INVARIABLE GENERATION OF THE SYMMETRIC GROUP

SEAN EBERHARD, KEVIN FORD, AND BEN GREEN

Abstract. We say that permutations $\pi_1, \dots, \pi_r \in \mathcal{S}_n$ *invariably generate* $\mathcal{S}_n$ if, no matter how one chooses conjugates $\pi_1', \dots, \pi_r'$ of these permutations, $\pi_1', \dots, \pi_r'$ generate $\mathcal{S}_n$. We show that if π_1, π_2, π_3 are chosen randomly from $\mathcal{S}_n$ then, with probability tending to 1 as $n \to \infty$, they do not invariably generate $\mathcal{S}_n$. By contrast it was shown recently by Pemantle, Peres and Rivin that four random elements do invariably generate $\mathcal{S}_n$ with probability bounded away from zero. We include a proof of this statement which, while sharing many features with their argument, is short and completely combinatorial.

1. Introduction

Albeit by Dixon's theorem [3] two random elements π_1, π_2 of the symmetric group $\mathcal{S}_n$ generate at least the whole alternating group $\mathcal{A}_n$ with high probability[1] as $n \to \infty$, it is less clear how large the group generated by π_1', π_2' must be when π_1' and π_2' are allowed to be arbitrary conjugates of π_1 and π_2. Following Dixon [4] we say that a list $\pi_1, \dots, \pi_r \in \mathcal{S}_n$ has a property P *invariably* if $\pi_1', \dots, \pi_r'$ has property P whenever π_i' is conjugate to π_i for every i. How many random elements of $\mathcal{S}_n$ must we take before we expect them to invariably generate $\mathcal{S}_n$?

Several authors [2, 4, 7, 9, 11, 12] have already considered this question, owing to its connection with computational Galois theory. To briefly explain this connection, suppose we are given a polynomial $f \in \mathbb{Z}[x]$ of degree n with no repeated factors. Information about the Galois group can be gained by reducing f modulo various primes p and factorizing the reduced polynomial $\bar{f}$ over $\mathbb{Z}/p\mathbb{Z}$. By classical Galois theory, if $\bar{f}$ has irreducible factors of degrees $n_1, \dots, n_r$ then the Galois group G of f over $\mathbb{Q}$ has an element with cycle lengths $n_1, \dots, n_r$. Moreover by Frobenius's density theorem, if $G = \mathcal{S}_n$ then the frequency with which a given cycle type arises is equal to the proportion of elements in $\mathcal{S}_n$ with that cycle type. Thus if we suspect that $G = \mathcal{S}_n$ then the number of times we expect to have to iterate this procedure before proving that $G = \mathcal{S}_n$ is controlled by the expected number of random elements required to invariably generate $\mathcal{S}_n$.

BG is supported by ERC Starting Grant 279438 "Approximate Algebraic Structure" and a Simons Investigator Grant.

KF is supported by National Science Foundation grants DMS-1201442 and DMS-1501982.

[1] We adopt the convention that for a sequence of events E_n in finite probability spaces depending on some parameter n, "E_n occurs with high probability" means with $\mathbb{P}(E_n) \to 1$ as $n \to \infty$.

Łuczak and Pyber [9] were the first to prove the existence of a constant C such that C random permutations $\pi_1, \dots, \pi_C \in \mathcal{S}_n$ invariably generate $\mathcal{S}_n$ with probability bounded away from zero. Their method does not directly yield a reasonable value of C, but recently Pemantle, Peres, and Rivin [12] proved that we may take $C = 4$.

Theorem 1.1 (Pemantle–Peres–Rivin [12])**.** *If $\pi_1, \pi_2, \pi_3, \pi_4 \in \mathcal{S}_n$ are chosen uniformly at random then the probability that $\pi_1, \pi_2, \pi_3, \pi_4$ invariably generate $\mathcal{S}_n$ is bounded away from zero.*

Incidentally, Pemantle, Peres, and Rivin only prove that $\pi_1, \pi_2, \pi_3, \pi_4$ invariably generate a transitive subgroup of $\mathcal{S}_n$, but it is little more work to prove the theorem as stated above. We give a somewhat simplified proof of this theorem in Section 2. Our main contribution however is the lower bound $C > 3$, which will be proved in Section 3. Thus C can be taken as small as 4, but no smaller.

Theorem 1.2. *If $\pi_1, \pi_2, \pi_3 \in \mathcal{S}_n$ are chosen uniformly at random then the probability that π_1, π_2, π_3 invariably generate a transitive subgroup (or, in particular, all of $\mathcal{S}_n$) tends to zero as $n \to \infty$. Equivalently, with probability tending to 1 there is a positive integer $k < n$ such that π_1, π_2, π_3 each have a fixed set of size k.*

As in our recent paper [5], our main tool is the following model for the small-cycle structure of a random permutation; see for example Arratia and Tavaré [1].

Lemma 1.3. *Let $\mathbf{X} = (X_1, X_2, \dots)$ be a sequence of independent Poisson random variables, where X_j has parameter $1/j$. If c_j is the number of cycles of length j in a random permutation $\pi \in \mathcal{S}_n$, then if k is fixed and $n \to \infty$ the distribution of $(c_1, \dots, c_k)$ converges to that of $(X_1, \dots, X_k)$.*

The set of fixed-set sizes of a random permutation is thus modeled by the random sumset

$$\mathscr{L}(\mathbf{X}) = \left\{ \sum_{j \geqslant 1} j x_j : 0 \leqslant x_j \leqslant X_j \right\}. \tag{1.1}$$

Thus unsurprisingly the main task in proving Theorem 1.1 is to show that

$$\mathbb{P}\big(\mathscr{L}(\mathbf{X}) \cap \mathscr{L}(\mathbf{X}') \cap \mathscr{L}(\mathbf{X}'') \cap \mathscr{L}(\mathbf{X}''') = \{0\}\big) > 0, \tag{1.2}$$

where $\mathbf{X}', \mathbf{X}'', \mathbf{X}'''$ are independent copies of $\mathbf{X}$. Similarly, Theorem 1.2 follows almost immediately from

$$\mathbb{P}\big(\mathscr{L}(\mathbf{X}) \cap \mathscr{L}(\mathbf{X}') \cap \mathscr{L}(\mathbf{X}'') = \{0\}\big) = 0. \tag{1.3}$$

Ultimately, these assertions come down to the inequalities $\log 2 < \frac{3}{4}$ and $\frac{2}{3} < \log 2$ respectively, as we shall see in the course of the proofs.

These questions about permutations have analogues in number theory. Our proof of Theorem 1.2 is modeled after that of the well-known theorem of Maier and Tenenbaum [10] on the *propinquity of divisors*: a random integer n (selected from $\{1, \dots, x\}$ for large x) has two distinct divisors d, d' with $d < d' \leqslant 2d$ with high probability (as $x \to \infty$). In particular, we make heavy use of Riesz products, a device closely related to the sums $\sum_{d|n} d^{i\theta}$ that one sees frequently in the propinquity literature.

The Maier–Tenenbaum theorem itself corresponds more perfectly with the assertion that with high probability a random permutation π has, for some k with $0 < k < n$, two different fixed sets of size k (a true statement, but not one we establish here).

The number-theoretic analogue of Theorem 1.1 is a statement of the following kind: if x is large and if we select four random integers n_1, n_2, n_3, n_4 independently at random from $\{1, \dots, x\}$ then, with probability bounded below by an absolute constant, any divisors $d_1|n_1, d_2|n_2, d_3|n_3, d_4|n_4$ should have $\max d_i > 2 \min d_i$.

The number-theoretic analogue of Theorem 1.2 is a statement of the following kind: if x is large and if we select three random integers n_1, n_2, n_3 independently at random from $\{1, \dots, x\}$ then, with probability tending to 1 as $x \to \infty$, there exist divisors $d_1|n_1, d_2|n_2, d_3|n_3$ with $\max d_i < 2 \min d_i$.

Both of these number-theoretical statements were established nearly 20 years ago by Raouj and Stef [13]. In fact, rather more precise statements are established in that paper. We thank Gérald Tenenbaum for bringing this paper to our attention.

The analogous problem of determining the expected number of random elements required to invariable generatean arbitrary finite group has been considered in several recent papers [6, 7, 8].

Notation. Throughout we use standard $O(\cdot)$ and $o(\cdot)$ notation, as well as the Vinogradov notation $X \ll Y$ to mean $X = O(Y)$.

2. Four generators are enough

The principal result needed for the proof of Theorem 1.1 is the following proposition.

Proposition 2.1. *The following is true uniformly for integers k, n with $1 \leqslant k \leqslant n/2$. If $\pi_1, \pi_2, \pi_3, \pi_4 \in \mathcal{S}_n$ are chosen uniformly at random, then the probability that there is some $\ell \in (k/2, k]$ such that $\pi_1, \pi_2, \pi_3, \pi_4$ each fix a set of size ℓ is $O(k^{-c})$ for some $c > 0$.*

We begin with a tool for counting permutations with a given number of cycles of length at most k. By the Poisson model mentioned in the Introduction (Lemma 1.3), if k is fixed and $n \to \infty$, this statistic has distribution approaching that of $X_1 + \cdots + X_k$, a Poisson variable with parameter $h_k = 1 + \frac{1}{2} + \cdots + \frac{1}{k}$. The next result tells us that the distribution is still approximately Poisson uniformly over all choices of parameters k and n.

Lemma 2.2. *Let n, k, ℓ be integers with $n \geqslant k \geqslant 1$ and $\ell \geqslant 0$. Select $\pi \in \mathcal{S}_n$ at random. Then*

$$\mathbb{P}(\pi \textit{ has exactly } \ell \textit{ cycles with length} \leqslant k) \leqslant \frac{e}{k} \frac{(1 + \log k)^\ell}{\ell!} \left(1 + \frac{\ell}{1 + \log k}\right).$$

In particular if $\ell \ll \log k$ then this is $O\big((1+\log k)^{\ell}/k\ell!\big)$, while if $\ell \gg \log k$ then this is $O\big((1+\log k)^{\ell-1}/k(\ell-1)!\big)$.

Proof. Denote by $\mathcal{S}_n(k,\ell)$ the set of $\pi \in \mathcal{S}_n$ containing exactly ℓ cycles of length at most k. Evidently

$$n|\mathcal{S}_n(k,\ell)| = \sum_{\pi\in\mathcal{S}_n(k,\ell)} \sum_{\substack{\sigma|\pi \\ \sigma \text{ a cycle}}} |\sigma|.$$

Here the inner sum is over cycles σ which are factors of (i.e., contained in) π, and $|\sigma|$ denotes the length of σ. Write $\pi = \sigma\pi'$, and observe that π' has either $\ell-1$ or ℓ cycles of length at most k, depending on whether $|\sigma| \leqslant k$ or not. Thus $\pi' \in S_{n-|\sigma|}(k,m)$, where $m=\ell-1$ or $m=\ell$, so

$$\begin{aligned} n|\mathcal{S}_n(k,\ell)| &\leqslant \sum_{j=1}^{n} \sum_{m=\ell-1}^{\ell} \sum_{\pi'\in\mathcal{S}_{n-j}(k,m)} \sum_{\substack{\sigma\in\mathcal{S}_n, |\sigma|=j \\ \sigma \text{ a cycle}}} j \\ &= \sum_{j=1}^{n} \sum_{m=\ell-1}^{\ell} \sum_{\pi'\in\mathcal{S}_{n-j}(k,m)} \frac{n!}{(n-j)!}. \end{aligned}$$

Now rearrange the sum according the cycle type $(c_1,\dots,c_n)$ of the permutation π', i.e., π' has c_i cycles of length i for $1 \leqslant i \leqslant n$, and $c_1+2c_2+\cdots+nc_n = n-j$ if $\pi' \in \mathcal{S}_{n-j}$. The well known *Cauchy formula* states that the number of $\pi' \in \mathcal{S}_{n-j}$ with a given cycle type is $(n-j)!/\prod_i c_i! i^{c_i}$. It follows that

$$\begin{aligned} n|\mathcal{S}_n(k,\ell)| &\leqslant n! \sum_{j=1}^{n} \sum_{\substack{c_1,\dots,c_n \geqslant 0 \\ c_1+2c_2+\cdots+nc_n=n-j \\ c_1+\cdots+c_k \in \{\ell-1,\ell\}}} \frac{1}{\prod_i c_i! i^{c_i}} \\ &\leqslant n! \sum_{\substack{c_1,\dots,c_n \geqslant 0 \\ c_1+\cdots+c_k \in \{\ell-1,\ell\}}} \frac{1}{\prod_i c_i! i^{c_i}} \\ &= n! \left(\sum_{\substack{c_1,\dots,c_k \geqslant 0 \\ c_1+\cdots+c_k=\ell-1}} \frac{1}{\prod_i c_i! i^{c_i}} + \sum_{\substack{c_1,\dots,c_k \geqslant 0 \\ c_1+\cdots+c_k=\ell}} \frac{1}{\prod_i c_i! i^{c_i}} \right) \sum_{c_{k+1},\dots,c_n \geqslant 0} \frac{1}{\prod_{i=k+1}^{n} c_i! i^{c_i}} \\ &= n! \left(\frac{h_k^{\ell-1}}{(\ell-1)!} + \frac{h_k^{\ell}}{\ell!} \right) \prod_{k<i\leqslant n} e^{1/i}, \end{aligned}$$

where in the last line we used the multinomial theorem. The claimed bound now follows using the inequalities $h_k \leqslant 1 + \log k$ and

$$\sum_{k<i\leqslant n} \frac{1}{i} = h_n - h_k \leqslant \log n - \log k + 1. \qquad \square$$

In our paper [5] we showed that the probability of a random permutation $\pi \in \mathcal{S}_n$ fixing some set of size k is $k^{-\delta+o(1)}$, where $\delta = 1 - \frac{1+\log\log 2}{\log 2} \approx 0.086$. As noted in that paper, the main contribution to this estimate comes from rather exceptional permutations with an unexpectedly large number, $\approx \log k/\log 2$, of cycles of length $\leqslant k$. By contrast a typical permutation has $\approx \log k$ cycles of length $\leqslant k$. By restricting to this "quenched" regime[2] we can establish a much stronger bound.

Lemma 2.3. *Suppose that k, n are integers with $1 \leqslant k \leqslant n/2$, $0 < \varepsilon \leqslant 1/2$, and choose $\pi \in \mathcal{S}_n$ uniformly at random. Then the probability that π fixes a set of size k and has at most $(1+\varepsilon)\log k$ cycles of length at most k is at most $O(k^{\log 2 - 1 + 2\varepsilon})$.*

Proof. Fix $\ell \leqslant (1+\varepsilon)\log k$ and consider permutations π with exactly ℓ cycles of length at most k. If π fixes some set X, $|X| = k$, write $\pi_1 = \pi|_X$ and $\pi_2 = \pi|_{[n]\setminus X}$ for the induced permutations on X and its complement. Then π_1 has ℓ_1 cycles of length $\leqslant k$, and π_2 has ℓ_2 cycles of length $\leqslant k$, where $\ell_1 + \ell_2 = \ell$. By Lemma 2.2 the number of such π, for a given choice of X and ℓ_1, ℓ_2, is bounded by a constant times

$$\frac{(1+\log k)^{\ell_1}}{k\ell_1!} k! \cdot \frac{(1+\log k)^{\ell_2}}{k\ell_2!} (n-k)!,$$

which means that the probability we are interested in is bounded by a constant times

$$\sum_{\ell_1+\ell_2=\ell} \frac{1}{k^2} \frac{(1+\log k)^{\ell}}{\ell_1!\ell_2!} = \frac{2^{\ell}(1+\log k)^{\ell}}{k^2 \ell!}.$$

By summing over all $\ell \leqslant \ell_0 = \lfloor (1+\varepsilon)\log k \rfloor$ we get the bound

$$\begin{aligned} \frac{1}{k^2} \sum_{\ell \leqslant (1+\varepsilon)\log k} \frac{2^{\ell}(1+\log k)^{\ell}}{\ell!} &\ll \frac{1}{k^2} \frac{2^{\ell_0}(1+\log k)^{\ell_0}}{\ell_0!} \\ &\ll \frac{1}{k^2} (2e/(1+\varepsilon))^{(1+\varepsilon)\log k} \\ &\ll \frac{1}{k^{1-\log 2 - 2\varepsilon}}. \qquad \square \end{aligned}$$

Proof of Proposition 2.1. Let $\varepsilon > 0$ be small and fixed. First we will use Lemma 2.2 to bound the probability that one of $\pi_1, \pi_2, \pi_3, \pi_4$ has more than $\ell_0 = \lfloor (1+\varepsilon)\log k \rfloor$ cycles of

[2] The terminology is from [12] and apparently comes from statistical physics.

length at most k. By that lemma, for each $\ell \geqslant \ell_0$, the probability that π_1 has ℓ cycles of length at most k is bounded by

$$O\left(\frac{(1+\log k)^{\ell-1}}{k(\ell-1)!}\right),$$

so the probability that π_1 has more than ℓ_0 cycles is bounded by a constant times

$$\sum_{\ell>\ell_0}\frac{(1+\log k)^{\ell-1}}{k(\ell-1)!} \ll \frac{(1+\log k)^{\ell_0-1}}{k(\ell_0-1)!} \ll \frac{1}{k}\left(\frac{e(1+\log k)}{\ell_0-1}\right)^{\ell_0-1} \ll \frac{1}{k}\left(\frac{e}{1+\varepsilon}\right)^{(1+\varepsilon)\log k}.$$

Now by a Taylor expansion of $-1+(1+\varepsilon)\log(e/(1+\varepsilon))$, this is bounded by $O(k^{-\varepsilon^2/3})$ if $\varepsilon \leqslant \frac{1}{2}$. Thus the probability that one of $\pi_1, \pi_2, \pi_3, \pi_4$ has more than ℓ_0 cycles of length at most k is also bounded by $O(k^{-\varepsilon^2/3})$.

On the other hand, by Lemma 2.3, for each $\ell \in (k/2, k]$ the probability that π_i has at most $(1+\varepsilon)\log k$ cycles of length at most k and fixes a set of size ℓ is at most $k^{\log 2-1+2\varepsilon}$. Thus the probability that $\pi_1, \pi_2, \pi_3, \pi_4$ each have at most $(1+\varepsilon)\log k$ cycles of length at most k and each fix a set of the same size ℓ for some $\ell \in (k/2, k]$ is at most $k^{1+4(\log 2-1+2\varepsilon)}$. Since $1+4(\log 2-1)<0$, we have $1+4(\log 2-1+2\varepsilon)<0$ if ε is small enough ($\varepsilon = 1/40$ works), and so the theorem holds with

$$c = \min(\varepsilon^2/3, -1-4(\log 2-1+2\varepsilon)). \qquad \square$$

An immediate corollary of Proposition 2.1 is obtained by fixing k, letting $n \to \infty$, and recalling the Poisson model (Lemma 1.3) and the definition (1.1) of $\mathscr{L}(\mathbf{X})$.

Corollary 2.4. *For any $k \geqslant 2$, the probability that $\mathscr{L}(\mathbf{X}) \cap \mathscr{L}(\mathbf{X}') \cap \mathscr{L}(\mathbf{X}'') \cap \mathscr{L}(\mathbf{X}''')$ contains an integer $\ell \in (k/2, k]$ is $O(k^{-c})$, for some $c > 0$.*

Remark. If one wished to prove only this, we could substitute Lemma 2.2 with a corresponding bound for $\mathbb{P}(X_1 + \cdots + X_k \leqslant \ell)$, which follows very quickly from the fact that $X_1 + \cdots + X_k$ is Poisson with parameter h_k.

Corollary 2.5. *$\mathscr{L}(\mathbf{X}) \cap \mathscr{L}(\mathbf{X}') \cap \mathscr{L}(\mathbf{X}'') \cap \mathscr{L}(\mathbf{X}''')$ is almost surely finite, and equal to $\{0\}$ with positive probability.*

Proof. Let F_k be the event that

$$\mathscr{L}(\mathbf{X}) \cap \mathscr{L}(\mathbf{X}') \cap \mathscr{L}(\mathbf{X}'') \cap \mathscr{L}(\mathbf{X}''') \cap (k, \infty)$$

is nonempty. By applying Corollary 2.4 with k replaced by $2^j k$, $j \in \mathbb{N}$, and summing the geometric series, we obtain $\mathbb{P}(F_k) \ll k^{-c}$ for $k \geqslant 1$. In particular $\mathbb{P}(F_k) \to 0$, so $\mathbb{P}\left(\bigcap F_k\right) = 0$, so the first part of the corollary holds. For the second part, fix k_0 such that $\mathbb{P}(F_{k_0}) < 1$.

Then

$$\begin{aligned}\mathbb{P}\left(\mathscr{L}(\mathbf{X})\cap\mathscr{L}(\mathbf{X}')\cap\mathscr{L}(\mathbf{X}'')\cap\mathscr{L}(\mathbf{X}''')=\{0\}\right) &\geqslant \mathbb{P}(X_j=0 \text{ for all } j\leqslant k_0, \text{ and } F_{k_0}^c)\\ &\geqslant \mathbb{P}(X_j=0 \text{ for all } j\leqslant k_0)\,\mathbb{P}(F_{k_0}^c)\\ &> 0.\end{aligned}$$

The second inequality here is a simple case of the FKG inequality [14, Theorem 1.19]. To see the inequality directly, define $\mathbf{X}^*=(X_1^*,X_2^*,\dots)$ by putting $X_j^*=X_j$ if $j>k_0$ and $X_j^*=0$ if $j\leqslant k_0$, and let $F_{k_0}^*$ be the event that

$$\mathscr{L}(\mathbf{X}^*)\cap\mathscr{L}(\mathbf{X}')\cap\mathscr{L}(\mathbf{X}'')\cap\mathscr{L}(\mathbf{X}''')\cap(k_0,\infty)$$

is nonempty. Clearly $F_{k_0}^*$ implies F_{k_0}, so

$$\begin{aligned}\mathbb{P}(X_j=0 \text{ for all } j\leqslant k_0, \text{ and } F_{k_0}^c) &= \mathbb{P}(X_j=0 \text{ for all } j\leqslant k_0, \text{ and } F_{k_0}^{*c})\\ &= \mathbb{P}(X_j=0 \text{ for all } j\leqslant k_0)\,\mathbb{P}(F_{k_0}^{*c})\\ &\geqslant \mathbb{P}(X_j=0 \text{ for all } j\leqslant k_0)\,\mathbb{P}(F_{k_0}^c).\end{aligned}$$ □

Shortly we will complete the proof of Theorem 1.1. In the proof, we will need a trick to deal with the possibility that $\pi_1,\pi_2,\pi_3,\pi_4\in\mathcal{A}_n$. The following lemma is helpful in this regard. It shows that random even and random odd permutations have the same small-cycle structure as random permutations with unconstrained parity (Lemma 1.3).

Lemma 2.6. *Let $\pi\in\mathcal{S}_n$ be a random even permutation, and let $c_j(\pi)$ be the number of cycles of length j. Fix $k\in\mathbb{N}$. Then as $n\to\infty$ the distribution of $(c_1(\pi),\dots,c_k(\pi))$ converges to that of $(X_1,\dots,X_k)$. The same is true if π is a random odd permutation.*

Proof. Choose $\pi\in\mathcal{S}_n$ uniformly at random, and define σ by putting $\sigma=1$ if π is even and $\sigma=(12)$ if π is odd. Then $\pi\sigma$ is uniformly distributed over $\mathcal{A}_n$. By Lemma 1.3, as $n\to\infty$, the number of cycles in π of length at most $2k$ approaches a Poisson distribution with parameter $h_{2k}\leqslant 1+\log 2k$. Thus, with high probability (as $n\to\infty$) the total number of points in cycles of π of length at most $2k$ is at most $2k\log n$, so with high probability each of these cycles is disjoint from (12). That is, the points 1 and 2 are both contained in cycles of π of length at least $2k+1$ with high probability. Now consider the probability that 1 and 2 are both contained in the same cycle and are close together. For each $\ell\geqslant 2k+1$, the number of cycles of length ℓ containing both 1 and 2, which are a distance $\leqslant k$ from each other, equals $\binom{n-2}{\ell-2}2k(\ell-2)!$. Hence, the number of permutations π containing such a cycle is at most

$$\sum_{2k+1\leqslant\ell\leqslant n} 2k(n-2)!\leqslant 2k(n-1)!.$$

Hence, with high probability, if 1 and 2 are in the same cycle they are a distance at least $k+1$ from each other. Thus, with high probability, $c_j(\pi\sigma)=c_j(\pi)$ for each $j\leqslant k$. Similarly $\pi\sigma(12)$ is uniformly distributed over odd permutations, and with high probability $c_j(\pi\sigma(12))=c_j(\pi)$. □

Proof of Theorem 1.1. Let $\pi_1, \pi_2, \pi_3, \pi_4 \in \mathcal{S}_n$ be random permutations with π_1 odd. Let $E_{n,k}$ be the event that $\pi_1, \pi_2, \pi_3, \pi_4$ each fix a set of size ℓ for some ℓ in the range $1 \leqslant \ell \leqslant k$, and let $F_{n,k}$ be the event that $\pi_1, \pi_2, \pi_3, \pi_4$ each fix a set of size ℓ for some ℓ in the range $k < \ell \leqslant n/2$. By Proposition 2.1 (and summing a geometric series as in the proof of Corollary 2.5) we have $\mathbb{P}(F_{n,k}) \ll k^{-c}$ uniformly for $1 \leqslant k \leqslant n/2$, while by Corollary 2.5 and Lemma 2.6 we have $\lim_{n\to\infty} \mathbb{P}(E_{n,k}) \leqslant 1 - \delta$ for all k, for some constant $\delta > 0$. Fix k_0 such that $\mathbb{P}(F_{n,k_0}) \leqslant \delta/3$ for all $n \geqslant 2k_0$. Then $\mathbb{P}(E_{n,k_0}) + \mathbb{P}(F_{n,k_0}) \leqslant 1 - \delta/3$ for all sufficiently large n, so we deduce that with probability bounded away from zero $\pi_1, \pi_2, \pi_3, \pi_4$ do not fix sets of the same size ℓ for any $\ell \in [1, n/2]$.

Thus with probability bounded away from zero $\pi_1, \pi_2, \pi_3, \pi_4$ invariably generate a transitive subgroup of $\mathcal{S}_n$. However by the Łuczak–Pyber theorem [9], π_1 is, with high probability, not contained in any transitive subgroup smaller than $\mathcal{A}_n$. Since $\pi_1 \notin \mathcal{A}_n$, with probability bounded away from zero $\pi_1, \pi_2, \pi_3, \pi_4$ invariably generate $\mathcal{S}_n$. □

3. Three generators are not enough

Theorem 1.2 follows immediately from the following more specific proposition.

Proposition 3.1. *For every $\varepsilon > 0$ there exists $k_0 = k_0(\varepsilon)$ and $n_0 = n_0(\varepsilon)$ such that if $n \geqslant n_0$ then with probability at least $1 - \varepsilon$ there is some $\ell \leqslant k_0$ such that π_1, π_2, π_3 each fix a set of size ℓ.*

Let $\mathbf{X}$ be defined as before, and let $\mathbf{Y}$ and $\mathbf{Z}$ be independent copies of $\mathbf{X}$. For I an interval in $\mathbb{N}$ let

$$\mathscr{L}(I, \mathbf{X}) = \left\{ \sum_{j\in I} j x_j : 0 \leqslant x_j \leqslant X_j \right\},$$

and define $\mathscr{L}(I, \mathbf{Y})$ and $\mathscr{L}(I, \mathbf{Z})$ analogously.

Lemma 3.2. *Let $I = \{1, \dots, k\}$ and let $\varepsilon > 0$. Then with probability at least $1 - \varepsilon$ we have $\mathscr{L}(I, \mathbf{X}), \mathscr{L}(I, \mathbf{Y}), \mathscr{L}(I, \mathbf{Z}) \subset [0, 3\varepsilon^{-1}k]$.*

Proof. Since $\mathbb{E}\sum_{j\in I} jX_j = |I| = k$, by Markov's inequality we have $\sum_{j\in I} jX_j \leqslant 3\varepsilon^{-1}k$ with probability at least $1 - \varepsilon/3$. Similarly $\sum_{j\in I} jY_j \leqslant 3\varepsilon^{-1}k$ and $\sum_{j\in I} jZ_j \leqslant 3\varepsilon^{-1}k$ each with probability at least $1 - \varepsilon/3$, and the lemma follows. □

Lemma 3.3. *Fix ε, $0 < \varepsilon < 1/2$. There is a constant $C(\varepsilon)$ so that with probability at least $1 - \varepsilon$ we have*

$$\begin{aligned}\sum_{m<j\leqslant k} X_j &\geqslant 0.99\log(k/m) - C(\varepsilon),\\ \sum_{m<j\leqslant k} Y_j &\geqslant 0.99\log(k/m) - C(\varepsilon), \text{ and}\\ \sum_{m<j\leqslant k} Z_j &\geqslant 0.99\log(k/m) - C(\varepsilon).\end{aligned}$$

for every nonnegative integer $m \leqslant k$.

Proof. Let $C = C(\varepsilon)$ be a constant whose properties will be specified later. It suffices to show that the first inequality holds for all $m \leqslant k$ with probability at least $1 - \varepsilon/3$. There is nothing to prove if $m \geqslant e^{-C}k$, so we may suppose $m \leqslant e^{-C}k$. We may also suppose that $C \geqslant 1$.

Let E be the event that

$$\sum_{m<j\leqslant k} X_j \geqslant 0.99\log(k/m) - 1$$

for all $m \leqslant e^{-C}k$. Suppose E fails, say

$$\sum_{m<j\leqslant k} X_j < 0.99\log(k/m) - 1$$

for some $m \leqslant e^{-C}k$. Writing m' for the smallest power of 2 with $m' > m$, we thus have

$$\sum_{m'<j\leqslant k} X_j \leqslant \sum_{m<j\leqslant k} X_j \leqslant 0.99\log(k/m) - 1 \leqslant 0.99\log(k/m').$$

Thus

$$1_{E^c} \leqslant \sum_{\substack{m'\leqslant 2e^{-C}k\\ \text{dyadic}}} 0.99^{\sum_{m'<j\leqslant k} X_j - 0.99\log(k/m')}.$$

Whenever P is Poisson of parameter λ and $a > 0$ we have $\mathbb{E}a^P = e^{(a-1)\lambda}$, and the sum $\sum_{m'<j\leqslant k} X_j$ is Poisson with parameter $\sum_{m'<j\leqslant k} 1/j = \log(k/m') + O(1)$, so

$$\begin{aligned}\mathbb{P}(E^c) &\ll \sum_{\substack{m'\leqslant 2e^{-C}k\\ \text{dyadic}}} \exp\left((0.99 - 1 - 0.99\log(0.99))\log(k/m')\right)\\ &\leqslant \sum_{\substack{m'\leqslant 2e^{-C}k\\ \text{dyadic}}} (k/m')^{-0.00005}\\ &\ll e^{-0.00005C}.\end{aligned}$$

Therefore, $\mathbb{P}(E^c) \leqslant \varepsilon/3$ if C is taken large enough. □

We need a standard estimate for the partial sums of the Fourier series $\sum_{j=1}^{\infty}\frac{\cos(2\pi j\theta)}{j} = -\log|2\sin(\pi\theta)|$. Denote by $\|x\|$ the distance from x to $\mathbb{Z}$.

Lemma 3.4.

$$\sum_{j\leqslant m}\frac{\cos(2\pi j\theta)}{j} = \log\min\left(\frac{1}{\|\theta\|}, m\right) + O(1) \quad \textit{for } \|\theta\| > 0.$$

Proof. We may assume that $0 < \theta \leqslant \frac{1}{2}$. Using the bound $\cos(2\pi j\theta) = 1 + O(j^2\theta^2)$, we get

$$\sum_{j\leqslant\min(m,1/\theta)}\frac{\cos(2\pi j\theta)}{j} = \log\min(m, 1/\theta) + O(1).$$

This proves the lemma if $\|\theta\| \leqslant 1/m$. Suppose, then, that $\|\theta\| > 1/m$. Set

$$S_j = \sum_{n=0}^{j} e^{2\pi i n\theta},$$

and note that by summing the geometric series we have

$$S_j = \frac{e^{2\pi i j\theta} - 1}{e^{2\pi i\theta} - 1} \ll \frac{1}{\theta}. \tag{3.1}$$

Thus (by "Abel summation"),

$$\begin{aligned}\sum_{1/\theta<j\leqslant m}\frac{\cos(2\pi j\theta)}{j} &= \Re\sum_{1/\theta<j\leqslant m}\frac{e^{2\pi i j\theta}}{j} = \Re\sum_{1/\theta<j\leqslant m}\frac{S_j - S_{j-1}}{j}\\ &= \Re\sum_{1/\theta<j\leqslant m-1}\frac{S_j}{j(j+1)} + \frac{S_m}{m} - \frac{S_{\lceil 1/\theta\rceil - 1}}{\lceil 1/\theta\rceil}.\end{aligned}$$

The latter two terms here are $O(1)$ by the trivial bound $|S_j| \leqslant j$, while from (3.1) the sum is bounded by a constant times

$$\frac{1}{\theta}\sum_{j>1/\theta}\frac{1}{j^2} \ll 1. \qquad \square$$

Let $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ be the unit torus, and denote $e(z) = e^{2\pi i z}$. Given $I, \mathbf{X}, \mathbf{Y}, \mathbf{Z}$ define $F : \mathbb{T}^2 \to \mathbb{C}$ by

$$F(\boldsymbol{\theta}) = \prod_{j\in I}\left(\frac{1+e(j\theta_1)}{2}\right)^{X_j}\left(\frac{1+e(j\theta_2)}{2}\right)^{Y_j}\left(\frac{1+e(j(-\theta_1-\theta_2))}{2}\right)^{Z_j}.$$

By expanding the product we see that $\hat{F} : \mathbb{Z}^2 \to \mathbb{C}$ is supported on the set

$$S(I, \mathbf{X}, \mathbf{Y}, \mathbf{Z}) = \{(n_1 - n_3, n_2 - n_3) : n_1 \in \mathscr{L}(I, \mathbf{X}), n_2 \in \mathscr{L}(I, \mathbf{Y}), n_3 \in \mathscr{L}(I, \mathbf{Z})\}. \tag{3.2}$$

Since $\sum_{a\in\mathbb{Z}^2}\hat{F}(a)=F(0)=1$, by Cauchy–Schwarz we have

$$1=\Big(\sum_{a\in\mathbb{Z}^2}\hat{F}(a)\Big)^2\leqslant\Big(\sum_{a:\hat{F}(a)\neq 0}1\Big)\sum_{a\in\mathbb{Z}^2}|\hat{F}(a)|^2\leqslant|S(I,\mathbf{X},\mathbf{Y},\mathbf{Z})|\sum_{a\in\mathbb{Z}^2}|\hat{F}(a)|^2.$$

Applying Parseval, we get

$$|S(I,\mathbf{X},\mathbf{Y},\mathbf{Z})|\geqslant\Big(\sum_{a\in\mathbb{Z}^2}|\hat{F}(a)|^2\Big)^{-1}=\Big(\int_{\mathbb{T}^2}|F(\boldsymbol{\theta})|^2\,d\boldsymbol{\theta}\Big)^{-1}. \tag{3.3}$$

Lemma 3.5. *Let*

$$\beta=1-\frac{2}{3\log 2}-0.02\approx 0.0182,$$

and let $I=(k^\beta,k]$. Fix $\varepsilon\in(0,1/2)$, and let $E=E(\varepsilon)$ be the event from Lemma 3.3. Then both of the bounds

$$\mathbb{E}1_E|F(\boldsymbol{\theta})|^2\ll_\varepsilon(k\|\theta_1\|^{1/3}\|\theta_2\|^{1/3}\|\theta_3\|^{1/3})^{-2.02} \tag{3.4}$$

and

$$\mathbb{E}1_E|F(\boldsymbol{\theta})|^2\ll_\varepsilon(k\|\theta_i\|^{1/2}\|\theta_j\|^{1/2})^{-1.3}\quad(\{i,j\}\subset\{1,2,3\}) \tag{3.5}$$

hold uniformly for $\boldsymbol{\theta}\in\mathbb{T}^2$, where $\theta_3=-\theta_1-\theta_2$. The expectation is over $\mathbf{X},\mathbf{Y},\mathbf{Z}$.

Proof. Define, for $i\in\{1,2,3\}$,

$$k_i=\begin{cases}k^\beta & \text{if } \|\theta_i\|\geqslant k^{-\beta};\\ 1/\|\theta_i\| & \text{if } 1/k<\|\theta_i\|<k^{-\beta};\\ k & \text{if } \|\theta_i\|\leqslant 1/k.\end{cases}$$

It is useful to note the (slightly crude) bound

$$k_i\leqslant\frac{k^\beta}{\|\theta_i\|^{1-\beta}}, \tag{3.6}$$

which follows by an analysis of the three cases in the definition of k_i. If E holds then

$$\sum_{k_1<j\leqslant k}X_j+\sum_{k_2<j\leqslant k}Y_j+\sum_{k_3<j\leqslant k}Z_j\geqslant 0.99\log(k^3/(k_1k_2k_3))-C(\varepsilon),$$

so

$$1_E|F(\boldsymbol{\theta})|^2\ll_\varepsilon(k^3/k_1k_2k_3)^{-0.99\log 2}|F(\boldsymbol{\theta})|^2 2^{\sum_{k_1<j\leqslant k}X_j+\sum_{k_2<j\leqslant k}Y_j+\sum_{k_3<j\leqslant k}Z_j}.$$

From (3.6) and the inequality $3\times 0.99\log 2\times(1-\beta)>2.02$, we deduce that

$$1_E|F(\boldsymbol{\theta})|^2\ll_\varepsilon(k\|\theta_1\|^{1/3}\|\theta_2\|^{1/3}\|\theta_3\|^{1/3})^{-2.02}|F(\boldsymbol{\theta})|^2 2^{\sum_{k_1<j\leqslant k}X_j+\sum_{k_2<j\leqslant k}Y_j+\sum_{k_3<j\leqslant k}Z_j}.$$

Thus (3.4) will follow if we can prove

$$\mathbb{E}|F(\boldsymbol{\theta})|^2 2^{\sum_{k_1<j\leqslant k}X_j+\sum_{k_2<j\leqslant k}Y_j+\sum_{k_3<j\leqslant k}Z_j}\ll 1. \tag{3.7}$$

Similarly, from (3.6) for $i = 1, 2$ and the trivial bound $k_3 \leqslant k$, and using $2 \times 0.99 \log 2 \times (1 - \beta) > 1.3$, we deduce that

$$1_E |F(\boldsymbol{\theta})|^2 \ll_\varepsilon (k\|\theta_1\|^{1/2}\|\theta_2\|^{1/2})^{-1.3} |F(\boldsymbol{\theta})|^2 2^{\sum_{k_1<j\leqslant k} X_j + \sum_{k_2<j\leqslant k} Y_j + \sum_{k_3<j\leqslant k} Z_j},$$

and similarly for other permutations of the indices $1, 2, 3$, so (3.5) will also follow from (3.7).

It remains only to prove (3.7). We have a factorization

$$\begin{aligned}
&\mathbb{E}|F(\boldsymbol{\theta})|^2 2^{\sum_{k_1<j\leqslant k} X_j + \sum_{k_2<j\leqslant k} Y_j + \sum_{k_3<j\leqslant k} Z_j} \\
&\qquad = \prod_{k^\beta < j \leqslant k_1} \mathbb{E}\left|\frac{1+e(j\theta_1)}{2}\right|^{2X_j} \prod_{k_1<j\leqslant k} \mathbb{E}\left(2\left|\frac{1+e(j\theta_1)}{2}\right|^2\right)^{X_j} \\
&\qquad \times \prod_{k^\beta < j \leqslant k_2} \mathbb{E}\left|\frac{1+e(j\theta_2)}{2}\right|^{2Y_j} \prod_{k_2<j\leqslant k} \mathbb{E}\left(2\left|\frac{1+e(j\theta_2)}{2}\right|^2\right)^{Y_j} \\
&\qquad \times \prod_{k^\beta < j \leqslant k_3} \mathbb{E}\left|\frac{1+e(j\theta_3)}{2}\right|^{2Z_j} \prod_{k_3<j\leqslant k} \mathbb{E}\left(2\left|\frac{1+e(j\theta_3)}{2}\right|^2\right)^{Z_j}.
\end{aligned}$$

By using again the calculation $\mathbb{E}a^P = e^{(a-1)\lambda}$ for P Poisson with parameter λ, we get

$$\begin{aligned}
&\mathbb{E}|F(\boldsymbol{\theta})|^2 2^{\sum_{k_1<j\leqslant k} X_j + \sum_{k_2<j\leqslant k} Y_j + \sum_{k_3<j\leqslant k} Z_j} \\
&\quad = \exp \sum_{i=1}^3 \left(\sum_{k^\beta<j\leqslant k_i} \frac{1}{j}\left(\left|\frac{1+e(j\theta_i)}{2}\right|^2 - 1\right) + \sum_{k_i<j\leqslant k} \frac{1}{j}\left(2\left|\frac{1+e(j\theta_i)}{2}\right|^2 - 1\right)\right) \\
&\quad = \exp \sum_{i=1}^3 \left(\sum_{k^\beta<j\leqslant k_i} \frac{\cos(2\pi j\theta_i) - 1}{2j} + \sum_{k_i<j\leqslant k} \frac{\cos(2\pi j\theta_i)}{j}\right) \\
&\quad = \exp \sum_{i=1}^3 \left(\frac{1}{2}\log\frac{\min(k_i, 1/\|\theta_i\|)}{\min(k^\beta, 1/\|\theta_i\|)} - \frac{1}{2}\log\frac{k_i}{k^\beta} + \log\frac{\min(k, 1/\|\theta_i\|)}{\min(k_i, 1/\|\theta_i\|)} + O(1)\right)
\end{aligned}$$

by Lemma 3.4. Checking the three cases in the definition of k_i separately, it can be confirmed that this is always $O(1)$. □

Corollary 3.6. *With notation as in Lemma 3.5, we have*

$$\int_{\mathbb{T}^2} \mathbb{E}1_E |F(\boldsymbol{\theta})|^2 \, d\boldsymbol{\theta} \ll_\varepsilon k^{-2}. \tag{3.8}$$

Proof. Divide $\mathbb{T}^2$ into three regions R_1, R_2, R_3 as follows:

$$\begin{aligned}
R_1 &= \{\boldsymbol{\theta} \in \mathbb{T}^2 : \|\theta_i\| \geqslant 1/k \text{ for all three } i \in \{1,2,3\}\}, \\
R_2 &= \{\boldsymbol{\theta} \in \mathbb{T}^2 : \|\theta_i\| \geqslant 1/k \text{ for exactly two } i \in \{1,2,3\}\}, \\
R_3 &= \{\boldsymbol{\theta} \in \mathbb{T}^2 : \|\theta_i\| \geqslant 1/k \text{ for at most one } i \in \{1,2,3\}\}.
\end{aligned}$$

We will bound the integral differently in each region.

Further subdivide R_1 according to which of $\|\theta_1\|, \|\theta_2\|, \|\theta_3\|$ is largest. In the subregion R_1' in which say $\|\theta_1\|$ is largest we have $\|\theta_1\| \geqslant \|\theta_2\|^{1/2}\|\theta_3\|^{1/2}$, so by (3.4) we have

$$\begin{aligned}\int_{R_1'} \mathbb{E}1_E|F(\boldsymbol{\theta})|^2\,d\boldsymbol{\theta} &\ll_\varepsilon \int_{R_1} (k\|\theta_2\|^{1/2}\|\theta_3\|^{1/2})^{-2.02}\,d\boldsymbol{\theta}\\ &= \left(\int_{\|\theta\|\geqslant 1/k} (k\|\theta\|)^{-1.01}\,d\theta\right)^2\\ &\asymp k^{-2}.\end{aligned}$$

We can bound the integral over the other subregions in the same way, so the integral over R_1 is indeed $\ll_\varepsilon k^{-2}$.

Similarly, subdivide R_2 according to the relative order of $\|\theta_1\|, \|\theta_2\|, \|\theta_3\|$, and focus for the moment on the subregion R_2' in which $\|\theta_1\| \leqslant \|\theta_2\| \leqslant \|\theta_3\|$. This implies in particular that $\|\theta_1\| \leqslant 1/k$ while $\|\theta_2\| \geqslant 1/k$. Thus by (3.5) with $i = 2$ and $j = 3$ we have

$$\int_{R_2'} \mathbb{E}1_E|F(\boldsymbol{\theta})|^2\,d\boldsymbol{\theta} \ll_\varepsilon \int_{R_2'} (k\|\theta_2\|)^{-1.3}\,d\boldsymbol{\theta} \asymp k^{-2}.$$

Again we can bound the integral over the other subregions in the same way, so the integral over R_2 is also $\ll_\varepsilon k^{-2}$.

Finally, in the region R_3 note that because $\theta_1 + \theta_2 + \theta_3 = 0$ we must have $\|\theta_i\| < 2/k$ for each i. Thus from the trivial bound $|F(\boldsymbol{\theta})| \leqslant 1$ we have

$$\int_{R_3} \mathbb{E}1_E|F(\boldsymbol{\theta})|^2\,d\boldsymbol{\theta} \leqslant \int_{R_3} 1 \asymp k^{-2}.$$ □

Recall the definition of $S(I, \mathbf{X}, \mathbf{Y}, \mathbf{Z})$, given in (3.2).

Proposition 3.7. *Let $I = (k^\beta, k]$. There is a constant $c > 0$ such that with probability at least $1/2$ we have $S(I, \mathbf{X}, \mathbf{Y}, \mathbf{Z}) \subset [-10k, 10k]^2$ and $|S(I, \mathbf{X}, \mathbf{Y}, \mathbf{Z})| \geqslant ck^2$.*

Proof. Apply Lemma 3.3 with $\varepsilon = 0.01$, and let E be the resulting event. By Corollary 3.6 (and interchanging the order of integration and expectation) we have

$$\mathbb{E}1_E \int_{\mathbb{T}^2} |F(\boldsymbol{\theta})|^2\,d\boldsymbol{\theta} \ll k^{-2}.$$

Thus by Markov's inequality there is a constant C such that $1_E \int_{\mathbb{T}^2} |F(\boldsymbol{\theta})|^2\,d\boldsymbol{\theta} \leqslant Ck^{-2}$ with probability at least 0.99. Since $\mathbb{P}(E) \geqslant 0.99$ we deduce that $\int_{\mathbb{T}^2} |F(\boldsymbol{\theta})|^2\,d\boldsymbol{\theta} \leqslant Ck^{-2}$ with probability at least 0.98. Applying (3.3), we have $|S(I, \mathbf{X}, \mathbf{Y}, \mathbf{Z})| \geqslant C^{-1}k^2$ with probability at least 0.98.

On the other hand, by Lemma 3.2 with $\varepsilon = 1/3$ we have $S(I, \mathbf{X}, \mathbf{Y}, \mathbf{Z}) \subset [-10k, 10k]^2$ with probability at least 2/3, so we must have both $S(I, \mathbf{X}, \mathbf{Y}, \mathbf{Z}) \subset [-10k, 10k]^2$ and $|S(I, \mathbf{X}, \mathbf{Y}, \mathbf{Z})| \geqslant C^{-1}k^2$ with probability at least $1 - 1/3 - 0.02 \geqslant 1/2$. □

Proposition 3.8. *Let $I = (k^\beta, 60k]$. Then with probability bounded away from zero we can find $(x_j)_{j\in I}, (y_j)_{j\in I}, (z_j)_{j\in I}$ not all zero such that $0 \leqslant x_j \leqslant X_j$, $0 \leqslant y_j \leqslant Y_j$, and $0 \leqslant z_j \leqslant Z_j$ for each $j \in I$ and*

$$\sum_{j\in I} jx_j = \sum_{j\in I} jy_j = \sum_{j\in I} jz_j.$$

Proof. Let $I' = (k^\beta, k]$. By Proposition 3.7, with probability at least 1/2 we have

$$S(I', \mathbf{X}, \mathbf{Y}, \mathbf{Z}) \subset [-10k, 10k]^2$$

and $|S(I', \mathbf{X}, \mathbf{Y}, \mathbf{Z})| \gg k^2$. This event depends only on X_j, Y_j, Z_j for $j \leqslant k$, so independently with probability at least 1/2 we can find $j_3 \in (20k, 50k]$ such that $Z_{j_3} > 0$, as

$$\mathbb{P}(Z_j = 0 \text{ for all } j \in (20k, 50k]) = \prod_{j\in(20k,50k]} e^{-1/j} \leqslant 1/2. \tag{3.9}$$

Given such a j_3 the set T of pairs of integers (j_1, j_2) such that $10k < j_1, j_2 \leqslant 60k$ and for which

$$j_1(1,0) + j_2(0,1) - j_3(1,1) \in -S(I', \mathbf{X}, \mathbf{Y}, \mathbf{Z})$$

has size $|T| \gg k^2$. In particular there is a set T_1 of integers j_1 in the range $10k < j_1 \leqslant 60k$ of size $|T_1| \gg k$ such that for each $j_1 \in T_1$ there are $\gg k$ integers j_2 in the same range $10k < j_2 \leqslant 60k$ such that $(j_1, j_2) \in T$. Thus by two further computations along the lines of (3.9), independently with probability $\gg 1$ we can find $j_1 \in T_1$ such that $X_{j_1} > 0$, and then j_2 such that $(j_1, j_2) \in T$ and such that $Y_{j_2} > 0$.

But then by definition of $S(I', \mathbf{X}, \mathbf{Y}, \mathbf{Z})$ we can find $(x_j)_{j\in I'}, (y_j)_{j\in I'}, (z_j)_{j\in I'}$ such that $0 \leqslant x_j \leqslant X_j$, $0 \leqslant y_j \leqslant Y_j$, and $0 \leqslant z_j \leqslant Z_j$ for all $j \in I'$ and such that

$$j_1 + \sum_{j\in I'} jx_j = j_2 + \sum_{j\in I'} jy_j = j_3 + \sum_{j\in I'} jz_j.$$

Thus the proposition follows from putting $x_{j_1} = y_{j_2} = z_{j_3} = 1$, and putting all other x_j, y_j, z_j with $j > k$ equal to 0. □

Corollary 3.9. *$\mathscr{L}(\mathbf{X}) \cap \mathscr{L}(\mathbf{Y}) \cap \mathscr{L}(\mathbf{Z})$ is almost surely infinite.*

Proof. Define k_1 to be sufficiently large, and thereafter $k_{i+1} = (60k_i)^{1/\beta}$. Then the intervals $I_i = (k_i^\beta, 60k_i]$ are pairwise disjoint and by the proposition for each the probability that we can find $(x_j)_{j\in I_i}, (y_j)_{j\in I_i}, (z_j)_{j\in I_i}$ not all zero such that $0 \leqslant x_j \leqslant X_j$, $0 \leqslant y_j \leqslant Y_j$, and $0 \leqslant z_j \leqslant Z_j$ for each $j \in I_i$ and

$$\sum_{j\in I_i} jx_j = \sum_{j\in I_i} jy_j = \sum_{j\in I_i} jz_j$$

is bounded away from zero. Since these events are independent for different values of i the corollary follows. □

Proof of Proposition 3.1. By Corollary 3.9 there is some $k_0 = k_0(\varepsilon)$ such that if $\mathscr{L}(\mathbf{X}) \cap \mathscr{L}(\mathbf{Y}) \cap \mathscr{L}(\mathbf{Z}) \cap [1, k_0]$ is nonempty with probability at least $1 - \varepsilon/2$. Thus by Lemma 1.3 there is some $n_0 = n_0(\varepsilon)$ such that if $n \geqslant n_0$ then with probability at least $1 - \varepsilon$ there is some $\ell \leqslant k_0$ such that π_1, π_2, π_3 each fix a set of size ℓ. □

Acknowledgments. The authors thank the referees for carefully reading the paper and for several helpful suggestions.

References

[1] R. Arratia and S. Tavaré, *The cycle structure of random permutations*, Ann. Probab. **20** (1992), no. 3, 1567–1591.

[2] J. H. Davenport and G. C. Smith, *Fast recognition of alternating and symmetric Galois groups*, J. Pure Appl. Algebra **153** (2000), no. 1, 17–25.

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

[4] J. Dixon, *Random sets which invariably generate the symmetric group*, Discrete Math. **105** (1992), 25–39.

[5] S. Eberhard, K. Ford and B. Green, *Permutations fixing a k-set*, http://arxiv.org/abs/1507.04465.

[6] W. M. Kantor, A. Lubotzky and A. Shalev: Invariable generation and the Chebotarev invariant of a finite group, J. Algebra **348** (2011), 302–314.

[7] E. Kowalski and D. Zywina, *The Chebotarev invariant of a finite group*, Exp. Math. **21** (2012), no. 1, 38–56.

[8] A. Lucchini, *The Chebotarev invariant of a finte group: a conjecture of Kowalski and Zywina*, preprint. ArXiv:1509.05859

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

[10] H. Maier and G. Tenenbaum, *On the set of divisors of an integer*, Invent. Math. **76** (1984), no. 1, 121–128.

[11] D. R. Musser. *On the efficiency of a polynomial irreducibility test*, J. Assoc. Comput. Mach. **25** (1978), no. 2, 271–282.

[12] R. Pemantle, Y. Peres and I. Rivin, *Four random permutations conjugated by an adversary generate S_n with high probability*, http://arxiv.org/abs/1412.3781.

[13] A. Raouj and A. Stef, *Sur la proximité des diviseurs des entiers,* J. Number Theory **76** (1999), no. 1, 66–93.

[14] T. Tao and V. Vu. *Additive Combinatorics*. Cambridge University Press, 2006.

Mathematical Institute, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, England

E-mail address: sean.eberhard@maths.ox.ac.uk

Department of Mathematics, 1409 West Green Street, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA

E-mail address: ford@math.uiuc.edu

Mathematical Institute, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, England

E-mail address: ben.green@maths.ox.ac.uk