



**HAL**  
open science

# Cycles of free words in several independent random permutations with restricted cycle lengths

Florent Benaych-Georges

► **To cite this version:**

Florent Benaych-Georges. Cycles of free words in several independent random permutations with restricted cycle lengths. 2007. hal-00114382v3

**HAL Id: hal-00114382**

**<https://hal.science/hal-00114382v3>**

Preprint submitted on 12 Dec 2007 (v3), last revised 1 Nov 2010 (v7)

**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 FREE WORDS IN SEVERAL INDEPENDENT RANDOM PERMUTATIONS WITH RESTRICTED CYCLE LENGTHS

FLORENT BENAYCH-GEORGES

ABSTRACT. In this text, extending results of [Ni94, Ne07, BG07], we consider random permutations which can be written as free words in several independent random permutations: we first fix a non trivial word  $w$  in letters  $g_1, g_1^{-1}, \dots, g_k, g_k^{-1}$ , secondly, for all  $n$ , we introduce a family  $s_1(n), \dots, s_k(n)$  of independent random permutations of  $\{1, \dots, n\}$ , and the random permutation  $\sigma_n$  we are going to consider is the one obtained by replacing any letter  $g_i$  in  $w$  by  $s_i(n)$ . As an example, for  $w = g_1 g_2 g_3 g_2^{-1}$ ,  $\sigma_n = s_1(n) \circ s_2(n) \circ s_3(n) \circ s_2(n)^{-1}$ . Moreover, we generalize the problem by allowing to restrict the set of possible lengths of the cycles of the  $s_i(n)$ 's: we fix sets  $A_1, \dots, A_k$  of positive integers and suppose that for all  $n$ , for all  $i$ ,  $s_i(n)$  is uniformly distributed on the set of permutations of  $\{1, \dots, n\}$  which have all their cycle lengths in  $A_i$ . For all positive integer  $l$ , we are going to give asymptotics (as  $n$  goes to infinity) on the number  $N_l(\sigma_n)$  of cycles of length  $l$  of  $\sigma_n$ . We shall even consider the joint distribution of the random vectors  $(N_1(\sigma_n), \dots, N_l(\sigma_n))$ . We first prove that the order of  $w$  in a certain quotient of the free group with generators  $g_1, \dots, g_k$  has an influence on the asymptotics of the random variables  $N_l(n)$  as  $n$  goes to infinity. We also prove that in many cases, the distribution of  $N_l(n)$  converges to a Poisson law with parameter  $1/l$  and that the family of random variables  $(N_1(n), \dots, N_l(\sigma_n))$  is asymptotically independent. We notice the pretty surprising fact that from this point of view, many things happen as if  $\sigma_n$  were uniformly distributed on the  $n$ -th symmetric group.

## CONTENTS

1. Introduction	2
1.1. General introduction	2
1.2. Role played by a quotient of the free group generated by $g_1, \dots, g_k$	3
1.3. Weak limit of the distributions of the $N_l(\sigma_n)$ 's	3
1.4. Comments on these results and open questions	4
1.5. Notations	4
2. Combinatorial preliminaries to the study of words in random permutations	5
2.1. Words and groups generated by relations	5
2.2. Admissible graphs and partitions. Colored graphs associated to words and permutations	6

---

*Date:* December 12, 2007.

*MSC 2000 subject classifications.* primary 20B30, 60B15, 20P05, secondary 60C05.

*Key words.* Random permutation, cycle, random permutation with restricted cycle length, free group.

2.3. Application to words in random permutations	19
3. Main results about words in random permutations	23
3.1. Asymptotic behavior of the random variables $N_l(\sigma_n)$ and quotient of the free group	24
3.2. Case when all $A_i$ 's are infinite	25
3.3. Case where $w = g_1 \cdots g_k$	26
References	37

## 1. INTRODUCTION

**1.1. General introduction.** It is well known that if  $\sigma_n$  is a uniformly distributed random permutation of  $\{1, \dots, n\}$ , then if for all  $l \geq 1$ , one denotes the number of cycles of  $\sigma_n$  with length  $l$  by  $N_l(\sigma_n)$ , the joint distribution of  $(N_1(\sigma_n), N_2(\sigma_n), \dots)$  converges in distribution, as  $n$  goes to infinity, to  $\text{Poisson}(1/1) \otimes \text{Poisson}(1/2) \otimes \cdots$  (see, e.g. [ABT05]). The law of "large cycles" can be recovered using the Poisson-Dirichlet distribution, but in this paper, we are only going to deal with "small cycles", i.e. cycles with a size which doesn't varies with  $n$ .

In [Ni94], Nica was the first to consider the case where  $\sigma_n$  is a free word in several independent random permutations: he fixed  $k \geq 1$  and a free word  $w$  in the letters  $g_1, g_1^{-1}, \dots, g_k, g_k^{-1}$ , he introduced, for all  $n$ , a family  $s_1(n), \dots, s_k(n)$  of independent random permutations uniformly distributed on the  $n$ -th symmetric group, and he proved that under the hypothesis that up to any conjugation,  $w$  is not a power of another word, if one defines  $\sigma_n$  to be the random permutation obtained by replacing any letter  $g_i$  in  $w$  by  $s_i(n)$ , then for all positive integer  $l$ ,  $N_l(\sigma_n)$  converges in distribution, as  $n$  goes to infinity, to a Poisson distribution with mean  $1/l$ . He did not consider to joint distribution of the  $N_l(\sigma_n)$ 's.

Besides, in [BG07], extending results proved by Neagu in [Ne07], the author of the present paper considered random permutations which distribution is not uniform on the whole symmetric group, but on the set of permutations of  $\{1, \dots, n\}$  which have all their cycle lengths in a fixed set  $A$  of positive integers. On one hand, he proved that if  $A$  is finite with greatest element  $d$ , then as  $n$  goes to infinity, such a random permutation tends to get not faraway from having order  $d$ : 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  $n$ . On the other hand, he proved that if  $A$  is infinite, then the order of such a random permutation shall go to infinity as  $n$  does it.

In the present paper, we shall somehow mix both of the previously presented problems: we shall fix  $k \geq 1$ , a free word  $w$  in the letters  $g_1, g_1^{-1}, \dots, g_k, g_k^{-1}$ , and a family  $A_1, \dots, A_k$  of positive integers satisfying a technical assumption<sup>1</sup>. Then for all  $n$  such that it is possible, we shall introduce a family  $s_1(n), \dots, s_k(n)$  of independent random permutations such that for all  $i$ ,  $s_i(n)$  is uniformly distributed on the set of permutations of  $\{1, \dots, n\}$  having all of their cycle lengths in  $A_i$  and define  $\sigma_n$  to be the random permutation obtained by replacing any letter  $g_i$  in  $w$  by  $s_i(n)$ . As an example, for  $w = g_1 g_2 g_3 g_2^{-1}$ ,  $\sigma_n = s_1(n) \circ s_2(n) \circ s_3(n) \circ s_2(n)^{-1}$ .

---

<sup>1</sup>Specifically, we suppose that for all  $i$ ,  $A_i$  is either finite or satisfies  $\sum_{\substack{j \geq 1 \\ j \notin A_i}} \frac{1}{j} < \infty$ , which means that  $A_i$  is either small enough or large enough.

**1.2. Role played by a quotient of the free group generated by  $g_1, \dots, g_k$ .** Since as explained above, for  $i$  such that  $A_i$  is finite,  $s_i(n)$  is not faraway from having order  $d_i := \max A_i$ , whereas for  $i$  such that  $A_i$  is infinite, the order of  $s_i(n)$  shall go to infinity as  $n$  does it, it is natural to expect that for large values of  $n$ , the distribution of  $\sigma_n$  will depend firstly on the word obtained from  $w$  by removing all sequences of the type  $g_i^{\pm d_i}$  for  $i$  such that  $A_i$  is finite. This is what has led us to introduce the group  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$  generated by free elements  $g_1, \dots, g_k$  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). Our more general results, respectively theorems 3.4 and 3.1, are the following ones:

- If the element of  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$  represented by  $w$  has finite order  $d \geq 1$ , then  $N_d(\sigma_n)/n$  converges to  $1/d$  and for all  $l \geq 1$  such that  $l \neq d$ ,  $N_l(\sigma_n)/n$  converges to 0. It means that  $\sigma_n$  is not faraway from having order  $d$ : the cardinality of the subset of  $\{1, \dots, n\}$  covered by the supports of the cycles with length  $d$  in such a random permutation is equivalent to  $n$ .
- If the element of  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$  represented by  $w$  has infinite order, then two cases can occur:
  - (i) The element of  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$  represented by  $w$  is not conjugated to an element represented by a word of the type  $g_i^\alpha$ , with  $i \in [k]$ ,  $\alpha$  integer. Then for all  $l \geq 1$ , as  $n$  goes to infinity,

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

- (ii) There is  $i \in [k]$  such that  $d_i = \infty$  and  $\alpha$  non null integer such that  $w$  represents the same element in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$  as the word  $g_i^\alpha$ . Then for all  $l \geq 1$  such that  $l|\alpha| \in A_i$ ,

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

It means that the cycles of the letters of  $w$  are going to mix in a hieratic enough way to give rise to cycles of most lengths, at least as much as in a uniform random permutation (indeed, if  $\sigma_n$  would have had the uniform distribution on  $\mathfrak{S}_n$ , for all  $l \leq n$ , we would have had  $\mathbb{E}(N_l(\sigma_n)) = 1/l$ ), even when the letters of  $w$  have very restricted cycle lengths.

**1.3. Weak limit of the distributions of the  $N_l(\sigma_n)$ 's.** Then, we are going to prove more precise results: under certain hypothesis on  $w$ , 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

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

just like if the distribution of  $\sigma_n$  would have been uniform on  $\mathfrak{S}_n$ . When all  $A_i$ 's are infinite (case treated in theorem 3.5), our hypothesis, for obtaining such a conclusion, is that  $w$  is neither a single letter nor 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, as explained in the beginning of section 3.2). If some of the  $A_i$ 's are finite, we prove this result for  $w = g_1 \cdots g_k$  (theorem 3.6), with the exception of the case  $k = 2$  and  $A_1 \cup A_2 \subset \{1, 2\}$  (i.e. of the product of two random involutions), where we prove that the  $N_l(\sigma_n)$ 's are still asymptotically independent, but that their asymptotic distributions are slightly different (theorem 3.10).

These 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  $w$ , up to any conjugation, is not a power of another word, for all  $l \geq 1$ , the distribution of  $N_l(\sigma_n)$  converges weakly to Poisson( $1/l$ ) (without considering the joint distribution), and on the other hand a result of M. Neagu, who proved in [Ne07] that the matrices of independent random permutations with restricted cycle lengths 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 these papers, and that we use many of their results.

**1.4. Comments on these results and open questions.** a) In this paper, only small cycles are concerned by our investigations. It would be interesting to know if we have a limit theorem for the whole random partition of  $\{1, \dots, n\}$  defined by the cycles of  $\sigma_n$ . Is it natural to expect a Poisson-Dirichlet distribution (see [P02] or [ABT05]).

b) We had to do several technical hypothesis to prove our results: in all of this paper, each set  $A_i$  is supposed to be either finite or satisfying  $\sum_{\substack{j \geq 1 \\ j \notin A_i}} \frac{1}{j} < \infty$  and in the case where not all the

$A_i$ 's are infinite, the result presented in section 1.3 is only proved when  $w = g_1 \cdots g_k$ . It would be interesting to know if these hypothesis are necessary.

c) In the case where  $\sigma_n$  is the product of two independent involutions (i.e. where  $w = g_1 g_2$  and  $A_1, A_2 \subset \{1, 2\}$ ), a surprising phenomenon appears when these random involutions are allowed to have fixed points (i.e. when  $1 \in A_1 \cup A_2$  and still more when  $1 \in A_1 \cap A_2$ ): while we have proved that in the case of a product of  $k \geq 3$  random permutations of a very general type (including random involutions) or of two random permutations which are not both random involutions, for all  $l$ , the asymptotic mean number of cycles with length  $l$  is  $1/l$  (because  $N_l(\sigma_n)$  has asymptotic distribution Poisson( $1/l$ )), the product of two random involutions has much more cycles of length  $l$ , and the more fixed points these involutions have, the more sharp this phenomenon is (see theorem 3.10). It would be interesting to have an explication for this important difference of behavior.

d) Another pretty interesting question arising from the similarity between  $\sigma_n$  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  $g_1, g_1^{-1}, \dots, g_k, g_k^{-1}$  such that for  $n$  large enough, the random permutation obtained by replacing any letter  $g_i$  of the word  $w$  by  $s_i(n)$  is uniformly distributed, with  $s_1(n), \dots, s_k(n)$  independent family of uniform random permutations in  $\mathfrak{S}_n$ ? This question has an analogue in any compact group, and it would also be interesting to compare the words which are convenient for different groups. There is a pretty obvious sufficient condition:  $w$  is an element of a base of the free group with generators  $g_1, \dots, g_k$ , which is equivalent (see [Ni24]) to the fact that there is a sequence of words  $w_0, w_1, \dots, w_p = w$  such that  $w_0$  is a single letter and for all  $i \in [p]$ ,  $w_i$  a Nielsen motion of  $w_{i-1}$ , where we call a *Nielsen motion* of a word  $u$  any word  $v$  such that there exists  $a, b \in \{g_1, g_1^{-1}, \dots, g_k, g_k^{-1}\}$  which are distinct and not inverse one of each other such that  $v$  can be deduced from  $u$  by replacing the letters  $a, a^{-1}$  every time it appears in  $u$  by respectively  $ab, b^{-1}a^{-1}$ . As an example,  $g_1 g_3 g_2 g_2 g_3 g_1 g_3 g_2 g_3^{-1} g_1^{-1}$  is a Nielsen motion of  $g_1 g_2 g_2 g_3 g_1 g_2 g_1^{-1}$  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.

**1.5. Notations.** In this text, for  $n$  integer, we shall denote by  $[n]$  the set  $\{1, \dots, n\}$  and by  $\mathfrak{S}_n$  the group of permutations of  $[n]$ . For  $A$  set of positive integers,  $\mathfrak{S}_n^{(A)}$  denotes the set of

permutations of  $[n]$  which cycles have length in  $A$ . For  $n$  large enough,  $\mathfrak{S}_n^{(A)}$  is non empty if and only if  $n$  is divided by the greatest common divisor of  $A$  (lemma 2.3 of [Ne07]). For  $\sigma \in \mathfrak{S}_n$  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  $\lambda > 0$ ,  $\text{Poisson}(\lambda)$  will denote the Poisson distribution with parameter  $\lambda$ .

## 2. COMBINATORIAL PRELIMINARIES TO THE STUDY OF WORDS IN RANDOM PERMUTATIONS

### 2.1. Words and groups generated by relations.

2.1.1. *Words.* Let, for  $k \geq 1$ ,  $\mathbb{M}_k$  be the set of *words* in the letters  $g_1, g_1^{-1}, \dots, g_k, g_k^{-1}$ , i.e. the set of sequences  $g_{i_1}^{\alpha_1} \dots g_{i_n}^{\alpha_n}$ , with  $n \geq 0$ ,  $i_1, \dots, i_n \in [k]$ ,  $\alpha_1, \dots, \alpha_n = \pm 1$ . A word  $w \in \mathbb{M}_k$  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 letters are not the inverses one of each other.

As an example, the words  $g_1 g_3 g_3^{-1} g_1, g_1 g_2 g_3 g_1^{-1}, g_1 g_2 g_1^{-1} g_2^{-1}$  are respectively: not reduced, reduced but not cyclically reduced, cyclically reduced.

It is easy to prove that for all  $w \in \mathbb{M}_k$  reduced, there is  $v \in \mathbb{M}_k$  cyclically reduced,  $m \geq 0$ ,  $i_1, \dots, i_m \in [k]$ ,  $\alpha_1, \dots, \alpha_m \in \{1, -1\}$  such that

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

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 easily be proved that any cyclically reduced word is a power of a primitive word.

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

2.1.2. *The quotient of the free group with  $k$  generators by the relations  $g_1^{d_1} = 1, \dots, g_k^{d_k} = 1$ .* Let  $F_k$  be the free group generated by  $g_1, \dots, g_k$ . It is the set of reduced words of  $\mathbb{M}_k$  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  $w, w_0 \in \mathbb{M}_k$  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. As an example,  $g_1 g_3 g_3^{-1} g_1$  is a writing of  $g_1^2$ .

Consider  $d_1, \dots, d_k \in \{2, 3, 4, \dots\} \cup \{\infty\}$ . Let  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$  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  $w \in \mathbb{M}_k$ ,  $w$  is said to *represent* or to be a *writing* of an element  $C$  of  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$  if it is a writing of an element of  $C$  (seen as a subset of  $F_k$  i.e. as a set of reduced words of  $\mathbb{M}_k$ ). As an example, for  $d_1 = 4, d_2 = 5$ ,  $g_1 g_2 g_1^{-1}$  represents the class of  $g_1 g_2^6 g_3 g_1^{-4} g_3^{-1} g_1^{-1}$  in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$ .

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

**Theorem 2.1.** (a) *Any element of  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$  has a writing of the type  $g_{i_1}^{\alpha_1} \dots g_{i_n}^{\alpha_n}$  with  $i_1 \neq i_2 \neq \dots \neq i_n \in [k]$ ,  $\alpha_1, \dots, \alpha_n$  integer numbers such that  $0 < |\alpha_1| < d_{i_1}, \dots, 0 < |\alpha_n| < d_{i_n}$ , and this writing is unique up to replacements of the type*

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

with  $j \in [n]$ .

(b) In any conjugation class of the group  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$ , 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  $g_{i_1}^{\alpha_1} \cdots g_{i_n}^{\alpha_n} \rightarrow g_{i_n}^{\alpha_n} g_{i_1}^{\alpha_1} \cdots g_{i_{n-1}}^{\alpha_{n-1}}$ .

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  $0 < |\alpha_1| < d_{i_1}, \dots$ ,  $0 < |\alpha_n| < d_{i_n}$ . As an example, for  $d_1 = 4, d_2 = 5$ ,  $g_1 g_2 g_3 g_1^3 g_2^{-4}$  is  $(d_1, \dots, d_k)$ -cyclically reduced, whereas  $g_1 g_2 g_3 g_1^3 g_2^{-4} g_1$  isn't.

Consider a cyclically reduced word  $w \in \mathbb{M}_k$ . We shall call a *partial  $(d_1, \dots, d_k)$ -cyclic reduction* of  $w$  a word which can be deduced from  $w$  in a finite number of steps of the following types:

- (a)  $uv \rightarrow vu$ , with  $u, v \in \mathbb{M}_k$ ,
- (b)  $u g_i^{\alpha} u^{-1} v \rightarrow v$ , with  $i \in [k]$ ,  $\alpha$  non null relative integer,  $u$  non empty word and  $v \in \mathbb{M}_k$  cyclically reduced word,
- (c)  $g_i^{\alpha} v \rightarrow v$ , with  $i \in [k]$ ,  $\alpha$  non null relative integer, and  $v$  word which can be written  $v = g_i^{\beta} v'$ , with  $\beta$  integer,  $|\beta| < d_i$  and  $v'$  word which first and last letters do not belong to  $\{g_i, g_i^{-1}\}$ .

A partial  $(d_1, \dots, d_k)$ -cyclic reduction of  $w$  which is  $(d_1, \dots, d_k)$ -cyclically reduced is called a  $(d_1, \dots, d_k)$ -cyclic reduction of  $w$ . In general, there are more than one  $(d_1, \dots, d_k)$ -cyclic reduction of  $w$ , but if there is only one, we call it *the  $(d_1, \dots, d_k)$ -cyclic reduction* of  $w$ .

As an example, for  $d_1 = 4, d_2 = 5$ , the following words are partial  $(d_1, \dots, d_k)$ -cyclic reductions of  $w = g_2^2 g_1 g_2^6 g_3 g_1^{-4} g_3^{-1} g_1^{-1} g_2^3$ :

$$g_1^{-1} g_2^5 g_1 g_2^6 g_3 g_1^{-4} g_3^{-1} g_1^{-1}, \quad g_2^6 g_3 g_1^{-4} g_3^{-1}, \quad g_2 g_3 g_1^{-4} g_3^{-1}, \quad g_3 g_1^{-4} g_3^{-1} g_2, \quad g_2.$$

The last one is a  $(d_1, \dots, d_k)$ -cyclic reduction of  $w$ .

**Remark 2.2.** 1. Note that 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 also  $(d_1, \dots, d_k)$ -cyclically reduced whenever the word is not of the type  $g_i^{\alpha}$ , with  $i \in [k]$ ,  $\alpha \neq 0$  such that  $d_i \leq l|\alpha|$ .  
 3. Note that since in any group with neutral element  $e$ ,  $e$  is the only one to be conjugated  $e$ , a word represents the neutral element in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$  if and only if it has the empty word for  $(d_1, \dots, d_k)$ -cyclic reduction.

## 2.2. Admissible graphs and partitions. Colored graphs associated to words and permutations.

2.2.1. *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  $\text{Beg}(e)$  (resp.  $\text{End}(e)$ ).  $e$  is often denoted by  $u \rightarrow v$ . 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  $v$ . In all this paper, the color set of the edges will always be  $[k]$ , hence it will often be implicate.

A graph  $(V; E_1, \dots, E_k)$  is said to be the *disjoint union* of the graphs  $(V'; E'_1, \dots, E'_k)$  and  $(V''; E''_1, \dots, E''_k)$  if  $V = V' \cup V''$ ,  $E_1 = E'_1 \cup E''_1$ ,  $\dots$ ,  $E_k = E'_k \cup E''_k$  and all these unions are disjoint.

A *subgraph* of a graph  $(V; E_1, \dots, E_k)$  is a graph of the type  $(W; F_1, \dots, F_k)$ , with  $W \subset V$ ,  $F_1 \subset E_1, \dots, F_k \subset E_k$ .

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

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

In this paper, we shall call *oriented graph* an oriented, edge-colored graph where all edges have the same color (which will usually not be specified).

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

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

A *mono-colored loop* (or *string*) of an oriented edge-colored graph is a subgraph which is a loop (or a string) where all edges have the same color.

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 which is connected.

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

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

**2.2.2. Partitions and graphs.** Recall that a *partition*  $\Delta$  of a set  $X$  is a set of pairwise disjoint, non empty subsets of  $X$  (called the *classes* of  $\Delta$ ) which union is  $X$ . In this case, for  $x, y \in X$ ,  $x = y \pmod{\Delta}$  means that  $x, y$  are in the same class of  $\Delta$ . Since  $\Delta$  is a set,  $|\Delta|$  denotes its cardinality.

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

In the section 2.2.1, we introduced the notion of oriented, edge-colored graph with color set  $[k]$ . 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 or the same ending vertex.

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

**Remark 2.3.** Note that clearly, if  $\Delta_1$  is a partition of  $V$  and  $\Delta_2$  is a partition of the vertex set of  $G/\Delta_1$  (which is nothing but the set of classes of the partition  $\Delta_1$ , i.e.  $\Delta_1$  itself !), then the oriented, edge-colored graph  $(G/\Delta_1)/\Delta_2$  is isomorphic to  $G/\Gamma$ , where  $\Gamma$  is the partition of



$V$  such that for all  $x, y \in V$ ,  $x = y \pmod{\Gamma}$  if and only if the classes of  $x$  and  $y$  in  $\Delta_1$  are in the same class of  $\Delta_2$ .

A partition  $\Delta$  of  $V$  is said to be *admissible* if the graph  $G/\Delta$  is admissible, i.e. if for all pair  $(e, f)$  of edges of  $G$ ,

$$\text{Beg}(e) = \text{Beg}(f) \pmod{\Delta} \iff \text{End}(e) = \text{End}(f) \pmod{\Delta}.$$

In this case, even though  $\Delta$  is a partition of the vertex set of  $G$  and not namely of  $G$ , we shall call  $\Delta$  an *admissible partition of  $G$* .

In the following proposition, which proof is obvious, we define the operator  $\text{Adm}$  on the set of oriented edge-colored graphs.

**Proposition 2.4.** *Let  $G$  be an oriented edge-colored graph. Let  $\Delta$  the partition of the vertex set of  $G$  which links two vertices  $r, s$  if and only if there is  $n \geq 0$ , a sequence  $t_0 = r, t_2, \dots, t_n = s$  of vertices of  $G$ , a sequence  $i_1, \dots, i_n$  of colors of  $[k]$ , and a sequence  $\varepsilon_1, \dots, \varepsilon_n$  of "senses" in  $\{\pm 1\}$  such that*

- the reduction of the word  $g_{i_1}^{\varepsilon_1} \dots g_{i_n}^{\varepsilon_n}$  is the empty word,
- for all  $l \in [n]$ , the  $i_l$ -colored edge  $t_{l-1} \rightarrow t_l$  (resp.  $t_{l-1} \leftarrow t_l$ ) belongs to  $G$  if  $\varepsilon_l = 1$  (resp. if  $\varepsilon_l = -1$ ).

Then  $\Delta$  is the minimal partition (with respect to the refinement order)  $P$  such that  $G/P$  is admissible.

With the notations of the previous proposition, the partition  $\Delta$  will be called the *minimal admissible partition* of  $G$  and  $G/P$  will be denoted by  $\text{Adm}(G)$ .

**Remark 2.5.** *Let  $H$  be an oriented edge-colored graph with vertex set  $W$ , and  $G$  be a subgraph of  $H$  with vertex set  $V$ . Then  $\text{Adm}(H)$  is isomorphic to the quotient of the graph obtained from  $\text{Adm}(G)$  by adding the vertices and edges of  $H$  which are not in  $G$  by its the minimal admissible partition. More specifically, if, for each vertex  $v$  of  $G$ , one denotes by  $\bar{v}$  the class of  $v$  in the minimal admissible partition of  $G$ , then  $\text{Adm}(H)$  can be identified, via an isomorphism, to  $\text{Adm}(H')$ , where  $H'$  is the oriented edge-colored graph which vertex set is the union of the vertex set of  $\text{Adm}(G)$  with the set  $W \setminus V$  and which set of edges of color  $i$ , for each  $i \in [k]$ , is the union of the set of edges of color  $i$  of  $\text{Adm}(G)$  with the set*

$$\begin{aligned} & \{w \rightarrow w'; w, w' \in W \setminus V, w \rightarrow w' \text{ } i\text{-colored edge of } H\} \\ & \cup \{\bar{v} \rightarrow w; v \in V, w \in W \setminus V, v \rightarrow w \text{ } i\text{-colored edge of } H\} \\ & \cup \{w \rightarrow \bar{v}; v \in V, w \in W \setminus V, w \rightarrow v \text{ } i\text{-colored edge of } H\}. \end{aligned}$$

**Lemma 2.6.** *Consider an oriented edge-colored graph  $G = (V; E_1, \dots, E_k)$ ,  $r, s, t \in V$ ,  $i \in [k]$  such that  $s \rightarrow t \in E_i$ . Then for  $H$  the oriented edge-colored graph obtained from  $G$  by adding, if it isn't already in  $G$ , the  $i$ -colored edge  $r \rightarrow t$  (resp.  $s \rightarrow r$ ),  $\text{Adm}(H)$  is isomorphic to  $\text{Adm}(G/\{r = s\})$  (resp.  $\text{Adm}(G/\{r = t\})$ ), where for  $u, v \in V$ ,  $\{u = v\}$  denotes the partition of  $V$  which classes are all singletons, except one:  $\{u, v\}$ .*

**Proof.** The proof is immediate with remark 2.3 and the following observation: for  $\Gamma$  admissible partition of  $G$ , if one denotes, for any vertex  $v$  of  $V$ , by  $\bar{v}$  the class of  $v$  in  $\Gamma$ , one has the equivalence:

$$\begin{aligned} \bar{r} = \bar{s} & \iff \bar{r} \rightarrow \bar{t} \text{ is an } i\text{-colored edge of } G/\Gamma \\ (\text{resp. } \bar{r} = \bar{t} & \iff \bar{s} \rightarrow \bar{r} \text{ is an } i\text{-colored edge of } G/\Gamma). \end{aligned}$$

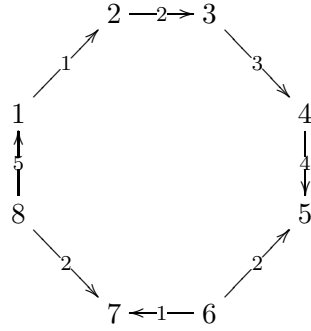
Note that it relies on the admissibility of the partition  $\Gamma$ , i.e. on the admissibility of the graph  $G/\Gamma$ .  $\square$

**2.2.3. The graph  $G(\sigma, w)$ .** Fix  $k, p \geq 1$ ,  $\sigma \in \mathfrak{S}_p$  and  $w = g_{i_1}^{\alpha_1} \cdots g_{i_{|w|}}^{\alpha_{|w|}} \in \mathbb{M}_k$  a non empty word. In [Ni94], Nica defined  $G(\sigma, w)$  (denoted by  $\mathcal{H}_{\sigma^{-1}} \star w$  in his paper) to be the directed, edge-colored 2-regular graph with vertex set  $V := [p] \times [|w|]$  and which edges are the following ones: for all  $(m, l) \in [p] \times [|w|]$ ,

$$\begin{aligned} \alpha_l = 1 &\Rightarrow (m, l) \rightarrow \begin{cases} (m, l+1) & \text{if } l \neq |w|, \\ (\sigma^{-1}(m), 1) & \text{if } l = |w|, \end{cases} \text{ is an } i_l\text{-colored edge of } G(\sigma, w), \\ \alpha_l = -1 &\Rightarrow (m, l) \leftarrow \begin{cases} (m, l+1) & \text{if } l \neq |w|, \\ (\sigma^{-1}(m), 1) & \text{if } l = |w|, \end{cases} \text{ is an } i_l\text{-colored edge of } G(\sigma, w). \end{aligned}$$

In the case where  $p = 1$  and  $\sigma = Id$ , we shall denote  $G(\sigma, w)$  by  $G(w)$  and identify its vertex set with  $[|w|]$  by  $(1, l) \simeq l$  for all  $l \in [|w|]$ . We will also use the convention that if  $w$  is the empty word, then  $G(w)$  is the graph having 1 for only vertex and no edge.

As an example, for  $w = g_1 g_2 g_3 g_4 g_2^{-1} g_1 g_2^{-1} g_5$ ,  $G(w)$  is the graph



where the colors of the edges appear on them. We shall give examples of graphs of the type  $G(\sigma, w)$  after the following lemma.

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  $G(w^\alpha)$ , with  $\alpha \geq 1$ .

**Lemma 2.7.**  $G(\sigma, w)$  is the disjoint union of  $N_1(\sigma)$  graphs isomorphic to  $G(w^1)$ ,  $N_2(\sigma)$  graphs isomorphic to  $G(w^2)$ ,  $\dots$ ,  $N_p(\sigma)$  graphs isomorphic to  $G(w^p)$ .

**Proof.** Let us denote  $G(\sigma, w) = (V; E_1, \dots, E_k)$ . If  $I, J$  are disjoint subsets of  $[p]$  stable by  $\sigma$ , 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  $\sigma$ , 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  $\sigma$  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.  $\square$

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

$$\begin{array}{ccccccccc} (1, 1) & \xrightarrow{-1} & (1, 2) & \xrightarrow{-2} & (1, 3) & \xleftarrow{-1} & (1, 4) & \xleftarrow{-2} & (3, 1) & \xrightarrow{-1} & (3, 2) \\ \downarrow \scriptstyle 2 & & & & & & & & & & \downarrow \scriptstyle 2 \\ (2, 4) & \xrightarrow{-1} & (2, 3) & \xleftarrow{-2} & (2, 2) & \xleftarrow{-1} & (2, 1) & \xrightarrow{-2} & (3, 4) & \xrightarrow{-1} & (3, 3) \end{array}$$

where the colors of the edges appear on them.

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

$$\begin{array}{ccccccc} (4, 1) & \xrightarrow{-1} & (4, 2) & \xrightarrow{-2} & (4, 3) & \xleftarrow{-1} & (4, 4) \\ \downarrow \scriptstyle 2 & & & & & & \uparrow \scriptstyle 2 \\ (5, 4) & \xrightarrow{-1} & (5, 3) & \xleftarrow{-2} & (5, 2) & \xleftarrow{-1} & (5, 1) \end{array}$$

**2.2.4. 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, none of them being  $\{1\}$ . Let us denote  $\sup A_1, \dots, \sup A_k$  by respectively  $d_1, \dots, d_k \in \{2, 3, \dots, +\infty\}$ .

If an oriented, edge-colored graph  $G$  with color set  $[k]$  is admissible and  $r \in [k]$ , since two different  $r$ -colored edges of  $G$  cannot have the same beginning or the same end, it is easy to see that the connected components of the graph deduced from  $G$  by erasing all edges which color is not  $r$  are all either single points, or strings and or loops (see section 2.2.1 for the definitions of strings and loops). If for each  $r \in [k]$ , all these strings have length  $< d_r$  and all these loops 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). A partition  $\Delta$  of the vertex set of an oriented, edge-colored graph  $G$  will be said to be an  $(A_1, \dots, A_k)$ -admissible partition (resp. a  $(d_1, \dots, d_k)$ -strongly admissible partition) if  $G/\Delta$  is  $(A_1, \dots, A_k)$ -admissible (resp.  $(d_1, \dots, d_k)$ -strongly admissible).

**Remark 2.8.** 1. Note that for any word  $w \in \mathbb{M}_k$ ,  $G(w)$  is admissible if and only if  $w$  is cyclically reduced.

2. Note also that for any word  $w \in \mathbb{M}_k$ ,  $G(w)$  is  $(A_1, \dots, A_k)$ -admissible if and only if up to a transformation of the type  $wv \rightarrow vu$ ,  $w$  is  $(d_1, \dots, d_k)$ -cyclically reduced and not of the type  $g_i^\alpha$  with  $i \in [k]$  and  $\alpha$  non null integer such that  $|\alpha| \notin A_i$ .

We define the *Neagu characteristic* of an admissible oriented edge-colored 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  $l/\infty = 0$ . Note that in the case where  $G$  is  $(d_1, \dots, d_k)$ -strongly admissible, its Neagu characteristic is its number of vertices minus its number of edges plus its number of mono-colored cycles.

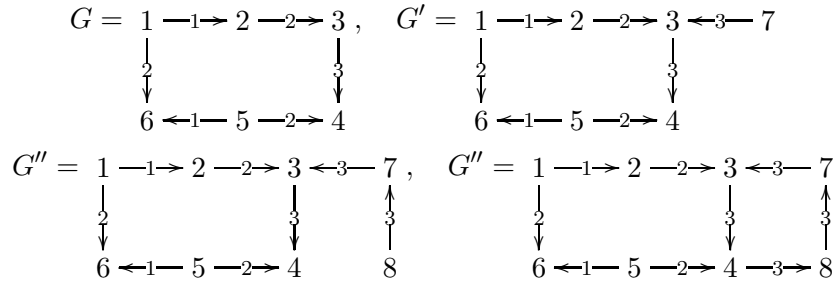
Let  $G = (V; E_1, \dots, E_k)$  be an admissible oriented edge-colored graph. A *direct extension* of  $G$  is a graph  $G'$  of one of the following types:

- $G' = (V \cup \{r\}; E_1, \dots, E_{i-1}, E_i \cup \{s \rightarrow r\}, E_{i+1}, \dots, E_k)$ , with  $r \notin V$ ,  $i \in [k]$ , and  $s \in V$  such that no edge of  $G$  with color  $i$  has  $s$  for beginning vertex,

- $G' = (V \cup \{r\}; E_1, \dots, E_{i-1}, E_i \cup \{r \rightarrow s\}, E_{i+1}, \dots, E_k)$ , with  $r \notin V$ ,  $i \in [k]$ , and  $s \in V$  such that no edge of  $G$  with color  $i$  has  $s$  for ending vertex,
- $G' = (V; E_1, \dots, E_{i-1}, E_i \cup \{r \rightarrow s\}, E_{i+1}, \dots, E_k)$ , with  $i \in [k]$  such that  $d_i < \infty$ ,  $r, s \in V$  such that no edge of  $G$  with color  $i$  has  $r$  for beginning vertex, no edge of  $G$  with color  $i$  has  $s$  for ending vertex, and there exists  $t_1, \dots, t_{d_i} \in V$  pairwise distinct such that  $t_1 = s, t_{d_i} = r$  and  $t_1 \rightarrow t_2, t_2 \rightarrow t_3, \dots, t_{d_i-1} \rightarrow t_{d_i} \in E_i$ .

In other words, a direct extension of  $G$  is an admissible oriented edge-colored graph which can be deduced from  $G$  either by adding a vertex and connecting this vertex to a vertex of  $G$  by an edge of any sense and color, or by adding an edge which closes a loop with color  $i \in [k]$  of length  $d_i$ . In the first case, the direct extension  $G \subset G'$  is said to be *vertex-adding*, whereas in the second one, it is said to be *loop-closing*.

As an exemple, for  $d_3 = 4$ , the graphs  $G, G', G'', G'''$  below (where the colors of the edges appear on them) are such that  $G \subset G' \subset G'' \subset G'''$  are direct extensions, the first ones being vertex-adding, whereas the last one is loop-closing.



An *extension* of  $G$  is an oriented edge-colored graph  $G'$  such that there is  $n \geq 0$ ,  $G_0 = G, \dots, G_n = G'$  such that for all  $i = 1, \dots, n$ ,  $G_i$  is a direct extension of  $G_{i-1}$ . Such an integer  $n$  is unique (it is the number of edges of  $G'$  minus the number of edges of  $G$ ) and will be called the *degree* of the extension.

In other words, an extension of  $G$  is an admissible oriented edge-colored graph which can be deduced from  $G$  by adding successively vertices and/or edges without adding neither any connected component nor any loop except possibly monocolored loops with length equal to  $d_i$ , where  $i$  is the color of the loop.

**Remark 2.9.** *It can easily be proved, using admissibility, that a vertex or an edge of an extension of  $G$  which is not a vertex of  $G$  cannot belong to a loop with color  $i \in [k]$  which length is not equal to  $d_i$ .*

**Lemma 2.10.** *The Neagu characteristic is preserved by extension.*

**Proof.** It suffices to prove that the Neagu characteristic is preserved by direct extension. In the case of a vertex-adding direct extension, it is obvious. In the case where the direct extension is loop-closing, it suffices to notice that the admissibility implies that exactly one mono-colored loop is closed.  $\square$

The following lemma is the key-result of this section. Recall that for  $u, v$  in a set  $V$ ,  $\{u = v\}$  denotes the partition of  $V$  which classes are all singletons, except one:  $\{u, v\}$ .

**Lemma 2.11.** *Consider an oriented edge-colored graph  $G$  which is an extension of the graph  $G(w)$ , with  $w \in \mathbb{M}_k$  cyclically reduced word such that the order, in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$ , of the*

element represented by  $w$  is either infinite or equal to one. Suppose that for a certain  $i \in [k]$  such that  $d_i < \infty$ ,  $G$  contains an  $i$ -colored string  $t_0 \rightarrow t_1 \rightarrow \dots \rightarrow t_{d_i}$  with length  $d_i$ . Then there is a partial  $(d_1, \dots, d_k)$ -reduction  $\tilde{w}$  of  $w$  such that  $\text{Adm}(G/\{t_0 = t_{d_i}\})$  is isomorphic to an extension of  $G(\tilde{w})$ .

Before the proof of the lemma, let us make a remark.

**Remark 2.12.** Note that by definition of the operator  $\text{Adm}$  and by remark 2.3, with the notations of the previous lemma, there is a partition  $\Delta$  of the vertex set of  $G$  such that  $\text{Adm}(G/\{t_0 = t_{d_i}\})$  can be identified to  $G/\Delta$ . Clearly, by definition of  $\{t_0 = t_{d_i}\}$  and of  $\text{Adm}$ , if two vertices of  $r, s$  of  $G$  are in the same class of  $\Delta$ , then there is  $n \geq 0$ , a sequence  $x_0 = r, x_1, \dots, x_n = s$  of vertices of  $G$ , a sequence  $i_1, \dots, i_n$  of colors of  $[k]$ , and a sequence  $\varepsilon_1, \dots, \varepsilon_n$  of "senses" in  $\{\pm 1\}$  such that

- the  $(d_1, \dots, d_k)$ -reduction of the word  $g_{i_1}^{\varepsilon_1} \dots g_{i_n}^{\varepsilon_n}$  is the empty word,
- for all  $l \in [n]$ , the  $i_l$ -colored edge  $x_{l-1} \rightarrow x_l$  (resp.  $x_{l-1} \leftarrow x_l$ ) belongs to  $G$  if  $\varepsilon_l = 1$  (resp. if  $\varepsilon_l = -1$ ).

**Proof of the lemma.** Let us endow the set of pairs of non negative integers with the lexicographic order:

$$(x, y) \preceq (z, t) \iff x < z \text{ or } (x = z \text{ and } y \leq t).$$

Since any non empty set of pairs of non negative integers has a minimum for this order, we can prove the lemma by induction on the pair  $(|w|, n)$  of non negative integers, where  $|w|$  denotes the length of  $w$  and  $n$  denotes the degree of the extension  $G(w) \subset G$ . More specifically, let us prove the following proposition by induction on  $(|w|, n)$ : for all  $w \in \mathbb{M}_k$  cyclically reduced word such that the order, in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$ , of the element represented by  $w$  is either infinite or equal to one, for all extension  $G$  of degree  $n$  of  $G(w)$ , if for a certain  $i \in [k]$  such that  $d_i < \infty$ ,  $G$  contains an  $i$ -colored string  $t_0 \rightarrow t_1 \rightarrow \dots \rightarrow t_{d_i}$  with length  $d_i$ , then  $\text{Adm}(G/\{t_0 = t_{d_i}\})$  is either isomorphic to an extension of  $G(w)$  with degree  $\leq n$  or isomorphic to an extension of  $G(\tilde{w})$  for a certain strict partial  $(d_1, \dots, d_k)$ -reduction  $\tilde{w}$  of  $w$ .

- For  $|w| = 0$  and  $n = 0$ , there is nothing to prove, since when  $n = 0$ ,  $G = G(w)$ , and when  $w$  is the empty word,  $G(w)$  has been defined to be the graph with unique vertex 1 and without any edge, hence  $G(w)$  doesn't contain any string with length  $d_i$  for  $i \in [k]$ .

- Now, let us consider a cyclically reduced word  $w$  such that the order, in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$ , of the element represented by  $w$  is either infinite or equal to one, and an extension  $G$  of  $G(w)$  with degree  $n$  such that  $(0, 0) \prec (|w|, n)$ , and let us suppose the result to be proved for any word  $w'$  and any extension  $G(w') \subset G'$  with degree  $n'$  such that  $(|w'|, n') \prec (|w|, n)$ . Suppose that  $G$  contains an  $i$ -colored string  $t_0 \rightarrow t_1 \rightarrow \dots \rightarrow t_{d_i}$  with length  $d_i$ .

- If the degree  $n$  of the extension  $G$  of  $G(w)$  is 0, then  $G = G(w)$ , and up to a cyclic permutation of the letters of  $w$  (which, up to an isomorphism, does not change  $G(w)$ ), one can suppose that one of the following cases occurs:

Case 1:  $w = ug_i^{\alpha d_i} u^{-1} \tilde{w}$ , with  $\alpha$  non null relative integer,  $u$  non empty word and  $\tilde{w} \in \mathbb{M}_k$  cyclically reduced word, and there is an integer  $j$ ,  $1 + |u| \leq j \leq 1 + |u| + (|\alpha| - 1)d_i$ , such that

$$\begin{cases} t_0 = j, t_1 = j + 1, \dots, t_{d_i} = j + d_i & \text{if } \alpha > 0, \\ t_0 = j + d_i, t_1 = j + d_i - 1, \dots, t_{d_i} = j & \text{if } \alpha < 0. \end{cases}$$

Case 2:  $w = g_i^{\alpha d_i} \tilde{w}$ , with  $\alpha$  non null relative integer and  $\tilde{w}$  word which can be written  $\tilde{w} = g_i^\beta v$ , with  $\beta$  integer,  $|\beta| < d_i$  and  $v$  non empty (except possibly if  $\beta = 0$ ) word which first and last letters do not belong to  $\{g_i, g_i^{-1}\}$ , and there is an integer  $j$ ,  $1 \leq j \leq 1 + (|\alpha| - 1)d_i + |\beta|$ , such that

$$\begin{cases} t_0 = j, t_1 = j + 1, \dots, t_{d_i} = j + d_i & \text{if } \alpha > 0, \\ t_0 = j + d_i, t_1 = j + d_i - 1, \dots, t_{d_i} = j & \text{if } \alpha < 0. \end{cases}$$

Note that in both cases,  $\tilde{w}$  is a strict partial  $(d_1, \dots, d_k)$ -reduction of  $w$ . We are going to prove that  $\text{Adm}(G(w)/\{t_0 = t_{d_i}\})$  is isomorphic to an extension of  $G(\tilde{w})$ .

In the case 1, let us denote  $u = g_{i_1}^{\varepsilon_1} \dots g_{i_{|u|}}^{\varepsilon_{|u|}}$ , with  $i_1, \dots, i_{|u|} \in [k]$ ,  $\varepsilon_1, \dots, \varepsilon_{|u|} \in \{\pm 1\}$ . Let us define the sequence of direct extensions (all of them being vertex-adding, except the last one, which is loop-closing)  $G(\tilde{w}) = G_0 \subset G_1 \subset \dots \subset G_{|u|+d_i}$  in the following way (for notations, we consider a copy  $1', 2', \dots$  of the set of positive integers):

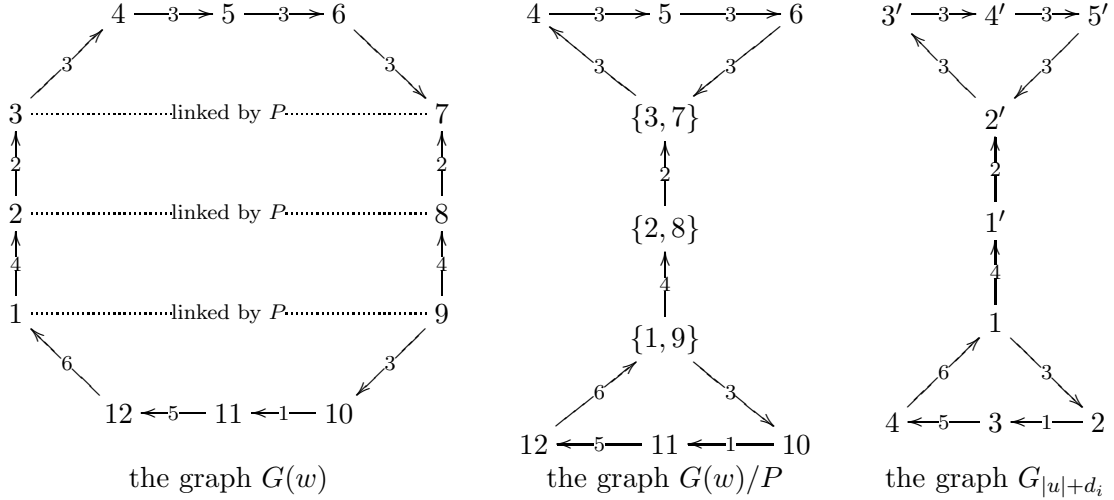
- 1) First add the vertex  $1'$  and the  $i_1$ -colored edge  $1 \rightarrow 1'$  or  $1 \leftarrow 1'$  according to whether  $\varepsilon_1 = 1$  or  $-1$ . It is actually a direct extension because since  $w$  is cyclically reduced, we know that if the last (resp. first) letter of  $\tilde{w}$  is  $g_{i_1}^\varepsilon$  with  $\varepsilon \in \{\pm 1\}$ , then  $\varepsilon = \varepsilon_1$  (resp.  $-\varepsilon_1$ ).
- 2) Then add the vertex  $2'$  and the  $i_2$ -colored edge  $1' \rightarrow 2'$  or  $1' \leftarrow 2'$  according to whether  $\varepsilon_2 = 1$  or  $-1$ . It is actually a direct extension because since  $w$  is cyclically reduced, we know that if  $i_1 = i_2$ , then  $\varepsilon_1 = \varepsilon_2$ .
- $\vdots$
- $|u|$ ) Then add the vertex  $|u|'$  and the  $i_{|u|}$ -colored edge  $(|u| - 1)' \rightarrow |u|'$  or  $(|u| - 1)' \leftarrow |u|'$  according to whether  $\varepsilon_{|u|} = 1$  or  $-1$ . It is actually a direct extension because since  $w$  is cyclically reduced, we know that if  $i_{|u|-1} = i_{|u|}$ , then  $\varepsilon_{|u|-1} = \varepsilon_{|u|}$ .
- $|u| + 1$ ) Then add the vertex  $(|u| + 1)'$  and the  $i$ -colored edge  $|u|' \rightarrow (|u| + 1)'$ . It is actually a direct extension because we know that  $i_{|u|} \neq i$ : indeed,  $w$  is cyclically reduced, and in one hand, the letter  $g_{i_{|u|}}^{\varepsilon_{|u|}}$  appears in before  $g_i^{\alpha d_i}$  in  $w$ , whereas in the other hand, the letter  $g_{i_{|u|}}^{-\varepsilon_{|u|}}$  appears in after  $g_i^{\alpha d_i}$  in  $w$ .
- $|u| + 2$ ) Then add the vertex  $(|u| + 2)'$  and the  $i$ -colored edge  $(|u| + 1)' \rightarrow (|u| + 2)'$ . It is clearly a direct extension.
- $\vdots$
- $|u| + d_i - 1$ ) Then add the vertex  $(|u| + d_i - 1)'$  and the  $i$ -colored edge  $(|u| + d_i - 2)' \rightarrow (|u| + d_i - 1)'$ . It is clearly a direct extension.
- $|u| + d_i$ ) Then add the  $i$ -colored edge  $(|u| + d_i - 1)' \rightarrow |u|'$ . It is actually a (loop-closing) direct extension because as explained at the  $|u| + 1$ th step,  $i_{|u|} \neq i$ .

Claim: the last graph of this sequence of direct extensions, namely  $G_{|u|+d_i}$ , is isomorphic to  $\text{Adm}(G(w)/\{t_0 = t_{d_i}\})$ . To prove it, let us first notice that by remark 2.3,  $\text{Adm}(G/\{t_0 = t_{d_i}\})$  is isomorphic to  $G(w)/P$ , where  $P$  is the partition of the vertex set of  $G$  which classes are singletons, except that:

- In the " $g_i^{\alpha d_i}$  part" of  $G(w)$ , vertices are linked every  $d_i$  edges. More specifically, for all  $x, y \in \{|u| + 1, \dots, |u| + |\alpha|d_i + 1\}$ ,  $x \stackrel{P}{\sim} y$  if and only if  $x = y \pmod{d_i}$ .

- In the " $ug_i^{\alpha d_i}u^{-1}$  part" of  $G(w)$ , symmetric vertices of "the  $u$  and  $u^{-1}$  parts" are linked by  $P$ . More specifically,  $1 \stackrel{P}{\sim} 2|u| + |\alpha|d_i + 1, 2 \stackrel{P}{\sim} 2|u| + |\alpha|d_i, 3 \stackrel{P}{\sim} 2|u| + |\alpha|d_i - 1, \dots, |u| \stackrel{P}{\sim} |u| + |\alpha|d_i + 2$ .

As an illustration, we draw the graphs  $G(w)$ ,  $G(w)/P$  and  $G_{|u|+d_i}$  for  $w = g_4g_2g_3^4g_2^{-1}g_4^{-1}g_3g_1g_5g_6$  and  $d_3 = 4$  (hence  $u = g_4g_2$ ,  $i = 3$ ,  $\alpha = 1$ ,  $\tilde{w} = g_3g_1g_5g_6$ ), linking by edges of the type  $\cdots$  the vertices of  $G(w)$  which are in the same class of  $P$  (but these edges do not belong to  $G(w)$ ).



Now, to be precise, let us give a bijective map  $\varphi$  from the vertex set of  $G_{|u|+d_i}$  to the one of  $G(w)/P$  which is an isomorphism of edge-colored oriented graphs. First, recall that the vertex set of  $G_{|u|+d_i}$  is

$$[[\tilde{w}]] \cup \{1', \dots, (|u| + d_i - 1)'\}$$

and that the vertex set of  $G(w)/P$  is

$$\begin{aligned} & \{\{1, 2|u| + |\alpha|d_i + 1\}, \{2, 2|u| + |\alpha|d_i\}, \{3, 2|u| + |\alpha|d_i - 1\}, \dots, \{|u|, |u| + |\alpha|d_i + 2\}\} \cup \\ & \quad \{\{|u| + 1 + ld_i; 0 \leq l \leq |\alpha|\}\} \cup \\ & \quad \{\{|u| + 2 + ld_i; 0 \leq l < |\alpha|\}, \dots, \{|u| + d_i + ld_i; 0 \leq l < |\alpha|\}\} \cup \\ & \quad \{\{2|u| + |\alpha|d_i + 2\}, \dots, \{2|u| + |\alpha|d_i + |\tilde{w}|\}\}. \end{aligned}$$

Now,  $\varphi$  is defined by

$$\begin{aligned} \forall x \in [[\tilde{w}]], \quad \varphi(x) &= \begin{cases} \{1, 2|u| + |\alpha|d_i + 1\} & \text{if } x = 1, \\ \{2|u| + |\alpha|d_i + x\} & \text{if } x > 1, \end{cases} \\ \forall x \in [|u| + d_i - 1], \quad \varphi(x') &= \begin{cases} \{x + 1, 2|u| + |\alpha|d_i + 1 - x\} & \text{if } x < |u|, \\ \{|u| + 1 + ld_i; 0 \leq l \leq |\alpha|\} & \text{if } x = |u|, \\ \{x + 1 + ld_i; 0 \leq l < |\alpha|\} & \text{if } x > |u| \text{ and } \alpha > 0, \\ \{2|u| + d_i + 1 - x + ld_i; 0 \leq l < |\alpha|\} & \text{if } x > |u| \text{ and } \alpha < 0. \end{cases} \end{aligned}$$

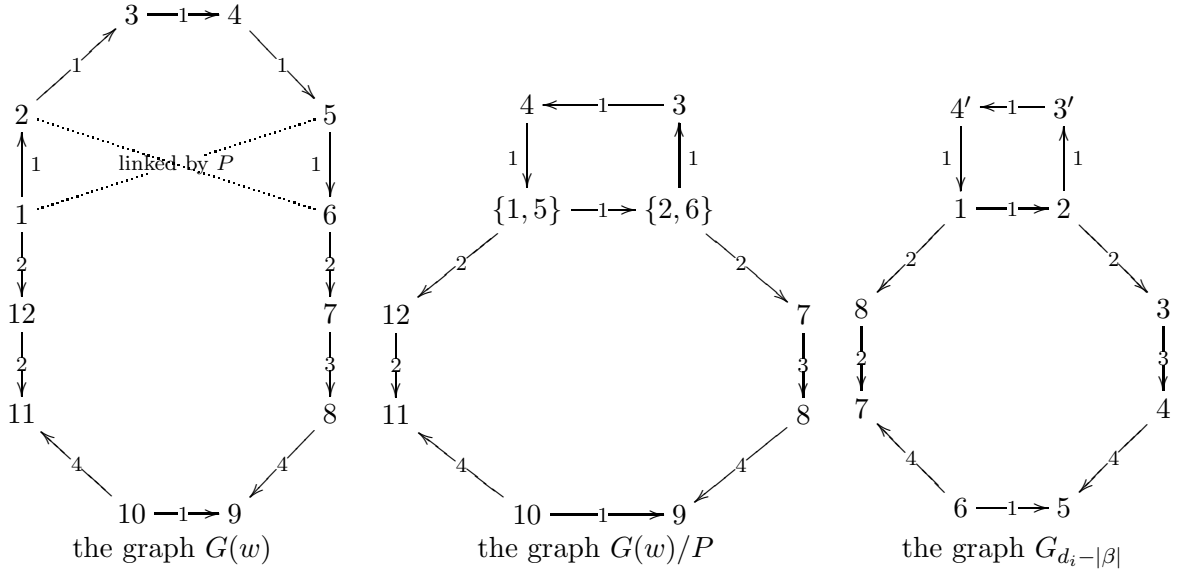
Hence  $G(w)/P$  is isomorphic to an extension of  $G(\tilde{w})$ .

In the case 2, let us define the sequence of direct extensions (all of them being vertex-adding, except the last one, which is loop-closing)  $G(v) = G_0 \subset G_1 \subset \dots \subset G_{d_i - |\beta|}$  in the following way (again, for notations, we consider a copy  $1', 2', \dots$  of the set of positive integers):

- 1) First add the vertex  $(|\beta| + 2)'$  and the  $i$ -colored edge  $|\beta| + 1 \rightarrow (|\beta| + 2)'$  or  $|\beta| + 1 \leftarrow (|\beta| + 2)'$  according to whether  $\beta \geq 0$  or  $< 0$ . It is actually a direct extension because  $v$  is a non empty (except possibly if  $\beta = 0$ ) word which first and last letters do not belong to  $\{g_i, g_i^{-1}\}$ .
- 2) Then add the vertex  $(|\beta| + 3)'$  and the  $i$ -colored edge  $(|\beta| + 2)' \rightarrow (|\beta| + 3)'$  or  $(|\beta| + 2)' \leftarrow (|\beta| + 3)'$  according to whether  $\beta \geq 0$  or  $< 0$ . It is clearly a direct extension.
- $\vdots$
- $d_i - |\beta| - 1$ ) Then add the vertex  $(d_i)'$  and the  $i$ -colored edge  $(d_i - 1)' \rightarrow (d_i)'$  or  $(d_i - 1)' \leftarrow (d_i)'$  according to whether  $\beta \geq 0$  or  $< 0$ . It is clearly a direct extension.
- $d_i - |\beta|$ ) Then add the  $i$ -colored edge  $(d_i)' \rightarrow 1$  or  $(d_i)' \leftarrow 1$  according to whether  $\beta \geq 0$  or  $< 0$ . It is actually a (loop-closing) direct extension because  $v$  is a non empty (except possibly if  $\beta = 0$ ) word which first and last letters do not belong to  $\{g_i, g_i^{-1}\}$ .

Claim: the last graph of this sequence of direct extensions, namely  $G_{d_i - |\beta|}$ , is isomorphic to  $\text{Adm}(G(w)/\{t_0 = t_{d_i}\})$ . To prove it, let us first notice that by remark 2.3,  $\text{Adm}(G/\{t_0 = t_{d_i}\})$  is isomorphic to  $G(w)/P$ , where  $P$  is the partition of the vertex set of  $G$  which classes are singletons, except that in the " $g_i^{\alpha d_i + \beta}$  part" of  $G$ , vertices are linked every  $d_i$  edges (more specifically, for all  $x, y \in [|\alpha d_i + \beta| + 1]$ ,  $x \stackrel{P}{\sim} y$  if and only if  $x = y \pmod{d_i}$ ).

As an illustration, we draw the graphs  $G(w)$ ,  $G(w)/P$  and  $G_{d_i - |\beta|}$ , with  $w = g_1^5 g_2 g_3 g_4 g_1^{-1} g_4 g_2^{-2}$  and  $d_1 = 4$  (hence  $i = 1$ ,  $\alpha = 1$ ,  $\beta = 1$ ,  $\tilde{w} = g_1 g_2 g_3 g_4 g_1^{-1} g_4 g_2^{-2}$ ), linking by edges of the type  $\dots\dots\dots$  the vertices of  $G(w)$  which are in the same class of  $P$  (but these edges do not belong to  $G(w)$ ).



Now, to be precise, let us give a bijective map  $\varphi$  from the vertex set of  $G_{d_i - |\beta|}$  to the one of  $G(w)/P$  which is an isomorphism of edge-colored oriented graphs. First, recall that the vertex set of  $G_{d_i - |\beta|}$  is

$$[|\tilde{w}|] \cup \{(|\beta| + 2)', \dots, (d_i)'\}$$

and that the vertex set of  $G(w)/P$  is

$$\{\{x \in [|\alpha d_i + \beta| + 1]; x = r \pmod{d_i}; r = 1, \dots, d_i\} \cup \{(|\alpha d_i + \beta| + 2)', \dots, (|\alpha d_i + |\tilde{w}|\})'\}$$



(to see why these are actually the vertex sets of the respective graphs and why  $\varphi$  is actually an edge-colored oriented graph isomorphism, recall that since  $w$  is cyclically reduced,  $\alpha$  and  $\beta$  have the same sign when  $\beta$  is non null).

Now,  $\varphi$  is defined by

$$\begin{aligned} \forall r \in [|\beta| + 1], \quad \varphi(r) &= \{x \in [|\alpha d_i + \beta| + 1]; x = r \pmod{d_i}\} \\ \forall r \in \{|\beta| + 2, \dots, d_i\}, \quad \varphi(r') &= \{x \in [|\alpha d_i + \beta| + 1]; x = r \pmod{d_i}\} \\ \forall r \in \{|\beta| + 2, \dots, |\tilde{w}|\}, \quad \varphi(r) &= \{|\alpha|d_i + r\} \end{aligned}$$

•• If the degree  $n$  of the extension  $G$  of  $G(w)$  is  $\geq 1$ , let us introduce a sequence  $G_0 = G(w) \subset G_1 \subset \dots \subset G_n = G$  and again, two cases will be to consider.

••• If  $t_0, \dots, t_{d_i}$  are not all vertices of  $G_{n-1}$ :

Since  $G_n$  is a direct extension of  $G_{n-1}$ , at most one vertex of  $G_n$  is not a vertex of  $G_{n-1}$ , hence exactly one vertex of  $G_n$  is not a vertex of  $G_{n-1}$ . We deduce that the direct extension  $G_{n-1} \subset G_n$  is vertex-adding, and that the vertex added is at the extremity of exactly one edge. Hence this vertex is either  $t_0$  or  $t_{d_i}$ . We suppose that it is  $t_{d_i}$ : the case where it is  $t_0$  can be treated analogously.

- If no  $i$ -colored edge of  $G_{n-1}$  has  $t_0$  for ending vertex, then  $\text{Adm}(G_n/\{t_0 = t_{d_i}\})$  can simply be identified with the graph obtained from  $G_{n-1}$  by adding the  $i$ -colored edge  $t_{d_{i-1}} \rightarrow t_0$ : this graph is a loop-closing direct extension of  $G_{n-1}$ , hence an extension of degree  $n$  of  $G(w)$ , so the result holds.
- If  $t_0$  is the ending vertex of a certain  $i$ -colored edge  $t_{-1} \rightarrow t_0$  of  $G_{n-1}$ , then notice first that by lemma 2.6,  $\text{Adm}(G_n/\{t_0 = t_{d_i}\})$  is isomorphic to  $\text{Adm}(G_{n-1}/\{t_{-1} = t_{d_{i-1}}\})$ . Hence by the induction hypothesis, it suffices to prove that  $t_{-1}, \dots, t_{d_{i-1}}$  are pairwise distinct: if it wasn't the case, since  $t_0, \dots, t_{d_{i-1}}$  are pairwise distinct, then we would have  $t_{-1} = t_l$  for some  $l \in \{0, \dots, d_i - 1\}$ , but it would imply that  $t_l$  is the beginning vertex of two distinct  $i$ -colored edges of  $G_n$  (the edges  $t_{-1} \rightarrow t_0$  and  $t_l \rightarrow t_{l+1}$ ), which is impossible since  $G_n$ , as an extension of  $G(w)$ , is admissible.

••• If  $t_0, \dots, t_{d_i}$  are all vertices of  $G_{n-1}$ :

There will be no ambiguity for us to also denote by  $\{t_0 = t_{d_i}\}$  the restriction of the partition  $\{t_0 = t_{d_i}\}$  to the vertex set of  $G_{n-1}$ . By definition of the operator  $\text{Adm}$  and by remark 2.3, there is a partition  $\Gamma$  of the vertex set of  $G_{n-1}$  such that  $\text{Adm}(G_{n-1}/\{t_0 = t_{d_i}\})$  is isomorphic to  $G_{n-1}/\Gamma$ . Let, for  $x$  vertex of  $G_{n-1}$ ,  $\bar{x}$  denote the class of  $x$  in  $\Gamma$ . We know, by the induction hypothesis, that  $G_{n-1}/\Gamma$  is either isomorphic to an extension of  $G(w)$  with degree  $\leq n - 1$  or isomorphic to an extension of  $G(\tilde{w})$  for a certain strict partial  $(d_1, \dots, d_k)$ -reduction  $\tilde{w}$  of  $w$ . Hence it suffices to prove one of the following properties:

- (P1)  $\text{Adm}(G_n/\{t_0 = t_{d_i}\})$  is isomorphic to  $G_{n-1}/\Gamma$ ,
- (P2)  $\text{Adm}(G_n/\{t_0 = t_{d_i}\})$  is isomorphic to a direct extension of  $G_{n-1}/\Gamma$ ,
- (P3) there is  $j \in [k]$  such that  $d_j < \infty$  and  $G_{n-1}/\Gamma$  contains a  $j$ -colored string with length  $d_j$  and extremity vertices  $x, y$  and such that  $\text{Adm}(G_n/\{t_0 = t_{d_i}\})$  is isomorphic to  $\text{Adm}((G_{n-1}/\Gamma)/\{x = y\})$ .

(The conclusion in the (P3) case requires to use the induction hypothesis again.)

Note that we have the following property:

(Q) for any  $j \in [k]$  such that  $d_j < \infty$ ,  $G(\tilde{w})$  doesn't contain any  $j$ -colored loop.

Indeed, we know that the order of the element of  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$  represented by  $w$  (hence by any partial  $(d_1, \dots, d_k)$ -cyclic reduction of  $w$ ) is either infinite or equal to one, hence none of the partial  $(d_1, \dots, d_k)$ -cyclic reductions of  $w$  is of the type  $g_l^\gamma$  with  $j \in [k]$  such that  $d_j < \infty$  and  $\gamma$  non null integer, and as a consequence, for any partial  $(d_1, \dots, d_k)$ -cyclic reduction  $\tilde{w}$  of  $w$ , for any  $j \in [k]$  such that  $d_j < \infty$ ,  $G(\tilde{w})$  doesn't contain any  $j$ -colored loop.

Now, again, we have two sub-cases to consider:

- If the extension  $G_{n-1} \subset G_n$  is vertex-adding: there is  $j \in [k]$ , a vertex  $r$  of  $G_n$ , a vertex  $s$  of  $G_{n-1}$  such that  $G_n$  can be deduced from  $G_{n-1}$  by the addition of the vertex  $r$  and of the  $j$ -colored edge  $s \rightarrow r$  (or  $r \rightarrow s$ ). Now, if no edge with color  $j$  has  $\bar{s}$  for beginning vertex (or respectively ending vertex) in  $G_{n-1}/\Gamma$ , then by remark 2.5,  $\text{Adm}(G_n/\{t_0 = t_{d_i}\})$  is clearly isomorphic to the vertex-adding direct extension of  $G_{n-1}/\Gamma$  obtained by adding the vertex  $r$  and the edge  $\bar{s} \rightarrow r$  (or respectively  $r \rightarrow \bar{s}$ ). On the other hand, if an edge with color  $j$  has  $\bar{s}$  for beginning vertex (or respectively ending vertex) in  $G_{n-1}/\Gamma$ , then  $\text{Adm}(G_n/\{t_0 = t_{d_i}\})$  is clearly isomorphic to  $G_{n-1}/\Gamma$ . In both cases, (P1) or (P2) holds.
- If the extension  $G_{n-1} \subset G_n$  is loop-closing: there is  $j \in [k]$  such that  $G_n$  can be deduced from  $G_{n-1}$  by adding an edge with color  $j$  between two vertices of  $G_{n-1}$  which are the extremities of a  $j$ -colored string with length  $d_j - 1$ . Let us denote by  $v_1, \dots, v_{d_j}$  the successive vertices of this string: the edge added in the direct extension  $G_{n-1} \subset G_n$  is  $v_{d_j} \rightarrow v_1$ , with color  $j$ . Notice that  $\bar{v}_1, \dots, \bar{v}_{d_j}$  are pairwise distinct vertices of  $G_{n-1}/\Gamma$ . Indeed, if it wasn't the case, since  $G_{n-1}$  contains the  $j$ -colored string  $v_1 \rightarrow \dots \rightarrow v_{d_j}$ ,  $G_{n-1}/\Gamma$  would contain a  $j$ -colored loop with length  $< d_j$ , which is impossible by property (Q) and remark 2.9. Again, two cases will be to consider.
  - a) If no  $j$ -colored edge of  $G_{n-1}/\Gamma$  has  $\bar{v}_{d_j}$  for beginning vertex or  $\bar{v}_1$  for ending vertex: then by remark 2.5,  $\text{Adm}(G_n/\{t_0 = t_{d_i}\})$  is isomorphic to the graph obtained from  $G_{n-1}/\Gamma$  by adding the vertex  $\bar{v}_{d_j} \rightarrow \bar{v}_1$ , which is a loop-closing extension of  $G_{n-1}/\Gamma$ : (P2) holds.
  - b) If a  $j$ -colored edge of  $G_{n-1}/\Gamma$  has  $\bar{v}_{d_j}$  for beginning vertex or  $\bar{v}_1$  for ending vertex. We can suppose that a  $j$ -colored edge of  $G_{n-1}/\Gamma$  has  $\bar{v}_1$  for ending vertex: the other case can be treated analogously. Hence there is a vertex  $V_0$  of  $G_{n-1}/\Gamma$  such that  $G_{n-1}/\Gamma$  contains the  $j$ -colored edge  $V_0 \rightarrow \bar{v}_1$ . Now, notice that by lemma 2.6,  $G_n/\{t_0 = t_{d_i}\}$  is isomorphic to  $(G_{n-1}/\Gamma)/\{\bar{v}_{d_j} = V_0\}$ : (P3) holds.

□

As an immediate consequence, one has the following lemma. It can be proved using remarks 2.3 and 2.12 by induction on the number of  $j$ -colored strings of  $G$  with length  $\geq d_j$ , for  $j \in [k]$ . Note that by remark 2.8, the hypothesis made on the  $(d_1, \dots, d_k)$ -cyclic reductions of  $w$  implies that its order in  $F_f/[g_1^{d_1}, \dots, g_k^{d_k}]$  is either infinite or equal to one, and that for all  $(d_1, \dots, d_k)$ -cyclic reduction  $w_{\text{red}}$  of  $w$ ,  $G(w_{\text{red}})$  is  $(A_1, \dots, A_k)$ -admissible.

**Lemma 2.13.** *Consider a cyclically reduced word  $w \in \mathbb{M}_k$  such that if  $w$  admits a  $(d_1, \dots, d_k)$ -cyclic reduction of the type  $g_i^\alpha$ , with  $i \in [k]$  and  $\alpha$  non null integer, then  $d_i = \infty$  and  $|\alpha| \in A_i$ . Consider an oriented edge-colored graph  $G$  which is an extension of the graph  $G(w)$ . Then  $G$  admits an  $(A_1, \dots, A_k)$ -admissible partition  $\Delta$  such that  $G/\Delta$  is isomorphic to an extension of  $G(w_{\text{red}})$ , for a certain  $(d_1, \dots, d_k)$ -reduction  $w_{\text{red}}$  of  $w$  and such that if two vertices of  $r, s$  of  $G$*

are in the same class of  $\Delta$ , then there is  $n \geq 0$ , a sequence  $t_0 = r, t_2, \dots, t_n = s$  of vertices of  $G$ , a sequence  $i_1, \dots, i_n$  of colors of  $[k]$ , and a sequence  $\varepsilon_1, \dots, \varepsilon_n$  of "senses" in  $\{\pm 1\}$  such that

- the  $(d_1, \dots, d_k)$ -reduction of the word  $g_{i_1}^{\varepsilon_1} \cdots g_{i_n}^{\varepsilon_n}$  is the empty word,
- for all  $l \in [n]$ , the  $i_l$ -colored edge  $t_{l-1} \rightarrow t_l$  (resp.  $t_{l-1} \leftarrow t_l$ ) belongs to  $G$  if  $\varepsilon_l = 1$  (resp. if  $\varepsilon_l = -1$ ).

The previous lemma allows us to prove the following theorem, which is the main result of this section.

**Theorem 2.14.** *Consider a cyclically reduced word  $w = g_{i_1}^{\alpha_1} \cdots g_{i_{|w|}}^{\alpha_{|w|}} \in \mathbb{M}_k$  such that if  $w$  admits a  $(d_1, \dots, d_k)$ -cyclic reduction of the type  $g_i^\alpha$ , with  $i \in [k]$  and  $\alpha$  non null integer, then  $d_i = \infty$  and  $|\alpha| \in A_i$ . Then  $G(w)$  admits an  $(A_1, \dots, A_k)$ -admissible partition  $\Delta$  such that :*

- (i)  $\chi(G(w)/\Delta) = \begin{cases} 1 & \text{if } w \text{ admits the empty word for } (d_1, \dots, d_k)\text{-cyclic reduction,} \\ 0 & \text{in the other case,} \end{cases}$
- (ii) for all  $r < s \in [|w|]$ ,  $r = s \pmod{\Delta}$  implies that one of the words

$$g_{i_r}^{\alpha_r} \cdots g_{i_{s-1}}^{\alpha_{s-1}}, \quad g_{i_s}^{\alpha_s} \cdots g_{i_{|w|}}^{\alpha_{|w|}} g_{i_1}^{\alpha_1} \cdots g_{i_{r-1}}^{\alpha_{r-1}}$$

admits the empty word for  $(d_1, \dots, d_k)$ -cyclic reduction.

**Proof.** Note that by hypothesis, for any  $(d_1, \dots, d_k)$ -cyclic reduction  $w_{\text{red}}$  of  $w$ ,  $G(w_{\text{red}})$  is an  $(A_1, \dots, A_k)$ -admissible graph with Neagu characteristic equal to 1 if the only  $(d_1, \dots, d_k)$ -cyclic reduction of  $w$  is the empty word, and to 0 in the other case. Hence by lemma 2.10, for any partition  $\Delta$  of the vertex set of  $G(w)$ , to have (i), it suffices to prove that  $G(w)/\Delta$  is an extension of  $G(w_{\text{red}})$ . Hence this theorem is an immediate consequence of the previous lemma, applied for  $G = G(w)$ .  $\square$

We shall use the following corollary later. For all  $l \geq 1$ ,  $(1 \cdots l)$  denotes the cyclic permutation of  $[l]$  which maps 1 to 2, 2 to 3, ...,  $l-1$  to  $l$  and  $l$  to 1.

**Corollary 2.15.** *Consider a positive integer  $l$  and a cyclically reduced word  $v \in \mathbb{M}_k$ .*

a) *Suppose that the order, in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$ , of the element represented by  $v$  is infinite and that in the case where  $v$  admits a  $(d_1, \dots, d_k)$ -cyclic reduction of the type  $g_i^\alpha$ , with  $i \in [k]$  and  $\alpha$  integer, then  $l|\alpha| \in A_i$ . Then  $G((1 \cdots l), v)$  admits an  $(A_1, \dots, A_k)$ -admissible partition  $\Delta$  such that :*

- (i)  $\chi(G((1 \cdots l), v)/\Delta) = 0$ ,
- (ii) for all  $m \neq m' \in [l]$ ,  $(m, 1) \neq (m', 1) \pmod{\Delta}$ .

b) *Suppose that the order, in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$ , of the element represented by  $w$  is equal to  $l$ . Then  $G((1 \cdots l), v)$  admits an  $(A_1, \dots, A_k)$ -admissible partition  $\Delta$  such that :*

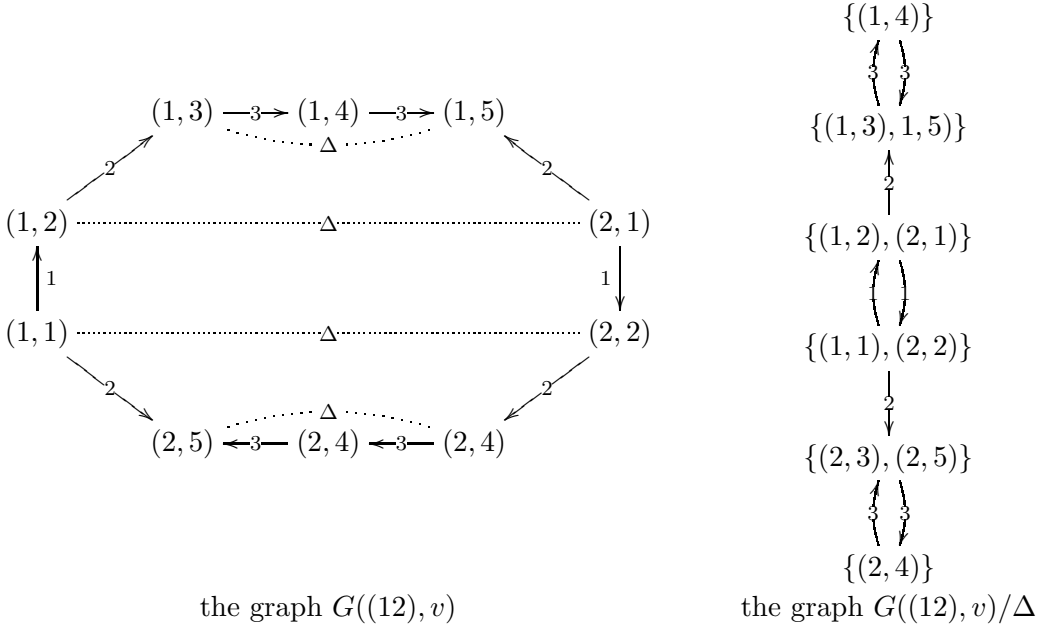
- (i)  $\chi(G((1 \cdots l), v)/\Delta) = 1$ ,
- (ii) for all  $m \neq m' \in [l]$ ,  $(m, 1) \neq (m', 1) \pmod{\Delta}$ .

**Proof.** Note that by lemma 2.7, for all  $l \geq 1$ , the function  $(m, i) \in [l] \times [|v|] \mapsto (l-m)|v| + i \in [l|v|]$  realizes an isomorphism between  $G((1 \cdots l), v)$  and  $G(v^l)$ , hence we are going to work with  $G(v^l)$  instead of  $G((1 \cdots l), v)$  (and the condition "for all  $m \neq m' \in [l]$ ,  $(m, 1) \neq (m', 1) \pmod{\Delta}$ " gets "for all  $m \neq m' \in [l]$ ,  $(m-1)|v| + 1 \neq (m'-1)|v| + 1 \pmod{\Delta}$ "). Then it suffices to apply theorem 2.14.  $\square$

Let us give examples. Consider  $v = g_1 g_2 g_3^2 g_2^{-1}$  with  $d_3 = 2$ . Then in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$ ,  $v$  represents the same element as  $g_1$  hence its order is  $d_1$  (possibly infinite). For  $l = 2$ , the partition

$$\Delta = \{(1, 1), (2, 2)\}, \{(1, 2), (2, 1)\}, \{(1, 3), (1, 5)\}, \{(2, 3), (2, 5)\}, \{(1, 4)\}, \{(2, 4)\}$$

satisfies what is asked in the previous corollary if  $d_1 = \infty$  and  $2 \in A_1$  (case a) or if  $d_1 = 2$  (case b)). Here is an illustration, where in  $G((12), v)$ , vertices linked by  $\Delta$  are linked by edges of the type  $\cdots\Delta\cdots$  (but these edges do not belong to  $G((12), v)$ ).



### 2.3. Application to words in random permutations.

**2.3.1. Admissible partitions of  $G(\sigma, w)$  and permutations.** We fix, until the end of section 2.3.1,  $k, p \geq 1$ ,  $\sigma \in \mathfrak{S}_p$  and  $w = g_{i_1}^{\alpha_1} \cdots g_{i_{|w|}}^{\alpha_{|w|}} \in \mathbb{M}_k$ , with  $i_1, \dots, i_{|w|} \in [k]$  and  $\alpha_1, \dots, \alpha_{|w|} \in \{-1, 1\}$ .

We also define  $V = [p] \times [|w|]$ , fix  $n \geq 1$ , and define, for any  $s = (s_1, \dots, s_k) \in (\mathfrak{S}_n)^k$ , the function

$$\gamma_s : (m, l) \in V \mapsto s_{i_l}^{\alpha_l} \cdots s_{i_1}^{\alpha_1}(m) \in [n].$$

**Lemma 2.16.** *Consider a function  $\gamma : V \rightarrow [n]$  whose level sets partition is an admissible partition of  $G(\sigma, w)$  and such that for all  $m = 1, \dots, p$ ,  $\gamma(m, 1) = \sigma(m)$ . For all  $s = (s_1, \dots, s_k) \in (\mathfrak{S}_n)^k$ ,  $\gamma_s = \gamma$  if and only if for all  $r = 1, \dots, k$ , for all edge  $e$  of  $G(\sigma, w)$  with color  $r$ ,*

$$(1) \quad s_r(\gamma(\text{End}(e))) = \gamma(\text{Beg}(e)).$$

**Proof.**  $(\Rightarrow)$  Consider an edge  $e$  of  $G(\sigma, w)$ . By definition of this graph, there exists  $m \in [p]$ ,  $l \in [|w|]$  such that the edge  $e$  has extremities  $(m, l)$  and either  $(m, l+1)$  or  $(m, \sigma^{-1}(l))$  according to whether  $l < |w|$  or  $l = |w|$ . The color of the edge  $e$  is  $i_l$ .

- If  $\alpha_l = 1$ . Then

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

and  $\text{Beg}(e) = (m, l)$ .

- If  $l = |w|$ , then

$$s_{i_l}(\gamma(\text{End}(e))) = s_{i_l}(\gamma(\sigma^{-1}(m), 1)) = s_{i_l}(\sigma(\sigma^{-1}(m))) = s_{i_{|w|}}(m) = \gamma_s(m, |w|) = \gamma(\text{Beg}(e)).$$

- If  $l < |w|$ , then

$$\begin{aligned} s_{i_l}(\gamma(\text{End}(e))) &= s_{i_l}(\gamma_s(m, l+1)) = s_{i_l}(s_{i_{l+1}}^{\alpha_{l+1}} \cdots s_{i_{|w|}}^{\alpha_{|w|}}(m)) \\ &= s_{i_l}^{\alpha_l} \cdots s_{i_{|w|}}^{\alpha_{|w|}}(m) = \gamma_s(\text{Beg}(e)) = \gamma(\text{Beg}(e)). \end{aligned}$$

- If  $\alpha_l = -1$ . Then  $\text{End}(e) = (m, l)$  and

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

- If  $l = |w|$ , then

$$s_{i_l}(\gamma(\text{End}(e))) = s_{i_{|w|}}(\gamma_s(m, |w|)) = s_{i_{|w|}}(s_{i_{|w|}}^{-1}(m)) = m = \sigma(\sigma^{-1}(m)) = \gamma(\text{Beg}(e)).$$

- If  $l < |w|$ , then

$$\begin{aligned} s_{i_l}(\gamma(\text{End}(e))) &= s_{i_l}(\gamma_s(m, l)) = s_{i_l}(s_{i_l}^{-1} s_{i_{l+1}}^{\alpha_{l+1}} \cdots s_{i_{|w|}}^{\alpha_{|w|}}(m)) \\ &= s_{i_{l+1}}^{\alpha_{l+1}} \cdots s_{i_{|w|}}^{\alpha_{|w|}}(m) = \gamma_s(\text{Beg}(e)) = \gamma(\text{Beg}(e)). \end{aligned}$$

( $\Leftarrow$ ) 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

$$(2) \quad s_{i_{|w|}}^{\alpha_{|w|}}(m) = \gamma(m, |w|).$$

- If  $\alpha_{|w|} = 1$ , then (2) follows from (1) for  $e$  the  $i_{|w|}$ -colored edge  $(m, |w|) \rightarrow (\sigma^{-1}(m), l)$ . Indeed,

$$s_{i_{|w|}}^{\alpha_{|w|}}(m) = s_{i_{|w|}}(\sigma(\sigma^{-1}(m))) = s_{i_{|w|}}(\gamma(\sigma^{-1}(m), 1)) = s_{i_{|w|}}(\gamma(\text{End}(e))) = \gamma(\text{Beg}(e)) = \gamma(m, |w|).$$

- If  $\alpha_{|w|} = -1$ , then (2) follows from (1) for  $e$  the  $i_{|w|}$ -colored edge  $(m, |w|) \leftarrow (\sigma^{-1}(m), l)$ . Indeed,

$$s_{i_{|w|}}^{\alpha_{|w|}}(m) = s_{i_{|w|}}^{-1}(\sigma(\sigma^{-1}(m))) = s_{i_{|w|}}^{-1}(\gamma(\sigma^{-1}(m), 1)) = s_{i_{|w|}}^{-1}(\gamma(\text{Beg}(e))) = \gamma(\text{End}(e)) = \gamma(m, |w|).$$

- 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

$$(3) \quad s_{i_l}^{\alpha_l} \underbrace{s_{i_{l+1}}^{\alpha_{l+1}} \cdots s_{i_{|w|}}^{\alpha_{|w|}}(m)}_{=\gamma(m, l+1) \text{ by induct. hyp.}} = \gamma(m, l).$$

- If  $\alpha_l = 1$ , then (3) follows from (1) for  $e$  the  $i_l$ -colored edge  $(m, l) \rightarrow (m, l+1)$ .

- If  $\alpha_l = -1$ , then for  $e$  the  $i_l$ -colored edge  $(m, l) \leftarrow (m, l + 1)$ ,  
 $s_{i_l}^{\alpha_l}(\gamma(m, l + 1)) = s_{i_l}^{-1}(\gamma(\text{Beg}(e))) = \gamma(\text{End}(e)) = \gamma(m, l)$ .

□

**Lemma 2.17.** *Consider two functions  $\gamma, \gamma' : V \rightarrow [n]$  such that*

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

and  $\gamma, \gamma'$  have the same level-set partition, which is supposed to be an admissible partition 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  $\tau s \tau^{-1}$  denotes the  $k$ -tuple of permutations  $(\tau s_1 \tau^{-1}, \dots, \tau s_k \tau^{-1})$ .

**Proof.** Since  $\gamma$  and  $\gamma'$  have the same level-set partition, 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  $r$ ,

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

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  $\gamma_s = \gamma$ . □

**2.3.2. Random permutations.** We fix  $k \geq 1$  and  $A_1, \dots, A_k$  non empty sets of positive integers (none of them being  $\{1\}$ ), such that for all  $i$ ,  $A_i$  is either finite or satisfies  $\sum_{\substack{j \geq 1 \\ j \notin A_i}} \frac{1}{j} < \infty$ .

We also fix  $w \in \mathbb{M}_k$  and 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  $\sigma_n = w(s_1(n), \dots, s_k(n))$ : the permutation obtained by replacing any  $g_i$  (or  $g_i^{-1}$ ) in  $w$  by  $s_i(n)$  (or  $s_i(n)^{-1}$ ). We shall use the notations of section 2.2.

We are going to study the random variables  $N_l(\sigma_n)$ . Note that none of them changes 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 2.1.1, one can suppose  $w$  to be cyclically reduced.

**Proposition 2.18.** *Consider  $p \geq 1$  and  $\sigma \in \mathfrak{S}_p$ . The probability of the event*

$$(4) \quad \{\forall m = 1, \dots, p, \sigma_n(m) = \sigma(m)\}$$

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

$$(5) \quad \frac{1}{n^p} \sum_{\Delta \in C(\sigma, w, A_1, \dots, A_k)} n^{\chi(G(\sigma, w)/\Delta)},$$

where  $C(\sigma, w, A_1, \dots, A_k)$  is the set of  $(A_1, \dots, A_k)$ -admissible partitions  $\Delta$  of  $G(\sigma, w)$  such that for all  $m \neq m' \in [p]$ ,  $(m, 1) \not\equiv (m', 1) \pmod{\Delta}$ .

**Proof.** First, it is clear that for all  $s \in (\mathfrak{S}_n)^k$  such that

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

the partition  $\text{Part}(\gamma_s)$  of level sets of this function is an admissible partition of  $G(\sigma, w)$ . It is also clear, by a descending induction on  $l$ , that for all  $m \neq m' \in [p]$ , for all  $l \in [|w|]$ ,  $(m, l) \not\equiv (m', l) \pmod{\text{Part}(\gamma_s)}$ .

Hence if  $V$  denotes the vertex set of  $G(\sigma, w)$ , the probability of the event

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

is the sum, over all functions  $\gamma : V \rightarrow [n]$  whose level set partition is an admissible partition of  $G(\sigma, w)$  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 2.17, for all function  $\gamma : V \rightarrow [n]$  whose level set partition is an admissible partition of  $G(\sigma, w)$  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 admissible partitions  $\Delta$  of  $G(\sigma, w)$ , of the number of functions  $\gamma : V \rightarrow [n]$  whose level set partition is  $\Delta$  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. Now, note first that for  $\Delta$  admissible partition of  $G(\sigma, w)$ , the number of such functions is

$$\begin{cases} n(n-1) \cdots (n - |\Delta| + p + 1) & \text{if } \forall m \neq m' \in [p], (m, 1) \not\equiv (m', 1) \pmod{\Delta}, \\ 0 & \text{in the other case.} \end{cases}$$

Secondly, let us define, for  $H$  edge-colored graph and  $r \in [k]$  a color,  $H[r]$  to be the mono-colored graph obtained from  $H$  by removing all edges which do not have color  $r$  and all vertices which are not the extremity of an  $r$ -colored edge. Then by lemma 2.16, the probability that  $\gamma_{s_1(n), \dots, s_k(n)}$  is a certain (fixed) of these functions is

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

where for all set  $A$  of positive integers  $F$  mono-colored graph,  $p_n^{(A)}(F)$  is the number defined in 3.8(a) of [Ne07].

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

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

and proposition 3.8 of [Ne07] allows to conclude.  $\square$

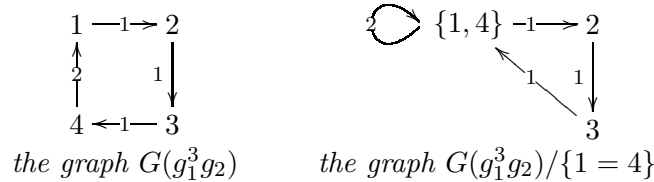
The following result is a direct application of corollary 1.7 of [BG07] applied with  $A$  equal to the set of all positive integers and of proposition 2.18. For all  $n$ ,  $\sigma_n$  is still the random permutation introduced above the previous proposition.

**Corollary 2.19.** *If  $w$  cyclically reduced 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  $(N_1(\sigma_n), \dots, N_l(\sigma_n))$  converges weakly, 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*

$$\text{Poisson}(1/1) \otimes \dots \otimes \text{Poisson}(1/l).$$

**Remark 2.20.** *The hypothesis of this corollary do not always hold.*

a) *As a first example, suppose that  $w = g_1^3 g_2$ , with  $A_1 = \{3, 4\}$ ,  $A_2 = \{1, 2\}$ . Then for  $p = 1$  and  $\sigma = \text{Id}$ , the quotient of the graph  $G(w)$  by the partition  $\{1 = 4\}$  which only links 1 and 4 has Neagu characteristic  $3 - 4 + 3/4 + 1/2 > 0$ :*



Since, as noticed in remark 1.8 of [BG07], we do not know if corollary 1.7 of this paper has an inverse implication, we cannot conclude that the conclusion of the corollary is false in this case. However, remark 3.2, applied for this word and  $l = 1$ , allows us to claim that the expectation of the number of fixed points of  $\sigma_n$  tends to infinity as  $n$  goes to infinity.

b) *In the previous example, it seems that  $A_i$ 's need to contain large elements which are not their supremums in order that the hypothesis of the corollary do not hold. In fact, it is not true: lemma 3.13 provides counterexamples.*

c) *However, we did not find any non trivial counterexample in the case where some  $A_i$ 's are infinite and all finite  $A_i$ 's are singletons (by "non trivial", we mean primitive words which  $(d_1, \dots, d_k)$ -reductions are not a power of a single letter).*

### 3. MAIN RESULTS ABOUT WORDS IN RANDOM PERMUTATIONS

We fix, until the end of section 3,  $k \geq 1$  and  $w \in \mathbb{M}_k$  cyclically reduced (as noticed in the beginning of section 2.3.2, this hypothesis on  $w$  is not restrictive). We also fix  $A_1, \dots, A_k$  non empty sets of positive integers (none 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

(which is equivalent, for  $n$  large enough, to the fact that for all  $i \in [k]$ ,  $n$  is divided by the greatest common divisor of  $A_i$ , by lemma 2.3 of [Ne07]), 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  $\sigma_n = w(s_1(n), \dots, s_k(n))$ . 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  $\sigma_n$ ).



**3.1. Asymptotic behavior of the random variables  $N_l(\sigma_n)$  and quotient of the free group.** The first interesting facts are the leading role played by the element of the group  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$  represented by  $w$  and the fact that for most words  $w$ , even though the lengths of the cycles of the letters of  $w(s_1(n), \dots, s_k(n))$  are supposed to belong to the specific sets  $A_1, \dots, A_k$  of positive integers, these cycles are going to mix enough to give birth to cycles of most lengths, at least as much as in a uniform random permutation.

3.1.1. *Case of a word with infinite order in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$ : existence of cycles of most lengths.*

**Theorem 3.1.** *Suppose that the order, in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$  of the element represented by  $w$  is infinite. Then two cases can occur:*

- (i) *None of the  $(d_1, \dots, d_k)$ -cyclic reductions of  $w$  is of the type  $g_i^\alpha$ , with  $i \in [k]$ ,  $\alpha$  integer. Then for all  $l \geq 1$ , as  $n$  goes to infinity in such a way that for all  $r = 1, \dots, k$ ,  $\mathfrak{S}_n^{(A_r)} \neq \emptyset$ ,*

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

- (ii) *There is  $i \in [k]$  such that  $d_i = \infty$  and the  $(d_1, \dots, d_k)$ -cyclic reduction of  $w$  is  $g_i^\alpha$ , with  $\alpha$  non null integer. Then for all  $l \geq 1$  such that  $l|\alpha \in A_i$ , as  $n$  goes to infinity in such a way that for all  $r = 1, \dots, k$ ,  $\mathfrak{S}_n^{(A_r)} \neq \emptyset$ ,*

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

**Remark 3.2.** *In fact, we prove the more general result: if  $c_l$  denotes the cycle  $(1 \cdots l)$ , then*

$$(6) \quad \forall \Delta \in C(c_l, w, A_1, \dots, A_k), \quad \liminf \frac{\mathbb{E}(N_l(\sigma_n))}{n\chi(G(c_l, w)/\Delta)} \geq \frac{1}{l}.$$

**Remark 3.3.** *Actually, in the particular case where all finite  $A_i$ 's are singletons, using Proposition 2.4.3 and the last sentence of corollary 2.6.6 of [Ni94], we can easily prove that if the  $(d_1, \dots, d_k)$ -cyclic reductions of  $w$  are primitive words with more than one letter, then for all  $l \geq 1$ ,  $\mathbb{E}(N_l(\sigma_n))$  tends to  $1/l$  as  $n$  tends to infinity.*

**Proof.** We have

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

But in the last sum, since the law of  $\sigma_n$  is invariant under conjugation, all terms are equal. Moreover, by this invariance principle again, each term is equal to the number of cycles of length  $l$  containing 1 times the probability that  $\sigma_n$  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 2.18 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 2.15 allows us to conclude.  $\square$

3.1.2. *Case of a word with finite order in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$ .* We see in the following theorem that in the case where  $(d_1, \dots, d_k)$ -cyclic reductions of  $w$  have order  $l \geq 1$  in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$ ,  $\sigma_n$  is not faraway from having order  $d$ : the cardinality of the subset of  $\{1, \dots, n\}$  covered by the supports of the cycles with length  $d$  in such a random permutation is equivalent to  $n$ .

**Theorem 3.4.** *Suppose the  $(d_1, \dots, d_k)$ -cyclic reductions of  $w$  have order  $d \geq 1$  in  $F_k/[g_1^{d_1}, \dots, g_k^{d_k}]$ . 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  $p \in [1, +\infty)$ ,  $N_d(\sigma_n)/n$  converges to  $1/d$  in  $L^p$  and for all  $l \geq 1$  such that  $j \neq l$ ,  $N_l(\sigma_n)/n$  converges to 0 in  $L^p$ .*

**Proof.** Notice first that for all  $n$ ,

$$(7) \quad \sum_{l \geq 1} l N_l(\sigma_n)/n \leq 1,$$

which implies that for all positive integer  $l$ , the sequence  $N_l(\sigma_n)/n$  is bounded by 0 and  $1/l$ . Now, recall that for a sequence  $(X_n)$  of random variables, if there exists  $M < \infty$  such that for all  $n$ ,  $0 \leq X_n \leq M$ , the convergence of  $X_n$  to a limit  $X$  in all  $L^p$  spaces is implied by this result for  $p = 1$  (indeed, under this hypothesis, if for a certain  $p \geq 1$ ,  $X_n$  doesn't converge to  $X$  in  $L^p$ , then a subsequence of  $(X_n)$  converges to  $X$  almost surely but not in  $L^p$ , which is impossible by the dominated convergence theorem).

Hence it suffices to prove that  $\mathbb{E}(N_d(\sigma_n)/n) \xrightarrow[n \rightarrow \infty]{} 1/d$  and that for all  $l \geq 1$  such that  $l \neq d$ ,  $\mathbb{E}(N_l(\sigma_n)/n) \xrightarrow[n \rightarrow \infty]{} 0$ . First notice that the second of these limits will follow from the first one and (7). Then, notice that the first of these limits is a consequence of (6) (which has been established in the proof of theorem 3.1 without using the specific hypothesis of this theorem), of corollary 2.15 and of the inequality  $N_d(\sigma_n)/n \leq 1/d$ .  $\square$

**3.2. Case when all  $A_i$ 's are infinite.** Note 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 going to suppose that  $w$  is primitive. Note at last that the case where  $|w| = 1$  has already been treated in [BG07], 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 3.5.** *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  $(N_1(\sigma_n), \dots, N_l(\sigma_n))$  converges weakly to*

$$\text{Poisson}(1/1) \otimes \dots \otimes \text{Poisson}(1/l).$$

**Proof.** This result is a direct consequence of corollary 2.19. 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  $\Delta$  admissible partition of  $G(\sigma, w)$ ,  $\chi(G(\sigma, w)/\Delta)$  is the number of classes of  $\Delta$  minus the number of edges of  $G(\sigma, w)/\Delta$ , hence isn't positive by Proposition 2.4.3 of [Ni94]. The last sentence of corollary 2.6.6 of the same article also says that there is only one admissible partition  $\Delta$  of  $G(\sigma, w)$  for which it is null and such that for all  $m \neq m' \in [p]$ ,  $(m, 1)$  and  $(m', 1)$  are not in the same class: it is the singletons partition. It remains only to prove that the singletons partition is in  $C(\sigma, w, A_1, \dots, A_k)$ :

- this partition is clearly admissible,
- clearly, for all  $m \neq m' \in [p]$ ,  $(m, 1)$  and  $(m', 1)$  are not in the same class of the singleton partition,

- there is no mono-colored loop in  $G(\sigma, w)$ : indeed, by lemma 2.7,  $G(\sigma, w)$  is a disjoint union of graphs of the type  $G(w^d)$  (with  $d \geq 1$ ), where there is no mono-colored loop since  $w$  is primitive and  $|w| > 1$ .  $\square$

**3.3. 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  $k \geq 2$  (since the case  $k = 1$  has already been treated in [BG07]).

**3.3.1. Case where  $k > 2$  or  $A_1 \cup A_2 \not\subseteq \{1, 2\}$ .** Here, we have a 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 3.6.** *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*

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

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

**Lemma 3.7.** *Let  $\mathcal{X}$  be a finite set, let  $\mathcal{B}$  be a set of subsets of  $\mathcal{X}$  which have all cardinality 2. Let  $\Delta$  be a partition of  $\mathcal{X}$  such that for all element  $\{x, y\}$  of  $\mathcal{B}$ ,  $x = y \pmod{\Delta}$ . Then we have  $|\Delta| \leq |\mathcal{X}| - |\mathcal{B}|$ .*

**Proof.** Let us define the set  $\Gamma$  of subsets 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  $\Delta$  is a union of elements of  $\Gamma$ , so  $|\Delta| \leq |\Gamma| = |\mathcal{X}| - |\mathcal{B}|$ .  $\square$

**Lemma 3.8.** *Consider  $w = g_1 \cdots g_k$ , with  $k \geq 2$ , and  $\sigma \in \mathfrak{S}_p$ , with  $p \geq 1$ . Let  $\Delta$  be an admissible partition of  $G(\sigma, w)$  such that for all  $i \neq j \in [p]$ ,  $(i, 1) \neq (j, 1) \pmod{\Delta}$ . Then*

- (i) *two different edges of  $G(\sigma, w)$  with the same color cannot have there beginning vertices in the same class of  $\Delta$ , and the same holds for ending vertices,*
- (ii) *the following inequalities hold:*

$$(a) \text{ if } k > 2, \text{ then } |\Delta| \leq pk - \sum_{r=1}^k \sum_{\substack{L \text{ loop of} \\ G(\sigma, w)/\Delta \\ \text{with color } r}} \text{length of } L,$$

$$(b) \text{ if } k = 2, \text{ then for all } r = 1, 2, |\Delta| \leq pk - \sum_{\substack{L \text{ loop of} \\ G(\sigma, w)/\Delta \\ \text{with color } r}} \text{length of } L.$$

**Remark 3.9.** *Note that (i) implies that there is a canonical identification between the set of edges of the graph  $G(\sigma, w)$  and the set of edges of the graph  $G/\Delta$ : if, for all vertex  $x$  of  $G(\sigma, w)$ , one denotes by  $\bar{x}$  the class of  $x$  in  $\Delta$ , then for all  $r \in [k]$ , the function from the set of  $r$ -colored edges of  $G(\sigma, w)$  to the set of  $r$ -colored edges of  $G(\sigma, w)/\Delta$  which maps any edge  $x \rightarrow y$  to  $\bar{x} \rightarrow \bar{y}$  is bijective.*

**Proof.** Note first that since for all  $i \neq j \in [p]$ ,  $(i, 1) \neq (j, 1) \pmod{\Delta}$ , and by definition of an admissible partition, one has (by an obvious induction on  $l$ ):

$$(8) \quad \forall i \neq j \in [p], \forall l \in [k], (i, l) \neq (j, l) \pmod{\Delta}.$$

Since two edges of  $G(\sigma, w)$  with the same color have beginning vertices (and ending vertices) with the same second coordinate, it implies (i).

The proofs of both points of (ii) will be applications of the previous lemma. First, note that as observed in remark 3.9, 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, via this identification, belong to an  $r$ -colored loop of  $G(\sigma, w)/\Delta$ . Define

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

*Claim:* no edge of  $G(\sigma, w)/\Delta$  can belong to more than one mono-colored loop of  $G(\sigma, w)/\Delta$ .

Indeed, if it were the case, there would be a color  $r \in [k]$ ,  $r$ -colored loops  $e, e', e''$  of  $G(\sigma, w)$  such that  $e'$  and  $e''$  both follow  $e$  in  $r$ -colored loops of  $G(\sigma, w)/\Delta$  and  $e' \neq e''$ . Since  $e'$  and  $e''$  follow  $e$  in loops of  $G(\sigma, w)/\Delta$ , we have  $\text{Beg}(e') = \text{End}(e) = \text{Beg}(e'') \pmod{\Delta}$ , which implies  $e' = e''$  by (i). Contradiction.

The first consequences of this claim are that

$$(9) \quad \sum_{r=1}^k \sum_{\substack{L \text{ loop of} \\ G(\sigma, w)/\Delta \\ \text{with color } r}} \text{length of } L = |\mathcal{L}|,$$

and that for all  $r = 1, \dots, k$ ,

$$(10) \quad \sum_{\substack{L \text{ loop of} \\ G(\sigma, w)/\Delta \\ \text{with color } r}} \text{length of } L = |\mathcal{L}[r]|.$$

Another consequence of the claim is that one can define a permutation  $\varphi$  of  $\mathcal{L}$  which maps any edge  $e \in \mathcal{L}$  to the edge which follows  $e$  in the mono-colored loop  $e$  belongs to. Let us define, for  $e \in \mathcal{L}$ ,

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

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

$$\text{End}(e) = \text{Beg}(\varphi(e)) \pmod{\Delta}.$$

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

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

or

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

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

If  $k > 2$ : let us prove that  $S(e) = S(f)$  with  $e \neq f$  is impossible. We have  $\text{End}(e) = \text{Beg}(\varphi(f))$ , so the color following the one of  $e$  in the cyclic order  $1, 2, \dots, k, 1, \dots$  is the one of  $\varphi(f)$ , i.e. of  $f$ . In the same way, the relation  $\text{End}(f) = \text{Beg}(\varphi(e))$  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:

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

which is impossible, since  $k > 2$ .

So the cardinality of  $\mathcal{A}$  is the one of  $\mathcal{L}$ , and by (9), the result (a) of the lemma 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 by (10), the result (b) is an immediate application of the previous lemma, for  $\mathcal{X} = [p] \times [|w|]$  and  $\mathcal{B} = \mathcal{A}[r]$ .  $\square$

Now we are able to prove theorem 3.6.

**Proof of the theorem.** Again, we are going to apply corollary 2.19. Let us fix  $p \geq 1$  and  $\sigma \in \mathfrak{S}_p$ .

Note that the singletons partition, denoted by  $\Delta_s$ , is in  $C(\sigma, w, A_1, \dots, A_k)$  (the proof is the same one as in the proof of theorem 3.5). Moreover, using lemma 2.7, one easily sees that the Neagu characteristic of  $G(\sigma, w)$  is 0.

Hence it suffices to prove that for all  $\Delta \in C(\sigma, w, A_1, \dots, A_k)$  such that  $\Delta \neq \Delta_s$ , the Neagu characteristic of  $G(\sigma, w)/\Delta$  is negative. Let us fix such a partition  $\Delta$ . By remark 3.9, we have to prove that

$$(11) \quad |\Delta| < pk - \sum_{r=1}^k \sum_{\substack{L \text{ loop of} \\ G(\sigma, w)/\Delta \\ \text{with color } r}} \frac{\text{length of } L}{d_r}.$$

- If there is no mono-colored loop in  $G(\sigma, w)/\Delta$ , then, since  $\Delta \neq \Delta_s$ ,  $|\Delta| < |[p] \times [|w|]| = pk$ , and hence (11) holds.

- If there is a mono-colored loop in  $G(\sigma, w)/\Delta$  and  $k > 2$ , then since for all  $r$ ,  $d_r \geq 2 > 1$ , by (ii) (a) of lemma 3.8, (11) holds.

- If there is a mono-colored loop in  $G(\sigma, w)/\Delta$  and  $k = 2$ . First note that adding (ii) (b) of lemma 3.8 for  $r = 1$  and  $r = 2$ , and then dividing by 2, one gets

$$(12) \quad |\Delta| \leq pk - \frac{1}{2} \sum_{r=1}^2 \sum_{\substack{L \text{ loop of} \\ G(\sigma, w)/\Delta \\ \text{with color } r}} \text{length of } L.$$

By hypothesis, one has either  $d_1 > 2$  or  $d_2 > 2$ . By symmetry, we will suppose that  $d_1 > 2$ . Now, we have to discuss whether there is or not a loop of color 1.

- If there is at least one loop of color 1 in  $G(\sigma, w)/\Delta$ . Then since  $d_1 > 2$ , the right hand term of (12) is strictly less than

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

so (11) holds.

- If there is no loop of color 1 in  $G(\sigma, w)/\Delta$ . Then there is at least one loop of color 2, and, since  $d_2 > 1$ , the right hand term in (ii) (b) of lemma 3.8 is strictly less than

$$pk - \sum_{\substack{L \text{ loop of} \\ G(\sigma, w)/\Delta \\ \text{with color 2}}} \frac{\text{length of } L}{d_2} = pk - \sum_{r=1}^2 \sum_{\substack{L \text{ loop of} \\ G(\sigma, w)/\Delta \\ \text{with color } r}} \frac{\text{length of } L}{d_r},$$

i.e. than the right hand term of (11). So (11) holds.

□

**3.3.2. Case where  $k = 2$  and  $A_1 \cup A_2 \subset \{1, 2\}$ .** Here, for  $n$  positive integer, we consider  $\sigma_n = s_1(n)s_2(n)$  with  $s_1(n), s_2(n)$  independent random involutions. There are three cases:

- (i)  $s_1(n), s_2(n)$  have both uniform distribution on the set of involutions of  $[n]$ :  $A_1 = A_2 = \{1, 2\}$ ,
- (ii)  $s_1(n), s_2(n)$  have both uniform distribution on the set of involutions of  $[n]$  without any fixed point:  $A_1 = A_2 = \{2\}$ ,
- (iii) one of the random involutions has uniform distribution on the set of involutions of  $[n]$  and the other one has uniform distribution on the set of involutions of  $[n]$  without any fixed point: since for  $s, s'$  involutions,  $ss'$  and  $s's$  are conjugated and for all  $l$ ,  $N_l(\sigma_n)$  is constant on any conjugation class, one can suppose that  $A_1 = \{2\}$ ,  $A_2 = \{1, 2\}$ .

**Theorem 3.10.** (i) *If  $A_1 = A_2 = \{1, 2\}$ , then as  $n$  goes to infinity, for all  $q \geq 1$ , the law of  $(N_1(\sigma_n), \dots, N_q(\sigma_n))$  converges weakly to  $\mu_1 \otimes \dots \otimes \mu_q$ , where for all  $l \geq 1$ ,  $\mu_l$  is the law of  $P_1 + 2P_{\frac{1}{2l}}$ , with  $P_1, P_{\frac{1}{2l}}$  independent random variables with distributions Poisson(1), Poisson( $\frac{1}{2l}$ ).*

- (ii) *If  $A_1 = A_2 = \{2\}$ , then as  $n$  even goes to infinity, for all  $q \geq 1$ , the law of*

$$\frac{1}{2}(N_1(\sigma_n), \dots, N_q(\sigma_n))$$

*converges weakly to Poisson(1/2)  $\otimes$  Poisson(1/4)  $\otimes \dots \otimes$  Poisson(1/2q).*

- (iii) *If  $A_1 = \{2\}$ ,  $A_2 = \{1, 2\}$ , then as  $n$  even goes to infinity, for all  $q \geq 1$ , the law of  $(N_1(\sigma_n), \dots, N_q(\sigma_n))$  converges weakly to  $\mu_1 \otimes \dots \otimes \mu_q$ , where for all  $l$  odd positive number,  $\mu_l$  is the law of  $2P_{\frac{1}{2l}}$  and for all  $l$  even positive number,  $\mu_l$  is the law of  $P_{\frac{1}{2}} + 2P_{\frac{1}{2l}}$ , with  $P_{\frac{1}{2}}, P_{\frac{1}{2l}}$  independent random variables with distributions Poisson( $\frac{1}{2}$ ), Poisson( $\frac{1}{2l}$ ).*

**Remark 3.11.** *Note that a consequence of (ii) of this theorem is that if  $A_1 = A_2 = \{2\}$ , for all  $l \geq 1$ , the probability of the fact that  $N_l(\sigma_n)$  is odd tends to zero as  $n$  goes to infinity. In fact, it can be proved that for all  $l \geq 1$ , the product of two involutions  $s, s'$  of a finite set without any fixed points cannot have an odd number of cycles of length  $l$ . Let us prove it. First, let us define two permutations  $c, r$  of  $[l]$  by:  $c$  is the cycle  $(12 \dots l)$  and  $r(1) = l, r(2) = l-1, \dots, r(l) = 1$  (i.e. for all  $x$ ,  $r(x) = l+1-x$ ). Note that since  $s^2 = s'^2 = Id$ , the function which maps any*

cycle  $(z_1 z_2 \cdots z_l)$  of  $s$ 's to  $(s(z_l) \cdots s(z_1))$  is a well defined involution of the set of cycles of length  $l$  of  $s$ 's. Hence it suffices to prove that this function has no fixed point. In the other case, there is a cycle  $(z_1 z_2 \cdots z_l)$  of  $s$ 's such that the cycles  $(z_1 z_2 \cdots z_l)$ ,  $(s(z_l) \cdots s(z_1))$  are equal. Hence there is  $k \in [l]$  such that

$$z_{c^k(1)} = s(z_{r(1)}), z_{c^k(2)} = s(z_{r(2)}), \dots, z_{c^k(l)} = s(z_{r(l)}).$$

It implies that we have the equalities (of vectors):

$$(s'(z_{c^k(1)}), s'(z_{c^k(2)}), \dots, s'(z_{c^k(l)})) = (s's(z_{r(1)}), \dots, s's(z_{r(l)})) = (z_{cr(1)}, \dots, z_{cr(l)}).$$

Since neither  $s$  nor  $s'$  have any fixed point, to find a contradiction, it suffices to prove that there is  $j \in [l]$  such that  $c^k(j) = r(j)$  or  $c^k(j) = cr(j)$ , i.e. such that  $j + k = 1 - j \pmod{l}$  or  $j + k = 2 - j \pmod{l}$ , i.e. such that  $l|2j + k - 1$  or  $l|2j + k - 2$ , which can easily be proved.

To prove the theorem, we shall need the following lemmas.

**Lemma 3.12.** Consider  $a, b$  positive real numbers and define the measure

$$\nu_{a,b} := e^{-\frac{1+2ab}{2b^2}} \sum_{r=0}^{+\infty} \frac{\mathbb{E}[(X+a)^r]}{r!b^r} \delta_r,$$

with  $X$  standard Gaussian random variable. Then  $\nu_{a,b}$  is the distribution of  $P_{\frac{a}{b}} + 2P_{\frac{1}{2b^2}}$ , with  $P_{\frac{a}{b}}, P_{\frac{1}{2b^2}}$  independent random variables with respective distributions Poisson( $a/b$ ), Poisson( $1/(2b^2)$ ).

**Proof.** Let us fix  $r \geq 0$ . By the well known formula of the moments of  $X$ , one has:

$$\begin{aligned} \nu_{a,b}(\{r\}) &= e^{-\frac{1+2ab}{2b^2}} \frac{1}{r!b^r} \sum_{\substack{j,l \geq 0 \\ j+l=r}} \binom{r}{l} \mathbb{E}(X^l) a^j = e^{-\frac{1+2ab}{2b^2}} \frac{1}{r!b^r} \sum_{\substack{j,k \geq 0 \\ j+2k=r}} \binom{r}{2k} \frac{(2k)!}{2^k k!} a^j \\ &= e^{-\frac{1+2ab}{2b^2}} \sum_{\substack{j,k \geq 0 \\ j+2k=r}} \frac{1}{j!k!} (a/b)^j (1/2b^2)^k = \sum_{\substack{j,k \geq 0 \\ j+2k=r}} P(P_{\frac{a}{b}} = j, P_{\frac{1}{2b^2}} = k). \end{aligned}$$

□

**Lemma 3.13.** Consider  $A_1, A_2$  as in (i), (ii) or (iii) of theorem 3.10. Fix  $p \geq 1$  and  $\sigma \in \mathfrak{S}_p$ . Then the following holds:

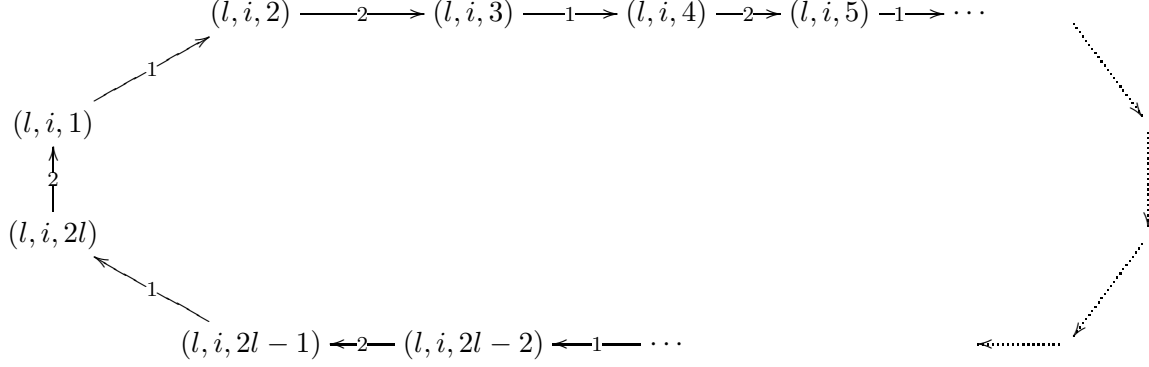
- for all  $\Delta \in C(\sigma, g_1 g_2, A_1, A_2)$ ,  $\chi(G(\sigma, g_1 g_2)/\Delta) = 0$ ,
- the cardinality of  $C(\sigma, g_1 g_2, A_1, A_2)$  is

$$\begin{cases} \prod_{l=1}^p \mathbb{E}((\sqrt{l}X + l + 1)^{N_l(\sigma)}) & \text{if } A_1 = A_2 = \{1, 2\}, \\ \prod_{l=1}^p \mathbb{E}((1 + \sqrt{l}X)^{N_l(\sigma)}) & \text{if } A_1 = A_2 = \{2\}, \\ \prod_{\substack{1 \leq l \leq p \\ l \text{ odd}}} \mathbb{E}[(\sqrt{l}X + 1)^{N_l(\sigma)}] \prod_{\substack{1 \leq l \leq p \\ l \text{ even}}} \mathbb{E}[(\sqrt{l}X + l/2 + 1)^{N_l(\sigma)}] & \text{if } A_1 = \{2\}, A_2 = \{1, 2\}, \end{cases}$$

where  $X$  is a standard Gaussian random variable.

**Proof.** Let, for  $l$  positive integer,  $c_{2l}$  be the cycle  $(1\ 2\ \dots\ 2l)$ .

First, we are going to use lemma 2.7: up to a renaming of its vertices and edges,  $G(\sigma, g_1g_2)$  is the disjoint union, for  $(l, i)$  such that  $l \in [p], i \in [N_l(\sigma)]$ , of the graphs  $H(l, i)$ , where each  $H(l, i)$  is the oriented edge-colored graph with color set  $\{1, 2\}$ , with vertex set  $\{(l, i, j); j \in [2l]\}$ , with 1-colored edge set  $\{(l, i, j) \rightarrow (l, i, c_{2l}(j)); j \in [2l] \text{ odd}\}$  and with 2-colored edge set  $\{(l, i, j) \rightarrow (l, i, c_{2l}(j)); j \in [2l] \text{ even}\}$ .  $H(l, i)$  can be represented as



With this renaming, for  $\Delta$  partition of the vertex set of  $G(\sigma, g_1g_2)$ , the condition

$$\forall m \neq m' \in [p], (m, 1) \neq (m', 1) \pmod{\Delta}$$

gets

$$\forall l, l' \in [p], \forall (i, i') \in [N_l(\sigma)] \times [N_{l'}(\sigma)], \forall (j, j') \in [2l] \times [2l'],$$

$$(13) \quad [(l, i, j) \neq (l', i', j') \text{ and } j = j' \pmod{2}] \Rightarrow [(l, i, j) \neq (l', i', j') \pmod{\Delta}].$$

Now, let us fix  $\Delta \in C(\sigma, g_1g_2, A_1, A_2)$ .

a) By remark 3.9,  $G(\sigma, w)/\Delta$  has  $2p$  edges.

b) By (13), the classes of  $\Delta$  cannot have more than two elements.

c)  $\Delta$  is an  $(A_1, A_2)$ -admissible partition, so no string of color either 1 or 2 of  $G(\sigma, g_1g_2)/\Delta$  can have length at least two. It implies that if two distinct edges of  $G(\sigma, g_1g_2)/\Delta$  have the same color and an extremity in common, then these edges are the ones of a cycle of length two, i.e. that the beginning of each of them is the end of the other one and vice versa.

d) Let us consider two distinct vertices  $(l, i, j) \neq (l', i', j')$  of  $G(\sigma, g_1g_2)$  which form together a class of  $\Delta$ .

( $\alpha$ ) By (13),  $j$  and  $j'$  do not have the same parity, hence the edge which begins at  $(l, i, j)$  has the color of the edge which ends at  $(l', i', j')$ , and vice versa. So by an immediate induction on  $|m|$  (using c)), one has:

$$(14) \quad \forall m \text{ positive or negative integer, } (l, i, c_{2l}^m(j)) = (l', i', c_{2l'}^{-m}(j')) \pmod{\Delta}.$$

( $\beta$ ) Suppose that  $l \neq l'$ . One can suppose that  $l < l'$ . Then by (14) for  $m = 2l$ ,  $(l, i, j) = (l, i, c_{2l}^{2l}(j))$  is in the same time linked, by  $\Delta$ , with  $(l', i', c_{2l'}^{-2l}(j'))$  and  $(l', i', j')$  which are not the same. By b), it is impossible. Hence  $l = l'$ .



( $\gamma_1$ ) Suppose that  $i \neq i'$ . Then by (14) for  $m = -j + 1, -j + 2, \dots, -j + 2l$ , there is a unique  $q \in [l]$  such that the classes, in  $\Delta$  of

$$(l, i, 1), (l, i, 2), \dots, (l, i, 2l), (l, i', 1), (l, i', 2), \dots, (l, i', 2l)$$

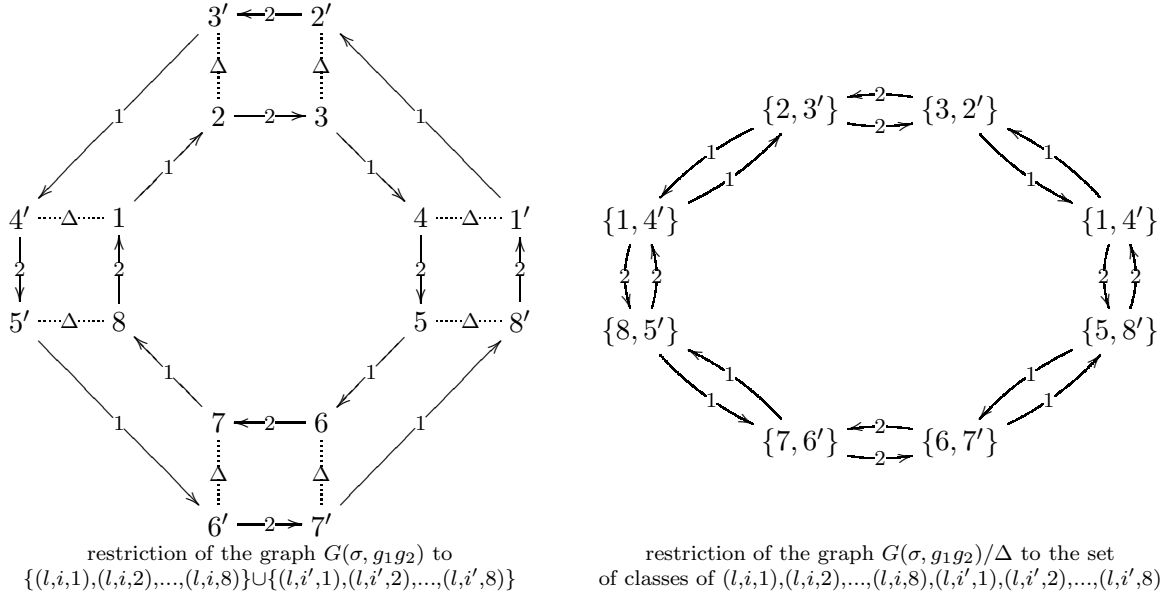
are

$$(15) \quad \{(l, i, 1), (l, i', 2q)\}, \{(l, i, 2), (l, i', c_{2l}^{-1}(2q))\}, \dots, \{(l, i, 2l), (l, i', c_{2l}^{-(2l-1)}(2q))\}.$$

Note that  $q$  depends on  $i$  and  $i'$  in a symmetric way, since the set of (15) can also be written

$$\{(l, i', 1), (l, i, 2q)\}, \{(l, i', 2), (l, i, c_{2l}^{-1}(2q))\}, \dots, \{(l, i', 2l), (l, i, c_{2l}^{-(2l-1)}(2q))\}.$$

Let us give an illustration of the case ( $\gamma_1$ ) with  $l = 4, q = 2$ . In the inner (resp. outer) octagon, the vertices were not denoted by  $(l, i, j)$  (resp.  $(l, i', j)$ ) but by  $j$  (resp.  $j'$ ), for  $j \in [8]$ , in order to lighten the figure. In  $G(\sigma, g_1 g_2)$ , vertices linked by  $\Delta$  are linked by edges of the type  $\cdots\Delta\cdots$  (but these edges do not belong to  $G(\sigma, g_1 g_2)$ ).



On this figure, it appears clearly that if two vertices of the left graph linked by an edge of the type  $\cdots\Delta\cdots$  are in the same class of  $\Delta$ , then since no string of color either 1 or 2 of  $G(\sigma, g_1 g_2)/\Delta$  can have length at least two, all the other pairs of vertices linked by an edge of the type  $\cdots\Delta\cdots$  must form classes of  $\Delta$ .

( $\gamma_2$ ) Let us prove that if  $i = i'$ , then there is  $j_0 \in [2l]$  such that the classes, in  $\Delta$ , of the elements  $(l, i, 1), (l, i, 2), \dots, (l, i, 2l)$  are

$$(16) \quad \{(l, i, j_0), (l, i, c_{2l}(j_0))\}, \{(l, i, c_{2l}^{-1}(j_0)), (l, i, c_{2l}^2(j_0))\}, \{(l, i, c_{2l}^{-2}(j_0)), (l, i, c_{2l}^3(j_0))\}, \\ \dots, \{(l, i, c_{2l}^{-(l-1)}(j_0)), (l, i, c_{2l}^l(j_0))\},$$

and that this  $j_0$  is unique up to a replacement by  $c_{2l}^l(j_0)$ .

Note first that if such a  $j_0$  exists, then its uniqueness up to a replacement by  $c_{2l}^l(j_0)$  is obvious. Indeed, if one denotes  $c_{2l}^l(j_0)$  by  $j'_0$ , then since  $c_{2l}$  is a cycle of length  $2l$ , the

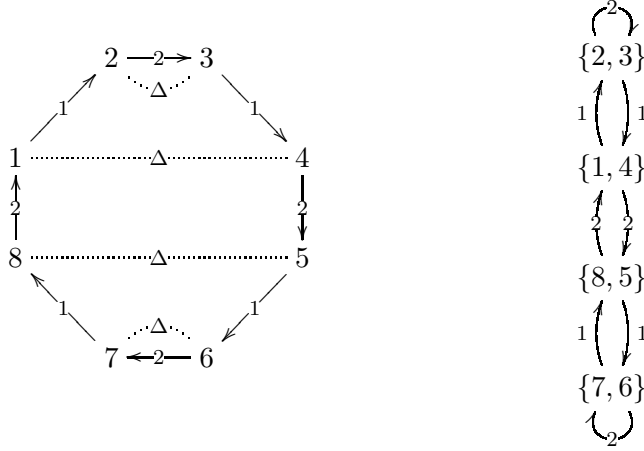
partition of (16) is equal to

$$\{(l, i, j'_0), (l, i, c_{2l}(j'_0))\}, \{(l, i, c_{2l}^{-1}(j'_0)), (l, i, c_{2l}^2(j'_0))\}, \{(l, i, c_{2l}^{-2}(j'_0)), (l, i, c_{2l}^3(j'_0))\}, \\ \dots, \{(l, i, c_{2l}^{-(l-1)}(j'_0)), (l, i, c_{2l}^l(j'_0))\},$$

and  $\{(l, i, j_0), (l, i, c_{2l}(j_0))\}, \{(l, i, c_{2l}^{-(l-1)}(j_0)), (l, i, c_{2l}^l(j_0))\} (= \{(l, i, j'_0), (l, i, c_{2l}(j'_0))\})$  are the only classes of the type  $\{(l, i, x), (l, i, c_{2l}(x))\}$  in the partition of (16).

To prove the existence of such a  $j_0$ , it suffices to notice that by (14) and b),  $j_0 = (j' + j - 1)/2$  is convenient.

Let us give an illustration of the case  $(\gamma_2)$  with  $l = 4, j_0 = 2$ . Here, the vertices were not denoted by  $(l, i, j)$  but by  $j$ , for  $j \in [8]$ , in order to lighten the figure. In  $G(\sigma, g_1g_2)$ , vertices linked by  $\Delta$  are linked by edges of the type  $\cdots\Delta\cdots$  (but these edges do not belong to  $G(\sigma, g_1g_2)$ ).



restriction of the graph  $G(\sigma, g_1g_2)$  to  $\{(l, i, 1), (l, i, 2), \dots, (l, i, 8)\}$

restriction of the graph  $G(\sigma, g_1g_2)/\Delta$  to the set of classes of  $(l, i, 1), (l, i, 2), \dots, (l, i, 8)$

On this figure, it appears clearly that if two vertices of the left graph linked by an edge of the type  $\cdots\Delta\cdots$  are in the same class of  $\Delta$ , then since no string of color either 1 or 2 of  $G(\sigma, g_1g_2)/\Delta$  can have length at least two, all the other pairs of vertices linked by an edge of the type  $\cdots\Delta\cdots$  must form classes of  $\Delta$ . It appears also that  $j_0 (= 2$  here) is unique up to its replacement by  $c_{2l}^l(j_0) (= 6$  here).

( $\gamma_3$ ) Now, notice that the case  $(\gamma_2)$  implies the existence of two loops with length 1 in  $G(\sigma, g_1g_2)/\Delta$ : indeed, the edges

$$(l, i, j_0) \rightarrow (l, i, c_{2l}(j_0)), \quad (l, i, c_{2l}^l(j_0)) \rightarrow (l, i, c_{2l}^{l+1}(j_0))$$

of  $G(\sigma, g_1g_2)$  give rise to the edges

$$\{(l, i, j_0), (l, i, c_{2l}(j_0))\} \circlearrowleft \quad \{(l, i, c_{2l}^l(j_0)), (l, i, c_{2l}^{l+1}(j_0))\} \circlearrowright$$

in  $G(\sigma, g_1g_2)/\Delta$ . The respective colors of these edges are

$$\begin{cases} 1, 1 & \text{if } j_0 \text{ is odd, } l \text{ even,} \\ 1, 2 & \text{if } j_0 \text{ is odd, } l \text{ odd,} \\ 2, 2 & \text{if } j_0 \text{ is even, } l \text{ even,} \\ 2, 1 & \text{if } j_0 \text{ is even, } l \text{ odd.} \end{cases}$$

Hence this case is excluded if  $A_1 = A_2 = \{2\}$ , and if  $A_1 = \{2\}, A_2 = \{1, 2\}$ , then  $j_0$  and  $l$  have to be even.

e) So we have proved that the only non singleton classes of  $\Delta$  are of two types:

- I.  $\{(l, i, j), (l, i', j')\}$  with  $l \in [p]$ ,  $i \neq i' \in [N_l(\sigma)]$ ,  $j, j' \in [2l]$ , and if there is such a class  $\{(l, i, j), (l, i', j')\}$  in  $\Delta$ , then there is a unique  $q \in [l]$  (depending symmetrically on  $i$  and  $i'$ ) such that the classes, in  $\Delta$ , of  $(l, i, 1), (l, i, 2), \dots, (l, i, 2l), (l, i', 1), (l, i', 2), \dots, (l, i', 2l)$  are given by (15). We shall denote this integer  $q$  by  $q_\Delta(l, \{i, i'\})$ .
- II.  $\{(l, i, j), (l, i, j')\}$  with  $l \in [p]$ ,  $i \in [N_l(\sigma)]$ ,  $j, j' \in [2l]$ , and that if there is such a class  $\{(l, i, j), (l, i, j')\}$  in  $\Delta$ , then there is  $j_0 \in [2l]$ , unique up to a replacement by  $c_{2l}^l(j_0)$  such that the classes, in  $\Delta$ , of  $(l, i, 1), (l, i, 2), \dots, (l, i, 2l)$  are given by (16).

We denote by  $T_l(\Delta)$  the set of such  $i$ 's in  $[N_l(\sigma)]$ .

If  $A_1 = A_2 = \{2\}$ , then this case cannot occur, hence  $T_l(\Delta) = \emptyset$ .

If  $A_1 = A_2 = \{1, 2\}$ , then there is no restriction on  $l$  and  $j_0$ , and we shall denote the unique element of  $\{j_0, c_{2l}^l(j_0)\} \cap [l]$  by  $q_\Delta(l, \{i\})$ .

If  $A_1 = \{2\}$ ,  $A_2 = \{1, 2\}$ , then the only restriction on  $l, j_0$  is that they have to be even, and we shall denote the unique element of  $\{\frac{1}{2}j_0, \frac{1}{2}c_{2l}^l(j_0)\} \cap [\frac{l}{2}]$  by  $q_\Delta(l, \{i\})$ .

If  $i \in [N_l(\sigma)]$  is such that for all  $j \in [2l]$ , the singleton  $\{(l, i, j)\}$  is a class of  $\Delta$ , then we define  $q_\Delta(l, \{i\})$  to be 0.

f) Let us define, for  $l \in [p]$ ,  $P_l(\Delta)$  to be the partition of  $[N_l(\sigma)]$  which links to elements  $i, i'$  if and only if there is  $j, j' \in [2l]$  such that  $(l, i, j)$  and  $(l, i', j')$  are linked by  $\Delta$  (we use the convention that the empty set has a unique partition, that this partition has cardinality zero and that if  $N_l(\sigma) = 0$ ,  $P_l(\Delta)$  is this partition).

g) It is easily seen that the number of vertices of  $G(\sigma, w)/\Delta$  is

$$\sum_{l=1}^p 2l|P_l(\Delta)| - l|T_l(\Delta)|,$$

that the sum of the number of 1-colored loops of length two and of the number of 2-colored loops of length two in  $G(\sigma, w)/\Delta$  is

$$\sum_{l=1}^p 2l|\{C \in P_l(\Delta); |C| = 2\}| + (l-1)|T_l(\Delta)|$$

and that the sum of the number of 1-colored loops of length one and of the number of 2-colored loops of length one in  $G(\sigma, w)/\Delta$  is

$$\sum_{l=1}^p 2|T_l(\Delta)|.$$

Hence by a), the Neagu characteristic of  $G(\sigma, w)/\Delta$  is

$$\begin{aligned} & \left( \sum_{l=1}^p 2l|P_l(\Delta)| - l|T_l(\Delta)| \right) - 2p + \left( \sum_{l=1}^p 2l|\{C \in P_l(\Delta); |C| = 2\}| + (l-1+1)|T_l(\Delta)| \right) \\ & = -2p + 2 \sum_{l=1}^p l(|P_l(\Delta)| + |\{C \in P_l(\Delta); |C| = 2\}|). \end{aligned}$$

But since for all  $l$ ,  $P_l(\Delta)$  is a partition of  $[N_l(\sigma)]$  where all classes have cardinality one or two,  $|P_l(\Delta)| + |\{C \in P_l(\Delta); |C| = 2\}| = |[N_l(\sigma)]| = N_l(\sigma)$ . Hence since  $\sum_{l=1}^p lN_l(\sigma) = p$  (recall indeed that  $\sigma$  is a permutation of  $[p]$ ), the Neagu characteristic of  $G(\sigma, w)/\Delta$  is null.

i) In the case where  $A_1 = A_2 = \{1, 2\}$ , let us prove that cardinality of  $C(\sigma, g_1 g_2, \{1, 2\}, \{1, 2\})$  is

$$(17) \quad \prod_{l=1}^p \mathbb{E}[(\sqrt{l}X + l + 1)^{N_l(\sigma)}],$$

for  $X$  normal standard random variable. Note first that if  $C(\sigma)$  denotes  $\{l \in [p]; N_l(\sigma) \neq 0\}$ , then (17) reduces to

$$\prod_{l \in C(\sigma)} \mathbb{E}[(\sqrt{l}X + l + 1)^{N_l(\sigma)}].$$

Note also that since all odd moments of  $X$  are null, for all  $l \in [p]$ ,

$$(18) \quad \mathbb{E}[(\sqrt{l}X + l + 1)^{N_l(\sigma)}] = \sum_{i=0}^{\lfloor N_l(\sigma)/2 \rfloor} \binom{N_l(\sigma)}{2i} l^i \mathbb{E}(X^{2i})(l + 1)^{N_l(\sigma) - 2i}.$$

Let us define, for  $N \geq 1$ ,  $\text{Part}_{2,1}(N)$  to be the set of partitions of  $[N]$  in which all classes have cardinality 1 or 2.

It is easy to see that the function

$$\begin{aligned} \varphi : C(\sigma, g_1 g_2, \{1, 2\}, \{1, 2\}) &\rightarrow \{(P_l, (q(l, A))_{A \in P_l})_{l \in C(\sigma)}; \forall l \in C(\sigma), P_l \in \text{Part}_{2,1}(N_l(\sigma)), \\ &\quad \forall A \in P_l \text{ such that } |A| = 2, q(l, A) \in [l] \text{ and} \\ &\quad \forall A \in P_l \text{ such that } |A| = 1, q(l, A) \in \{0\} \cup [l]\} \\ \Delta &\mapsto (P_l(\Delta), (q_\Delta(l, A))_{A \in P_l(\Delta)})_{l \in C(\sigma)} \end{aligned}$$

is a bijection. Hence by (18), it suffices to prove that for all  $l \geq 1$ ,  $N \geq 1$ , the cardinality of the set of pairs  $(P, (q(A))_{A \in P})$  such that  $P \in \text{Part}_{2,1}(N)$  and for all  $A \in P$ ,  $q(A) \in [l]$  if  $|A| = 2$  and  $q(A) \in \{0\} \cup [l]$  in the other case, is equal to

$$\sum_{i=0}^{\lfloor N/2 \rfloor} \binom{N}{2i} l^i \mathbb{E}(X^{2i})(l + 1)^{N - 2i}.$$

It follows easily from the well known fact (called Wick's formula) that for all  $i \geq 1$ , the number of partitions of a set with cardinality  $2i$  in which all classes have two elements is equal to  $\mathbb{E}(X^{2i})$ .

To prove that cardinalities of  $C(\sigma, g_1 g_2, \{2\}, \{2\})$  and of  $C(\sigma, g_1 g_2, \{2\}, \{1, 2\})$  are the ones given in the statement of the lemma, we use the same technique, replacing the bijection  $\varphi$  by the respective bijections

$$\begin{aligned} \phi : C(\sigma, g_1 g_2, \{2\}, \{2\}) &\rightarrow \{(P_l, (q(l, A))_{A \in P_l})_{l \in C(\sigma)}; \forall l \in C(\sigma), P_l \in \text{Part}_{2,1}(N_l(\sigma)) \text{ and} \\ &\quad \forall A \in P_l \text{ such that } |A| = 2, q(l, A) \in [l], \\ &\quad \forall A \in P_l \text{ such that } |A| = 1, q(l, A) = 1\} \\ \Delta &\mapsto (P_l(\Delta), (q_\Delta(l, A))_{A \in P_l(\Delta)})_{l \in C(\sigma)} \end{aligned}$$

$$\begin{aligned} \psi : C(\sigma, g_1 g_2, \{2\}, \{1, 2\}) &\rightarrow \{(P_l, (q(l, A))_{A \in P_l})_{l \in C(\sigma)}; \forall l \in C(\sigma), P_l \in \text{Part}_{2,1}(N_l(\sigma)), \\ &\quad \forall l \in C(\sigma), \forall A \in P_l \text{ such that } |A| = 2, q(l, A) \in [l], \\ &\quad \forall l \text{ even}, \forall A \in P_l \text{ such that } |A| = 1, q(l, A) \in \{0\} \cup [l/2]\} \text{ and} \\ &\quad \forall l \text{ odd}, \forall A \in P_l \text{ such that } |A| = 1, q(l, A) = 1\} \\ \Delta &\mapsto (P_l(\Delta), (q_\Delta(l, A))_{A \in P_l(\Delta)})_{l \in C(\sigma)} \end{aligned}$$

□

**Proof of theorem 3.10.** (i) Let us fix  $q \geq 1$ . To prove that the law of  $(N_1(\sigma_n), \dots, N_q(\sigma_n))$  converges weakly to  $\mu_1 \otimes \dots \otimes \mu_q$ , we are going to apply theorem 1.5 of [BG07] for  $l_1 = 1, l_2 = 2, \dots, l_q = q$  and  $\mu_1, \dots, \mu_q$  the probability measures given in the statement of theorem 3.10 (i). Note that for all  $q$ -tuple of non negative integers  $k = (k_1, \dots, k_q)$ , denoting  $k_1 1 + \dots + k_q q$  by  $p$ , for all  $\sigma \in \mathfrak{S}_p$  which has  $k_1$  cycles of length 1,  $\dots$ ,  $k_q$  cycles of length  $q$ , proposition 2.18 and lemma 3.13 allow us to claim that

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

converges, as  $n$  goes to infinity, to

$$S_k := \frac{1}{1^{k_1} \dots q^{k_q} k_1! \dots k_q!} \prod_{l=1}^p \mathbb{E}[(\sqrt{l}X + l + 1)^{N_l(\sigma)}] = \prod_{l=1}^q \frac{1}{k_l!} \mathbb{E}[(\sqrt{l}X + l + 1)/l]^{k_l},$$

where  $X$  is a standard Gaussian random variable. Hence we have to prove that for all  $r_1, \dots, r_q \geq 0$ , the series

$$\sum_{k_1 \geq r_1} \dots \sum_{k_q \geq r_q} (-1)^{k_1 - r_1 + \dots + k_q - r_q} \binom{k_1}{r_1} \dots \binom{k_q}{r_q} \prod_{l=1}^q \frac{1}{k_l!} \mathbb{E}[(\sqrt{l}X + l + 1)/l]^{k_l}$$

converges to  $\prod_{l=1}^q \mu_l(r_l)$ , which is equal, by lemma 3.12, to  $\prod_{l=1}^q e^{-1 - \frac{1}{2l}} \frac{\mathbb{E}[(X + \sqrt{l})^{r_l}]}{r_l! l^{r_l/2}}$ . First of all,

note that since this series factorize and by remark 1.6 of [BG07], it suffices to prove that for  $l \geq 1, r \geq 1$ , the series  $\sum_{k \geq r} (-1)^{k-r} \binom{k}{r} \frac{1}{k!} \mathbb{E}[(\sqrt{l}X + l + 1)/l]^k$  converges to  $e^{-1 - \frac{1}{2l}} \frac{\mathbb{E}[(X + \sqrt{l})^r]}{r! l^{r/2}}$ .

It follows from an application of the dominated convergence theorem to the sequence  $Y_n :=$

$$\sum_{r \leq k \leq n+r} (-1)^{k-r} \binom{k}{r} \frac{1}{k!} ((\sqrt{l}X + l + 1)/l)^k, \text{ which converges to } Y := \frac{((\sqrt{l}X + l + 1)/l)^r}{r!} e^{-(\sqrt{l}X + l + 1)/l}$$

and is dominated by  $\frac{|(\sqrt{l}X + l + 1)/l|^r}{r!} e^{|\sqrt{l}X + l + 1|/l}$ . Indeed,

$$\mathbb{E}(Y) = \frac{1}{r! l^{\frac{r}{2}}} \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} \left(x + \frac{1}{\sqrt{l}} + \sqrt{l}\right)^r e^{-\frac{1}{2}(x^2 + 2\frac{x}{\sqrt{l}} + \frac{1}{l}) + \frac{1-2l-2}{2l}} dx = e^{-1 - \frac{1}{2l}} \frac{\mathbb{E}[(X + \sqrt{l})^r]}{r! l^{r/2}}.$$

(ii) Let us fix  $q \geq 1$ . Let us apply theorem 1.5 of [BG07] for  $l_1 = 1, l_2 = 2, \dots, l_q = q$  and  $\mu_1, \dots, \mu_q$  the push-forwards by the function  $x \mapsto 2x$  of respectively Poisson(1/2), Poisson(1/4),  $\dots$ , Poisson(1/2l). Note that for all  $k = (k_1, \dots, k_q)$   $q$ -tuple of non negative integers, denoting  $k_1 1 + \dots + k_q q$  by  $p$ , for all  $\sigma \in \mathfrak{S}_p$  which has  $k_1$  cycles of length 1,  $\dots$ ,  $k_q$  cycles of length  $q$ , proposition 2.18 and lemma 3.13 allow us to claim that

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

converges, as  $n$  goes to infinity, to

$$S_k := \frac{1}{1^{k_1} \dots q^{k_q} k_1! \dots k_q!} \prod_{l=1}^p \mathbb{E}[(1 + \sqrt{l}X)^{N_l(\sigma)}] = \prod_{l=1}^q \frac{1}{k_l!} \mathbb{E}[(1 + \sqrt{l}X)/l]^{k_l},$$

where  $X$  is a standard Gaussian random variable. Hence we have to prove that for all  $r_1, \dots, r_q \geq 0$ , the series

$$\sum_{k_1 \geq r_1} \dots \sum_{k_q \geq r_q} (-1)^{k_1 - r_1 + \dots + k_q - r_q} \binom{k_1}{r_1} \dots \binom{k_q}{r_q} \prod_{l=1}^q \frac{1}{k_l!} \mathbb{E}[(1 + \sqrt{l}X)/l]^{k_l}$$

converges to 0 if one of the  $r_i$ 's is odd, and to  $\prod_{1 \leq l \leq q} e^{-\frac{1}{2l}} \frac{1}{(r_l/2)!} \frac{1}{(2l)^{r_l/2}}$  in the other case.

First of all, note that since this series factorize and by remark 1.6 of [BG07], it suffices to prove that for  $l \geq 1$ ,  $r \geq 1$ , the series  $\sum_{k \geq r} (-1)^{k-r} \binom{k}{r} \frac{1}{k!} \mathbb{E}[(1 + \sqrt{l}X)/l]^k$  converges to

0 if  $r$  is odd, and to  $e^{-\frac{1}{2l}} \frac{1}{(r/2)!} \frac{1}{(2l)^{r/2}}$  if  $r$  is even, i.e. to  $e^{-\frac{1}{2l}} \mathbb{E}(X^r)/(r!l^{\frac{r}{2}})$  for all  $r$ . It follows from an application of the dominated convergence theorem to the sequence  $Y_n := \sum_{r \leq k \leq n+r} (-1)^{k-r} \binom{k}{r} \frac{1}{k!} ((1 + \sqrt{l}X)/l)^k$ , which converges to  $Y := \frac{((1 + \sqrt{l}X)/l)^r}{r!} e^{-(1 + \sqrt{l}X)/l}$  and

is dominated by  $\frac{|(1 + \sqrt{l}X)/l|^r}{r!} e^{|1 + \sqrt{l}X|/l}$ . Indeed,

$$\mathbb{E}(Y) = \frac{1}{\sqrt{2\pi r!} l^{\frac{r}{2}}} \int_{\mathbb{R}} \left(\frac{1}{\sqrt{l}} + x\right)^r e^{-\frac{1}{2}(x^2 + 2\frac{x}{\sqrt{l}} + \frac{2}{l})} dx = \frac{e^{-\frac{1}{2l}}}{\sqrt{2\pi r!} l^{\frac{r}{2}}} \int_{\mathbb{R}} y^r e^{-\frac{y^2}{2}} dy = e^{-\frac{1}{2l}} \frac{\mathbb{E}(X^r)}{r! l^{\frac{r}{2}}}.$$

(iii) One proceeds as in (i). The only specific equality to verify here is that for all positive even integer  $l$ , the series  $\sum_{k \geq r} (-1)^{k-r} \binom{k}{r} \frac{1}{k!} \mathbb{E}[(\sqrt{l}X + l/2 + 1)/l]^k$  converges to  $e^{-\frac{l+1}{2l}} \frac{\mathbb{E}[(X + \sqrt{l}/2)^r]}{r! l^{r/2}}$ ,

where  $X$  is a standard Gaussian random variable. It follows from an application of the dominated convergence theorem to the sequence  $Y_n := \sum_{r \leq k \leq n+r} (-1)^{k-r} \binom{k}{r} \frac{1}{k!} ((\sqrt{l}X + l/2 + 1)/l)^k$ , which

converges to  $Y := \frac{((\sqrt{l}X + l/2 + 1)/l)^r}{r!} e^{-(\sqrt{l}X + l/2 + 1)/l}$  and is dominated. Indeed,

$$\mathbb{E}(Y) = \frac{1}{r! l^{\frac{r}{2}}} \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} \left(x + \frac{1}{\sqrt{l}} + \sqrt{l}/2\right)^r e^{-\frac{1}{2}(x^2 + 2\frac{x}{\sqrt{l}} + \frac{l+1}{l}) - \frac{l+1}{2l}} dx = e^{-\frac{l+1}{2l}} \frac{\mathbb{E}[(X + \sqrt{l}/2)^r]}{r! l^{r/2}}.$$

□

## 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.
- [BG07] Benaych-Georges, Florent *Cycles of random permutations with restricted cycle 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
- [MKS66] Magnus, W. Karass, A. Solitar, D. *Combinatorial group theory*. 1966
- [Ne07] Neagu, M. *Asymptotic freeness of random permutation matrices with restricted cycles lengths*. arXiv, to appear in Indiana University Math. Journal
- [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
- [Ni24] Nielsen, J *Die Isomorphismengruppe der freien Gruppen*. Math. Ann., 91 (1924), 169-209.
- [P02] Pitman, J. *Combinatorial stochastic processes. Lectures from the 32nd Summer School on Probability Theory held in Saint-Flour, July 7-24, 2002* Lecture Notes in Mathematics, 1875. Springer-Verlag, Berlin, 2006.

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`