

A Note on the Expected Length of the Longest Common Subsequences of two i.i.d. Random Permutations

Christian Houdré*

School of Mathematics
Georgia Institute of Technology
Atlanta, Georgia, U.S.A.

houdre@math.gatech.edu

Chen Xu

School of Mathematics
Georgia Institute of Technology
Atlanta, Georgia, U.S.A.

cxu60@gatech.edu

Submitted: Apr 17, 2017; Accepted: May 22, 2018; Published: TBD

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

Abstract

We address a question and a conjecture on the expected length of the longest common subsequences of two i.i.d. random permutations of $[n] := \{1, 2, \dots, n\}$. The question is resolved by showing that the minimal expectation is not attained in the uniform case. The conjecture asserts that $\sqrt{n}$ is a lower bound on this expectation, but we only obtain $\sqrt[3]{n}$ for it.

Mathematics Subject Classifications: 05A05, 60C05

1 Introduction

The length of the longest increasing subsequences (*LISs*) of a uniform random permutation $\sigma \in \mathcal{S}_n$ (where $\mathcal{S}_n$ is the symmetric group) is well studied and we refer to the monograph [5] for precise results and a comprehensive bibliography on this subject. Recently, [3] showed that for two independent random permutations $\sigma_1, \sigma_2 \in \mathcal{S}_n$, and as long as σ_1 is uniformly distributed and regardless of the distribution of σ_2 , the length of the longest common subsequences (*LCSs*) of the two permutations is identical in law to the length of the *LISs* of σ_1 , i.e. $LCS(\sigma_1, \sigma_2) \stackrel{\mathcal{L}}{=} LIS(\sigma_1)$. This equality ensures, in particular, that when σ_1 and σ_2 are uniformly distributed, $\mathbb{E}LCS(\sigma_1, \sigma_2)$ is upper bounded by $2\sqrt{n}$, for any n , (see [4]) and asymptotically of order $2\sqrt{n}$ ([5]). It is then rather natural to study the behavior of $LCS(\sigma_1, \sigma_2)$, when σ_1 and σ_2 are i.i.d. but not necessarily uniform. In this respect, Bukh and Zhou raised, in [2], two issues which can be rephrased as follows:

*Research supported in part by the grants # 246283 and # 524678 from the Simons Foundation.

Conjecture/Question 1. Let P be an arbitrary probability distribution on $\mathcal{S}_n$. Let σ_1 and σ_2 be two i.i.d. permutations sampled from P . Then $\mathbb{E}_P[LCS(\sigma_1, \sigma_2)] \geq \sqrt{n}$. It might even be true that the uniform distribution U on $\mathcal{S}_n$ gives a minimizer.

Below we prove the suboptimality of the uniform distribution by explicitly building a distribution having a smaller expectation. In the next section, before presenting and proving our main result, we give a few definitions and formalize this minimizing problem as a quadratic programming one. Section 3 further explore some properties of the spectrum of the coefficient matrix of our quadratic program. In the concluding section, a quick cubic root lower bound is given along with a few pointers for future research.

2 Main Results

We begin with a few notations. Throughout, σ and π are, respectively, used for random and deterministic permutations. By convention, $[n] := \{1, 2, 3, \dots, n\}$ and so $\{\pi_i\}_{i \in [n]} = \mathcal{S}_n$ is a particular ordered enumeration of $\mathcal{S}_n$. (Some other orderings of $\mathcal{S}_n$ will be given when necessary.) Next, a random permutation σ is said to be sampled from $P = (p_i)_{i \in [n!]}$, if $\mathbb{P}_P(\sigma = \pi_i) = p_i$. The uniform distribution is therefore $U = (1/n!)_{i \in [n!]}$ and, for simplification, it is denoted by $E/n!$, where $E = (1)_{i \in [n!]}$ is the n -tuple only made up of ones. When needed, a superscript will indicate the degree of the symmetric group we are studying, e.g., $\sigma^{(n)}$ and $P^{(n)}$ are respectively a random permutation and distribution from $\mathcal{S}_n$.

Let us now formalize the expectation as a quadratic form:

$$\begin{aligned} \mathbb{E}_P[LCS(\sigma_1, \sigma_2)] &= \sum_{i,j \in [n!]} p_i LCS(\pi_i, \pi_j) p_j \\ &= \sum_{i,j \in [n!]} p_i \ell_{ij} p_j = P^T L^{(n)} P, \end{aligned} \tag{1}$$

where $\ell_{ij} := LCS(\pi_i, \pi_j)$ and $L^{(n)} := \{\ell_{ij}\}_{(i,j) \in [n!] \times [n!]}$. It is clear that $\ell_{ij} = \ell_{ji}$ and that $\ell_{ii} = n$. A quick analysis of the cases $n = 2$ or 3 shows that both $L^{(2)}$ and $L^{(3)}$ are positive semi-definite. However, this property does not hold further:

Lemma 2. For $n \geq 4$, the smallest eigenvalue $\lambda_1^{(n)}$ of $L^{(n)}$ is negative.

Proof. Linear algebra gives $\lambda_1^{(2)} = 1$ and $\lambda_1^{(3)} = 0$. So to prove the result, it suffices to show that $\lambda_1^{(k+1)} < \lambda_1^{(k)}$, $k \geq 1$ and this is done by induction. The base case is true, since $\lambda_1^{(2)} = 1 > 0 = \lambda_1^{(3)}$. To reveal the connection between $L^{(k+1)}$ and $L^{(k)}$, the enumeration of $\mathcal{S}_{k+1}$ is iteratively built on that of $\mathcal{S}_k$ by inserting the new element $(k+1)$ into the permutations from $\mathcal{S}_k$ in the following way: the enumeration of the $(k+1)!$ permutations is split into $(k+1)$ trunks of equal size $k!$. In the i th trunk, the new element $(k+1)$ is inserted behind the $(k+1-i)$ th digit in the permutation from $\mathcal{S}_k$. (For example, if $\mathcal{S}_2$ is enumerated as $\{[12], [21]\}$, then the enumeration of the first trunk in $\mathcal{S}_3$ is $\{[123], [213]\}$, the second is $\{[132], [231]\}$ and the third is $\{[312], [321]\}$. Then the overall enumeration for $\mathcal{S}_3$ is $\{[123], [213], [132], [231], [312], [321]\}$.)

Via this enumeration, the principal minor of size $k! \times k!$ is row and column indexed by the enumeration of the permutations $\{\pi_i^{(k)}\}_{i \in [k!]}$ from $\mathcal{S}_k$ with $(k+1)$ as the last digit, i.e., $\{[\pi_i^{(k)}(k+1)]\}_{i \in [k!]} \subseteq \mathcal{S}_{k+1}$. Then the (i, j) entry of the submatrix is

$$LCS([\pi_i(k+1)], [\pi_j(k+1)]) = LCS(\pi_i, \pi_j) + 1,$$

since the last digit $(k+1)$ adds an extra element into the longest common subsequences. Hence, the $k! \times k!$ principal minor of $L^{(k+1)}$ is $L^{(k)} + E^{(k)}(E^{(k)})^T$, where $E^{(k)}$ is the vector of $\mathbb{R}^{k!}$ only made up of ones. Moreover, notice that the sum of the π_i -indexed row of $L^{(k)}$ is

$$\begin{aligned} \sum_{j \in [k!]} LCS(\pi_i, \pi_j) &= \sum_{j \in [k!]} LCS(id, \pi_i^{-1}\pi_j) \\ &= \sum_{j \in [k!]} LIS(\pi_i^{-1}\pi_j), \end{aligned}$$

since simultaneously relabeling π_i and π_j does not change the length of the LCS s and also since a particular relabeling to make π_i to be the identity permutation, which is equivalent to left composition by π_i^{-1} , is applied here. Further, any LCS of the identity permutation and of $\pi_i^{-1}\pi_j$ is a LIS of $\pi_i^{-1}\pi_j$ and vice versa. So the row sum is equal to

$$\sum_{j \in [k!]} LIS(\pi_i^{-1}\pi_j) = \sum_{\pi \in \mathcal{S}_k} LIS(\pi),$$

since left composition by π_i^{-1} is a bijection from $\mathcal{S}_k$ to $\mathcal{S}_k$. This indicates that all the row sums of $L^{(k)}$ are equal. Hence, $E^{(k)}$ is actually a right eigenvector of $L^{(k)}$ and is associated with the row sum $\sum_{\pi \in \mathcal{S}_k} LIS(\pi) > 0$ as its eigenvalue, which is distinct from the smallest eigenvalue $\lambda_1^{(k)} \leq 0$.

On the other hand, since $L^{(k)}$ is symmetric, the eigenvectors $R_1^{(k)}$ and $E^{(k)}$ associated with the eigenvalues $\lambda_1^{(k)}$ and $\sum_{\pi \in \mathcal{S}_k} LIS(\pi)$ are orthogonal, i.e.,

$$(E^{(k)})^T R_1^{(k)} = 0. \quad (2)$$

Without loss of generality, let $R_1^{(k)}$ be a unit vector, then from (2),

$$\begin{aligned} \lambda_1^{(k)} &= (R_1^{(k)})^T L^{(k)} (R_1^{(k)}) \\ &= (R_1^{(k)})^T (L^{(k)} + E^{(k)}(E^{(k)})^T) R_1^{(k)}. \end{aligned} \quad (3)$$

As $L^{(k)} + E^{(k)}(E^{(k)})^T$ is the $k! \times k!$ principal minor of $L^{(k+1)}$, (3) becomes

$$\begin{bmatrix} R_1^{(k)} \\ 0 \end{bmatrix}^T L^{(k+1)} \begin{bmatrix} R_1^{(k)} \\ 0 \end{bmatrix} \geq \min_{R^T E=0, \|R\|=1} R^T L^{(k+1)} R = \lambda_1^{(k+1)}, \quad (4)$$

where $R_1^{(k)}$ is properly extended to $\begin{bmatrix} R_1^{(k)} \\ 0 \end{bmatrix} \in \mathbb{R}^{(k+1)!}$ and where the above inequality holds true since $\begin{bmatrix} R_1^{(k)} \\ 0 \end{bmatrix}^T E^{(k+1)} = (R_1^{(k)})^T E^{(k)} = 0$ and $\left\| \begin{bmatrix} R_1^{(k)} \\ 0 \end{bmatrix} \right\| = \|R_1^{(k)}\| = 1$, where $\|\cdot\|$ denotes the corresponding Euclidean norm. Moreover, equality in (4) holds if and only if $\begin{bmatrix} R_1^{(k)} \\ 0 \end{bmatrix}$ is a eigenvector of $L^{(k+1)}$ associated with $\lambda_1^{(k+1)}$. We show next, by contradiction, that this cannot be the case. Indeed, assume that

$$L^{(k+1)} \begin{bmatrix} R_1^{(k)} \\ 0 \end{bmatrix} = \lambda_1^{(k+1)} \begin{bmatrix} R_1^{(k)} \\ 0 \end{bmatrix}. \quad (5)$$

Now, consider the $k! \times k!$ submatrix at the bottom-left corner of $L^{(k+1)}$, which is row-indexed by $\{(k+1)\pi_i\}_{i \in [k]}$ and column-indexed by $\{\pi_i(k+1)\}_{i \in [k]}$. Notice that the (i, j) -entry of this submatrix is

$$LCS([(k+1)\pi_i], [\pi_j(k+1)]) = LCS(\pi_i, \pi_j),$$

since $(k+1)$ can be in some LCS only if the length of this LCS is 1. So this submatrix is in fact equal to $L^{(k)}$. Further, the vector consisting of the bottom $k!$ elements on the left-hand-side of (5) is $L^{(k)} R_1^{(k)} = \lambda_1^{(k)} R_1^{(k)}$, which is a non-zero vector. However, on the right-hand-side, the corresponding bottom $k!$ elements of the vector $\begin{bmatrix} R_1^{(k)} \\ 0 \end{bmatrix}$ form the zero vector. This leads to a contradiction. So,

$$\lambda_1^{(2)} = 1 > 0 = \lambda_1^{(3)} > \lambda_1^{(4)} > \lambda_1^{(5)} \dots$$

□

The above result on the smallest negative eigenvalue, and its associated eigenvector, will help build a distribution on $\mathcal{S}_n$, for which the LCS s have a smaller expectation than for the uniform one.

Theorem 3. *Let σ_1 and σ_2 be two i.i.d. random permutations sampled from a distribution P on the symmetric group $\mathcal{S}_n$. Then, for $n \leq 3$, the uniform distribution U minimizes $\mathbb{E}_P[LCS(\sigma_1, \sigma_2)]$, while, for $n \geq 4$, U is sub-optimal.*

Proof. As we have seen in (1),

$$\begin{aligned} \mathbb{E}_P[LCS(\sigma_1, \sigma_2)] &= P^T L P \\ &= (P - U)^T L (P - U) + 2P^T L U - U^T L U \\ &= (P - U)^T L (P - U) + 2U^T L U - U^T L U \\ &= (P - U)^T L (P - U) + U^T L U, \end{aligned} \quad (6)$$

where $P^T L U = U^T L U$, since U is an eigenvector of L and $P^T U = 1$.

When $n = 2, 3$, $L^{(n)}$ is positive semi-definite and therefore $(P - U)^T L(P - U) \geq 0$. So, $P^T L P \geq U^T L U$.

However, when $n \geq 4$, by Lemma 2, the smallest eigenvalue $\lambda_1^{(n)}$ is strictly negative and the associated eigenvector $R_1^{(n)}$ is such that $U^T R_1^{(n)} = 0 = E^T R_1^{(n)}$. Hence, there exists a positive constant c such that $cR_1^{(n)} \succeq -1/n!$, where $\succeq$ stands for componentwise inequality. Let P_0 be such that $P_0 - U = cR_1^{(n)}$, then it is immediate that

$$E^T P_0 = E^T (U + cR_1^{(n)}) = 1 + 0 = 1,$$

and that

$$P_0 = U + cR_1^{(n)} \succeq 0.$$

Therefore, P_0 is a well-defined distribution on $\mathcal{S}_n$. On the other hand, by (6), the expectation under P_0 is such that

$$\begin{aligned} \mathbb{E}_{P_0}[LCS(\sigma_1, \sigma_2)] &= (P_0 - U)^T L(P_0 - U) + U^T L U \\ &= c^2 (R_1^{(n)})^T L(R_1^{(n)}) + U^T L U \\ &= c^2 \lambda_1^{(n)} + U^T L U \\ &< U^T L U. \end{aligned} \tag{7}$$

However, the right-hand side of (7) is nothing but the expectation under the uniform distribution, namely, $\mathbb{E}_U[LCS(\sigma_1, \sigma_2)]$. $\square$

The existence of negative eigenvalues contributes to the above construction and to the corresponding counterexample. So, as a next step, properties of this smallest negative eigenvalue and of the spectrum of the coefficient matrix $L^{(n)}$ are explored.

3 Further Properties of $L^{(n)}$

As we have seen, the vector $E^{(n)}$ which is made up of only ones is an eigenvector associated with the eigenvalue $\sum_{\pi \in S_n} LIS(\pi)$. It is not hard to show that this eigenvalue is, in fact, the spectral radius of $L^{(n)}$.

Proposition 4. $\sum_{\pi \in S_k} LIS(\pi)$ is the spectral radius of $L^{(n)}$.

Proof. Without loss of generality, let (λ, R) be a pair of eigenvalue and corresponding eigenvector of $L^{(n)}$ such that $\max_{i \in [n!]} |r_i| = 1$, where $R = (r_1, \dots, r_{n!})^T$, and let i_0 be the index such that $|r_{i_0}| = 1$. Let us focus now on the i_0 th element of λR . Then, since $L^{(n)}R = \lambda R$,

$$\begin{aligned} |\lambda| &= |\lambda r_{i_0}| \\ &= \left| \sum_{j \in [n!]} LCS(\pi_{i_0}, \pi_j) r_j \right| \end{aligned}$$

$$\begin{aligned}
&\leq \sum_{j \in [n!]} LCS(\pi_{i_0}, \pi_j) \\
&= \sum_{j \in [n!]} LIS(\pi_{i_0}^{-1} \pi_j) \\
&= \sum_{\pi \in S_n} LIS(\pi),
\end{aligned}$$

with equality if and only if all the r_j 's have the same sign and have absolute value equal to 1. $\square$

This gives a trivial bound on the smallest negative value $\lambda_1^{(n)}$: namely,

$$\lambda_1^{(n)} \geq - \sum_{\pi \in S_n} LIS(\pi).$$

Moreover, since the expectation of the longest increasing subsequence of a uniform random permutation is asymptotically $2\sqrt{n}$, this gives an asymptotic order of $-2n!\sqrt{n}$ for the lower bound. On the other hand, we are interested in an upper bound for $\lambda_1^{(n)}$. The next result shows that $\lambda_1^{(n)}$ decreases at least exponentially fast, in n .

Proposition 5. $\lambda_1^{(n)} \leq 2^{n-4} \lambda_1^{(4)} = -2^{n-3} < 0$.

Proof. This is proved by showing that $\lambda_1^{(n+1)} \leq 2\lambda_1^{(n)}$. As well known,

$$\lambda_1^{(n+1)} = \min_{E^T R = 0} \frac{R^T L^{(n+1)} R}{R^T R}. \quad (8)$$

Let $\lambda_1^{(n)}$ be the smallest eigenvalues of $L^{(n)}$ and let $R^{(n)}$ be the corresponding eigenvector. Then, in generating $L^{(n+1)}$ from $L^{(n)}$ as done in the proof of Lemma 2, the $n! \times n!$ principal minor of $L^{(n+1)}$ is $L^{(n)} + EE^T$, while its bottom-left $n! \times n!$ submatrix is $L^{(n)}$. Symmetrically, it can be proved that the top-right $n! \times n!$ submatrix is also $L^{(n)}$, while the bottom-right $n! \times n!$ submatrix is $L^{(n)} + EE^T$, i.e., $L^{(n+1)}$ is

$$\begin{bmatrix} L^{(n)} + EE^T & \cdots & L^{(n)} \\ \vdots & \ddots & \vdots \\ L^{(n)} & \cdots & L^{(n)} + EE^T \end{bmatrix}.$$

Further, let

$$R = \begin{bmatrix} R_1^{(n)} \\ 0 \\ \vdots \\ 0 \\ R_1^{(n)} \end{bmatrix}.$$

Then $E^T R = E^T R_1^{(n)} + E^T R_1^{(n)} = 0$, where, by an abuse of notation, E denotes the vector only made up of ones and of the appropriate dimension. Also,

$$\|R\|^2 = R^T R = 2 \left\| R_1^{(n)} \right\|^2 = 2.$$

In (8), the corresponding numerator $R^T L^{(n+1)} R$ is

$$\begin{aligned} & \begin{bmatrix} R_1^{(n)} \\ 0 \\ \vdots \\ 0 \\ R_1^{(n)} \end{bmatrix}^T \begin{bmatrix} L^{(n)} + EE^T & \cdots & L^{(n)} \\ \vdots & \ddots & \vdots \\ L^{(n)} & \cdots & L^{(n)} + EE^T \end{bmatrix} \begin{bmatrix} R_1^{(n)} \\ 0 \\ \vdots \\ 0 \\ R_1^{(n)} \end{bmatrix} \\ &= 2 \left(R_1^{(n)} \right)^T (L^{(n)} + EE^T) \left(R_1^{(n)} \right) + 2 \left(R_1^{(n)} \right)^T L^{(n)} \left(R_1^{(n)} \right) \\ &= 4 \left(R_1^{(n)} \right)^T L^{(n)} \left(R_1^{(n)} \right) = 4\lambda_1^{(n)}. \end{aligned}$$

Thus,

$$\lambda_1^{(n+1)} \leq 2\lambda_1^{(n)}.$$

□

By a very similar method, it can also be proved, as shown next, that the second largest eigenvalue $\lambda_{n!-1}^{(n)}$, which is positive, grows at least exponentially fast.

Proposition 6. $\lambda_{n!-1}^{(n)} \geq 2^{n-2} \lambda_1^{(2)} = 2^{n-2} > 0$.

Proof. Using the identity

$$\lambda_{(n+1)!-1}^{(n+1)} = \max_{E^T R=0} \frac{R^T L^{(n+1)} R}{R^T R},$$

with a particular choice of

$$R = \begin{bmatrix} R_{n!-1}^{(n)} \\ 0 \\ \vdots \\ 0 \\ R_{n!-1}^{(n)} \end{bmatrix},$$

where $R_{n!-1}^{(n)}$ is the eigenvector associated with the second largest eigenvalue $\lambda_{n!-1}^{(n)}$ of $L^{(n)}$, leads to $\lambda_{(n+1)!-1}^{(n+1)} \geq 2\lambda_{n!-1}^{(n)}$ and thus proves the result. □

The above bounds for $\lambda_1^{(n)}$ and $\lambda_{n!-1}^{(n)}$ are far from tight even as far as their asymptotic orders are concerned. Numerical evidence is collected in the following table:

n	$\lambda_1^{(n)}$	$\lambda_1^{(n+1)}/\lambda_1^{(n)}$	$\lambda_{n!-1}^{(n)}$	$\lambda_{(n+1)!-1}^{(n+1)}/\lambda_{n!-1}^{(n)}$
4	-2	1	6.6055	1
5	-5.0835	2.5417	30.0293	4.5460
6	-20.2413	3.9817	166.1372	5.5324
7	-102.9541	5.0860	1083.7641	6.5233

A reasonable conjecture will be that both the smallest and the second largest eigenvalues grow at a factorial-like speed. More precisely, we believe that

$$\lim_{n \rightarrow +\infty} \frac{\lambda_1^{(n+1)}}{\lambda_1^{(n)}(n-1)} = c_1 \geq 1,$$

and that

$$\lim_{n \rightarrow +\infty} \frac{\lambda_{(n+1)!-1}^{(n+1)}}{\lambda_{n!-1}^{(n)}(n+1/2)} = c_2 \geq 1.$$

4 Concluding Remarks

The $\sqrt{n}$ lower-bound conjecture of Bukh and Zhou is still open and seems quite reasonable in view of the fact that $\mathbb{E}LCS(\sigma_1, \sigma_2) \sim 2\sqrt{n}$, in case σ_1 is uniform and σ_2 arbitrary (again, see [3]). We do not have a proof of this conjecture, but let us nevertheless present, next, a quick $\sqrt[3]{n}$ lower bound result.

We start with a lemma describing a balanced property among the lengths of the LCS s of pairs of any three arbitrary deterministic permutations. This result is essentially due to Beame and Huynh-Ngoc ([1]).

Lemma 7. *For any $\pi_i \in \mathcal{S}_n$ ($i = 1, 2, 3$),*

$$LCS(\pi_1, \pi_2)LCS(\pi_2, \pi_3)LCS(\pi_3, \pi_1) \geq n.$$

Proof. The proof of Lemma 5.9 in [1] applies here with slight modification. We further note that this inequality is tight, since letting $\pi_1 = \pi_2 = id$ and $\pi_3 = rev(id)$, which is the reversal of the identity permutation gives, $LCS(\pi_1, \pi_2)LCS(\pi_2, \pi_3)LCS(\pi_3, \pi_1) = n$. $\square$

In Lemma 7, taking $(\pi_1, \pi_2) = (id, rev(id))$ gives, for any third permutation π_3 , $LCS(id, \pi_3)LCS(rev(id), \pi_3) \geq n/LCS(id, rev(id)) = n$. But, since $LCS(id, \pi_3)$ and $LCS(rev(id), \pi_3)$ are respectively the lengths of the longest increasing/decreasing subsequences of π_3 , this lemma can be considered to be a generalization of a well-known classical result of Erdős and Szekeres (see [5]).

We are now ready for the cubic root lower bound.

Proposition 8. *Let P be an arbitrary probability distribution on $\mathcal{S}_n$ and let σ_1 and σ_2 be two i.i.d. random permutations sampled from P . Then, for any $n \geq 1$, $\mathbb{E}_P[LCS(\sigma_1, \sigma_2)] \geq \sqrt[3]{n}$.*

Proof. Let π_1, π_2 and $\pi_3 \in S_n$ and set

$$L(\pi_i) := \sum_{\pi_1 \in S_n} p(\pi_1) LCS(\pi_1, \pi_i) = \sum_{\pi_1 \in S_n} LCS(\pi_i, \pi_1) p(\pi_1),$$

for $i = 2, 3$. Then,

$$\begin{aligned} & L(\pi_2) + LCS(\pi_2, \pi_3) + L(\pi_3) \\ &= \sum_{\pi_1 \in S_n} p(\pi_1) (LCS(\pi_1, \pi_2) + LCS(\pi_2, \pi_3) + LCS(\pi_3, \pi_1)) = 3\sqrt[3]{n} \sum_{\pi_1 \in S_n} p(\pi_1) = 3\sqrt[3]{n}, \end{aligned} \quad (9)$$

by the arithmetic mean-geometric mean inequality and the previous lemma. Further, summing over $p(\pi_2)$ in (9) gives:

$$\begin{aligned} & \sum_{\pi_2 \in S_n} p(\pi_2) (L(\pi_2) + LCS(\pi_2, \pi_3) + L(\pi_3)) \\ &= \sum_{\pi_2 \in S_n} p(\pi_2) L(\pi_2) + L(\pi_3) + L(\pi_3) \geq 3\sqrt[3]{n}. \end{aligned}$$

Repeating this last procedure but with weights over $p(\pi_3)$ leads to

$$\sum_{\pi_2 \in S_n} p(\pi_2) L(\pi_2) + 2 \sum_{\pi_3 \in S_n} p(\pi_3) L(\pi_3) = 3 \sum_{\pi \in S_n} p(\pi) L(\pi) \geq 3\sqrt[3]{n}. \quad (10)$$

However,

$$\begin{aligned} \mathbb{E}_P[LCS(\sigma_1, \sigma_2)] &= \sum_{\pi_1 \in S_n} \sum_{\pi_2 \in S_n} p(\pi_1) LCS(\pi_1, \pi_2) p(\pi_2) \\ &= \sum_{\pi_1 \in S_n} p(\pi_1) \sum_{\pi_2 \in S_n} LCS(\pi_1, \pi_2) p(\pi_2) \\ &= \sum_{\pi \in S_n} p(\pi) L(\pi). \end{aligned}$$

Combining this last identity with (10) proves the result. $\square$

The above proof is simple; it basically averages out each $LCS(\cdot, \cdot)$ as $\sqrt[3]{n}$ on the summation weighted by P . However, in view of the original conjecture, our partial results, as well as those mentioned in the introductory section, the cubic root lower-bound is not tight. Apart from our curiosity concerning this $\sqrt{n}$ conjecture, it would be interesting to know the exact asymptotic order of the smallest eigenvalue $\lambda_1^{(n)}$ of $L^{(n)}$. In contrast, the largest eigenvalue $\lambda_{n!}^{(n)}$ corresponding to the uniform distribution is known to be asymptotically of order $2n!\sqrt{n}$, since it is equal to the length of the *LISs* of a uniform random permutation of $[n]$ scaled by $n!$. In this sense, the study of the length of the *LCSs* between a pair of i.i.d. random permutations having an arbitrary distribution, or equivalently, the study of $L^{(n)}$, can be viewed as an extension of the study of the length of the *LISs* of a uniform random permutation of $[n]$. Having a complete knowledge of the distribution of all the eigenvalues of $L^{(n)}$ would be a nice achievement.

References

- [1] Paul Beame and Dang-Trinh Huynh-Ngoc. On the value of multiple read/write streams for approximating frequency moments. In *Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on*, pages 499–508. IEEE, 2008.
- [2] Boris Bukh and Lidong Zhou. Twins in words and long common subsequences in permutations. *Israel Journal of Mathematics*, 213(1):183–209, 2016.
- [3] Christian Houdré and Ümit Işlak. A central limit theorem for the length of the longest common subsequence in random words. *arXiv preprint arXiv:1408.1559v4*, 2017.
- [4] Shaiy Pilpel. Descending subsequences of random permutations. *Journal of Combinatorial Theory, Series A*, 53(1):96–116, 1990.
- [5] Dan Romik. *The surprising mathematics of longest increasing subsequences*, volume 4. Cambridge University Press, 2015.