Combinatorics, Probability and Computing (2021), **30**, pp. 800–810
doi:10.1017/S0963548321000043

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Permutations with equal orders

Huseyin Acan[1], Charles Burnette[2], Sean Eberhard[3], Eric Schmutz[1,*] and James Thomas[1]

[1]Department of Mathematics, Drexel University, Philadelphia, PA 19104, USA, [2]Mathematics Department, Xavier University of Louisiana, New Orleans, LA 70125, USA and [3]Department of Pure Mathematics and Mathematical Statistics, Centre for Mathematical Sciences, University of Cambridge, Cambridge CB3 0WB, UK
*Corresponding author. Email: schmutze@drexel.edu

(Received 7 January 2019; revised 15 May 2020; accepted 31 July 2020; first published online 27 January 2021)

Abstract
Let $\mathbb{P}(\operatorname{ord}\pi = \operatorname{ord}\pi')$ be the probability that two independent, uniformly random permutations of $[n]$ have the same order. Answering a question of Thibault Godin, we prove that $\mathbb{P}(\operatorname{ord}\pi = \operatorname{ord}\pi') = n^{-2+o(1)}$ and that $\mathbb{P}(\operatorname{ord}\pi = \operatorname{ord}\pi') \geqslant \frac{1}{2}n^{-2}\lg^{\star} n$ for infinitely many n. (Here $\lg^{\star} n$ is the height of the tallest tower of twos that is less than or equal to n.)

2020 MSC Code: 60C05

1. Introduction

1.1 The problem

Let π be a random permutation of $[n]$. Write $\operatorname{ord}\pi$ for the order of a permutation π, *i.e.* the least common multiple of its cycle lengths. The distribution of $\operatorname{ord}\pi$ is an object of basic interest in probabilistic group theory. For example, a beautiful theorem of Erdős and Turán [3] asserts that $\log \operatorname{ord}\pi$ is asymptotically normal with mean $\log^2 n/2$ and variance $\log^3 n/3$. Many more features of the distribution of $\operatorname{ord}\pi$ are visible through the lens of the theory of logarithmic combinatorial structures: see for example the book of Arratia, Barbour and Tavaré [1]. For example, the largest cycles of π, which determine the magnitude of $\operatorname{ord}\pi$ and its divisibility by large primes, follow a Poisson–Dirichlet law.

A more subtle feature of the distribution of $\operatorname{ord}\pi$ is its collision entropy. Recall that the *collision entropy* or *Rényi 2-entropy* of a random variable X is defined by

$$H_2(X) = -\log \mathbb{P}(X = X'),$$

where X' is an independent copy of X. In other words, for $X = \operatorname{ord}\pi$, the problem is to estimate

$$e^{-H_2(\operatorname{ord}\pi)} = \mathbb{P}(\operatorname{ord}\pi = \operatorname{ord}\pi').$$

This problem was highlighted recently by Godin [7] in connection with automaton groups. We are grateful to Sergey Dovgal for bringing this problem to our attention.

Let $\operatorname{type}\pi$ denote the cycle type of π, *i.e.* the multi-set of its cycle lengths. Since permutations with the same type have the same order, it is clear that

$$\mathbb{P}(\operatorname{ord}\pi = \operatorname{ord}\pi') \geqslant \mathbb{P}(\operatorname{type}\pi = \operatorname{type}\pi').$$

Using methods of analytic combinatorics, Flajolet, Fusy, Gourdon, Panario and Pouyanne [5, Proposition 4] proved that

$$\mathbb{P}(\text{type}\,\pi = \text{type}\,\pi') = \frac{c_0}{n^2} + O\left(\frac{1}{n^3}\right), \quad c_0 = \prod_{k\geqslant 1} I\left(\frac{1}{k^2}\right) \approx 4.26,$$

where $I(z) = \sum_{n\geqslant 0} z^n/n!^2$. Based on this lower bound and computations, Godin conjectured that

$$\lim_{n\to\infty} n^2\mathbb{P}(\text{ord}\,\pi = \text{ord}\,\pi') = K \tag{1.1}$$

for some constant K with $c_0 \leqslant K \leqslant 12$ (see [7, Conjecture 15]).

It follows from the Erdős–Turán limit law for $\log \text{ord}\,\pi$ that $\mathbb{P}(\text{ord}\,\pi = \text{ord}\,\pi') = o(1)$, but establishing any explicit rate of decay is already non-trivial. A crude bound was established in an earlier version of this paper and in the fifth author's thesis [16]. Briefly, using estimates for the probability that $\text{ord}\,\pi$ is coprime to a given integer, one can prove that with high probability there is a prime in the interval $[\log n, 2\log n]$ that divides exactly one of $\text{ord}\,\pi$ and $\text{ord}\,\pi'$. This argument leads to a bound of the form $O(\log\log n/\log n)$, but does not come close to Godin's conjecture.

We can contrast the effort involved in estimating the collision entropies of type π and $\text{ord}\,\pi$ even further. Suppose $k = o(n)$ and let $\lambda = \langle 1^{\lambda_1}, 2^{\lambda_2}, \ldots\rangle$ be a partition of k. Then

$$\mathbb{P}(\pi \text{ and } \pi' \text{ have type } \langle\lambda, n-k\rangle) = \frac{1}{(n-k)^2}\prod_{j\geqslant 1}\frac{1}{j^{2\lambda_j}(\lambda_j!)^2} \approx \frac{1}{n^2}\prod_{j\geqslant 1}\frac{1}{j^{2\lambda_j}(\lambda_j!)^2}. \tag{1.2}$$

Heuristically summing the rightmost approximation over all such k and λ yields a substantial partial sum of

$$\frac{1}{n^2}\sum_{k\geqslant 0}\sum_{\lambda\vdash k}\prod_{j\geqslant 1}\frac{1}{j^{2\lambda_j}(\lambda_j!)^2} = \frac{c_0}{n^2}, \tag{1.3}$$

where $\lambda \vdash k$ has the usual meaning that λ is a partition of k (*i.e.* a multiset of positive integers whose sum is k). This together with the analysis of [5] shows that the main contribution to $n^2\mathbb{P}(\text{type}\,\pi = \text{type}\,\pi')$ comes from pairs of permutations having a cycle of length $n - o(n)$. Motivated by this, one may ask whether at least $n^2\mathbb{P}(\text{ord}\,\pi = \text{ord}\,\pi' \wedge E)$ is bounded, where E is the event that π and π' each have a cycle of length at least $n - k(n)$, where $k(n)$ is some slowly growing function. This, however, is not the case.

In this paper we prove two main results. First we refute (1.1) by showing that

$$\limsup_{n\to\infty} n^2\mathbb{P}(\text{ord}\,\pi = \text{ord}\,\pi') = \infty.$$

Quantitatively, we show that there is a sequence $n_i \to \infty$ such that if π, π' are drawn independently from S_{n_i} then

$$\mathbb{P}(\text{ord}\,\pi = \text{ord}\,\pi') \geqslant \mathbb{P}(\text{ord}\,\pi = \text{ord}\,\pi = n_i - o(n_i)) \geqslant \frac{1}{2}n_i^{-2}\,\text{lg}^\star\, n_i,$$

where $\text{lg}^\star\, n$ is the height of the tallest tower of twos that does not exceed n. This precludes any heuristic similar to (1.2) and (1.3) from succeeding here. On the other hand we show that (1.1) is nearly true, in the sense that

$$\mathbb{P}(\text{ord}\,\pi = \text{ord}\,\pi') \leqslant n^{-2+o(1)}. \tag{1.4}$$

It would be interesting to estimate $\mathbb{P}(\text{ord}\,\pi = \text{ord}\,\pi')$ more precisely, but this appears to be a complicated question tied to arithmetic considerations about n.

https://doi.org/10.1017/S0963548321000043 Published online by Cambridge University Press

For a broader perspective, readers may be interested in the survey of Niemeyer, Praeger and Seress on the applications of probabilistic and enumerative techniques to the analysis of group-theoretic algorithms [12].

1.2 Analytic combinatorics

Analytic combinatorics relates the analytic behaviour of a generating function to the asymptotic behaviour of its coefficients. While the problem of estimating $\mathbb{P}(\text{type } \pi = \text{type } \pi')$ is well suited to the methods of analytic combinatorics, the same does not seem to be true of $\mathbb{P}(\text{ord } \pi = \text{ord } \pi')$. We offer some brief comments about why this may be.

Elementary combinatorial techniques are sufficient for enumerating the ordered pairs of conjugate permutations. As a result, the numbers $\mathbb{P}(\text{type } \pi = \text{type } \pi')$ are expressible as the coefficients of a well-behaved infinite product generating function closely related to the cycle index of the symmetric group (as explained in [5, Section 4.2].

In contrast consider $\mathbb{P}(\text{ord } \pi = \text{ord } \pi')$. For any fixed positive integer m, the exponential formula yields

$$F_m(x) = \sum_n \mathbb{P}(\text{ord } \pi \text{ divides } m)x^n = \exp\left(\sum_{d|m} \frac{x^d}{d}\right). \tag{1.5}$$

An application of Möbius inversion to (1.5) thus yields

$$G_m(x) = \sum_n \mathbb{P}(\text{ord } \pi = m)x^n = \sum_{d|m} \mu\left(\frac{m}{d}\right) F_d(x). \tag{1.6}$$

Using Möbius and Lagrange inversion, and the saddle-point method, Wilf [18] used (1.6) to derive an asymptotic formula for $\mathbb{P}(\text{ord } \pi = m)$ for *fixed* m, but as m grows Wilf's formula becomes more complicated and the asymptotics are less well understood. In the special case of $m = n$ there is a theorem of Warlimont [17] that

$$\mathbb{P}(\text{ord } \pi = n) = 1/n + O(1/n^2),$$

and this estimate has been extended by Niemeyer and Praeger [11] to various other values of m. A general understanding of $\mathbb{P}(\text{ord } \pi = m)$ is lacking, and indeed complicated for arithmetic reasons. As such, one cannot simply plug these asymptotic estimates into the sum $\sum_m \mathbb{P}(\text{ord } \pi = m)^2$ to answer Godin's question.

There is a rich literature about methods for extracting the coefficients of multivariate generating functions [13, 14]. Certainly we may define a bivariate generating function $H(x, y) = \sum_m G_m(x)G_m(y)$, and

$$\mathbb{P}(\text{ord } \pi = \text{ord } \pi') = [[x^n y^n]]H(x, y). \tag{1.7}$$

In some formal sense this is an answer, but we do not see any way to extract an asymptotic formula from (1.2).

Analytic combinatorics, by itself, is likely inadequate for attaining a thorough asymptotic analysis of the sequence $\mathbb{P}(\text{ord } \pi = m)$ because the order of a permutation depends on arithmetic data not easily extracted from the classical generating functions associated with permutations. Any hope for a purely symbolic calculus that can handle the sequence $\mathbb{P}(\text{ord } \pi = \text{ord } \pi')$ might hinge on techniques that are more in the realm of analytic number theory, such as a Mellin transform or a Dirichlet series generating function.

Another notable obstruction to a generating-function-based approach is the apparently erratic dependence of $\mathbb{P}(\text{ord } \pi = \text{ord } \pi')$ on n, which may be observed numerically. If the sequence $\mathbb{P}(\text{ord } \pi = \text{ord } \pi')$ were realized as the coefficients of a generating function, the behaviour of that function near its singularity would have to be similarly complicated.

https://doi.org/10.1017/S0963548321000043 Published online by Cambridge University Press

1.3 The anatomy of integers

In sharp relief to the beautiful formalism of analytic combinatorics, our proof of (1.1) is dirty and hands-on, and more closely connected with the 'anatomy of integers': see Granville [9] for an explanation of this term, and Ford [6] or the book of Hall and Tenenbaum [10] for a sense of the scope of the theory. We have mentioned already that $\log \operatorname{ord} \pi$ is asymptotically normal with mean $\log^2 n/2$ and variance $\log^3 n/3$, and that the largest cycles of π are distributed asymptotically according to the Poisson–Dirichlet law. By further analysing the distribution of the cycles of π, we show that apart from an exceptional event of probability $n^{-1+o(1)}$, including for instance the event that π is an n-cycle or an $(n-1)$-cycle, the integer $m = \operatorname{ord} \pi$ will have many large prime divisors, so many in fact that the collision probability $\mathbb{P}(\operatorname{ord} \pi' = m)$ is negligible. It follows that the probability that $\operatorname{ord} \pi = \operatorname{ord} \pi'$ is dominated by the event that π and π' are both exceptional.

2. Disproof of Godin's conjecture

The results in this section are based on the third author's `mathoverflow` post [15]. Define $\operatorname{Tow}(h)$ to be a tower of twos of height h, *i.e.* $\operatorname{Tow}(0) = 1$, and for $h > 0$, $\operatorname{Tow}(h) = 2^{\operatorname{Tow}(h-1)}$. Also define $\lg^\star n = \max\{h \colon \operatorname{Tow}(h) \leqslant n\}$.

Theorem 2.1. *For infinitely many positive integers n,*

$$\mathbb{P}(\operatorname{ord} \pi = \operatorname{ord} \pi') \geqslant \frac{\lg^\star n}{2n^2}.$$

Proof. For a positive integer n, let $K_n = \{k \colon 1 \leqslant k < n/2 \text{ and } k! \text{ divides } n-k\}$. If π has a cycle of length $n-k$, with $k \in K_n$, then all other cycles have length at most k. Since the lengths of these other cycles are at most k, they all divide $k!$, which in turn divides $n-k$ (by the definition of K_n). Therefore $\operatorname{ord} \pi = n-k$. The probability that π has a cycle of length $n-k$ is exactly $1/(n-k)$. Since $n-k > n/2$, these events are disjoint, since there cannot be more than one cycle of length greater than $n/2$. We therefore have

$$\mathbb{P}(\operatorname{ord} \pi = \operatorname{ord} \pi') \geqslant \sum_{k \in K_n} \frac{1}{(n-k)^2} \geqslant \frac{|K_n|}{n^2}.$$

Now consider the subsequence $(n_i)_{i \geqslant 1}$ defined by $n_1 = 3$ and $n_{i+1} = n_i + n_i!$ for $i \geqslant 1$. We will prove that the sets K_{n_i} are nested and that $|K_{n_i}| = i$ for all i. From the definition of K_n, it is easy to check that

- $K_{n_1} = \{1\}$;
- $n_i \notin K_{n_i}$;
- $k \in K_{n_i} \implies k \in K_{n_{i+1}}$, since if $k! \mid n_i - k$ and $k \leqslant n_i$ then also $k! \mid n_{i+1} - k$;
- $n_i \in K_{n_{i+1}}$, for the same reason.

Also note that

- $k \notin K_{n_{i+1}}$ for $k > n_i$ since $k!$ is too big to divide $n_{i+1} - k$;
- if $k < n_i$ and $k \in K_{n_{i+1}}$, then we already have $k \in K_{n_i}$, since $k < n_i \implies k! \mid n_i!$, which in turn implies $k! \mid n_i - k$.

We therefore have $K_{n_{i+1}} = K_{n_i} \cup \{n_i\}$ and $n_i \notin K_{n_i}$, so inductively

$$K_{n_i} = \{1, n_1, n_2, \ldots, n_{i-1}\}.$$

https://doi.org/10.1017/S0963548321000043 Published online by Cambridge University Press

This proves that $|K_{n_i}| = i$ for all i. Since $|K_{n_i}| \to \infty$ as $i \to \infty$, it is now clear that

$$\limsup_{n\to\infty} n^2 \mathbb{P}(\operatorname{ord}\pi = \operatorname{ord}\pi') = \infty.$$

To finish proving Theorem 2.1, we need to find a lower bound for i that is expressed in terms of n_i. Since $2^{n^2} \geqslant (n+1)! \geqslant n! + n$ for any positive integer n, we have

$$\lg^*(n_{i+1}) = \lg^*(n_i! + n_i) \leqslant \lg^*(2^{n_i^2}) = 1 + \lg^*(n_i^2) \leqslant 1 + \lg^*(2^{n_i}) = 2 + \lg^*(n_i).$$

It follows from induction on i that $\lg^*(n_i) \leqslant 2i$ or equivalently, $i \geqslant \lg^*(n_i)/2$. Hence

$$\frac{|K_{n_i}|}{n_i^2} = \frac{i}{n_i^2} \geqslant \frac{\lg^*(n_i)}{2n_i^2}.$$

3. Main proposition and proof sketch

Throughout let π be a random permutation of $[n]$. Our main result is the following.

Theorem 3.1. *There is a set $\mathcal{M}$ with the following properties.*

(1) If $m \notin \mathcal{M}$ then $\mathbb{P}(\operatorname{ord}\pi = m) = O(n^{-100})$.
(2) $\mathbb{P}(\operatorname{ord}\pi \in \mathcal{M}) \leqslant n^{-1+o(1)}$.

Although the proof of Theorem 3.1 is postponed, we can immediately deduce a non-trivial upper bound for the probability that two random permutations have the same order.

Corollary 3.1. $\mathbb{P}(\operatorname{ord}\pi = \operatorname{ord}\pi') \leqslant n^{-2+o(1)}$.

Proof. By considering whether the collision occurs in $\mathcal{M}$ or $\mathcal{M}^c$, we have

$$\begin{aligned}\mathbb{P}(\operatorname{ord}\pi = \operatorname{ord}\pi') &\leqslant \mathbb{P}(\operatorname{ord}\pi \in \mathcal{M})^2 + \sum_{m\notin\mathcal{M}} \mathbb{P}(\operatorname{ord}\pi = m)^2 \\ &\leqslant \mathbb{P}(\operatorname{ord}\pi \in \mathcal{M})^2 + \max_{m\notin\mathcal{M}} \mathbb{P}(\operatorname{ord}\pi = m).\end{aligned}$$

The first term is bounded by $n^{-2+o(1)}$ and the second term is bounded by $O(n^{-100})$. □

For the proof of Theorem 3.1, we construct a specific example of such a set $\mathcal{M}$. For the remainder of this paper, let $\delta = \delta(n) = 1/\log\log\log n$, and let $\eta = e^{-10/\delta} = 1/(\log\log n)^{10}$, though the specific choice is largely irrelevant: all we require is that δ and η decay sufficiently slowly, with δ decaying much more slowly than η. Let $\mathcal{M}$ be the set of all positive integers m having at most $\delta \log n$ distinct prime divisors $p > n^\eta$.

Let us now informally sketch the proof of Theorem 3.1 (some readers may prefer to skip ahead to the next section for the rigorous proofs). It suffices to consider the case where π has $k \geqslant 2\delta \log n$ cycles, because all except $n^{-1+o(1)}$ permutations have this property (recall $\delta = o(1)$). These k cycles will be drawn at random from $\{1, \dots, n\}$ according to a harmonic weighting (conditional on their sum being n). Using Mertens' third theorem to bound the harmonic weight of the set of n^η-smooth numbers, we expect at least half of our $2\delta \log n$ cycles to fail to be n^η-smooth. Therefore we expect $\operatorname{ord}\pi$ to be divisible by some $\delta \log n$ primes $p > n^\eta$, proving part (2) of Theorem 3.1. The proof of part (1) is easier, and follows from a simple union bound over all the ways that the cycles of π might be divisible by the primes dividing m.

https://doi.org/10.1017/S0963548321000043 Published online by Cambridge University Press

4. Proof of Theorem 3.1, part (2)

Write $Z = Z(\pi)$ for the number of cycles in a random $\pi \in S_n$. It is well known that $Z - 1$ is approximately Poisson with parameter $\log n$. (See, for example, the final section of [2] for tail bounds.) The following lemma's quantitative formulation is particularly convenient for us.

Lemma 4.1. *Let $n, k \geqslant 1$, and let $\pi \in S_n$ be random. Then*

$$\mathbb{P}(Z(\pi) = k) \leqslant \frac{1}{n} \frac{h_n^{k-1}}{(k-1)!},$$

where $h_n = \sum_{j=1}^{n} 1/j$.

Proof. Write $p_{n,k}$ for $\mathbb{P}(Z(\pi) = k)$. From Cauchy's formula for the number of permutations in a conjugacy class, we have

$$p_{n,k} = \sum \frac{1}{c_1! \cdots c_n! 1^{c_1} \cdots n^{c_n}},$$

where the sum ranges over all $c_1, \ldots, c_n \geqslant 0$ such that $\sum_{i=1}^{n} c_i = k$ and $\sum_{i=1}^{n} i c_i = n$. We can 'smooth this out' by using

$$p_{n,k} = \frac{1}{n} \sum_{j=1}^{n} p_{n-j,k-1},$$

which follows from conditioning on the length of one of the cycles of π. Thus we have

$$\begin{aligned} p_{n,k} &= \frac{1}{n} \sum_{j=1}^{n} \sum_{\substack{\sum c_i = k-1 \\ \sum i c_i = n-j}} \frac{1}{c_1! \cdots c_n! 1^{c_1} \cdots n^{c_n}} \\ &\leqslant \frac{1}{n} \sum_{\sum c_i = k-1} \frac{1}{c_1! \cdots c_n! 1^{c_1} \cdots n^{c_n}} \\ &= \frac{1}{n} \frac{h_n^{k-1}}{(k-1)!}. \end{aligned}$$

The last line is an application of the multinomial theorem. □

Using Stirling's formula, and monotonicity of the bound

$$\frac{1}{n} \frac{h_n^{k-1}}{(k-1)!}$$

as a function of k, we can prove the following corollary.

Corollary 4.2. *The probability that π has $o(\log n)$ cycles is $n^{-1+o(1)}$, and the probability that π has more than $10 \log n$ cycles is $O(n^{-14})$.*

Proof. Let $\xi = h_n/\omega$, where $\omega = \omega(n) \to \infty$. By calculating the ratios of successive terms, one can verify that the bound

$$\frac{1}{n} \frac{h_n^{k-1}}{(k-1)!}$$

https://doi.org/10.1017/S0963548321000043 Published online by Cambridge University Press

is increasing as a function of k when $k \leqslant \xi + 1$. Thus

$$\mathbb{P}(Z \leqslant \xi + 1) \leqslant (\xi + 1)\frac{1}{n}\frac{h_n^{\xi}}{(\xi+1)!} \leqslant \frac{1}{n}(e\omega)^{\xi} = n^{-1+o(1)}.$$

Similarly, when $k > 10h_n$, the bound is decreasing as a function of k. In this range, a crude version of Stirling's formula yields

$$\frac{h_n^{k-1}}{k!} \leqslant \left(\frac{eh_n}{k}\right)^k \leqslant \left(\frac{e}{10}\right)^k.$$

Therefore

$$\mathbb{P}(Z \geqslant 10\log n) \leqslant \frac{1}{n}\sum_{k \geqslant 10h_n}\left(\frac{e}{10}\right)^k = O\left(n^{10\log(e/10)-1}\right). \qquad \square$$

We use only Corollary 4.2 in the proof, but a similar argument establishes that, for fixed positive ε, the probability that π has more than $(1+\varepsilon)\log n$ cycles is bounded by $n^{-f(\varepsilon)+o(1)}$, where $f(\varepsilon) = (1+\varepsilon)\log(1+\varepsilon) - \varepsilon$.

Lemma 4.3. *Let $A_1, \dots, A_Z$ be the cycle lengths of π in a random order. Then, for any $k \geqslant 0$ and any k-tuple $(a_1, \dots, a_k)$ of positive integers such that $a_1 + \cdots + a_k = n$, we have*

$$\mathbb{P}(Z = k, A_1 = a_1, \dots, A_k = a_k) = \frac{1}{k!}\frac{1}{a_1 \cdots a_k}.$$

Proof. Let the multiplicities among $a_1, \dots, a_k$ be $m_1, \dots, m_s$ (so that $\sum_i m_i = k$). Then by Cauchy's formula the probability that this cycle type arises is

$$\frac{1}{m_1! \cdots m_s! a_1 \cdots a_k}.$$

When these cycles are ordered randomly, the probability that we get $a_1, \dots, a_k$ in order is

$$\binom{k}{m_1 \ \cdots \ m_k}^{-1}.$$

The result follows from multiplying the previous two displays. $\square$

The combined message of the previous two lemmas is that we may assume π has between $\delta \log n$ and $10 \log n$ cycles (for any slowly decaying δ), while, conditional on k, these cycles are distributed roughly independently according to a harmonic weighting.

For any set S of integers, let us call $h_S = \sum_{j \in S} 1/j$ the *harmonic weight* of S. If P is any set of prime numbers, a positive integer n is P-smooth if and only if all prime divisors of n are elements of P.

Lemma 4.4. *Let $N \geqslant 1$. Let P be the set of all primes $p \leqslant N$, as well as some $o(N)$ further primes. Then the harmonic weight of the set of P-smooth numbers is*

$$(1 + o(1))e^{\gamma}\log N,$$

where γ is the Euler–Mascheroni constant.

Proof. The harmonic weight of the set of P-smooth numbers is

$$\prod_{p \in P}(1 - 1/p)^{-1}.$$

https://doi.org/10.1017/S0963548321000043 Published online by Cambridge University Press

By Mertens' third theorem we have

$$\prod_{p\leqslant N}(1-1/p)^{-1}\sim e^{\gamma}\log N.$$

On the other hand we have

$$\prod_{p\in P, p>N}(1-1/p)^{-1}=\exp\sum_{p\in P, p>N}O(1/p)=e^{o(1)}. \qquad \square$$

Recall that $\delta=1/\log\log\log n$, and $\eta=e^{-10/\delta}=1/(\log\log n)^{10}$. With this choice of δ and η we have the following proposition.

Proposition 4.5. *Let π be drawn from S_n uniformly at random. Then, apart from an event of probability $n^{-1+o(1)}$, π has at least $\delta\log n$ cycles and* ord π *is divisible by at least $\delta\log n$ primes $p>n^{\eta}$.*

Proof. Let $A_1,\dots,A_Z$ be the cycle lengths of π in a random order. By Lemma 4.3, provided that $a_1+\cdots+a_k=n$ we have

$$\mathbb{P}(Z=k, A_1=a_1,\dots,A_k=a_k)=\frac{1}{k!}\frac{1}{a_1\cdots a_k}.$$

Define sets of primes P_i as follows.

(1) Let P_0 be the set of all primes $p\leqslant n^{\eta}$.
(2) For $0<i\leqslant k$, if A_i is P_{i-1}-smooth, put $P_i=P_{i-1}$. Otherwise pick a prime $p_i\notin P_{i-1}$ dividing A_i (the smallest such, say), and let $P_i=P_{i-1}\cup\{p_i\}$.

Each set P_i contains at most k primes $p>n^{\eta}$, so as long as $k=o(n^{\eta})$ Lemma 4.4 implies that the set of P_i-smooth numbers has harmonic weight at most $2\eta h_n$.

Let I be the set of indices $i\in\{1,\dots,k\}$ such that A_i is P_{i-1}-smooth (and hence $P_i=P_{i-1}$). Assuming $k\geqslant 2\delta\log n$, if $|I|\leqslant k/2$ then we find that P_k contains at least $\delta\log n$ distinct primes $p>n^{\eta}$, as desired. We will bound the probability that $|I|>k/2$.

Let E_k be the event that π has k cycles and $|I|>k/2$. Then, assuming $2\delta\log n\leqslant k\leqslant 10\log n$,

$$\begin{aligned}
\mathbb{P}(E_k)&=\sum_{I_0:\,|I_0|>k/2}\mathbb{P}(Z(\pi)=k \text{ and } I=I_0)\\
&=\sum_{I_0:\,|I_0|>k/2}\sum_{\substack{a_1,\dots,a_k\geqslant 1\\ a_1+\cdots+a_k=n}}\frac{1}{k!}\frac{1_{a_i \text{is} P_{i-1}-\text{smooth for each } i\in I_0}}{a_1\cdots a_k}\\
&\leqslant\sum_{I_0:\,|I_0|>k/2}\frac{1}{k!}h_n^{k-|I_0|}(2\eta h_n)^{|I_0|}\\
&\leqslant\frac{h_n^k}{k!}2^k(2\eta)^{k/2}\\
&\leqslant\frac{h_n^k}{k!}(8\eta)^{\delta\log n}\\
&\leqslant\frac{h_n^k}{k!}n^{-10+o(1)}.
\end{aligned}$$

https://doi.org/10.1017/S0963548321000043 Published online by Cambridge University Press

Hence

$$\mathbb{P}\left(\bigcup_{2\delta \log n \leqslant k \leqslant 10 \log n} E_k\right) \leqslant e^{h_n} n^{-10+o(1)} = n^{-9+o(1)}.$$

On the other hand, by Corollary 4.2 the probability that π has either fewer than $2\delta \log n$ cycles or more than $10 \log n$ cycles is bounded by $n^{-1+o(1)}$. This proves the lemma. □

This finishes the proof of part (2) of Theorem 3.1.

5. Proof of Theorem 3.1, part (1)

Recall that $\delta = 1/\log\log\log n$, and $\eta = e^{-10/\delta} = 1/(\log\log n)^{10}$.

Lemma 5.1. *Let m be an integer having at least $\delta \log n$ prime divisors $p > n^{\eta}$. Then*

$$\mathbb{P}(\operatorname{ord} \pi = m) \leqslant e^{-c\delta\eta \log^2 n}.$$

Proof. Recall that the cycle lengths of a random permutation can be sampled using the following process. Start by picking a_1 uniformly from $\{1, \dots, n\}$. If $a_1 < n$, pick a_2 uniformly from $\{1, \dots, n - a_1\}$, *etc.* The process continues until $a_1 + \cdots + a_k = n$.

Fix a set P of $\lceil \delta \log n \rceil$ prime divisors $p > n^{\eta}$ of m. Now sample $\pi \in S_n$ using the process just described. For each fixed i and p, the probability that a_i is divisible by p is at most $1/p$, independently of the previous steps in the process. In fact, for any set of primes $p_1, \dots, p_t \in P$, the probability that a_i is divisible by each of $p_1, \dots, p_t$ is at most $1/(p_1 \cdots p_t)$. On the other hand, in order that $\operatorname{ord} \pi = m$, for each $p \in P$ there must be an index i such that a_i is divisible by P.

The event that π has more than $(\log n)^3$ cycles is negligible (it has probability $o(e^{-c(\log n)^3})$). On the other hand, the probability that π has at most $(\log n)^3$ cycles and that for each $p \in P$ there is some i such that a_i is divisible by p is bounded by

$$\begin{aligned}((\log n)^3)^{|P|} \cdot \prod_{p \in P} 1/p &\leqslant (\log n)^{O(\log n)} (n^{-\eta})^{\delta \log n} \\ &\leqslant e^{-c\delta\eta \log^2 n}.\end{aligned}$$

This finishes the proof of Theorem 3.1. □

6. Conclusion

While we have established that $\mathbb{P}(\operatorname{ord} \pi = \operatorname{ord} \pi')$ is generically larger than $O(1/n^2)$ but no larger than $n^{-2+o(1)}$, its exact order of magnitude remains mysterious and appears to be linked with arithmetical properties of n, as in the proof of Theorem 2.1. Establishing more precise estimates should be of interest to anyone who considers themself to be a problem-solver (in the sense of Gowers' essay [8]), just because it is an easily stated problem that is not readily solved. We list here a few related observations and open questions.

(1) What is the lim inf of $n^2\mathbb{P}(\operatorname{ord} \pi = \operatorname{ord} \pi')$ as n tends to infinity? The integers n constructed by Theorem 2.1 have a particular arithmetic form. What is the behaviour for n of the form $k! + 1$?

https://doi.org/10.1017/S0963548321000043 Published online by Cambridge University Press

(2) What is $\max_m \mathbb{P}(\operatorname{ord}\pi = m)$, and for what value(s) of m is it attained? Theorem 3.1 gives an upper bound of $n^{-1+o(1)}$ for this probability. Clearly the max is at least $1/n$, since π is an n-cycle with probability $1/n$. In fact the max is at least $1/(n-1)$, for the same reason but with $(n-1)$-cycles. The answer may be close to this, but we saw in the proof of Theorem 2.1 that

$$\mathbb{P}(\operatorname{ord}\pi = n-k) \geqslant 1/(n-k)$$

for any $k \in K_n$, so the maximum can be larger. This problem was mentioned by Erdős and Turán in [4].

(3) Let π_n be a random element of S_n. The quantity $\mathbb{P}(\operatorname{ord}\pi_n = m)$ as a function of m and n can be very sensitive to the value of n. For example, if n is prime then $\mathbb{P}(\operatorname{ord}\pi_n = n) = 1/n$ but $\mathbb{P}(\operatorname{ord}\pi_{n-1} = n) = 0$.

(4) As a generalization of Godin's problem, one might consider symmetric groups of different sizes. Consider random permutations $(\pi_1, \pi_2) \in S_{n_1} \times S_{n_2}$, and estimate the probability they have the same order. An upper bound is immediate from Corollary 3.1 and the Cauchy–Schwarz inequality:

$$\begin{aligned}\mathbb{P}(\operatorname{ord}\pi_1 = \operatorname{ord}\pi_2) &= \sum_m \mathbb{P}(\operatorname{ord}\pi_1 = m)\mathbb{P}(\operatorname{ord}\pi_2 = m)\\ &\leqslant \mathbb{P}(\operatorname{ord}\pi_1 = \operatorname{ord}\pi_1')^{1/2}\mathbb{P}(\operatorname{ord}\pi_2 = \operatorname{ord}\pi_2')^{1/2}\\ &\leqslant n_1^{-1+o(1)} n_2^{-1+o(1)}.\end{aligned}$$

References

[1] Arratia, R., Barbour, A. D. and Tavaré, S. (2003) *Logarithmic Combinatorial Structures: A Probabilistic Approach*, EMS Monographs in Mathematics. European Mathematical Society (EMS).

[2] Devroye, L. (1988) Applications of the theory of records in the study of random trees. *Acta Inform.* **26** 123–130.

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

[4] Erdős, P. and Turán, P. (1968) On some problems of a statistical group-theory, IV. *Acta Math. Acad. Sci. Hungar.* **19** 413–435.

[5] Flajolet, P., Fusy, E., Gourdon, X., Panario, D. and Pouyanne, N. (2006) A hybrid of Darboux's method and singularity analysis in combinatorial asymptotics. *Electron. J. Combin.* **13** R103.

[6] Ford, K. Anatomy of integers and random permutations course lecture notes. https://faculty.math.illinois.edu/~ford/Anatomy_lectnotes.pdf

[7] Godin, T. (2017) An analogue to Dixon's theorem for automaton groups. In *2017 Proceedings of the Fourteenth Workshop on Analytic Algorithmics and Combinatorics (ANALCO)*, pp. 164–173. SIAM.

[8] Gowers, W. T. (2000) The two cultures of mathematics. In *Mathematics: Frontiers and Perspectives* (V. Arnold *et al.*, eds), pp. 65–78. AMS.

[9] Granville, A. The anatomy of integers and permutations. https://www.dms.umontreal.ca/~andrew/MSI/AnatomyForTheBook.pdf

[10] Hall, R. R. and Tenenbaum, G. (1988) *Divisors*, Vol. 90 of Cambridge Tracts in Mathematics. Cambridge University Press.

[11] Niemeyer, A. C. and Praeger, C. E. (2007) On permutations of order dividing a given integer. *J. Algebraic Combin.* **26** 125–142.

[12] Niemeyer, A. C., Praeger, C. E. and Seress, A. (2013) Estimation problems and randomised group algorithms. In *Probabilistic Group Theory, Combinatorics, and Computing*, Vol. 2070 of Lecture Notes in Mathematics, pp. 35–82. Springer.

[13] Pemantle, R. and Wilson, M. C. (2013) *Analytic Combinatorics in Several Variables*, Vol. 140 of Cambridge Studies in Advanced Mathematics. Cambridge University Press.

[14] Raichev, A. (2011) New software for computing asymptotics of multivariate generating functions. *ACM Commun. Comput. Algebra* **45** 183–185.

https://doi.org/10.1017/S0963548321000043 Published online by Cambridge University Press

[15] Thibo (2016) 'What is the probability that two random permutations have the same order?', `mathoverflow`. http://mathoverflow.net/a/230276
[16] Thomas, J. (2020) Three problems in the asymptotic order of group elements. PhD thesis, Drexel University.
[17] Warlimont, R. (1978) Über die Anzahl der Lösungen von $x^n = 1$ in der symmetrischen Gruppe S_n. *Arch. Math. (Basel)* **30** 591–594.
[18] Wilf, H. S. (1986) The asymptotics of $e^{P(z)}$ and the number of elements of each order in S_n. *Bull. Amer. Math. Soc. (N.S.)* **15** 228–232.

Cite this article: Acan H, Burnette C, Eberhard S, Schmutz E and Thomas J (2021). Permutations with equal orders. *Combinatorics, Probability and Computing* **30**, 800–810. https://doi.org/10.1017/S0963548321000043