

On the longest common subsequence of conjugation invariant random permutations

Mohamed Slim Kammoun^{*†}

Department of Mathematics and Statistics
Lancaster University
Lancaster, U.K.

`m.kammoun@lancaster.ac.uk`

Submitted: Apr 15, 2019; Accepted: Oct 4, 2020; Published: Oct 16, 2020

© The author. Released under the CC BY-ND license (International 4.0).

Abstract

Bukh and Zhou conjectured that the expectation of the length of the longest common subsequence of two i.i.d. random permutations of size n is greater than \sqrt{n} . We prove in this paper that there exists a universal constant n_0 such that their conjecture is satisfied for any pair of i.i.d. conjugation invariant permutations of size greater than n_0 . More generally, in the case where the laws of the two permutations are not necessarily the same, we give a lower bound for the expectation. In particular, we prove that if one of the permutations is conjugation invariant and with a good control of the expectation of the number of its cycles, the limiting fluctuations of the length of the longest common subsequence are of Tracy-Widom type. This result holds independently of the law of the second permutation.

Mathematics Subject Classifications: 60C05, 60B20, 60F05, 05A16, 05A05.

1 Introduction and statements of the main results

Let \mathfrak{S}_n be the symmetric group, namely the group of permutations of $\{1, \dots, n\}$. Given $\sigma \in \mathfrak{S}_n$, $(\sigma(i_1), \dots, \sigma(i_k))$ is a subsequence of σ of length k if $i_1 < i_2 < \dots < i_k$. We denote by $LCS(\sigma, \rho)$ the length of the longest common subsequence (LCS) of the two permutations σ and ρ .

^{*}Mainly supported by the Labex CEMPI ANR-11-LABX-0007-01.

[†]Partially supported by a Leverhulme Trust Research Project Grant RPG-2020-103.

Historically, the study of the LCS of random words preceded that of permutations. For further details, one can see, for example, [19]. The study of the LCS of independent random permutations was initiated by Houdré and Işlak who proved in [6], using the simple argument that when at least one of the permutations is uniform, $LCS(\sigma_n, \rho_n)$ behaves like the length of the longest increasing subsequence of a uniform random permutation. A direct consequence is that

$$\mathbb{E}(LCS(\sigma_n, \rho_n)) \geq \sqrt{n}.$$

Bukh and Zhou conjectured in [2] that this bound holds true for i.i.d. random permutations of \mathfrak{S}_n . Recently, Houdré and Işlak showed in [7] that for i.i.d. random permutations of \mathfrak{S}_n , the minimal expectation is not attained by the uniform permutation and that

$$\mathbb{E}(LCS(\sigma_n, \rho_n)) \geq \sqrt[3]{n}.$$

In the sequel, we consider two sequences of random permutations $(\sigma_n)_{n \geq 1}$ and $(\rho_n)_{n \geq 1}$ with joint distribution \mathbb{P} and associated expectation \mathbb{E} such that σ_n and ρ_n are independent and supported on \mathfrak{S}_n . We obtain in this article asymptotic bounds in the case where the law of at least one of the two permutations is conjugation invariant. We say that the random permutation σ_n is *conjugation invariant* if for any $\hat{\sigma} \in \mathfrak{S}_n$, $\hat{\sigma} \circ \sigma_n \circ \hat{\sigma}^{-1}$ is equal in distribution to σ_n .

We first study the case where both permutations are conjugation invariant. We give, in Theorem 1, an asymptotic lower bound for the LCS of two independent random permutations. Under a good control of the number of fixed points, we give a better bound in Proposition 2. Finally, as an application of Proposition 2, we give an asymptotically optimal lower bound for i.i.d. conjugation invariant random permutations in Corollary 3.

Theorem 1. *Assume that for any $n \geq 1$, σ_n and ρ_n are independent and that they are both conjugation invariant. Then*

$$\liminf_{n \rightarrow \infty} \frac{\mathbb{E}(LCS(\sigma_n, \rho_n))}{\sqrt{n}} \geq 2\sqrt{\theta} \simeq 0.564,$$

where θ is the unique solution of $G(2\sqrt{x}) = \frac{2+x}{12}$,

$$\begin{aligned} G &:= [0, 2] \rightarrow \left[0, \frac{1}{2}\right] \\ x &\mapsto \int_{-1}^1 \left(\Omega(s) - \left|s + \frac{x}{2}\right| - \frac{x}{2} \right)_+ ds, \end{aligned} \tag{1}$$

and

$$\Omega(s) := \begin{cases} \frac{2}{\pi}(s \arcsin(s) + \sqrt{1-s^2}) & \text{if } |s| < 1 \\ |s| & \text{if } |s| \geq 1 \end{cases}. \tag{2}$$

The function Ω appears as the Vershik-Kerov-Logan-Shepp limiting shape. For more details, one can see (11) and Figure 2. We will prove this result in Section 5 by comparing $\sigma_n^{-1} \circ \rho_n$ with the uniform distribution on \mathfrak{S}_n and the uniform distribution on the set of involutions.

Under a good control of the number of fixed points, we obtain a better bound.

Proposition 2. *Assume that for any $n \geq 1$, σ_n and ρ_n are independent and that they are both conjugation invariant.*

- If

$$\lim_{n \rightarrow \infty} \max(\mathbb{P}(\sigma_n(1) = 1), \mathbb{P}(\rho_n(1) = 1)) = 0, \quad (3)$$

then

$$\liminf_{n \rightarrow \infty} \frac{\mathbb{E}(LCS(\sigma_n, \rho_n))}{\sqrt{n}} \geq 2. \quad (4)$$

- If for some $0 < \alpha \leq 2$,

$$\liminf_{n \rightarrow \infty} \sqrt{n} \mathbb{P}(\sigma_n(1) = 1) \mathbb{P}(\rho_n(1) = 1) \geq \alpha, \quad (5)$$

then

$$\liminf_{n \rightarrow \infty} \frac{\mathbb{E}(LCS(\sigma_n, \rho_n))}{\sqrt{n}} \geq \alpha. \quad (6)$$

Consequently, we obtain the following result for i.i.d. random permutations.

Corollary 3. *Assume that for any $n \geq 1$, σ_n and ρ_n are two i.i.d. conjugation invariant random permutations. Then*

$$\liminf_{n \rightarrow \infty} \frac{\mathbb{E}(LCS(\sigma_n, \rho_n))}{\sqrt{n}} \geq 2.$$

In particular, there exists n_0 such that, for any $n > n_0$, for any i.i.d. conjugation invariant permutation σ_n and ρ_n on \mathfrak{S}_n , $\mathbb{E}(LCS(\sigma_n, \rho_n)) \geq \sqrt{n}$.

We conjecture that we can get rid of (3) and (5); the conjugation invariance is sufficient to obtain (4) which is equivalent to replace $2\sqrt{\theta}$ by 2 in Theorem 1. We will prove Proposition 2 and Corollary 3 in Section 4. The idea of the proof is to study the longest increasing subsequence of $\sigma_n^{-1} \circ \rho_n$: under a good control of the number of fixed points of the two permutations, the number of cycles of $\sigma_n^{-1} \circ \rho_n$ is sufficiently small to compare it with the uniform distribution.

When ρ_n is not conjugation invariant, we give in Theorem 4 an asymptotic lower bound on $\frac{\mathbb{E}(LCS(\sigma_n, \rho_n))}{\sqrt{n}}$. Moreover, we prove in Proposition 5 that under a good control of the number of cycles of σ_n , $\lim_{n \rightarrow \infty} \frac{\mathbb{E}(LCS(\sigma_n, \rho_n))}{\sqrt{n}} = 2$ and under a stronger control, we have Tracy-Widom fluctuations for $LCS(\sigma_n, \rho_n)$. These are stated next.

Theorem 4. Assume that for any $n \geq 1$, σ_n and ρ_n are independent and σ_n is conjugation invariant. Then

$$\liminf_{n \rightarrow \infty} \frac{\mathbb{E}(LCS(\sigma_n, \rho_n))}{\sqrt{n}} \geq G^{-1} \left(\liminf_{n \rightarrow \infty} \frac{\mathbb{E}(\#(\sigma_n))}{2n} \right),$$

where $\#(\sigma)$ is the number of cycles of σ and G is defined in (1). In particular, if $\lim_{n \rightarrow \infty} \mathbb{E} \left(\frac{\#(\sigma_n)}{n} \right) = 0$, we have

$$\liminf_{n \rightarrow \infty} \frac{\mathbb{E}(LCS(\sigma_n, \rho_n))}{\sqrt{n}} \geq 2.$$

With an additional control on the cycle structure, we have the following.

Proposition 5. Assume that for any $n \geq 1$, σ_n and ρ_n are independent and the law of σ_n is conjugation invariant.

- If $\frac{\#(\sigma_n)}{n^{\frac{1}{6}}} \xrightarrow{\mathbb{P}} 0$, then for any $s \in \mathbb{R}$,

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\frac{LCS(\sigma_n, \rho_n) - 2\sqrt{n}}{n^{\frac{1}{6}}} \leq s \right) = F_2(s),$$

where F_2 is the cumulative distribution function of the Tracy-Widom distribution.

- If $\frac{\#(\sigma_n)}{\sqrt{n}} \xrightarrow{\mathbb{P}} 0$, then $\frac{LCS(\sigma_n, \rho_n)}{\sqrt{n}} \xrightarrow{\mathbb{P}} 2$.

- If $\lim_{n \rightarrow \infty} \mathbb{E} \left(\frac{\#(\sigma_n)}{\sqrt{n}} \right) = 0$, then $\lim_{n \rightarrow \infty} \frac{\mathbb{E}(LCS(\sigma_n, \rho_n))}{\sqrt{n}} = 2$.

Note that in Theorem 4 and in Proposition 5, we do not have any assumption on the distribution of ρ_n . The proofs in Section 5 are based on a coupling argument between σ_n and a uniform permutation.

2 General tools related to the longest increasing subsequence

We will present in this section some control results related to the longest increasing subsequences. Those controls will be the main tools to prove the results presented in the previous section. Given $\sigma \in \mathfrak{S}_n$ and $1 \leq i_1 < i_2 < \dots < i_k \leq n$, the subsequence $(\sigma(i_1), \dots, \sigma(i_k))$ is an increasing subsequence of σ if $\sigma(i_1) < \dots < \sigma(i_k)$. We denote by $\ell(\sigma)$ the length of the longest increasing subsequence of σ . The study of the longest common subsequence is strongly related to the notion of the longest increasing subsequence. More precisely, we have the following classical result. For any $\sigma, \rho \in \mathfrak{S}_n$,

$$LCS(\sigma, \rho) = LCS(\sigma^{-1} \circ \sigma, \sigma^{-1} \circ \rho) = LCS(Id_n, \sigma^{-1} \circ \rho) = \ell(\sigma^{-1} \circ \rho) = \ell(\rho^{-1} \circ \sigma). \quad (7)$$

We will use in the remainder of this paper the Robinson–Schensted correspondence [15, 17]. Given $\sigma \in \mathfrak{S}_n$, we denote by $\lambda(\sigma) = \{\lambda_i(\sigma)\}_{i \geq 1}$ the shape of the image of σ by this correspondence. We will not include here a detailed description of the algorithm. For further reading, we recommend [16, Chapter 3].

One key property of $\lambda(\sigma)$ is the following. Let

$$\mathfrak{I}_1(\sigma) := \{s \subset \{1, \dots, n\} : \forall i, j \in s, (i - j)(\sigma(i) - \sigma(j)) \geq 0\}$$

and

$$\mathfrak{I}_{k+1}(\sigma) := \{s \cup s' : s \in \mathfrak{I}_k, s' \in \mathfrak{I}_1\}.$$

Greene [5] proved that for any permutation $\sigma \in \mathfrak{S}_n$,

$$\max_{s \in \mathfrak{I}_i(\sigma)} |s| = \sum_{k=1}^i \lambda_k(\sigma). \text{ In particular, } \ell(\sigma) = \max_{s \in \mathfrak{I}_1(\sigma)} |s| = \lambda_1(\sigma). \quad (8)$$

Let $L_{\lambda(\sigma)}$ be the height function of $\lambda(\sigma)$ rotated by $\frac{7\pi}{4}$ and extended by the function $x \mapsto |x|$ to obtain a function defined on \mathbb{R} . For example, if $\lambda(\sigma) = (7, 5, 2, 1, 1, \underline{0})$, then the associated function $L_{\lambda(\sigma)}$ is represented by Figure 1. The image of the uniform per-

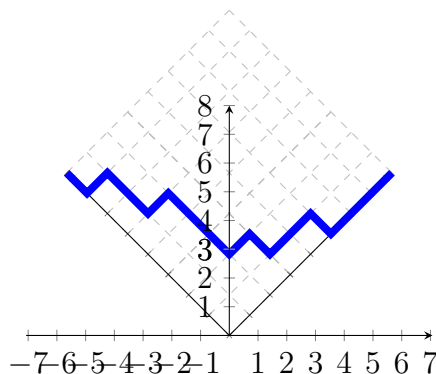


Figure 1: $L_{(7,5,2,1,1,0)}$

mutation by the Robinson–Schensted correspondence is known as the Plancherel measure. Its typical shape was studied separately by Logan and Shepp [13] and Vershik and Kerov [20]. Stronger results have been proved in [21]. In 1993, Kerov studied the limiting fluctuations but did not publish his results. One can see [8] for further details.

To prove our results, we will use the Markov operator T defined on \mathfrak{S}_n and associated to the stochastic matrix $\left[\frac{1_{A_\sigma}(\rho)}{\text{card}(A_\sigma)} \right]_{\sigma, \rho \in \mathfrak{S}_n}$ where

$$A_\sigma = \begin{cases} \{\sigma\} & \text{if } \#(\sigma) = 1 \\ \{\rho \in \mathfrak{S}_n, \sigma^{-1} \circ \rho = (i_1, i_2) \circ (i_1, i_3) \cdots \circ (i_1, i_{\#(\sigma)}) \text{ and } \#(\rho) = 1\} & \text{if } \#(\sigma) > 1 \end{cases}.$$

We recall that $\#(\sigma)$ is the number of cycles of σ . T is then the Markov operator mapping a permutation σ to a permutation uniformly chosen at random among the permutations obtained by merging the cycles of σ using transpositions having all a common point. Note that A_σ is not empty since any choice of one point in each cycle gives a possible $(i_1, i_2, \dots, i_{\#(\sigma)})$ and a correspondent permutation ρ . We obtain then the following control.

Lemma 6. *For any permutation $\sigma \in \mathfrak{S}_n$, almost surely,*

$$\max_{i \geq 1} \left| \sum_{k=1}^i (\lambda_k(\sigma) - \lambda_k(T(\sigma))) \right| \leq \#(\sigma). \quad (9)$$

In particular, almost surely,

$$|\ell(T(\sigma)) - \ell(\sigma)| \leq \#(\sigma). \quad (10)$$

Moreover, for any conjugation invariant random permutation σ_n on \mathfrak{S}_n , the law of $T(\sigma_n)$ is the uniform distribution on permutations with a unique cycle.

Note that the uniform distribution on permutations with a unique cycle is also known as the Ewens' distribution with parameter 0. We denote it by $Ew(0)$. An interesting property of $Ew(0)$ is the following. Assume that the distribution of $\tilde{\sigma}_n$ is $Ew(0)$. Then for all $\varepsilon > 0$,

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\sup_{s \in \mathbb{R}} \left| \frac{1}{\sqrt{2n}} L_{\lambda(\tilde{\sigma}_n)}(s\sqrt{2n}) - \Omega(s) \right| < \varepsilon \right) = 1, \quad (11)$$

where we recall that Ω is defined in (2). This is a particular case of [9, Theorem 1.8]. For the remainder of this paper, we will refer to this limiting shape as the Vershik-Kerov-Logan-Shepp shape. See Figure 2¹. This convergence is closely related to the Wigner's semi-circular law. For further details, one can see [10, 12, 11, 18].

Proof of Lemma 6. Let $\sigma \in \mathfrak{S}_n$ be a permutation. By definition of $\ell(\sigma)$, there exist $i_1 < i_2 < \dots < i_{\ell(\sigma)}$ such that $\sigma(i_1) < \dots < \sigma(i_{\ell(\sigma)})$. Let $\rho = \sigma \circ (j_1, j_2) \circ (j_1, j_3) \circ \dots \circ (j_1, j_{\#(\sigma)})$ be a permutation with a unique cycle and i'_1, i'_2, \dots, i'_m be the same sequence as $i_1, i_2, \dots, i_{\ell(\sigma)}$ after removing $j_1, j_2, \dots, j_{\#(\sigma)}$ if needed. We have $\ell(\sigma) - \#(\sigma) \leq m$ and $\sigma(i'_1) < \dots < \sigma(i'_m)$. As for all $i \notin \{j_1, j_2, \dots, j_{\#(\sigma)}\}$, $\rho(i) = \sigma(i)$, so that $\rho(i'_1) < \dots < \rho(i'_m)$. Therefore, $m \leq \ell(\rho)$ and $\ell(\sigma) - \ell(\rho) \leq \#(\sigma)$. We can obtain the reverse inequality in (10) using the same techniques. Similarly, to prove (9), let $l \geq 1$ and $\{i_1, i_2, \dots, i_{\sum_{k=1}^l \lambda_k(\sigma)}\} \in \mathfrak{I}_l(\sigma)$. The equality (8) guarantees the existence of such integers. Let i'_1, i'_2, \dots, i'_m be the same sequence as $i_1, i_2, \dots, i_{\sum_{k=1}^l \lambda_k(\sigma)}$ after removing $j_1, j_2, \dots, j_{\#(\sigma)}$ if needed. We have $\{i'_1, i'_2, \dots, i'_m\} \in \mathfrak{I}_l(\rho)$ and we conclude as in the proof of

¹This figure is generated by DPPy [4]

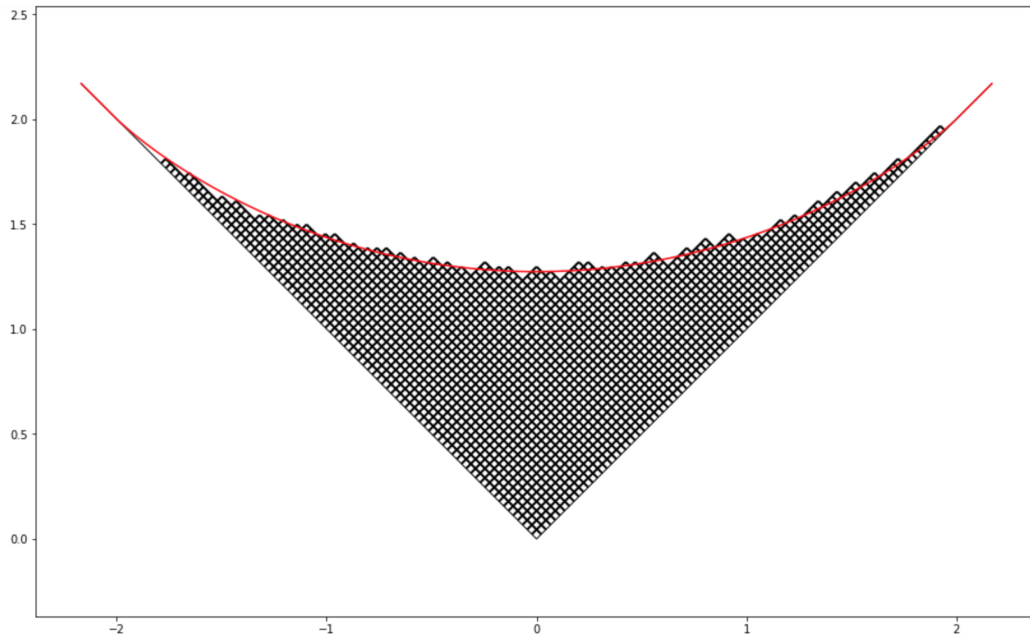


Figure 2: Illustration of the Vershik-Kerov-Logan-Shepp convergence

(10). To prove the last part of this result, one can check that the law of $T(\sigma_n)$ is clearly conjugation invariant. Indeed, let $\sigma, \rho \in \mathfrak{S}_n$.

$$\begin{aligned}
 \mathbb{P}(T(\sigma_n) = \sigma) &= \mathbf{1}_{\#(\sigma)=1} \sum_{\hat{\sigma} \in \mathfrak{S}_n} \mathbf{1}_{\sigma \in A_{\hat{\sigma}}} \frac{\mathbb{P}(\sigma_n = \hat{\sigma})}{\text{card}(A_{\hat{\sigma}})} \\
 &= \mathbf{1}_{\#(\sigma)=1} \sum_{\hat{\sigma} \in \mathfrak{S}_n} \mathbf{1}_{\rho \circ \sigma \circ \rho^{-1} \in A_{\rho \circ \hat{\sigma} \circ \rho^{-1}}} \frac{\mathbb{P}(\rho \circ \sigma_n \circ \rho^{-1} = \rho \circ \hat{\sigma} \circ \rho^{-1})}{\text{card}(A_{\rho \circ \hat{\sigma} \circ \rho^{-1}})} \\
 &= \mathbf{1}_{\#(\sigma)=1} \sum_{\hat{\sigma} \in \mathfrak{S}_n} \mathbf{1}_{\rho \circ \sigma \circ \rho^{-1} \in A_{\hat{\sigma}}} \frac{\mathbb{P}(\rho \circ \sigma_n \circ \rho^{-1} = \hat{\sigma})}{\text{card}(A_{\hat{\sigma}})} \\
 &= \mathbf{1}_{\#(\rho \circ \sigma \circ \rho^{-1})=1} \sum_{\hat{\sigma} \in \mathfrak{S}_n} \mathbf{1}_{\rho \circ \sigma \circ \rho^{-1} \in A_{\hat{\sigma}}} \frac{\mathbb{P}(\sigma_n = \hat{\sigma})}{\text{card}(A_{\hat{\sigma}})} \\
 &= \mathbb{P}(T(\sigma_n) = \rho \circ \sigma \circ \rho^{-1}).
 \end{aligned}$$

Moreover, by construction, almost surely, $\#(T(\sigma_n)) = 1$. Consequently, the law of $T(\sigma_n)$ is $Ew(0)$. \square

For more details, one can see [9]. We used the same techniques of proof with a different Markov operator. Here, the bound is better thanks to the use of the same point i_1 to merge cycles. The key control lemma will be the following.

Lemma 7. For any permutation $\sigma \in \mathfrak{S}_n$, for any $\alpha \geq 0$, almost surely,

$$\left| \sum_{i=1}^{\infty} (\lambda_i(\sigma) - \alpha\sqrt{n})_+ - \sum_{i=1}^{\infty} (\lambda_i(T(\sigma)) - \alpha\sqrt{n})_+ \right| \leq \#(\sigma), \quad (12)$$

$$\sup \left\{ k \in \mathbb{N}, \sum_{i=1}^{\infty} (\lambda_i(T(\sigma)) - k)_+ \geq \#(\sigma) \right\} \leq \ell(\sigma), \quad (13)$$

and

$$\sup \left\{ k \in \mathbb{N}, \sum_{i=1}^{\infty} (\lambda_i(\sigma) - k)_+ \geq \#(\sigma) \right\} \leq \ell(T(\sigma)). \quad (14)$$

Proof. We prove first that

$$\sum_{i=1}^{\infty} (\lambda_i(\sigma) - \alpha\sqrt{n})_+ - \sum_{i=1}^{\infty} (\lambda_i(T(\sigma)) - \alpha\sqrt{n})_+ \leq \#(\sigma).$$

If $\lambda_1(\sigma) \leq \alpha\sqrt{n}$, the inequality is trivial as the right-hand side is non-negative and the left-hand side is non-positive. Otherwise, let $k := \max\{j \geq 1, \lambda_j(\sigma) > \alpha\sqrt{n}\}$. We have

$$\sum_{i=1}^{\infty} (\lambda_i(\sigma) - \alpha\sqrt{n})_+ = \sum_{i=1}^k (\lambda_i(\sigma) - \alpha\sqrt{n})_+ + \sum_{i=k+1}^{\infty} (\lambda_i(\sigma_n) - \alpha\sqrt{n})_+ = \sum_{i=1}^k (\lambda_i(\sigma) - \alpha\sqrt{n}),$$

and

$$\sum_{i=1}^{\infty} (\lambda_i(T(\sigma)) - \alpha\sqrt{n})_+ \geq \sum_{i=1}^k (\lambda_i(T(\sigma)) - \alpha\sqrt{n})_+ \geq \sum_{i=1}^k (\lambda_i(T(\sigma)) - \alpha\sqrt{n}).$$

Using (9), we obtain

$$\sum_{i=1}^{\infty} (\lambda_i(\sigma) - \alpha\sqrt{n})_+ - \sum_{i=1}^{\infty} (\lambda_i(T(\sigma)) - \alpha\sqrt{n})_+ \leq \sum_{i=1}^k \lambda_i(\sigma) - \lambda_i(T(\sigma)) \leq \#(\sigma).$$

The reverse inequality in (12) is obtained by exchanging the role of σ and $T(\sigma)$. Finally, Using the equivalence between $\{\ell(\sigma) > k\}$ and $\{\sum_{i=1}^{\infty} (\lambda_i(\sigma) - k)_+ > 0\}$, (13) and (14) are a direct application of (12). \square

Lemma 7 implies the following asymptotic controls.

Lemma 8. Assume that the distribution of $\tilde{\sigma}_n$ is $Ew(0)$ on \mathfrak{S}_n . Then for any $0 \leq \gamma \leq 2$, for any $\varepsilon > 0$,

$$\mathbb{P} \left(\frac{\sum_{i=1}^n (\lambda_i(\tilde{\sigma}_n) - \gamma\sqrt{n})_+}{n} > 2G(\gamma) - \varepsilon \right) \rightarrow 1. \quad (15)$$

Consequently, for any $\alpha < 2$, there exist $\beta > 0$ and $n_\alpha > 0$ such that for any $n > n_\alpha$, for any conjugation invariant random permutation σ_n satisfying $\mathbb{E}(\#\sigma_n) < n\beta$, we have

$$\mathbb{E}(\ell(\sigma_n)) \geq \alpha\sqrt{n}.$$

Proof. This is a direct application of (11). One can see that $\frac{\sum_{i=1}^n (\lambda_i(\sigma) - \gamma\sqrt{n})_+}{2n}$ is the area of the region delimited by the curves of the functions $x \mapsto |x|$, $x \mapsto \gamma + x$ and $x \mapsto \frac{L_{\lambda(\sigma)}(x\sqrt{2n})}{\sqrt{2n}}$, see Figure 3. By construction, this area is equal to

$$\int_{-\infty}^{\infty} \left(\frac{L_{\lambda(\sigma)}(s\sqrt{2n})}{\sqrt{2n}} - \left| s + \frac{\gamma}{2} \right| - \frac{\gamma}{2} \right)_+ ds.$$

By (11),

$$\int_{-1}^1 \left(\frac{L_{\lambda(\tilde{\sigma}_n)}(s\sqrt{2n})}{\sqrt{2n}} - \left| s + \frac{\gamma}{2} \right| - \frac{\gamma}{2} \right)_+ ds \xrightarrow{\mathbb{P}} G(\gamma).$$

We can conclude then that

$$\begin{aligned} \frac{\sum_{i=1}^n (\lambda_i(\tilde{\sigma}_n) - \gamma\sqrt{n})_+}{n} &= 2 \int_{-\infty}^{\infty} \left(\frac{L_{\lambda(\tilde{\sigma}_n)}(s\sqrt{2n})}{\sqrt{2n}} - \left| s + \frac{\gamma}{2} \right| - \frac{\gamma}{2} \right)_+ ds \\ &\geq 2 \int_{-1}^1 \left(\frac{L_{\lambda(\tilde{\sigma}_n)}(s\sqrt{2n})}{\sqrt{2n}} - \left| s + \frac{\gamma}{2} \right| - \frac{\gamma}{2} \right)_+ ds \xrightarrow{\mathbb{P}} 2G(\gamma). \end{aligned}$$

This yields (15).

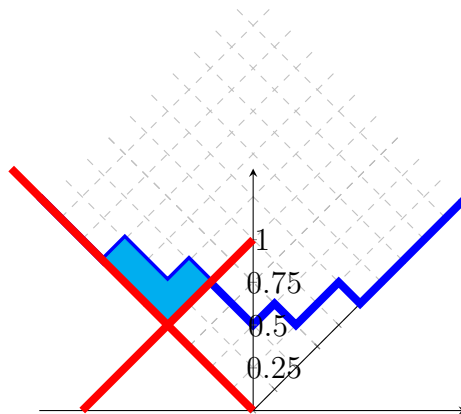


Figure 3: $\lambda = (7, 2, 2, 1, 1, \underline{0})$ and $\gamma = 1$

Note that it is not difficult to prove that

$$\frac{\sum_{i=1}^n (\lambda_i(\sigma_n) - \gamma\sqrt{n})_+}{n} \xrightarrow{\mathbb{P}} 2G(\gamma).$$

We do not provide the proof of this last fact here as we only need (15) in the sequel.

Now Let $\alpha < \gamma < 2$, $\varepsilon > 0$ and $\beta > 0$ such that $1 - \frac{\beta}{G(\gamma)} - \varepsilon > \frac{\alpha}{\gamma}$. Using (15), we obtain the existence of n_α such that for any $n > n_\alpha$,

$$\mathbb{P} \left(\frac{\sum_{i=1}^n (\lambda_i(T(\sigma_n)) - \gamma\sqrt{n})_+}{n} > G(\gamma) \right) > 1 - \varepsilon.$$

Since $\{\ell(\sigma) > k\}$ is equivalent to $\{\sum_{i=1}^{\infty}(\lambda_i(\sigma) - k)_+ > 0\}$ and by Markov inequality, we obtain

$$\begin{aligned}\mathbb{E}(\ell(\sigma_n)) &\geq \gamma\sqrt{n}\mathbb{P}(\ell(\sigma_n) \geq \gamma\sqrt{n}) \\ &\geq \gamma\sqrt{n}\mathbb{P}\left(\frac{\sum_{i=1}^n(\lambda_i(T(\sigma_n)) - \gamma\sqrt{n})_+}{n} > G(\gamma), \frac{\#(\sigma_n)}{n} < G(\gamma)\right) \\ &\geq \gamma\sqrt{n}\left(1 - \frac{\beta}{G(\gamma)} - \varepsilon\right) \geq \alpha\sqrt{n}.\end{aligned}\quad \square$$

3 Cycle structure of a product of two permutations

To prove Proposition 2 and Corollary 3, we distinguish two cases. For the first case, we suppose that the number of fixed points is large enough. We use the fact that for a given permutation, the length of the longest increasing subsequence is bigger than the number of fixed points. For the second case, when the number of fixed points is controlled, we prove in Lemma 12 that the number of cycles of $(\sigma_n)^{-1} \circ \rho_n$ is sufficiently small to compare its longest increasing subsequence with that of the uniform distribution. In both cases, we can conclude by (7). To prove Lemma 12, we will introduce in this section some new objects. To a couple of permutations, we will associate a couple of graphs.

We denote by \mathbb{G}_k^n the set of oriented graphs with vertices $\{1, 2, \dots, n\}$ and having exactly k edges. We allow here loops but not multiple edges.

For example, $\mathbb{G}_1^2 = \left\{ \begin{array}{c} \text{1} \rightarrow \text{2} \\ \text{2} \rightarrow \text{1} \\ \text{1} \rightarrow \text{1} \\ \text{2} \rightarrow \text{2} \end{array} \right\}.$

Given $g \in \mathbb{G}_k^n$, we denote by E_g the set of its edges and by $A_g := [\mathbb{1}_{(i,j) \in E_g}]_{1 \leq i,j \leq n}$ its adjacency matrix. A connected component of g is called *trivial* if it does not have any edge and a vertex i of g is called *isolated* if E_g does not contain any edge of the form (i, j) or (j, i) . We say that two oriented simple graphs g_1 and g_2 are *isomorphic* if one can obtain g_2 by changing the labels of the vertices of g_1 . In particular, if $g_1, g_2 \in \mathbb{G}_k^n$ then g_1, g_2 are isomorphic if and only if there exists a permutation matrix σ such that $A_{g_1}\sigma = \sigma A_{g_2}$. Let $g \in \mathbb{G}_k^n$, we denote by \tilde{g} the graph obtained from g after removing isolated vertices. Let \mathcal{R} be the equivalence relation such that $g_1 \mathcal{R} g_2$ if \tilde{g}_1 and \tilde{g}_2 are isomorphic. We denote by $\hat{\mathbb{G}}_k := \cup_{n \geq 1} \mathbb{G}_k^n / \mathcal{R}$ the set of equivalence classes of $\cup_{n \geq 1} \mathbb{G}_k^n$ for the relation \mathcal{R} .

For example, $\begin{array}{c} \text{1} \rightarrow \text{2} \\ \text{2} \rightarrow \text{1} \end{array} \mathcal{R} \begin{array}{c} \text{1} \rightarrow \text{1} \\ \text{2} \rightarrow \text{2} \end{array}$ and $\hat{\mathbb{G}}_1 = \left\{ \begin{array}{c} \text{ } \rightarrow \text{ } \\ \text{ } \rightarrow \text{ } \end{array} \right\}.$

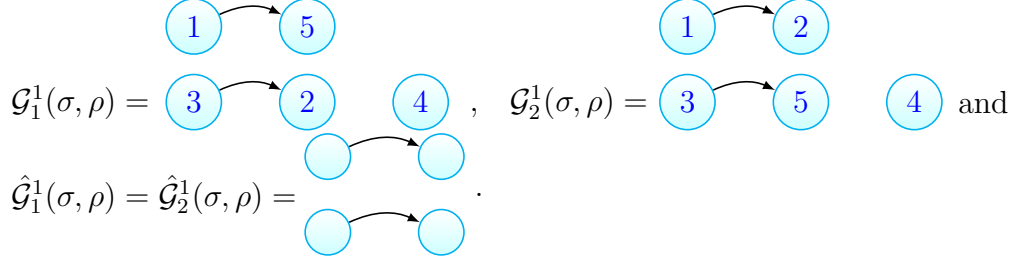
Let n be a positive integer and $\sigma, \rho \in \mathfrak{S}_n$. Let $k_m := c_m(\sigma^{-1} \circ \rho)$, $(i_1^m = m, i_2^m, \dots, i_{k_m}^m)$ be the cycle of $\sigma^{-1} \circ \rho$ containing m and $j_l^m := \rho(i_l^m)$. In particular, $i_1^m, i_2^m, \dots, i_{k_m}^m$ are pairwise distinct and $j_1^m, j_2^m, \dots, j_{k_m}^m$ are pairwise distinct. We denote by $\mathcal{G}_1^m(\sigma, \rho) \in \mathbb{G}_{k_m}^n$ the graph such that $E_{\mathcal{G}_1^m(\sigma, \rho)} = \{(i_1^m, j_{k_m}^m)\} \cup \left(\bigcup_{l=1}^{k_m-1} \{(i_l^m, j_{l+1}^m)\}\right)$. We denote also by $\mathcal{G}_2^m(\sigma, \rho) \in \mathbb{G}_{k_m}^n$ the graph such that $E_{\mathcal{G}_2^m(\sigma, \rho)} = \bigcup_{l=1}^{k_m} \{(i_l^m, j_l^m)\}$. In particular, $\mathcal{G}_1^m(\sigma, \rho)$

and $\mathcal{G}_2^m(\sigma, \rho)$ have the same set of non-isolated vertices. For $i \in \{1, 2\}$, let $\hat{\mathcal{G}}_i^m(\sigma, \rho)$ be the equivalence class of $\mathcal{G}_i^m(\sigma, \rho)$.

For example, if

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix} \quad \text{and} \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix},$$

we obtain $E_{\mathcal{G}_1^1(\sigma, \rho)} = \{(1, 5), (3, 2)\}$, $E_{\mathcal{G}_2^1(\sigma, \rho)} = \{(1, 2), (3, 5)\}$,



Finally, given $g \in \mathbb{G}_k^n$, we denote by $\mathfrak{S}_{n,g} := \{\sigma \in \mathfrak{S}_n : \forall (i, j) \in E_g, \sigma(i) = j\}$. It is not difficult to prove the two following results.

Lemma 9. *If $m_1 \in \{i_l^{m_2} : 1 \leq l \leq k_{m_2}\}$, then $\mathcal{G}_1^{m_1}(\sigma, \rho) = \mathcal{G}_1^{m_2}(\sigma, \rho)$ and $\mathcal{G}_2^{m_1}(\sigma, \rho) = \mathcal{G}_2^{m_2}(\sigma, \rho)$.*

Proof. If $m_1 \in \{i_l^{m_2} : 1 \leq l \leq k_{m_2}\}$, then there exists $1 \leq l \leq k_{m_1}$ such that $(\sigma_1^{-1} \circ \rho)^l(m_1) = m_2$. Consequently, $k_{m_1} = k_{m_2}$,

$$(i_1^{m_2}, i_2^{m_2}, \dots, i_{k_{m_2}}^{m_2}) = (i_l^{m_1}, i_{l+1}^{m_1}, \dots, i_{k_{m_1}}^{m_1}, i_1^{m_1}, \dots, i_{l-1}^{m_1})$$

$$\text{and } (j_1^{m_2}, j_2^{m_2}, \dots, j_{k_{m_2}}^{m_2}) = (j_l^{m_1}, j_{l+1}^{m_1}, \dots, j_{k_{m_1}}^{m_1}, j_1^{m_1}, \dots, j_{l-1}^{m_1})$$

and we can check easily that $\mathcal{G}_1^{m_1}(\sigma, \rho) = \mathcal{G}_1^{m_2}(\sigma, \rho)$ and $\mathcal{G}_2^{m_1}(\sigma, \rho) = \mathcal{G}_2^{m_2}(\sigma, \rho)$. \square

To obtain a combinatorial control, we prove first the following result.

Proposition 10. *Let $g_1, g_2 \in \mathbb{G}_k^n$. Assume that there exists $\rho \in \mathfrak{S}_n$ such that $A_{g_2}\rho = \rho A_{g_1}$. If ρ has a fixed point on any non-trivial connected component of g_1 , then $\mathfrak{S}_{n,g_1} \cap \mathfrak{S}_{n,g_2} = \emptyset$ or $A_{g_1} = A_{g_2}$.*


Proof. Let $\rho \in \mathfrak{S}_n$ be a permutation having a fixed point on any non-trivial connected component of g_1 such that $A_{g_2}\rho = \rho A_{g_1}$. Assume that $A_{g_1} \neq A_{g_2}$. There exists necessarily $(i, j) \in E_{g_1}$ such that $\rho(i) = i$ and $\rho(j) \neq j$ or $\rho(j) = j$ and $\rho(i) \neq i$. This is true because if we choose any connected component of g_1 having a non fixed point of ρ , this component contains by hypotheses at least one fixed point of ρ . Since this component contains both fixed and non-fixed points of ρ , one can choose two adjacent points one a fixed and the other a non-fixed point ρ . In the first case ($\rho(i) = i$ and $\rho(j) \neq j$), $\mathfrak{S}_{n,g_1} \cap \mathfrak{S}_{n,g_2} \subset \{\sigma \in \mathfrak{S}_n : \sigma(i) = j, \sigma(i) = \rho(j)\} = \emptyset$. In the second case, $\mathfrak{S}_{n,g_1} \cap \mathfrak{S}_{n,g_2} \subset \{\sigma \in \mathfrak{S}_n : \sigma(i) = j, \sigma(\rho(i)) = j\} = \emptyset$. \square

This yields the following.

Corollary 11. For any graph $g \in \mathbb{G}_k^n$ having p non-trivial connected components and v non-isolated vertices, for any conjugation invariant random permutation σ_n on \mathfrak{S}_n ,

$$\mathbb{P}(\sigma_n \in \mathfrak{S}_{n,g}) \leq \frac{(n-v)!}{(n-p)!}.$$

Proof. If there exist i, j, l , with $j \neq l$ such that $\{(i, j) \cup (i, l)\} \subset E_g$ or $\{(j, i) \cup (l, i)\} \subset E_g$ then $\mathfrak{S}_{n,g} = \emptyset$. Therefore, if $\mathfrak{S}_{n,g} \neq \emptyset$, then non-trivial connected components of g having w vertices are either cycles of length w or isomorphic to \bar{g}_w , where $A_{\bar{g}_w} = [\mathbb{1}_{j=i+1}]_{1 \leq i, j \leq w}$.

For example, $\bar{g}_5 =$ . Let $g \in \mathbb{G}_k^n$ such that $\mathfrak{S}_{n,g} \neq \emptyset$. Fix p vertices x_1, x_2, \dots, x_p each belonging to a different non-trivial connected components of g . Let $\{x_1, x_2, \dots, x_p, \dots, x_v\}$ be the set of non-isolated vertices of g . Let

$$F = \{(y_i)_{p+1 \leq i \leq v}; y_i \in \{1, \dots, n\} \setminus \{x_1, \dots, x_p\} \text{ pairwise distinct}\}.$$

Given $y = (y_i)_{p+1 \leq i \leq v} \in F$, we denote by $g_y \in \mathbb{G}_k^n$ the graph isomorphic to g obtained by fixing the labels of x_1, x_2, \dots, x_p and by changing the labels of x_i by y_i for $p+1 \leq i \leq v$. Since non trivial connected components of g of length w are either cycles or isomorphic to \bar{g}_w , if $y \neq y' \in F$, then $g_y \neq g_{y'}$ and by Proposition 10, $\mathfrak{S}_{n,g_y} \cap \mathfrak{S}_{n,g_{y'}} = \emptyset$. Since σ_n is conjugation invariant, we have $\mathbb{P}(\sigma_n \in \mathfrak{S}_{n,g_y}) = \mathbb{P}(\sigma_n \in \mathfrak{S}_{n,g_{y'}}) = \mathbb{P}(\sigma_n \in \mathfrak{S}_{n,g})$. Therefore,

$$\mathbb{P}(\sigma_n \in \mathfrak{S}_{n,g}) = \frac{\sum_{y \in F} \mathbb{P}(\sigma_n \in \mathfrak{S}_{n,g_y})}{\text{card}(F)} = \frac{\mathbb{P}(\sigma_n \in \cup_{y \in F} \mathfrak{S}_{n,g_y})}{\text{card}(F)} \leq \frac{1}{\text{card}(F)} = \frac{(n-v)!}{(n-p)!}. \quad \square$$

4 Proof of Proposition 2 and Corollary 3

The key lemma to prove Proposition 2 and Corollary 3 is the following.

Lemma 12. For any $k \geq 2$, there exists $C, C' > 0$ such that for any $n \geq 1$, for any independent random permutations σ_n and ρ_n with conjugation invariant distributions,

$$\mathbb{P}(c_1((\sigma_n)^{-1} \circ \rho_n) = k) \leq \frac{C}{n} + C'(\mathbb{P}(\sigma_n(1) = 1) + \mathbb{P}(\rho_n(1) = 1)),$$

where $c_m(\sigma)$ is the length of the cycle of σ containing m .

Proof. Note that $\hat{\mathbb{G}}_k$ is finite. Therefore, it is sufficient to prove that for any $\hat{g}_1, \hat{g}_2 \in \hat{\mathbb{G}}_k$ having the same number of vertices, there exist two constants $C_{\hat{g}_1, \hat{g}_2}$ and $C'_{\hat{g}_1, \hat{g}_2}$ such that for any integer n ,

$$\mathbb{P}((\hat{\mathcal{G}}_1^1(\sigma_n, \rho_n), \hat{\mathcal{G}}_2^1(\sigma_n, \rho_n)) = (\hat{g}_1, \hat{g}_2)) \leq \frac{C_{\hat{g}_1, \hat{g}_2}}{n} + C'_{\hat{g}_1, \hat{g}_2}(\mathbb{P}(\sigma_n(1) = 1) + \mathbb{P}(\rho_n(1) = 1)).$$

Let $\hat{g}_1, \hat{g}_2 \in \hat{\mathbb{G}}_k$ be two unlabeled graphs having respectively p_1 and p_2 connected component and $v \leq 2k$ vertices. Let $B_{\hat{g}_1, \hat{g}_2}^n$ be the set of couples $(g_1, g_2) \in (\mathbb{G}_k^n)^2$ having the same non-isolated vertices such that 1 is a non-isolated vertex of both graphs and, for $i \in \{1, 2\}$, the equivalence class of g_i is \hat{g}_i .

- Suppose that \hat{g}_1 and \hat{g}_2 do not contain any loop i.e. no edges of type (i, i) . Then $p_1 \leq \frac{v}{2}$ and $p_2 \leq \frac{v}{2}$. Consequently,

$$\begin{aligned}
& \mathbb{P}((\hat{\mathcal{G}}_1^1(\sigma_n, \rho_n), \hat{\mathcal{G}}_2^1(\sigma_n, \rho_n)) = (\hat{g}_1, \hat{g}_2)) \\
&= \sum_{(g_1, g_2) \in B_{\hat{g}_1, \hat{g}_2}^n} \mathbb{P}((\mathcal{G}_1^1(\sigma_n, \rho_n), \mathcal{G}_2^1(\sigma_n, \rho_n)) = (g_1, g_2)) \\
&\leq \sum_{(g_1, g_2) \in B_{\hat{g}_1, \hat{g}_2}^n} \mathbb{P}(\sigma_n \in \mathfrak{S}_{n, g_1}, \rho_n \in \mathfrak{S}_{n, g_2}) \\
&= \sum_{(g_1, g_2) \in B_{\hat{g}_1, \hat{g}_2}^n} \mathbb{P}(\sigma_n \in \mathfrak{S}_{n, g_1}) \mathbb{P}(\rho_n \in \mathfrak{S}_{n, g_2}) \\
&\leq \sum_{(g_1, g_2) \in B_{\hat{g}_1, \hat{g}_2}^n} \frac{(n-v)!}{(n-p_1)!} \frac{(n-v)!}{(n-p_2)!} \\
&= \text{card}(B_{\hat{g}_1, \hat{g}_2}^n) \frac{(n-v)!}{(n-p_1)!} \frac{(n-v)!}{(n-p_2)!} \\
&\leq \binom{n-1}{v-1} v!^2 \frac{(n-v)!}{(n-p_1)!} \frac{(n-v)!}{(n-p_2)!} \\
&\leq C_{g_1, g_2} n^{v-1-(v-p_1+v-p_2)} = C_{g_1, g_2} n^{p_1+p_2-v-1} \leq \frac{C_{g_1, g_2}}{n}.
\end{aligned}$$

- Suppose that \hat{g}_1 contains a loop. By Lemma 9, if $\hat{\mathcal{G}}_1^m(\sigma, \rho) = \hat{g}_1$, then there exists j a fixed point of σ such that $k_j = k$ and $j \in \{i_l^m, 1 \leq l \leq k\}$. Thus, almost surely,

$$\sum_{i=1}^n \mathbf{1}_{\hat{\mathcal{G}}_1^i(\sigma_n, \rho_n) = \hat{g}_1} \leq k \text{ card}(\{i \in \text{fix}(\sigma_n) : k_i = k\}) \leq k \text{ card}(\text{fix}(\sigma_n)),$$

where $\text{fix}(\sigma)$ is the set of fixed points of σ . Consequently, since σ_n is conjugation invariant,

$$\begin{aligned}
\mathbb{P}\left((\hat{\mathcal{G}}_1^1(\sigma_n, \rho_n), \hat{\mathcal{G}}_2^1(\sigma_n, \rho_n)) = (\hat{g}_1, \hat{g}_2)\right) &\leq \mathbb{P}\left(\hat{\mathcal{G}}_1^1(\sigma_n, \rho_n) = \hat{g}_1\right) \\
&= \frac{\sum_{i=1}^n \mathbb{P}\left(\hat{\mathcal{G}}_1^i(\sigma_n, \rho_n) = \hat{g}_1\right)}{n} \\
&\leq k \frac{\mathbb{E}(\text{card}(\text{fix}(\sigma_n)))}{n} \\
&= k \mathbb{P}(\sigma_n(1) = 1).
\end{aligned}$$

Similarly, if \hat{g}_2 contains a loop, then

$$\mathbb{P}\left((\hat{\mathcal{G}}_1^1(\sigma_n, \rho_n), \hat{\mathcal{G}}_2^1(\sigma_n, \rho_n)) = (\hat{g}_1, \hat{g}_2)\right) \leq k \mathbb{P}(\rho_n(1) = 1).$$

□

We will now prove Proposition 2.

Proof of Proposition 2. Suppose that for any $n \geq 1$, σ_n and ρ_n are independent and that they are both conjugation invariant.

- Assume that

$$\liminf_{n \rightarrow \infty} \sqrt{n} \mathbb{P}(\sigma_n(1) = 1) \mathbb{P}(\rho_n(1) = 1) \geq \alpha.$$

In this case,

$$\begin{aligned} \liminf_{n \rightarrow \infty} \frac{\mathbb{E}(LCS(\sigma_n, \rho_n))}{\sqrt{n}} &\geq \liminf_{n \rightarrow \infty} \frac{\mathbb{E}(\text{card}(\text{fix}(\sigma_n \circ \rho_n^{-1})))}{\sqrt{n}} \\ &\geq \liminf_{n \rightarrow \infty} \sqrt{n} \mathbb{P}(\sigma_n(1) = 1) \mathbb{P}(\rho_n(1) = 1) \geq \alpha. \end{aligned}$$

- Assume that

$$\lim_{n \rightarrow \infty} \max(\mathbb{P}(\sigma_n(1) = 1), \mathbb{P}(\rho_n(1) = 1)) = 0. \quad (16)$$

In this case,

$$\begin{aligned} \mathbb{P}(\sigma_n^{-1} \circ \rho_n(1) = 1) &= \sum_{i=1}^n \mathbb{P}(\sigma_n(1) = i) \mathbb{P}(\rho_n(1) = i) \\ &= \mathbb{P}(\sigma_n(1) = 1) \mathbb{P}(\rho_n(1) = 1) \\ &\quad + \frac{(1 - \mathbb{P}(\sigma_n(1) = 1))(1 - \mathbb{P}(\rho_n(1) = 1))}{n-1} \\ &= o(1). \end{aligned}$$

For any conjugation invariant random permutation σ_n on \mathfrak{S}_n

$$\mathbb{E}(\#(\sigma_n)) = \mathbb{E}\left(\sum_{i=1}^n \frac{1}{c_i(\sigma_n)}\right) = \sum_{i=1}^n \mathbb{E}\left(\frac{1}{c_i(\sigma_n)}\right) = n \mathbb{E}\left(\frac{1}{c_1(\sigma_n)}\right),$$

and for $n_\beta := \lfloor \frac{1}{\beta} \rfloor + 1$, with the same β as in Lemma 8,

$$\begin{aligned} \frac{\mathbb{E}(\#(\sigma_n))}{n} &= \sum_{k=1}^{\infty} \frac{1}{k} \mathbb{P}(c_1(\sigma_n) = k) \\ &\leq \mathbb{P}(c_1(\sigma_n) = 1) + \sum_{k=2}^{n_\beta} \mathbb{P}(c_1(\sigma_n) = k) + \frac{1}{n_\beta + 1} \sum_{k=n_\beta+1}^{\infty} \mathbb{P}(c_1(\sigma_n) = k) \\ &\leq \mathbb{P}(\sigma_n(1) = 1) + \sum_{k=2}^{n_\beta} \mathbb{P}(c_1(\sigma_n) = k) + \frac{1}{n_\beta + 1}. \end{aligned}$$

Consequently, under (16), by Lemma 12, we have

$$\frac{\mathbb{E}(\#(\sigma_n \circ \rho_n^{-1}))}{n} \leq \frac{1}{n_\beta + 1} + o(1) < \beta + o(1).$$

Hence, we obtain Proposition 2 thanks to Lemma 8. \square

Proof of Corollary 3. This is a direct application of Proposition 2. In fact, if

$$\mathbb{P}(\sigma_n(1) = 1) \geq \frac{\sqrt{2}}{\sqrt[4]{n}},$$

then

$$\liminf_{n \rightarrow \infty} \sqrt{n} \mathbb{P}(\sigma_n(1) = 1) \mathbb{P}(\rho_n(1) = 1) \geq 2.$$

Otherwise,

$$\lim_{n \rightarrow \infty} \max(\mathbb{P}(\sigma_n(1) = 1), \mathbb{P}(\rho_n(1) = 1)) = 0. \quad \square$$

5 Proof of Theorem 1, Theorem 4 and Proposition 5.

By observing that if σ_n and ρ_n are independent random permutations with conjugation invariant distributions then $\sigma_n^{-1} \circ \rho_n$ is conjugation invariant, proving Theorem 1 is equivalent to prove the following.

Theorem 13. *For any sequence of conjugation invariant random permutations $\{\sigma_n\}_{n \geq 1}$,*

$$\liminf_{n \rightarrow \infty} \frac{\mathbb{E}(\ell(\sigma_n))}{\sqrt{n}} \geq 2\sqrt{\theta}.$$

The argument will be by comparison with the uniform measure on \mathfrak{S}_n and the uniform measure on the set of involutions. We will use the uniform permutation on \mathfrak{S}_n if we have few cycles. Otherwise, we will use the uniform measure on the set of involutions since it has approximately $\frac{n}{2}$ cycles with high probability. In this section, we denote by $\mathfrak{S}_n^2 := \{\sigma \in \mathfrak{S}_n, \sigma \circ \sigma = Id_n\}$ the set of involutions of \mathfrak{S}_n . If σ_n is distributed according to the uniform distribution on \mathfrak{S}_n^2 , the distribution of $\lambda(\sigma_n)$ on the set of Young diagrams \mathbb{Y}_n is known as the Gelfand distribution. For our purpose we recall that [14, Theorem 1] guarantees that

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\sup_{s \in \mathbb{R}} \left| \frac{1}{\sqrt{2n}} L_{\lambda(\sigma_n)}(s\sqrt{2n}) - \Omega(s) \right| < \varepsilon \right) = 1$$

and one can find the proof that

$$\lim_{n \rightarrow \infty} \frac{\mathbb{E}(\text{card}(\text{fix}(\sigma_n)))}{\sqrt{n}} = 1$$

in [3, Page 692, Proposition IX.19] which yields the following result.

Lemma 14. *If σ_n is conjugation invariant and supported on \mathfrak{S}_n^2 then*

$$\liminf_{n \rightarrow \infty} \frac{\mathbb{E}(\ell(\sigma_n))}{\sqrt{n}} \geq 2.$$

Idea of the proof. If $\frac{\mathbb{E}(\text{card}(\text{fix}(\sigma_n)))}{\sqrt{n}} \geq 2$ the result is trivial. Otherwise, the technique of proof is identical to that of Lemma 8. Going back to Lemma 6, we replace A_σ by

$$A'_\sigma := \{\rho \in \mathfrak{S}_n; \sigma = \rho \circ (i_1, i_2) \circ \cdots \circ (i_{\text{card}(\text{fix}(\sigma))-1}, i_{\text{card}(\text{fix}(\sigma))}), \text{fix}(\rho) = \emptyset\}$$

if n is even and by

$$A'_\sigma := \{\rho \in \mathfrak{S}_n; \sigma = \rho \circ (i_1, i_2) \circ \cdots \circ (i_{\text{card}(\text{fix}(\sigma))-2}, i_{\text{card}(\text{fix}(\sigma))-1}), \text{card}(\text{fix}(\rho)) = 1\}$$

if n is odd. We denote by T' the Markov operator on \mathfrak{S}_n^2 associated to the stochastic matrix $\left[\frac{1_{A'_\sigma}(\rho)}{\text{card}(A_\sigma)} \right]_{\sigma, \rho \in \mathfrak{S}_n^2}$. It means that we merge couples of fixed points to obtain the uniform distribution on permutations having only cycles of length 2 when n is even and having an additional fixed point when n is odd. Similarly to that we did in Lemma 6, for any permutation σ , we have the following.

- Almost surely,

$$|\ell(T'(\sigma)) - \ell(\sigma)| \leq \text{card}(\text{fix}(\sigma)).$$

- More generally, almost surely,

$$\max_{i \geq 1} \left| \sum_{k=1}^i (\lambda_k(\sigma) - \lambda_k(T'(\sigma))) \right| \leq \text{card}(\text{fix}(\sigma)).$$

Moreover, if σ_n is conjugation invariant, the law of $T'(\sigma_n)$ does not depend on the law of σ_n . Consequently, Lemma 14 follows using the same techniques as in the proof of Lemma 8. \square

For our purpose, one can obtain then a lower asymptotic bound.

Proposition 15. *Let $\{\sigma_n\}_{n \geq 1}$ be a sequence of random permutations each one being conjugation invariant. Assume that there exists a sequence $(\beta_n)_{n \geq 1}$ such that*

$$\lim_{n \rightarrow \infty} \beta_n = +\infty,$$

and for any $n \geq 1$,

$$\mathbb{P}(\text{card}(\text{fix}(\sigma_n^2)) > \beta_n) = 1.$$

Then

$$\liminf_{n \rightarrow \infty} \frac{\mathbb{E}(\ell(\sigma_n))}{\sqrt{\beta_n}} \geq 2.$$

Proof. Giving $A \subset \mathbb{N}$ finite, we denote by \mathfrak{S}_A (resp. \mathfrak{S}_A^2) the set of permutations (resp. involutions) of A . A random permutation σ_A supported on \mathfrak{S}_A is called *conjugation invariant* if for any $\sigma \in \mathfrak{S}_A$, $\sigma \circ \sigma_A \circ \sigma^{-1}$ is equal in distribution to σ_A .

Fix $\varepsilon > 0$. By Lemma 14, there exists n_0 such that for any $A \subset \mathbb{N}$ with $n_0 < \text{card}(A) < +\infty$, for any random permutation $\hat{\sigma}_A$ supported on \mathfrak{S}_A^2 conjugation invariant,

$$\frac{\mathbb{E}(\ell(\hat{\sigma}_A))}{\sqrt{\text{card}(A)}} \geq 2 - \varepsilon.$$

Let σ_n be a conjugation invariant random permutation and σ'_n be the restriction of σ_n on $\text{fix}(\sigma_n^2)$. In particular, almost surely $\ell(\sigma'_n) \leq \ell(\sigma_n)$. One can see that for any $A \subset \{1, \dots, n\}$ such that $\mathbb{P}(\text{fix}(\sigma_n^2) = A) > 0$, for any $\hat{\sigma}_1, \hat{\sigma}_2 \in \mathfrak{S}_A$,

$$\mathbb{P}(\sigma'_n = \hat{\sigma}_1 | \text{fix}(\sigma_n^2) = A) = \mathbb{P}(\sigma'_n = \hat{\sigma}_2 \circ \hat{\sigma}_1 \circ \hat{\sigma}_2^{-1} | \text{fix}(\sigma_n^2) = A). \quad (17)$$

Consequently, if $\beta_n > n_0$,

$$\begin{aligned} \frac{\mathbb{E}(\ell(\sigma_n))}{\sqrt{\beta_n}} &= \sum_{\substack{|A| > \beta_n \\ \mathbb{P}(\text{fix}(\sigma_n^2) = A) > 0}} \frac{\mathbb{E}(\ell(\sigma_n) | \text{fix}(\sigma_n^2) = A)}{\sqrt{\beta_n}} \mathbb{P}(\text{fix}(\sigma_n^2) = A) \\ &\geq \sum_{\substack{|A| > \beta_n \\ \mathbb{P}(\text{fix}(\sigma_n^2) = A) > 0}} (2 - \varepsilon) \sqrt{\frac{\text{card}(A)}{\beta_n}} \mathbb{P}(\text{fix}(\sigma_n^2) = A) \\ &\geq \sum_{\substack{|A| > \beta_n \\ \mathbb{P}(\text{fix}(\sigma_n^2) = A) > 0}} (2 - \varepsilon) \mathbb{P}(\text{fix}(\sigma_n^2) = A) = 2 - \varepsilon. \end{aligned}$$

This yields Proposition 15. □

We will now prove Theorem 13.

Proof. In this proof, we use the following convention. Let $A, B \subset \mathfrak{S}_n$ and $f : \mathfrak{S}_n \rightarrow \mathbb{R}$. If $\mathbb{P}(\sigma_n \in A) = 0$, we assign $\mathbb{P}(\sigma_n \in B | \sigma_n \in A) = 0$ and $\mathbb{E}(f(\sigma_n) | \sigma_n \in A) = 0$.

We have

$$\begin{aligned} \mathbb{E}(\ell(\sigma_n)) &= \mathbb{E}\left(\ell(\sigma_n) \middle| \#(\sigma_n) \leq \frac{(2+\theta)n}{6}\right) \mathbb{P}\left(\#(\sigma_n) \leq \frac{(2+\theta)n}{6}\right) \\ &\quad + \mathbb{E}\left(\ell(\sigma_n) \middle| \#(\sigma_n) > \frac{(2+\theta)n}{6}\right) \mathbb{P}\left(\#(\sigma_n) > \frac{(2+\theta)n}{6}\right). \end{aligned}$$

Since the condition on the number of cycles is conjugation invariant, it is sufficient to prove Theorem 13 in the two particular cases.

- Assume that almost surely $\#(\sigma_n) \leq \frac{(2+\theta)n}{6}$. By Lemma 7, for any $0 < \gamma < 2$,

$$\mathbb{P}\left(\frac{\ell(\sigma_n)}{\sqrt{n}} > \gamma\right) \geq \mathbb{P}\left(\frac{\sum_{i=1}^n (\lambda_i(T(\sigma_n)) - \gamma\sqrt{n})_+}{n} > \frac{2+\theta}{6}\right).$$

As $T(\sigma_n)$ is distributed according to the $Ew(0)$, by choosing $\gamma = 2\sqrt{\theta} - \varepsilon$ for some $\varepsilon > 0$ in Lemma 8, we can conclude that the right-hand side goes to 1 as n goes to infinity.

- Assume that almost surely $\#(\sigma_n) > \frac{(2+\theta)n}{6}$. We can write,

$$\begin{aligned}\mathbb{E}(\ell(\sigma_n)) &= \mathbb{E}\left(\ell(\sigma_n) \middle| \text{card}(\text{fix}(\sigma_n)) \geq 2\sqrt{n\theta}\right) \mathbb{P}\left(\text{card}(\text{fix}(\sigma_n)) \geq 2\sqrt{n\theta}\right) \\ &\quad + \mathbb{E}\left(\ell(\sigma_n) \middle| \text{card}(\text{fix}(\sigma_n)) < 2\sqrt{n\theta}\right) \mathbb{P}\left(\text{card}(\text{fix}(\sigma_n)) < 2\sqrt{n\theta}\right).\end{aligned}$$

Clearly, if $\mathbb{P}\left(\text{card}(\text{fix}(\sigma_n)) \geq 2\sqrt{n\theta}\right) > 0$, then

$$\mathbb{E}\left(\ell(\sigma_n) \middle| \text{card}(\text{fix}(\sigma_n)) \geq 2\sqrt{n\theta}\right) > 2\sqrt{n\theta}.$$

One can check easily that for any $\sigma \in \mathfrak{S}_n$

$$\text{card}(\text{fix}(\sigma^2)) \geq 6\#(\sigma) - 3\text{card}(\text{fix}(\sigma)) - 2n.$$

Consequently, under the condition $\text{card}(\text{fix}(\sigma_n)) < 2\sqrt{n\theta}$, almost surely,

$$\text{card}(\text{fix}(\sigma_n^2)) > \theta n - 6\sqrt{\theta n}.$$

We can then conclude by Proposition 15 that if $\mathbb{P}\left(\text{card}(\text{fix}(\sigma_n)) < 2\sqrt{n\theta}\right) > 0$, then

$$\liminf_{n \rightarrow \infty} \frac{\mathbb{E}\left(\ell(\sigma_n) \middle| \text{card}(\text{fix}(\sigma_n)) < 2\sqrt{n\theta}\right)}{\sqrt{\theta n} - 6\sqrt{n\theta}} \geq 2.$$

Thus, if $\mathbb{P}\left(\text{card}(\text{fix}(\sigma_n)) < 2\sqrt{n\theta}\right) > 0$, then

$$\liminf_{n \rightarrow \infty} \frac{\mathbb{E}\left(\ell(\sigma_n) \middle| \text{card}(\text{fix}(\sigma_n)) < 2\sqrt{n\theta}\right)}{\sqrt{n}} \geq 2\sqrt{\theta}. \quad \square$$

The proofs of Theorem 4 and Proposition 5 are based on the following observation.

Lemma 16. *For any permutations σ, ρ , almost surely,*

$$|LCS(\sigma, \rho) - LCS(T(\sigma), \rho)| \leq \#(\sigma).$$

The proof is identical to that of Lemma 6. This guarantees the convergence when one of the permutations follows the $Ew(0)$ distribution.

Lemma 17. Assume that the law of $\tilde{\sigma}_n$ is $Ew(0)$ and $\tilde{\sigma}_n$ and ρ_n are independent. Then

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\frac{LCS(\tilde{\sigma}_n, \rho_n) - 2\sqrt{n}}{n^{\frac{1}{6}}} \leq s \right) = F_2(s),$$

$$\lim_{n \rightarrow \infty} \frac{\mathbb{E}(LCS(\tilde{\sigma}_n, \rho_n))}{\sqrt{n}} = 2 \quad \text{and} \quad \frac{LCS(\tilde{\sigma}_n, \rho_n)}{\sqrt{n}} \xrightarrow[n \rightarrow \infty]{\mathbb{P}} 2.$$

This result, with a similar proof, is a consequence of a corresponding result when $\tilde{\sigma}_n$ is uniform in [6].

Proof. Note that if σ_n is distributed according the uniform distribution, one can see that the independence between σ_n and ρ_n implies that $\sigma_n^{-1} \circ \rho_n$ follows also the uniform distribution. In this case,

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\frac{LCS(\sigma_n, \rho_n) - 2\sqrt{n}}{n^{\frac{1}{6}}} \leq s \right) = \lim_{n \rightarrow \infty} \mathbb{P} \left(\frac{\ell(\sigma_n) - 2\sqrt{n}}{n^{\frac{1}{6}}} \leq s \right) = F_2(s), \quad (18)$$

$$\lim_{n \rightarrow \infty} \frac{\mathbb{E}(LCS(\sigma_n, \rho_n))}{\sqrt{n}} = \lim_{n \rightarrow \infty} \frac{\mathbb{E}(\ell(\sigma_n))}{\sqrt{n}} = 2, \quad (19)$$

and

$$\frac{LCS(\sigma_n, \rho_n)}{\sqrt{n}} \stackrel{d}{=} \frac{\ell(\sigma_n)}{\sqrt{n}} \xrightarrow[n \rightarrow \infty]{\mathbb{P}} 2. \quad (20)$$

The second equality of (18) is due to Baik, Deift and Johansson [1] and the second equality of (19) and the convergence of (20) are due to Vershik and Kerov [20]. Hence, one can conclude by Lemma 16 since $\mathbb{E}(\#(\sigma_n)) = \log(n) + O(1)$ and $LCS(\tilde{\sigma}_n, \rho_n)$ is equal in distribution to $LCS(T(\sigma_n), \rho_n)$. \square

Using again Lemma 16, Lemma 17 implies Proposition 5 since $T(\sigma_n)$ is distributed according to $Ew(0)$. Finally we give a sketch of proof of Theorem 4.

Sketch of proof of Theorem 4. Using the same technique as in Lemma 8, we can prove that for any $\varepsilon > 0$,

$$\mathbb{P} \left(\frac{LCS(\sigma_n, \rho_n)}{\sqrt{n}} > G^{-1} \left(\frac{\#(\sigma_n)}{2n} + \varepsilon \right) - \varepsilon \right) \xrightarrow[n \rightarrow \infty]{} 1.$$

Consequently,

$$\liminf_{n \rightarrow \infty} \frac{\mathbb{E}(LCS(\sigma_n, \rho_n))}{\sqrt{n}} \geq \mathbb{E} \left(G^{-1} \left(\liminf_{n \rightarrow \infty} \frac{\#(\sigma_n)}{2n} \right) \right).$$

Since G^{-1} is convex, we can conclude using Jensen's inequality. \square

Acknowledgements

The author would like to acknowledge many extremely useful conversations with Mylène Maïda, Adrien Hardy and Christan Houdré and their great help to improve the coherence of this paper. He would also acknowledge a useful discussion with Pierre-Loïc Méliot about Gelfand measures. He also thanks anonymous referees for the careful reading of the paper and their suggestions.

References

- [1] J. Baik, P. Deift, and K. Johansson. On the distribution of the length of the longest increasing subsequence of random permutations. *J. Amer. Math. Soc.*, 12(4):1119–1178, 1999.
- [2] B. Bukh and L. Zhou. Twins in words and long common subsequences in permutations. *Israel J. Math.*, 213(1):183–209, 2016.
- [3] P. Flajolet and R. Sedgewick. *Analytic Combinatorics*. Cambridge University Press, 2009.
- [4] G. Gautier, G. Polito, R. Bardenet, and M. Valko. Dppy: Dpp sampling with python. *J. Mach. Learn. Res.*, 20:180:1–180:7, 2019.
- [5] C. Greene. An extension of Schensted’s theorem. *Advances in Math.*, 14:254–265, 1974.
- [6] C. Houdré and Ü. Işlak. A central limit theorem for the length of the longest common subsequences in random words. [arXiv:1408.1559](https://arxiv.org/abs/1408.1559), 2014.
- [7] C. Houdré and C. Xu. A note on the expected length of the longest common subsequences of two i.i.d. random permutations. *Electron. J. Combin.*, 25(2):#P2.50, 2018.
- [8] V. Ivanov and G. Olshanski. Kerov’s central limit theorem for the Plancherel measure on Young diagrams. In *Symmetric functions 2001: surveys of developments and perspectives*, volume 74 of *NATO Sci. Ser. II Math. Phys. Chem.*, pages 93–151. Kluwer Acad. Publ., Dordrecht, 2002.
- [9] M. S. Kammoun. Monotonous subsequences and the descent process of invariant random permutations. *Electron. J. Probab.*, 23:31 pp., 2018.
- [10] S. Kerov. The asymptotics of interlacing sequences and the growth of continual Young diagrams. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, 205(Differential prime naya Geom. Gruppy Li i Mekh. 13):21–29, 179, 1993.
- [11] S. Kerov. A differential model for the growth of Young diagrams. In *Proceedings of the St. Petersburg Mathematical Society, Vol. IV*, volume 188 of *Amer. Math. Soc. Transl. Ser. 2*, pages 111–130. Amer. Math. Soc., Providence, RI, 1999.
- [12] S. V. Kerov. Transition probabilities of continual Young diagrams and the Markov moment problem. *Funktsional. Anal. i Prilozhen.*, 27(2):32–49, 96, 1993.

- [13] B. F. Logan and L. A. Shepp. A variational problem for random Young tableaux. *Advances in Math.*, 26(2):206–222, 1977.
- [14] P.-L. Méliot. Kerov’s central limit theorem for Schur-Weyl and Gelfand measures (extended abstract). In M. Bousquet-Mélou, M. Wachs, and A. Hultman, editors, *23rd International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC 2011)*, volume DMTCS Proceedings vol. AO, 23rd International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC 2011) of *DMTCS Proceedings*, pages 669–680, Reykjavik, Iceland, 2011. Discrete Mathematics and Theoretical Computer Science.
- [15] G. d. B. Robinson. On the Representations of the Symmetric Group. *Amer. J. Math.*, 60(3):745–760, 1938.
- [16] B. E. Sagan. *The symmetric group*, volume 203 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001. Representations, combinatorial algorithms, and symmetric functions.
- [17] C. Schensted. Longest increasing and decreasing subsequences. *Canad. J. Math.*, 13:179–191, 1961.
- [18] S. Sodin. Fluctuations of interlacing sequences. *Zurnal matematicheskoy fiziki, analiza, geometrii*, 13(4):364–401, Dec 2017.
- [19] J. Steele. *Probability Theory and Combinatorial Optimization*. CBMS-NSF Regional Conference Series in Applied Mathematics. Society for Industrial and Applied Mathematics, 1997.
- [20] A. M. Vershik and S. V. Kerov. Asymptotic behavior of the Plancherel measure of the symmetric group and the limit form of Young tableaux. *Dokl. Akad. Nauk SSSR*, 233(6):1024–1027, 1977.
- [21] A. M. Vershik and S. V. Kerov. Asymptotic behavior of the maximum and generic dimensions of irreducible representations of the symmetric group. *Funktsional. Anal. i Prilozhen.*, 19(1):25–36, 96, 1985.