# On the length of the longest monotone subsequence in a random permutation

Alan Frieze*
Department of Mathematics, Carnegie-Mellon University,
Pittsburgh, U.S.A.

June 26, 1997

In this short note we prove a concentration result for the length $L_n$ of the longest monotone increasing subsequence of a random permutation of the set $\{1, 2, ..., n\}$. It is known, Logan and Shepp [6], Vershik and Kerov [9] that

$$\lim_{n \to \infty} \frac{\mathbf{E} L_n}{\sqrt{n}} = 2 \tag{1}$$

but less is known about the concentration of $L_n$ around its mean. Our aim here is to prove the following.

**Theorem 1** *Suppose that* $\alpha > \frac{1}{3}$. *Then there exists* $\beta = \beta(\alpha) > 0$ *such that for* $n$ *sufficiently large*

$$\mathbf{Pr}(|L_n - \mathbf{E} L_n| \geq n^\alpha) \;\leq\; exp\{-n^\beta\}$$

□

*Supported by NSF grant CCR-8900112

Our main tool in the proof of this theorem is a simple inequality arising from the theory of martingales. It is often referred to as Azuma's inequality. See Bollobás [2] [3] and McDiarmid [7] for surveys on its use in random graphs, probabilistic analiysis of algorithms etc., and Azuma [1] for the original result. A similar stronger inequality can be read out from Hoeffding [4]. We will use the result in the following form.

Suppose we have a random variable $Z = Z(U), U = (U_1, U_2, ..., U_m)$ where $U_1, U_2, ..., U_m$ are chosen independently from probability spaces $\Omega_1, \Omega_2, ..., \Omega_m$ i.e. $U \in \Omega = \Omega_1 \times \Omega_2 \times ... \times \Omega_m$. Assume next that $Z$ does not change by much if $U$ does not change by much. More precisely write $U \simeq V$ for $U, V \in \Omega$ when $U, V$ differ in at most one component i.e. $|\{i : U_i \neq V_i\}| = 1$. We state the inequality we need as a theorem.

**Theorem 2** *Suppose $Z$ above satisfies the following inequality;*

$$U \simeq V \textit{ implies } |Z(U) - Z(V)| \leq 1$$

*then*

$$\mathbf{Pr}(|Z - \mathbf{E}Z| \geq u) \leq 2exp\{-\frac{2u^2}{m}\},$$

*for any real $u \geq 0$.*

□

The value m is the *width* of the inequality and to obtain sharp concentration of measure we need $m = o((\mathbf{E}Z)^2)$.

We will make use of the following crude probability inequality for $L_s$, where $s$ is an arbitrary (large) positive integer.

**Lemma 1**

$$\mathbf{Pr}(L_s \geq 2e\sqrt{s}) < e^{-2e\sqrt{s}}$$

**Proof** Let $s_0 = \lceil 2e\sqrt{s} \rceil$. Then, where $\sigma$ denotes the number of increasing subsequences of $X_1, X_2, ..., X_s$ which are of length $s_0$,

$$\begin{aligned} \mathbf{Pr}(L_s \geq s_0) &\leq \mathbf{E}(\sigma) \\ &= \binom{s}{s_0} / s_0! \\ &\leq \left(\frac{se^2}{s_0{}^2}\right)^{s_0} \\ &< e^{-2e\sqrt{s}} \end{aligned}$$

□

**Proof**(of Theorem 1) Let $X = (X_1, X_2, ...X_n)$ be a sequence of independent uniform [0,1] random variables. We can clearly assume that $L_n$ is the length of the longest monotone increasing subsequence of $X$.

Before getting on with the proof proper observe that although changing one $X_i$ only changes $L_n$ by at most 1, the width $n$ is too large in relation to the mean $2\sqrt{n}$ for us to obtain a sharp concentration result. It therefore appears that to use the theorem in this case requires us to reduce the width by a more careful choice for $Z$.

For a set $I = \{i_1 < i_2 < ... < i_k\} \subseteq [n]$ we let $\lambda(I)$ denote the length of the longest increasing subsequence of $X_{i_1}, X_{i_2}, ...X_{i_k}$. So for example $\lambda([n]) = L_n$.

Let $m = \lceil n^b \rceil, 0 < b < 1$ where a range for $b$ will be given later. Let $\nu = \lfloor n/m \rfloor$ and $\mu = n - m\nu$. Let $I_1, I_2, ...I_m$ be the partition of $[n] = \{1, 2, ..., n\}$ into consecutive intervals where the first $\mu$ have $|I_j| = \nu + 1$ and the remaining $m-\mu$ have $|I_j| = \nu$ (precisely: $I_j = \{k_{j-1}+1, k_{j-1}+2, ...k_j\}, j = 1, 2, ..., m$ where $k_j = j(\nu+1)$ for $j = 0, 1, ...\mu$ and $k_j = j\nu + \mu$ for $j = \mu+1, ..., m$.) For $S \subseteq [m]$ we let $I_S = \bigcup_{j \in S} I_j$.

Let $\theta = n^a$ and $\epsilon = 2e^{-2\theta}$. Define $l$ by

$$l = max\{t : \mathbf{Pr}(L_n \leq t-1) \leq \epsilon\},$$

so that in particular

$$\mathbf{Pr}(L_n < l) \leq \epsilon. \tag{2}$$

Now let

$$Z_n = max\{|S| : S \subseteq [m] \text{ and } \lambda(I_S) \leq l\}.$$

Note that if $L_n = \lambda([m]) \leq l$ then $Z_n = m$ and so the definition of $l$ gives

$$\mathbf{Pr}(Z_n = m) > \epsilon \tag{3}$$

Note next that for any $j \in [m]$, changing the value of $U_j = \{X_i : i \in I_j\}$, can only change the value of $Z_n$ by at most one. We can thus apply Theorem 2 to obtain

$$\mathbf{Pr}(|Z_n - \mathbf{E}Z_n| \geq u) \leq 2exp\{-\frac{2u^2}{m}\} \tag{4}$$

Hence, putting $u = \sqrt{m\theta}$ in (4) and comparing with (3) we see that

$$\mathbf{E}Z_n > m - \sqrt{m\theta}.$$

Applying (4) once again with the same value for u we obtain

$$\mathbf{Pr}(Z_n \leq m - 2\sqrt{m\theta}) \leq \epsilon \tag{5}$$

Let now $s = \lceil 2\sqrt{m\theta} \rceil$ and let $\mathcal{E}$ denote the event

$$\{\exists S \subseteq [m] : |S| = s \text{ and } \lambda(I_S) \geq 6\sqrt{\frac{sn}{m}}\}.$$

Now if $|S| = s$ then $|I_S| = (1 + o(1))(sn/m)$ and so on applying Lemma 1 above we get

$$\begin{aligned}
\mathbf{Pr}(\mathcal{E}) &\leq \binom{m}{s} e^{-2e\sqrt{sn/m}} \\
&\leq exp\{s \ln m - 2e\sqrt{\frac{sn}{m}}\} \\
&\leq \epsilon_1 = exp\{e(n^{\frac{a+b}{2}} \ln m - 2n^{\frac{1}{2}+\frac{a}{4}-\frac{b}{4}})\}
\end{aligned}$$

Notice that $\epsilon_1$ is small if

$$a + 3b < 2. \tag{6}$$

Now if $Z_n > m - 2\sqrt{m\theta}$ and $\mathcal{E}$ does not occur then

$$L_n \leq l + 6\sqrt{\frac{sn}{m}}. \tag{7}$$

To see this let $S \subseteq [m]$ be such that $|S| = Z_n$ and $\lambda(I_S) \leq l$. If $T = [m] - S$ then $|T| \leq s$ and so as $\mathcal{E}$ does not occur we have $\lambda(I_T) < 6\sqrt{\frac{sn}{m}}$ and (7) follows since $L_n \leq \lambda(I_S) + \lambda(I_T)$.

So

$$\mathbf{Pr}(L_n > l + 6\sqrt{\frac{sn}{m}}) \leq \epsilon + \epsilon_1. \tag{8}$$

Putting $l_0 = l + 3\sqrt{\frac{sn}{m}}$ we see from (2) and (8) that

$$\mathbf{Pr}(|L_n - l_0| > 3\sqrt{\frac{sn}{m}}) \leq 2\epsilon + \epsilon_1. \tag{9}$$

The theorem follows by choosing any $a, b, \beta$ such that (6) holds and

$$\beta < \frac{1}{2} + \frac{a}{4} - \frac{b}{4} < \alpha$$

□

We observe next that Steele [8] has generalised (1) in the following way: let now $k$ be a fixed positive integer and given a random permutation let $L_{k,n}$ denote the length of the longest subsequence which can be decomposed into $k+1$ successive monotone sequences, alternately increasing and decreasing. The monotone case above corresponds to k=0. In analogy to (1) Steele proves

$$\lim_{n\to\infty}\frac{\mathbf{E}L_{k,n}}{\sqrt{n}} = 2\sqrt{k+1}.$$

Theorem 1 generalises easily to include this problem. In fact we only need to change $L_n$ to $L_{k,n}$ throughout. In order to avoid complicating the proof of Lemma 1, it suffices to prove

$$\mathbf{Pr}(L_s \geq 2(k+1)e\sqrt{s}) \leq e^{-2e\sqrt{s}}.$$

This follows from Lemma 1 since if the 'up and down' sequence is of length at least $2(k+1)e\sqrt{s}$ then one of the monotone pieces is at least $2e\sqrt{s}$ in length.

There is at least one more related case in which a concentration result can be proved by the above method. Before giving the details it might be useful to abstract the properties of $L_n$ which make the method work. These are

$$\lambda(I_S) \leq \lambda(I_{S\cup T}) \leq \lambda(I_S) + \lambda(I_T) \tag{10}$$

for $S \cap T = \emptyset$.

$$\mathbf{Pr}(L_s \geq A\sqrt{s}) \leq e^{-B\sqrt{s}} \tag{11}$$

for sufficiently large positive integer s and some absolute constants $A, B > 0$.

Inequality (10) is needed to show that the random variable $Z_n$ changes by at most one for a change in one set $I_t$. It is also needed to show that if $Z_n$

is close to $m$ then $L_n$ is unlikely to be much larger than $l$. It is here that we need (11) as well.

Our final result concerns the number $T_n = T_n(X_1, X_2, ..., X_n)$ of increasing subsequences among $X_1, X_2, ...X_n$. This was studied by Lifschitz and Pittel [5]. Let now $\hat{L}_n = \ln T_n$. The main result of [5] is that there exists an absolute constant $a, 2\ln 2 \leq a \leq 2$ such that

$$\hat{L}_n n^{-1/2} \to a, \text{ as } n \to \infty$$

in probability and in mean.

It is now easy to see that Theorem 1 holds with $L_n$ replaced by $\hat{L}_n$. Indeed, on replacing $\lambda, Z_n$ by $\hat{\lambda}, \hat{Z}_n$ we need only verify (10),(11) above. But (10) should be clear and

$$\begin{aligned} \mathbf{Pr}(\hat{L}_n \geq 3\sqrt{n}) &= \mathbf{Pr}(T_n \geq e^{3\sqrt{n}}) \\ &\leq e^{-3\sqrt{n}}\mathbf{E}(T_n) \\ &\leq e^{-\sqrt{n}} \end{aligned}$$

since Lifschitz and Pittel have shown that

$$\mathbf{E}(T_n) \approx 0.171 n^{-1/4} e^{2\sqrt{n}}.$$

This completes our analysis of $\hat{L_n}$.

# References


[1] K.Azuma, *Weighted sums of certain dependent random variables*, Tokuku Mathematics Journal 19, (1967) 357-367.

[2] B.Bollobás, *Martingales, isoperimetric inequalities and random graphs*, in Combinatorics, A.Hajnal, L.Lovász and V.T.Sós Ed., Colloq. Math. Sci. Janos Bolyai 52, North Holland 1988.

[3] B.Bollobás, *Sharp concentration of measure phenomena in random graphs*, to appear in Proceedings of Random Graphs '87, M.Karonski Ed., Annals of Discrete Mathematics Series, North-Holland.

[4] W.Hoeffding, *Probability inequalities for sums of bounded random variables*, Journal of the American Statistical Association 27, (1963) 13-30.

[5] V.Lifschitz and B.Pittel, *The number of increasing subsequences of the random permutation*, Journal of Combinatorial Theory A 31 (1981) 1-20.

[6] B.F.Logan and L.A.Shepp, *A variational problem for Young tableaux*, Advances in Mathematics 26 (1977) 206-222.

[7] C.J.H.McDiarmid, *On the method of bounded differences*, Surveys in Combinatorics, 1989, Invited papers at the Twelfth British Combinatorial Conference, Edited by J.Siemons, Cambridge University Press, 148-188.

[8] J.M.Steele, *Long unimodal subsequences: a problem of F.R.K.Chung*, Discrete Mathematics 33 (1981) 223-225.

[9] A.M.Vershik and C.V.Kerov, *Asymptotics of the Plancherel measure of the symmetric group and a limiting form for Young Tableau*, Dokl. Akad. Nauk. U.S.S.R. 233 (1977) 1024-1027.