THE AVERAGE ORDER OF A PERMUTATION

Richard Stong

Department of Mathematics
Rice University
Houston, TX 77005
stong@math.rice.edu

Submitted: May 11, 1998; Accepted: June 23, 1998

Abstract. We show that the average order μ_n of a permutation in S_n satisfies

$$\log \mu_n \;=\; C\sqrt{\frac{n}{\log n}} + O\left(\frac{\sqrt{n}\log\log n}{\log n}\right),$$

which refines earlier results of Erdős and Turán, Schmutz, and Goh and Schmutz.

1. Introduction.

For $\sigma \in S_n$ let $N(\sigma)$ be the order of σ in the group S_n. Erdős and Turán [2] showed that if one chooses a permutation uniformly at random from S_n then for n large $\log N(\sigma)$ is asymptotically normal with mean $(\log^2 n)/2$ and variance $(\log^3 n)/3$. Define the average order of an element of S_n to be

$$\mu_n \;=\; \frac{1}{n!}\sum_{\sigma\in S_n} N(\sigma).$$

It turns out that $\log \mu_n$ is much larger than $(\log^2 n)/2$, being dominated by the contribution of a relatively small number of permutations of very high order. This was first shown by Erdős and Turán [3], who showed that $\log \mu_n = \mathbf{O}\left(\sqrt{n/\log n}\right)$. This result was sharpened by Schmutz [6], and later by Goh and Schmutz [4] to show that $\log \mu_n \sim C\sqrt{n/\log n}$, for an explicit constant C. The purpose of this note is to show that

$$\log \mu_n \;=\; C\sqrt{\frac{n}{\log n}} \;+\; \mathbf{O}\left(\frac{\sqrt{n}\log\log n}{\log n}\right),$$

where $C = 2.99047\ldots$ is an explicit constant defined below. Our argument shares some similarities with that of [4], but is more elementary and permits a more explicit

1991 *Mathematics Subject Classification*. Primary 11N37.

bound on the error term. The proof will be divided into three steps. First we will give upper and lower bounds on μ_n involving the coefficients of a certain power series, then we will use a Tauberian theorem to bound these coefficients.

For a partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_s)$ let $c_i(\lambda)$ be the number of parts of λ of size i, let $|\lambda| = \lambda_1 + \lambda_2 + \cdots + \lambda_s$ and let $m(\lambda) = \text{l.c.m.}(\lambda_1, \lambda_2, \ldots, \lambda_s)$. We will say that λ is a partition of $|\lambda|$. By a sub-partition of λ we will mean any subset of $(\lambda_1, \lambda_2, \ldots, \lambda_s)$ viewed as a partition of some smaller number. Then

$$\mu_n = \sum_{|\lambda|=n} \frac{m(\lambda)}{1^{c_1(\lambda)} 2^{c_2(\lambda)} \ldots c_1(\lambda)! c_2(\lambda)! \ldots}.$$

2. The Upper Bound.

Call a partition $\pi = (\pi_1, \pi_2, \ldots, \pi_s)$ minimal if for each sub-partition π' of π we have $m(\pi') < m(\pi)$. For each partition λ of n choose a minimal sub-partition π with $m(\pi) = m(\lambda)$ and write $\lambda = \pi \cup \omega$ for some partition ω. Let M_n be the set of all minimal partitions π with $|\pi| \le n$ and for any $\pi \in M_n$ let Ω_π be the set of all partitions ω that occur with π in decompositions as above. Then

$$\begin{aligned} \mu_n &= \sum_{\pi \in M_n} \sum_{\omega \in \Omega_\pi} \frac{m(\pi)}{1^{c_1(\pi)} 2^{c_2(\pi)} \ldots 1^{c_1(\omega)} 2^{c_2(\omega)} \ldots c_1(\pi \cup \omega)! c_2(\pi \cup \omega)! \ldots}, \\ &\le \sum_{\pi \in M_n} \frac{m(\pi)}{\pi_1 \pi_2 \ldots} \sum_{\omega \in \Omega_\pi} \frac{1}{1^{c_1(\omega)} 2^{c_2(\omega)} \ldots c_1(\omega)! c_2(\omega)! \ldots}, \\ &\le \sum_{\pi \in M_n} \frac{m(\pi)}{\pi_1 \pi_2 \ldots}, \end{aligned}$$

where the first inequality follows by rewriting $1^{c_1(\pi)} 2^{c_2(\pi)} \ldots$ as $\pi_1 \pi_2 \ldots$ and using $c_i(\pi \cup \omega) \ge c_i(\omega)$ and the second follows by noting that if the inner sum were over all partitions ω with $|\omega| = n - |\pi|$ instead of just a subset of them, then it would be 1.

For each minimal $\pi = (\pi_1, \pi_2, \ldots, \pi_s)$ choose integers $(d_1, d_2, \ldots, d_s)$ with the following properties:

(1) d_i divides π_i,
(2) g.c.d. $(d_i, d_j) = 1$ for $i \ne j$,
(3) $\prod_{i=1}^{s} d_i = m(\pi)$.

(An explicit construction of the d_i is given in [6].) Note that since π is minimal the d_i are all greater than 1. Define integers k_i by $\pi_i = k_i d_i$. Then $\pi_1 \pi_2 \ldots \pi_s = m(\pi) k_1 k_2 \ldots k_s$. Let D_n be the set of all unordered sets $(d) = (d_1, d_2, \ldots, d_s)$ of pairwise relatively prime integers greater than 1 with $d_1 + d_2 + \cdots + d_s \le n$ and for any $(d) \in D_n$ let $K_{(d)}$ be the set of all $(k_1, k_2, \ldots, k_s)$ with $k_1 d_1 + k_2 d_2 + \cdots + k_s d_s \le n$. Then the bound above becomes

$$\mu_n \le \sum_{(d) \in D_n} \sum_{(k) \in K_{(d)}} \frac{1}{k_1 k_2 \ldots}.$$

The sets $(d_1, d_2, \dots, d_s)$ can be broken up into two subsets: the prime elements and the composite elements. Any composite d_i must be divisible by some prime p with $p \le \sqrt{n}$ and since the d_i are relatively prime p divides only one element. Therefore there are at most $\pi(\sqrt{n}) < C\frac{\sqrt{n}}{\log n}$ composite elements. Each composite element contributes at most $\sum_{k=1}^{n} \frac{1}{k} = \log n + \mathbf{O}(1)$. Therefore all the composite elements together contribute at most $\exp\left\{\mathbf{O}\left(\frac{\sqrt{n}\log\log n}{\log n}\right)\right\}$ to μ_n. Let P_n be the set of all unordered sets $(d) = (d_1, d_2, \dots, d_s)$ of distinct primes with $d_1 + d_2 + \cdots + d_s \le n$. Then the bound above becomes

$$\mu_n \;\le\; \sum_{(d)\in P_n} \sum_{(k)\in K_{(d)}} \frac{1}{k_1 k_2 \dots} \;\exp\left\{\mathbf{O}\left(\frac{\sqrt{n}\log\log n}{\log n}\right)\right\}.$$

The sum above can be rewritten in a convenient form. Let $p_1,\ p_2, \dots$ be all the primes in order and consider infinite sequences $(k_1, k_2, \dots)$ with only finitely many nonzero terms with $\sum_{i=1}^{\infty} k_i p_i \le n$. Then the sum above is the sum over all such sequences of the product of the reciprocals of the nonzero k_i's. Explicitly

$$\mu_n \;\le\; \sum_{(k):\Sigma k_i p_i \le n} \;\prod_{i:k_i\neq 0} \frac{1}{k_i} \exp\left\{\mathbf{O}\left(\frac{\sqrt{n}\log\log n}{\log n}\right)\right\}.$$

If we define a function $h(t)$ and a sequence a_m by

$$h(t) \;=\; \prod_{p \text{ prime}} \left(1 - \log(1 - e^{-pt})\right) \;=\; \sum_{m=0}^{\infty} a_m e^{-mt},$$

then the bound above says that

$$\mu_n \;\le\; \sum_{m=0}^{n} a_m \exp\left\{\mathbf{O}\left(\frac{\sqrt{n}\log\log n}{\log n}\right)\right\},$$

Before analyzing the a_m's in detail we will first derive a lower bound comparable to this upper bound.

3. The Lower Bound.

Consider only partitions λ of n of the following nice form $\lambda = \pi \cup \omega$ where $\pi = (\pi_1, \pi_2, \dots, \pi_s)$ and each $\pi_i = k_i d_i$ where the d_i are distinct primes greater than $\sqrt{n}$ and $|\omega| < q$ where q is the smallest prime larger than $\sqrt{n}$. For such a λ we have $m(\lambda) \ge d_1 d_2 \dots d_s$ and for all i either $c_i(\lambda) = c_i(\omega)$ or $c_i(\lambda) = 1$ and $c_i(\omega) = 0$. In either case $c_i(\lambda)! = c_i(\omega)!$. Therefore taking only the terms corresponding to these λ's in our expression for μ_n above gives

$$\mu_n \;\ge\; \sum_{\pi} \frac{1}{k_1 k_2 \dots} \sum_{\omega} \frac{1}{1^{c_1(\omega)} 2^{c_2(\omega)} \dots c_1(\omega)! c_2(\omega)! \dots} \;=\; \sum_{\pi} \frac{1}{k_1 k_2 \dots},$$

where the outer sum runs over all π which occur in some partition as above and the second equality follows by noting that the inner sum is over all partitions ω with $|\omega| = n - |\pi|$ and hence is 1. This lower bound can be rewritten as we did for the upper bound. Let $q = q_1 < q_2 < \dots$ be all the primes greater than $\sqrt{n}$ in order and consider all infinite sequences $(k_1, k_2, \dots)$ with only finitely many terms nonzero such that $n - q < \sum_{i=1}^{\infty} k_i q_i \leq n$. Then as above the lower bound is the sum over all such sequences of the product of the reciprocals of the nonzero k_i's. Define a functions $z_n(t)$ and sequences $b_m^{(n)}$ by

$$z_n(t) \;=\; \prod_{p>\sqrt{n} \text{ prime}} 1 - \log\left(1 - e^{-pt}\right) \;=\; \sum_{m=0}^{\infty} b_m^{(n)} e^{-mt}.$$

Then the lower bound above becomes

$$\mu_n \;\geq\; \sum_{m=n-q+1}^{n} b_m^{(n)}.$$

We need only relate the $b_m^{(n)}$ to the a_m defined earlier. Unfortunately the sum above extends over only a short range of indices; we must first correct this imbalance.

For any $m \leq n - q$ and any prime q_i greater than $\sqrt{n}$ and any sequence (k) that contributes to $b_m^{(n)}$ we obtain a sequence that contributes to $b_{m+q_i}^{(n)}$ by adding one to k_i. In the worst case this changes k_i from 1 to 2 and halves the contribution of this term. Therefore $b_m^{(n)} \leq 2b_{m+q_i}^{(n)}$. Since there is a prime p between $(n-m)/2$ and $n - m$ (which we may assume is greater than $\sqrt{n}$ since we may always take $p = q$) we may halve the distance from m to n by one application of this inequality. After at most $\log_2 n$ applications of the above inequality we obtain $b_m^{(n)} \leq n b_s^{(n)}$ for some $n - q < s \leq n$. Therefore we have

$$\sum_{m=0}^{n} b_m^{(n)} \;\leq\; n^2 \sum_{m=n-q+1}^{n} b_m^{(n)}$$

therefore with only negligible error we may replace the sum in the lower bound above by the sum over all $m \leq n$.

To compare this sequence to the a_m's note that

$$h(t) \;=\; z_n(t) \prod_{p\leq\sqrt{n} \text{ prime}} \left(1 - \log(1 - e^{-pt})\right).$$

If the second factor on the right hand side is expanded as $\sum_{m=0}^{\infty} c_m^{(n)} e^{-mt}$, then

$$a_m = \sum_{k=0}^{m} b_k^{(n)} c_{m-k}^{(n)}.$$

The second factor of $h(t)$ is a product of $\pi(\sqrt{n}) < C\frac{\sqrt{n}}{\log n}$ terms each of which contributes at most $1+\sum_{k=1}^{m}\frac{1}{k} = \log m + \mathbf{O}(1)$ to $c_m^{(n)}$. Therefore for all $m \le n$ we see $c_m^{(n)} \le \exp\left\{\mathbf{O}\left(\frac{\sqrt{n}\log\log n}{\log n}\right)\right\}$, so $a_m \le \sum_{k=0}^{m} b_k^{(n)} \exp\left\{\mathbf{O}\left(\frac{\sqrt{n}\log\log n}{\log n}\right)\right\}$. Summing over m gives

$$\mu_n \;\ge\; \frac{1}{n^2}\sum_{m=0}^{n} b_m^{(n)} \;\ge\; \sum_{m=0}^{n} a_m \exp\left\{-\mathbf{O}\left(\frac{\sqrt{n}\log\log n}{\log n}\right)\right\}.$$

Combining this with the upper bound above gives

$$\log \mu_n \;=\; \log \sum_{m=0}^{n} a_m + \mathbf{O}\left(\frac{\sqrt{n}\log\log n}{\log n}\right).$$

To complete the proof we need only bound $\log\sum_{m=0}^{n} a_m$.

4. The Tauberian Theorem.

We will apply the following result of Erdős and Turán [3].

Lemma (Erdős and Turán) Let $f(t) = \sum_{m=0}^{\infty} a_m e^{-mt}$ and suppose

$$\log f(t) \;=\; \frac{A}{t\log 1/t} \;+\; \mathbf{O}\left(\frac{\log\log 1/t}{t(\log 1/t)^2}\right) \quad \text{as} \quad t \to 0^+.$$

Then

$$\sum_{m=0}^{n} a_m \;=\; \exp\left\{2\sqrt{2A\frac{n}{\log n}} \;+\; \mathbf{O}\left(\frac{\sqrt{n}\log\log n}{\log n}\right)\right\}.$$

Thus we need only analyze $\log h(t)$ as $t \to 0^+$. As in [3] we have

$$\begin{aligned}
\log h(t) \;&=\; \sum_{p \text{ prime}} \log\left(1-\log(1-e^{-pt})\right) \;=\; \int_0^\infty \log\left(1-\log(1-e^{-xt})\right) d\pi(x),\\
&=\; \int_0^\infty \frac{t\pi(x)e^{-xt}}{(1-e^{-xt})\,(1-\log(1-e^{-xt}))}\, dx,\\
&=\; \int_0^\infty \frac{\pi(s/t)e^{-s}}{(1-e^{-s})\,(1-\log(1-e^{-s}))}\, ds.
\end{aligned}$$

The integrand is bounded by $C_1 t^{-1}$ for s small (using the bound $\pi(x) \le x$). Therefore the contribution to the integral from the interval $[0, t^{1/2})$ is bounded by $C_1 t^{-1/2}$. Hence we may replace the lower endpoint by $t^{1/2}$ with only a negligible error. For any x we have

$$\pi(x) \;=\; \frac{x}{\log x} \;+\; \mathbf{O}\left(\frac{x}{(\log x)^2}\right),$$

(see for example [5, Thm 23, p. 65]) hence

$$\pi(s,t) \;=\; \frac{1}{t}\frac{s}{\log 1/t + \log s} \;+\; \mathbf{O}\left(\frac{1}{t}\frac{s}{(\log 1/t + \log s)^2}\right).$$

Since $s \geq t^{1/2}$ we have $\log s \geq -1/2 \log(1/t)$ and thus

$$\begin{aligned}
\pi(s,t) &= \frac{s}{t\log 1/t} - \frac{s\log s}{t\log 1/t(\log 1/t + \log s} + \mathbf{O}\left(\frac{s}{t(\log 1/t)^2}\right), \\
&= \frac{s}{t\log 1/t} + \mathbf{O}\left(\frac{s(1+|\log s|)}{t(\log 1/t)^2}\right).
\end{aligned}$$

Plugging this into the integral and extending the lower endpoint back to 0 (which again introduces only negligible error terms) gives

$$\log h(t) = \frac{1}{t\log 1/t}\int_0^\infty \frac{se^{-s}}{(1-e^{-s})\,(1-\log(e^{-s}))}\,ds + \mathbf{O}\left(\frac{1}{t(\log 1/t)^2}\right).$$

So the Tauberian theorem of Erdős and Turán gives

$$\log \mu_n = 2\sqrt{2A}\sqrt{\frac{n}{\log n}} + \mathbf{O}\left(\frac{\sqrt{n}\log\log n}{\log n}\right)$$

where

$$\begin{aligned}
A &= \int_0^\infty \frac{se^{-s}}{(1-e^{-s})\,(1-\log(1-e^{-s}))}\,ds = \int_0^\infty \frac{\log(s+1)}{e^{-s}-1}\,ds \\
&= \sum_{n=1}^\infty \frac{e^n}{n}E_1(n) = 1.11786415\ldots .
\end{aligned}$$

where $E_1(n)$ is the exponential integral (see [1, Eqn. 5.1.1, p. 228]).

Acknowledgements. The author was partially supported by an Alfred P. Sloan Research Fellowship.

References

1. M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*, National Bureau of Standards, Washington DC, 1972.
2. P. Erdős and P. Turán, *On some problems of a statistical group theory, III,*, Acta Math. Acad. Sci. Hungar. **18** (1967), 309–320.
3. P. Erdős and P. Turán, *On some problems of a statistical group theory, IV*, Acta Math. Acad. Sci. Hungar. **19** (1968), 413–435.
4. W. Goh and E. Schmutz, *The expected order of a random permutation*, Bull. Lond. Math. Soc. **23** (1991), 34–42.
5. A. E. Ingham, *The Distribution of Prime Numbers*, Cambridge University Press, Cambridge, 1990.
6. E. Schmutz, *Proof of a conjecture of Erdős and Turán*, Jour. No. Th. **31** (1989), 260–271.