INvariable generation of the symmetric group

SEAN EBERHARD, KEVIN FORD, AND BEN GREEN

Abstract. We say that permutations $\pi_1, \ldots, \pi_r \in S_n$ invariably generate $S_n$ if, no matter how one chooses conjugates $\pi'_1, \ldots, \pi'_r$ of these permutations, $\pi'_1, \ldots, \pi'_r$ generate $S_n$. We show that if $\pi_1, \pi_2, \pi_3$ are chosen randomly from $S_n$ then, almost surely as $n \to \infty$, they do not invariably generate $S_n$. By contrast it was shown recently by Pemantle, Peres and Rivin that four random elements do invariably generate $S_n$ with positive probability. 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 $\pi_1, \pi_2$ of the symmetric group $S_n$ generate at least the whole alternating group $A_n$ almost surely as $n \to \infty$, it is less clear how large the group generated by $\pi'_1, \pi'_2$ must be when $\pi'_1$ and $\pi'_2$ are allowed to be arbitrary conjugates of $\pi_1$ and $\pi_2$. Following Dixon [4] we say that a list $\pi_1, \ldots, \pi_r \in S_n$ has a property $P$ invariably if $\pi'_1, \ldots, \pi'_r$ has property $P$ whenever $\pi'_i$ is conjugate to $\pi_i$ for every $i$. How many random elements of $S_n$ must we take before we expect them to invariably generate $S_n$?

Several authors [2, 4, 6, 7, 9, 10] 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 $\overline{f}$ over $\mathbb{Z}/p\mathbb{Z}$. By classical Galois theory, if $\overline{f}$ has irreducible factors of degrees $n_1, \ldots, n_r$ then the Galois group $G$ of $f$ over $\mathbb{Q}$ has an element with cycle lengths $n_1, \ldots, n_r$. Moreover by Frobenius’s density theorem, if $G = S_n$ then the frequency with which a given cycle type arises is equal to the proportion of elements in $S_n$ with that cycle type. Thus if we suspect that $G = S_n$ then the number of times we expect to have to iterate this procedure before proving that $G = S_n$ is controlled by the expected number of random elements required to invariably generate $S_n$.

Luczak and Pyber [7] were the first to prove the existence of a constant $C$ such that $C$ random permutations $\pi_1, \ldots, \pi_C \in S_n$ invariably generate $S_n$ with probability bounded away from zero. Their method does not directly yield a reasonable value of $C$, but recently Pemantle, Peres, and Rivin [10] proved that we may take $C = 4$. 

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.
Theorem 1.1 (Pemantle-Peres-Rivin [10]). If \( \pi_1, \pi_2, \pi_3, \pi_4 \in S_n \) are chosen uniformly at random then the probability that \( \pi_1, \pi_2, \pi_3, \pi_4 \) invariably generate \( S_n \) 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 \( S_n \), 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 \( \pi_1, \pi_2, \pi_3 \in S_n \) are chosen uniformly at random then the probability that \( \pi_1, \pi_2, \pi_3 \) invariably generate a transitive subgroup (or, in particular, all of \( S_n \)) tends to zero as \( n \to \infty \). Equivalently, with probability tending to 1 there is a positive integer \( k < n \) such that \( \pi_1, \pi_2, \pi_3 \) 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 \( X = (X_1, X_2, \ldots) \) 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 \( \pi \in S_n \), then if \( k \) is fixed and \( n \to \infty \) the distribution of \( (c_1, \ldots, c_k) \) converges to that of \( (X_1, \ldots, X_k) \).

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

\[ \mathcal{L}(X) = \left\{ \sum_{j \geq 1} jx_j : 0 \leq x_j \leq X_j \right\}. \] (1.1)

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

\[ \mathbb{P}(\mathcal{L}(X) \cap \mathcal{L}(X') \cap \mathcal{L}(X'') \cap \mathcal{L}(X''') = \{0\}) > 0, \] (1.2)

where \( X', X'', X''' \) are independent copies of \( X \). Similarly, Theorem 1.2 follows almost immediately from

\[ \mathbb{P}(\mathcal{L}(X) \cap \mathcal{L}(X') \cap \mathcal{L}(X'') = \{0\}) = 0. \] (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.

Our proof of Theorem 1.2 is modeled after that of the well known theorem of Maier and Tenenbaum [8] on the propinquity of divisors: a random integer \( n \) (selected from \( \{1, \ldots, x\} \) for large \( x \)) has two distinct divisors \( d, d' \) with \( d < d' \leq 2d \) almost surely (as \( x \to \infty \)). In particular, we make heavy use of Riesz products, a device closely related to the sums \( \sum_{d|n} d^\theta \) that one sees frequently in the propinquity literature. The Maier-Tenenbaum theorem itself corresponds more perfectly with the assertion that a random permutation \( \pi \) almost surely has two different fixed sets of the same size (a true statement, but not one we establish here).
The correspondence between problems about fixed sets of random permutations and divisors of random integers is sufficiently close that we feel certain that results analogous to Theorems 1.1 and 1.2 should hold in the number theory setting, and can be established by very similar means. Thus we expect that three random integers \( n_1, n_2, n_3 \) selected independently from \( \{1, \ldots, x\} \) should, almost surely as \( x \to \infty \), have divisors \( d_1 | n_1, d_2 | n_2, d_3 | n_3 \) with \( \max d_i < 1.001 \min d_i \), but that if we select four random integers \( n_1, n_2, n_3, n_4 \) then, with positive probability, any divisors \( d_1 | n_1, d_2 | n_2, d_3 | n_3, d_4 | n_4 \) should have \( \max d_i > 1000 \min d_i \).

We plan to return to these questions in a future paper.

2. Four generators are enough

Proposition 2.1. The following is true uniformly for integers \( k, n \) with \( 1 \leq k \leq n/2 \). If \( \pi_1, \pi_2, \pi_3, \pi_4 \in S_n \) 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 \( \ell \) 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 \( n, k, \ell \) be integers with \( n \geq k \geq 1 \) and \( \ell \geq 0 \). Select \( \pi \in S_n \) at random. Then

\[
P(\pi \text{ has exactly } \ell \text{ cycles with length } \leq k) \leq \frac{e}{k} \frac{(1 + \log k)\ell}{\ell!} \left(1 + \frac{\ell}{1 + \log k}\right).
\]

In particular if \( \ell = O(\log k) \) then this is \( O((1 + \log k)^{\ell}/k\ell!) \).

Proof. Denote by \( S_n(k, \ell) \) the set of \( \pi \in S_n \) containing exactly \( \ell \) cycles of length at most \( k \). Evidently

\[
n|S_n(k, \ell)| = \sum_{\pi \in S_n(k, \ell)} \sum_{\sigma: \text{a cycle}} |\sigma|.
\]

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

$$n|\mathcal{S}_n(k, \ell)| \leq \sum_{j=1}^{n} \sum_{m=\ell-1}^{\ell} \sum_{\pi' \in \mathcal{S}_{n-j}(k, m)} \sum_{\sigma \in \mathcal{S}_n, |\sigma| = j} j \frac{n!}{(n-j)!}.$$

Now rearrange the sum according the cycle type $(c_1, \ldots, c_n)$ of the permutation $\pi'$, i.e. $\pi'$ has $c_i$ cycles of length $i$ for $1 \leq i \leq n$, 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

$$n|\mathcal{S}_n(k, \ell)| \leq \sum_{j=1}^{n} \sum_{m=\ell-1}^{\ell} \sum_{\pi' \in \mathcal{S}_{n-j}(k, m)} \frac{n!}{(n-j)!} \prod_{i=1}^{\ell} \left( \frac{1}{c_i!i^{c_i}} \right) \frac{1}{\prod_{i=1}^{\ell} c_i!i^{c_i}} \prod_{k \leq c_i \leq \ell} e^{1/i},$$

Here, $h_k = 1 + \frac{1}{2} + \cdots + \frac{1}{k}$ as before, and in the last step we used the multinomial theorem. The claimed bound now follows using the inequalities

$$h_k \leq 1 + \log k$$

and

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

In our paper [5] we showed that the probability of a random permutation $\pi \in S_n$ 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 $\leq k$. By contrast a typical permutation has $\approx \log k$ cycles of length $\leq k$. By restricting to this “quenched” regime we can establish a much stronger bound.

\footnote{The terminology is from [10] and apparently comes from statistical physics.}
Lemma 2.3. Suppose that \( k,n \) are integers with \( 1 \leq k \leq n/2 \), \( 0 < \varepsilon \leq 1/2 \), and choose \( \pi \in S_n \) uniformly at random. Then the probability that \( \pi \) 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 \( \ell \leq (1 + \varepsilon) \log k \) and consider permutations \( \pi \) with exactly \( \ell \) cycles of length at most \( k \). If \( \pi \) 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 \( \pi_1 \) has \( \ell_1 \) cycles of length \( \leq k \), and \( \pi_2 \) has \( \ell_2 \) cycles of length \( \leq k \), where \( \ell_1 + \ell_2 = \ell \). By Lemma 2.2 the number of such \( \pi \), for a given choice of \( X \) and \( \ell_1, \ell_2 \), is bounded by a constant times

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

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

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

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

\[
\frac{1}{k^2} \sum_{\ell \leq (1+\varepsilon) \log k} \frac{2^\ell (1 + \log k)^\ell}{\ell!} \ll \frac{1}{k^2} \frac{2^{\ell_0} (1 + \log k)^{\ell_0}}{\ell_0!}
\]

\[
\ll \frac{1}{k^2} \frac{(2\varepsilon/(1 + \varepsilon))^{(1+\varepsilon) \log k}}{(1+\varepsilon) \log k}
\]

\[
\ll \frac{1}{k^{1-\log 2-2\varepsilon}}.
\]

\[\square\]

Proof of Proposition 2.1. Let \( \varepsilon > 0 \) be a small and fixed. By Lemma 2.2, with probability \( O(k^{-\varepsilon^2/3}) \) one of \( \pi_1, \pi_2, \pi_3, \pi_4 \) is not “quenched”; has more than \((1 + \varepsilon) \log k \) cycles of length at most \( k \). By Lemma 2.3, for each \( \ell \in (k/2, k] \) the probability that \( \pi_1 \) is quenched and fixes a set of size \( \ell \) is at most \( k^{\log 2-1+2\varepsilon} \). Thus the probability that \( \pi_1, \pi_2, \pi_3, \pi_4 \) are all quenched and each fix a set of the same size \( \ell \) for some \( \ell \in (k/2, k] \) is at most \( k^{1+4(\log 2-1+2\varepsilon)} \). Since \( 1 + 4(\log 2 - 1) < 0 \), the result follows if \( \varepsilon \) is small enough (\( \varepsilon = 1/40 \) works). \[\square\]

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 \( \mathcal{L}(X) \).

Corollary 2.4. For any \( k \geq 2 \), the probability that \( \mathcal{L}(X) \cap \mathcal{L}(X') \cap \mathcal{L}(X'') \cap \mathcal{L}(X'''') \) 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 \( \mathbb{P}(X_1 + \cdots + X_k \leq \ell) \), which follows very quickly from the fact that \( X_1 + \cdots + X_k \) is Poisson with parameter \( h_k \).

Corollary 2.5. \( \mathcal{L}(X) \cap \mathcal{L}(X') \cap \mathcal{L}(X'') \cap \mathcal{L}(X'''') \) is almost surely finite, and equal to \( \{0\} \) with positive probability.
Proof. Let $E_k$ be the event that
\[
\mathcal{L}(X) \cap \mathcal{L}(X') \cap \mathcal{L}(X'') \cap \mathcal{L}(X''') \cap [1, k]
\]
is nonempty, and let $F_k$ be the event that
\[
\mathcal{L}(X) \cap \mathcal{L}(X') \cap \mathcal{L}(X'') \cap \mathcal{L}(X''') \cap (k, \infty)
\]
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 $k \geq 1$. The first part of the corollary follows immediately. For the second part, use the estimate just obtained to find $\mathbb{P}(F_{k_0}) < 1$. Define $X^* = (X_1^*, X_2^*, \ldots)$ by putting $X_i^* = X_i$ if $i > k_0$ and $X_i^* = 0$ if $i \leq k_0$. Let $F_{k_0}^*$ be the event that
\[
\mathcal{L}(X^*) \cap \mathcal{L}(X') \cap \mathcal{L}(X'') \cap \mathcal{L}(X''') \cap (k_0, \infty)
\]
is nonempty. Clearly $F_{k_0}^*$ implies $F_{k_0}$ and it follows that
\[
\mathbb{P}(F_{k_0} | X_1 = \cdots = X_{k_0} = 0) = \mathbb{P}(F_{k_0}^*) \leq \mathbb{P}(F_{k_0}).
\]
Consequently,
\[
\mathbb{P}(\{X_1 = \cdots = X_{k_0} = 0\} \cap F_{k_0}) \leq \mathbb{P}(X_1 = \cdots = X_{k_0} = 0) \mathbb{P}(F_{k_0}).
\]
Thus
\[
\mathbb{P}(\mathcal{L}(X) \cap \mathcal{L}(X') \cap \mathcal{L}(X'') \cap \mathcal{L}(X''') \neq \{0\}) = \mathbb{P}(E_{k_0} \cup F_{k_0}) \\
\leq \mathbb{P}(\{X_i > 0\text{ for some } i \leq k_0\} \cup F_{k_0}) \\
= \mathbb{P}(X_i > 0\text{ for some } i \leq k_0) + \mathbb{P}(\{X_1 = \cdots = X_{k_0} = 0\} \cap F_{k_0}) \\
\leq \mathbb{P}(X_i > 0\text{ for some } i \leq k_0) + \mathbb{P}(X_1 = \cdots = X_{k_0} = 0) \mathbb{P}(F_{k_0}) \\
= 1 - (1 - \mathbb{P}(F_{k_0})) \mathbb{P}(X_1 = \cdots = X_{k_0} = 0) \\
< 1. \quad \square
\]

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 $(c_1(\pi), \ldots, c_k(\pi))$ converges to that of $(X_1, \ldots, X_k)$. The same is true if $\pi$ is a random odd permutation.

Proof. Choose $\pi \in \mathcal{S}_n$ uniformly at random, and define $\sigma$ by putting $\sigma = 1$ if $\pi$ is even and $\sigma = (12)$ if $\pi$ 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 $\pi$ of length at most $2k$ approaches a Poisson distribution with parameter $h_{2k} \leq 1 + \log 2k$. Thus, almost surely (as $n \to \infty$) the total number of points in cycles of $\pi$ of length at most $2k$ is at most $2k \log n$, so almost surely each of these cycles
is disjoint from (12). That is, the points 1 and 2 are almost surely both contained in cycles of \( \pi \) of length at least \( 2k + 1 \). Now consider the probability that 1 and 2 are both contained in cycles of the same length \( \ell \geq 2k + 1 \), the number of cycles of length \( \ell \) containing both 1 and 2, which are a distance \( \leq k \) from each other, equals \( \binom{\ell - 2}{2} 2k(\ell - 2)! \).

Hence, the number of permutations \( \pi \) containing such a cycle is at most
\[
\sum_{2k+1 \leq \ell \leq n} 2k(n-2)! \leq 2k(n-1)!.
\]

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

}\end{proof}

\begin{proof}[Proof of Theorem 1.1] Let \( \pi_1, \pi_2, \pi_3, \pi_4 \in S_n \) be random permutations with \( \pi_1 \) odd. Let \( E_{n,k} \) be the event that \( \pi_1, \pi_2, \pi_3, \pi_4 \) each fix a set of size \( \ell \) for some \( \ell \) in the range \( 1 \leq \ell \leq k \), and let \( F_{n,k} \) be the event that \( \pi_1, \pi_2, \pi_3, \pi_4 \) each fix a set of size \( \ell \) for some \( \ell \) in the range \( k < \ell \leq n/2 \).

By Proposition 2.1 we have \( \mathbb{P}(F_{n,k}) \ll k^{-6} \) uniformly for \( 1 \leq k \leq n/2 \), while by Corollary 2.5 and Lemma 2.6 we have \( \lim_{n \to \infty} \mathbb{P}(E_{n,k}) \leq 1 - \delta \) for all \( k \), for some constant \( \delta > 0 \). Fix \( k_0 \) such that \( \mathbb{P}(F_{n,k_0}) \leq \delta/3 \) for all \( n \geq 2k_0 \). Then \( \mathbb{P}(E_{n,k_0}) + \mathbb{P}(F_{n,k_0}) \leq 1 - \delta/3 \) 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 \( \ell \) 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 \( S_n \). However by the Luczak-Pyber theorem \([7]\), \( \pi_1 \) is almost surely not contained in any transitive subgroup smaller than \( A_n \). Since \( \pi_1 \notin A_n \), with probability bounded away from zero \( \pi_1, \pi_2, \pi_3, \pi_4 \) invariably generate \( S_n \).

\end{proof}

3. Three generators are not enough

Theorem 1.2 follows immediately from the following more specific proposition.

\begin{proposition}
\label{prop:three-gens}
Let \( \varepsilon > 0 \). If \( k \geq k_0(\varepsilon) \) and \( n \geq n_0(\varepsilon, k) \) then with probability at least \( 1 - \varepsilon \) there is some \( \ell \leq k \) such that \( \pi_1, \pi_2, \pi_3 \) each fix a set of size \( \ell \).
\end{proposition}

Let \( X \) be defined as before, and let \( Y \) and \( Z \) be independent copies of \( X \). For \( I \) an interval in \( \mathbb{N} \) let
\[
\mathcal{L}(I, X) = \left\{ \sum_{j \in I} j x_j : 0 \leq x_j \leq X_j \right\},
\]
and define \( \mathcal{L}(I, Y) \) and \( \mathcal{L}(I, Z) \) analogously.

\begin{lemma}
\label{lem:sums}
Let \( I = (0, k] \) and let \( \varepsilon > 0 \). Then with probability at least \( 1 - \varepsilon \) we have \( \mathcal{L}(I, X), \mathcal{L}(I, Y), \mathcal{L}(I, Z) \subset [0, 3\varepsilon^{-1}k] \).
\end{lemma}

\begin{proof}
Since \( \mathbb{E} \sum_{j \in I} j X_j = |I| \leq k \), by Markov’s inequality we have \( \sum_{j \in I} j X_j \leq 3\varepsilon^{-1}k \) with probability at least \( 1 - \varepsilon/3 \). Similarly \( \sum_{j \in I} j Y_j \leq 3\varepsilon^{-1}k \) and \( \sum_{j \in I} j Z_j \leq 3\varepsilon^{-1}k \) each with probability at least \( 1 - \varepsilon/3 \), and the lemma follows.
\end{proof}
Lemma 3.3. Fix $\varepsilon$, $0 < \varepsilon < 1/2$. There is a constant $C(\varepsilon)$ so that with probability at least $1 - \varepsilon$ we have

$$\sum_{m < j \leq k} X_j \geq 0.99 \log(k/m) - C(\varepsilon),$$

$$\sum_{m < j \leq k} Y_j \geq 0.99 \log(k/m) - C(\varepsilon),$$

$$\sum_{m < j \leq k} Z_j \geq 0.99 \log(k/m) - C(\varepsilon).$$

for every nonnegative integer $m \leq k$.

Proof. Let $C = C(\varepsilon)$ be a constant whose properties will be specified later. There is nothing to prove if $m \geq e^{-C}k$, so we may suppose $m \leq e^{-C}k$. We may also suppose that $C \geq 1$. Let $E$ be the event that

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

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

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

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

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

Thus

$$1_E = \sum_{m' \leq 2e^{-C}k \text{ dyadic}} 0.99 \sum_{m' < j \leq k} X_j - 0.99 \log(k/m').$$

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

$$\mathbb{P}(E_1^c) \leq \sum_{m' \leq 2e^{-C}k \text{ dyadic}} \exp\left((0.99 - 1 - 0.99 \log(0.99)) \log(k/m')\right)$$

$$\leq \sum_{m' \leq 2e^{-C}k \text{ dyadic}} (k/m')^{-0.00005}$$

$$\leq e^{-0.00005C}. $$

Therefore, $\mathbb{P}(E_1^c) \leq \varepsilon/3$ if $C$ is taken large enough. 

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


Lemma 3.4.  
\[
\sum_{j \leq m} \frac{\cos(2\pi j \theta)}{j} = \log \min \left( \frac{1}{\|\theta\|}, m \right) + O(1) \quad \text{for } 0 < \|\theta\|.
\]

Proof. We may assume that \(0 < \theta \leq \frac{1}{2}\). Using the bound \(\cos(2\pi j \theta) = 1 + O(j^2 \theta^2)\), we get
\[
\sum_{j \leq \min(m, 1/\theta)} \frac{\cos(2\pi j \theta)}{j} = \log \min(m, 1/\theta) + O(1),
\]
which proves the lemma if \(\|\theta\| \leq 1/m\). Suppose, then, that \(\|\theta\| > 1/m\). Set
\[
S_j = \sum_{n=0}^{j} e^{2\pi in\theta},
\]
and note that by summing the geometric series we have
\[
S_j = \frac{e^{2\pi ij\theta} - 1}{e^{2\pi i\theta} - 1} \ll \frac{1}{\theta}.
\]
Thus ("Abel summation")
\[
\sum_{1/\theta < j \leq m} \frac{\cos(2\pi j \theta)}{j} = \Re \sum_{1/\theta < j \leq m} \frac{e^{2\pi ij\theta}}{j} = \Re \sum_{1/\theta < j \leq m} \frac{S_j - S_{j-1}}{j} = \Re \sum_{1/\theta < j \leq m-1} \frac{S_j}{j(j+1)} + \frac{S_m}{m} - \frac{S_{1/\theta-1}}{[1/\theta]}.
\]
and therefore
\[
\sum_{1/\theta < j \leq m} \frac{\cos(2\pi j \theta)}{j} \ll 1 + \frac{1}{\theta} \sum_{1/\theta < j \leq m-1} \frac{1}{j^2} \ll 1. \quad \square
\]

Let \(T = \mathbb{R}/\mathbb{Z}\) be the unit torus, and denote \(e(z) = e^{2\pi iz}\). Given \(I, X, Y, Z\) define \(F : T^2 \to \mathbb{C}\) by
\[
F(\theta) = \prod_{j \in I} \left( \frac{1 + e(j\theta_1)}{2} \right)^{X_j} \left( \frac{1 + e(j\theta_2)}{2} \right)^{Y_j} \left( \frac{1 + e(j(-\theta_1 - \theta_2))}{2} \right)^{Z_j}.
\]
By expanding the product we see that \(\hat{F} : \mathbb{Z}^2 \to \mathbb{C}\) is supported on the set
\[
S(I, X, Y, Z) = \{(n_1 - n_3, n_2 - n_3) : n_1 \in \mathcal{L}(I, X), n_2 \in \mathcal{L}(I, Y), n_3 \in \mathcal{L}(I, Z)\}. \quad (3.1)
\]
Since \(\sum_{a \in \mathbb{Z}^2} \hat{F}(a) = F(0) = 1\), by Cauchy-Schwarz we have
\[
1 = \left( \sum_{a \in \mathbb{Z}^2} \hat{F}(a) \right)^2 \leq \left( \sum_{a : F(a) \neq 0} 1 \right) \sum_{a \in \mathbb{Z}^2} |\hat{F}(a)|^2 \leq |S(I, X, Y, Z)| \sum_{a \in \mathbb{Z}^2} |\hat{F}(a)|^2.
\]
Applying Parseval, we get
\[
|S(I, X, Y, Z)| \geq \left( \sum_{a \in \mathbb{Z}^2} |\hat{F}(a)|^2 \right)^{-1} = \left( \int_{\mathbb{T}^2} |F(\theta)|^2 \, d\theta \right)^{-1}.
\] (3.2)

Denote by \(\|x\|\) be the distance from \(x\) to \(\mathbb{Z}\). Also let
\[
\beta = 1 - \frac{2}{3 \log 2} - 0.02 \approx 0.0182.
\]

**Lemma 3.5.** Fix \(\varepsilon, 0 < \varepsilon < \frac{1}{2}\). Let \(I = (k^\beta, k)\) and let \(E = E(\varepsilon)\) be the event from Lemma 3.3. Then both of the bounds
\[
\mathbb{E}_{1_E} |F(\theta)|^2 \ll_{\varepsilon} (k\|\theta_1\|^{1/3}\|\theta_2\|^{1/3}\|\theta_3\|^{1/3})^{-2.02}
\] (3.3)
and
\[
\mathbb{E}_{1_E} |F(\theta)|^2 \ll_{\varepsilon} (k\|\theta_i\|^{1/2}\|\theta_j\|^{1/2})^{-1.3} \quad \text{for } \{i,j\} \subset \{1,2,3\}
\] (3.4)
hold uniformly for \(\theta \in \mathbb{T}^2\), where \(\theta_3 = -\theta_1 - \theta_2\). The expectation is over \(X, Y, Z\).

**Proof.** Define, for \(i \in \{1,2,3\}\),
\[
k_i^\beta = \begin{cases} 
  k^\beta & \text{if } \|\theta_i\| \geq k^{-\beta}; \\
  1/\|\theta_i\| & \text{if } 1/k < \|\theta_i\| < k^{-\beta}; \\
  k & \text{if } \|\theta_i\| \leq 1/k.
\end{cases}
\]

It is useful to note the (slightly crude) bound
\[
k_i \leq \frac{k^\beta}{\|\theta_i\|^{1-\beta}},
\] (3.5)
which follows by an analysis of the three cases in the definition of \(k_i\). If \(E\) holds then
\[
\sum_{k_1 < j \leq k} X_j + \sum_{k_2 < j \leq k} Y_j + \sum_{k_3 < j \leq k} Z_j \geq 0.99 \log(k^3/(k_1k_2k_3)) - C(\varepsilon),
\]
so
\[
1_E |F(\theta)|^2 \ll_{\varepsilon} (k^3/k_1k_2k_3)^{-0.99 \log 2} |F(\theta)|^2 \sum_{k_1 < j \leq k} X_j + \sum_{k_2 < j \leq k} Y_j + \sum_{k_3 < j \leq k} Z_j.
\]
From (3.5) and the inequality \(3 \times 0.99 \log 2 \times (1-\beta) > 2.02\), we deduce that
\[
1_E |F(\theta)|^2 \ll_{\varepsilon} (k\|\theta_1\|^{1/3}\|\theta_2\|^{1/3}\|\theta_3\|^{1/3})^{-2.02} |F(\theta)|^2 \sum_{k_1 < j \leq k} X_j + \sum_{k_2 < j \leq k} Y_j + \sum_{k_3 < j \leq k} Z_j.
\]
Thus (3.3) will follow if we can prove
\[
\mathbb{E} |F(\theta)|^2 \sum_{k_1 < j \leq k} X_j + \sum_{k_2 < j \leq k} Y_j + \sum_{k_3 < j \leq k} Z_j \ll 1.
\] (3.6)

Similarly, from (3.5) for \(i = 1,2\) and the trivial bound \(k_3 \leq k\), and using \(2 \times 0.99 \log 2 \times (1-\beta) > 1.3\), we deduce that
\[
1_E |F(\theta)|^2 \ll_{\varepsilon} (k\|\theta_1\|^{1/2}\|\theta_2\|^{1/2})^{-1.3} |F(\theta)|^2 \sum_{k_1 < j \leq k} X_j + \sum_{k_2 < j \leq k} Y_j + \sum_{k_3 < j \leq k} Z_j,
\]
and similarly for other permutations of the indices 1,2,3, so (3.4) will also follow from (3.6).
Proposition 3.7. By using again the calculation \( E \) of Corollary 3.6. With notation as in Lemma 3.5, we have

\[ \mathbb{E}[F(\theta)]^2 \frac{2}{\mathcal{S}} \sum_{1<j<k} X_j + \frac{2}{\mathcal{S}} \sum_{1<j<k} Y_j + \sum_{1<j<k} Z_j \]

\[ = \prod_{k^3 < j \leq k_1} \mathbb{E} \left[ \frac{1 + e(j\theta_i)}{2} \right]^{2X_j} \prod_{k^3 < j \leq k_2} \mathbb{E} \left[ \frac{1 + e(j\theta_i)}{2} \right]^{2Y_j} \prod_{k^3 < j \leq k_3} \mathbb{E} \left[ \frac{1 + e(j\theta_i)}{2} \right]^{2Z_j} \]

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

\[ \mathbb{E}[F(\theta)]^2 \frac{2}{\mathcal{S}} \sum_{1<j<k} X_j + \frac{2}{\mathcal{S}} \sum_{1<j<k} Y_j + \sum_{1<j<k} Z_j \]

\[ = \exp \left( \sum_{i=1}^{3} \left( \sum_{k^3 < j \leq k_1} \frac{1}{j} \left( \left| \frac{1 + e(j\theta_i)}{2} \right|^2 - 1 \right) + \sum_{k^3 < j \leq k_2} \frac{1}{j} \left( \left| \frac{1 + e(j\theta_i)}{2} \right|^2 - 1 \right) \right) \right) \]

\[ = \exp \left( \sum_{i=1}^{3} \left( \sum_{k^3 < j \leq k_1} \cos(2\pi j\theta_i) - \frac{1}{2j} + \sum_{k^3 < j \leq k_2} \frac{\cos(2\pi j\theta_i)}{j} \right) \right) \]

\[ = \exp \left( \sum_{i=1}^{3} \left( \frac{1}{2} \log \frac{\min(k^3, 1/|\theta_i|)}{\min(k^3, 1/|\theta_i|)} - \frac{1}{2} \log \frac{k_i}{k^3} + \log \frac{\min(k, 1/|\theta_i|)}{\min(k, 1/|\theta_i|)} + O(1) \right) \right) \]

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

\[ \int_{T^2} \mathbb{E} |F(\theta)|^2 \, d\theta \ll \varepsilon \frac{k}{k^2}. \]

Proof. If \( \|\theta_i\| > 1/k \) for every \( i \), use (3.3) and the fact that for any \( \theta \) and some permutation \( i, j, l \) of the indices 1, 2, 3 we have \( \|\theta_i\| \geq \|\theta_j\| \geq \|\theta_l\| \). If \( \|\theta_i\| < 1/k \) for some \( \ell \) but \( \|\theta_i\|, \|\theta_j\| \geq 2/k \) for \( \{i, j\} \), then use (3.4); in this case \( \|\theta_i\| - \|\theta_j\| \leq 1/k \). Finally if \( \|\theta_i\| < 1/k \) and \( \|\theta_j\| < 2/k \) for some \( i, j \), it follows that \( \|\theta_i\|, \|\theta_j\| \leq 3/k \). Then use the trivial bound \( |F(\theta)| \leq 1 \).

Recall the definition of \( S(I, X, Y, Z) \), given in (3.1).

Proposition 3.7. Let \( I = \{k^3, k\} \). Then with probability at least 1/2 we have \( S(I, X, Y, Z) \subset [-10k, 10k]^2 \) and \( |S(I, X, Y, Z)| \approx k^2 \).
Proof. By Lemma 3.2 with $\varepsilon = 1/3$ the first condition holds with probability at least $2/3$. Now apply Lemma 3.3 with $\varepsilon = 1/10$, and let $E$ be the resulting event. By Lemma 3.5 we have
\[ \mathbb{E}1_E \int_{T^2} |F(\theta)|^2 \, d\theta \ll k^{-2}, \]
so by Markov’s inequality we have $\int_{T^2} |F(\theta)|^2 \, d\theta \ll k^{-2}$ with probability at least $8/10$. Thus by (3.2) we have $|S(I, X, Y, Z)| \gg k^2$ with probability at least $8/10$. \hfill \Box

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 $0 \leq x_j \leq X_j, 0 \leq y_j \leq Y_j, 0 \leq z_j \leq Z_j$ 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
\[ S(I', X, Y, Z) \subset [-10k, 10k]^2 \]
and $|S(I', X, Y, Z)| \gg k^2$. Independently with probability $\geq 1/2$ we can find $j_3 \in (20k, 50k]$ such that $Z_{j_3} > 0$. Given such a $j_3$ the number of pairs of integers $(j_1, j_2)$ such that $10k < j_1, j_2 \leq 60k$ and for which
\[ j_1(1, 0) + j_2(0, 1) - j_3(1, 1) \in -S(I', X, Y, Z) \]
is $\gg k^2$, so independently with probability $\gg 1$ we can find such a pair for which $Y_{j_2} > 0$ and $Z_{j_3} > 0$. But then by definition of $S(I', X, Y, Z)$ we can find $(x_j)_{j \in I'}, (y_j)_{j \in I'}, (z_j)_{j \in I'}$ such that $0 \leq x_j \leq X_j, 0 \leq y_j \leq Y_j, 0 \leq z_j \leq Z_j$ for all $j \in I'$ and such that
\[ j_1 + \sum_{j \in I'} jx_j = j_2 + \sum_{j \in I'} jy_j = j_3 + \sum_{j \in I'} jz_j. \]
\hfill \Box

Corollary 3.9. $\mathcal{L}(X) \cap \mathcal{L}(Y) \cap \mathcal{L}(Z)$ 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 $0 \leq x_j \leq X_j, 0 \leq y_j \leq Y_j, 0 \leq z_j \leq Z_j$ 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. \hfill \Box

Proof of Proposition 3.1. By Corollary 3.9 there is some $k_0 = k_0(\varepsilon)$ such that if $k \geq k_0$ then $\mathcal{L}(X) \cap \mathcal{L}(Y) \cap \mathcal{L}(Z) \cap [1, k]$ is nonempty with probability at least $1 - \varepsilon/2$. Thus by Lemma 1.3 there is some $n_0 = n_0(\varepsilon, k)$ such that if $n \geq n_0$ then with probability at least $1 - \varepsilon$ there is some $\ell \leq k$ such that $\pi_1, \pi_2, \pi_3$ each fix a set of size $\ell$. \hfill \Box
References


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