The Rényi entropy of the order of a random permutation

Adrian Beker

University of Zagreb

July 6, 2026

The order of a random permutation

- For a permutation $\pi \in S_n$, its order is

$$\mathrm{ord}(\pi) := \min\{k \in \mathbb{N} \mid \pi^k = e\}$$

- $\mathrm{ord}(\pi)$ is the least common multiple of the cycle lengths of π, e.g.

$$\mathrm{ord}\big((1\ 3)(2\ 4\ 5)\big) = \mathrm{lcm}(2, 3) = 6$$

- Let π_n be a permutation drawn uniformly at random from S_n

Question

How is $\mathrm{ord}(\pi_n)$ distributed?

The order of a random permutation

- For a permutation $\pi \in S_n$, its order is

$$\mathrm{ord}(\pi) := \min\{k \in \mathbb{N} \mid \pi^k = e\}$$

- $\mathrm{ord}(\pi)$ is the least common multiple of the cycle lengths of π, e.g.

$$\mathrm{ord}\big((1\ 3)(2\ 4\ 5)\big) = \mathrm{lcm}(2, 3) = 6$$

- Let π_n be a permutation drawn uniformly at random from S_n

Question

How is $\mathrm{ord}(\pi_n)$ distributed?

The order of a random permutation

- For a permutation $\pi \in S_n$, its order is

$$\mathrm{ord}(\pi) := \min\{k \in \mathbb{N} \mid \pi^k = e\}$$

- $\mathrm{ord}(\pi)$ is the least common multiple of the cycle lengths of π, e.g.

$$\mathrm{ord}\big((1\ 3)(2\ 4\ 5)\big) = \mathrm{lcm}(2, 3) = 6$$

- Let π_n be a permutation drawn uniformly at random from S_n

Question

How is $\mathrm{ord}(\pi_n)$ distributed?

The order of a random permutation

- For a permutation $\pi \in S_n$, its order is

$$\operatorname{ord}(\pi) := \min\{k \in \mathbb{N} \mid \pi^k = e\}$$

- $\operatorname{ord}(\pi)$ is the least common multiple of the cycle lengths of π, e.g.

$$\operatorname{ord}\big((1\ 3)(2\ 4\ 5)\big) = \operatorname{lcm}(2,3) = 6$$

- Let π_n be a permutation drawn uniformly at random from S_n

Question

How is $\operatorname{ord}(\pi_n)$ distributed?

The collision probability of the order

Acan, Burnette, Eberhard, Schmutz and Thomas (2021) studied the collision probability

$$P_2(n) := \mathbb{P}(\mathrm{ord}(\pi_n) = \mathrm{ord}(\pi'_n)),$$

where π'_n is an independent copy of π_n. Writing $p_n(m) := \mathbb{P}(\mathrm{ord}(\pi_n) = m)$,

$$P_2(n) = \sum_{m \in \mathbb{N}} p_n(m)^2 = \|p_n\|_2^2.$$

More generally, for $q \in (1, \infty]$,

$$P_q(n) := \begin{cases} \|p_n\|_q^q & \text{if } q < \infty \\ \|p_n\|_\infty & \text{if } q = \infty \end{cases}.$$

$P_\infty(n)$ is the maximum probability of achieving a particular value of the order.

The probabilities $P_q(n)$ are closely related to the Rényi entropy of $\mathrm{ord}(\pi_n)$.

Trivially, $P_\infty(n) \geq \mathbb{P}(\pi_n \text{ is an } n\text{-cycle}) = 1/n$ and hence $P_2(n) \geq 1/n^2$.

The collision probability of the order

Acan, Burnette, Eberhard, Schmutz and Thomas (2021) studied the collision probability

$$P_2(n) := \mathbb{P}(\mathrm{ord}(\pi_n) = \mathrm{ord}(\pi'_n)),$$

where π'_n is an independent copy of π_n. Writing $p_n(m) := \mathbb{P}(\mathrm{ord}(\pi_n) = m)$,

$$P_2(n) = \sum_{m \in \mathbb{N}} p_n(m)^2 = \|p_n\|_2^2.$$

More generally, for $q \in (1, \infty]$,

$$P_q(n) := \begin{cases} \|p_n\|_q^q & \text{if } q < \infty \\ \|p_n\|_\infty & \text{if } q = \infty \end{cases}.$$

$P_\infty(n)$ is the maximum probability of achieving a particular value of the order.

The probabilities $P_q(n)$ are closely related to the Rényi entropy of $\mathrm{ord}(\pi_n)$.

Trivially, $P_\infty(n) \geq \mathbb{P}(\pi_n \text{ is an } n\text{-cycle}) = 1/n$ and hence $P_2(n) \geq 1/n^2$.

The collision probability of the order

Acan, Burnette, Eberhard, Schmutz and Thomas (2021) studied the collision probability

$$P_2(n) := \mathbb{P}(\mathrm{ord}(\pi_n) = \mathrm{ord}(\pi_n')),$$

where π_n' is an independent copy of π_n. Writing $p_n(m) := \mathbb{P}(\mathrm{ord}(\pi_n) = m)$,

$$P_2(n) = \sum_{m \in \mathbb{N}} p_n(m)^2 = \|p_n\|_2^2.$$

More generally, for $q \in (1, \infty]$,

$$P_q(n) := \begin{cases} \|p_n\|_q^q & \text{if } q < \infty \\ \|p_n\|_\infty & \text{if } q = \infty \end{cases}.$$

$P_\infty(n)$ is the maximum probability of achieving a particular value of the order.

The probabilities $P_q(n)$ are closely related to the Rényi entropy of $\mathrm{ord}(\pi_n)$.

Trivially, $P_\infty(n) \geq \mathbb{P}(\pi_n \text{ is an } n\text{-cycle}) = 1/n$ and hence $P_2(n) \geq 1/n^2$.

The collision probability of the order

Acan, Burnette, Eberhard, Schmutz and Thomas (2021) studied the collision probability

$$P_2(n) := \mathbb{P}(\mathrm{ord}(\pi_n) = \mathrm{ord}(\pi'_n)),$$

where π'_n is an independent copy of π_n. Writing $p_n(m) := \mathbb{P}(\mathrm{ord}(\pi_n) = m)$,

$$P_2(n) = \sum_{m \in \mathbb{N}} p_n(m)^2 = \|p_n\|_2^2.$$

More generally, for $q \in (1, \infty]$,

$$P_q(n) := \begin{cases} \|p_n\|_q^q & \text{if } q < \infty \\ \|p_n\|_\infty & \text{if } q = \infty \end{cases}.$$

$P_\infty(n)$ is the maximum probability of achieving a particular value of the order.

The probabilities $P_q(n)$ are closely related to the Rényi entropy of $\mathrm{ord}(\pi_n)$.

Trivially, $P_\infty(n) \geq \mathbb{P}(\pi_n \text{ is an } n\text{-cycle}) = 1/n$ and hence $P_2(n) \geq 1/n^2$.

The collision probability of the order

Acan, Burnette, Eberhard, Schmutz and Thomas (2021) studied the collision probability

$$P_2(n) := \mathbb{P}(\mathrm{ord}(\pi_n) = \mathrm{ord}(\pi'_n)),$$

where π'_n is an independent copy of π_n. Writing $p_n(m) := \mathbb{P}(\mathrm{ord}(\pi_n) = m)$,

$$P_2(n) = \sum_{m\in\mathbb{N}} p_n(m)^2 = \|p_n\|_2^2.$$

More generally, for $q \in (1, \infty]$,

$$P_q(n) := \begin{cases} \|p_n\|_q^q & \text{if } q < \infty \\ \|p_n\|_\infty & \text{if } q = \infty \end{cases}.$$

$P_\infty(n)$ is the maximum probability of achieving a particular value of the order.

The probabilities $P_q(n)$ are closely related to the Rényi entropy of $\mathrm{ord}(\pi_n)$.

Trivially, $P_\infty(n) \geq \mathbb{P}(\pi_n \text{ is an } n\text{-cycle}) = 1/n$ and hence $P_2(n) \geq 1/n^2$.

The collision probability of the order

Acan, Burnette, Eberhard, Schmutz and Thomas (2021) studied the collision probability

$$P_2(n) := \mathbb{P}(\mathrm{ord}(\pi_n) = \mathrm{ord}(\pi_n')),$$

where π_n' is an independent copy of π_n. Writing $p_n(m) := \mathbb{P}(\mathrm{ord}(\pi_n) = m)$,

$$P_2(n) = \sum_{m \in \mathbb{N}} p_n(m)^2 = \|p_n\|_2^2.$$

More generally, for $q \in (1, \infty]$,

$$P_q(n) := \begin{cases} \|p_n\|_q^q & \text{if } q < \infty \\ \|p_n\|_\infty & \text{if } q = \infty \end{cases}.$$

$P_\infty(n)$ is the maximum probability of achieving a particular value of the order.

The probabilities $P_q(n)$ are closely related to the Rényi entropy of $\mathrm{ord}(\pi_n)$.

Trivially, $P_\infty(n) \geq \mathbb{P}(\pi_n \text{ is an } n\text{-cycle}) = 1/n$ and hence $P_2(n) \geq 1/n^2$.

Previous results and open problems

Theorem (Acan et al., 2021)

$P_2(n)$ is not $O(1/n^2)$ as $n \to \infty$. Nevertheless, $P_2(n) \leq n^{-2+o(1)}$.

Problem (Acan et al., 2021)

Can one prove more precise upper bounds for $P_2(n)$? Is it true that

$$\liminf_{n\to\infty} n^2 P_2(n) < \infty?$$

Question (Acan et al., 2021; Erdős–Turán, 1960s)

What is the maximum of $\mathbb{P}(\mathrm{ord}(\pi_n) = m)$ and for what m is it achieved?

Since $\|p_n\|_\infty \leq \|p_n\|_2$, the results of Acan et al. imply $P_\infty(n) \leq n^{-1+o(1)}$.

Previous results and open problems

Theorem (Acan et al., 2021)

$P_2(n)$ is not $O(1/n^2)$ as $n \to \infty$. Nevertheless, $P_2(n) \leq n^{-2+o(1)}$.

Problem (Acan et al., 2021)

Can one prove more precise upper bounds for $P_2(n)$? Is it true that

$$\liminf_{n\to\infty} n^2 P_2(n) < \infty?$$

Question (Acan et al., 2021; Erdős–Turán, 1960s)

What is the maximum of $\mathbb{P}(\mathrm{ord}(\pi_n) = m)$ and for what m is it achieved?

Since $\|p_n\|_\infty \leq \|p_n\|_2$, the results of Acan et al. imply $P_\infty(n) \leq n^{-1+o(1)}$.

Previous results and open problems

Theorem (Acan et al., 2021)

$P_2(n)$ is not $O(1/n^2)$ as $n \to \infty$. Nevertheless, $P_2(n) \le n^{-2+o(1)}$.

Problem (Acan et al., 2021)

Can one prove more precise upper bounds for $P_2(n)$? Is it true that

$$\liminf_{n\to\infty} n^2 P_2(n) < \infty?$$

Question (Acan et al., 2021; Erdős–Turán, 1960s)

What is the maximum of $\mathbb{P}(\mathrm{ord}(\pi_n) = m)$ and for what m is it achieved?

Since $\|p_n\|_\infty \le \|p_n\|_2$, the results of Acan et al. imply $P_\infty(n) \le n^{-1+o(1)}$.

Previous results and open problems

Theorem (Acan et al., 2021)

$P_2(n)$ is not $O(1/n^2)$ as $n \to \infty$. Nevertheless, $P_2(n) \leq n^{-2+o(1)}$.

Problem (Acan et al., 2021)

Can one prove more precise upper bounds for $P_2(n)$? Is it true that

$$\liminf_{n\to\infty} n^2 P_2(n) < \infty?$$

Question (Acan et al., 2021; Erdős–Turán, 1960s)

What is the maximum of $\mathbb{P}(\mathrm{ord}(\pi_n) = m)$ and for what m is it achieved?

Since $\|p_n\|_\infty \leq \|p_n\|_2$, the results of Acan et al. imply $P_\infty(n) \leq n^{-1+o(1)}$.

Exceptionally popular orders

For a large positive integer n, let

$$K_n := \{k \in \{0, 1, \ldots, n-1\} \mid \mathrm{lcm}(1, \ldots, k) \text{ divides } n-k\}.$$

For $k \in K_n$,

$$\mathbb{P}(\mathrm{ord}(\pi_n) = n-k) \geq \mathbb{P}(\pi_n \text{ contains an } (n-k)\text{-cycle}) = 1/(n-k).$$

Hence,

$$P_\infty(n) \geq \frac{1}{n - \max K_n}, \quad P_2(n) \geq \frac{|K_n|}{n^2}.$$

Acan et al. showed that $|K_n| \geq \log^* n - O(1)$ for infinitely many n, whence

$$\limsup_{n\to\infty} n^2 P_2(n) = \infty.$$

Exceptionally popular orders

For a large positive integer n, let

$$K_n := \left\{ k \in \{0, 1, \dots, n-1\} \mid \operatorname{lcm}(1, \dots, k) \text{ divides } n - k \right\}.$$

For $k \in K_n$,

$$\mathbb{P}(\operatorname{ord}(\pi_n) = n - k) \geq \mathbb{P}(\pi_n \text{ contains an } (n-k)\text{-cycle}) = 1/(n-k).$$

Hence,

$$P_\infty(n) \geq \frac{1}{n - \max K_n}, \quad P_2(n) \geq \frac{|K_n|}{n^2}.$$

Acan et al. showed that $|K_n| \geq \log^* n - O(1)$ for infinitely many n, whence

$$\limsup_{n \to \infty} n^2 P_2(n) = \infty.$$

Exceptionally popular orders

For a large positive integer n, let

$$K_n := \big\{k \in \{0, 1, \ldots, n-1\} \mid \operatorname{lcm}(1, \ldots, k) \text{ divides } n - k\big\}.$$

For $k \in K_n$,

$$\mathbb{P}(\operatorname{ord}(\pi_n) = n - k) \geq \mathbb{P}(\pi_n \text{ contains an } (n-k)\text{-cycle}) = 1/(n-k).$$

Hence,

$$P_\infty(n) \geq \frac{1}{n - \max K_n}, \quad P_2(n) \geq \frac{|K_n|}{n^2}.$$

Acan et al. showed that $|K_n| \geq \log^* n - O(1)$ for infinitely many n, whence

$$\limsup_{n\to\infty} n^2 P_2(n) = \infty.$$

Exceptionally popular orders

For a large positive integer n, let

$$K_n := \big\{ k \in \{0, 1, \ldots, n-1\} \mid \operatorname{lcm}(1, \ldots, k) \text{ divides } n-k \big\}.$$

For $k \in K_n$,

$$\mathbb{P}(\operatorname{ord}(\pi_n) = n-k) \geq \mathbb{P}(\pi_n \text{ contains an } (n-k)\text{-cycle}) = 1/(n-k).$$

Hence,

$$P_\infty(n) \geq \frac{1}{n - \max K_n}, \quad P_2(n) \geq \frac{|K_n|}{n^2}.$$

Acan et al. showed that $|K_n| \geq \log^* n - O(1)$ for infinitely many n, whence

$$\limsup_{n\to\infty} n^2 P_2(n) = \infty.$$

New results – most probable order

An asymptotic for the maximum of $p_n(m)$ together with a stability result:

Theorem (B., 2026)

We have the asymptotic $P_\infty(n) = (1+o(1))/n$. 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 $k \in K_n$.

An exact description of the maximiser of $p_n(m)$:

Theorem (B., 2026)

For all sufficiently large n, we have $p_n(m) = P_\infty(n)$ if and only if $m = n - \max K_n$.

New results – collision probability

An sharp upper bound for the collision probability:

Theorem (B., 2026)

For any n, we have $n^2 P_2(n) \leq \log^* n + O(1)$.

The average and lower limit behaviour of the collision probability:

Theorem (B., 2026)

We have $\frac{1}{N}\sum_{n=1}^{N} n^2 P_2(n) = O(1)$. In particular,

$$\liminf_{n\to\infty} n^2 P_2(n) < \infty.$$

Proof ideas

Given $m \in \mathbb{N}$, we want to bound $\mathbb{P}(\mathrm{ord}(\pi_n) = m)$.

Let $c(\pi_n)$ be the number of cycles of π_n.

Lemma

For any $\ell, m, n \in \mathbb{N}$ with $\ell > 1$,

$$\mathbb{P}(c(\pi_n) = \ell,\ \mathrm{ord}(\pi_n) \mid m) \leq \frac{\left(\sum_{d|m} 1/d\right)^{\ell-1}}{n(\ell-1)!} \leq \frac{1}{n}\left(\frac{eh(m)}{\ell-1}\right)^{\ell-1}.$$

Here, $h(m)$ is the sum of reciprocal divisors of m. We have $h(m) = O(\log\log m)$.

If ℓ is much larger than $\log\log m$, the above is $o(1/n)$, so can assume

$$\ell \leq O(\log\log m).$$

Proof ideas

Given $m \in \mathbb{N}$, we want to bound $\mathbb{P}(\mathrm{ord}(\pi_n) = m)$.

Let $c(\pi_n)$ be the number of cycles of π_n.

Lemma

For any $\ell, m, n \in \mathbb{N}$ with $\ell > 1$,

$$\mathbb{P}(c(\pi_n) = \ell,\ \mathrm{ord}(\pi_n) \mid m) \leq \frac{\left(\sum_{d|m} 1/d\right)^{\ell-1}}{n(\ell-1)!} \leq \frac{1}{n}\left(\frac{eh(m)}{\ell-1}\right)^{\ell-1}.$$

Here, $h(m)$ is the sum of reciprocal divisors of m. We have $h(m) = O(\log \log m)$.

If ℓ is much larger than $\log \log m$, the above is $o(1/n)$, so can assume

$$\ell \leq O(\log \log m).$$

Proof ideas

Given $m \in \mathbb{N}$, we want to bound $\mathbb{P}(\mathrm{ord}(\pi_n) = m)$.

Let $c(\pi_n)$ be the number of cycles of π_n.

Lemma

For any $\ell, m, n \in \mathbb{N}$ with $\ell > 1$,

$$\mathbb{P}(c(\pi_n) = \ell,\ \mathrm{ord}(\pi_n) \mid m) \leq \frac{\left(\sum_{d|m} 1/d\right)^{\ell-1}}{n(\ell-1)!} \leq \frac{1}{n}\left(\frac{eh(m)}{\ell-1}\right)^{\ell-1}.$$

Here, $h(m)$ is the sum of reciprocal divisors of m. We have $h(m) = O(\log\log m)$.

If ℓ is much larger than $\log\log m$, the above is $o(1/n)$, so can assume

$$\ell \leq O(\log\log m).$$

Proof ideas

Given $m \in \mathbb{N}$, we want to bound $\mathbb{P}(\operatorname{ord}(\pi_n) = m)$.

Let $c(\pi_n)$ be the number of cycles of π_n.

Lemma

For any $\ell, m, n \in \mathbb{N}$ with $\ell > 1$,

$$\mathbb{P}(c(\pi_n) = \ell,\ \operatorname{ord}(\pi_n) \mid m) \leq \frac{\left(\sum_{d|m} 1/d\right)^{\ell-1}}{n(\ell-1)!} \leq \frac{1}{n}\left(\frac{eh(m)}{\ell-1}\right)^{\ell-1}.$$

Here, $h(m)$ is the sum of reciprocal divisors of m. We have $h(m) = O(\log\log m)$.

If ℓ is much larger than $\log\log m$, the above is $o(1/n)$, so can assume

$$\ell \leq O(\log\log m).$$

Proof ideas

It remains to bound $\mathbb{P}(c(\pi_n) \leq O(\log\log m),\ \mathrm{ord}(\pi_n) = m)$.

Lemma

For any $\ell, m, n \in \mathbb{N}$,

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

Here, $\omega(m)$ is the number of prime factors of m. We have $\omega(m) = O\left(\frac{\log m}{\log\log m}\right)$.

Hence, the above is at most $m^{-1+o(1)}$, which is $o(1/n)$ if $m \geq n^{1.1}$.

Proof ideas

It remains to bound $\mathbb{P}(c(\pi_n) \le O(\log\log m),\ \mathrm{ord}(\pi_n) = m)$.

Lemma

For any $\ell, m, n \in \mathbb{N}$,

$$\mathbb{P}(c(\pi_n) = \ell,\ m \mid \mathrm{ord}(\pi_n)) \le \frac{\ell^{\omega(m)}}{m}.$$

Here, $\omega(m)$ is the number of prime factors of m. We have $\omega(m) = O\left(\frac{\log m}{\log\log m}\right)$.

Hence, the above is at most $m^{-1+o(1)}$, which is $o(1/n)$ if $m \ge n^{1.1}$.

Proof ideas

It remains to bound $\mathbb{P}(c(\pi_n) \leq O(\log\log m),\ \mathrm{ord}(\pi_n) = m)$.

Lemma

For any $\ell, m, n \in \mathbb{N}$,

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

Here, $\omega(m)$ is the number of prime factors of m. We have $\omega(m) = O\left(\frac{\log m}{\log\log m}\right)$.

Hence, the above is at most $m^{-1+o(1)}$, which is $o(1/n)$ if $m \geq n^{1.1}$.

Proof ideas

To deal with $m \leq n^{1.1}$, we use:

Lemma

For any $m, n \in \mathbb{N}$,

$$\mathbb{P}(\mathrm{ord}(\pi_n) = m) = \frac{1}{n} \sum_{\substack{0 \leq x < n \\ n-x \mid m}} \mathbb{P}\big(\mathrm{lcm}(\mathrm{ord}(\pi_x), n-x) = m\big). \qquad (*)$$

In particular, $\mathbb{P}(\mathrm{ord}(\pi_n) \mid m) \leq \frac{\tau(m)}{n}$, where $\tau(m)$ is the number of divisors of m.

Since $\tau(m) \leq m^{o(1)}$, the contribution of all $x > n^{0.1}$ in $(*)$ is at most

$$\frac{1}{n} \cdot \tau(m) \cdot \frac{\tau(m)}{n^{0.1}} = o(1/n).$$

There is at most one $x \leq n^{0.1}$ with $n - x \mid m$, so $\mathbb{P}(\mathrm{ord}(\pi_n) = m) \leq (1 + o(1))/n$.

Proof ideas

To deal with $m \le n^{1.1}$, we use:

Lemma

For any $m, n \in \mathbb{N}$,

$$\mathbb{P}(\mathrm{ord}(\pi_n) = m) = \frac{1}{n} \sum_{\substack{0 \le x < n \\ n-x \mid m}} \mathbb{P}\big(\mathrm{lcm}(\mathrm{ord}(\pi_x), n-x) = m\big). \qquad (*)$$

In particular, $\mathbb{P}(\mathrm{ord}(\pi_n) \mid m) \le \frac{\tau(m)}{n}$, where $\tau(m)$ is the number of divisors of m.

Since $\tau(m) \le m^{o(1)}$, the contribution of all $x > n^{0.1}$ in $(*)$ is at most

$$\frac{1}{n} \cdot \tau(m) \cdot \frac{\tau(m)}{n^{0.1}} = o(1/n).$$

There is at most one $x \le n^{0.1}$ with $n - x \mid m$, so $\mathbb{P}(\mathrm{ord}(\pi_n) = m) \le (1 + o(1))/n$.

Proof ideas

To deal with $m \leq n^{1.1}$, we use:

Lemma

For any $m, n \in \mathbb{N}$,

$$\mathbb{P}(\mathrm{ord}(\pi_n) = m) = \frac{1}{n} \sum_{\substack{0 \leq x < n \\ n-x \mid m}} \mathbb{P}\big(\mathrm{lcm}(\mathrm{ord}(\pi_x), n-x) = m\big). \qquad (*)$$

In particular, $\mathbb{P}(\mathrm{ord}(\pi_n) \mid m) \leq \frac{\tau(m)}{n}$, where $\tau(m)$ is the number of divisors of m.

Since $\tau(m) \leq m^{o(1)}$, the contribution of all $x > n^{0.1}$ in $(*)$ is at most

$$\frac{1}{n} \cdot \tau(m) \cdot \frac{\tau(m)}{n^{0.1}} = o(1/n).$$

There is at most one $x \leq n^{0.1}$ with $n - x \mid m$, so $\mathbb{P}(\mathrm{ord}(\pi_n) = m) \leq (1 + o(1))/n$.