A concentration bound for the longest increasing subsequence of a randomly chosen involution

Marcos Kiwi

Departamento de Ingeniería Matemática y Centro de Modelamiento Matemático, UMI 2807, Universidad de Chile, Correo 3, Santiago 170-3, Chile

Abstract

In this short note we prove a concentration result for the length of the longest increasing subsequence (LIS) of a randomly and uniformly chosen involution of $\{1, \ldots, s\}$.

Keywords: Ulam's problem; Longest increasing subsequence; Random involutions

1. Introduction

A class of problems—important for their applications to computer science and computational biology as well as for their inherent mathematical interest—is the statistical analysis of random symbols. Many applications of sequence comparison start with the observation or detection of what seems to be a high degree of similarity (or small distance) between two sequences. Often it is important to decide whether the similarity is truly large or whether it could have occurred by coincidence.

It was suspected that random string comparison problems, like the longest common subsequence (LCS) problem, were related to statistics of random permutations. This suspicion is confirmed in [11], where the 20 year old conjecture of Sankoff and Mainville [14] is proved correct. Indeed, string comparison problems are cast, in [11], as questions concerning random bipartite graphs. These questions are shown to be fundamentally intertwined with issues concerning increasing sequences of randomly chosen permutations. Symmeterized versions of the aforementioned problems concerning random bipartite graphs are easily seen to relate to increasing sequences of symmeterized randomly chosen permutations in general, and involutions in particular. It is known that the expected length of the LIS of a randomly chosen involution of $\{1, \ldots, s\}$ equals (asymptotically) $2\sqrt{s}$. It is then natural to address the following problem which has been glossed over in the literature:

How well concentrated is the length of the LIS of a randomly chosen involution of $\{1, \ldots, s\}$?

E-mail address: mkiwi@dim.uchile.cl
URL: http://www.dim.uchile.cl/∼ mkiwi.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 2 & 1 & 6 & 11 & 5 & 3 & 7 & 8 & 10 & 9 & 4 \end{pmatrix}$$

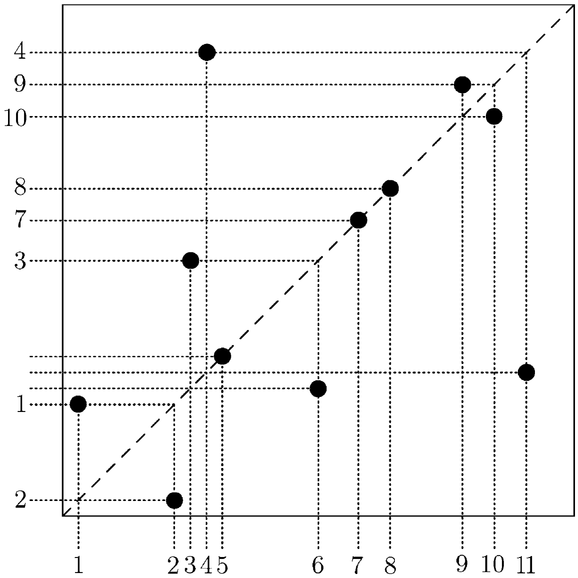

Fig. 1. Geometric view of an involution $\pi \in I_{3,4}$.

The asymptotic law (probability distribution) of the length of the LIS of a randomly chosen permutation has been extensively studied (also under the name of "Ulam's problem"). Over the last 30 years, a variety of increasingly technically sophisticated methods have been developed in order to address the problem for general permutations and involutions in particular. For an in depth discussion of these techniques see the surveys by Aldous and Diaconis [1] and Stanley [15] as well as references therein. In contrast, we focus on elementary arguments in order to address the stated concentration question.

We adopt the standard convention of denoting the set of integers $\{1, \ldots, k\}$ by $[k]$. Henceforth, we let $s = m + 2n$. We denote by $I_{m,n}$ the collection of involutions of $[s]$ with m fixed points and by $\mathscr{I}_{m,n}$ the uniform distribution over $I_{m,n}$. Similarly, we denote by $\mathscr{I}_s$ the uniform distribution over the set I_s of involutions of $[s]$. Finally, we denote by $L(\mathscr{D})$ the length of a LIS of a permutation randomly chosen according to the distribution $\mathscr{D}$. Our aim is to prove the following result.

Theorem 1. *For* $0 < \varepsilon < 1/4$ *and sufficiently large* s,

$$\mathbb{P}[|L(\mathscr{I}_s) - \mathbb{E}[L(\mathscr{I}_s)]| > \mathrm{O}(1)s^{\varepsilon+1/4}] \leqslant \mathrm{e}^{-\mathrm{O}(1)s^{2\varepsilon}}.$$

In order to achieve our objective we shall heavily rely on an alternative useful view of the $\mathscr{I}_{m,n}$ model. In it, one selects n points $P_1, \ldots, P_n$ in the off diagonal region of the square $[0, 1] \times [0, 1]$ and m points $D_1, \ldots, D_m$ in the $x = y$ diagonal of the same square. Each point is selected independently of the others and uniformly in its corresponding sample space. For $P = (x, y)$ let $P^{\boxslash} = (y, x)$ and consider the collection of points

$$\mathscr{P} = \{D_i\}_{i=1}^{m} \cup \{P_i, P_i^{\boxslash}\}_{i=1}^{n}.$$

With probability 1 no two points of $\mathscr{P}$ have the same x- nor y-coordinates. Enumerating the points in $\mathscr{P}$ according to the x-coordinate going from left to right and then reading the points' labels bottom up defines a permutation π (see Fig. 1). Clearly, π is an involution of $[s]$ with m fixed points with probability 1. Each length l increasing subsequence of

π is in one-to-one correspondence with a sequence of points $Q_1, \ldots, Q_l$ such that $Q_1 \prec \cdots \prec Q_l$, where $\prec$ denotes the canonical partial order relation for points in the plane. We shall henceforth also refer to such a sequence $Q_1, \ldots, Q_l$ as an increasing subsequence. The size of the largest such sequence is distributed as the length of the LIS of a permutation chosen according to $\mathscr{I}_{m,n}$, i.e., as the length of a randomly chosen involution of $[m+2n]$ with m fixed points [5].

We conclude this section with a high-level discussion of the strategy we employ for establishing Theorem 1. First, we prove a crude tail bound for $L(\mathscr{I}_{m,n})$ which allows us to give an upper bound for a median of $L(\mathscr{I}_{m,n})$. We then use a concentration inequality due to Talagrand [16] to derive a concentration result for the length of a LIS of an involution of $[m+2n]$ with m fixed points, i.e., a concentration result for $L(\mathscr{I}_{m,n})$. Finally, we establish Theorem 1 relying on the fact that the distribution $\mathscr{I}_s$, where $s = m+2n$, is "close" to the distribution $\mathscr{I}_{m,n}$ for $m \sim \sqrt{s}$ and $2n = s - m$.

Except for the final step, the above described proof strategy is somewhat reminiscent of and argument of Frieze [8] for deriving a concentration result for the length of a LIS of a randomly chosen permutation. However, instead of relying on the usually weaker Azuma inequality [9, Theorem 2.25] we apply Talagrand's inequality which was not available to Frieze back in the early 1990s.

2. Related work

The concentration around its mean of the length of the LIS of a permutation uniformly chosen among the permutations of $\{1, \ldots, n\}$, say LIS_n, has been studied, in particular by Frieze [8] who established a sharp concentration bound. An observation of Bollobás and Brightwell [6] concerning Frieze's proof argument yields a stronger concentration bound. Sharper results were obtained by Talagrand [16] as a simple consequence of what has become known as Talagrand's inequality (see also [7,10] for related results). In a celebrated work, Baik et al. [3] determined the asymptotic distribution of LIS_n.

The asymptotic behavior of $L(\mathscr{I}_{m,n})$ and $L(\mathscr{I}_s)$ are well understood. Their limiting distributions under different regimes were determined by Baik and Rains [4] who showed [4, Theorem 3.1] that $\mathbb{E}[L(\mathscr{I}_{m,n})]/\sqrt{m+2n} \to 2$ for $m = \lfloor\sqrt{2n}\rfloor$ as $n \to \infty$. Moreover, they also establish [4, Theorem 3.4] that $\mathbb{E}[L(\mathscr{I}_s)]/\sqrt{s} \to 2$ as $s \to \infty$.

Although the techniques of [4] should suffice for deriving a concentration bound of the sort we seek [2], they have not been applied to explicitly calculate it. Moreover, our arguments are completely self-contained and, in comparison with the techniques of [4], are quite elementary and direct.

3. Concentration bound for the length of a LIS of a randomly chosen involution

In this section, we prove Theorem 1. In order to avoid unnecessarily cumbersome notation, throughout this section we denote $L(\mathscr{I}_{m,n})$ and $L(\mathscr{I}_s)$ by $L_{m,n}$ and L_s, respectively.

First, we derive a crude bound on the upper tail of $L_{m,n}$. This will immediately imply an upper bound on a median of $L_{m,n}$.

Lemma 2. *For* $m_0 = \lfloor\sqrt{2\mathrm{e}^3 m}\rfloor$ *and* $n_0 = \lfloor\sqrt{2\mathrm{e}^3 n}\rfloor$,

$$\mathbb{P}[L_{m,n} \geqslant m_0 + n_0] \leqslant (m_0 + n_0)\mathrm{e}^{-(m_0+n_0)}.$$

Proof. We consider the geometric model of $\mathscr{I}_{m,n}$. Thus, let $\{D_i\}_{i=1}^m$ and $\{P_j, P_j^{\boxslash}\}_{j=1}^n$ be chosen as previously described. Let T denote the total number of increasing subsequences of $\{D_i\}_{i=1}^m \cup \{P_j, P_j^{\boxslash}\}_{j=1}^n$ which are of length $m_0 + n_0$. For convenience sake, we denote $m_0 + n_0$ by s_0. For $A = \{a_1, \ldots, a_i\} \subseteq [m]$ and $B = \{b_1, \ldots, b_j\} \subseteq [n]$ let $T_{A,B}$ be the indicator of the event $\mathscr{P}' = \{D_a\}_{a\in A} \cup \{P_b, P_b^{\boxslash}\}_{b\in B}$ contains an increasing subsequence of length $i + j$. Since P_b and $P_b^{\boxslash}$ cannot both belong to the same increasing sequence, it is impossible for $\mathscr{P}'$ to contain an increasing subsequence of length larger than $i + j$. In fact, for $\mathscr{P}'$ to contain a subsequence of such length it must be the case that both $\{D_a\}_{a\in A}$ and $\{P_b, P_b^{\boxslash}\}_{b\in B}$ contain increasing subsequences of length i and j, respectively. Hence, the following inequality holds and is the basis of our strategy for deriving the sought after bound:

$$\mathbb{P}[L_{m,n} \geqslant s_0] \leqslant \mathbb{E}[T] = \sum \mathbb{E}[T_{A,B}], \tag{1}$$

where the summation is over all $A \subseteq [m]$, $B \subseteq [n]$ such that $|A|=i$, $|B|=j$, and $i+j=s_0$. We thus focus on bounding $\mathbb{E}[T_{A,B}]$ for $|A|=i$, $|B|=j$, and $i+j=s_0$. We claim that

$$\mathbb{E}[T_{A,B}] = \sum_{j_1+\cdots+j_{i+1}=j} \binom{j}{j_1,\ldots,j_{i+1}} \prod_{l=1}^{i+1} \frac{2^{j_l-1}}{j_l!} \int_{\substack{y_1,\ldots,y_{i+1}\geqslant 0\\ y_1+\cdots+y_{i+1}=1}} y_1^{2j_1}\cdots y_{i+1}^{2j_{i+1}}\,\mathrm{d}y_1\ldots\mathrm{d}y_{i+1}. \tag{2}$$

In order to show that this last identity holds, recall that $\mathscr{P}'$ denotes $\{D_a\}_{a\in A} \cup \{P_b, P_b^{\boxslash}\}_{b\in B}$ and that it contains an increasing subsequence of size $i+j$ if and only if $\{D_a\}_{a\in A}$ and $\{P_b, P_b^{\boxslash}\}_{b\in B}$ contain increasing subsequences of size i and j, respectively. Since $A=\{a_1,\ldots,a_i\}$, without loss of generality we can assume that $(0,0)=D_{a_0} \prec D_{a_1} \prec D_{a_2} \prec \cdots \prec D_{a_i} \prec D_{a_{i+1}}=(1,1)$. We arrive at a crucial observation; there is an increasing subsequence of size $i+j$ in $\mathscr{P}'$ if and only if each pair $\{P_b, P_b^{\boxslash}\}$ falls within one of the squares of corners $(D_{a_{l-1}}, D_{a_l})$, $l=1,\ldots,i+1$. We can partition B according to the square on which P_b and $P_b^{\boxslash}$ lie. Summarizing, if $\mathscr{P}'$ contains an increasing subsequence of size $i+j$, then there must be an ordered partition $(B_1,\ldots,B_{i+1})$ of B such that for all $l\in\{1,\ldots,i+1\}$

$$b\in B_l \iff D_{a_{l-1}} \prec P_b, P_b^{\boxslash} \prec D_{a_l}. \tag{3}$$

Let y_l be the distance in the y-coordinate between $D_{a_{l-1}}$ and D_{a_l}. We have that (3) holds if and only if every $P\in\{P_b\}_{b\in B_l}$ lands in the square of area y_l^2 with corners $(D_{a_{l-1}}, D_{a_l})$. Let $j_l=|B_l|$. Since each $P\in\{P_b\}_{b\in B}$ is uniformly and independently chosen in the square $[0,1]\times[0,1]$ it follows that the probability that (3) holds, for a fixed ordered partition $(B_1,\ldots,B_{i+1})$ of B and all l, is $y_1^{2j_1}\cdots y_{i+1}^{2j_{i+1}}$.

We will now justify the factor in front of the integral in (2). Note that there is a one-to-one correspondence between involutions of $[2k]$ without fixed points and partitions of $[2k]$ into 2-element subsets. Hence, the number of involutions of $[2k]$ without fixed points is $(2k)!/(k!2^k)$. Let π be one such involution that has an increasing subsequence of length k, say $i_1<i_2<\cdots<i_k$ such that $i'_1=\pi(i_1)<\cdots<i'_k=\pi(i_k)$. Since π is an involution without fixed points, $\{i_1,\ldots,i_k\}$ and $\{i'_1,\ldots,i'_k\}$ are disjoint. This partition of $[2k]$ into k-element subsets uniquely determines π. Thus, there are $\binom{2k}{k}/2!$ distinct fixed point free involutions of $[2k]$ that contain an increasing subsequence of length k. The probability that there is an increasing sequence of length j_l in $\{P_b, P_b^{\boxslash}\}_{b\in B_l}$ is thus

$$\frac{\binom{2j_l}{j_l}/2!}{(2j_l)!/(j_l!2^{j_l})} = \frac{2^{j_l-1}}{j_l!}.$$

We now have all the necessary pieces to establish (2). Indeed, since $y_1,\ldots,y_{i+1}$ are not fixed in advance and can take any non-negative value subject to the restriction $y_1+\cdots+y_{i+1}=1$, we conclude that the probability that (3) holds for a given ordered partition $(B_1,\ldots,B_{i+1})$ of B, $|B_l|=j_l$, and $\{D_a\}_{a\in A}\cup\{P_b, P_b^{\boxslash}\}_{b\in B}$ contains an increasing subsequence of length $i+j$ is

$$\prod_{l=1}^{i+1} \frac{2^{j_l-1}}{j_l!} \int_{\substack{y_1,\ldots,y_{i+1}\geqslant 0\\ y_1+\cdots+y_{i+1}=1}} y_1^{2j_1}\cdots y_{i+1}^{2j_{i+1}}\,\mathrm{d}y_1\ldots\mathrm{d}y_{i+1}.$$

There are $\binom{j}{j_1,\ldots,j_{i+1}}$ choices for $(B_1,\ldots,B_{i+1})$. Hence, (2) follows.

In order to bound the right-hand side expression in (2) we define,

$$I(j_1,\ldots,j_{i+1}) = \int_{\substack{y_1,\ldots,y_{i+1}\geqslant 0\\ y_1+\cdots+y_{i+1}=1}} y_1^{2j_1}\cdots y_{i+1}^{2j_{i+1}}\,\mathrm{d}y_1\ldots\mathrm{d}y_{i+1}.$$

Performing the change of variables $x_l=y_l/(1-y_{i+1})$ for $l=1,\ldots,i$, and $y=y_{i+1}$, we obtain that

$$I(j_1,\ldots,j_{i+1}) = I(j_1,\ldots,j_i)\int_0^1 y^{2j_{i+1}}(1-y)^{2(j-j_{i+1})+i}\,\mathrm{d}y. \tag{4}$$

The well known probability distribution Beta(a, b) has density function [13, Section 5.4]

$$f(y) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)}\, y^{a-1}(1-y)^{b-1}, \quad 0 < y < 1,$$

where $\Gamma(\cdot)$ is the standard gamma function. Since a density function integrates to 1 and $\Gamma(a+1) = a!$ for any non-negative integer a, we conclude that

$$I(j_1, \ldots, j_{i+1}) = \frac{\Gamma(2j_{i+1}+1)\Gamma(2(j-j_{i+1})+i+1)}{\Gamma(2j+i+2)} \cdot I(j_1, \ldots, j_i) = \frac{(2j_1)! \cdots (2j_{i+1})!}{(2j+i+1)!}.$$

Substituting in (2) and rearranging terms we get

$$\mathbb{E}[T_{A,B}] = 2^{j-(i+1)}\, \frac{j!}{(2j+i+1)!} \sum_{j_1+\cdots+j_{i+1}=j} \prod_{l=1}^{i+1} \binom{2j_l}{j_l}.$$

The summation in the above expression has a closed form. Indeed, it corresponds to the coefficient of x^j in the series expansion of $(\varphi(x))^{i+1}$, where $\varphi(x) = \sum_{n \geqslant 0} \binom{2n}{n} x^n$. It is well known that the generating function for the Catalan numbers is $\Psi(x) = \sum_{n \geqslant 0} \binom{2n}{n} x^n/(n+1) = (1-\sqrt{1-4x})/2x$. Since the derivative of $x\Psi(x)$ equals $\varphi(x)$, we have that $\varphi(x) = (1-4x)^{-1/2}$. Relying on the standard notation $(x)_n = x(x-1)(x-2)\cdots(x-n+1)$ and $\binom{x}{n} = (x)_n/n!$, we see that the coefficient of x^j in the series expansion of $(\varphi(x))^{i+1} = (1-4x)^{-(i+1)/2}$ is

$$\binom{j+\frac{1}{2}(i-1)}{j} 4^j = \frac{(2j+i)!}{i!j!(j+\frac{1}{2}i)_j} \leqslant \frac{(2j+i)!}{i!(j!)^2}.$$

Hence, recalling that $i + j = s_0$,

$$\mathbb{E}[T_{A,B}] = 2^{j-(i+1)} \frac{j!}{(2j+i+1)!} \binom{j+\frac{1}{2}(i-1)}{j} 4^j \leqslant 2^{j-(i+1)} \frac{1}{i!j!} \leqslant 2^{s_0-1} \frac{1}{i!j!}.$$

Since there are $\binom{m}{i}$ choices for A and $\binom{n}{j}$ choices for B, substituting in (1) we get that

$$\mathbb{P}[L_{m,n} \geqslant s_0] \leqslant 2^{s_0-1} \sum_{i+j=s_0} \binom{m}{i} \frac{1}{i!} \binom{n}{j} \frac{1}{j!}. \tag{5}$$

The remaining part of the proof is easy. It consists of upper bounding each term of the previous summation by one whose maximum we can determine using standard calculus. Given that $\binom{h}{k} \leqslant (eh/k)^k$ and $k! \geqslant (k/e)^k$,

$$\sum_{i+j=s_0} \binom{m}{i} \frac{1}{i!} \binom{n}{j} \frac{1}{j!} \leqslant \mathrm{e}^{2s_0} \sum_{i+j=s_0} \left(\frac{m}{i^2}\right)^i \left(\frac{n}{j^2}\right)^j.$$

Consider now the real-valued function defined over the interval $0 \leqslant x \leqslant s_0$ given by

$$F_{s_0}(x) = \ln\left(\left(\frac{m}{x^2}\right)^x \left(\frac{n}{(s_0-x)^2}\right)^{s_0-x}\right) = x(\ln m - 2\ln x) + (s_0-x)(\ln n - 2\ln(s_0-x)).$$

It is easy to verify that

$$F'_{s_0}(x) = \ln m - 2\ln x - \ln n + 2\ln(s_0-x),$$

$$F''_{s_0}(x) = -2\left(\frac{1}{x} + \frac{1}{s_0-x}\right).$$

Hence, F_{s_0} has a unique maximum on the interval $0 \leqslant x \leqslant s_0$ located at $x_{\max} = C_0\sqrt{m}$, where $C_0 = s_0/(\sqrt{m} + \sqrt{n})$. Note that $s_0 - x_{\max} = C_0\sqrt{n}$. Thus, for $i + j = s_0$ such that $i, j \geqslant 0$, it holds that

$$\left(\frac{m}{i^2}\right)^i \left(\frac{n}{j^2}\right)^j = \exp(F_{s_0}(i)) \leqslant \exp(F_{s_0}(C_0\sqrt{m})) = \left(\frac{1}{C_0^2}\right)^{s_0}.$$

Since $C_0 \geqslant \sqrt{2\mathrm{e}^3}$, from (5) we get that

$$\mathbb{P}[L_{m,n} \geqslant s_0] \leqslant \frac{1}{2}(s_0 + 1)\left(\frac{2\mathrm{e}^2}{C_0^2}\right)^{s_0} \leqslant s_0 \mathrm{e}^{-s_0}. \qquad \square$$

From Lemma 2 we easily derive the following result.

Corollary 3. *Let $m_0 = \lfloor\sqrt{2\mathrm{e}^3 m}\rfloor$ and $n_0 = \lfloor\sqrt{2\mathrm{e}^3 n}\rfloor$. For sufficiently large $\sqrt{m} + \sqrt{n}$, there is a median of $L_{m,n}$ which is less than $m_0 + n_0$.*

Proof. Let $m + n$ be sufficiently large so $(m_0 + n_0)\mathrm{e}^{-(m_0+n_0)}$ is less than $\frac{1}{2}$. By Lemma 2 it follows that $\mathbb{P}[L_{m,n} \geqslant m_0 + n_0] < \frac{1}{2}$. Hence, there is a median of $L_{m,n}$ which is less than $m_0 + n_0$. $\square$

The sought after concentration bound for $L_{m,n}$ will be obtained from the following version of Talagrand's inequality (see [9, Theorem 2.29]):

Theorem 4. *Suppose that $Z_1, \ldots, Z_N$ are independent random variables taking their values in some set Λ. Let $X = f(Z_1, \ldots, Z_N)$, where $f : \Lambda^N \to \mathbb{R}$ is a function such that the following two conditions hold for some number c and a function ψ:*

(L) *If $z, z' \in \Lambda^N$ differ only in one coordinate, then $|f(z) - f(z')| \leqslant c$.*
(W) *If $z \in \Lambda^N$ and $r \in \mathbb{R}$ with $f(z) \geqslant r$, then there exists a witness $(\omega_j : j \in J)$, $J \subseteq \{1, \ldots, N\}$, $|J| \leqslant \psi(r)/c^2$, such that for all $y \in \Lambda^N$ with $y_i = \omega_i$ when $i \in J$, we have $f(y) \geqslant r$.*

Let m be a median of X. Then, for all $t \geqslant 0$,

$$\mathbb{P}[X \geqslant m + t] \leqslant 2\mathrm{e}^{-t^2/4\psi(m+t)}$$

and

$$\mathbb{P}[X \leqslant m - t] \leqslant 2\mathrm{e}^{-t^2/4\psi(m)}.$$

We can now establish that $L_{m,n}$ is strongly concentrated.

Theorem 5. *For $C = 2\mathrm{e}^{3/2}$, a sufficiently large $s = m + 2n$, and all $t \geqslant 0$,*

$$\mathbb{P}[|L_{m,n} - \mathbb{E}[L_{m,n}]| \geqslant t + 32 s^{1/4}] \leqslant \begin{cases} 4\mathrm{e}^{-t^2/8C\sqrt{s}}, & 0 \leqslant t \leqslant C\sqrt{s}, \\ 2\mathrm{e}^{-t/8}, & t > C\sqrt{s}. \end{cases}$$

Proof. We again consider the geometric model of $\mathscr{I}_{m,n}$, denote by $\{D_i\}_{i=1}^m$ the points chosen over the $x = y$ diagonal and by $\{P_j, P_j^{\boxslash}\}_{j=1}^n$ the off diagonal points. Changing the value of one of the D_i's or the pair of values $\{P_j, P_j^{\boxslash}\}$ changes the value of $L_{m,n}$ by at most 1. Hence, $L_{m,n}$ is 1-Lipschitz. Furthermore, the value of ω elements of $\{D_i\}_{i=1}^m \cup \{P_j, P_j^{\boxslash}\}_{j=1}^n$ suffice to certify the existence of an increasing sequence of ω points. Thus, Talagrand's inequality applies and, with M denoting a median of $L_{m,n}$, yields that for $t \geqslant 0$,

$$\mathbb{P}[L_{m,n} \geqslant M + t] \leqslant 2\mathrm{e}^{-t^2/4(M+t)} \quad \text{and} \quad \mathbb{P}[L_{m,n} \leqslant M - t] \leqslant 2\mathrm{e}^{-t^2/4M},$$

which implies, by Corollary 3 and since $L_{m,n}$ is non-negative, that

$$\mathbb{P}[|L_{m,n} - M| \geqslant t] \leqslant \begin{cases} 4\mathrm{e}^{-t^2/8M}, & 0 \leqslant t \leqslant M, \\ 2\mathrm{e}^{-t/8}, & t > M. \end{cases}$$

Hence,

$$\begin{aligned} |\mathbb{E}[L_{m,n}] - M| &\leqslant \int_0^\infty \mathbb{P}[|L_{m,n} - M| > t]\,\mathrm{d}t \\ &\leqslant \int_0^M 4\mathrm{e}^{-t^2/8M}\,\mathrm{d}t + \int_M^\infty 2\mathrm{e}^{-t/8}\,\mathrm{d}t \\ &\leqslant 4\sqrt{2\pi M} + 16. \end{aligned}$$

Let $s = m + 2n$ and $C = 2\mathrm{e}^{3/2}$. Observe that $M \leqslant m_0 + n_0 \leqslant C\sqrt{s}$. Hence, $8\sqrt{\pi\sqrt{\mathrm{e}^3 s}} + 16 \leqslant 32 s^{1/4}$ for sufficiently large s. Since, $|L_{m,n} - M| \leqslant |L_{m,n} - \mathbb{E}[L_{m,n}]| + |\mathbb{E}[L_{m,n}] - M|$ we obtain that

$$\mathbb{P}[|L_{m,n} - \mathbb{E}[L_{m,n}]| \geqslant t + 32 s^{1/4}] \leqslant \begin{cases} 4\mathrm{e}^{-t^2/8C\sqrt{s}}, & 0 \leqslant t \leqslant M, \\ 2\mathrm{e}^{-t/8}, & t > M. \end{cases}$$

The desired conclusion follows from the fact that $2\mathrm{e}^{-t/8} \leqslant 4\mathrm{e}^{-t^2/8C\sqrt{s}}$ for $M \leqslant t \leqslant C\sqrt{s}$. □

Partitioning the collection of involutions of $[s]$ according to the number of their fixed points, we derive from Theorem 5 the sought after concentration bound for $L(\mathscr{I}_s)$.

Proof of Theorem 1. Clearly, $I_s = \bigcup_{m+2n=s} I_{m,n}$. Moreover, it is known that as $s \to \infty$ the main contribution to the sum $|I_s| = \sum_{m+2n=s} |I_{m,n}|$ comes from $\sqrt{s} - 2s^{\varepsilon+1/4} \leqslant m \leqslant \sqrt{s} + 2s^{\varepsilon+1/4}$. Specifically, it was observed in Knuth [12, pp. 62–64] that for sufficiently small $\varepsilon > 0$ and sufficiently large s,

$$\sum_{m+2n=s:|m-\sqrt{s}|>2s^{\varepsilon+1/4}} \frac{|I_{m,n}|}{|I_s|} \leqslant s \cdot \exp(-2s^{2\varepsilon}).$$

(It is implicit in [12, pp. 62–64] that the stated claim holds for all $\varepsilon < \frac{1}{4}$.) Hence, for all $\widetilde{t} \geqslant 0$,

$$\begin{aligned} &\mathbb{P}[|L_s - \mathbb{E}[L_s]| \geqslant \widetilde{t} + 5s^{\varepsilon+1/4}] \\ &\quad \leqslant s \cdot \mathrm{e}^{-2s^{2\varepsilon}} + \sum_{\substack{m+2n=s,\\ |m-\sqrt{s}| \leqslant 2s^{\varepsilon+1/4}}} \frac{|I_{m,n}|}{|I_s|}\,\mathbb{P}[|L_{m,n} - \mathbb{E}[L_s]| \geqslant \widetilde{t} + 5s^{\varepsilon+1/4}]. \end{aligned} \tag{6}$$

Let n' be the unique non-negative integer such that $\lfloor\sqrt{2n'}\rfloor + 2n' = s$, and let $m' = \lfloor\sqrt{2n'}\rfloor$. Perform the following process with probability $|I_{m,n}|/|I_s|$, where $m + 2n = s$:

(1) Choose points $D_1, \ldots, D_m$ uniformly and independently over the $x = y$ diagonal of the unit square. Also, choose points $P_1, \ldots, P_n$ uniformly and independently in the unit square.
(2) Let X_s be the length of the largest increasing sequence of points in $\mathscr{P} = \{D_i\}_{i=1}^m \cup \{P_j, P_j^{\boxslash}\}_{j=1}^n$.
(3) If $m < m'$, then randomly choose $m' - m$ points among $\{D_i\}_{i=1}^m$ and remove them from $\mathscr{P}$. Also, choose $(m' - m)/2$ points P uniformly and independently in the unit square and add $\{P, P^{\boxslash}\}$ to $\mathscr{P}$. If $m \geqslant m'$, then randomly choose $m - m'$ points uniformly and independently over the $x = y$ diagonal of the unit square and add them to $\mathscr{P}$. Also, randomly choose $(m - m')/2$ pairs of points $\{P, P^{\boxslash}\}$ among $\{P_j, P_j^{\boxslash}\}_{j=1}^n$ and remove them from $\mathscr{P}$.
(4) Denote by $\mathscr{P}'$ the collection of points obtained in the previous step.
(5) Let $X_{m',n'}$ be the length of the largest increasing sequence of points in $\mathscr{P}'$.

Observe that X_s and L_s have the same distribution. Moreover, $X_{m',n'}$ and $L_{m',n'}$ are also identically distributed. It is easy to see that $|X_s - X_{m',n'}| \leqslant |m-m'|+|n-n'|$. Then, for $|m-\sqrt{s}| \leqslant 2s^{\varepsilon+1/4}$, $m' = \lfloor \sqrt{2n'} \rfloor$ and $m+2n = m'+2n' = s$, we have that $|X_s - X_{m',n'}| \leqslant 5s^{\varepsilon+1/4}$. From (6) we conclude that

$$\mathbb{P}[|L_s - \mathbb{E}[L_s]| \geqslant \widetilde{t} + 5s^{\varepsilon+1/4}] \leqslant s \cdot \exp(-2s^{2\varepsilon}) + \mathbb{P}[|L_{m',n'} - \mathbb{E}[L_s]| \geqslant \widetilde{t}]. \qquad (7)$$

A similar argument shows that for sufficiently large s,

$$|\mathbb{E}[L_{m',n'}] - \mathbb{E}[L_s]| \leqslant s^2 \cdot \exp(-2s^{2\varepsilon}) + 5s^{\varepsilon+1/4} \leqslant 6s^{\varepsilon+1/4}. \qquad (8)$$

From (7) and (8), taking $\widetilde{t} = t + 32s^{1/4} + 6s^{\varepsilon+1/4}$ we conclude that

$$\begin{aligned} &\mathbb{P}[|L_s - \mathbb{E}[L_s]| \geqslant t + 32s^{1/4} + 11s^{\varepsilon+1/4}] \\ &\quad \leqslant s \cdot \exp(-2s^{2\varepsilon}) + \mathbb{P}[|L_{m',n'} - \mathbb{E}[L_{m',n'}]| \geqslant t + 32s^{1/4}]. \end{aligned}$$

Applying Theorem 5, the desired conclusion follows immediately. □

Acknowledgements

Gratefully acknowledges the support of ICM P01-05 and Fondecyt 1010689.

References

[1] D. Aldous, P. Diaconis, Longest increasing subsequences: from patience sorting to the Baik–Deift–Johansson theorem, Bull. AMS 36 (4) (1999) 413–432.
[2] J. Baik, Private communication, September 2003.
[3] J. Baik, P.A. Deift, K. Johansson, On the distribution of the length of the longest increasing subsequence of random permutations, J. Amer. Math. Soc. 12 (1999) 1119–1178.
[4] J. Baik, E.M. Rains, The asymptotics of monotone subsequences of involutions, Duke Math. J. 2 (109) (2001) 205–281.
[5] J. Baik, E.M. Rains, Symmetrized random permutations, in: Random Matrix Models and their Applications, Math. Sci. Res. Inst. Publ., vol. 40, Cambridge University Press, Cambridge, 2001, pp. 1–19.
[6] B. Bollobás, B. Brightwell, The height of a random partial order: concentration of measure, Ann. Probab. 2 (4) (1992) 1009–1018.
[7] B. Bollobás, S. Janson, On the length of the longest increasing subsequence in a random permutation, in: Combinatorics, Geometry and Probability Proceedings, P. Erdös' 80th Birthday, Cambridge University Press, Cambridge, 1993, pp. 121–128.
[8] A. Frieze, On the length of the longest monotone subsequence in a random permutation, Ann. Appl. Probab. 1 (2) (1991) 301–305.
[9] S. Janson, T. Łuczak, A. Ruciński, Random Graphs, Wiley, New York, 2000.
[10] J.H. Kim, On increasing subsequences of random permutations, J. Combin. Theory, Ser. A 76 (1) (1996) 148–155.
[11] M. Kiwi, M. Loebl, J. Matoušek, Expected length of the largest common subsequence for large alphabets, Adv. Math. 197(2) (2005) 480–498.
[12] D.E. Knuth, The Art of Computer Programming, vol. 3, second edition, Addison-Wesley, 1997.
[13] S. Ross, A First Course in Probability Theory, third edition, Macmillan Publishing Company, New York, 1988.
[14] in: D. Sankoff, J. Kruskal (Eds.), Common Subsequences and Monotone Subsequences, Addison-Wesley, Reading, MA, 1983, pp. 363–365, (chapter 17).
[15] R.P. Stanley, Recent progress in algebraic combinatorics, Bull. AMS 40 (1) (2002) 55–68.
[16] M. Talagrand, Concentration of measure and isoperimetric inequalities in product spaces, Inst. Hautes Études Sci. Publ. Math. 81 (1995) 73–205.