Combinatorics, Probability and Computing (2011) 20, 289–298. © Cambridge University Press 2010
doi:10.1017/S0963548310000337

Period Lengths for Iterated Functions

ERIC SCHMUTZ

Mathematics Department, Drexel University, 3401 Market Street, Philadelphia, Pa., 19104, USA
(e-mail: Eric.Jonathan.Schmutz@drexel.edu)

Received 2 November 2007; revised 6 August 2010; first published online 16 September 2010

Let Ω_n be the n^n-element set consisting of all functions that have $\{1, 2, 3, \ldots, n\}$ as both domain and codomain. Let $\mathbf{T}(f)$ be the order of f, *i.e.*, the period of the sequence $f, f^{(2)}, f^{(3)}, f^{(4)} \ldots$ of compositional iterates. A closely related number, $\mathbf{B}(f) =$ the product of the lengths of the cycles of f, has previously been used as an approximation for $\mathbf{T}$. This paper proves that the average values of these two quantities are quite different. The expected value of $\mathbf{T}$ is

$$\frac{1}{n^n} \sum_{f \in \Omega_n} \mathbf{T}(f) = \exp\left(k_0 \sqrt[3]{\frac{n}{\log^2 n}}(1 + o(1))\right),$$

where k_0 is a complicated but explicitly defined constant that is approximately 3.36. The expected value of $\mathbf{B}$ is much larger:

$$\frac{1}{n^n} \sum_{f \in \Omega_n} \mathbf{B}(f) = \exp\left(\frac{3}{2} \sqrt[3]{n}(1 + o(1))\right).$$

1. Introduction

Let Ω_n be the n^n-element set consisting of all functions that have $[n] = \{1, 2, 3, \ldots, n\}$ as both domain and codomain, and let $f^{(t)}$ denote f composed with itself t times. Since Ω_n is finite, it is clear that, for any $f \in \Omega_n$, the sequence of compositional iterates

$$f, f^{(2)}, f^{(3)}, f^{(4)} \ldots$$

must eventually repeat. Define $\mathbf{T}(f)$ to be the period of this sequence, *i.e.*, the least T such that, for all $m \geqslant n$,

$$f^{(m+T)} = f^{(m)}.$$

We say $v \in [n]$ is a *cyclic vertex* if there is a t such that $f^{(t)}(v) = v$. The restriction of f to its cyclic vertices is a permutation of the cyclic vertices, and the period $\mathbf{T}$ is just the order of this permutation, *i.e.*, the least common multiple of the cycle lengths.

Harris showed that $\mathbf{T}(f) = e^{\frac{1}{8}\log^2 n(1+o(1))}$ for most functions f. To make this precise, let $\mathbb{P}_n$ denote the uniform probability measure on Ω_n; $\mathbb{P}_n(\{f\}) = n^{-n}$ for all f. Define

$$h_n = \frac{1}{8}\log^2 n, \quad b_n = \frac{1}{\sqrt{24}}\log^{3/2} n, \quad \text{and} \quad \phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt.$$

Using Erdős and Turán's seminal results [5], Harris proved the following.

Theorem 1.1 (Harris [10]). *For any fixed x,*

$$\lim_{n\to\infty} \mathbb{P}_n\left(\frac{\log \mathbf{T} - h_n}{b_n} \leqslant x\right) = \phi(x).$$

Remark. Harris actually stated his theorem for a closely related random variable $\mathbf{O}(f) =$ the number of distinct functions in the sequence $f, f^{(2)}, f^{(3)}, \ldots$. However, it is clear from his proof that Theorem 1.1 holds too. In fact, it is straightforward to verify that, for all $f \in \Omega_n$, $|\mathbf{O}(f) - \mathbf{T}(f)| < n$. Related inequalities have been proved by Dénes [4].

Let $\mathbf{B}(f)$ be the product, with multiplicities, of the lengths of the cycles of f. Obviously $\mathbf{T}(f) \leqslant \mathbf{B}(f)$ for all f, and for some exceptional functions $\mathbf{B}(f)$ is *much* larger than $\mathbf{T}(f)$. For example, if f is a permutation with $n/3$ cycles of length 3, then $\mathbf{B}(f) = 3^{n/3}$, but $\mathbf{T}(f) = 3$. (See sequence A000792 in [15] for information about the maximum value that $\mathbf{B}$ can have.) On the other hand, the maximum value $\mathbf{T}$ can have is $e^{\sqrt{n\log n}(1+o(1))}$ [11, 12, 17]. However, for most random functions $f \in \Omega_n$, $\mathbf{B}(f)$ is a reasonably good approximation for $\mathbf{T}(f)$. For example, consider the proposition stated below, which will be deduced in Section 3 from earlier work by Arratia and Tavaré [2].

Proposition 1.2. *There is a constant $c > 0$ such that, for any positive integer n and any positive real number ℓ,*

$$\mathbb{P}_n(\log \mathbf{B} - \log \mathbf{T} \geqslant \ell) \leqslant \frac{c \log n (\log\log n)^2}{\ell}.$$

Although $\log \mathbf{B}(f)$ and $\log \mathbf{T}(f)$ are approximately equal for most functions f, the set of exceptional functions is nevertheless sufficiently large that the expected values of the two random variables $\mathbf{B}$ and $\mathbf{T}$ are quite different. The following theorem will be proved in Section 2.

Theorem 1.3.

$$\frac{1}{n^n}\sum_{f\in\Omega_n} \mathbf{B}(f) = \exp\left(\frac{3}{2}\sqrt[3]{n}\big(1+o(1)\big)\right).$$

To state a corresponding theorem for $\mathbf{T}$, we need to define some constants. First define

$$I = \int_0^\infty \log\log\left(\frac{e}{1-e^{-t}}\right)dt.$$

Then define $k_0 = \frac{3}{2}(3I)^{2/3}$. The following result will be proved in Section 3.

Theorem 1.4.

$$\frac{1}{n^n}\sum_{f\in\Omega_n}\mathbf{T}(f)=\exp\left(k_0\sqrt[3]{\frac{n}{\log^2 n}}\big(1+o(1)\big)\right).$$

2. Expected value of B

Let $\mathcal{Z}(f)$ be the set of cyclic vertices of f, and let $\mathbf{Z}=|\mathcal{Z}|$ be the number of cyclic vertices. It is well known that the restriction of a uniform random mapping to its set $\mathcal{Z}$ of cyclic vertices is a uniform random permutation of $\mathcal{Z}$. Let S_m be the set of all bijections from $[m]$ onto $[m]$. Let $\mu_0=1$, and for $m\geqslant 1$, let

$$\mu_m=\frac{1}{m!}\sum_{\sigma\in S_m}\mathbf{B}(\sigma)$$

be the expected value of the product of the cycle lengths of a uniform random permutation of $[m]$. Then

$$\mathbb{E}_n(\mathbf{B})=\sum_{m=1}^{n}\mathbb{P}_n(\mathbf{Z}=m)\mathbb{E}_n(\mathbf{B}|\mathbf{Z}=m)=\sum_{m=1}^{n}\mathbb{P}_n(\mathbf{Z}=m)\mu_m. \tag{2.1}$$

Theorem 1.3 will be proved directly by estimating the sum in (2.1). Two lemmas make this possible. The first of the two lemmas is an explicit formula for $\mathbb{P}_n(\mathbf{Z}=m)$ that appears in [9] and is attributed to Rubin and Sitgreaves.

Lemma 2.1.

$$\mathbb{P}_n(\mathbf{Z}=m)=\frac{n!m}{(n-m)!n^{m+1}}\leqslant\frac{n!}{(n-m)!n^m}.$$

The second of the two lemmas that are needed for the proof of Theorem 1.3 is Lemma 2.2 below. This asymptotic formula for μ_m appeared in the author's doctoral dissertation [14].

Lemma 2.2.

$$\mu_m\sim\frac{e^{2\sqrt{m}}}{2\sqrt{\pi e}m^{3/4}}.$$

Proof. If $\sigma\in S_m$ is factored into disjoint cycles, then there is a unique cycle τ_σ that contains the number n. Let V_σ be the set of numbers in this cycle. Consider the unique factorization

$$\sigma=\tau_\sigma\pi_\sigma, \tag{2.2}$$

where π_σ is the permutation of $V_\sigma^c=[m]\backslash V_\sigma$ that is obtained by restricting σ to V_σ^c. Since the length of the cycle τ_σ is $|V_\sigma|$, we have

$$\mathbf{B}(\sigma) = |V_\sigma|\mathbf{B}(\pi_\sigma).$$

Given a set $V \subseteq [m]$, there are exactly $(|V|-1)!$ ways to form a cycle from the elements of V. Hence

$$\mu_m = \frac{1}{m!}\sum_{V\subseteq[m],m\in V}(|V|-1)!\sum_{\pi}|V|\mathbf{B}(\pi), \tag{2.3}$$

where, in the inner sum, π is summed over all $(m-|V|)!$ permutations of V^c. Therefore

$$\mu_m = \frac{1}{m!}\sum_{V\subseteq[m],m\in V}|V|!(m-|V|)!\mu_{m-|V|} = \frac{1}{m!}\sum_{\ell=1}^{m}\binom{m-1}{\ell-1}\ell!(m-\ell)!\mu_{m-\ell}.$$

Thus we have a very simple recurrence formula: for all $m \geqslant 1$,

$$m\mu_m = \sum_{\ell=1}^{m}\ell\mu_{m-\ell}. \tag{2.4}$$

Now consider the generating function

$$F(x) = e^{\frac{x}{1-x}} = 1 + x + \frac{3}{2}x^2 + \frac{13}{6}x^3 + \cdots.$$

Observe that

$$xF'(x) = F(x)\sum_{\ell=1}^{\infty}\ell x^{\ell}.$$

Thus the coefficients of F satisfy the recurrence (2.4), and

$$F(x) = \sum_{m=0}^{\infty}\mu_m x^n = e^{\frac{x}{1-x}}.$$

Flajolet and Sedgewick point out that this is the exponential generating function for the number of 'fragmented permutations'. On p. 562 of [6], they describe how the saddle point method can be used to prove that

$$\mu_m \sim \frac{e^{2\sqrt{m}}}{2\sqrt{\pi e}m^{3/4}}. \qquad \square$$

For the purposes of proving Theorem 1.3, we need only a weak corollary to Lemma 2.2.

Corollary 2.3. *For any $\epsilon > 0$, there is an N_ϵ such that, for all $m > N_\epsilon$,*

$$e^{(2-\epsilon)\sqrt{m}} < \mu_m < e^{(2+\epsilon)\sqrt{m}}.$$

We have now assembled everything that is needed to prove Theorem 1.3.

Proof of Theorem 1.3. Let $m_* = \lfloor n^{2/3}\rfloor$. Given $\epsilon > 0$ we can, by Corollary 2.3, choose n sufficiently large that $m_* > N_\epsilon$ and $\mu_{m_*} > e^{(2-\epsilon)\sqrt{m_*}}$. Putting this, and Lemma 2.1, into

(2.1), we get

$$\mathbb{E}_n(\mathbf{B}) \geqslant \mathbb{P}_n(\mathbf{Z} = m_*)\mu_{m_*} = \frac{n!m_*}{(n-m_*)!n^{m_*+1}} e^{(2-\epsilon)\sqrt{m_*}}. \tag{2.5}$$

Applying Stirling's formula, we get

$$\log\left(\frac{n!m_*}{(n-m_*)!n^{m_*+1}} e^{(2-\epsilon)\sqrt{m_*}}\right) = -\frac{m_*^2}{2n} + (2-\epsilon)\sqrt{m_*} + O(\log n).$$

Therefore, for all sufficiently large n, we have the lower bound

$$\mathbb{E}_n(\mathbf{B}) \geqslant e^{(1-\epsilon)\frac{3}{2}\sqrt[3]{n}}.$$

For the upper bound, define

$$U_{n,\epsilon}(m) = n \cdot \frac{n!}{(n-m)!n^m} e^{(1+\epsilon)2\sqrt{m}},$$

and $H_{n,\epsilon}(m) = \log U_{n,\epsilon}(m)$. From Lemma 2.1 and Corollary 2.3, we have, for all sufficiently large n,

$$\mathbb{E}_n(\mathbf{B}) \leqslant n \max_{m\leqslant n} \mathbb{P}_n(\mathbf{Z} = m)\mu_m \leqslant \max_{m\leqslant n} U_{n,\epsilon}(m) = \exp\Big(\max_{m\leqslant n} H_{n,\epsilon}(m)\Big). \tag{2.6}$$

Therefore our goal is to prove an upper bound for $\max_{m\leqslant n} H_{n,\epsilon}(m)$.

If we write $(n-m)! = \Gamma(n+1-m)$, then we can extend the domain of $H_{n,\epsilon}(m)$ to include all real numbers in $[1,n]$. This can only increase the maximum, and with this relaxation, $H_{n,\epsilon}(x)$ is twice differentiable. Let

$$\Psi(y) = \frac{\Gamma'(y)}{\Gamma(y)}$$

be the logarithmic derivative of the Gamma function so that the first two derivatives of $H_{n,\epsilon}$ are

$$H'_{n,\epsilon}(x) = \Psi(n+1-x) - \log n + \frac{1+\epsilon}{\sqrt{x}}, \tag{2.7}$$

and

$$H''_{n,\epsilon}(x) = -\Psi'(n+1-x) - \frac{1+\epsilon}{2x^{3/2}}. \tag{2.8}$$

It is well known [1, p. 260, equation 6.4.10] that

$$\Psi'(y) = \sum_{k=0}^{\infty} \frac{1}{(y+k)^2} > 0. \tag{2.9}$$

Thus both terms of (2.8) are negative, and, for $1 \leqslant x \leqslant n$, we have

$$H''_{n,\epsilon}(x) < 0. \tag{2.10}$$

Let x_* be the unique solution to $H'_{n,\epsilon}(x) = 0$ at which $H_{n,\epsilon}$ attains its maximum. We need to estimate x_*, and then use that estimate to approximate $H_{n,\epsilon}(x_*)$.

Define $a = (1+\epsilon)^{2/3}n^{2/3}$. This first guess for the approximate location of x_* was obtained heuristically from (2.7) by first replacing $\Psi(n+1-x)$ with the approximation

$\log n - \frac{x}{n}$, and then solving the resulting equation

$$\frac{-x}{n} + \frac{1+\epsilon}{\sqrt{x}} = 0$$

for x. (To simplify notation, we write a instead of $a_{n,\epsilon}$, and x_* instead of $x_{n,\epsilon}$; it is implicit that a and x_* depend on both n and ϵ.) Also let $\delta = 1/n^{1/3}$. To prove that $(1-\delta)a < x_* < (1+\delta)a$, it suffices to verify that $H'_{n,\epsilon}((1-\delta)a) > 0$ and that $H'_{n,\epsilon}((1+\delta)a) < 0$.

It is well known [1] that

$$\Psi(y) = \log y + O\left(\frac{1}{y}\right). \tag{2.11}$$

Put (2.11) into (2.7) with $y = n+1-x$ and $x = (1-\delta)a$. Also observe that

$$\log(n+1-x) - \log n = \log\left(1 - \frac{x}{n}\right) + O\left(\frac{1}{n}\right) = -\frac{x}{n} - \frac{x^2}{2n^2} + O\left(\frac{1}{n}\right).$$

Hence

$$\begin{aligned} H'_{n,\epsilon}((1-\delta)a) &= -\frac{(1-\delta)a}{n} + \frac{1+\epsilon}{\sqrt{(1-\delta)a}} - \frac{(1-\delta)^2a^2}{2n^2} + O\left(\frac{1}{n}\right) \\ &= \frac{(1+\epsilon)^{2/3}}{n^{1/3}}\left(\delta - 1 + \frac{1}{\sqrt{1-\delta}} - \frac{(1-\delta)^2(1+\epsilon)^{2/3}}{2n^{1/3}}\right) + O\left(\frac{1}{n}\right). \end{aligned}$$

Using

$$\delta - 1 + \frac{1}{\sqrt{1-\delta}} = \frac{3\delta}{2} + O(\delta^2) \quad \text{and} \quad \delta = \frac{1}{n^{1/3}},$$

we get

$$H'_{n,\epsilon}((1-\delta)a) = \frac{(1+\epsilon)^{2/3}}{2n^{2/3}}\left\{3 - (1+\epsilon)^{2/3} + O\left(\frac{1}{n^{1/3}}\right)\right\} + O\left(\frac{1}{n}\right).$$

If ϵ is a small positive constant, then $3 > (1+\epsilon)^{2/3}$. Therefore $H'_{n,\epsilon}((1-\delta)a) > 0$ for all sufficiently large n. By a similar argument, $H'_{n,\epsilon}((1+\delta)a) < 0$. This completes the proof that, for all sufficiently large n, $a(1-\delta) < x_* < a(1+\delta)$.

At this point, we know that

$$x_* = \left(1 + O\left(\frac{1}{n^{1/3}}\right)\right)(1+\epsilon)^{2/3}n^{2/3}.$$

We also know from (2.6) that, for all sufficiently large n,

$$\mathbb{E}_n(\mathbf{B}) \leqslant n\frac{n!}{(n-x^*)!n^{x^*}}e^{(2+\epsilon)\sqrt{x^*}}. \tag{2.12}$$

Therefore, by Stirling's formula,

$$\log \mathbb{E}_n(\mathbf{B}) \leqslant \frac{-x_*^2}{2n} + (2+\epsilon)\sqrt{x_*} + O(\log n) < \frac{3}{2}(1+\epsilon)\sqrt[3]{n}\big(1+o(1)\big).$$

Since ϵ can be chosen arbitrarily small, Theorem 1.3 is proved. □

https://doi.org/10.1017/S0963548310000337 Published online by Cambridge University Press

It may be possible to strengthen Theorem 1.3 by combining the methods of Hansen [8] with a Tauberian theorem or related methods for estimating the coefficients of generating functions [13]. It is surprisingly difficult to prove that the sequence $\langle \mathbb{E}_n(\mathbf{B})\rangle_{n=1}^{\infty}$ is increasing, but clearly the partial sums $\langle \sum_{m=1}^{n} \mathbb{E}_m(\mathbf{B})\rangle_{n=1}^{\infty}$ are.

3. Order

The main goal in this section is the proof of Theorem 1.4, an estimate for the average period $\mathbb{E}_n(\mathbf{T})$. First, however, for comparison and perspective, we prove Proposition 1.2, concerning the typical period, which was stated in the Introduction.

Proof of Proposition 1.2. Let $\mathbf{Z}(f)$ denote the number of cyclic vertices of f. Then

$$\mathbb{P}_n(\log \mathbf{B} - \log \mathbf{T} > \ell_n) = \sum_m \mathbb{P}_n(\mathbf{Z} = m)\mathbb{P}_n(\log \mathbf{B} - \log \mathbf{T} > \ell_n | \mathbf{Z} = m). \tag{3.1}$$

In the proof of Theorem 8 of [2, p. 333], Arratia and Tavaré computed the expected value of $\log \mathbf{B} - \log \mathbf{T}$ given the number of cyclic vertices:

$$\mathbb{E}_n(\log \mathbf{B} - \log \mathbf{T} | \mathbf{Z} = m) = O(\log m (\log\log m)^2).$$

Therefore, by Markov's inequality, there is a constant $c > 0$ such that, for all $\ell > 0$,

$$\mathbb{P}_n(\log \mathbf{B} - \log \mathbf{T} > \ell | \mathbf{Z} = m) \leqslant \frac{c \log m (\log\log m)^2}{\ell} \leqslant \frac{c \log n (\log\log n)^2}{\ell}. \tag{3.2}$$

Putting (3.2) back into the sum (3.1), we get the proposition. □

The proof of Theorem 1.4 is similar to that of Theorem 1.3. Instead of estimates for μ_m, we need estimates for the $M_m = \frac{1}{m!}\sum_{f\in S_m} \mathbf{T}(f)$. Define $\beta_0 = \sqrt{8I}$ where, as before,

$$I = \int_0^{\infty} \log\log\left(\frac{e}{1-e^{-t}}\right) dt.$$

The constant β_0 first appears in [7], where it is proved that the expected order of a random permutation is $\exp(\beta_0\sqrt{n/\log n}(1+o(1)))$. However, Stong obtained a better error term [16], and this added precision is used in the proof of Theorem 1.4. See [3], and its references, for further information about the asymptotic distribution of $\mathbf{T}$ for random permutations.

Lemma 3.1 (Stong [16]).

$$\log M_m = \beta_0\sqrt{m/\log m} + O\left(\frac{\sqrt{m}\log\log m}{\log m}\right).$$

With Lemma 2.1 and Lemma 3.1 available, we can prove Theorem 1.4.

https://doi.org/10.1017/S0963548310000337 Published online by Cambridge University Press

Proof of Theorem 1.4. Define $\alpha_0 = \sqrt[3]{3I}$, and let m_0^* be the closest integer to $\alpha_0 \sqrt[3]{n^2/\log n}$. For the lower bound, we use the trivial inequality

$$\mathbb{E}_n(\mathbf{T}) = \sum_m \mathbb{P}_n(\mathbf{Z} = m) M_m \geqslant \mathbb{P}_n(\mathbf{Z} = m_0^*) M_{m_0^*}.$$

Then, by Lemma 2.1, Theorem 3.1, and Stirling's formula, $\mathbb{E}_n(\mathbf{T})$ is greater than

$$\exp\left(-\frac{(m_0^*)^2}{2n} + O\left(\frac{(m_0^*)^3}{n^2}\right) + \beta_0\sqrt{\frac{m_0^*}{\log m_0^*}} + O\left(\frac{\sqrt{m_0^*}\log\log m_0^*}{\log m_0^*}\right)\right)$$
$$= \exp\left(\frac{k_0 n^{1/3}}{\log^{2/3} n} + O\left(\frac{n^{1/3}\log\log n}{\log^{7/6} n}\right)\right).$$

For the upper bound, suppose $\epsilon > 0$ is a fixed but arbitrarily small positive number. Define

$$\beta_\epsilon = \beta_0 + \epsilon, \quad \text{and} \quad w_\epsilon(m) = \frac{n!}{(n-m)!n^{m-1}} e^{\beta_\epsilon \sqrt{m/\log m}}.$$

By Theorem 3.1, $M_m \leqslant e^{\beta_\epsilon \sqrt{m/\log m}}$ for all sufficiently large m. Therefore, for all sufficiently large n,

$$\mathbb{E}_n(\mathbf{T}) \leqslant n \max_{m \leqslant n} \mathbb{P}_n(Z = m) M_m \leqslant \max_{m \leqslant n} w_\epsilon(m). \tag{3.3}$$

For $6 \leqslant m \leqslant n$, let $G_{n,\epsilon}(m) = \log w_\epsilon(m)$. As in (2.7), we can extend the domain and differentiate. If $6 \leqslant x \leqslant n$, then

$$G'_{n,\epsilon}(x) = \Psi(n+1-x) - \log n + \frac{\beta_\epsilon}{2\sqrt{x\log x}}\left(1 - \frac{1}{\log x}\right), \tag{3.4}$$

and

$$G''_{n,\epsilon}(x) = -\Psi'(n+1-x) + \frac{\beta_\epsilon}{4}\frac{(3-\log^2 x)}{x^{3/2}\log^{5/2} x}. \tag{3.5}$$

As in (2.10), we use (2.9) to deduce that both terms of (3.5) are negative and $G''_{n,\epsilon}(x) < 0$ for $6 \leqslant x \leqslant n$. Let x^* be the unique solution to $G'_{n,\epsilon}(x) = 0$ at which $G_{n,\epsilon}$ attains its maximum.

As a rough approximation for x^*, define

$$m^* = \beta_\epsilon^{2/3} \sqrt[3]{3/8} \frac{n^{2/3}}{(\log n)^{1/3}}.$$

Let

$$\delta_n = \frac{(\log\log n)^2}{\log n}.$$

In order to prove that

$$(1-\delta_n)m^* < x^* < (1+\delta_n)m^*, \tag{3.6}$$

it suffices to verify that $G'_{n,\epsilon}((1-\delta_n)m^*) > 0$ and $G'_{n,\epsilon}((1+\delta_n)m^*) < 0$. Putting (2.11) into (3.4), we get

$$G'_{n,\epsilon}((1-\delta_n)m^*) = \frac{\sqrt[3]{3\beta_\epsilon^2}}{\sqrt[3]{8n\log n}}\left\{\delta_n - 1 + \frac{1}{\sqrt{1-\delta_n}} + O\left(\frac{\log\log n}{\log n}\right)\right\}. \tag{3.7}$$

In (3.7), the quantity inside braces is positive for large n because

$$\delta_n = \frac{(\log\log n)^2}{\log n} \quad \text{and} \quad \delta_n - 1 + \frac{1}{\sqrt{1-\delta_n}} = \frac{3\delta_n}{2} + O(\delta_n^2).$$

Therefore $G'_{n,\epsilon}((1-\delta_n)m^*) > 0$ for all sufficiently large n. By similar reasoning $G'_{n,\epsilon}((1+\delta_n)m^*) < 0$. Therefore

$$x^* = m^*\left(1 + O\left(\frac{(\log\log n)^2}{\log n}\right)\right).$$

But then, by Stirling's formula,

$$G_{n,\epsilon}(x^*) = \frac{k_\epsilon n^{1/3}}{\log^{2/3} n}\big(1+o(1)\big),$$

where

$$k_\epsilon = -\frac{(\beta_\epsilon^{2/3}\sqrt[3]{3/8})^2}{2} + \beta_\epsilon\sqrt{\frac{\beta_\epsilon^{2/3}\sqrt[3]{3/8}}{2/3}}.$$

The theorem now follows from the fact that ϵ was an arbitrarily small positive number, and $\lim_{\epsilon\to 0^+} k_\epsilon = k_0$. □

Acknowledgements

I wish to thank both the editors and an anonymous referee for noticing an error in my proof of Theorem 1.3 and making helpful suggestions. The problem of estimating $\mathbb{E}_n(\mathbf{T})$ was suggested to me by Boris Pittel. Portions of this work were done while the author was a visitor at the University of Delaware.

References

[1] Abramowitz, M. and Stegun, I. A. (1964) *Handbook of Mathematical Functions: With Formulas, Graphs, and Mathematical Tables*, Dover.

[2] Arratia, R. and Tavaré, S. (1992) Limit theorems for combinatorial structures via discrete process approximations. *Random Struct. Alg.* **3** 321–345.

[3] Barbour, A. D. and Tavaré, S. (1994) A rate for the Erdős–Turán law. *Combin. Probab. Comput.* **3** 167–176.

[4] Deńes, J. (1970) Some combinatorial properties of transformations and their connections with the theory of graphs. *J. Combin. Theory* **9** 108–116.

[5] Erdős, P. and Turán, P. (1967) On some problems of a statistical group theory III. *Acta Math. Acad. Sci. Hungar.* **18** 309–320.

[6] Flajolet, P. and Sedgewick, R. (2009) *Analytic Combinatorics*, Cambridge University Press.

[7] Goh, W. and Schmutz, E. (1991) The expected order of a random permutation. *Bull. London Math. Soc.* **23** 34–42.

[8] Hansen, J. C. (1989) A functional central limit theorem for random mappings. *Ann. Probab.* **17** 317–332.
[9] Harris, B. (1960) Probability distributions related to random mappings. *Ann. Math. Statist.* **31** 1045–1062.
[10] Harris, B. (1973) The asymptotic distribution of the order of elements in symmetric semigroups. *J. Combin. Theory Ser. A* **15** 66–74.
[11] Landau, E. (1953) *Handbuch der Lehre von der Verteilung der Primzahlen*, Vol. 2, Chelsea Publishing, pp. 222–229.
[12] Massias, J. P., Nicolas, J. L. and Robin, G. (1988) Évaluation asymptotique de l'ordre maximum d'un élément du groupe symétrique. *Acta Arith.* **50** 221–242.
[13] Odlyzko, A. M. (1992) Explicit Tauberian estimates for functions with positive coefficients. *J. Comput. Appl. Math.* **41** 187–197.
[14] Schmutz, E. (1988) Statistical group theory. Doctoral Dissertation, Mathematics Department, University of Pennsylvania, Philadelphia, USA.
[15] Sloane, N. J. A. *The On-Line Encyclopedia of Integer Sequences*, published electronically at: `www.research.att.com/~njas/sequences/`, sequence A000792, accessed March 2010.
[16] Stong, R. (1998) The average order of a permutation. *Electron. J. Combin.* **5** #41.
[17] Szalay, M. (1980) On the maximal order in S_n and S_n^*. *Acta Arith.* **37** 321–331.