ALGEBRAIC
COMBINATORICS

Sean Eberhard & Daniele Garzoni

Random generation with cycle type restrictions

Volume 4, issue 1 (2021), p. 1-25.

<http://alco.centre-mersenne.org/item/ALCO_2021__4_1_1_0>

Algebraic Combinatorics
Volume 4, issue 1 (2021), p. 1–25
https://doi.org/10.5802/alco.149

Random generation with cycle type restrictions

Sean Eberhard & Daniele Garzoni

Abstract We study random generation in the symmetric group when cycle type restrictions are imposed. Given $\pi, \pi' \in S_n$, we prove that π and a random conjugate of π' are likely to generate at least A_n provided only that π and π' have not too many fixed points and not too many 2-cycles. As an application, we investigate the following question: For which positive integers m should we expect two random elements of order m to generate A_n? Among other things, we give a positive answer for any m having any divisor d in the range $3 \leqslant d \leqslant o(n^{1/2})$.

1. Introduction

Fix two conjugacy classes $\mathcal{C}, \mathcal{C}'$ of the symmetric group S_n. Should we expect random elements $\pi \in \mathcal{C}, \pi' \in \mathcal{C}'$ to generate at least A_n?

Clearly not if $\mathcal{C}$ and $\mathcal{C}'$ both represent elements with many fixed points, for then it is likely that π and π' have a common fixed point, and therefore cannot possibly generate A_n. Also not if $\mathcal{C}$ and $\mathcal{C}'$ both represent elements with many 2-cycles: If both $\mathcal{C}$ and $\mathcal{C}'$ represent elements with $\Omega(n)$ 2-cycles, then it is not hard to see that the probability that π and π' have a common 2-cycle is bounded away from zero.

The purpose of this paper is to prove that, apart from these two basic obstructions, yes we should expect π, π' to generate at least A_n. The following is our main theorem.

Theorem 1.1. *Let $\mathcal{C}, \mathcal{C}' \subset S_n$ be fixed conjugacy classes. For each j let c_j be the number of j-cycles in a representative element of $\mathcal{C}$, and similarly c_j' for $\mathcal{C}'$. Let $\pi \in \mathcal{C}, \pi' \in \mathcal{C}'$ be chosen uniformly at random. Assume that $c_1, c_1' = o(n^{2/3})$. Then*

(1) $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = 1 - o(1)$ *if and only if*
$$(c_1 + c_2^{1/2})(c_1' + {c_2'}^{1/2}) = o(n);$$
(2) $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = \Omega(1)$ *if and only if*
$$\begin{aligned} &(c_1 + c_2^{1/2})(c_1' + {c_2'}^{1/2}) = O(n), \ \text{and} \\ &c_2 + c_2' = n - \Omega(n). \end{aligned}$$

In fact the hypothesis $c_1, c_1' = o(n^{2/3})$ is not needed for the "only if" statements.

The point of the theorem is that the likelihood of $\langle \pi, \pi'^{\sigma} \rangle \geqslant A_n$ is more-or-less completely characterized by counting fixed points and 2-cycles. The symmetric version of the theorem is illustrative:

Manuscript received 29th April 2019, revised 25th June 2020, accepted 2nd September 2020.

Keywords. symmetric group, random generation.

ISSN: 2589-5486 http://algebraic-combinatorics.org/

Corollary 1.2. *Assume $c_1 = c'_1$ and $c_2 = c'_2$.*

(1) $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = 1 - o(1)$ *if and only if* $c_1 = o(n^{1/2})$ *and* $c_2 = o(n)$.

(2) $\mathbf{P}(\langle \pi, \pi' \rangle \geqslant A_n) = \Omega(1)$ *if and only if* $c_1 = O(n^{1/2})$ *and* $c_2 = n/2 - \Omega(n)$.

Our theorem refines some previous results about random generation in S_n. The most well-known and basic of these is Dixon's theorem [4], confirming a conjecture of Netto, that two random elements of S_n almost surely generate at least A_n. Confirming a conjecture of Robinson, Shalev [11] proved that this remains true if we require the two elements to be conjugate. One can view Theorem 1.1 as a common generalization of these two results, since a random permutation almost surely has very few fixed points and very few 2-cycles.[(1)] In another direction, Babai and Hayes [2] proved that if π is fixed and π' is uniformly random, then π and π' will almost surely generate at least A_n if and only if π has $o(n)$ fixed points. This does not follow from our theorem (because of the $c_1, c'_1 = o(n^{2/3})$ restriction), but it certainly has a similar flavour.

Our original motivation was the following question. Let $\operatorname{ord} S_n$ be the set of all m which occur as the order of at least one $\pi \in S_n$. Fix $m \in \operatorname{ord} S_n$, and let π and π' be two random elements of order m. Should we expect π and π' to generate at least A_n? For the almost-sure version of the question, we give a positive answer for a broad class of m. Specifically, we prove the following theorem.

Theorem 1.3. *Let $m \in \operatorname{ord} S_n$, and assume that either*

(1) *m has a divisor d in the range $3 \leqslant d \leqslant o(n^{1/2})$, or*

(2) *m is even and there is at least one $\pi \in S_n$ with $o(n^{1/2})$ fixed points and $o(n)$ 2-cycles.*

Then two random elements of S_n of order m almost surely generate at least A_n.

For the positive-probability version of the question, we give a complete characterization.

Theorem 1.4. *Let $m \in \operatorname{ord} S_n$. Then two random elements of order m generate at least A_n with probability bounded away from zero if and only if*

(1) *m is odd and there is at least one $\pi \in S_n$ of order m with $O(n^{1/2})$ fixed points, or*

(2) *m is even and not 2.*

The novelty of these results is the wide range we allow for m. The case of bounded m is included in work of Liebeck and Shalev, see [8], and particularly [9]. In the latter paper the authors consider more generally random homomorphisms $\Gamma \to S_n$ for any Fuchsian group Γ: Thus for example they prove that A_n is generated by random elements satisfying $x^2 = y^3 = (xy)^7 = 1$. It is clear that our rather elementary approach, relying essentially on the independence of the generators, does not apply to such a problem. On the other hand we are not aware of any previous results for unbounded m.

1.1. Notation and idiosyncrasies. Much of our notation has already appeared. We consistently write π and π' for our two permutations, which we assume are random subject to having c_j and c'_j j-cycles, respectively, for each j. We will write c and c' for the total number of cycles:

$$c = c_1 + \cdots + c_n$$
$$c' = c'_1 + \cdots + c'_n.$$

[(1)] To be precise, for any $\omega_n \to \infty$, the probability that π has at most ω_n fixed points tends to 1 as $n \to \infty$, and similarly for 2-cycles.

Occasionally, we will denote cycle types using exponent notation: Thus for example the conjugacy class $\mathcal{C}$ consists of all permutations with cycle type $(1^{c_1}, 2^{c_2}, \dots, n^{c_n})$.

We write Ω for our ground set of size n, and we write S_n and A_n for the symmetric and alternating groups on Ω. If G acts on a set X, $g \in G$, $x \in X$, we write x^g for the image of x under g. In particular, if $g, h \in G$ we write h^g for $g^{-1}hg$. Thus if $\operatorname{fix}_X(g)$ is the fixed point set of g then we have

$$\operatorname{fix}_X(g^h) = \operatorname{fix}_X(g)^h.$$

We use standard big-O and little-o without reservation, all understood with respect to the limit $n \to \infty$. That is, if x and y are quantities depending on n, $x = O(y)$ means there is an constant C such that $|x| \leqslant Cy$ for all sufficiently large n, while $x = o(y)$ means $x/y \to 0$ as $n \to \infty$. Similarly, $x = \Omega(y)$ means there is a constant $c > 0$ such that $x \geqslant cy$, and $x = \omega(y)$ means $x/y \to \infty$. Often, $O(x)$ or $o(x)$ is used to indicate an error that is bounded as claimed, but note that the notation indicates nothing about the sign of the error (so, e.g. $-O(x) = O(x)$); by contrast Ω notation does include a sign assertion: $\Omega(1)$ denotes a positive constant bounded away from zero, while $-\Omega(1)$ denotes a negative constant bounded away from zero (e.g. as in Corollary 1.2(2)). Additionally, for positive quantities we use the Vinogradov notation $x \ll y$ to mean $x = O(y)$, and $x \asymp y$ to mean $x \ll y$ and $x \gg y$ (i.e. x/y is bounded above and below by positive constants). We will use subscripts such as $O_{k,m}$ or $\ll_{k,m}$ to warn that the implicit constant may depend on the parameters k, m.

As will be clear already and annoying to some readers, we are mainly interested in asymptotic properties of S_n as $n \to \infty$, so almost all of our results are expressed with inexplicit error terms like $o(1)$ or $1 - o(1)$. None of our methods are especially advanced, so it is certainly possible to prove everything with explicit error terms, but doing so would be notationally cumbersome and, we feel, distracting. Instead, we have prioritized statements which are as general as possible with respect to the conjugacy classes $\mathcal{C}$ and $\mathcal{C}'$. If ever our theorem is needed with an explicit error term for specific conjugacy classes, it will be easy enough to rehash the essential arguments.

In line with this philosophy, we do not hesitate to say "almost surely", when really we mean "with probability tending to 1 as $n \to \infty$", and "with positive probability" instead of "with probability bounded away from 0", etc. This technically imprecise language could actually be made precise by working with an ultraproduct of $(S_n)_{n=1}^{\infty}$ instead of the finite groups S_n, but there is no reader whom this would help.

1.2. Organization of the paper.

We now briefly sketch the proof of Theorem 1.1, and explain the organization of the paper.

First, we prove the "only if" statements in Theorem 1.1 in Section 2. We also give a few examples justifying the $c_1, c_1' = o(n^{2/3})$ hypothesis. We hope that starting with a wealth of examples will orient the reader, and motivate the rest of the paper.

In particular, it will be clear from these examples that the main obstruction in Theorem 1.1 is transitivity. Therefore in Section 3 we estimate the probability that $G = \langle \pi, \pi' \rangle$ is transitive by studying the distribution of the number N of orbits of G of size less than $n/2$. This is the most technical part of the paper. We will prove that if

$$(c_1 + c_2^{1/2})(c_1' + {c_2'}^{1/2}) = o(n)$$

then $\mathbf{E}N = o(1)$, and hence G is almost surely transitive. Otherwise, if

$$(c_1 + c_2^{1/2})(c_1' + {c_2'}^{1/2}) = O(n)$$

and

$$c_2 + c_2' = n - \Omega(n)$$

then we will prove $\mathbf{E}N = O(1)$. We will then use the method of moments to prove the Poisson-type approximation

$$\mathbf{P}(N=0) = \mathrm{e}^{-\mathbf{E}N} + o(1).$$

Hence G is transitive with probability bounded away from zero.

If G is transitive, then very likely $G \geqslant A_n$. We prove this in Section 4. We treat the imprimitive and primitive cases separately. Neither argument is very difficult, and the bounds are much stronger than the bounds we give for the intransitive case. For the primitive case we use results depending the classification of finite simple groups. This will complete the proof of Theorem 1.1.

Finally, in Section 5 we study fixed-order generation. Again we give a wealth of examples, and we prove Theorems 1.3 and 1.4 using Theorem 1.1.

2. Necessity of the hypotheses

Our first order of business is to discuss the necessity of the various hypotheses in Theorem 1.1. We prove the stated "only if" conditions, and additionally we discuss some examples where $c_1 + c_1'$ exceeds $n^{2/3}$.

2.1. The case $c_1c_1'/n = \Omega(1)$ or $c_1c_1'/n = \omega(1)$.

If π and π' each have many fixed points then it is likely that they have a common fixed point. The expected number of common fixed points of π and π' is exactly c_1c_1'/n. We claim that if $c_1c_1'/n = \Omega(1)$ then there is a nonvanishing probability that π and π' have a common fixed point, and if $c_1c_1'/n = \omega(1)$ then almost surely π and π' have a common fixed point. To see this, note that $\mathrm{fix}(\pi)$ is just a random set of size c_1 and $\mathrm{fix}(\pi')$ is just a random set of size c_1'. The probability that two random sets of size c_1 and c_1' are disjoint is

$$\begin{aligned}\frac{n-c_1}{n}\frac{n-c_1-1}{n-1}\cdots\frac{n-c_1-c_1'+1}{n-c_1'+1} &\leqslant \exp\left(-\frac{c_1}{n}-\frac{c_1}{n-1}-\cdots-\frac{c_1}{n-c_1'+1}\right)\\ &\leqslant \exp\left(-\frac{c_1c_1'}{n}\right).\end{aligned}$$

This proves both our claims.

2.2. The case $c_2c_2' \gg n^2$.

Suppose that $c_2c_2' \gg n^2$. We claim that there is a nonvanishing probability that π and π' have a common 2-cycle. To see this, fix the c_2 2-cycles of π, and consider picking the c_2' 2-cycles of π' in order. The k-th 2-cycle is chosen uniformly from a pool of $\binom{n-2k+2}{2}$ possibilities, of which at least $c_2 - 2k + 2$ are also 2-cycles of π. Thus the probability that each of these fails to be a common 2-cycle is bounded by

$$\prod_{k \leqslant c_2', c_2/2} \left(1 - \frac{c_2 - 2k+2}{\binom{n-2k+2}{2}}\right).$$

Ignoring the terms with $k > c_2/4$, and using $\binom{n-2k+2}{2} \gg n^2$, this is bounded by

$$\left(1-\Omega(c_2/n^2)\right)^{\lfloor c_2'/2\rfloor}.$$

Using the inequality $1 - x \leqslant \exp(-x)$, this is bounded by

$$\exp\left(-\Omega\left(\frac{c_2c_2'}{n^2}\right)\right).$$

If $c_2c_2' \gg n^2$ then this is bounded away from 1.

2.3. The case ${c_1 c_2'}^{1/2}/n = \Omega(1)$ or ${c_1 c_2'}^{1/2}/n = \omega(1)$, or vice versa. Morally, a similar argument applies if $c_1^2 c_2' \gg n^2$, but the situation is complicated by the need to track two "state variables": the number of remaining 2-cycles to place, and the number of exhausted fixed points. Instead we use moment methods.

Assume $c_1^2 c_2' \gg n^2$, and let N be the number of 2-cycles (xy) of π' such that x, y are both fixed points of π. Each of the c_2' cycles of π' has a $c_1(c_1-1)/(n(n-1))$ chance to be a pair of fixed points of π, so

$$\mathbf{E}N = \frac{c_1(c_1-1)c_2'}{n(n-1)}.$$

Since $c_1 - 1 = c_1(1+O(1/c_1))$ and $(n-1)^{-1} = n^{-1}(1+O(1/n)) = n^{-1}(1+O(1/c_1))$, we may write this as

$$\mathbf{E}N = \frac{c_1^2 c_2'}{n^2}(1+O(1/c_1)).$$

Similarly, each ordered pair $((xy),(wz))$ of 2-cycles of π' has a $\binom{c_1}{4}/\binom{n}{4}$ chance of being a quadruple of fixed points of π, so

$$\mathbf{E}(N(N-1)) = \frac{c_1(c_1-1)(c_1-2)(c_1-3)c_2'(c_2'-1)}{n(n-1)(n-2)(n-3)}.$$

Using $c_i - O(1) = c_i(1+O(1/c_i))$ several times, as well as $(n-O(1))^{-1} = n^{-1}(1+O(1/n))$, we get

$$\mathbf{E}(N(N-1)) = \left(\frac{c_1^2 c_2'}{n^2}\right)^2 (1+O(1/c_1 + 1/c_2')).$$

Hence

$$\operatorname{Var} N = \mathbf{E}N + \mathbf{E}(N(N-1)) - (\mathbf{E}N)^2 \leqslant \mathbf{E}N + O(1/c_1 + 1/c_2')(\mathbf{E}N)^2,$$

so, by the second moment method,[2]

$$\mathbf{P}(N=0) \leqslant \frac{\operatorname{Var} N}{(\mathbf{E}N)^2} = \frac{1}{\mathbf{E}N} + O(1/c_1 + 1/c_2').$$

Note now that if $c_1^2 c_2' \gg n^2$ then $c_1 \gg n^{1/2}$. The case in which $c_1 \asymp n$ and $c_2' \asymp 1$ can be handled separately, so assume also $c_2' = \omega(1)$. Then we have

$$\mathbf{P}(N=0) \leqslant \frac{1}{\mathbf{E}N} + o(1), \text{ where}$$
$$\mathbf{E}N \sim \frac{c_1^2 c_2'}{n^2}.$$

Thus if $c_1^2 c_2'/n^2 = \omega(1)$ then $\mathbf{P}(N=0) = o(1)$.

The case in which $c_1^2 c_2'/n^2 \asymp 1$ is a little more delicate, but can be handled with the method of moments. By a similar argument we have

$$\mathbf{E}(N(N-1)\cdots(N-k+1)) = \left(\frac{c_1^2 c_2'}{n^2}\right)^k (1+O_k(1/c_1 + 1/c_2')).$$

Moreover,

$$\mathbf{E}(N(N-1)\cdots(N-k+1)) \leqslant \left(\frac{c_1^2 c_2'}{n^2}\right)^k.$$

[2] Chebyshev's inequatity asserts that $\mathbf{P}(|N - \mathbf{E}N| \geqslant \lambda) \leqslant \operatorname{Var} N/\lambda^2$. We are using the case $\lambda = \mathbf{E}N$ to bound $\mathbf{P}(N=0)$.

Thus from Bonferroni's inequalities, for any integer $K \geqslant 0$ we have

$$\begin{aligned}\mathbf{P}(N=0) &= \sum_{k=0}^{K-1}(-1)^k\mathbf{E}\binom{N}{k} + O\left(\mathbf{E}\binom{N}{K}\right)\\ &= \sum_{k=0}^{K-1}\frac{(-1)^k}{k!}\left(\frac{c_1^2c_2'}{n^2}\right)^k(1+O_k(1/c_1+1/c_2')) + O\left(\frac{1}{K!}\left(\frac{c_1^2c_2'}{n^2}\right)^K\right)\\ &= \mathrm{e}^{-c_1^2c_2'/n^2} + O_K\left(1/c_1+1/c_2'\right) + O\left(\frac{1}{K!}\left(\frac{c_1^2c_2'}{n^2}\right)^K\right).\end{aligned}$$

Assuming $c_1^2c_2'/n^2 \asymp 1$, we can choose $K = O_\epsilon(1)$ so that the second error term is smaller than ϵ, and then as before the first error term is $o_\epsilon(1)$. Hence

$$\mathbf{P}(N=0) = \mathrm{e}^{-c_1^2c_2'/n^2} + o(1).$$

In particular, $\mathbf{P}(N=0)$ is bounded away from 1.

We will use a similar argument later, in Subsection 3.2, to prove the positive direction of Theorem 1.1(2).

2.4. The case $c_2, c_2' = n/2 - o(n)$. Now suppose that $c_2, c_2' = n/2 - o(n)$. We have already shown that the probability that π and π' have a common 2-cycle is bounded away from zero. We claim further that $\langle \pi, \pi' \rangle$ is almost surely intransitive. We do not claim however that π and π' almost surely have a common 2-cycle – instead we use a more involved argument.

Let N be the number of sets $X \subset \Omega$ with the following properties:

(1) $0 < |X| < n^{1/3}$,
(2) X is preserved by both π and π',
(3) $\pi|_X$ and $\pi'|_X$ both consist only of 2-cycles, and
(4) $\langle \pi, \pi' \rangle|_X$ is transitive.

In other words, N is the number of orbits of $\langle \pi, \pi' \rangle$, of size less than $n^{1/3}$, consisting exclusively of 2-cycles. We claim that N is almost surely positive, so in particular $\langle \pi, \pi' \rangle$ is almost surely not transitive.

To prove this we use the second moment method. Let N_k be the number of such sets of size $2k$. Then

$$\mathbf{E}N_k = \binom{n}{2k}^{-1}\binom{c_2}{k}\binom{c_2'}{k}p(k),$$

where $p(k)$ is the probability that two elements of S_{2k}, each of cycle type $(2^{k/2})$, generate a transitive subgroup. Using $k = o(n^{1/2})$ and Stirling's approximation,

$$\mathbf{E}N_k \sim \left(\frac{c_2c_2'}{n^2}\right)^k\frac{(2k)!}{k!^2}p(k) \asymp \left(\frac{4c_2c_2'}{n^2}\right)^k\frac{p(k)}{k^{1/2}}.$$

Next we need to estimate $p(k)$.

Lemma 2.1. $p(k) \asymp k^{-1/2}$.

Proof. There is a bijection between ordered pairs of permutations $\sigma, \sigma' \in S_{2k}$ of cycle type (2^k) and permutations $\tau \in S_{2k}$ having only even-length cycles, defined as follows (see Figure 1). Given σ, σ', define τ by repeating the following process: Find the smallest (in some arbitrary but fixed order) element x at which we have not yet defined τ, and define

$$x \xrightarrow{\tau} x^\sigma \xrightarrow{\tau} x^{\sigma\sigma'} \xrightarrow{\tau} x^{\sigma\sigma'\sigma} \xrightarrow{\tau} \cdots \xrightarrow{\tau} x.$$

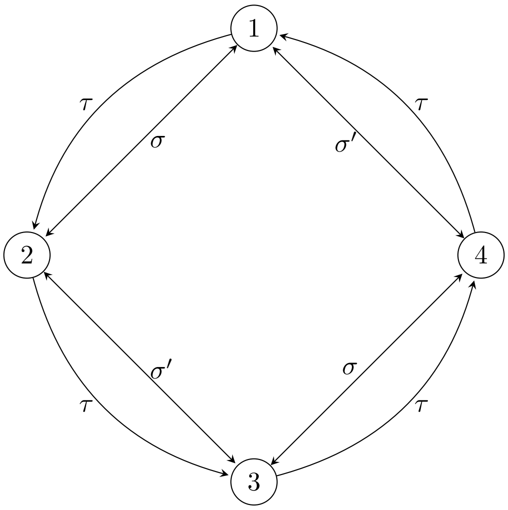

Figure 1. Bijection between pairs of permutations σ, σ' of cycle type (2^k) and permutations τ having only even-length cycles

It is easy to see that the cycle must terminate after an even number of steps, so the process does indeed define a permutation having only even-length cycles. In the other direction, suppose $\tau \in S_{2k}$ has only even-length cycles. On a given cycle of τ, find the smallest element x and define

$$x \overset{\sigma}{\longleftrightarrow} x^\tau \overset{\sigma'}{\longleftrightarrow} x^{\tau^2} \overset{\sigma}{\longleftrightarrow} x^{\tau^3} \overset{\sigma'}{\longleftrightarrow} \cdots \overset{\sigma'}{\longleftrightarrow} x.$$

These maps are clearly mutually inverse.

Now note that $\langle \sigma, \sigma' \rangle$ is transitive if and only if τ is a $2k$-cycle. Thus

$$\begin{aligned} p(k) &= \mathbf{P}(\langle \sigma, \sigma' \rangle \text{ transitive}) \\ &= \frac{|\{\tau : \tau \text{ is a } 2k\text{-cycle}\}|}{|\{\sigma : \sigma \text{ has cycle type } (2^k)\}|^2} \\ &= \frac{(2k)!/(2k)}{((2k)!/(2^k k!))^2} \\ &= \frac{4^k k!^2}{2k(2k)!} \\ &\sim \frac{\sqrt{\pi}}{2} k^{-1/2}. \end{aligned}$$

In the last line we applied Stirling's approximation. □

Hence

$$\mathbf{E} N_k \asymp \left(\frac{4 c_2 c_2'}{n^2} \right)^k \frac{1}{k},$$

and

$$\mathbf{E} N = \sum_{1 \leqslant k < n^{1/3}} \mathbf{E} N_k \asymp \sum_{1 \leqslant k < n^{1/3}} \left(\frac{4 c_2 c_2'}{n^2} \right)^k \frac{1}{k}.$$

As long as $c_2, c_2' = n/2 - o(n)$, this is $\omega(1)$.

In order to estimate $\operatorname{Var} N$, consider $\mathbf{E}(N(N-1))$. This is the expected number of ordered pairs of distinct sets X, Y satisfying conditions (1) through (4). Let E_X be the event that X satisfies (1) through (4). If $|X| = 2k$, we have

$$\mathbf{P}(E_X) = \frac{\binom{c_2}{k}\binom{c_2'}{k}}{\binom{n}{2k}^2} p(k).$$

Because of condition (4), $E_X \cap E_Y = \varnothing$ unless $X = Y$ or $X \cap Y = \varnothing$. If $X \cap Y = \varnothing$, and $|X| = 2k$ and $|Y| = 2l$ say, then

$$\begin{aligned} \mathbf{P}(E_X \cap E_Y) &= \frac{\binom{c_2}{k,l,c_2-k-l}\binom{c_2'}{k,l,c_2'-k-l}}{\binom{n}{2k,2l,n-2k-2l}^2} p(k)p(l) \\ &= \mathbf{P}(E_X)\mathbf{P}(E_Y)(1 + O((k+l)^2/n)). \end{aligned}$$

It follows from this that

$$\mathbf{E}(N(N-1)) \leqslant (\mathbf{E}N)^2(1 + O(n^{-1/3})),$$

and so

$$\operatorname{Var} N = \mathbf{E}N + \mathbf{E}(N(N-1)) - (\mathbf{E}N)^2 \leqslant \mathbf{E}N + O(n^{-1/3})(\mathbf{E}N)^2.$$

Thus

$$\mathbf{P}(N = 0) \leqslant \frac{\operatorname{Var} N}{\mathbf{E}N^2} \leqslant \frac{1}{\mathbf{E}N} + O(n^{-1/3}).$$

Since $\mathbf{E}N = \omega(1)$, this implies $N > 0$ almost surely.

2.5. Cases in which $c_1 + c_1' \gg n^{2/3}$.

We now discuss some examples in which $c_1 + c_1' \gg n^{2/3}$, say $c_1 \gg n^{2/3}$. First, suppose that $c_1^3 c_3' \gg n^3$. In this case a straightforward modification of our argument in the $c_1^2 c_2' \gg n^2$ case (Subsection 2.3) shows that there is likely a 3-cycle (xyz) of π' such that x, y, z are fixed points of π. Similarly if $c_1^4 c_4' \gg n^4$, etc.

These examples are not too troubling. In fact, a slight elaboration of our proof shows that if $c_1 + c_1' \leqslant n^{1-\Omega(1)}$ then it is enough to assume

$$(c_1 + c_2^{1/2} + \cdots + c_n^{1/n})(c_1' + {c_2'}^{1/2} + \cdots + {c_n'}^{1/n}) = o(n)$$

for the almost-sure problem, and

$$\begin{aligned} &(c_1 + c_2^{1/2} + \cdots + c_n^{1/n})(c_1' + {c_2'}^{1/2} + \cdots + {c_n'}^{1/n}) = O(n) \\ &c_2 + c_2' = n - \Omega(n) \end{aligned}$$

for the positive-probability problem. (Note that if $c_1 + c_1' \leqslant n^{1-\Omega(1)}$ then really only boundedly many terms in these expressions are important.)

The following example is more troubling. Suppose π is a random n-cycle and π' a random transposition. Then up to conjugacy π is $(12\cdots n)$ and π' is (xn) for some x chosen uniformly from $\{1, \dots, n-1\}$. Let $G = \langle \pi, \pi' \rangle$. Then G is determined by $\gcd(x, n)$: If $\gcd(x, n) > 1$ then G is imprimitive, while if $\gcd(x, n) = 1$ then $G = S_n$. Thus the probability that $G \geqslant A_n$ is $\varphi(n)/(n-1)$, which can be small or large depending on the arithmetic of n. This example illustrates the difficulty of pinning down a pithy if-and-only-if condition without any a priori hypothesis on $c_1 + c_1'$.

Finally, we note that if $c + c' > n + 1$ then there are in fact no $\pi \in \mathcal{C}$ and $\pi' \in \mathcal{C}'$ such that $\langle \pi, \pi' \rangle$ is transitive.

3. Intransitive subgroups

Let $G = \langle \pi, \pi' \rangle$. As so often the case in random generation problems in S_n, the main obstruction is transitivity: If G is transitive then very likely $G \geqslant A_n$ (we will prove this in Section 4). In other words, our main job is to estimate the probability that π and π' have a common fixed set of some size k.

Let N_k be the number of orbits of G of size k, in other words the number of k-sets fixed by G and on which G acts transitively. Let

$$N = \sum_{1 \leqslant k \leqslant n/2} N_k.$$

Our goal is to estimate $\mathbf{P}(N = 0)$. We will accomplish this in two stages:

(1) We will bound $\lambda = \mathbf{E}N$. This will already establish what we need for the almost-sure problem, since $\mathbf{P}(N = 0) \geqslant 1 - \lambda$.

(2) We will prove a Poisson-type approximation for N which shows that $\mathbf{P}(N = 0) \approx \mathrm{e}^{-\lambda}$.

3.1. Bounding $\lambda = \mathbf{E}N$. There are many ways we can form a fixed k-set from the cycles of π and π'. For any two partitions

$$k = d_1 1 + d_2 2 + \cdots + d_k k, \tag{1}$$

$$k = d'_1 1 + d'_2 2 + \cdots + d'_k k, \tag{2}$$

such that $d_j \leqslant c_j, d'_j \leqslant c'_j$ for each j, we can form a fixed k-set by taking d_j j-cycles from π and d'_j j-cycles from π', for each j. The probability that these k-sets coincide after π' is conjugated by σ is $1/\binom{n}{k}$. Thus we have

$$\mathbf{E}N_k = \sum_{(1),(2)} \frac{\binom{c_1}{d_1} \cdots \binom{c_k}{d_k} \binom{c'_1}{d'_1} \cdots \binom{c'_k}{d'_k}}{\binom{n}{k}} p(d_1, \ldots, d_k; d'_1, \ldots, d'_k), \tag{3}$$

where $p(d_1, \ldots, d_k; d'_1, \ldots, d'_k)$ denotes the probability that random permutations $\tau, \tau' \in S_k$ with cycle types $(1^{d_1}, \ldots, k^{d_k})$ and $(1^{d'_1}, \ldots, k^{d'_k})$ generate a transitive subgroup.[(3)]

In this subsection we simply ignore $p(d_1, \ldots, d_k; d'_1, \ldots, d'_k)$, bounding it by 1. Thus from (3) we have simply

$$\mathbf{E}N_k \leqslant \frac{f_k f'_k}{\binom{n}{k}},$$

where

$$f_k = \sum_{(1)} \binom{c_1}{d_1} \cdots \binom{c_k}{d_k} \tag{4}$$

is the number of k-sets fixed by π, and similarly f'_k. (In the next subsection we will need the full force of (3).)

Lemma 3.1. *We have*

$$f_k \leqslant \min_{x>0} x^{-k} (1+x)^{c_1} (1+x^2)^{c_2} \cdots (1+x^k)^{c_k}.$$

[(3)] Of course, this is the very thing we are trying to estimate in this section. This "self-similarity" is largely incidental: When we write $p(d_1, \ldots, d_k; d'_1, \ldots, d'_k)$ we usually have in mind $k, d_1, \ldots, d'_k$ of bounded size, whereas in the bigger picture of this section we are concerned with asymptotics.

Proof. This follows from

$$\begin{aligned} f_k x^k &= \sum_{(1)} \binom{c_1}{d_1} \cdots \binom{c_k}{d_k} x^{d_1 1 + \cdots + d_k k} \\ &\leqslant \sum_{d_1, \ldots, d_k \geqslant 0} \binom{c_1}{d_1} \cdots \binom{c_k}{d_k} x^{d_1 1 + \cdots + d_k k} \\ &= (1+x)^{c_1} (1+x^2)^{c_2} \cdots (1+x^k)^{c_k}. \end{aligned}$$ □

Define the function h by

$$h(x) = x \log \frac{1}{x} + (1-x) \log \frac{1}{1-x}.$$

It is well known that

$$k^{-1/2} \, \mathrm{e}^{h(k/n)n} \ll \binom{n}{k} \leqslant \mathrm{e}^{h(k/n)n} \qquad (1 \leqslant k \leqslant n/2).$$

The latter inequality follows from

$$\binom{n}{k} x^k \leqslant (1+x)^n,$$

with $x = k/(n-k)$, since in this case

(5) $$x^{-k}(1+x)^n = \mathrm{e}^{h(k/n)n}.$$

The former inequality follows from Stirling's approximation.

Lemma 3.2. *For any $\epsilon \in (0, 1/2)$ we have*

$$f_k \leqslant \left(\frac{c_1}{k}\right)^k \mathrm{e}^{O(\epsilon^{-2}k)} + \mathrm{e}^{h\left(\frac{k}{2c_2}\right)c_2 + \epsilon k} + \left(\frac{n}{k}\right)^{k/3} \mathrm{e}^{O(\epsilon^{-2}k)}.$$

To be clear, the assertion is that there is a constant C not depending on ϵ such that, for all $\epsilon \in (0, 1/2)$,

$$f_k \leqslant \left(\frac{c_1}{k}\right)^k \mathrm{e}^{C\epsilon^{-2}k} + \mathrm{e}^{h\left(\frac{k}{2c_2}\right)c_2 + \epsilon k} + \left(\frac{n}{k}\right)^{k/3} \mathrm{e}^{C\epsilon^{-2}k}.$$

Hence ϵ is an optimizable parameter.

Note that the middle term here is of the form

$$\left(\frac{c_2}{k}\right)^{k/2} \mathrm{e}^{O(k)}.$$

The more precise bound is important to us, however.

Proof. First note that we may assume $k \leqslant 3c/2$, for if $k \geqslant 3c/2$ then directly from (4) we have

$$f_k \leqslant 2^c \leqslant 2^{2k/3},$$

which is subsumed by the third term in the claim.

Now assume $k \leqslant 3c/2$. By the previous lemma we have, if $x \leqslant 1$,

(6) $$f_k \leqslant x^{-k}(1+x)^{c_1}(1+x^2)^{c_2}(1+x^3)^c.$$

We consider three cases[(4)] depending on which of

$$c_1/k, \quad \frac{1}{2}\epsilon(c_2/k)^{1/2}, \quad (c/k)^{1/3}$$

is largest.

(1) First suppose $c_1/k \geqslant \frac{1}{2}\epsilon(c_2/k)^{1/2}, (c/k)^{1/3}$. Take $x = k/c_1$ in (6). The result is

$$f_k \leqslant \left(\frac{c_1}{k}\right)^k \mathrm{e}^{\left(\frac{k}{c_1}\right)c_1 + \left(\frac{k}{c_1}\right)^2 c_2 + \left(\frac{k}{c_1}\right)^3 c} \leqslant \left(\frac{c_1}{k}\right)^k \mathrm{e}^{O(\epsilon^{-2}k)}.$$

(2) Next suppose $\frac{1}{2}\epsilon(c_2/k)^{1/2} \geqslant c_1/k, (c/k)^{1/3}$. Note the latter condition implies $k \leqslant \epsilon^6 c_2 \leqslant c_2/2$. Take

$$x = \left(\frac{k}{2c_2 - k}\right)^{1/2}$$

in (6). Using

$$f_k \leqslant x^{-k}(1+x^2)^{c_2}\,\mathrm{e}^{xc_1 + x^3 c_3} = \left((x^2)^{-k}(1+x^2)^{2c_2}\right)^{1/2} \mathrm{e}^{xc_1 + x^3 c_3}$$

and (5), we have

$$f_k \leqslant \mathrm{e}^{h\left(\frac{k}{2c_2}\right)c_2 + \left(\frac{k}{2c_2 - k}\right)^{1/2} c_1 + \left(\frac{k}{2c_2-k}\right)^{3/2} c}.$$

Now by hypothesis

$$\left(\frac{k}{2c_2 - k}\right)^{1/2} c_1 \leqslant \left(\frac{k}{c_2}\right)^{1/2} c_1 \leqslant \epsilon k/2$$

and

$$\left(\frac{k}{2c_2 - k}\right)^{3/2} c \leqslant \left(\frac{k}{c_2}\right)^{3/2} c \leqslant (\epsilon/2)^3 k \leqslant \epsilon k/2,$$

so

$$f_k \leqslant \mathrm{e}^{h\left(\frac{k}{2c_2}\right)c_2 + \epsilon k}.$$

(3) Finally, suppose $(c/k)^{1/3} \geqslant \frac{1}{2}\epsilon(c_2/k)^{1/2}, c_1/k$. Take $x = (k/c)^{1/3}$ in (6). The result is

$$f_k \leqslant \left(\frac{c}{k}\right)^{k/3} \mathrm{e}^{\left(\frac{k}{c}\right)^{1/3} c_1 + \left(\frac{k}{c}\right)^{2/3} c_2 + \left(\frac{k}{c}\right)c} \leqslant \left(\frac{c}{k}\right)^{k/3} \mathrm{e}^{O(\epsilon^{-2}k)}.$$

Since $c \leqslant n$ this proves the lemma. □

Lemma 3.3. *We have*

$$\mathbf{E}N_k \ll \left(\frac{(c_1 + c_2^{1/2})(c_1' + {c_2'}^{1/2})}{n} + \frac{c_1 + c_1'}{n^{2/3}} + \left(\frac{k}{n}\right)^{1/6}\right)^k \mathrm{e}^{O(k)}.$$

Moreover, if $c_2 + c_2' = n - \Omega(n)$ *then*

$$\mathbf{E}N_k \ll \frac{1}{k^{k/3}}\left(\frac{c_1c_1' + c_1{c_2'}^{1/2} + {c_2}^{1/2}c_1'}{n} + \frac{c_1 + c_1'}{n^{2/3}}\right)^k O(1)^k + (1 - \Omega(1))^k + O(k/n)^{k/6}.$$

[(4)] To motivate the three cases, note that the unique minimizer of (6) satisfies

$$-\frac{k}{x} + \frac{c_1}{1+x} + \frac{2c_2x}{1+x^2} + \frac{3cx^2}{1+x^3} = 0,$$

and hence

$$c_1\left(\frac{x}{1+x}\right) + 2c_2\left(\frac{x^2}{1+x^2}\right) + 3c\left(\frac{x^3}{1+x^3}\right) = k.$$

The solution to this equation is comparable to the smallest of k/c_1, $(k/c_2)^{1/2}$, $(k/c)^{1/3}$. We consider these three cases separately, taking extra care with the c_2 dependence.

Proof. We have

$$\mathbf{E}N_k \leqslant f_k f_k' \Big/ \binom{n}{k}.$$

Bounding each of f_k and f_k' using the previous lemma and expanding the product, we get

$$\begin{aligned}\mathbf{E}N_k \ll{}& \frac{1}{k^k}\left(\frac{c_1 c_1'}{n}\right)^k \mathrm{e}^{O(\epsilon^{-2}k)} \\ &+ \frac{1}{k^{k/2}}\left(\frac{c_1 {c_2'}^{1/2} + {c_2}^{1/2} c_1'}{n}\right)^k \mathrm{e}^{O(\epsilon^{-2}k)} \\ &+ \frac{1}{k^{k/3}}\left(\frac{c_1 + c_1'}{n^{2/3}}\right)^k \mathrm{e}^{O(\epsilon^{-2}k)} \\ &+ \left(\frac{k}{n}\right)^{k/6} \mathrm{e}^{O(\epsilon^{-2}k)} \\ &+ k^{1/2}\,\mathrm{e}^{h\left(\frac{k}{2c_2}\right)c_2 + h\left(\frac{k}{2c_2'}\right)c_2' - h(k/n)n + 2\epsilon k}.\end{aligned}$$

Here we used the simple bound $\binom{n}{k} \geqslant (n/k)^k$ for every term except the one involving both c_2 and c_2', where we used the more precise bound $\binom{n}{k} \gg k^{-1/2}\,\mathrm{e}^{h(k/n)n}$. Additionally, for the other terms involving c_2 or c_2' we used

$$\mathrm{e}^{h\left(\frac{k}{2c_2}\right)c_2} \leqslant \left(\frac{c_2}{k}\right)^{k/2} \mathrm{e}^{O(k)}.$$

If we apply this bound also to the c_2, c_2' term, and bound various things crudely, then we get the first statement in the lemma.

To get the second statement, the only term which requires further comment is the c_2, c_2' term. Since h is concave and $h'(x) = \log(1/x - 1)$, we have

$$h(x) \leqslant h(k/n) + (x - k/n)\log(n/k - 1).$$

Hence, by a short calculation,

$$\begin{aligned} h\left(\frac{k}{2c_2}\right)c_2 + h\left(\frac{k}{2c_2'}\right)c_2' - h\left(\frac{k}{n}\right)n &\leqslant -(n - c_2 - c_2')\log\left(\frac{n}{n-k}\right) \\ &\leqslant -(n - c_2 - c_2')k/n. \end{aligned}$$

Assuming $c_2 + c_2' = n - \Omega(n)$, this is $-\Omega(k)$, so the lemma follows from taking ϵ appropriately small. □

The above lemma suffices as long as $k = o(n)$. For larger k it is convenient to argue a little differently (and more simply).

Lemma 3.4. *Assume $c_1 + c_1' = o(n)$ and $c + c' \leqslant n - \Omega(n)$. Then for $k \leqslant n/2$ we have*

$$\mathbf{E}N_k \leqslant \mathrm{e}^{-\Omega(k) + o(n)}.$$

Proof. From Lemma 3.1 we have, for $0 < x < 1$,

$$f_k f_k' \leqslant x^{-2k}(1+x)^{c_1 + c_1'}(1+x^2)^{c+c'}.$$

Take $x = (k/(n-k))^{1/2}$. We have

$$(1+x)^{c_1+c_1'} \leqslant \mathrm{e}^{x(c_1+c_1')} \leqslant \mathrm{e}^{(2k/n)^{1/2}(c_1+c_1')}$$

and

$$(1+x^2)^{c+c'} = (1+x^2)^n(1-k/n)^{n-c-c'} \leqslant (1+x^2)^n\,\mathrm{e}^{-k(n-c-c')/n}.$$

Hence

$$f_k f_k' \leqslant \mathrm{e}^{h(k/n)n}\,\mathrm{e}^{(2k/n)^{1/2}(c_1+c_1')-k(n-c-c')/n},$$

and

$$\mathbf{E}N_k \leqslant \frac{f_k f_k'}{\binom{n}{k}} \leqslant \mathrm{e}^{O(\log k)+(2k/n)^{1/2}(c_1+c_1')-k(n-c-c')/n}\,.$$

Assuming $c_1 + c_1' = o(n)$ and $c + c' \leqslant (1-\epsilon)n$, this is bounded by

$$\mathrm{e}^{O(\log k)+o((2kn)^{1/2})-\epsilon k} = \mathrm{e}^{o(n)-\epsilon k},$$

as claimed. □

The following theorem follows by combining the previous two lemmas.

Theorem 3.5.

1. *If* $c_1 + c_1' = o(n^{2/3})$ *and* $(c_1 + {c_2}^{1/2})(c_1' + {c_2'}^{1/2}) = o(n)$ *then* $\mathbf{E}N = o(1)$.
2. *If* $c_1 + c_1' = O(n^{2/3})$, $(c_1 + {c_2}^{1/2})(c_1' + {c_2'}^{1/2}) = O(n)$, *and* $c_2 + c_2' = n - \Omega(n)$, *then* $\mathbf{E}N = O(1)$.

3.2. A Poisson approximation.

In the previous subsection we bounded the expectation $\mathbf{E}N$ of N. In this subsection we apply the method of moments to show that, under similar hypotheses, if $\mathbf{E}N$ is bounded then in fact

$$\mathbf{P}(N=0) \approx \mathrm{e}^{-\mathbf{E}N}\,.$$

The method of moments depends on being able to prove moment estimates of the form

$$\mathbf{E}N(N-1)\cdots(N-m+1) \approx (\mathbf{E}N)^m.$$

We therefore now turn our attention to the estimation of the moments and mixed moments of $(N_k)_{k\geqslant 1}$.

Recall from (3) that

$$\mathbf{E}N_k = \sum_{(1),(2)} \frac{\prod_{j=1}^k \binom{c_j}{d_j}\binom{c_j'}{d_j'}}{\binom{n}{k}} p(d_1,\dots,d_k;d_1',\dots,d_k').$$

We first ask to what extent we have, for $k = O(1)$,

$$\mathbf{E}N_k \approx \sum_{(1),(2)} \frac{\prod_{j=1}^k \frac{c_j^{d_j}}{d_j!}\frac{{c_j'}^{d_j'}}{d_j'!}}{\frac{n^k}{k!}} p(d_1,\dots,d_k;d_1',\dots,d_k').$$

We have

$$\binom{c}{d} = (1+O_d(1/c))\frac{c^d}{d!},$$

so the approximation is appropriate for the factors in which c_j, c_j' are large, as well as the ones in which $d_j \leqslant 1$. Our contention is that the other terms do not contribute significantly, so overall the approximation is fine.

Lemma 3.6. *We have*

$$f_k \ll_k (c_1 + c^{1/2})^k.$$

Moreover, for any particular index j and any $t \geqslant 0$ we have

$$\sum_{(1),d_j\geqslant t} \binom{c_1}{d_1}\cdots\binom{c_k}{d_k} \ll_k \left(\frac{c_j}{(c_1+c^{1/2})^j}\right)^t (c_1+c^{1/2})^k.$$

Proof. We revisit the calculation of the previous section, now armed with the restrictive hypothesis $k = O(1)$. From (4),

$$f_k \asymp_k \max_{(1)} c_1^{d_1} \cdots c_k^{d_k}.$$

The maximum is not difficult to analyze: in fact the maximum over real d_i is precisely

$$\max\{c_1^k, c_2^{k/2}, \dots, c_k^{k/k}\}.$$

We bound this crudely by

$$\max\{c_1^k, c^{k/2}\} \asymp_k (c_1 + c^{1/2})^k.$$

Now consider the part of the sum in which $d_j \geqslant t$. By the same token we have

$$\begin{aligned} \max_{(1), d_j \geqslant t} c_1^{d_1} \cdots c_k^{d_k} &= c_j^t \max_{d_1 1 + \cdots + d_k k = k - tj} c_1^{d_1} \cdots c_k^{d_k} \\ &\ll_k c_j^t (c_1 + c^{1/2})^{k-tj}. \end{aligned}$$

This proves the lemma. □

Lemma 3.7.

$$\begin{aligned} \mathbf{E} N_k = \sum_{(1),(2)} & \frac{\prod_{j=1}^k \frac{c_j^{d_j}}{d_j!} \frac{{c'_j}^{d'_j}}{d'_j!}}{\frac{n^k}{k!}} p(d_1, \dots, d_k; d'_1, \dots, d'_k) \\ & + O_k\left(\frac{1}{\min\{c_1 + c^{1/2}, c'_1 + {c'}^{1/2}\}^{2/3}} \frac{((c_1 + c^{1/2})(c'_1 + {c'}^{1/2}))^k}{n^k} \right). \end{aligned}$$

Proof. Let δ be a parameter, and split the sum according to whether there is any j such that $d_j \geqslant 2$ and $c_j \leqslant \delta(c_1 + c^{1/2})^j$, or $d'_j \geqslant 2$ and $c'_j \leqslant \delta(c'_1 + {c'}^{1/2})^j$. By the previous lemma, the part of the sum where there is some such j is bounded by

$$O_k(\delta^2)(c_1 + c^{1/2})^k (c'_1 + {c'}^{1/2})^k.$$

On the other hand, if $c_j \geqslant \delta(c_1 + c^{1/2})^j$ whenever $d_j \geqslant 2$ then we have

$$\binom{c_1}{d_1} \cdots \binom{c_k}{d_k} = \frac{c_1^{d_1}}{d_1!} \cdots \frac{c_k^{d_k}}{d_k!} \left(1 + O_k\left(\frac{1}{\delta(c_1 + c^{1/2})}\right)\right),$$

and similarly for the primed variables. Thus the error in our approximation is bounded by

$$O_k\left(\delta^2 + \frac{1}{\delta(c_1 + c^{1/2})} + \frac{1}{\delta(c'_1 + {c'}^{1/2})}\right) \frac{(c_1 + c^{1/2})^k (c'_1 + {c'}^{1/2})^k}{n^k}.$$

To get the best bound we take

$$\delta^3 = \min\{c_1 + c^{1/2}, c'_1 + {c'}^{1/2}\}^{-1}.$$

This gives the claimed bound. □

There is a similar estimate for the mixed moment

$$\mathbf{E}[(N_1)_{m_1} \cdots (N_k)_{m_k}].$$

Here we write $(x)_{m_i} = x(x-1)\cdots(x - m_i + 1)$ for the "falling factorial", with the standard convention $(x)_0 = 1$. Let

$$\begin{aligned} m &= m_1 + \cdots + m_k, \\ M &= m_1 1 + \cdots + m_k k. \end{aligned}$$

Define $k_1, \ldots, k_m$ by

$$(k_1, \ldots, k_m) = (\overbrace{1, \ldots, 1}^{m_1}, \ldots, \overbrace{k, \ldots, k}^{m_k}),$$

i.e. $k_i = j$ if

$$m_1 + \cdots + m_{j-1} \leqslant i \leqslant m_1 + \cdots + m_j.$$

For example, if $(m_1, m_2, m_3) = (3, 2, 1)$ then $m = 6$, $M = 10$, and

$$(k_1, k_2, k_3, k_4, k_5, k_6) = (1, 1, 1, 2, 2, 3).$$

The product

$$(N_1)_{m_1} \cdots (N_k)_{m_k}$$

counts m-tuples of distinct orbits of $\langle \pi, \pi' \rangle$, of which m_1 are 1-sets, m_2 are 2-sets, and so on, all these sets being *disjoint* (this is why we count orbits rather than fixed sets). To choose such sets we have to choose, for every such size k_i, d_{i1} 1-cycles, d_{i2} 2-cycles, … of π, and likewise d'_{i1} 1-cycles, d'_{i2} 2-cycles, … of π'. This reasoning leads to the following estimate.

Lemma 3.8.

$$\begin{aligned}\mathbf{E}[(N_1)_{m_1} \cdots (N_k)_{m_k}] \\ = \sum \prod_{i=1}^{m} \frac{\prod_{j=1}^{k} \frac{c_j^{d_{ij}}}{d_{ij}!} \frac{{c'_j}^{d'_{ij}}}{d'_{ij}!}}{\frac{n^{k_i}}{k_i!}} p(d_{i1}, \ldots, d_{ik}; d'_{i1}, \ldots, d'_{ik}) \\ + O_M\left(\frac{1}{\min\{c_1 + c^{1/2}, c'_1 + {c'}^{1/2}\}^{2/3}} \frac{((c_1 + c^{1/2})(c'_1 + {c'}^{1/2}))^M}{n^M} \right).\end{aligned}$$

The sum runs over all (d_{ij}), (d'_{ij}) such that

$$d_{i1}1 + \cdots + d_{ik}k = d'_{i1}1 + \cdots + d'_{ik}k = k_i \qquad (i \in \{1, \ldots, m\}).$$

Proof. We have[5]

$$\mathbf{E}[(N_1)_{m_1} \cdots (N_k)_{m_k}] = \sum \frac{\prod_{j=1}^{k} \binom{c_j}{d_{1j}, \ldots, d_{mj}} \binom{c'_j}{d'_{1j}, \ldots, d'_{mj}}}{\binom{n}{k_1, \ldots, k_m}} \prod_{i=1}^{m} p(d_{i1}, \ldots, d_{ik}; d'_{i1}, \ldots, d'_{ik}).$$

The rest of the proof is the same as in the previous lemma. □

Write $N_{\leqslant k} = N_1 + \cdots + N_k$ and $N_{>k} = N - N_{\leqslant k}$. These are the number of orbits of G of size at most k and of size greater than k, respectively.

Theorem 3.9. *Let*

$$B = \max\{(c_1 + c^{1/2})(c'_1 + {c'}^{1/2})/n, 1\}.$$

Then

$$\mathbf{E}[(N_1)_{m_1} \cdots (N_k)_{m_k}] - (\mathbf{E}N_1)^{m_1} \cdots (\mathbf{E}N_k)^{m_k} \ll_M \frac{B^M}{\min\{c_1 + c^{1/2}, c'_1 + {c'}^{1/2}\}^{2/3}}.$$

Thus also, for any k, m,

$$\mathbf{E}[(N_{\leqslant k})_m] - (\mathbf{E}N_{\leqslant k})^m \ll_{k,m} \frac{B^{km}}{\min\{c_1 + c^{1/2}, c'_1 + {c'}^{1/2}\}^{2/3}}.$$

[5] We are using a slightly nonstandard, but backwards-compatible, notation for multinomial coefficients: $\binom{n}{a,b} = \frac{n!}{a!b!(n-a-b)!}$, etc.

Proof. The first bound follows immediately from the previous two lemmas. For the second bound, we use

$$(N_{\leqslant k})_m = m! \sum_{m_1+\cdots+m_k=m} \frac{(N_1)_{m_1}}{m_1!} \cdots \frac{(N_k)_{m_k}}{m_k!},$$

and similarly

$$(\mathbf{E}N_{\leqslant k})^m = m! \sum_{m_1+\cdots+m_k=m} \frac{(\mathbf{E}N_1)^{m_1}}{m_1!} \cdots \frac{(\mathbf{E}N_k)^{m_k}}{m_k!}.$$

Note that the value of $M = 1m_1 + \cdots + km_k$ over $m_1 + \cdots + m_k = m$ ranges between m and km. This proves the theorem. □

Theorem 3.10. *Assume* $c_1+c'_1 = o(n^{2/3})$, $(c_1+c_2^{1/2})(c'_1+{c'_2}^{1/2}) = O(n)$, *and* $c_2+c'_2 = n - \Omega(n)$. *Then*

$$\mathbf{P}(N = 0) = \mathrm{e}^{-\mathbf{E}N} + o(1).$$

Proof. By Lemmas 3.3 and 3.4 from the previous subsection, there is a $k = O_\epsilon(1)$ such that $\mathbf{E}N_{>k}$ is smaller than ϵ, and

$$\mathbf{P}(N = 0) \leqslant \mathbf{P}(N_{\leqslant k} = 0) \leqslant \mathbf{P}(N = 0) + \mathbf{P}(N_{>k} > 0),$$

so the main thing to understand is $\mathbf{E}N_{\leqslant k}$. From Bonferroni's inequalities we have, for any $M \geqslant 0$,

$$1_{N_{\leqslant k}=0} = \sum_{m=0}^{M-1} (-1)^m \binom{N_{\leqslant k}}{m} + O\left(\binom{N_{\leqslant k}}{M}\right).$$

(The left-hand side of this equation is the indicator that $N_{\leqslant k} = 0$.) Therefore, from the previous theorem,

$$\begin{aligned}
\mathbf{P}(N_{\leqslant k} = 0) &= \sum_{m=0}^{M-1} (-1)^m \frac{\mathbf{E}[(N_{\leqslant k})_m]}{m!} + O\left(\frac{\mathbf{E}[(N_{\leqslant k})_M]}{M!}\right) \\
&= \sum_{m=0}^{M-1} (-1)^m \frac{(\mathbf{E}N_{\leqslant k})^m}{m!} + O\left(\frac{(\mathbf{E}N_{\leqslant k})^M}{M!}\right) \\
&\qquad + O_{k,M}\left(\frac{B^{kM}}{\min\{c_1 + c^{1/2}, c'_1 + {c'}^{1/2}\}^{2/3}}\right) \\
&= \mathrm{e}^{-\mathbf{E}N_{\leqslant k}} + O\left(\frac{(\mathbf{E}N_{\leqslant k})^M}{M!}\right) \\
&\qquad + O_{k,M}\left(\frac{B^{kM}}{\min\{c_1 + c^{1/2}, c'_1 + {c'}^{1/2}\}^{2/3}}\right).
\end{aligned}$$

Since $\mathbf{E}N_{\leqslant k} = O_\epsilon(1)$ (by Lemma 3.3 again), we can choose $M = O_\epsilon(1)$ so that the first error term here is smaller than ϵ. Note also $B = O(1)$ by hypothesis. Putting all this together, we have

$$\mathbf{P}(N = 0) = \mathrm{e}^{-\mathbf{E}N} + O(\epsilon) + O_\epsilon\left(\min\{c_1 + c^{1/2}, c'_1 + {c'}^{1/2}\}^{-2/3}\right).$$

Finally, note that the hypothesis $c_1 + c'_1 = o(n^{2/3})$ ensures that either

$$(c_1 + c^{1/2})(c'_1 + {c'}^{1/2}) = o(n),$$

in which case we are already done by Theorem 3.5, or

$$\min\{c_1 + c^{1/2}, c'_1 + {c'}^{1/2}\} \gg n^{1/3}.$$

Thus

$$\mathbf{P}(N=0)=\mathrm{e}^{-\mathbf{E}N}+o(1),$$

as claimed. □

Remark 3.11. An argument along the same line shows that N is asymptotically distributed as Poisson$(\mathbf{E}N)$, and indeed for any fixed k the random variables $N_1,\dots,N_k$ are asymptotically distributed as independent Poisson random variables.

4. Transitive subgroups

In the previous section we estimated the probability that $G=\langle\pi,\pi'\rangle$ is transitive. In this section we show that G is almost surely not a transitive subgroup smaller than A_n. The proof is easier (modulo known results about primitive groups), and the bounds rather stronger.

The following rather trivial lemma (which was already used implicitly in the previous section) seems worth isolating.

Lemma 4.1. *Suppose G acts transitively on a set X, and suppose $\pi_1,\pi_2\in G$ have k_1 and k_2 fixed points in X, respectively. Draw $\sigma\in G$ uniformly at random. Then*

$$\mathbf{P}(\operatorname{fix}(\pi_1)\cap\operatorname{fix}(\pi_2^\sigma)\neq\varnothing)\leqslant k_1k_2/|X|.$$

Proof. This is immediate from

$$\mathbf{E}|\operatorname{fix}(\pi_1)\cap\operatorname{fix}(\pi_2^\sigma)|=\mathbf{E}|\operatorname{fix}(\pi_1)\cap\operatorname{fix}(\pi_2)^\sigma|=k_1k_2/|X|.$$ □

The utility of the lemma is easy to explain. Most maximal subgroups of S_n are given explicitly as the stabilizer of a point in some natural action. For each such subgroup M, we need to show that π,π' are not simultaneously trapped in a conjugate of M, i.e. do not have a common fixed point in the given action. By the lemma it will suffice to bound the number of fixed points of π and π' (with more than a square-root saving).

4.1. Imprimitive subgroups. First consider imprimitive transitive subgroups. To show that π,π' are not simultaneously trapped by any such subgroup, we need to show π,π' do not simultaneously preserve a partition of Ω into k blocks of size m for some $m,k>1$ such that $n=mk$.

Let X_k be the set of all k-(equi)partitions of Ω, i.e. partitions

$$\Omega=\Omega_1\cup\cdots\cup\Omega_k \tag{7}$$

such that $|\Omega_i|=n/k$ for each i. The order of the cells $\Omega_1,\dots,\Omega_k$ is not considered significant. We have

$$|X_k|=\frac{n!}{k!(n/k)!^k}.$$

Note that S_n acts transitively on X_k, and $\langle\pi,\pi'\rangle$ preserves a k-partition if and only if π and π' have a common fixed point in X_k. By Lemma 4.1 it suffices to bound $|\operatorname{fix}_{X_k}(\pi)|$.

Remark 4.2. The "dual" problem of estimating the number of π fixing at least one k-partition was considered in Diaconis–Fulman–Guralnick [3, Sections 5 and 6] and Eberhard–Ford–Koukoulopoulos [5, Theorem 1.2].

Lemma 4.3. *Suppose $\pi\in S_n$ has c cycles. Then $|\operatorname{fix}_{X_k}(\pi)|\leqslant k^c$.*

Proof. Fixed points in X_k correspond to k-partitions (7) preserved by π, i.e. such that for some $\tau\in S_k$ we have

$$\Omega_i^\pi=\Omega_{i^\tau}\qquad(i\in\{1,\dots,k\}). \tag{8}$$

Fix $\tau \in S_k$, and let us count the *ordered* partitions satisfying (8). For each cycle of π, pick a base point. The position of the base point in the partition $\{\Omega_1, \dots, \Omega_k\}$, together with τ, determines the position of every other point in the cycle. Thus there are at most k choices for how to partition the cycle, and therefore at most k^c choices for the partition.

To deduce a bound for $|\operatorname{fix}_{X_k}(\pi)|$ we need to (1) sum over all possibilities for $\tau \in S_k$, and (2) divide by $k!$ because the order of the cells in a partition is not important, so we just get k^c again. □

We need a stronger bound when k is very large, say when $k = n/2$ or $k = n/3$. In this regime we can use the following lemma.

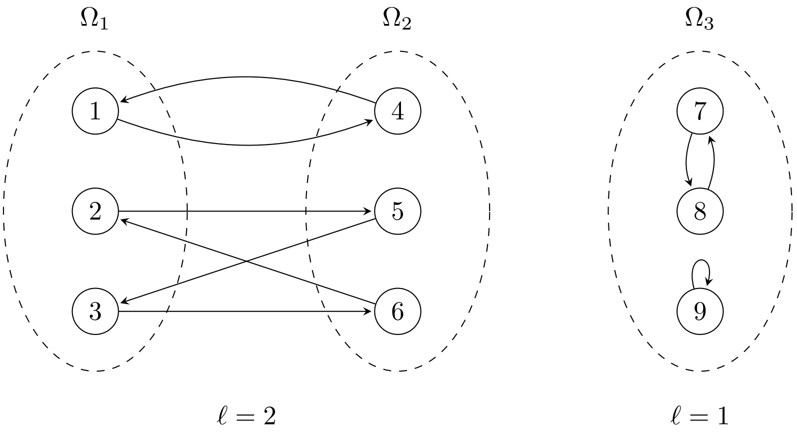

Figure 2. A π-invariant partition with $m = 3$, and the data indicated in the proof of Lemma 4.4

Lemma 4.4. *Suppose π has c cycles. Then $|\operatorname{fix}_{X_{n/m}}(\pi)| \leqslant m^{O(n)} c^{(1-1/m)c}$.*

Proof. A π-invariant n/m-partition is determined by the following data (see Figure 2):

(1) Each j-cycle of π must induce on the partition a cycle of length $\ell = j/d$ for some $d \leqslant m$. Label each cycle of π by this integer ℓ.
(2) Next, organize the cycles of π into piles of cycles of a common label so that in any pile with label ℓ, the sum of the lengths of the cycles is exactly ℓm.
(3) Finally, within each pile, determine how the cycles should be aligned.

Clearly there are at most m^c options for step 1. In step 3, we have at most j options for each j-cycle, so all together we have at most

$$\prod_{j=1}^{n} j^{c_j} \leqslant \prod_{j=1}^{n} \mathrm{e}^{jc_j} = \mathrm{e}^n$$

options. The number of options in step 2 is bounded crudely by the number of ways of partitioning the c cycles into piles of size at most m, which is at most

$$\frac{c^c}{\lfloor c/m \rfloor !}.$$

Now note

$$\lfloor x \rfloor ! \gg x^x / O(1)^x$$

for all $x \geqslant 0$: if $x < 10$ then this is clear, since both sides are bounded and nonzero, while if $x \geqslant 10$ then

$$\lfloor x \rfloor ! \geqslant (\lfloor x \rfloor / \mathrm{e})^{\lfloor x \rfloor} \geqslant (x/(2\,\mathrm{e}))^{x-1} \geqslant x^x/O(1)^x.$$

Applying this with $x = c/m$, the number of options in step 2 is

$$\ll O(1)^{c/m} c^c/(c/m)^{c/m} = O(m)^{c/m} c^{c-c/m}.$$

Hence all together the number of options is bounded by

$$m^c \cdot O(m)^{c/m} c^{c-c/m} \cdot \mathrm{e}^n \leqslant O(m)^n c^{(1-1/m)c} \leqslant m^{O(n)} c^{(1-1/m)c}.$$

(In the last inequality we used the fact that $m \geqslant 2$.) □

Lemma 4.5. *Suppose that π has c cycles and π' has c' cycles. Assume that $c + c' \leqslant (1-\delta)n$ for some $\delta \geqslant \omega(\log\log n/\log n)$ (e.g. a constant). Then the probability that $\langle \pi, \pi' \rangle$ is contained in an imprimitive transitive subgroup is bounded by $2^{-\delta n + o(n)}$.*

Proof. By Lemmas 4.1 and 4.3, the probability that π and π' share a fixed point in X_k is bounded by

$$\frac{k^{c+c'}}{|X_k|} = \frac{k^{c+c'} k! m!^k}{n!} \leqslant \frac{k^{c+c'+k} m!^k}{n!}. \tag{9}$$

Using Stirling's approximation we have

$$\frac{m!^k}{n!} \asymp \frac{O(m)^{k/2}(m/\mathrm{e})^n}{n^{1/2}(n/\mathrm{e})^n} = \frac{O(1)^k n^{k/2-1/2}}{k^{k/2+n}}.$$

Hence (9) is bounded by

$$O(1)^k k^{c+c'+k/2-n} n^{k/2-1/2}.$$

This bound is log-convex in k, so its maximum in the range $2 \leqslant k \leqslant n/\log n$ occurs at one of the end points. At $k = 2$ we get

$$O(2^{c+c'-n} n^{1/2})$$

and at $k \asymp n/\log n$ we get, since $n^{k/2} = O(1)^n$,

$$O(1)^n (n/\log n)^{c+c'-n} \leqslant O(1)^n (\log n)^n n^{c+c'-n}.$$

For $k \geqslant n/\log n$ we use Lemma 4.4 instead of Lemma 4.3. Let $m = n/k$. Repeating the same calculation, we find that the probability that π and π' share a fixed point is bounded by

$$m^{O(n)} n^{(1-1/m)(c+c')} k^{k/2-n} n^{k/2-1/2} \leqslant m^{O(n)} n^{(1-1/m)(c+c'-n)}.$$

We obtain a bound for the probability that $\langle \pi, \pi' \rangle$ is imprimitive by summing over k. The result is

$$O(2^{c+c'-n} n^{3/2}) + (\log n)^{O(n)} n^{c+c'-n}.$$

If $c + c' \leqslant (1-\delta)n$ (where $\delta \geqslant \omega(\log\log n/\log n)$) then the first term dominates, and the lemma follows. □

Remark 4.6. The lemma is likely not sharp, but improving it would require more careful methods. For example, suppose π and π' both have cycle type $(2^{n/2})$, so that $c + c' = n$. As in Lemma 2.1, there is a bijection between such pairs (π, π') and permutations $\tau \in S_n$ having only even cycles, and $\langle \pi, \pi' \rangle$ preserves a k-partition if and only if τ does. This problem is similar to the one considered by Łuczak and Pyber: see [10].

4.2. Primitive subgroups. Finally we must consider the possibility that π and π' get trapped in a primitive subgroup. To some extent we could carry on as we have done for intransitive and imprimitive subgroups, since many families of primitive subgroups of S_n are explicitly given as the stabilizer of a point in some action,[6] but at some point we will need to use some deeper knowledge about simple groups. Fortunately, at this point there is a convenient sledgehammer: Primitive subgroups are few and small, while every conjugacy class with few cycles is big.

Lemma 4.7. *Assume π has c cycles. Then $|\pi^{S_n}| \geqslant n!/n^c$.*

Proof. We have
$$|\pi^{S_n}| = \frac{n!}{\prod_{j=1}^n j^{c_j} c_j!} \geqslant \frac{n!}{\prod_{j=1}^n (jc_j)^{c_j}} \geqslant \frac{n!}{n^c}. \qquad \square$$

Lemma 4.8. *Let M be a primitive maximal subgroup of S_n, other than S_n or A_n. Let f_M be the number of conjugates of M containing π (equivalently, the number of fixed points of π in the action of S_n on the conjugates of M). Then*
$$f_M \leqslant n^c.$$

Proof. The probability that a random conjugate of M contains π is the same as the probability that a random conjugate of π is contained in M, so
$$\frac{f_M}{|S_n : M|} = \frac{|\pi^{S_n} \cap M|}{|\pi^{S_n}|}.$$
(That $|S_n : M|$ is the number of conjugates of M follows from maximality.) Therefore, by the previous lemma,
$$f_M = \frac{n! |\pi^{S_n} \cap M|}{|M| |\pi^{S_n}|} \leqslant \frac{n!}{|\pi^{S_n}|} \leqslant n^c. \qquad \square$$

Lemma 4.9. *The probability that $\langle \pi, \pi' \rangle$ is contained in a primitive subgroup other than S_n or A_n is bounded by $n^{c+c'+\sqrt{n}}/n!$.*

In particular, if $c + c' \leqslant (1-\delta)n$ then this probability is bounded by $n^{-\delta n} \mathrm{e}^{O(n)}$.

Proof. Let M be a maximal primitive subgroup other than S_n or A_n. By Lemma 4.1 again, along with the previous lemma, the probability that π, π' are both contained in a conjugate of M is bounded by
$$\frac{f_M f'_M}{|S_n : M|} \leqslant \frac{|M| n^{c+c'}}{n!}.$$

Now as in Babai [1, Lemma 2.5 and the proof of Theorem 1.4], the sum of $|M|$ over all conjugacy classes of primitive maximal subgroups of S_n (other than S_n and A_n) is bounded by $n^{\sqrt{n}}$. This proves the lemma. $\square$

Remark 4.10. There do exist permutations π such that π and a random conjugate are trapped in a common primitive subgroup with positive probability. For example, suppose $n = k^2$, and consider $S_k \wr S_2$ acting on the cartesian square $\{1, \dots, k\}^2$. This gives us a map $S_k \wr S_2 \to S_n$ whose image is a primitive subgroup M of order $2k!^2$, and different conjugates of M correspond to different labelling maps $\{1, \dots, k\}^2 \to \{1, \dots, n\}$. Let π be the element of M which swaps the first two rows, and let π' be the element which swaps the third and fourth rows. Then π and π' are elements of cycle type (2^k) with disjoint supports, and conversely any two elements of cycle

[6] This is more or less the content of the O'Nan–Scott theorem (see [7] for an exposition and proof).

type (2^k) with disjoint supports are contained in a conjugate of M. Note that two random elements of cycle type (2^k) have disjoint supports with probability $\sim \mathrm{e}^{-4}$.

This may be essentially the only counterexample, however. We formalize this in the following conjecture, which we have so far not been able to prove.

Conjecture 4.11. *Let $\mathcal{C}, \mathcal{C}' \subset S_n$ be fixed nontrivial conjugacy classes, and let $\pi \in \mathcal{C}$ and $\pi' \in \mathcal{C}'$ be random. Then almost surely $\langle \pi, \pi' \rangle$ is not contained in any primitive subgroup apart from S_n, A_n, and any conjugate of $S_{\sqrt{n}} \wr S_2$ or $A_{\sqrt{n}} \wr S_2$.*

In any case, we have now proved under the hypotheses of Theorem 1.1 that $G = \langle \pi, \pi' \rangle$ is almost surely not a transitive subgroup smaller than A_n, which completes the proof.

5. Generators with a given order

In this section we will apply Theorem 1.1 to deduce some results concerning random generation of S_n under order constraints. Let $\operatorname{ord} S_n = \{\operatorname{ord} \pi : \pi \in S_n\}$. For $m \in \operatorname{ord} S_n$, we are interested in the probability that two random elements of order m generate at least A_n.

We may think of drawing a random $\pi \in S_n$ of order m in two stages: first we pick a conjugacy class $\mathcal{C}$ of elements of order m with probability proportional to $|\mathcal{C}|$, then we pick $\pi \in \mathcal{C}$ uniformly. As a consequence of this and Theorem 1.1, we have the following criteria:

(1) Assume almost all elements of order m have $o(n^{1/2})$ fixed points and $o(n)$ 2-cycles. Then two random elements of order m almost surely generate at least A_n.

(2) Assume almost all elements of order m have $O(n^{1/2})$ fixed points and $n/2 - \Omega(n)$ 2-cycles. Then two random elements of order m generate at least A_n with probability bounded away from zero.

Clearly, the converses in Theorem 1.1 also apply. For instance, if a positive proportion of elements of order m have $\Omega(n^{1/2})$ fixed points, the probability of generating at least A_n will be bounded away from 1.

Therefore, our business in this section is to understand which conditions on m ensure that a random element of order m has few fixed points and few 2-cycles. This condition is certainly not automatic, as the following examples show.

Example 5.1. The case $m = 2$ is rather special. A random permutation of order 2 has $\sim n^{1/2}$ fixed points (see [6, Proposition IX.19]) so random pairs of elements of order 2 do not generate. In fact, since any two elements of order 2 generate a dihedral group, indeed no two elements of order 2 generate A_n.

Example 5.2. Suppose $m = p$ for some prime $p \sim 3n/4$. Then any element of order m has $\Omega(n)$ fixed points, so random elements of order m almost surely do not generate.

Example 5.3. Similarly, suppose $m = 2p$ for some $p \sim 3n/4$. Then all π of order m have one p-cycle and either $\Omega(n)$ fixed points or $\Omega(n)$ 2-cycles. It is not hard to see that random elements of order m have $\Theta(n^{1/2})$ fixed points, so by Theorem 1.1 random pairs of elements of order m generate with probability bounded away from 0 and from 1.

Example 5.4. There are also examples with much larger m. Let $p_1 < \cdots < p_k$ be primes, let $m = p_1 \cdots p_k$, and let

$$n = \sum_{i=1}^{k} p_i + p_1 - 1.$$

Then any $\pi \in S_n$ has one p_i-cycle for each i and $p_1 - 1$ fixed points. If p_1 is large compared to $n^{1/2}$ then random pairs of permutations of order m almost surely do not generate.

In each of these examples, the arithmetic of m guarantees that *all* permutations of order m have either many fixed points or many 2-cycles. As a last resort, one might hope at least for a "zero–one law": Perhaps as long as there is at least one permutation of order m with few fixed points and few 2-cycles, then almost all permutations of order m are such. Our last example also dashes this hope.

Example 5.5. Let p and q distinct primes of roughly the same size with $p < q$, let $n = pq+p-1$, and let $m = pq$. There are just two ways that $\pi \in S_n$ can have order m:

(1) π might be a pq-cycle. Any such π has $p - 1 \sim n^{1/2}$ fixed points.
(2) π has cycle type $p^\mu q^\nu$ for some $\mu, \nu \geqslant 1$. There is some π of this type with no fixed points. Indeed, by the Frobenius postage stamp problem, any integer $x > pq-p-q$ is a positive linear combination of p and q. Since $n > pq-p-q$, there are $\mu, \nu \geqslant 0$ such that
$$n = \mu p + \nu q,$$
so an element of cycle type $p^\mu q^\nu$ has no fixed points.

The proportion of elements of the first type is
$$\frac{1}{pq(p-1)!} \approx \frac{1}{(n^{1/2})!}.$$
The proportion of elements of the second type is at most
$$\frac{1}{p^\mu \mu! q^\nu \nu! (n-\mu p-\nu q)!} \lesssim \frac{1}{(n^{1/2})!^2}.$$
Summing over μ, ν adds just another two factors of n, so almost all π of order m are pq-cycles. Therefore the probability that two random elements of order m generate is bounded away from 1.

Having moderated our expectations, we will prove the following positive results. Assume $m \in \operatorname{ord} S_n$.

(1) If m has a divisor d in the range $3 \leqslant d \leqslant o(n^{1/2})$, then two random elements of order m almost surely generate.
(2) If m is even and there is at least one $\pi \in S_n$ with $o(n^{1/2})$ fixed points and $o(n)$ 2-cycles, then two random elements of order m almost surely generate.
(3) If m is odd and there is at least one $\pi \in S_n$ with $O(n^{1/2})$ fixed points, then two random elements of order m generate with positive probability.
(4) If $m > 2$ is even, then two random elements of order m generate with positive probability.

The first two of these points are the content of Theorem 1.3; the latter two are the content of Theorem 1.4.

5.1. Theorem 1.3: Almost-sure generation.

To prove Theorem 1.3 we will use a map of conjugacy classes that turns d lots of fixed points into d-cycles, and another map which turns d lots of 2-cycles into 2 lots of d-cycles. This map is defined by the following lemma with $u \in \{1, 2\}$.

Lemma 5.6. *Let $u, d \leqslant n$ and let $k \geqslant 1$. If $\mathcal{C}$ is a conjugacy class of S_n with $c_u \geqslant kd$, define $\mathcal{C}'$ by replacing kd u-cycles by ku d-cycles, i.e.*

$$\begin{aligned} c'_u &= c_u - kd, \\ c'_d &= c_d + ku, \\ c'_j &= c_j \qquad \text{(all other } j\text{)}. \end{aligned}$$

The map $\mathcal{C} \mapsto \mathcal{C}'$ is a bijection from conjugacy classes with $c_u \geqslant kd$ to conjugacy classes with $c_d \geqslant ku$. Moreover, if $c_u \geqslant 2kd$,

$$\frac{|\mathcal{C}|}{|\mathcal{C}'|} \leqslant \left(\frac{(c_d + ku)^u d^u}{(kd)^d u^d}\right)^k \leqslant \left(\frac{n^u}{(kd)^d}\right)^k.$$

Proof. The claim that $\mathcal{C} \mapsto \mathcal{C}'$ is a bijection is clear from the definition. The second claim is a calculation:

$$\frac{|\mathcal{C}|}{|\mathcal{C}'|} = \frac{\prod_j c'_j! j^{c'_j}}{\prod_j c_j! j^{c_j}} = \frac{(c_u - kd)!(c_d + ku)! d^{ku}}{c_u! c_d! u^{kd}} \leqslant \frac{(c_d + ku)^{ku} d^{ku}}{(kd)^{kd} u^{kd}}.$$

For the last inequality, note that $(c_d + ku)d = c'_d d \leqslant n$. □

To prove the first part of Theorem 1.3 we must show that if m has a small divisor (other than 2) then almost all π of order m have $o(n^{1/2})$ fixed points and $o(n)$ 2-cycles. This is the content of the following lemma.

Lemma 5.7. *Assume m has a divisor d such that $3 \leqslant d \leqslant o(n^{1/2})$. Then almost all permutations of order m have $o(n^{1/2})$ fixed points and $o(n)$ 2-cycles.*

Proof. Let k be such that $n^{1/2}/\log n \leqslant kd \leqslant o(n^{1/2})$. We will show that almost all permutations of order m have at most $2kd = o(n^{1/2})$ fixed points. Use the map $\mathcal{C} \mapsto \mathcal{C}'$ from the previous lemma with $u = 1$. If $c_1 \geqslant 2kd$, we have

$$\frac{|\mathcal{C}|}{|\mathcal{C}'|} \leqslant \left(n^{-1/2+o(1)}\right)^k = o(1).$$

Therefore we have injectively associated to every conjugacy class of permutations of order m with $c_1 \geqslant 2kd$ some much larger conjugacy class of permutations of order m, so it follows that almost all $\pi \in S_n$ of order m have fewer than $2kd = o(n^{1/2})$ fixed points.

The proof for 2-cycles is the same, starting with k such that $n/\log n \leqslant kd \leqslant o(n)$. Use the map $\mathcal{C} \mapsto \mathcal{C}'$ from the previous lemma with $u = 2$. If $c_2 \geqslant 2kd$ then

$$\frac{|\mathcal{C}|}{|\mathcal{C}'|} \leqslant \left(\frac{n^2}{n^{3-o(1)}}\right)^k = o(1).$$

Hence almost all $\pi \in S_n$ of order m have fewer than $2kd = o(n)$ 2-cycles. □

Assume now m is even. Then we can prove the zero–one law suggested earlier.

Lemma 5.8. *Assume m is even, and assume there is an element of order m having $o(n^{1/2})$ fixed points and $o(n)$ 2-cycles. Then almost all elements of order m have the same property.*

Proof. If m has any small odd divisor, then we conclude by Lemma 5.7. Hence assume that m has no small odd divisors.

Apply Lemma 5.6 with $u = 1$ and $d = 2$, and $k = o(n^{1/2})$ to be chosen. Whenever $c_1 \geqslant 4k$ we have

$$\frac{|\mathcal{C}|}{|\mathcal{C}'|} \leqslant \left(\frac{c_2 + k}{(2k)^2}\right)^k.$$

This is small unless $c_2 \geqslant k^2$. This means that the number of permutations of order m with $c_1 \geqslant 4k$ is dominated by the number of permutations of order m with either $c_1 < 4k$ or $c_2 \geqslant k^2$. Hence it suffices to show that the permutations of order m with $c_2 \geqslant k^2$ make up $o(1)$ of the set of permutations of order m.

Note, from Cauchy's formula for the size of a conjugacy class, that the density of permutations with $c_2 \geqslant k^2$ is bounded by $1/(k^2)!$.

Let $\mathcal{C}_0$ be a conjugacy class of elements of order m having $o(n^{1/2})$ fixed points and $o(n)$ 2-cycles, which exists by hypothesis. Write a_j for the number of j-cycles. Since m has no small odd divisors, the elements of $\mathcal{C}_0$ have $o(n)$ cycles. Therefore

$$\frac{|\mathcal{C}_0|}{n!} = \frac{1}{\prod a_j! j^{a_j}} \geqslant \frac{1}{\prod (j a_j)^{a_j}} \geqslant n^{-o(n)}.$$

Therefore we can choose $k = o(n^{1/2})$ so that $1/(k^2)! = o(|\mathcal{C}_0|/n!)$. It follows that $\mathcal{C}_0$ is much bigger than the set of all permutations with $c_2 \geqslant k^2$, and this completes the proof. □

This completes the proof of Theorem 1.3.

5.2. Theorem 1.4: Positive-probability generation.

Now we investigate the conditions under which two random elements of order m generate with positive probability. We are able to give a complete characterization of this property.

Lemma 5.9. *Let $m \in \operatorname{ord} S_n$.*

(1) *Assume m is odd, and assume there exists a permutation of order m having $O(n^{1/2})$ fixed points. Then almost all permutations of order m have the same property.*

(2) *Assume $m \neq 2$ is even. Then almost all permutations of order m have $O(n^{1/2})$ fixed points and $n/2 - \Omega(n)$ 2-cycles.*

Proof. (1) Let d denote the smallest nontrivial divisor of m. If $d = o(n^{1/2})$, we conclude by Lemma 5.7. Assume then $d = \Omega(n^{1/2})$. By Cauchy's formula, the density of permutations having at least $bn^{1/2}$ fixed points (for some constant b) is at most $1/(bn^{1/2})!$. Moreover, if $\mathcal{C}_0$ is a conjugacy class of elements of order m having $O(n^{1/2})$ fixed points, then the elements of $\mathcal{C}_0$ have $O(n^{1/2})$ cycles, and

$$\frac{|\mathcal{C}_0|}{n!} \geqslant n^{-O(n^{1/2})}.$$

Thus if b is a sufficiently large constant then $|\mathcal{C}_0|/n!$ dominates $1/(bn^{1/2})!$, so indeed almost all elements of order m have $O(n^{1/2})$ fixed points.

(2) Let d denote the smallest divisor of m larger than 2. Note that d is either 4 or prime. As in part (1), we may assume $d = \Omega(n^{1/2})$. Applying Lemma 5.6 with $u = 2$ and $k = 1$, almost all elements of order m have at most $2d$ 2-cycles. On the other hand any element of order m must have a cycle of length at least d. Thus almost all permutations have at most $\min\{2d, (n-d)/2\}$ 2-cycles. This is at most $2n/5 = n/2 - \Omega(n)$, so the statement on 2-cycles is proved.

Regarding fixed points, we apply Lemma 5.6 with $u = 1$, $d = 2$, and $k = \lfloor n^{1/2} \rfloor$, getting

$$\frac{|\mathcal{C}|}{|\mathcal{C}'|} \leqslant \left(\frac{n}{4 \lfloor n^{1/2} \rfloor^2} \right)^{\lfloor n^{1/2} \rfloor} = o(1).$$

This shows that almost all elements of S_n of order m have at most $4n^{1/2}$ fixed points, and the proof is concluded. □

Theorem 1.4 follows immediately from this and Theorem 1.1.

References

[1] László Babai, *The probability of generating the symmetric group*, J. Combin. Theory Ser. A **52** (1989), no. 1, 148–153.

[2] László Babai and Thomas P. Hayes, *The probability of generating the symmetric group when one of the generators is random*, Publ. Math. Debrecen **69** (2006), no. 3, 271–280.

[3] Persi Diaconis, Jason Fulman, and Robert Guralnick, *On fixed points of permutations*, J. Algebraic Combin. **28** (2008), no. 1, 189–218.

[4] John D. Dixon, *The probability of generating the symmetric group*, Math. Z. **110** (1969), 199–205.

[5] Sean Eberhard, Kevin Ford, and Dimitris Koukoulopoulos, *Permutations contained in transitive subgroups*, Discrete Anal. (2016), Paper no. 12 (34 pages).

[6] Philippe Flajolet and Robert Sedgewick, *Analytic combinatorics*, Cambridge University Press, Cambridge, 2009.

[7] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl, *On the O'Nan–Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. Ser. A **44** (1988), no. 3, 389–396.

[8] Martin W. Liebeck and Aner Shalev, *Classical groups, probabilistic methods, and the* $(2,3)$*-generation problem*, Ann. of Math. (2) **144** (1996), no. 1, 77–125.

[9] ———, *Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks*, J. Algebra **276** (2004), no. 2, 552–601.

[10] Tomasz Łuczak and László Pyber, *On random generation of the symmetric group*, Combin. Probab. Comput. **2** (1993), no. 4, 505–512.

[11] Aner Shalev, *Random generation of simple groups by two conjugate elements*, Bull. London Math. Soc. **29** (1997), no. 5, 571–576.

Sean Eberhard, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, U.K.
E-mail : `eberhard@maths.cam.ac.uk`

Daniele Garzoni, Dipartimento di Matematica "Tullio Levi–Civita", Università degli Studi di Padova, Padova, Italy
E-mail : `daniele.garzoni@phd.unipd.it`