

The most probable order of a random permutation

Adrian Beker*

October 14, 2025

Abstract

Given positive integers n and m , let $p_n(m)$ be the probability that a uniform random permutation of $[n]$ has order exactly m . We show that, as $n \rightarrow \infty$, the maximum of $p_n(m)$ over all m is asymptotic to $1/n$, the probability of an n -cycle. Furthermore, for sufficiently large n , we show that the maximum is attained precisely if m is the least positive integer divisible by all positive integers less than or equal to $n - m$. This answers a question of Acan, Burnette, Eberhard, Schmutz and Thomas, originally attributed to work of Erdős and Turán from 1968.

1 Introduction

Let π_n be a permutation chosen uniformly at random from S_n , the symmetric group on n letters. Let $\text{ord}(\pi_n)$ denote the order of π_n , which can be computed as the least common multiple of the lengths of its cycles. Understanding the distribution of $\text{ord}(\pi_n)$ is a fundamental problem in probabilistic group theory. Its study goes back more than a hundred years to the work of Landau [9], which established that the maximum of its support, now known as Landau's function, is of the form $e^{(1+o(1))\sqrt{n \log n}}$. Later on, a rather systematic treatment of this subject was undertaken by Erdős and Turán. In a series of works starting in the 1960s, they established a number of results concerning the distribution of (the logarithm of) $\text{ord}(\pi_n)$, including a weak law of large numbers [3], a central limit theorem [5] and a log-asymptotic for the size of the support [6]. For a more complete account of the literature on this and related topics, we recommend the reference [8].

While the macroscopic behaviour of $\text{ord}(\pi_n)$ is by now fairly well understood, obtaining local limit results has proved considerably more challenging. In this direction, Acan, Burnette, Eberhard, Schmutz and Thomas [1] recently studied the so-called collision entropy of $\text{ord}(\pi_n)$. Letting π'_n be an independent copy of π_n , they were interested in estimating the probability that $\text{ord}(\pi_n)$ equals $\text{ord}(\pi'_n)$. They proved that, somewhat surprisingly, this quantity is not $O(1/n^2)$, the lower bound coming from the event that π_n and π'_n are both n -cycles (see also [2]). They also established the corresponding upper bound

$$\mathbb{P}(\text{ord}(\pi_n) = \text{ord}(\pi'_n)) \leq n^{-2+o(1)}. \quad (1)$$

Writing p_n for the probability mass function of $\text{ord}(\pi_n)$, i.e. $p_n(m) := \mathbb{P}(\text{ord}(\pi_n) = m)$ for $m \in \mathbb{N}$, this can be recast as a statement about the ℓ^2 -norm of p_n , namely $\|p_n\|_{\ell^2(\mathbb{N})} \leq n^{-1+o(1)}$.

Motivated by a question of Erdős and Turán [6, p. 414], also reiterated by Acan et al. [1, §6], we are instead interested in the maximum probability that $\text{ord}(\pi_n)$ equals a particular value. Writing $M(n) := \|p_n\|_{\ell^\infty(\mathbb{N})}$ for this quantity, one readily observes that

$$M(n) \geq p_n(n) \geq \mathbb{P}(\pi_n \text{ is an } n\text{-cycle}) = 1/n. \quad (2)$$

In the other direction, since $\|p_n\|_{\ell^\infty(\mathbb{N})} \leq \|p_n\|_{\ell^2(\mathbb{N})}$, the results of [1] imply a bound of the form

$$M(n) \leq n^{-1+o(1)}. \quad (3)$$

*University of Zagreb, Faculty of Science, Department of Mathematics, Zagreb, Croatia. Email: `adrian.beker@math.hr`

Our goal is to obtain sharper bounds on $M(n)$. To this end, it will be useful to recall the following setup from [2]. We define

$$K_n := \{k \in \{0, 1, \dots, n-1\} \mid \text{lcm}(1, 2, \dots, k) \mid n-k\}$$

and note the key property that for $k \in K_n$, the existence of a cycle of length $n-k$ in π_n guarantees that $\text{ord}(\pi_n) = n-k$. Note also that K_n always contains $\{0, 1\}$ and the prime number theorem implies that $\max K_n \ll \log n$. In particular, if n is large enough, then π_n can only contain one cycle of length $n-k$ with $k \in K_n$, and this happens with probability exactly $1/(n-k)$.

Our first result can be regarded as an anticoncentration estimate for $\text{ord}(\pi_n)$ confirming that the lower bound (2) on $M(n)$ is asymptotically tight. As a byproduct, we also obtain a structural description of those m for which $p_n(m)$ is close to its maximum value.

Theorem 1.1. *We have the asymptotic $M(n) \sim 1/n$. Moreover, if n is sufficiently large, then any m such that $p_n(m) \geq 1/n$ is of the form $n-k$ for some $k \in K_n$.*

The second result identifies the mode of the distribution of $\text{ord}(\pi_n)$, i.e. the value of m for which $p_n(m)$ attains its maximum, at least when n is large enough. Together with Theorem 1.1, this gives an essentially complete answer to the questions raised Erdős and Turán and Acan et al.

Theorem 1.2. *For all sufficiently large n , we have $p_n(m) = M(n)$ if and only if $m = n - \max K_n$.*

Remark 1.3. In principle, one could extract from our arguments a bound on how large n needs to be for the above results to hold. However, what one gets is most probably not small enough in order to check the remaining cases by a naive method. Nevertheless, one cannot entirely drop the assumption that n is sufficiently large since numerical evidence shows that counterexamples do exist for small values n .

In order to prove Theorem 1.1, the idea is to consider the joint distribution of the order and the number of cycles, and apply different local limit laws according to whether the number of cycles is large, intermediate or small. In doing so, a key difficulty is avoiding the use of lower tail bounds for the number of cycles – such an approach is unlikely to produce a bound better than (3). Nevertheless, after making certain refinements, we are able to make use of some of the methods of [1]. To establish Theorem 1.2, it remains to prove a local limit law confirming the prediction that $\mathbb{P}(\text{ord}(\pi_n) = n-k)$ equals $1/(n-k)$ up to a suitably small error. This can be accomplished by adapting some of the existing results in the literature pertaining to the case $k = 0$.

The rest of the paper is organised as follows. In Section 2, we collect some preliminary facts about the distribution of the cycle type of π_n that we will need. Section 3 is devoted to the proof of Theorem 1.1. Finally, in Section 4, we present the proof of Theorem 1.2.

Notation. We use Vinogradov asymptotic notation. Given quantities A and B , we write $A \ll B$ to mean $A \leq O(B)$, that is to say there is an absolute constant $C > 0$ such that $|A| \leq C|B|$. This is equivalent to the notation $B \gg A$, i.e. $B \geq \Omega(A)$. For functions $f, g: \mathbb{N} \rightarrow \mathbb{R}$, we write $f(n) = o(g(n))$ and $f(n) \sim g(n)$ to mean that $\lim_{n \rightarrow \infty} f(n)/g(n) = 0$ and $\lim_{n \rightarrow \infty} f(n)/g(n) = 1$ respectively.

2 Preliminaries

It will be useful to recall that the cycle type of a random permutation can be sampled as follows. Given a positive integer n , consider the Markov chain $(X_j^{(n)})_{j \geq 0}$ with state space $\mathbb{N}_0$, initial distribution $\mathbb{P}(X_0^{(n)} = n) = 1$ and transition probabilities

$$\mathbb{P}(X_{j+1}^{(n)} = u \mid X_j^{(n)} = v) = \begin{cases} \frac{1}{v} & \text{if } u < v \\ 1 & \text{if } u = v = 0 \\ 0 & \text{otherwise} \end{cases}.$$

Letting $T^{(n)} := \min\{j \geq 0 \mid X_j^{(n)} = 0\}$ be the time of hitting 0, we have the following well-known fact (see e.g. [7, p. 257-258]).

Fact 2.1. *The cycle type of π_n has the same distribution as the multiset*

$$\{X_j^{(n)} - X_{j+1}^{(n)} \mid 0 \leq j < T^{(n)}\}.$$

In particular, $\text{ord}(\pi_n)$ has the same distribution as $\text{lcm}\{X_j^{(n)} - X_{j+1}^{(n)} \mid 0 \leq j < T^{(n)}\}$.

Conditioning on the first step of $(X_j^{(n)})_{j \geq 0}$, we obtain the following recursive expression for $p_n(m)$. Here and throughout, we use the standard notation $\tau(m)$, $\sigma(m)$ and $\omega(m)$ for the number, sum of positive divisors and the number of prime factors of m , respectively. We also recall the well-known fact that $\tau(m) \leq m^{o(1)}$ (see e.g. Theorem 2 in Chapter I.5 of [10]), which will be used several times in the paper.

Corollary 2.2. *For any $m, n \in \mathbb{N}$ we have*

$$\mathbb{P}(\text{ord}(\pi_n) = m) = \frac{1}{n} \sum_{\substack{0 \leq n' < n \\ n - n' \mid m}} \mathbb{P}(\text{lcm}(\text{ord}(\pi_{n'}), n - n') = m).$$

In particular, for any $m, n \in \mathbb{N}$ we have

$$\mathbb{P}(\text{ord}(\pi_n) \mid m) \leq \frac{\tau(m)}{n}.$$

We now turn to a lemma that will serve as a key tool in the proof of Theorem 1.1. Before stating it, we quickly set up some terminology. For a permutation $\pi \in S_n$, we define $c(\pi)$ to be the number of cycles in π . For an arbitrary set $I \subseteq \mathbb{N}$, we say π is *I-restricted* if the length of each cycle in π belongs to I .

Lemma 2.3. *For any $\ell, n \in \mathbb{N}$ and $I \subseteq \mathbb{N}$ we have*

$$\mathbb{P}(c(\pi_n) = \ell, \pi_n \text{ is } I\text{-restricted}) \leq \frac{\left(\sum_{i \in I} 1/i\right)^{\ell-1}}{n(\ell-1)!}.$$

Lemma 2.3 is a special case of [8, Theorem 1.5], a more general local limit law for counts of cycle lengths in disjoint sets – it follows by taking $r = 2$, $(I_1, I_2) = (I, [n] \setminus I)$ and $(m_1, m_2) = (\ell, 0)$. At the same time, it can be obtained by a straightforward generalisation of the argument behind [1, Lemma 4.1], which corresponds to the case $I = [n]$.

Taking I to be the set of divisors of a given positive integer m , we obtain the following corollary, which is effective when ℓ is not too small and m is not exceedingly large.

Corollary 2.4. *For any $\ell, m, n \in \mathbb{N}$ we have*

$$\mathbb{P}(c(\pi_n) = \ell, \text{ord}(\pi_n) \mid m) \leq \frac{1}{n(\ell-1)!} \left(\frac{\sigma(m)}{m}\right)^{\ell-1}.$$

Finally, we require the following lemma, which will be useful in the regime when the number of cycles is significantly below its expected value and the order is somewhat large. It is based on Fact 2.1 and can essentially be read out of the proof of [1, Lemma 5.1].

Lemma 2.5. *For any $\ell, m, n \in \mathbb{N}$ we have*

$$\mathbb{P}(c(\pi_n) = \ell, m \mid \text{ord}(\pi_n)) \leq \frac{\ell^{\omega(m)}}{m},$$

where $\omega(m)$ is the number of distinct prime factors of m .

Proof sketch. Let $m = \prod_{i=1}^{\omega(m)} p_i^{\alpha_i}$ be the prime factorisation of m . Then m divides the order if and only if for each $i \in [\omega(m)]$ there exists a cycle of length divisible by $p_i^{\alpha_i}$. Provided the number of cycles is ℓ , there are $\ell^{\omega(m)}$ ways to assign a cycle to each prime factor. For any such assignment, the probability of the corresponding divisibility conditions being satisfied does not exceed $1/m$. Indeed, the Markov property implies that, conditional on any earlier divisibility constraints, the probability that the length of a cycle is divisible by all prime powers to which it is assigned is at most the reciprocal of their product. The desired conclusion now follows from the union bound. $\square$

3 Proof of Theorem 1.1

The following proposition is the main stepping stone towards Theorem 1.1. Roughly speaking, it says that one can restrict attention to values of the order that are not much larger than n .

Proposition 3.1. *For any $\varepsilon > 0$, we have*

$$\max_{m \geq n^{1+\varepsilon}} p_n(m) = o(1/n).$$

Proof. Fix $\varepsilon > 0$, let n be sufficiently large in terms of ε and suppose that $m \geq n^{1+\varepsilon}$. The event that π_n has order m can be decomposed into the following three events according to the number of cycles in π_n :

$$E_1 := \{c(\pi_n) \leq C_1 \log \log n, \text{ ord}(\pi_n) = m\},$$

$$E_2 := \{C_1 \log \log n < c(\pi_n) \leq C_2 \log n, \text{ ord}(\pi_n) = m\},$$

$$E_3 := \{c(\pi_n) > C_2 \log n, \text{ ord}(\pi_n) = m\},$$

where $C_1, C_2 > 0$ are sufficiently large absolute constants. We estimate the probabilities of these events in turn. First, the upper tail bound for the number of cycles (see e.g. [1, Corollary 4.2]) gives

$$\mathbb{P}(E_3) \leq \mathbb{P}(c(\pi_n) > C_2 \log n) = o(1/n)$$

provided C_2 is large enough. Next, since the order of a permutation is at most the product of the lengths of its cycles, we have $\text{ord}(\pi_n) \leq n^{c(\pi_n)}$. Thus, if $m > n^{C_2 \log n}$, then $\mathbb{P}(E_2) = 0$. Otherwise, employing the standard estimate $\sigma(m) \ll m \log \log m$ (see e.g. Theorem 5 in Chapter I.5 of [10]), we obtain $\sigma(m)/m \leq C \log \log n$ for some absolute constant $C > 0$. Hence, using Corollary 2.4 and the estimate $k! \geq (k/e)^k$, we obtain

$$\mathbb{P}(E_2) = \sum_{C_1 \log \log n < \ell \leq C_2 \log n} \mathbb{P}(c(\pi_n) = \ell, \text{ ord}(\pi_n) = m) \leq C_2 \log n \cdot \frac{1}{n} \left(\frac{2Ce}{C_1} \right)^{\frac{1}{2} C_1 \log \log n} = o(1/n)$$

provided C_1 is large enough. Finally, by Lemma 2.5 and the standard estimate $\omega(m) \ll \frac{\log m}{\log \log m}$ (see e.g. Theorem 3 in Chapter I.5 of [10]), for any $\ell \leq C_1 \log \log n$ we have

$$\mathbb{P}(c(\pi_n) = \ell, \text{ ord}(\pi_n) = m) \leq \exp \left(O \left(\frac{\log m}{\log \log n} \cdot \log \log \log n \right) - \log m \right) \leq \frac{1}{n^{1+\varepsilon/2}}.$$

By summing over all ℓ in this range, it follows that

$$\mathbb{P}(E_1) = \sum_{\ell \leq C_1 \log \log n} \mathbb{P}(c(\pi_n) = \ell, \text{ ord}(\pi_n) = m) \leq \frac{C_1 \log \log n}{n^{1+\varepsilon/2}} = o(1/n),$$

which concludes the proof. $\square$

Remark 3.2. Following similar lines as above, one can give a somewhat shorter proof of (1) than in [1]. Indeed, by an argument analogous to the estimation of the probabilities of the events E_2 and E_3 , one can obtain

$$\mathbb{P}(c(\pi_n) \geq L, \text{ord}(\pi_n) = m) \leq o(1/n^2), \quad (4)$$

where $m \in \mathbb{N}$ is arbitrary and we set $L := C \log n / \log \log n$ for some large constant $C > 0$. Hence, by dividing into cases according to the number of cycles in π_n and π'_n , one can bound the left-hand side of (1) by

$$\mathbb{P}(\text{ord}(\pi_n) = \text{ord}(\pi'_n), c(\pi_n), c(\pi'_n) \leq L) + 2\mathbb{P}(\text{ord}(\pi_n) = \text{ord}(\pi'_n), c(\pi_n) \geq L).$$

By conditioning on the order of π'_n and using (4), the second term can be seen to be $o(n^{-2})$. On the other hand, the lower tail bound for the number of cycles [1, Corollary 4.2] implies that the first term is at most

$$\mathbb{P}(c(\pi_n) \leq L)^2 \leq n^{-2+o(1)},$$

whence (1) follows.

We are now ready to prove Theorem 1.1. In view of (2), it suffices to show that, under the assumption that n is sufficiently large and m satisfies $p_n(m) \geq 1/n$, we have $p_n(m) \leq (1 + o(1))/n$ and $n - m \in K_n$. In particular, by Proposition 3.1, we may assume that $m \leq n^{4/3}$ say. The starting point is an application of Corollary 2.2. By the first statement, we have

$$p_n(m) = \frac{1}{n} \sum_{\substack{0 \leq k < n \\ n-k|m}} \mathbb{P}(\text{lcm}(\text{ord}(\pi_k), n-k) = m), \quad (5)$$

and by the second statement (applied with k in place of n),

$$\mathbb{P}(\text{lcm}(\text{ord}(\pi_k), n-k) = m) \leq \frac{\tau(m)}{k} \quad (6)$$

whenever $0 < k < n$. It follows that the total contribution of all $k \geq n^{1/2}$ to the right-hand side of (5) is at most

$$\frac{1}{n} \cdot \tau(m) \cdot \frac{\tau(m)}{n^{1/2}} = \frac{\tau(m)^2}{n^{3/2}} \ll n^{-4/3}.$$

On the other hand, out of those k that are less than $n^{1/2}$, at most one contributes to $p_n(m)$. Indeed, if this were not the case, then m would have two divisors in the interval $(n - n^{1/2}, n]$, call them $d_1 < d_2$. This would lead to a contradiction since

$$\text{lcm}(d_1, d_2) = \frac{d_1 d_2}{\gcd(d_1, d_2)} \geq \frac{d_1 d_2}{d_2 - d_1} \geq \frac{(n - n^{1/2})^2}{n^{1/2}} > m.$$

Thus, m has a unique divisor $d \in (n - n^{1/2}, n]$ and we have

$$p_n(m) \leq \frac{1}{n} \mathbb{P}(\text{lcm}(\text{ord}(\pi_{n-d}), d) = m) + O(n^{-4/3}).$$

In particular, we have $p_n(m) \leq (1 + o(1))/n$. Moreover, since m was assumed to satisfy $p_n(m) \geq 1/n$, it follows that

$$\mathbb{P}(\text{lcm}(\text{ord}(\pi_{n-d}), d) \neq m) \ll n^{-1/3}. \quad (7)$$

We contend that this forces d to be divisible by all positive integers less than or equal to $n - d$. Indeed, suppose this does not hold. Then there exists a prime p such that the largest power of p not exceeding $n - d$, call it q , doesn't divide d . In particular, by maximality of q , we have

$$q^2 \geq pq > n - d. \quad (8)$$

Let E be the event that the order of π_{n-d} is divisible by q . Then on E , the p -adic valuation of $\text{lcm}(\text{ord}(\pi_{n-d}), d)$ equals that of q , and on E^c , it is strictly less than that of q . Consequently, at least one of E , E^c is contained in the event on the left-hand side of (7), so $\min(\mathbb{P}(E), \mathbb{P}(E^c)) \ll n^{-1/3}$. But by [4, Lemma 1], we have the exact expression

$$\mathbb{P}(E^c) = \prod_{j=1}^{\lfloor (n-d)/q \rfloor} \left(1 - \frac{1}{jq}\right).$$

Hence, using (8), we obtain the approximation

$$\frac{1}{q} \leq \mathbb{P}(E) \leq \sum_{j=1}^{\lfloor (n-d)/q \rfloor} \frac{1}{jq} \ll \frac{\log q}{q}. \quad (9)$$

Note that by (7), we certainly have

$$\mathbb{P}(\text{lcm}(\text{ord}(\pi_{n-d}), d) = m) \geq \frac{1}{2},$$

so (6) implies $n - d \leq 2\tau(m)$. This means that $q \ll n^{1/4}$ say, whence the lower bound (9) implies $\mathbb{P}(E) \gg n^{-1/4}$. Thus, we cannot have $\mathbb{P}(E) \ll n^{-1/3}$, so the only remaining option is $\mathbb{P}(E^c) \ll n^{-1/3}$. In view of the upper bound (9), this means that $q \ll 1$. Hence, by (8), we also have $n - d \ll 1$. But then necessarily $\mathbb{P}(E^c) = 0$, which is absurd since $\mathbb{P}(\text{ord}(\pi_{n-d}) = 1) > 0$. Therefore, the claim follows, so in particular $d = m$. In other words, we conclude that $m = n - k$ for some $k \in K_n$, thereby completing the proof.

4 Proof of Theorem 1.2

Theorem 1.2 follows by combining Theorem 1.1 and the following proposition, which gives accurate control on the point probabilities $\mathbb{P}(\text{ord}(\pi_n) = n - k)$ for $k \in K_n$.

Proposition 4.1. *For any $k \in K_n$ we have*

$$\mathbb{P}(\text{ord}(\pi_n) = n - k) = \frac{1}{n - k} + \eta(n, k) + O(n^{-3+o(1)}),$$

where we define

$$\eta(n, k) := \begin{cases} 0 & \text{if } k \in \{0, 1\} \text{ or } 2^{\lfloor \log_2 k \rfloor + 1} \mid n - k \\ \frac{2^{1 - \lfloor \log_2 k \rfloor}}{(n - k)^2} & \text{otherwise} \end{cases}.$$

Proof. The proof is a relatively straightforward adaptation of the arguments of Warlimont [11], which deal with the case $k = 0$.¹ Hence, we will be fairly brief on the details. As in [11], we start by using Cauchy's formula [8, Theorem 1.2] to express

$$\mathbb{P}(\text{ord}(\pi_n) = n - k) = \frac{1}{n - k} + \sum_{\substack{m, m_1, \dots, m_r \in \mathbb{N}_0 \\ m + \sum_{j=1}^r m_j d_j = n \\ \text{lcm}\{d_j \mid j \in [r], m_j > 0\} = n - k}} \frac{1}{m!} \prod_{j=1}^r \frac{1}{m_j! d_j^{m_j}},$$

where $1 < d_1 < \dots < d_r < n - k$ are the divisors of $n - k$. For each $i \in \mathbb{N}_0$, we let T_i be the total contribution of the terms satisfying $\sum_{j=s+1}^r m_j = i$, where s is the number of $j \in [r]$ for which

¹In fact, Warlimont considers the probability that the order divides n instead of being exactly equal to n , but this distinction is not significant.

$d_j < n^{1-\delta}$, and $\delta > 0$ is some small parameter. One can then proceed in the same way as in [11] to bound

$$\sum_{i=3}^{\infty} T_i \ll (\tau(n-k)n^{\delta-1})^3.$$

Furthermore, in analogy to [11], one can establish that

$$T_0 \leq F(n, k), \quad T_1 \leq \tau(n-k)n^{\delta-1}F(n, k),$$

where we define

$$F(n, k) := n \sum_{m \geq A(n, k)} \frac{1}{m!} + 2^{-B(n, k)} \tau(n-k) \exp(\tau(n-k)),$$

$$A(n, k) := \frac{n}{6\tau(n-k)}, \quad B(n, k) := \frac{n^\delta}{6\tau(n-k)}.$$

In a similar vein, the total contribution to T_2 of all terms apart from those with

$$d_r = \frac{n-k}{2}, \quad m_r = 2, \quad m_{s+1} = \dots = m_{r-1} = 0 \quad (10)$$

is at most $O((\tau(n-k)n^{\delta-1})^2 F(n, k))$. It therefore remains to show that the contribution of the terms satisfying (10) is precisely $\eta(n, k)$. Indeed, if n is large enough, then we have $\tau(n-k) \leq n^{\delta/3}$ and hence

$$A(n, k) \geq \frac{1}{6}n^{1-\delta/3}, \quad B(n, k) \geq \frac{1}{6}n^{2\delta/3}.$$

Consequently, we may bound

$$\sum_{i=3}^{\infty} T_i \ll n^{-3+4\delta}$$

and also

$$F(n, k) \ll \exp\left(-\frac{1}{6}n^{1-\delta/3}\right) + \exp\left(-\frac{\log 2}{6}n^{2\delta/3} + n^{\delta/3} + \frac{\delta}{3}\log n\right),$$

which is certainly $O(n^{-3})$. Since $\delta > 0$ is arbitrary, we obtain an error term of the desired form.

To finish the proof, we carefully examine the terms that satisfy (10). For such terms, we have $m + \sum_{j=1}^s m_j d_j = k$. In order to have $\text{lcm}\{d_j \mid j \in [r], m_j > 0\} = n-k$, there must exist $j \in [s]$ such that $m_j > 0$ and $\nu_2(d_j) = \nu_2(n-k)$, where ν_2 denotes 2-adic valuation. For this to be possible, we need $\nu_2(n-k)$ to be equal to the maximum of $\nu_2(t)$ over all $t \in [k]$. In particular, if $k \in \{0, 1\}$ or $\nu_2(n-k) > \lfloor \log_2 k \rfloor$, this is not possible. Otherwise, the terms of interest are precisely those which in addition to (10) satisfy $m_j = 1$ for the unique $j \in [s]$ such that $d_j = 2^{\lfloor \log_2 k \rfloor}$. Their total contribution is easily seen to be

$$\frac{1}{2\left(\frac{n-k}{2}\right)^2 \cdot 2^{\lfloor \log_2 k \rfloor}} = \frac{2^{1-\lfloor \log_2 k \rfloor}}{(n-k)^2},$$

as desired. $\square$

To prove Theorem 1.2, assume n is sufficiently large and let $k_0 := \max K_n$. By Theorem 1.1, it suffices to prove that $p_n(n-k_0) > p_n(n-k)$ for all $k \in K_n \setminus \{k_0\}$. Hence, by Proposition 4.1, it is enough to show that

$$\frac{k_0 - k}{(n-k_0)(n-k)} + \eta(n, k_0) - \eta(n, k) \geq \frac{1}{(n-k)^2}. \quad (11)$$

If $k \in \{0, 1\}$, then $\eta(n, k) = 0$, so (11) certainly holds. Hence, we may assume that $k \geq 2$, so in particular $\eta(n, k) \leq 1/(n-k)^2$. Since $\text{lcm}(1, 2, \dots, k)$ divides both $n-k$ and $n-k_0$, it must divide $k_0 - k$. Therefore, $k_0 - k \geq 2$, so the left-hand side of (11) is at least

$$\frac{2}{(n-k_0)(n-k)} - \frac{1}{(n-k)^2} > \frac{1}{(n-k)^2},$$

as desired.

Remark 4.2. As a consequence of Theorem 1.2 and Proposition 4.1, one obtains the more refined asymptotic

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

The error term here is best possible up to constants, as can be seen by considering n of the form $\text{lcm}(1, 2, \dots, k) + k$ for $k \in \mathbb{N}$.

Acknowledgements. This work was supported by the Croatian Science Foundation under the project number HRZZ-IP-2022-10-5116 (FANAP). The author would like to thank Rudi Mrazović for reading an earlier draft of this paper and Sean Eberhard for many useful comments and remarks.

References

- [1] Huseyin Acan, Charles Burnette, Sean Eberhard, Eric Schmutz, and James Thomas. Permutations with equal orders. *Combin. Probab. Comput.*, 30(5):800–810, 2021.
- [2] Sean Eberhard. What is the probability that two random permutations have the same order? MathOverflow. <https://mathoverflow.net/q/312352> (version: 2018-10-09).
- [3] P. Erdős and P. Turán. On some problems of a statistical group-theory. I. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 4:175–186, 1965.
- [4] P. Erdős and P. Turán. On some problems of a statistical group-theory. II. *Acta Math. Acad. Sci. Hungar.*, 18:151–163, 1967.
- [5] P. Erdős and P. Turán. On some problems of a statistical group-theory. III. *Acta Math. Acad. Sci. Hungar.*, 18:309–320, 1967.
- [6] P. Erdős and P. Turán. On some problems of a statistical group-theory. IV. *Acta Math. Acad. Sci. Hungar.*, 19:413–435, 1968.
- [7] William Feller. *An Introduction to Probability Theory and Its Applications*, volume 1 of *Wiley Series in Probability and Statistics*. John Wiley & Sons, Inc., third edition, 1968.
- [8] Kevin Ford. Cycle Type of Random Permutations: a Toolkit. *Discrete Anal.*, pages Paper No. 9, 36, 2022.
- [9] Edmund Landau. Über die Maximalordnung der Permutationen gegebenen Grades [on the maximal order of permutations of given degree]. *Arch. Math. Phys. Ser. 3*, 5, 1903.
- [10] Gérald Tenenbaum. *Introduction to Analytic and Probabilistic Number Theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015.
- [11] Richard Warlimont. über die Anzahl der Lösungen von $x^n = 1$ in der symmetrischen Gruppe S_n . *Arch. Math. (Basel)*, 30(6):591–594, 1978.