COMBINATORICA
Bolyai Society – Springer-Verlag

COMBINATORICA **29** (2) (2009) 131–151
DOI: 10.1007/s00493-009-2343-3

THE DISTRIBUTION OF THE ROOT DEGREE OF A RANDOM PERMUTATION

BÉLA BOLLOBÁS*, BORIS PITTEL†

Received August 16, 2006

Given a permutation ω of $\{1,\dots,n\}$, let $R(\omega)$ be the root degree of ω, i.e. the smallest (prime) integer r such that there is a permutation σ with $\omega=\sigma^r$. We show that, for ω chosen uniformly at random, $R(\omega)=(\ln\ln n-3\ln\ln\ln n+O_p(1))^{-1}\ln n$, and find the limiting distribution of the remainder term.

1. Introduction and main results

Given permutations ω and σ of $[n]=\{1,\dots,n\}$, and an integer $r\ge 2$, we say that σ is an rth root of ω if $\omega=\sigma^r$, i.e., if ω is the rth power of σ. The problem of estimating the number of permutations of $[n]$ that are rth powers has attracted much attention since Turán [10] proved an upper bound for r prime, and Blum [2] gave a sharp estimate for $r=2$. Bender [1] established an asymptotic formula for the partial sum of these numbers. Bolker and Gleason [3] found a sharp asymptotic formula for the case when r is prime, and Bóna, McLennan and White [5] showed that the fraction of those ω decreases with n. Recently Pouyanne [7] proved that, for a fixed $r\ge 2$, this fraction is asymptotic to $b_r n^{-(1-\phi(r)/r)}$ where, as usual, $\phi(\cdot)$ is the Euler totient function, so that $\phi(r)$ is the number of integers up to n that are relative prime to r. Of course, this fraction is simply the probability that a

Mathematics Subject Classification (2000): 05A15, 05A16, 60C05, 60F05

* Research supported in part by NSF grants CCR-0225610, DMS-0505550 and ARO grant W911NF-06-1-0076.

† Research supported by NSF grant DMS-0406024.

permutation ω chosen uniformly at random among all $n!$ permutations of $[n]$ has an rth degree root.

The aim of this paper is to continue Pouyanne's work and to study the limiting distribution of the root degree $R_n = R(\omega)$, the smallest (necessarily prime) integer $r \geq 2$ such that ω has an rth root.

First, let us give a short proof of the fact that $R_n/(\ln n)$ is bounded in probability. Let p be a prime. A permutation ω is a pth power iff $C_j(\omega)$, the number of cycles of ω of length j, is divisible by p whenever j is divisible by p. Now

$$C_j(\omega) = \sum_{A \subset [n]\,:\,|A|=j} \mathbf{I}_A(\omega),$$

where $\mathbf{I}_A(\omega)$ is the indicator of the event "A is the vertex set of a j-long cycle of ω". For the uniformly random ω,

$$\mathrm{E}[\mathbf{1}_A] = \frac{(j-1)!(n-j)!}{n!}.$$

So

$$\begin{aligned} \mathrm{E}\left[\sum_{\{j:\,p|j\}} C_j\right] &= \sum_{\{j:\,p|j\}} \frac{\binom{n}{j}(j-1)!(n-j)!}{n!} \\ &= \sum_{\{j:\,p|j\}} \frac{1}{j} \leq 2\,\frac{\ln n}{p}. \end{aligned}$$

By Bertrand's postulate, if $a \geq 2$ and $n \geq 2$ then there is a prime $p = p(n,a) \in [a \ln n, 2a \ln n]$. Consequently,

$$\mathrm{P}\{C_j = 0,\, \forall j \equiv 0 (\mathrm{mod}\ p)\} \geq 1 - \frac{2 \ln n}{p} \geq 1 - \frac{2}{a}.$$

It remains to notice that if the event $\{\omega : C_j(\omega) = 0, \forall j \equiv 0 (\mathrm{mod}\ p)\}$ holds then ω has a pth root.

We shall prove that, in fact,

$$R(\omega) = \frac{\ln n}{\ln \ln n - 3 \ln \ln \ln n + O_p(1)},$$

where $O_p(1)$ denotes a random variable $X_n = X_n(\omega)$ bounded in probability as $n \to \infty$, i.e., $\mathrm{P}\{X_n \leq \gamma_n\} \to 1$ for $\gamma_n \to \infty$ however slowly. More precisely, we shall show that the total number of primes

$$p \leq \frac{\ln n}{\ln \ln n - 3 \ln \ln \ln n + x}, \quad x \in (-\infty, \infty),$$

such that ω is a pth power tends in distribution to a Poisson variable with parameter $\lambda = e^{-x}$. To prove this result we shall extend Pouyanne's asymptotic formula to the case when r may grow polylogarithmically with n. The analysis is rather technical since the total number of algebraic singularities of the relevant generating function increases with n. A key tool of the proof of Poisson convergence is the following form of the prime number theorem (PNT) with a remainder term (see, e.g., Tenenbaum [9]):

$$\pi(x) = \int_2^x \frac{dy}{\ln y} + O\big(x \exp\big(-(\ln x)^{1/2}\big)\big), \quad x \to \infty.$$

Here and elsewhere we use the big-Oh notation for the order of magnitude of various remainder terms, as the appropriate parameter tends to a certain limit (usually $n \to \infty$).

2. Statements and proofs

Let ω be a permutation of $[n] = \{1, \dots, n\}$ and $r > 1$ an integer. Let $p_1 < \dots < p_k$ be the distinct prime factors of r, of multiplicity $a_1, \dots, a_k$, so that $r = \prod_{i \in [k]} p_i^{a_i}$. Write q for the largest square-free divisor of r, i.e., $q = \prod_{i \in [k]} p_i$. Given $S \subseteq [k]$, define $r(S) = \prod_{i \in S} p_i^{a_i}$. Let $\mathbf{C} = \mathbf{C}(\omega) = (C_j(\omega))_{j=1}^n$, where $C_j(\omega)$ is the number of cycles of length j in the canonical representation of ω. Pouyanne [7] proved that ω is an rth power iff $C_j(\omega)$ is divisible by $r(S)$ whenever j is divisible by $\prod_{i \in S} p_i$. We shall denote by $\mathcal{C}_r$ the set of integer sequences $\mathbf{c} = (c_j)_{j=1}^n$ satisfying this condition.

Suppose ω is chosen uniformly at random among all $n!$ permutations. Set $\mathbf{C}(n) = \mathbf{C}(\omega)$, and $P(\mathcal{C}_r) = \mathrm{P}\{\mathbf{C}(n) \in \mathcal{C}_r\}$. In the proposition below, $\phi(\cdot)$ is again Euler's totient function, so that $\phi(n) = n \prod_{p|n} \big(1 - \frac{1}{p}\big)$, with the sum over the primes dividing n. Furthermore, again as usual, $\mu(\cdot)$ is the Möbius function, so that $\phi(n) = n \sum_{d|n} \mu(d)/d$; in particular, for the square-free number $q = p_1 \cdots p_k$ we have $\phi(q) = \prod_{i=1}^k (p_i - 1) = q \sum_{d|q} \mu(d)/d$.

Proposition. *There exists an absolute constant $c^* > 0$ such that if r is an integer with k prime divisors and*

$$2^k \ln r \le c \frac{\ln n}{\ln \ln n}, \quad c < c^*, \tag{1}$$

then

$$P(\mathcal{C}_r) = \frac{1 + O(\varepsilon_n)}{n^{1 - \phi(r)/r}} \cdot \frac{\beta_r}{\Gamma(\phi(r)/r)} \prod_{d|r} d^{-\mu(d)/d},$$

where

$$\varepsilon_n = \exp\left(-(c^* - c)\frac{\ln n}{\ln\ln n}\right),$$

(2) $$\beta_r = \prod_{\{j\geq 1:\ gcd(j,r)>1\}} Exp_{r_j}(1/j), \quad Exp_d\,(x) := \sum_{\nu\equiv 0(mod\ d)} \frac{x^\nu}{\nu!},$$

and

(3) $$r_j = r(S_j) = \prod_{i\in S_j} p_i^{a_i}, \quad S_j = \{p_i : p_i \mid j\}.$$

Remarks. (a) For a fixed r, and without an explicit remainder term estimate, this was proved in [7].

(b) It is known (see, e.g., Hardy and Wright [6]) that most of the large integers r have less than $\log_2 \ln r$ (prime) divisors. For those typical r's the condition (1) is met if

$$r \leq \exp\left[\left(c\,\frac{\ln n}{\ln\ln n}\right)^{1/2}\right].$$

(c) Pouyanne's result implies that $R_n = R(\omega)$, the root degree of the random ω, is unbounded in probability. We shall use Proposition to determine the *likely* order of R_n.

(d) Now that r is allowed to grow with n, analytical issues become noticeably less standard. It turns out to be helpful to use some auxiliary *independent* random variables, which approximate the cycle counts $C_j(\omega)$'s.

Proof of Proposition. Lloyd and Shepp [8] proved that $(C_j)_{j\geq 1}$ coincides in distribution with the sequence $\mathbf{Z} = (Z_j)_{j\geq 1}$ of independent Poisson random variables (z^j/j), conditioned on the event $\{\mathbf{Z} \in A_n\}$, $A_n := \{\mathbf{c} : \sum_j jc_j = n\}$. Here $z < 1$ is arbitrary. Since for $|x| < z^{-1}$ we have

$$\mathrm{E}\big[x^{\sum_j jZ_j}\big] = \prod_j \exp\left(-\frac{z^j}{j} + \frac{(xz)^j}{j}\right) = \frac{1-z}{1-xz},$$

we see that $\sum_j jZ_j$ is geometrically distributed, with parameter $1-z$. In particular

(4) $$P(A_n) = \mathrm{P}\{\mathbf{Z} \in A_n\} = (1-z)z^n.$$

As in [8], to maximize $P(A_n)$ we take $z = 1 - n^{-1}$. Thus

(5)
$$\mathrm{P}\{\mathbf{C}(n) \in \mathcal{C}_r\} = \frac{\mathrm{P}\{\mathbf{Z} \in \mathcal{C}_r\,;\, \mathbf{Z} \in A_n\}}{\mathrm{P}\{\mathbf{Z} \in A_n\}} = \frac{\mathrm{P}\{\mathbf{Z} \in A_n \mid \mathbf{Z} \in \mathcal{C}_r\}\mathrm{P}\{\mathbf{Z} \in \mathcal{C}_r\}}{\mathrm{P}\{\mathbf{Z} \in A_n\}}.$$

Let us remark that there is nothing special about the set $\mathcal{C}_r$: relation (5) holds for every collection of finite sequences of nonnegative integers. Having said this, we add that $\mathcal{C}_r$ is defined by the divisibility condition imposed on the individual components of $\mathbf{c}=(c_1,c_2,\dots)$. This simple observation implies that, *conditioned on the event* $\{\mathbf{Z}\in C_r\}$, the random variables Z_j remain independent. Moreover, for $\gcd(j,r)=1$, conditioning does not affect the distribution of the variable Z_j, and for $\gcd(j,r)>1$, the variable Z_j becomes distributed as the random variable Z_j^* defined by

$$\mathrm{P}\{Z_j^*=r_jt\}=\frac{\mathrm{P}\{Z_j=r_jt\}}{\sum_{\tau\ge 0}\mathrm{P}\{Z_j=r_j\tau\}}=\frac{\frac{(z^j/j)^{r_jt}}{(r_jt)!}}{\sum_{\tau\ge 0}\frac{(z^j/j)^{r_j\tau}}{(r_j\tau)!}},\quad t\ge 0,$$

where $r_j=r(S_j)$ is defined in (3). Since r_j is at least 2, it follows that

$$\begin{aligned} E\left[\sum_{\gcd(j,r)>1} jZ_j^*\right] &= \sum_{\gcd(j,r)>1} j\left(\frac{z^j}{j}\right)^{r_j}\cdot\frac{\sum_{t\ge 0}\frac{\left(\frac{z^j}{j}\right)^{r_jt}}{(r_j(t+1)-1)!}}{\sum_{\tau\ge 0}\frac{\left(\frac{z^j}{j}\right)^{r_j\tau}}{(r_j\tau)!}}\\ &\le\sum_{j\ge 1}\frac{z^j}{j}=\ln\frac{1}{1-z}=\ln n. \end{aligned}\tag{6}$$

Therefore, for every $\lambda>0$, we have

$$\mathrm{P}\left\{\sum_{\gcd(j,r)>1} jZ_j^*\ge\lambda\right\}\le\lambda^{-1}\ln n.\tag{7}$$

Next, we examine the conditional probability in (5). Using Z_j^*, we write

$$\begin{aligned} Q_n := \mathrm{P}\{\mathbf{Z}\in A_n\mid \mathbf{Z}\in\mathcal{C}_r\} = \sum_{m\le n}\mathrm{P}&\left\{\sum_{\gcd(j,r)=1} jZ_j=n-m\right\}\\ &\times\mathrm{P}\left\{\sum_{\gcd(j,r)>1} jZ_j^*=m\right\}. \end{aligned}\tag{8}$$

Let us take a sequence $m_n\to\infty$, such that $\ln n=o(m_n)$, $m_n=o(n)$, postponing its exact definition until the end of the proof. By (7), the contribution of the m's from $[m_n,n]$ to the sum in (8) is at most

$$\sum_{m=m_n}^{n}\mathrm{P}\left\{\sum_{\gcd(j,r)>1} jZ_j^*=m\right\}\le m_n^{-1}\ln n.\tag{9}$$

Thus, we are left with the task of evaluating asymptotically $\mathrm{P}\{\sum_{\gcd(j,r)=1} jZ_j = n-m\}$ for $m \le m_n$. To this end, we go back and express this probability using the variables $C_j(n-m)$ counting the number of cycles in a random permutation of $[n-m]$:

$$\mathrm{P}\left\{\bigcap_{\gcd(j,r)>1}\{C_j(n-m)=0\}\right\} = \frac{\mathrm{P}\Big\{\sum_{\gcd(j,r)=1} jZ_j = n-m\Big\}\mathrm{P}\Big\{\bigcap_{\gcd(j,r)>1}\{Z_j=0\}\Big\}}{\mathrm{P}\Big\{\sum_{j\ge 1} jZ_j = n-m\Big\}}.$$

By formula (4),

$$\mathrm{P}\left\{\sum_{j\ge 1} jZ_j = n-m\right\} = (1-z)z^{n-m};$$

so, by (9), identity (8) becomes

(10)
$$Q_n = \frac{(1-z)z^n}{\mathrm{P}\left\{\bigcap_{\gcd(j,r)>1}\{Z_j=0\}\right\}} \times \left[\sum_{m<m_n} z^{-m}\mathrm{P}\left\{\bigcap_{\gcd(j,r)>1}\{C_j(n-m)=0\}\right\} \mathrm{P}\left\{\sum_{\gcd(j,r)>1} jZ_j^* = m\right\} + O(m_n^{-1}\ln n)\right];$$

as $z^{-m} \le z^{-n} \le e^{-1}$ for $m \le n$. Since $\sum_{\gcd(j,r)>1} jZ_j^* \le m_n$ with probability $1-o(1)$, and $z^m \sim 1$ for $m \le m_n$, it remains to give a sharp estimate for $\mathrm{P}\{\cap_{\gcd(j,r)>1}\{C_j(\nu)=0\}\}$ when $\nu \approx n$.

Applying Cauchy's formula for the number of permutations with given counts of cycles of various lengths, we obtain that if $\nu > 0$ then

(11)
$$\mathrm{P}\left\{\bigcap_{\gcd(j,r)>1}\{C_j(\nu)=0\}\right\} = \sum_{\sum_{\gcd(j,r)=1} j\alpha_j = \nu} \prod_{\gcd(j,r)=1} \frac{(1/j)^{\alpha_j}}{\alpha_j!}$$
$$= [x^\nu]\exp\left(\sum_{\gcd(j,r)=1} \frac{x^j}{j}\right) = [x^\nu]F(x).$$

By the inclusion-exclusion principle, for $|x|<1$ we find that

$$F(x) = \exp\left(\sum_{j\ge 1}\frac{x^j}{j} + \sum_{\ell=1}^{k}(-1)^\ell \sum_{i_1<\cdots<i_\ell}\frac{1}{p_{i_1}\cdots p_{i_\ell}}\sum_{p_{i_1},\dots,p_{i_\ell}|j\ge 1}\frac{x^j}{j}\right)$$

$$(12)\qquad = \exp\left(\ln\frac{1}{1-x} + \sum_{\ell=1}^{k}(-1)^\ell \sum_{i_1<\cdots<i_\ell}\frac{1}{p_{i_1}\cdots p_{i_\ell}}\ln\frac{1}{1-x^{p_{i_1}\cdots p_\ell}}\right)$$

$$= \exp\left(\sum_{d|r}\frac{\mu(d)}{d}\ln\frac{1}{1-x^d}\right) = \prod_{d|r}(1-x^d)^{-\mu(d)/d},$$

with $\mu(\cdot)$ the Möbius function. This key identity was proved differently in [7]. Clearly, for every $d>0$,

$$1-x^d = \prod_{\tau=0}^{d-1}\bigl(1-xe^{-i2\pi\tau/d}\bigr).$$

Hence (12) can be written as

$$(13)\qquad F(x) = \prod_{d|r}\prod_{\tau=0}^{d-1}\bigl(1-xe^{-i2\pi\tau/d}\bigr)^{-\mu(d)/d}, \quad |x|<1.$$

Recall that $q=\prod_s p_s$. Since $\mu(d)\neq 0$ if $d\,|\,q$, each $e^{-i2\pi\tau/d}$ that is actually present in the double product is a root of $x^q=1$, i.e., of the form $x_t=e^{i2\pi t/q}$ for some t, $0\le t<q$. Consequently, (13) is equivalent to

$$(14)\qquad F(x) = \prod_{t=0}^{q-1}\bigl(1-xe^{-i2\pi t/q}\bigr)^{-\alpha_t}, \quad |x|<1,$$

where

$$\alpha_t = \sum_{\emptyset\subseteq S\subseteq[k]}\frac{(-1)^{|S|}}{q(S)}\mathbf{1}_{\{q(S^c)|t\}}, \quad q(A) := \prod_{s\in A}p_s.$$

Putting this another way, setting $D_t=\{s: p_s\,|\,t\}$ we have

$$(15)\qquad \alpha_t = \frac{(-1)^k}{q}\sum_{\emptyset\subseteq A\subseteq D_t}(-1)^{|A|}q(A) = \frac{(-1)^k}{q}\prod_{s\in D_t}(1-p_s)$$

(cf. Lemma in [7]). Therefore $|\alpha_t|<1$ and, as $D_0=[k]$,

$$(16)\qquad \alpha_0 = \frac{\phi(q)}{q}.$$

As $2 \le p_1 < \cdots < p_k$, we have

$$\min\{\alpha_0 - \alpha_t : 0 < t < q\} \ge \frac{\phi(q)}{q} - \frac{1}{q}\prod_{s=3}^{k}(p_s - 1) \ge \frac{1}{2}\frac{\phi(q)}{q}, \tag{17}$$

since

$$(p_1 - 1)(p_2 - 1) \ge (2-1)(3-1) = 2.$$

Therefore x_0 is the dominant singularity, of order α_0, and $\alpha_t \in [-1, 1/2]$ for $t \ne 0$. Furthermore,

$$\begin{aligned}\sum_t |\alpha_t| &= \frac{1}{q}\sum_{D\subseteq[k]}\prod_{s\in D}(p_s - 1)|\{0 \le t < q : D_t = D\}| \\ &= \frac{1}{q}\sum_{D\subseteq[k]}\prod_{s\in D}(p_s - 1)\prod_{s'\in D^c}(p_{s'} - 1) \\ &= \frac{\phi(q)}{q}2^k \le 2^k,\end{aligned} \tag{18}$$

a bound which depends only on the number of prime divisors of r.

By relation (14), the function $F(x)$ has an analytic continuation, which with a slight abuse of notation we also denote by $F(x)$, to the whole complex plane without the radial cuts $R_t = \{x = ux_t, u \ge 1\}$, $0 \le t \le q-1$. This continuation is obtained by setting, for $x \notin R_t$,

$$\left(1 - xe^{-i2\pi t/q}\right)^{-\alpha_t} = \exp\left[-\alpha_t\left(\ln|1 - xe^{-i2\pi t/q}| + i\mathrm{Arg}(1 - xe^{-i2\pi t/q})\right)\right],$$

$\mathrm{Arg} \in (-\pi, \pi)$.

Picking a small $\delta > 0$, let $L = L_\delta$ be a counterclockwise oriented closed contour consisting of q circular arcs A_s alternating with q double radial segments B_s:

$$\begin{aligned}A_s &= \left\{x = (1+\delta)e^{i\theta} : (s-1)\frac{2\pi}{q} \le \theta < s\frac{2\pi}{q}\right\}, \quad 1 \le s \le q, \\ B_s &= \left\{x = ue^{i2\pi s/q} : 1 < u \le 1+\delta\right\}, \quad 1 \le s \le q.\end{aligned}$$

By "double" we mean that each B_s is traversed first downwards from $u = 1+\delta$ to $u = 1+$, and then upwards from $u = 1+$ to $u = 1+\delta$. This contour L is the limit of smooth contours tightly enclosing the δ-long initial segment of the cut R_s. (Shortly, we shall let $\delta = \delta_n \to 0$.) Since $\alpha_s < 1$, and L is the limit of smooth contours enclosing 0 and avoiding the cuts, we have

$$[x^\nu]F(x) = \frac{1}{2\pi i}\oint_L \frac{F(x)}{x^{\nu+1}}\,dx.$$

Here, for $x \in B_s$ we set $F(x) := \lim_{y\to x} F(y)$, with $\arg y < 2\pi s/q$ when traveling downwards, and with $\arg y > 2\pi s/q$ when traveling upwards.

Let us show that the value of the integral is asymptotic to that over the cut B_0. First of all, for $|x| = 1+\delta$,

$$\delta \le |1-x| \le 2+\delta,$$

so that, for $2+\delta < 1/\delta$, i.e., $\delta < \sqrt{2}-1$,

$$|1-x|^{-\alpha_t} \le \left(\frac{1}{\delta}\right)^{|\alpha_t|}.$$

Therefore, by (18),

$$\begin{aligned}\max\{|F(x)| : x \in \cup_s A_s\} &\le \prod_{t=0}^{q-1} \left(\frac{1}{\delta}\right)^{|\alpha_t|} \\ &\le \left(\frac{1}{\delta}\right)^{\sum_t |\alpha_t|} \le \left(\frac{1}{\delta}\right)^{2^k},\end{aligned}$$

so

$$\frac{1}{2\pi} \int\limits_{\cup_s A_s} \frac{|F(x)|}{|x|^{\nu+1}} \, |dx| \le \delta^{-2^k} (1+\delta)^{-\nu}. \tag{19}$$

Consider now the contribution of a cut B_τ, $0 < \tau < q$. Suppose that $q \ge 3$. We have

$$\begin{aligned}\max_{x\in B_\tau} \prod_{t\neq\tau} \left|1 - xe^{-i2\pi t/q}\right|^{-\alpha_t} &= \max_{u\in[1,1+\delta]} \prod_{t\neq\tau} \left|1 - ue^{i2\pi(\tau-t)/q}\right|^{-\alpha_t} \\ &\le q^{\sum_{t=0}^{q} |\alpha_t|} \le q^{2^k},\end{aligned} \tag{20}$$

because, for $|\tau - t| \ge 1$,

$$4/q \le \left|1 - e^{i2\pi/q}\right| \le \left|1 - ue^{i2\pi(\tau-t)/q}\right| \le 2+\delta \le q, \tag{21}$$

if $\delta \le 1$. For $q=2$, we have $\tau = 1$, $t=0$, and $\alpha_0 = 1/2$. So

$$\max_{x\in B_1} |1-x|^{-\alpha_0} = \max_{u\in[1,1+\delta]} |1+u|^{-1/2} = 2^{-1/2},$$

whence (20) holds for $q=2$ as well.

The absolute value of the integral of the omitted τth factor over B_τ is bounded by

$$I_\tau := \int_{B_\tau} \frac{|1 - xe^{-i2\pi\tau}|^{-\alpha_\tau}}{|x|^{\nu+1}}\,|dx| = 2\int_1^{1+\delta} (u-1)^{-\alpha_\tau} u^{-\nu-1}\,du$$
$$= \frac{2}{\nu^{1-\alpha_\tau}} \int_0^{\nu\delta} w^{-\alpha_\tau}(1+w/\nu)^{-\nu-1}\,dw. \tag{22}$$

Since $\alpha_\tau \le 1/2$ for $\tau \neq 0$, the last integral is asymptotic to $\Gamma(1-\alpha_\tau)$ provided that $\nu\delta \to \infty$, in which case the integral over B_τ is of order $\nu^{-1+\alpha_\tau}$. Therefore the contribution of B_τ is of order $q^{2^k}\nu^{-1+\alpha_\tau}$, and so

$$\int_{x\in\bigcup_{\tau\neq 0} B_\tau} \frac{|F(x)|}{|x|^{\nu+1}}\,|dx| = O\Big(q^{2^k+1}\sum_{\tau\neq 0}\nu^{-1+\alpha_\tau}\Big)$$
$$= O\big(q^{2^k+1}\,\nu^{-1+\alpha_0}\nu^{\max_{\tau\neq 0}(\alpha_\tau-\alpha_0)}\big)$$
$$= O\big(q^{2^k+1}\,\nu^{-1+\alpha_0/2}\big), \tag{23}$$

as $\alpha_\tau \le \alpha_0/2$.

Finally, we turn to the cut B_0. For $x \in B_0$,

$$F(x) = (1-x)^{-\alpha_0} G(x),$$

where

$$G(x) := \prod_{\tau\neq 0}\big(1 - xe^{-i2\pi\tau/q}\big)^{-\alpha_\tau}$$

and

$$(1-x)^{-\alpha_0} = |1-x|^{-\alpha_0} \times \begin{cases} e^{-i\alpha_0\pi}, & \text{for } x \text{ from } 1+\delta \text{ to } 1,\\ e^{i\alpha_0\pi}, & \text{for } x \text{ from } 1 \text{ to } 1+\delta.\end{cases}$$

In addition,

$$G(x) = G(1) + O\Big(|x-1| \max_{1\le y\le 1+\delta} |G'(y)|\Big), \quad x \to 1$$

where

$$G'(y) = G(y)\sum_{\tau\neq 0}\frac{\alpha_\tau e^{-i2\pi\tau/q}}{1 - ye^{-i2\pi\tau/q}}.$$

Therefore, by (20) and (21), we have

$$G(x) = G(1) + O\big(|x-1| q^{2^k+2}\big), \quad x \to 1.$$

Here, using $\alpha_0 = \phi(q)/q = \phi(r)/r$ and (12),

$$G(1) = \lim_{x\uparrow 1}(1-x)^{\alpha_0}F(x) = \lim_{x\uparrow 1}\prod_{d'|r}(1-x)^{\mu(d')/d'}\prod_{d|r}(1-x^d)^{-\mu(d)/d}$$
$$= \prod_{d|r} d^{-\mu(d)/d}.$$

Putting these pieces together, we see that

$$\int_{B_0}\frac{F(x)}{x^{\nu+1}}\,dx = i2\sin(\alpha_0\pi)G(1)\int_1^{1+\delta}(u-1)^{-\alpha_0}u^{-\nu-1}\,du + O(\mathcal{R}_\delta),$$
$$\mathcal{R}_\delta := q^{2^k+2}\int_1^{1+\delta}(u-1)^{1-\alpha_0}u^{-\nu-1}\,du$$

(cf. (22)); $O(\mathcal{R}_\delta)$ stands for a remainder term whose absolute value is at most $\mathcal{R}_\delta$ times an absolute constant. Since $1-\alpha_0 \ge 0$, the integral in $\mathcal{R}_\delta$ is of order $\nu^{-2+\alpha_0}$, hence the remainder term is $O\big(q^{2^k+2}\nu^{-2+\alpha_0}\big)$. If, in addition to $\nu\delta \to \infty$, we impose the restriction that $\delta = o(\nu^{-1/2})$ then, as $(1+w/\nu)^\nu = (1+O(w^2/\nu))e^w, \quad w = o(\nu^{1/2})$,

$$\int_1^{1+\delta}(u-1)^{-\alpha_0}u^{-\nu-1}\,du = (1+O(\nu\delta^2))\frac{\Gamma(1-\alpha_0)}{\nu^{1-\alpha_0}},$$

holds *uniformly* for $\alpha_0 < 1$.

Therefore

$$\frac{1}{2\pi i}\int_{B_0}\frac{F(x)}{x^{\nu+1}}\,dx = (1+O(\nu\delta^2))\frac{\prod_{d|r} d^{-\mu(d)/d}}{\Gamma(\alpha_0)}\nu^{-1+\alpha_0} + O\big(q^{2^k+2}\nu^{-2+\alpha_0}\big), \tag{24}$$

where we have used that

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}, \quad z \ne 0, -1, \ldots.$$

By (19), (23) and (24), we have

$$[x^\nu]F(x) = \frac{1}{2\pi i}\oint_L \frac{F(x)}{x^{\nu+1}}\,dx = (1+O(\nu\delta^2))\frac{\prod_{d|r} d^{-\mu(d)/d}}{\Gamma(\alpha_0)}\nu^{-1+\alpha_0} + O\big(\delta^{-2^k}(1+\delta)^{-\nu} + q^{2^k+1}\nu^{-1+\alpha_0/2} + q^{2^k+2}\nu^{-2+\alpha_0}\big), \tag{25}$$

provided that $\nu\delta\to\infty$ and $\delta=o(\nu^{-1/2})$. Note that

$$\prod_{d|r} d^{-\mu(d)/d} = \exp\left(-\sum_{d|r}\frac{\mu(d)}{d}\ln d\right) = \exp\left(\sum_{p|q}\frac{\phi(q/p)}{q}\ln p\right) \ge 1,$$

and $\Gamma(\alpha_0)\le 1/\alpha_0$, since $\alpha_0\in(0,1)$; therefore

$$\frac{\prod_{d|r} d^{-\mu(d)/d}}{\Gamma(\alpha_0)} \ge \alpha_0 = \frac{\phi(q)}{q}.$$

We know that (see, e.g., Hardy and Wright [6, Thm. 328])

$$a := \inf_{\ell\ge 2}\frac{\phi(\ell)\ln\ln(\ell+1)}{\ell} > 0. \tag{26}$$

Consequently, assuming that $q\le n$, the fraction above is at least $a/\ln\ln n$.

Let us turn to the remainder term in (25). Recall that $\nu\in[n-m_n,n]$, with $m=m_n=o(n)$. Starting with the middle summand, note that

$$q^{2^k+1}\nu^{-1+\alpha_0/2} \le \exp\bigl[(2^k+1)\ln r-(1-\alpha_0/2)\ln\nu\bigr] \le \exp\bigl[2^{k+1}\ln r-0.5\ln\nu\bigr] \le n^{-(0.5-2c_1)}\to 0,$$

if

$$2^k\ln r\le c_1\ln n,\quad c_1<0.25, \tag{27}$$

in which case it dwarfs the third summand.

Set $\delta=n^{-\gamma}$, $\gamma\in(1/2,1)$. Then

$$\delta^{-2^k}(1+\delta)^{-\nu}\le\exp\bigl[2^k\ln n-0.5n^{1-\gamma}\bigr],$$

which by (26) is also negligible compared to the second summand. Therefore the remainder term in (25) is of order $O\bigl(q^{2^k+1}n^{-1+\alpha_0/2}\bigr)$.

Now, using (26) again, we find that

$$\frac{q^{2^k+1}n^{-1+\alpha_0/2}}{n^{-1+\alpha_0}} \le \exp\left(22^k\ln q-\frac{\phi(q)}{2q}\right) \le \exp\left[2\left(2^k\ln q-\frac{a}{4}\frac{\ln n}{\ln\ln n}\right)\right] \le \exp\left[-2(a/4-c)\frac{\ln n}{\ln\ln n}\right]$$

if

$$2^k \ln q \le c \frac{\ln n}{\ln\ln n}, \quad c < \frac{a}{4}. \tag{28}$$

Relations (27) and (28) hold simultaneously if

$$2^k \ln r \le c \frac{\ln n}{\ln\ln n}, \quad c < c^* := \min\{0.25, a/4\},$$

in which case (26) becomes

$$\begin{aligned} \mathrm{P}\left\{ \bigcap_{\gcd(j,r)>1} \{C_j(\nu) = 0\} \right\} &= [x^\nu]F(x) \\ &= (1 + O(\varepsilon_n)) \frac{\prod_{d|r} d^{-\mu(d)/d}}{\Gamma(\alpha_0)} \nu^{-1+\alpha_0}, \end{aligned} \tag{29}$$

where

$$\varepsilon_n := \exp\left(-(c^* - c) \frac{\ln n}{\ln\ln n} \right).$$

By (29) we find that the sum in (10) is

$$(1 + O(m_n/n + \varepsilon_n)) \frac{\prod_{d|r} d^{-\mu(d)/d}}{\Gamma(\alpha_0)} n^{-1+\alpha_0}\, \mathrm{P}\left\{ \sum_{\gcd(j,r)>1} jZ_j^* < m_n \right\},$$

and the last probability is at least $1 - m_n^{-1} \ln n$ (see (9)). Plugging this expression into (10), and using (4), this shows that

$$\begin{aligned} Q_n = &\frac{(1-z)z^n}{\mathrm{P}\left\{ \bigcap_{\gcd(j,r)>1} \{Z_j = 0\} \right\}} \\ &\times \left(1 + O(\varepsilon_n + m_n/n + n^{1-\alpha_0} m_n^{-1} \ln n)\right) \frac{\prod_{d|r} d^{-\mu(d)/d}}{\Gamma(\alpha_0)} n^{-1+\alpha_0}. \end{aligned} \tag{30}$$

Clearly,

$$m_n = n^{1-\alpha_0/2} \sqrt{\ln n} \quad (\ge n^{1/2})$$

is the best choice, in which case

$$m_n/n + n^{1-\alpha_0} m_n^{-1} \ln n = 2n^{-\alpha_0/2}\sqrt{\ln n} \le \sqrt{\ln n}\exp\left(-\frac{a}{2}\frac{\ln n}{\ln\ln n}\right) \ll \varepsilon_n = \exp\left[-(a/4-c)\frac{\ln n}{\ln\ln n}\right].$$

Consequently the 1-plus-big Oh factor in (30) is simply $1+O(\varepsilon_n)$.

By (30) and (5) we have

$$\begin{aligned}\mathrm{P}\{\mathbf{C}(n)\in\mathcal{C}_r\} &= Q_n\frac{\mathrm{P}\{\mathbf{Z}\in\mathcal{C}_r\}}{\mathrm{P}\{\mathbf{Z}\in A_n\}}\\ &= (1+O(\varepsilon_n))\frac{\prod_{d|r} d^{-\mu(d)/d}}{\Gamma(\alpha_0)} n^{-1+\alpha_0}\cdot\frac{\mathrm{P}\{\mathbf{Z}\in\mathcal{C}_r\}}{\mathrm{P}\left\{\bigcap_{\gcd(j,r)>1}\{Z_j=0\}\right\}}.\end{aligned}\tag{31}$$

Finally, the last ratio of the probabilities is

$$\prod_{\gcd(j,r)>1}\left(\sum_{t\ge 0}\frac{(z^j/j)^{r_jt}}{(r_jt)!}\right) = (1+O(n^{-1}))\prod_{\gcd(j,r)>1}\left(\sum_{t\ge 0}\frac{(1/j)^{r_jt}}{(r_jt)!}\right).\tag{32}$$

Indeed, the jth factor is

$$\sum_{t\ge 0}\frac{(1/j)^{r_jt}}{(r_jt)!} + O\left(n^{-1}\sum_{t\ge 1}\frac{(1/j)^{r_jt-1}}{(r_jt-1)!}\right) = \left(1+O\left(n^{-1}\frac{(1/j)^{r_j}}{(r_j-1)!}\right)\right)\sum_{t\ge 0}\frac{(1/j)^{r_jt}}{(r_jt)!}$$

and

$$\sum_{\gcd(j,r)>1}\frac{(1/j)^{r_j}}{(r_j-1)!} \le \sum_{j\ge 1}\frac{1}{j^2} < \infty.$$

This completes our proof of the proposition. ∎

After this substantial preparation, we are ready to prove the main result of this note.

Theorem. *Let $R_n = R(\omega)$ denote the smallest prime r such that $\omega = \sigma^r$ for some permutation $\sigma = \sigma(\omega, r)$. Then, for each fixed x,*

$$\lim_{n\to\infty} P\left\{R_n \le \frac{\ln n}{\ln\ln n - 3\ln\ln\ln n + x}\right\} = 1 - e^{-e^{-x}}.$$

Consequently

$$R_n = \frac{\ln n}{\ln\ln n - 3\ln\ln\ln n + O_p(1)},$$

where $O_p(1)$ stands for a random variable bounded in probability as $n \to \infty$.

Proof. Let us choose a sequence of integers (m_n) with $m_n \sim (\ln\ln n)^{-1}\ln n$, and write $X_n = X(\omega)$ for the total number of primes $p \le m_n$ such that ω is the pth power of some permutation σ. Equivalently,

$$X_n = X(\omega) = \sum_{p\le m_n} \mathbf{1}_{\mathcal{C}_p}(\mathbf{C}(\omega)).$$

Note that, by our Proposition,

$$\mathrm{E}\big[\mathbf{1}_{\mathcal{C}_p}(\mathbf{C}(\omega))\big] = P(\mathcal{C}_p) = \frac{1+O(\varepsilon_n)}{n^{1/p}}\cdot\frac{\beta_p p^{1/p}}{\Gamma(1-p^{-1})}. \tag{33}$$

Since $\sup_p\big[\beta_p p^{1/p}/\Gamma(1-1/p)\big] < \infty$, for $m_n^- = (\alpha\ln\ln n)^{-1}\ln n$, we have

$$\sum_{p\le m_n^-} P(\mathcal{C}_p) \le \frac{\ln n}{\alpha\ln\ln n}\exp\big(-\alpha\ln\ln n\big) \to 0$$

if $\alpha > 1$.

Therefore, with high probability (whp), i.e., with probability $1-o(1)$, there is no prime $p \le m_n^-$ such that ω is a pth power. To put it differently, whp $X_n = Y_n$ where Y_n is the number of admissible primes, i.e., the primes p between m_n^- and m_n for which ω is a pth power:

$$Y_n := \sum_{m_n^- < p \le m_n} \mathbf{1}_{\mathcal{C}_p}(\mathbf{C}(\omega)).$$

Now, for $p > m_n^- \to \infty$, the second fraction in (33) is asymptotic to 1, hence

$$\mathrm{E}[Y_n] \sim \sum_{m_n^- < p \le m_n} n^{-1/p}. \tag{34}$$

More generally, given $k\ge 1$, writing $(Y_n)_k = Y_n(Y_n-1)\cdots(Y_n-k+1)$ for the number of *ordered* k-tuples $(p_{i_1},\dots,p_{i_k})$ of admissible primes, we have

$$(Y_n)_k = \sum_{m_n^- < p_{i_1}\neq\cdots\neq p_{i_k}\le m_n} \prod_{\ell=1}^k \mathbf{1}_{\mathcal{C}_{p_{i_\ell}}}(\mathbf{C}(\omega)).$$

Observe that

$$\prod_{\ell=1}^k \mathbf{1}_{\mathcal{C}_{p_{i_\ell}}}(\mathbf{C}(\omega)) = \mathbf{1}_{\mathcal{C}_q}(\mathbf{C}(\omega)), \quad q=\prod_{\ell=1}^k p_{i_\ell}.$$

Indeed, the product on the right is 1 iff $C_j(\omega)$ is divisible by $\prod_{\ell\in[k]} p_{i_\ell}$ whenever j is divisible by $\prod_{\ell\in[k]} p_{i_\ell}$. By our Proposition,

$$\mathrm{E}[\mathbf{1}_{\mathcal{C}_q}] = P(\mathcal{C}_q) \sim \frac{1}{n^{1-\phi(q)/q}},$$

as the omitted factor in the formula for $P(\mathcal{C}_q)$ is asymptotic to 1. Furthermore, since

$$1-\frac{\phi(q)}{q} = 1-\prod_{\ell=1}^k\left(1-\frac{1}{p_\ell}\right) = \sum_{\ell=1}^k \frac{1}{p_{i_\ell}} + O\big(2^k (m_n^-)^{-2}\big),$$

we have

$$\frac{1}{n^{1-\phi(q)/q}} = \prod_{\ell=1}^k n^{-1/p_{i_\ell}} \cdot \exp\big[O\big(2^k \ln n/(m_n^-)^2\big)\big] \sim \prod_{\ell=1}^k n^{-1/p_{i_\ell}},$$

as

$$\frac{\ln n}{(m_n^-)^2} = \frac{(\alpha\ln\ln n)^2}{\ln n} \to 0.$$

Therefore

$$\mathrm{E}[(Y_n)_k] \sim \sum_{m_n^- < p_{i_1}\neq\cdots\neq p_{i_k}\le m_n} \prod_{\ell=1}^k n^{-1/p_{i_\ell}}. \tag{35}$$

Note that, for $k\ge 2$,

$$\sum_{\substack{m_n^- < p_{i_1},\dots,p_{i_k}\le m_n\\ \exists 1\le u\neq v\le k:\ p_{i_u}=p_{i_v}}} \prod_{\ell=1}^k n^{-1/p_{i_\ell}} \le \binom{k}{2} n^{-2/m_n} \sum_{m_n^- < p_{i_1},\dots,p_{i_{k-2}}\le m_n} \prod_{\ell=1}^{k-2} n^{-1/p_{i_\ell}}$$

$$= \binom{k}{2} n^{-2/m_n}\left(\sum_{m_n^- < p\le m_n} n^{-1/p}\right)^k.$$

Since

$$n^{-2/m_n} = \exp\left(-2(1+o(1))\ln n \frac{\ln\ln n}{\ln n}\right) \le (\ln n)^{-1},$$

relation (35) implies that

$$\text{(36)} \qquad \mathrm{E}[(Y_n)_k] \sim S_n^k + O\big((\ln n)^{-1} S_n^{k-2}\big), \quad S_n := \sum_{m_n^- < p \le m_n} n^{-1/p}.$$

It remains to show that, for some sequence (m_n) with $m_n \sim (\ln\ln n)^{-1} \ln n$, the sequence (S_n) tends to a (finite) limit.

Let $p_1 = 2 < p_2 = 3 < \dots$ be the sequence of primes in increasing order and, as usual, write $\pi(x)$ for the number of primes at most x, so that $\pi(x) = \max\{t\colon p_t \le x\}$. As we remarked earlier, by the PNT with a remainder term (see, e.g., Tenenbaum [9]), we have

$$\text{(37)} \qquad \begin{aligned} \pi(x) &= \mathrm{Li}(x) + O\big(xe^{-(\ln x)^{1/2}}\big), \quad x \to \infty, \\ \mathrm{Li}(x) &:= \int_2^x \frac{dy}{\ln y} \sim \frac{x}{\ln x}, \quad x \to \infty. \end{aligned}$$

Consequently

$$\text{(38)} \qquad t = \mathrm{Li}(p_t) + O\big(p_t e^{-(\ln p_t)^{1/2}}\big).$$

Let $H(\cdot)$ denote the inverse function of $\mathrm{Li}(\cdot)$. From the formula for $\mathrm{Li}(x)$ it follows that

$$H(x) : [0,\infty) \to [2,\infty), \quad H(x) \sim x \ln x,\ x \to \infty.$$

Then

$$\text{(39)} \qquad H'(y) = \frac{1}{\mathrm{Li}'(H(y))} = \ln(H(y)) \sim \ln y, \quad y \to \infty.$$

This formula and (38), together with $p_t \sim t \ln t$, imply that

$$\text{(40)} \qquad p_t = H(t) + O\big(t(\ln t)^2 e^{-(\ln t)^{1/2}}\big).$$

Let

$$[t^-, t^+] = \{t : m_n^- < p_t \le m_n\}.$$

Then

$$\text{(41)} \qquad \begin{aligned} t^- &= \pi(m_n^-) + 1 \sim \frac{\ln n}{\alpha(\ln\ln n)^2}, \\ t^+ &= \pi(m_n) = \mathrm{Li}(m_n) + O\big(m_n e^{-(\ln m_n)^{1/2}}\big) \sim \frac{\ln n}{(\ln\ln n)^2}. \end{aligned}$$

Consequently, for $t\in[t^-,t^+]$,

$$\begin{aligned}\frac{\ln n}{p_t} &= \frac{\ln n}{H(t)+O(t(\ln t)^2 e^{-(\ln t)^{1/2}})}\\ &= \frac{\ln n}{H(t)} + O\big(t^{-1}e^{-(\ln t)^{1/2}}\ln n\big)\\ &= \frac{\ln n}{H(t)} + O\big((\ln\ln n)^2\exp(-0.9(\ln\ln n)^{1/2})\big)\\ &= \frac{\ln n}{H(t)} + o(1),\end{aligned}$$

and so formula (36) for S_n becomes

$$S_n \sim S_n^* := \sum_{t=t^-}^{t^+} \exp\left(-\frac{\ln n}{H(t)}\right).$$

Now, by (39),

$$\frac{d}{dt}\frac{1}{H(t)} = -\frac{1}{(H(t))^2}\ln H(t)$$

and, as $H(t)\geq 2$,

$$\frac{d^2}{dt^2}\frac{1}{H(t)} = \frac{1}{(H(t))^3}\big[2(\ln H(t))^2 - \ln H(t)\big] > 0, \tag{42}$$

showing that $-1/H(t)$ is convex. Consequently

$$\begin{aligned}S_n^* &\leq \exp\left(-\frac{\ln n}{H(t^+)}\right)\sum_{t=t^-}^{t^+}\exp\left((\ln n)\frac{\ln H(t^+)}{(H(t^+))^2}(t-t^+)\right)\\ &\leq \exp\left(-\frac{\ln n}{H(t^+)}\right)\left[1-\exp\left(-(\ln n)\frac{\ln H(t^+)}{(H(t^+))^2}\right)\right]^{-1}\\ &\sim \exp\left(-\frac{\ln n}{H(t^+)}\right)\cdot\frac{(H(t^+))^2}{\ln H(t^+)\ln n},\end{aligned}$$

since

$$(\ln n)\frac{\ln H(t^+)}{(H(t^+))^2} = O((\ln n)^{-1}\ln\ln n) \to 0.$$

By (39) and (41),

$$\begin{aligned}H(t^+) &= H(\mathrm{Li}(m_n)) + O\big(m_n(\ln\ln n)e^{-(\ln m_n)^{1/2}}\big)\\ &= m_n + O\big(e^{-0.9(\ln\ln n)^{1/2}}\ln n\big)\\ &= m_n\big(1+O\big(e^{-0.9(\ln\ln n)^{1/2}}\ln\ln n\big)\big).\end{aligned}$$

Therefore

$$\frac{(H(t^+))^2}{\ln H(t^+)\ln n} \sim \frac{(m_n)^2}{\ln m_n \ln n},$$

and

$$\frac{\ln n}{H(t^+)} = \frac{\ln n}{m_n}\big(1 + O\big(e^{-0.9(\ln\ln n)^{1/2}}\ln\ln n\big)\big)$$
$$= \frac{\ln n}{m_n} + O\big(e^{-0.9(\ln\ln n)^{1/2}}(\ln\ln n)^2\big).$$

Since $m_n^{-1}\ln n$ is of order $\ln\ln n$, we conclude that

$$S_n^* \lesssim \exp\left(-\frac{\ln n}{m_n}\right)\frac{(m_n)^2}{\ln m_n \ln n}. \tag{43}$$

Furthermore, it follows from (41) and (42) that

$$\frac{d^2}{dt^2}\frac{1}{H(t)} = O\big((t^+)^{-3}(\ln t^+)^{-1}\big), \quad t \in [t^-, t^+].$$

Hence, for

$$t \in I_n := \big[t^+(1 - (\ln\ln n)^{-1/2}), t^+\big]$$

we have

$$\frac{1}{H(t)} = \frac{1}{H(t^+)} - \frac{\ln H(t^+)}{(H(t^+))^2}(t - t^+)\big(1 + O\big((\ln\ln n)^{-1/2}\big)\big).$$

Consequently,

$$\begin{aligned}
S_n^* &\geq \sum_{t\in I_n}\exp\left(-\frac{\ln n}{H(t)}\right)\\
&\geq \exp\left(-\frac{\ln n}{H(t^+)}\right)\frac{1-\exp\left(-0.9t^+(\ln\ln n)^{-1/2}\ \frac{\ln n \ln H(t^+)}{(H(t^+))^2}\right)}{1-\exp\left(-(1+o(1))\frac{\ln n\ln H(t^+)}{(H(t^+))^2}\right)}\\
&\gtrsim \exp\left(-\frac{\ln n}{H(t^+)}\right)\frac{1}{1-\exp\left(-(1+o(1))\frac{\ln n\ln H(t^+)}{(H(t^+))^2}\right)}\\
&\sim \exp\left(-\frac{\ln n}{H(t^+)}\right)\cdot\frac{(H(t^+))^2}{\ln H(t^+)\ln n}.
\end{aligned} \tag{44}$$

As

$$t^+(\ln\ln n)^{-1/2}\frac{\ln n\ln H(t^+)}{(H(t^+))^2} \ge c_1\frac{(\ln\ln n)^{-1/2}\ln n}{t^+\ln t^+} \ge c_2(\ln\ln n)^{1/2},$$

relations (43) and (44) imply that

$$S_n^* \sim \exp\left(-\frac{\ln n}{m_n}\right)\frac{(m_n)^2}{\ln m_n \ln n}. \tag{45}$$

Recall that (45) has been proved under the condition that (m_n) is an integer sequence and $m_n \sim (\ln\ln n)^{-1}\ln n$. To choose an appropriate sequence (m_n), let

$$\mu_n(x) := \frac{\ln n}{\ln\ln n - 3\ln\ln\ln n + x}, \quad x\in\mathbb{R},$$

and set $m_n = \lfloor \mu_n(x)\rfloor$.

Simple algebra shows that

$$\begin{aligned} m_n &= \frac{\ln n}{\ln\ln n - 3\ln\ln\ln n + x} + O(1) \\ &= \frac{\ln n}{\ln\ln n - 3\ln\ln\ln n + x_n}, \\ x_n &= x + O\big((\ln n)^{-1}(\ln\ln n)^2\big). \end{aligned}$$

Consequently, for this sequence (m_n) we have

$$\begin{aligned} \lim_{n\to\infty} S_n^* &= \lim_{n\to\infty}\left[\exp\big(-\ln\ln n + 3\ln\ln\ln n - x_n\big)\frac{(\ln n)^2(\ln\ln n)^{-2}}{(\ln\ln n)\ln n}\right] \\ &= e^{-x}. \end{aligned} \tag{46}$$

Thus, recalling that $S_n \sim S_n^*$ and using (36),

$$\lim_{n\to\infty} \mathrm{E}[(Y_n)^k] = (e^{-x})^k, \quad k\ge 1.$$

This implies (see, e.g., [4]) that Y_n, and hence X_n, converges in distribution to Poisson (λ), $\lambda = e^{-x}$,

$$\lim_{n\to\infty} \mathrm{P}\{X_n = k\} = e^{-\lambda}\frac{\lambda^k}{k!}, \quad k\ge 1.$$

Consequently

$$\lim_{n\to\infty} \mathrm{P}\left\{R_n \le \frac{\ln n}{\ln\ln n - 3\ln\ln\ln n + x}\right\} = \lim_{n\to\infty}\mathrm{P}\{X_n > 0\} = 1 - e^{-e^{-x}},$$

completing our proof. ∎

Acknowledgement. We thank a referee who read the paper with a fine comb and provided us with four pages of detailed critical comments and helpful suggestions.

References

[1] E. A. Bender: Asymptotical methods in enumeration, *Siam Rev.* **16** (1974), 485–515.

[2] J. Blum: Enumeration of the square permutations in S_n, *J. Comb. Theory (A)* **17** (1974), 156–161.

[3] E. D. Bolker and A. M. Gleason: Counting permutations, *J. Comb. Theory (A)* **29** (1980), 236–242.

[4] B. Bollobás: *Random Graphs*, 2nd Edition, Cambridge Univ. Press (2001).

[5] M. Bóna, A. McLennan and D. White: Permutations with roots, *Random Structures and Algorithms* **17** (2000), 157–167.

[6] G. H. Hardy and E. M. Wright: *An Introduction to the Theory of Numbers*, 5th ed., Oxford (1979).

[7] N. Pouyanne: On the number of permutations admitting an mth root, *Electronic J. Comb.* **9** (2002), #R3.

[8] L. A. Shepp and S. P. Lloyd: Ordered cycle lengths in a random permutation, *Trans. Amer. Math. Soc.* **121** (1966), 340–357.

[9] G. Tenenbaum: *Introduction to Analysis and Probabilistic Number Theory*, Cambridge University Press (1995).

[10] P. Turán: On some connections between combinatorics and group theory, *Colloq. Math. Soc. János Bolyai (P. Erdős, A. Rényi and V. T. Sós, eds.)*, pp. 1055–1082, North Holland, Amsterdam (1970).

Béla Bollobás

Department of Pure Mathematics
& Mathematical Statistics
University of Cambridge
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WB
UK
and
Department of Mathematical Sciences
University of Memphis
Memphis, Tennessee 38152-3240
USA
bollobas@msci.memphis.edu

Boris Pittel

Department of Mathematics
Ohio State University
Columbus, Ohio 43210-1174
USA
bgp@math.ohio-state.edu