta| < |\hat{\Delta}| - \sum_{r=1}^{k} \sum_{\substack{L \text{ loop of} \\ (G(\sigma,w)/\Delta)[r]}} \frac{\text{length of } L}{d_r}.$$

By (i) of lemma 5.7, $|\hat{\Delta}| = pk$. So we have to prove that

$$|\Delta| < pk - \sum_{r=1}^{k} \sum_{\substack{L \text{ loop of} \\ (G(\sigma,w)/\Delta)[r]}} \frac{\text{length of } L}{d_r}. \tag{20}$$

- If $\sum_{r=1}^{k} \sum_{\substack{L \text{ loop of} \\ (G(\sigma,w)/\Delta)[r]}} \text{length of } L = 0$, then, since $\Delta \neq \Delta_s$, so $|\Delta| < |[p]\times[|w|]| = pk$, and hence (20) holds.
- If $\sum_{r=1}^{k} \sum_{\substack{L \text{ loop of} \\ (G(\sigma,w)/\Delta)[r]}} \text{length of } L > 0$ and $k > 2$, then since for all r, $d_r \geq 2 > 1$, by (ii) (a) of lemma 5.7, (20) holds.
- If $\sum_{r=1}^{k} \sum_{\substack{L \text{ loop of} \\ (G(\sigma,w)/\Delta)[r]}} \text{length of } L > 0$ and $k = 2$. First note that adding (ii) (b) of lemma 5.7 for $r = 1$ and $r = 2$, and then dividing by 2, one gets

$$|\Delta| \leq pk - \frac{1}{2} \sum_{r=1}^{2} \sum_{\substack{L \text{ loop of} \\ (G(\sigma,w)/\Delta)[r]}} \text{length of } L. \tag{21}$$

  By hypothesis, one has either $d_1 > 2$ or $d_2 > 2$. Since both cases can be treated in the same way, we will suppose that $d_1 > 2$. Now, we have to discuss wether there is or not a loop of color 1.

- If there is at least one loop of color 1. Then since $d_1 > 2$, the right hand term of (21) is strictly less than

$$pk - \sum_{r=1}^{2} \sum_{\substack{L \text{ loop of} \\ (G(\sigma,w)/\Delta)[r]}} \frac{\text{length of } L}{d_r},$$

so (20) holds.

- If there is no loop of color 1. Then there is at least one loop of color 2, and, since $d_2 > 1$, the right hand term in (ii) (b) of lemma 5.7 is strictly less than

$$pk - \sum_{\substack{L \text{ loop of} \\ (G(\sigma,w)/\Delta)[2]}} \frac{\text{length of } L}{d_2},$$

which is equal to

$$pk - \sum_{r=1}^{2} \sum_{\substack{L \text{ loop of} \\ (G(\sigma,w)/\Delta)[r]}} \frac{\text{length of } L}{d_r},$$

i.e. to the right hand term of (20). So (20) holds.

□

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.

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

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

[MKS66] Magnus, W. Karass, A. Solitar, D. *Combinatorial group theory.* 1966

[Ne05] Neagu, M. *Asymptotic freeness of random permutation matrices with restricted cycles lengths* arXiv

[Ni94] Nica, A. *On the number of cycles of a given length of a free word in several random permutations.* Random Structures and Algorithms, Vol. 5, No. 5, 703-730, 1994

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