S. Eberhard, K. Ford, and B. Green. () "Permutations fixing a k-set,"
International Mathematics Research Notices, Vol. , Article ID , 17 pages.
doi:10.1093/imrn/

Permutations fixing a k-set

Sean Eberhard[1], Kevin Ford[2], and Ben Green[1]

[1]Mathematical Institute, Radcliffe Observatory Quarter, Woodstock Road, Oxford, OX2 6GG, UK and [2]Department of Mathematics, 1409 West Green Street, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA

Correspondence to be sent to: eberhard@maths.ox.ac.uk

Let $i(n,k)$ be the proportion of permutations $\pi \in \mathcal{S}_n$ having an invariant set of size k. In this note we adapt arguments of the second author to prove that $i(n,k) \asymp k^{-\delta}(1+\log k)^{-3/2}$ uniformly for $1 \leqslant k \leqslant n/2$, where $\delta = 1 - \frac{1+\log\log 2}{\log 2}$. As an application we show that the proportion of $\pi \in \mathcal{S}_n$ contained in a transitive subgroup not containing $\mathcal{A}_n$ is at least $n^{-\delta+o(1)}$ if n is even.

1 Introduction and notation

Let k, n be integers with $1 \leqslant k \leqslant n/2$ and select a permutation $\pi \in \mathcal{S}_n$, that is to say a permutation of $\{1, \dots, n\}$, at random. What is $i(n,k)$, the probability that π fixes some set of size k? Equivalently, what is the probability that the cycle decomposition of π contains disjoint cycles with lengths summing to k?

Somewhat surprisingly, $i(n,k)$ has only recently been at all well understood in the published literature. The lower bound $\lim_{n\to\infty} i(n,k) \gg \log k/k$ is contained in a paper of Diaconis, Fulman and Guralnick [5], while the upper bound $i(n,k) \ll k^{-1/100}$ may be found in work of Łuczak and Pyber [9]. (These authors did not make any special effort to optimise the constant 1/100, but their method does not lead to a sharp bound.) Here and throughout $X \ll Y$ means $X \leqslant CY$ for some constant $C > 0$. The notation $X \asymp Y$ will be used to mean $X \ll Y$ and $X \gg Y$. In the limit as $n \to \infty$ with k fixed, a much better bound was very recently obtained by Pemantle, Peres, and Rivin [10, Theorem 1.7]. They prove that $\lim_{n\to\infty} i(n,k) = k^{-\delta+o(1)}$, where

$$\delta = 1 - \frac{1+\log\log 2}{\log 2} \approx 0.08607.$$

Received ; Revised ; Accepted
Communicated by

They also note a connection between the problem of estimating $i(n,k)$ and a certain number-theoretic problem, an analogy that will be also be key to our work. The same connection has also been observed by Diaconis and Soundararajan [11, page 14].

Let us explain the connection with number theory. There is a well known analogy (see, for example, [1]) between the cycle decomposition of a random permutation and the prime factorisation of a random integer. Specifically, if π is a random permutation with cycles of lengths $a_1 \leqslant a_2 \leqslant \dots$, and if n is a random integer with prime factors $p_1 < p_2 < \dots$ then one expects both sequences $\log a_1, \log a_2, \dots$ and $\log\log p_1, \log\log p_2, \dots$ to behave roughly like Poisson processes with intensity 1. (Of course, this does not make sense if taken too literally, since the a_i are all integers, and the p_i are all primes, plus we have not specified exactly what we mean by either a "random permutation" or a "random integer".) The condition that $a_{i_1} + \cdots + a_{i_m} = k$ (that is, that a particular set of cycle lengths sum to k) is, because the a_i are all integers, equivalent to $k \leqslant a_{i_1} + \cdots + a_{i_m} < k+1$. Pursuing the analogy between cycles and primes, we may equate this with the condition $k \leqslant \log p_{i_1} + \cdots + \log p_{i_m} \leqslant k+1$, or in other words $e^k \leqslant p_{i_1} \cdots p_{i_m} \leqslant e^{k+1}$. This then suggests that we might compare $i(n,k)$ with $\tilde{i}(n,k)$, the probability that a random very large integer (selected uniformly from $[e^n, e^{n+1})$, say) has a divisor in the range $[e^k, e^{k+1})$.

This last problem has a long history, originating as a problem of Besicovitch [3] in 1934, and was solved (up to a constant factor) by the second author [6, 7]. In those papers it was shown that $\tilde{i}(n,k) \asymp k^{-\delta}(1+\log k)^{-3/2}$ uniformly for $k \leqslant n/2$, where δ is the constant mentioned above. In this paper we use the same method to prove the same rate of decay for $i(n,k)$.

Theorem 1.1. $i(n,k) \asymp k^{-\delta}(1+\log k)^{-3/2}$ uniformly for $1 \leqslant k \leqslant n/2$. □

Since $i(n, n-k) = i(n,k)$, Theorem 1.1 establishes the order of $i(n,k)$ for all n, k.

Theorem 1.1 has implications for a conjecture of Cameron related to random generation of the symmetric group. Cameron conjectured that the proportion of $\pi \in \mathcal{S}_n$ contained in a transitive subgroup not containing $\mathcal{A}_n$ tends to zero: this was proved by Łuczak and Pyber [9] using their bound $i(n,k) \ll k^{-1/100}$. Cameron further guessed that this proportion might decay as fast as $n^{-1/2+o(1)}$ (see [9, Section 5]). However Theorem 1.1 has the following corollary.

Corollary 1.2. The proportion of $\pi \in \mathcal{S}_n$ contained in a transitive subgroup not containing $\mathcal{A}_n$ is $\gg n^{-\delta}(\log n)^{-3/2}$, provided that n is even and greater than 2. □

Proof. By Theorem 1.1 the proportion of $\pi \in \mathcal{S}_n$ fixing a set B_1 of size $n/2$ is $\asymp n^{-\delta}(\log n)^{-3/2}$. Such a permutation π must also fix the set $B_2 = \{1,\dots,n\} \setminus B_1$, and thus preserve the partition $\{B_1, B_2\}$ of $\{1,\dots,n\}$. Since $|B_1| = |B_2|$, the set of all τ preserving this partition is a transitive subgroup not containing $\mathcal{A}_n$. ■

We believe that a matching upper bound $O(n^{-\delta}(\log n)^{-3/2})$ holds in Corollary 1.2, and that for odd n there is an upper bound of the form $O(n^{-\delta'})$ for some $\delta' > \delta$. We intend to return to this problem in a subsequent paper.

Whether or not a permutation π has a fixed set of size k depends only on the vector $\mathbf{c} = (c_1(\pi), c_2(\pi), \ldots, c_k(\pi))$ listing the number of cycles of length $1, 2, \ldots, k$, respectively, in π. Crucial to our argument is the well known fact (see, e.g., [1]) that for *fixed* k, $\mathbf{c}$ has limiting distribution (as $n \to \infty$) equal to $\mathbf{X}_k = (X_1, X_2, \ldots, X_k)$, where the X_i are independent and X_i has Poisson distribution with parameter $1/i$ (for short, $X_i \overset{d}{=} \text{Pois}(1/i)$). A simple corollary is that the limit $i(\infty, k) = \lim_{n\to\infty} i(n, k)$ exists for every k. Define, for any finite list $\mathbf{c} = (c_1, c_2, \ldots, c_k)$ of non-negative integers, the quantity

$$\mathscr{L}(\mathbf{c}) = \{m_1 + 2m_2 + \cdots + km_k : 0 \leqslant m_j \leqslant c_j \ \text{ for } j = 1, 2, \ldots, k\}. \tag{1}$$

We immediately obtain that

$$i(\infty, k) = \mathbb{P}(k \in \mathscr{L}(\mathbf{X}_k)). \tag{2}$$

This makes it easy to compute $i(\infty, k)$ for small values of k. For example we have the extremely well known result (derangements) that

$$i(\infty, 1) = \mathbb{P}(X_1 \geqslant 1) = 1 - \frac{1}{e} \approx 0.6321,$$

and the less well known fact that

$$i(\infty, 2) = 1 - \mathbb{P}(X_1 = X_2 = 0) - \mathbb{P}(X_1 = 1, X_2 = 0) = 1 - 2e^{-3/2} \approx 0.5537.$$

When k is allowed to grow with n, the vector $\mathbf{c}$ is still close to being distributed as $\mathbf{X}_k$, the total variation distance between the two distributions decaying rapidly as $n/k \to \infty$ [2]. This fact is, however, not strong enough for our application. We must establish an approximate analog of (2), showing that $i(n, k)$ has about the same order as $\mathbb{P}(k \in \mathscr{L}(\mathbf{X}_k))$, uniformly in $k \leqslant n/2$.

Instead of directly estimating the probability of a single number lying in $\mathscr{L}(\mathbf{X}_k)$, however, we apply a local-to-global principle used in [6, 7] to reduce the problem to studying the *size* of $\mathscr{L}(\mathbf{X}_k)$. We expect a positive proportion of the elements of $\mathscr{L}(\mathbf{X}_k)$ to lie in the range $[\frac{1}{10}k, 10k]$ (say). The reason for this is that we expect to find ~ 1 index j for which $X_j > 0$ in any interval $[e^i, e^{i+1}]$. In particular, it is fairly likely that there is some such j with $j > k/10$, in which case at least half of the sums $m_1 + 2m_2 + \cdots + km_k$ will be $\geqslant k/10$ (those with $m_j > 0$), yet at the same time it is reasonably likely that *all* elements of $\mathscr{L}(\mathbf{X}_k)$ are $< 10k$. Assuming this heuristic is reasonable, we might expect that

$$i(n, k) \asymp \mathbb{P}(k \in \mathscr{L}(\mathbf{X}_k)) \asymp \frac{1}{k}\mathbb{E}|\mathscr{L}(\mathbf{X}_k)|. \tag{3}$$

In Section 3, we will show that (3) does indeed hold. The main result of that section is the following.

Proposition 1.3. $i(n, k) \asymp \frac{1}{k}\mathbb{E}|\mathscr{L}(\mathbf{X}_k)|$ uniformly for $1 \leqslant k \leqslant n/2$. □

Our main theorem follows immediately from this and the next proposition, whose proof occupies Sections 4 (lower bound) and 5 (upper bound). Note that in these propositions we operate with the sequence $\mathbf{X}_k = (X_1, X_2, \ldots, X_k)$ of genuinely independent random variables, which is independent of n.

Proposition 1.4. $\mathbb{E}|\mathscr{L}(\mathbf{X}_k)| \asymp k^{1-\delta}(1+\log k)^{-3/2}$. □

To briefly explain the origin of the exponent δ, we first observe the simple inequalities

$$|\mathscr{L}(\mathbf{X}_k)| \leqslant \min\left(2^{X_1+\cdots+X_k}, 1 + X_1 + 2X_2 + \cdots + kX_k\right). \tag{4}$$

Assume this is close to being sharp with reasonably high probability, and condition on $Y = X_1 + \cdots + X_k$, the number of cycles of length at most k in a random permutation. Following our earlier heuristic, the second term on the right side of (4) is $\asymp k$ most of the time, and so there is a change of behaviour around $Y = \frac{\log k}{\log 2} + O(1)$. Since Y is Poisson with parameter $\log k + O(1)$, a short calculation reveals that $\mathbb{E}\min(2^Y, k) \asymp k^{1-\delta}(\log k)^{-1/2}$. We err in the logarithmic term due to the fact that (4) is only sharp with probability about $1/\log k$, a fact that is related to order statistics [7, Sec. 4].

Let us finally mention two open questions.

Question 1. Is there some constant C such that $i(\infty, k) \sim Ck^{-\delta}(\log k)^{-3/2}$? □

It would be surprising if this were not the case.

Question 2. Is $i(\infty, k)$ monotonically decreasing in k? □

Data collected by Britnell and Wildon [4] shows that this is so at least as far as $i(\infty, 30)$, and of course a positive answer is plausible just from the fact that $i(\infty, k) \to 0$.

2 A permutation sieve

As mentioned in the introduction, the asymptotic distribution (as $n \to \infty$ with k fixed) of the cycle lengths $(c_1(\pi), \ldots, c_k(\pi))$ of a random $\pi \in \mathcal{S}_n$ is that of $\mathbf{X}_k = (X_1, \ldots, X_k)$, where the X_i are independent with $X_i \overset{d}{=} \mathrm{Pois}(1/i)$. In the nonasymptotic regime, where n may be as small as $2k$, this property is lost. We do, however, have the following substitute which will suffice for this paper.

Proposition 2.1. Let $1 \leqslant m < n$ and $c_1, \ldots, c_m$ be non-negative integers satisfying

$$c_1 + 2c_2 + \cdots + mc_m \leqslant n - m - 1.$$

Suppose that $\pi \in \mathcal{S}_n$ is chosen uniformly at random. Then

$$\frac{1}{(2m+2)\prod_{i=1}^m c_i! i^{c_i}} \leqslant \mathbb{P}(c_1(\pi) = c_1, \ldots, c_m(\pi) = c_m) \leqslant \frac{1}{(m+1)\prod_{i=1}^m c_i! i^{c_i}}.$$

□

We will prove this shortly, but first let us fix some notation. As every permutation $\pi \in \mathcal{S}_n$ factors uniquely as a product of disjoint cycles, in keeping with the analogy with integers we say that any product of these cycles, including the empty product, is a *factor* or *divisor* of π. The sets induced by these factors are precisely the invariant sets of π. We make the following further definitions:

- $\mathcal{C}_{k,n}$ is the set of cycles of length k in $\mathcal{S}_n$;
- $|\sigma|$ is the length of any factor σ (of some permutation in $\mathcal{S}_n$);
- $\tau|\pi$ means that τ is an invariant set or divisor of π.

The following lemma is a slight generalization of the well known formula of Cauchy.

Lemma 2.2. Let $1 \leqslant m \leqslant n$, and let $c_1, \dots, c_m$ be non-negative integers with $t = c_1 + 2c_2 + \cdots + mc_m \leqslant n$. Then the number of ways of choosing $c_1 + \cdots + c_m$ disjoint cycles consisting of c_i cycles in $\mathcal{C}_{i,n}$ for $1 \leqslant i \leqslant m$ is

$$\frac{n!}{(n-t)!} \prod_{j=1}^{m} \frac{1}{c_j! j^{c_j}}.$$

□

Proof. First count the number of ways of choosing the subsets that make up the cycles, and then multiply by the number of ways to arrange the elements of these subsets into cycles. The result is

$$\binom{n}{\underbrace{1\cdots 1}_{c_1}\underbrace{2\cdots 2}_{c_2}\cdots\underbrace{m\cdots m}_{c_m}} \frac{1}{c_1!\cdots c_m!} \times \prod_{j=1}^{m} (j-1)!^{c_j},$$

which simplifies to the claimed expression. ■

Our next lemma is an analogue for permutations of a basic lemma from sieve theory.

Lemma 2.3. Suppose that m, n are integers with $1 \leqslant m \leqslant n$. Let $\pi \in \mathcal{S}_n$ be chosen uniformly at random. Then

$$\frac{1}{2m} \leqslant \mathbb{P}(\pi \text{ has no cycle of length} < m) \leqslant \frac{1}{m}.$$

□

Remarks. Both upper and lower bounds are best possible, since trivially the probability in question is exactly $1/n$ when $n/2 < m \leqslant n$ (if a permutation has no cycle of length $< m$, with m in this range, then it must be an n-cycle). In fact, it is not difficult to prove an asymptotic formula $\sim \omega(n/m)/m$ ($n \to \infty$, $m \to \infty$, $m \leqslant n$) for the probability in question, where ω is Buchstab's function and $\omega(u) \to e^{-\gamma}$ as $u \to \infty$ [8, Theorem 2.2].

Proof. (See the proof of [8, Theorem 2.2]). We phrase the proof combinatorially rather than probabilistically; thus let $c(n,m)$ be the number of permutations of $\mathcal{S}_n$ that have no cycles of length $< m$. We proceed by induction on n, the result being trivial when $n=1$. Let $\sum^*$ denote a sum over permutations with no cycle of length $< m$. Using the fact that the sum of lengths of cycles in a permutation in $\mathcal{S}_n$ is n, we get

$$\begin{aligned} nc(n,m) &= \sum_{\pi\in\mathcal{S}_n}{}^{*} n = \sum_{\pi\in\mathcal{S}_n}{}^{*} \sum_{\substack{\sigma|\pi \\ \sigma \text{ a cycle}}} |\sigma| = \sum_{k\geqslant m} k \sum_{\sigma\in\mathcal{C}_{k,n}} \sum_{\substack{\pi\in\mathcal{S}_n \\ \sigma|\pi}}{}^{*} 1 \\ &= \sum_{m\leqslant k\leqslant n-m} k \sum_{\sigma\in\mathcal{C}_{k,n}} c(n-k,m) + \sum_{\sigma\in\mathcal{C}_{n,n}} n \\ &= n! + \sum_{m\leqslant k\leqslant n-m} \frac{n!}{(n-k)!} c(n-k,m). \end{aligned}$$

If $\frac{n}{2} < m \leqslant n$, then $c(n,m) = \frac{n!}{n}$ and the result follows. Otherwise, by the induction hypothesis,

$$nc(n,m) \leqslant n! + \sum_{m\leqslant k\leqslant n-m} \frac{n!}{m} = n!\left(1 + \frac{n-2m+1}{m}\right) \leqslant \frac{n!\cdot n}{m}$$

and

$$nc(n,m) \geqslant n! + \sum_{m\leqslant k\leqslant n-m} \frac{n!}{2m} = n!\left(1 + \frac{n-2m+1}{2m}\right) \geqslant \frac{n!\cdot n}{2m}. \qquad \blacksquare$$

It is now a simple matter to establish Proposition 2.1.

Proof of Proposition 2.1. Let $t = c_1 + 2c_2 + \cdots + mc_m$. For each choice of the $c_1 + \cdots + c_m$ disjoint cycles consisting of c_j cycles from $\mathcal{C}_{j,n}$ $(1 \leqslant j \leqslant m)$, there are $c(n-t, m+1)$ permutations $\pi \in \mathcal{S}_n$ containing these cycles as factors and no other cycles of length at most m, where $c(n-t,m+1)$ is the number of permutations on $n-t$ letters with no cycle of length $< m+1$, as in the proof of Lemma 2.3. Applying Lemmas 2.2 and 2.3 completes the proof. ■

3 The local-to-global principle

As in the introduction, let $X_1, X_2, \ldots$ be independent random variables with distribution $X_j \overset{d}{=} \mathrm{Pois}(1/j)$. We record here that

$$\mathbb{E}|\mathscr{L}(\mathbf{X}_k)| = \sum_{c_1,\ldots,c_k\geqslant 0} |\mathscr{L}(\mathbf{c})|\mathbb{P}(X_1 = c_1)\cdots\mathbb{P}(X_k = c_k) = e^{-h_k} \sum_{c_1,\ldots,c_k\geqslant 0} \frac{|\mathscr{L}(\mathbf{c})|}{\prod_{i=1}^k c_i! i^{c_i}}, \tag{5}$$

where $h_k = 1 + \frac{1}{2} + \cdots + \frac{1}{k}$. We also record the inequalities

$$\log(k+1) \leqslant h_k \leqslant 1 + \log k, \qquad (k \geqslant 1) \tag{6}$$

which may be proved, for example, by summing the obvious inequalities $\frac{1}{n+1} \leqslant \int_n^{n+1} dt/t \leqslant \frac{1}{n}$.

Lemma 3.1. Let $k \in \mathbb{N}$, $c_1, \dots, c_k \geqslant 0$, $I \subset [k]$ and $c'_i = c_i$ for $i \notin I$, $c'_i = 0$ for $i \in I$. then

$$|\mathscr{L}(\mathbf{c})| \leqslant |\mathscr{L}(\mathbf{c}')| \prod_{i \in I}(c_i + 1).$$

□

Proof. Clearly, $\mathscr{L}(\mathbf{c})$ is the union of $\prod_{i \in I}(c_i + 1)$ translates of $\mathscr{L}(\mathbf{c}')$. ■

Lemma 3.2. Suppose that $\ell' \leqslant \ell$. Then

$$\frac{1}{\ell}\mathbb{E}|\mathscr{L}(\mathbf{X}_\ell)| \leqslant \frac{1}{\ell'}\mathbb{E}|\mathscr{L}(\mathbf{X}_{\ell'})|.$$

□

Proof. By Lemma 3.1, $|\mathscr{L}(\mathbf{X}_\ell)| \leqslant (1 + X_{\ell'+1}) \cdots (1 + X_\ell)|\mathscr{L}(\mathbf{X}_{\ell'})|$. Thus by independence,

$$\mathbb{E}|\mathscr{L}(\mathbf{X}_\ell)| \leqslant \left(\prod_{i=\ell'+1}^{\ell} \mathbb{E}(1 + X_i)\right)\mathbb{E}|\mathscr{L}(\mathbf{X}_{\ell'})| = \frac{\ell + 1}{\ell' + 1}\mathbb{E}|\mathscr{L}(\mathbf{X}_{\ell'})| \leqslant \frac{\ell}{\ell'}\mathbb{E}|\mathscr{L}(\mathbf{X}_{\ell'})|.$$ ■

We also need to compute the mixed moments of $|\mathscr{L}(\mathbf{X}_k)|$ with powers of some X_j. Recall that the mth moment $\mathbb{E}X^m$, if $X \overset{d}{=} \mathrm{Pois}(1)$, is the mth Bell number B_m. The sequence of Bell numbers starts $1, 2, 5, 15, 52, 203, \dots$.

Lemma 3.3. Suppose that $j_1, \dots, j_h \leqslant k$ are distinct integers and that $a_1, \dots, a_h$ are positive integers. Then

$$\mathbb{E}|\mathscr{L}(\mathbf{X}_k)|X_{j_1}^{a_1} \cdots X_{j_h}^{a_h} \leqslant \frac{C_{a_1,\dots,a_h}}{j_1 \cdots j_h}\mathbb{E}|\mathscr{L}(\mathbf{X}_k)|.$$

We may take $C_{a_1,\dots,a_h} = \prod_{i=1}^{h}(B_{a_i} + B_{a_i+1})$. In particular we may take $C_1 = 3$. □

Proof. Define $\mathbf{X}'_k$ by putting $X'_{j_1} = \cdots = X'_{j_h} = 0$ and $X'_j = X_j$ for all other j. By Lemma 3.1, we have

$$|\mathscr{L}(\mathbf{X}_k)| \leqslant |\mathscr{L}(\mathbf{X}'_k)|(1 + X_{j_1}) \cdots (1 + X_{j_h}).$$

Thus by independence

$$\mathbb{E}|\mathscr{L}(\mathbf{X}_k)|X_{j_1}^{a_1} \cdots X_{j_h}^{a_h} \leqslant \mathbb{E}|\mathscr{L}(\mathbf{X}'_k)| \prod_{i=1}^{h}(\mathbb{E}X_{j_i}^{a_i} + \mathbb{E}X_{j_i}^{a_{i+1}}). \tag{7}$$

For $X \overset{d}{=} \mathrm{Pois}(\lambda)$ we have $\mathbb{E}X^m = \phi_m(\lambda)$, where $\phi_m(\lambda)$ is the m-th Touchard (or Bell) polynomial, a polynomial with positive coefficients and zero constant coefficient. If $\lambda \leqslant 1$, it follows that $\mathbb{E}X^m \leqslant \lambda B_m$ for $m \geqslant 1$. The result follows immediately from this, (7), and the observation that $\mathbb{E}|\mathscr{L}(\mathbf{X}'_k)| \leqslant \mathbb{E}|\mathscr{L}(\mathbf{X}_k)|$. ■

We turn now to the proof of Proposition 1.3. In what follows write $S(\mathbf{X}_\ell) = X_1 + 2X_2 + \cdots + \ell X_\ell = \max \mathscr{L}(\mathbf{X}_\ell)$. We will treat the lower bound and upper bound in Proposition 1.3 separately, the former being somewhat more straightforward than the latter.

Proof of Proposition 1.3 (Lower bound). If $k < 40$ then $i(n,k) \asymp i(\infty,k) \asymp 1 \asymp \frac{1}{k}\mathbb{E}|\mathscr{L}(\mathbf{X}_k)|$, so we may assume $k \geqslant 40$. Let $r = \lfloor k/20 \rfloor$ (so $r \geqslant 2$), and consider the permutations $\pi = \alpha\sigma_1\sigma_2\beta \in \mathcal{S}_n$, where σ_1 and σ_2 are cycles, $|\alpha| \leqslant 4r < |\sigma_1| < |\sigma_2| < 16r$, all cycles in α have length $\leqslant r$, all cycles in β have length at least $16r$, and $\alpha\sigma_1\sigma_2$ has a fixed set of size k. Because of the size restrictions on $\alpha, \sigma_1, \sigma_2$, if α is of type $\mathbf{c} = (c_1, \dots, c_r)$, with c_i cycles of length i for $1 \leqslant i \leqslant r$, then the last condition is equivalent to $k - |\sigma_1| - |\sigma_2| \in \mathscr{L}(\mathbf{c})$. In particular $|\sigma_1| + |\sigma_2| \leqslant k$, and hence $n - |\alpha| - |\sigma_1| - |\sigma_2| \geqslant \frac{4}{5}k \geqslant 16r$. Fix $\mathbf{c}$ and ℓ_1, ℓ_2 with $4r < \ell_1 < \ell_2 < 16r$ such that $k - \ell_1 - \ell_2 \in \mathscr{L}(\mathbf{c})$. By Proposition 2.1, the probability that a random $\pi \in \mathcal{S}_n$ has c_i cycles of length i ($1 \leqslant i \leqslant r$), one cycle each of length ℓ_1, ℓ_2 and no other cycles of length $< 16r$ is at least

$$\frac{1}{32r\ell_1\ell_2 \prod_{i=1}^r c_i! i^{c_i}} \geqslant \frac{1}{2^{13} r^3 \prod_{i=1}^r c_i! i^{c_i}}.$$

For any ℓ_1 satisfying $4r + 1 \leqslant \ell_1 \leqslant 8r - 1$, there are $|\mathscr{L}(\mathbf{c})|$ admissible values of $\ell_2 > \ell_1$ for which $k - \ell_1 - \ell_2 \in \mathscr{L}(\mathbf{c})$, since $\max \mathscr{L}(\mathbf{c}) \leqslant 4r \leqslant k/5$. We conclude that

$$i(n,k) \geqslant \frac{4r-1}{2^{13}r^3} \sum_{\substack{c_1, \cdots, c_r \geqslant 0 \\ S(\mathbf{c}) \leqslant 4r}} \frac{|\mathscr{L}(\mathbf{c})|}{\prod_{i=1}^r c_i! i^{c_i}}.$$

As in (5), the sum above equals $e^{h_r}\mathbb{E}|\mathscr{L}(\mathbf{X}_r)| 1_{S(\mathbf{X}_r) \leqslant 4r}$. Hence, by (6), we see that

$$i(n,k) \geqslant \frac{1}{2^{11}r}\mathbb{E}|\mathscr{L}(\mathbf{X}_r)| 1_{S(\mathbf{X}_r) \leqslant 4r}.$$

To estimate this, we use the inequality

$$1_{S(\mathbf{X}_r) \leqslant 4r} \geqslant 1 - \frac{S(\mathbf{X}_r)}{4r}.$$

By Lemma 3.3 we have

$$\mathbb{E}|\mathscr{L}(\mathbf{X}_r)| S(\mathbf{X}_r) = \sum_{j=1}^r \mathbb{E}|\mathscr{L}(\mathbf{X}_r)| j X_j \leqslant 3r\mathbb{E}|\mathscr{L}(\mathbf{X}_r)|.$$

It follows that

$$i(n,k) \geqslant \frac{1}{2^{13}r}\mathbb{E}|\mathscr{L}(\mathbf{X}_r)|.$$

Finally, the lower bound in Proposition 1.3 is a consequence of this and Lemma 3.2*. ∎

*Strictly for the purposes of proving our main theorem, this appeal to Lemma 3.2 is unnecessary. However, that lemma is straightforward and it is more aesthetically pleasing to have $\mathbb{E}|\mathscr{L}(\mathbf{X}_k)|$ in the lower bound for $i(n,k)$ rather than $\mathbb{E}|\mathscr{L}(\mathbf{X}_r)|$.

Proof of Proposition 1.3 (Upper bound). Temporarily impose a total ordering on the set of all cycles $\bigcup_{k=1}^{n} \mathcal{C}_{k,n}$, first ordering them by length, then imposing an arbitrary ordering of the cycles of a given length. Let $\pi \in \mathcal{S}_n$ have an invariant set of size k. Let $k_1 = k$ and $k_2 = n-k$. Then $\pi = \pi_1\pi_2$, where π_j is a product of cycles which, all together, have total length k_j, for $j = 1, 2$. For some $j \in \{1, 2\}$, the largest cycle in π, with respect to our total ordering, lies in π_{3-j}. Let σ be the largest cycle in π_j, and note that $|\sigma| \leqslant \min(k_1, k_2) = k$. Write $\pi = \alpha\sigma\beta$, where α is the product of all cycles dividing π which are smaller than σ and β is the product of all cycles which are larger than σ. In particular $|\beta| \geqslant |\sigma|$ since β contains the largest cycle in π as a factor, and thus $|\sigma| \leqslant |\beta| = n - |\sigma| - |\alpha|$.

By definition of σ and α, $\alpha\sigma$ has a divisor of size k_j. Suppose $|\sigma| = \ell$ and $\mathbf{c} = (c_1, c_2, \ldots, c_\ell)$ represents how many cycles α has of length $1, 2, \ldots, \ell$, respectively. Then $k_j - \ell \in \mathscr{L}(\mathbf{c})$. For ℓ and $\mathbf{c}$ satisfying this last condition, the number of possible pairs α, σ is at most (by Lemma 2.2)

$$\frac{n!}{(n-|\alpha|-|\sigma|)!} \prod_{i<\ell} \frac{1}{c_i! i^{c_i}} \times \frac{1}{(c_\ell+1)!\ell^{c_\ell+1}} \leqslant \frac{n!}{\ell(n-|\alpha|-|\sigma|)!} \prod_{i\leqslant\ell} \frac{1}{c_i! i^{c_i}}.$$

Given α and σ, since $|\sigma| \leqslant n - |\alpha| - |\sigma|$, Lemma 2.3 implies that the number of choices for β is at most $(n-|\alpha|-|\sigma|)!/|\sigma|$. Thus

$$i(n,k) \leqslant \sum_{j=1}^{2}\sum_{\ell=1}^{k} \frac{1}{\ell^2} \sum_{\substack{c_1,\ldots,c_\ell\geqslant 0\\ k_j-\ell\in\mathscr{L}(\mathbf{c})}} \prod_{i\leqslant\ell} \frac{1}{c_i! i^{c_i}} = \sum_{j=1}^{2} \sum_{c_1,\ldots,c_k\geqslant 0} \prod_{i\leqslant k} \frac{1}{c_i! i^{c_i}} \sum_{\substack{m(\mathbf{c})\leqslant\ell\leqslant k\\ k_j-\ell\in\mathscr{L}(\mathbf{c})}} \frac{1}{\ell^2},$$

where $m(\mathbf{c}) = \max\{i : c_i > 0\} \cup \{1\}$. With $\mathbf{c}$ fixed, note that $\ell \geqslant \max(m(\mathbf{c}), k_j - S(\mathbf{c}))$. Also, the number of ℓ such that $k_j - \ell \in \mathscr{L}(\mathbf{c})$ is at most $|\mathscr{L}(\mathbf{c})|$. Thus, the innermost sum on the right side above is at most

$$\frac{|\mathscr{L}(\mathbf{c})|}{\max(m(\mathbf{c}), k_j - S(\mathbf{c}))^2}.$$

Like (5), using (6) we thus see that

$$i(n,k) \leqslant 2ek\,\mathbb{E}\,\frac{|\mathscr{L}(\mathbf{X}_k)|}{\max(m(\mathbf{X}_k), k - S(\mathbf{X}_k))^2}. \tag{8}$$

To bound this we use the inequality

$$\frac{1}{\max(m, k-S)^2} \leqslant \frac{4}{k^2}\left(1 + \frac{S^2}{m^2}\right),$$

which can be checked in the cases $S \geqslant k/2$ and $S \leqslant k/2$ separately. It follows from this and (8) that

$$i(n,k) \leqslant 8e\frac{1}{k}\mathbb{E}|\mathscr{L}(\mathbf{X}_k)| + 8e\frac{1}{k}\mathbb{E}\frac{|\mathscr{L}(\mathbf{X}_k)|S(\mathbf{X}_k)^2}{m(\mathbf{X}_k)^2}. \tag{9}$$

The first of these two terms is what we want, but the second requires a keener analysis. By conditioning on $m = m(\mathbf{X}_k)$ we have

$$\begin{aligned}\mathbb{E}\frac{|\mathscr{L}(\mathbf{X}_k)|S(\mathbf{X}_k)^2}{m(\mathbf{X}_k)^2} &= \sum_{m=1}^{k} \frac{1}{m^2} \sum_{\substack{c_1,\dots,c_m \geqslant 0 \\ c_m \geqslant 1}} |\mathscr{L}(\mathbf{c})|S(\mathbf{c})^2 \mathbb{P}(\mathbf{X}_m = \mathbf{c})\mathbb{P}(X_{m+1} = \cdots = X_{k_j} = 0) \\ &= \sum_{m=1}^{k_j} \frac{1}{m^2} \mathbb{E}\,\mathbf{Y}_m S(\mathbf{X}_m)^2 1_{X_m \geqslant 1} \exp\Big(- \sum_{j=m+1}^{k} \frac{1}{j}\Big) \\ &\leqslant \frac{e}{k} \sum_{m=1}^{k} \frac{1}{m} \mathbb{E}\,\mathbf{Y}_m S(\mathbf{X}_m)^2 X_m.\end{aligned}$$

Here we have written $\mathbf{Y}_m = |\mathscr{L}(\mathbf{X}_m)|$ for brevity, and in the last step we used the crude inequality $1_{X_m \geqslant 1} \leqslant X_m$. Expanding $S(\mathbf{X}_m)^2 = (X_1 + 2X_2 + \cdots + mX_m)^2$ and using (9), we arrive at

$$i(n,k) \ll \frac{1}{k}\mathbb{E}|\mathscr{L}(\mathbf{X}_k)| + \frac{1}{k^2} \sum_{m=1}^{k} \frac{1}{m} \sum_{i,i'=1}^{m} ii'\mathbb{E}\mathbf{Y}_m X_i X_{i'} X_m. \tag{10}$$

The innermost sum is estimated using Lemma 3.3, splitting into various cases depending on the set of distinct values among i, i', m.

Case 1 i, i', m all distinct. Then $ii'\mathbb{E}\mathbf{Y}_m X_i X_{i'} X_m \leqslant \frac{C_{1,1,1}}{m}\mathbb{E}\mathbf{Y}_m = \frac{27}{m}\mathbb{E}\mathbf{Y}_m$.

Case 2 $i = i' \neq m$. Then $ii'\mathbb{E}\mathbf{Y}_m X_i X_{i'} X_m \leqslant \frac{C_{1,2}i}{m}\mathbb{E}\mathbf{Y}_m \leqslant C_{1,2}\mathbb{E}\mathbf{Y}_m = 21\mathbb{E}\mathbf{Y}_m$.

Case 3 $i = i' = m$. Then $ii'\mathbb{E}\mathbf{Y}_m X_i X_{i'} X_m \leqslant C_3 m\mathbb{E}\mathbf{Y}_m = 20m\mathbb{E}\mathbf{Y}_m$.

Case 4 $i \neq i' = m$ or $i' \neq i = m$. In both cases $ii'\mathbb{E}\mathbf{Y}_m X_i X_{i'} X_m \leqslant 21\mathbb{E}\mathbf{Y}_m$.

Summing over all cases, it follows that

$$\sum_{i,i'=1}^{m} ii'\mathbb{E}\mathbf{Y}_m X_i X_{i'} X_m \ll m\mathbb{E}\mathbf{Y}_m.$$

Since clearly $\mathbb{E}\mathbf{Y}_m \leqslant \mathbb{E}\mathbf{Y}_k$ for every $m \leqslant k$ the result follows from this and (10). ∎

4 The lower bound in Proposition 1.4

In this section we prove the lower bound in Proposition 1.4, and hence the lower bound in our main theorem. We begin by noting that from (5) and (6) follows

$$\mathbb{E}|\mathscr{L}(\mathbf{X}_k)| \geqslant \frac{1}{ek} \sum_{c_1,\dots,c_k \geqslant 0} \frac{|\mathscr{L}(\mathbf{c})|}{\prod_{i=1}^{k} c_i! i^{c_i}}. \tag{11}$$

If we fix $r = c_1 + \cdots + c_k$, which we may think of as the number of cycles in a random permutation, then

$$\sum_{c_1+\cdots+c_k=r} \frac{|\mathscr{L}(\mathbf{c})|}{\prod_{i=1}^k c_i! i^{c_i}} = \frac{1}{r!} \sum_{a_1,\ldots,a_r=1}^{k} \frac{|\mathscr{L}^*(\mathbf{a})|}{a_1 \cdots a_r}, \tag{12}$$

where

$$\mathscr{L}^*(\mathbf{a}) = \Big\{ \sum_{i \in I} a_i : I \subset [r] \Big\}. \tag{13}$$

The equality is most easily seen by starting from the right side and setting $c_i = |\{j : a_j = i\}|$ for each i: then $\mathscr{L}(\mathbf{c}) = \mathscr{L}^*(\mathbf{a})$, $\prod_{i=1}^k i^{c_i} = a_1 \cdots a_k$, and each $\mathbf{c} = (c_1, \ldots, c_k)$ comes from $\frac{r!}{c_1! \cdots c_k!}$ different choices of $a_1, \ldots, a_k$. One may think of $a_1, \ldots, a_r$ as the (unordered) cycle lengths in a random permutation, in this case conditioned so that there are r total cycles.

Now let $J = \left\lfloor \frac{\log k}{\log 2} \right\rfloor$ and suppose that $b_1, \ldots, b_J$ are arbitrary non-negative integers with sum r. Consider the part of the sum in which

$$b_i = \sum_{j=2^{i-1}}^{2^i - 1} c_j \;\; (i = 1, 2, \ldots, J), \qquad c_j = 0 \; (j > 2^J - 1).$$

Equivalently, suppose there are exactly b_i of the a_j in each interval $[2^{i-1}, 2^i - 1]$. Writing $\mathscr{D}(\mathbf{b}) = \prod_{i=1}^J \{2^{i-1}, \ldots, 2^i - 1\}^{b_i}$, we have

$$\frac{1}{r!} \sum_{a_1,\ldots,a_r=1}^{2^J-1} \frac{|\mathscr{L}^*(\mathbf{a})|}{a_1 \cdots a_r} = \sum_{b_1,\ldots,b_J} \frac{1}{b_1! \cdots b_J!} \sum_{\mathbf{d} \in \mathscr{D}(\mathbf{b})} \frac{|\mathscr{L}^*(\mathbf{d})|}{d_1 \cdots d_r}. \tag{14}$$

To see this, fix $b_1, \ldots, b_J$ and observe that there are $\frac{r!}{b_1! \cdots b_J!}$ ways to choose which b_i of the variables $a_1, \ldots, a_r$ lie in $[2^{i-1}, 2^i - 1]$ for $1 \leqslant i \leqslant J$.

Combining (11), (12) and (14) gives

$$\mathbb{E}|\mathscr{L}(\mathbf{X}_k)| \gg \frac{1}{k} \sum_r \sum_{b_1+\cdots+b_J=r} \frac{1}{b_1! \cdots b_J!} \sum_{\mathbf{d} \in \mathscr{D}(\mathbf{b})} \frac{|\mathscr{L}^*(\mathbf{d})|}{d_1 \cdots d_r}.$$

Thus in particular one has

$$\mathbb{E}|\mathscr{L}(\mathbf{X}_k)| \gg \frac{1}{k} \sum_{b_1+\cdots+b_J=J} \frac{1}{b_1! \cdots b_J!} \sum_{\mathbf{d} \in \mathscr{D}(\mathbf{b})} \frac{|\mathscr{L}^*(\mathbf{d})|}{d_1 \cdots d_J}. \tag{15}$$

(This may seem wasteful at first sight, but in fact a more careful – though unnecessary – analysis would reveal that the main contribution is from $r = J + O(1)$, so this is not in fact the case.) In the light of this, the motivation for proving the following lemma is clear.

Lemma 4.1. For any $\mathbf{b} = (b_1, \dots, b_J)$ with $b_1 + \cdots + b_J = J$ we have

$$\sum_{\mathbf{d} \in \mathscr{D}(\mathbf{b})} \frac{|\mathscr{L}^*(\mathbf{d})|}{d_1 \cdots d_J} \gg \frac{(2\log 2)^J}{\sum_{i=1}^J 2^{b_1 + \cdots + b_i - i}}.$$

□

Proof. Given $\ell \in \mathbb{N}$, let $R(\mathbf{d}, \ell)$ be the number of $I \subset [J]$ with $\ell = \sum_{i \in I} d_i$ (One should think of the number of cycles with lengths summing to precisely ℓ in a random permutation.) Then $\sum_\ell R(\mathbf{d}, \ell) = 2^J$. Also, define $\lambda_i = \sum_{j=2^{i-1}}^{2^i - 1} 1/j$ for $1 \leqslant i \leqslant J$ (thus $\lambda_i \approx \log 2$). By Cauchy-Schwarz,

$$\begin{aligned} 2^{2J} \prod_{j=1}^J \lambda_j^{2b_j} &= \Big(\sum_{\mathbf{d} \in \mathscr{D}(\mathbf{b})} \frac{1}{d_1 \cdots d_J} \sum_\ell R(\mathbf{d}, \ell) \Big)^2 \\ &= \Big(\sum_{\mathbf{d} \in \mathscr{D}(\mathbf{b})} \frac{1}{d_1 \cdots d_J} \sum_{\ell \in \mathscr{L}^*(\mathbf{d})} R(\mathbf{d}, \ell) \Big)^2 \\ &\leqslant \Big(\sum_{\mathbf{d} \in \mathscr{D}(\mathbf{b}), \ell} \frac{R(\mathbf{d}, \ell)^2}{d_1 \cdots d_J} \Big) \Big(\sum_{\mathbf{d} \in \mathscr{D}(\mathbf{b})} \frac{|\mathscr{L}^*(\mathbf{d})|}{d_1 \cdots d_J} \Big). \end{aligned} \tag{16}$$

Our next aim is to establish an upper bound for the first sum on the right side. We have

$$\sum_{\mathbf{d} \in \mathscr{D}(\mathbf{b}), \ell} \frac{R(\mathbf{d}, \ell)^2}{d_1 \cdots d_J} = \sum_{I_1, I_2 \subset [J]} S(I_1, I_2), \tag{17}$$

where

$$S(I_1, I_2) = \sum_{\substack{\mathbf{d} \in \mathscr{D}(\mathbf{b}) \\ \sum_{i \in I_1} d_i = \sum_{i \in I_2} d_i.}} \frac{1}{d_1 \cdots d_J}$$

If $I_1 = I_2$, then evidently $S(I_1, I_2) = \lambda_1^{b_1} \cdots \lambda_J^{b_J}$. If I_1 and I_2 are distinct, let $j = \max(I_1 \triangle I_2)$ be the largest coordinate at which I_1 and I_2 differ. With all of the quantities d_i fixed except for d_j, we see that d_j is uniquely determined by the relation $\sum_{i \in I_1} d_i = \sum_{i \in I_2} d_i$. If we define $e(j) \in [J]$ uniquely by

$$b_1 + \cdots + b_{e(j)-1} + 1 \leqslant j \leqslant b_1 + \cdots + b_{e(j)},$$

then $d_j \geqslant 2^{e(j)-1}$, regardless of the choice of $d_1, \dots, d_{j-1}, d_{j+1}, \dots, d_J$ and thus

$$S(I_1, I_2) \leqslant \prod_{\substack{i=1 \\ i \neq j}}^J \Big(\sum_{d_i} \frac{1}{d_i} \Big) \cdot \frac{1}{2^{e(j)-1}} = \frac{\lambda_1^{b_1} \cdots \lambda_J^{b_J} \lambda_{e(j)}^{-1}}{2^{e(j)-1}} \ll \frac{\lambda_1^{b_1} \cdots \lambda_J^{b_J}}{2^{e(j)}}.$$

(Here, the sums over d_i are over the appropriate dyadic intervals required so that $\mathbf{d} \in \mathscr{D}(\mathbf{b})$.) Here we used the fact that $\lambda_i \asymp 1$; in fact one may note that $\lambda_i \geqslant \lambda_{i+1}$ for all i (since $\frac{1}{n} \geqslant \frac{1}{2n} + \frac{1}{2n+1}$) and that $\lim_{i\to\infty} \lambda_i = \log 2$, so in fact $\lambda_i \geqslant \log 2$ for all i.

Since the number of pairs of subsets $I_1, I_2 \subset [J]$ with $\max(I_1 \triangle I_2) = j$ is exactly 2^{J+j-1}, we get from this and (17) that

$$\prod_{j=1}^{J} \lambda_j^{-b_j} \sum_{d\in\mathscr{D}(\mathbf{b}),\ell} \frac{R(\mathbf{d},\ell)^2}{d_1\cdots d_J} \ll 2^J + 2^J \sum_{j=1}^{J} 2^{j-e(j)} = 2^J + 2^J \sum_{i=1}^{J} 2^{-i} \sum_{j:e(j)=i} 2^j$$
$$\ll 2^J + 2^J \sum_{i=1}^{J} 2^{b_1+\cdots+b_i-i}$$
$$\ll 2^J \sum_{i=1}^{J} 2^{b_1+\cdots+b_i-i}.$$

Comparing with (16), and using again that $\lambda_i \geqslant \log 2$, completes the proof. ■

Combining Lemma 4.1 and (15), we obtain

$$\mathbb{E}|\mathscr{L}(\mathbf{X}_k)| \gg \frac{(2\log 2)^J}{k} \sum_{b_1+\cdots+b_J=J} \frac{1}{b_1!\cdots b_J! \sum_{i=1}^{J} 2^{b_1+\cdots+b_i-i}}. \tag{18}$$

Somewhat surprisingly, the right hand side here can be evaluated explicitly using the "cycle lemma", as in [7]. The key trick is to add an additional averaging over the J cyclic permutations of $b_1, \dots, b_J$ to the inner summation.

Lemma 4.2. Let $x_1, \dots, x_J$ be positive reals such that $x_1 \cdots x_J = 1$. Then the average of $\big(\sum_{i=1}^{J} x_1 \cdots x_i\big)^{-1}$ over cyclic permutations of $x_1, \dots, x_J$ is exactly $1/J$. □

Proof. Reading indices modulo J we have

$$\sum_{t=1}^{J} \frac{1}{\sum_{i=1}^{J} x_{t+1}\cdots x_{t+i}} = \sum_{t=1}^{J} \frac{x_1\cdots x_t}{\sum_{i=1}^{J} x_1\cdots x_{t+i}} = 1.$$ ■

Applying the cycle lemma with $x_i = 2^{b_i-1}$ gives (noting that cyclic permutation of the variables is a 1-1 map on the set of $(b_1, \dots, b_J)$ with $b_1 + \cdots + b_J = J$) that

$$\sum_{b_1+\cdots+b_J=J} \frac{1}{b_1!\cdots b_J! \sum_{i=1}^{J} 2^{b_1+\cdots+b_i-i}} = \frac{1}{J} \sum_{b_1+\cdots+b_J=J} \frac{1}{b_1!\cdots b_J!} = \frac{1}{J}\cdot\frac{J^J}{J!},$$

the second equality being a consequence of the multinomial theorem.

Substituting into (18), and recalling that $J = \frac{\log k}{\log 2} + O(1)$, the lower bound in Proposition 1.4 now follows from Stirling's formula.

5 The upper bound in Proposition 1.4

In this section we turn to the upper bound in Proposition 1.4, that is to say the bound

$$\mathbb{E}|\mathscr{L}(\mathbf{X}_k)| \ll k^{\alpha}(\log k)^{-3/2}.$$

As with the lower bound, we condition on the number of cycles of length at most k in a random permutation. Recall from (13) the definition of $\mathscr{L}^*(\mathbf{a})$:

$$\mathscr{L}^*(\mathbf{a}) = \Big\{ \sum_{i\in I} a_i : I \subset [r] \Big\}.$$

From (5), (6) and (12) we have

$$\mathbb{E}|\mathscr{L}(\mathbf{X}_k)| \leqslant \frac{1}{k}\sum_r \frac{1}{r!} \sum_{a_1,\dots,a_r=1}^{k} \frac{|\mathscr{L}^*(\mathbf{a})|}{a_1\cdots a_r}. \tag{19}$$

The most common way for $|\mathscr{L}^*(\mathbf{a})|$ to be small is when there are many of the a_i which are small. To capture this, let $\tilde{a}_1, \tilde{a}_2, \dots$ be the increasing rearrangement of the sequence $\mathbf{a}$, so that $\tilde{a}_1 \leqslant \tilde{a}_2 \leqslant \cdots$. For any j satisfying $0 \leqslant j \leqslant r$, we have

$$\mathscr{L}^*(\mathbf{a}) \subset \left\{ m + \sum_{i\in I} \tilde{a}_i : 0 \leqslant m \leqslant \sum_{i=1}^{j} \tilde{a}_i,\ I \subset \{j+1,\dots,r\} \right\},$$

from which it follows immediately that

$$|\mathscr{L}^*(\mathbf{a})| \leqslant G(\mathbf{a}),$$

where

$$G(\mathbf{a}) = \min_{0\leqslant j\leqslant r} 2^{r-j}\left(\tilde{a}_1 + \cdots + \tilde{a}_j + 1\right). \tag{20}$$

It is reasonable to expect that

$$\sum_{a_1,\dots,a_r=1}^{k} \frac{G(\mathbf{a})}{a_1\cdots a_r} \sim \int_1^k \cdots \int_1^k \frac{G(\mathbf{t})}{t_1\cdots t_r} d\mathbf{t} = (\log k)^r \int_0^1 \cdots \int_0^1 G(e^{\xi_1 \log k}, \dots, e^{\xi_r \log k}) d\boldsymbol{\xi}, \tag{21}$$

where we have enlarged the domain of G to include r-tuples of positive real numbers. However, G is not an especially regular function and so (21) is perhaps too much to hope for. The function G is, however, increasing in every coordinate and we may exploit this to prove an approximate version of (21).

Lemma 5.1. For any $r \geqslant 1$, we have

$$\sum_{a_1,\dots,a_r=1}^{k} \frac{|\mathscr{L}^*(\mathbf{a})|}{a_1\cdots a_r} \ll (2h_k)^r r! \int_{\Omega_r} \min_{0\leqslant j\leqslant r} 2^{-j}(k^{\xi_1} + \cdots + k^{\xi_j} + 1) d\boldsymbol{\xi},$$

where $\Omega_r = \{(\xi_1, \ldots, \xi_r) : 0 \leqslant \xi_1 \leqslant \xi_2 \leqslant \ldots \leqslant \xi_r \leqslant 1\}$. □

Proof. Motivated by the fact that $1/a = \int_{\exp(h_{a-1})}^{\exp(h_a)} dt/t$, define the product sets

$$R(\mathbf{a}) = \prod_{i=1}^{r} \left[\exp\left(h_{a_i - 1}\right), \exp\left(h_{a_i}\right)\right].$$

By (20), we have

$$\sum_{a_1,\ldots,a_r=1}^{k} \frac{|\mathscr{L}^*(\mathbf{a})|}{a_1 \cdots a_r} \leqslant \sum_{a_1,\ldots,a_r=1}^{k} \frac{G(\mathbf{a})}{a_1 \cdots a_r} = \sum_{a_1,\ldots,a_r=1}^{k} G(\mathbf{a}) \int_{R(\mathbf{a})} \frac{d\mathbf{t}}{t_1 \cdots t_r}.$$

Consider some $\mathbf{t} \in R(\mathbf{a})$. Writing $\tilde{t}_1 \leqslant \tilde{t}_2 \leqslant \ldots \leqslant \tilde{t}_r$ for the non-decreasing rearrangement of $\mathbf{t}$, we have

$$\exp\left(h_{\tilde{a}_i - 1}\right) \leqslant \tilde{t}_i \leqslant \exp\left(h_{\tilde{a}_i}\right) \quad \text{for } 1 \leqslant i \leqslant r.$$

From (6) we see that $\tilde{t}_i \geqslant \tilde{a}_i$ for all i. Hence

$$G(\mathbf{a}) \leqslant \min_{0 \leqslant j \leqslant r} 2^{r-j}(\tilde{t_1} + \cdots + \tilde{t_j} + 1) = G(\mathbf{t}) \quad \text{for all } \mathbf{t} \in R(\mathbf{a}).$$

This yields

$$\sum_{a_1,\ldots,a_r=1}^{k} G(\mathbf{a}) \int_{R(\mathbf{a})} \frac{d\mathbf{t}}{t_1 \cdots t_r} \leqslant \sum_{a_1,\ldots,a_r=1}^{k} \int_{R(\mathbf{a})} \frac{G(\mathbf{t})}{t_1 \cdots t_r} d\mathbf{t} = \int_1^{\exp(h_k)} \cdots \int_1^{\exp(h_k)} \frac{G(\mathbf{t})}{t_1 \cdots t_r} d\mathbf{t}.$$

The integrand on the right is symmetric in $t_1, \ldots, t_r$. Making the change of variables $t_i = e^{\xi_i h_k}$ yields

$$\sum_{a_1,\ldots,a_r=1}^{k} \frac{|\mathscr{L}^*(\mathbf{a})|}{a_1 \cdots a_r} \leqslant (2h_k)^r r! \int_{\Omega_r} \min_{0 \leqslant j \leqslant r} 2^{-j} \left(e^{\xi_1 h_k} + \cdots + e^{\xi_j h_k} + 1\right) d\boldsymbol{\xi}.$$

The lemma follows from the upper bound in (6), namely $h_k \leqslant 1 + \log k$. ■

With Lemma 5.1 established, we may conclude the proof of the upper bound in Proposition 1.4 by quoting [7, Lemma 3.6]. Indeed, in the notation of that paper

$$\int_{\Omega_r} \min_{0 \leqslant j \leqslant r} 2^{-j} \left(k^{\xi_1} + \cdots + k^{\xi_j} + 1\right) d\boldsymbol{\xi} = U_r(\log_2 k),$$

and thus by (19) and Lemma 5.1 we have

$$\mathbb{E}|\mathscr{L}(\mathbf{X}_k)| \ll \frac{1}{k} \sum_r (2h_k)^r U_r(\log_2 k). \tag{22}$$

Now [7, Lemma 3.6] provides the bound

$$U_r(\log_2 k) \ll \frac{1 + |\log_2 k - r|^2}{(r+1)!(2^{r - \log_2 k} + 1)},$$

uniformly for $0 \leqslant r \leqslant 10 \log_2 k$. Set

$$r_* = \lfloor \log_2 k \rfloor.$$

In what follows, we will use the observation that $a^n/(n+1)!$ is increasing for $n \leqslant a - 2$ and decreasing thereafter. If $r = r_* + m$ with $m \leqslant 9 \log_2 k$, $m \in \mathbb{Z}_{\geqslant 0}$, then we have

$$\begin{aligned} (2h_k)^r U_r(\log_2 k) &\ll \frac{(\frac{4}{3}h_k)^r}{(r+1)!} \cdot \left(\frac{3}{2}\right)^r \cdot \frac{1+m^2}{2^m} \\ &\ll \frac{(\frac{4}{3}h_k)^{r_*}}{(r_*+1)!} \cdot \left(\frac{3}{2}\right)^{r_*} \cdot \frac{1+m^2}{(\frac{4}{3})^m} \\ &\ll k^{1 + \frac{1 + \log\log 2}{\log 2}} (\log k)^{-3/2} \cdot \frac{1+m^2}{(\frac{4}{3})^m}. \end{aligned}$$

In the first step we used the observation (and the fact that $\frac{4}{3} < \frac{1}{\log 2}$), and in the second step we used Stirling's formula and (6). Summed over m, this is of course rapidly convergent and shows that the contribution to (22) from this range of r is acceptable.

Next suppose that $r = r_* - m$, $m \in \mathbb{N}$. Then we have

$$\begin{aligned} (2h_k)^r U_r(\log_2 k) &\ll \frac{(\frac{3}{2}h_k)^r}{(r+1)!} \cdot \left(\frac{4}{3}\right)^r \cdot (1+m^2) \\ &\ll \frac{(\frac{3}{2}h_k)^{r_*}}{(r_*+1)!} \cdot \left(\frac{4}{3}\right)^r \cdot (1+m^2) \\ &\ll k^{1 + \frac{1 + \log\log 2}{\log 2}} (\log k)^{-3/2} \cdot \frac{1+m^2}{(\frac{4}{3})^m}. \end{aligned}$$

Here, we used the observation (and the fact that $\frac{3}{2} > \frac{1}{\log 2}$) and a second application of Stirling's formula. Summed over m, this is once again rapidly convergent and the contribution to (22) from this range of r is acceptable.

There remains the range $r > 10 \log_2 k$. Here, we use the trivial bound $U_r(\log_2 k) \leqslant 1/r!$ and thus

$$\sum_{r > 10 \log_2 k} (2h_k)^r U_r(\log_2 k) \ll \sum_{r > 10 \log_2 k} \frac{(2h_k)^r}{r!} \ll k^{-10},$$

which is obviously minuscule in comparison to the other terms.

Remarks. It is obvious from this analysis and the lower bound in our main theorem that a proportion $\geqslant 1 - \varepsilon$ of all permutations fixing some set of size k have $\log_2 k + O(\log(1/\varepsilon))$ cycles of length at most k. It is most probably also true that for a proportion $\geqslant 1 - \varepsilon$ of all permutations fixing some set of size k we have

$\log \tilde{a}_j \geqslant j \log 2 - O_\varepsilon(1)$ for $j \leqslant \log_2 k - O_\varepsilon(1)$, where the $\tilde{a}_j$ are the (ordered) cycle lengths of the permutation. To establish this would require opening up some of the arguments used to bound the quantities U_k in [7]. We plan to return to this and other issues in a future paper.

Acknolwedgments. BG is supported by ERC Starting Grant number 279438, *Approximate algebraic structure and applications*, and a Simons Investigator Award. KF is supported by National Science Foundation grants DMS-1201442 and DMS-1501982.

References

[1] R. Arratia, A. D. Barbour, and S. Tavaré. Random combinatorial structures and prime factorizations. *Notices Amer. Math. Soc.*, 44(8):903–910, 1997.

[2] R. Arratia and S. Tavaré. The cycle structure of random permutations. *Ann. Probab.*, 20(3):1567–1591, 1992.

[3] A. S. Besicovitch. On the density of certain sequences of integers. *Math. Ann.*, 110:336–341, 1934.

[4] J. Britnell and M. Wildon. Computing derangement probabilities of the symmetric group acting on k-sets. `http://arxiv.org/abs/1511.04106`.

[5] P. Diaconis, J. Fulman, and R. Guralnick. On fixed points of permutations. *J. Algebraic Combin.*, 28(1):189–218, 2008.

[6] K. Ford. The distribution of integers with a divisor in a given interval. *Ann. of Math. (2)*, 168(2):367–433, 2008.

[7] K. Ford. Integers with a divisor in $(y, 2y]$. In *Anatomy of integers*, volume 46 of *CRM Proc. Lecture Notes*, pages 65–80. Amer. Math. Soc., Providence, RI, 2008.

[8] A. Granville. Cycle lengths in a permutation are typically Poisson. *Electron. J. Combin.*, 13(1):Research Paper 107, 23, 2006.

[9] T. Łuczak and L. Pyber. On random generation of the symmetric group. *Combin. Probab. Comput.*, 2(4):505–512, 1993.

[10] 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`.

[11] K. Soundararajan. *in* Srinivasa Ramanujan, Going Strong at 125, Part II. *Notices Amer. Math. Soc.*, 60(1):10–22, 2013.