






RESEARCH ARTICLE

Improved covering results for conjugacy classes of symmetric groups via hypercontractivity

Nathan Keller ¹, Noam Lifshitz ² and Ohad Sheinfeld ³

¹Department of Mathematics, Bar-Ilan University; E-mail: Nathan.Keller@biu.ac.il.

²Einstein Institute of Mathematics, Hebrew University; E-mail: noamlifshitz@gmail.com.

³Department of Mathematics, Bar-Ilan University; E-mail: oshenfeld@gmail.com (corresponding author).

Received: 5 February 2024; **Revised:** 2 May 2024; **Accepted:** 21 May 2024

2020 Mathematics Subject Classification: *Primary* – 20B30, 05D05; *Secondary* – 20C30

Abstract

We study covering numbers of subsets of the symmetric group S_n that exhibit closure under conjugation, known as *normal* sets. We show that for any $\epsilon > 0$, there exists n_0 such that if $n > n_0$ and A is a normal subset of the symmetric group S_n of density $\geq e^{-n^{2/5-\epsilon}}$, then $A^2 \supseteq A_n$. This improves upon a seminal result of Larsen and Shalev (Inventiones Math., 2008), with our $2/5$ in the double exponent replacing their $1/4$.

Our proof strategy combines two types of techniques. The first is ‘traditional’ techniques rooted in character bounds and asymptotics for the Witten zeta function, drawing from the foundational works of Liebeck–Shalev, Larsen–Shalev, and more recently, Larsen–Tiep. The second is a sharp hypercontractivity theorem in the symmetric group, which was recently obtained by Keevash and Lifshitz. This synthesis of algebraic and analytic methodologies not only allows us to attain our improved bounds but also provides new insights into the behavior of general independent sets in normal Cayley graphs over symmetric groups.

1. Introduction

This paper employs tools from analysis of Boolean functions to address problems studied independently by group theorists and combinatorialists. The problems we study are those which can be reformulated as investigations about independent sets in Cayley graphs over symmetric groups.

1.1. Covering numbers of subsets of symmetric groups

The *covering number* of a generating set A in a group G is the minimal ℓ such that $A^\ell = G$. The problem of determining the covering numbers of conjugacy classes and their unions is fundamental in group theory, with highlights including the breakthroughs of Guralnick, Larsen, Liebeck, Shalev and Tiep [12, 24, 26, 30].

A particular question that has been studied extensively is characterizing sets A such that $A^2 = G$. A well-known open problem in this area is Thompson’s conjecture which asserts that every finite simple group G contains a conjugacy class whose square is G .

Much of the research on characterizing sets whose square is the entire group has focused on the symmetric group, where this study goes back to Gleason, who showed in 1962 that for any n -cycle $\sigma \in S_n$, the conjugacy class σ^{S_n} satisfies $(\sigma^{S_n})^2 = A_n$ (see [13, Proposition 4]). For many years, results of this kind were achieved only for very restricted families of conjugacy classes, like the case where σ

consists of two cycles (see, for example, [1, 2, 32]). In a breakthrough paper from 2007, Larsen and Shalev [24] showed that for a sufficiently large n , if $\sigma \in S_n$ has at most $n^{1/128}$ cycles, then $(\sigma^{S_n})^2 = A_n$. As a random permutation $\sigma \in S_n$ has $O(\log n)$ cycles a.s., this shows that asymptotically, $(\sigma^{S_n})^2 = A_n$ holds for almost all permutations. In another breakthrough which followed shortly after, Larsen and Shalev [23] proved the same assertion for any $\sigma \in S_n$ that has at most $n^{1/4-\epsilon}$ cycles. Namely, they showed the following:

Theorem 1.1 [23, Theorem 1.10]. *For any $\epsilon > 0$, there exists an integer n_0 , such that for any $n > n_0$ and for any $\sigma \in S_n$ that has at most $n^{1/4-\epsilon}$ cycles, we have $(\sigma^{S_n})^2 = A_n$.*

The number of cycles of a permutation is closely related to the density of its conjugacy class. (Throughout the paper, for finite sets A, B , the density of A inside B is $\mu_B(A) = \frac{|A \cap B|}{|B|}$, and when B is clear from the context, we shorten the notation to $\mu(A)$). Theorem 1.1 can be easily seen to be equivalent to the following:

Theorem 1.2 [23, Theorem 1.20]. *For any $\epsilon > 0$, there exists an integer n_0 , such that for any $n > n_0$ and for any normal subset $A \subset S_n$ with $\mu(A) \geq e^{-n^{1/4-\epsilon}}$, we have $A^2 \supseteq A_n$.*

Determining the minimal density $\alpha(n)$ such that for any normal subset of S_n with density $\geq \alpha(n)$ we have $A^2 \supseteq A_n$, remains a very challenging open problem, and the results of [23] remained the ‘state of the art’ in the last 15 years (see, for example, [31]).

1.1.1. Our results

We show that the assertions of Theorems 1.1 and 1.2 hold under a significantly weaker assumption on the set A .

Theorem 1.3. *For any $\epsilon > 0$, there exists an integer n_0 , such that for any $n > n_0$ and for any $\sigma \in S_n$ that has at most $n^{2/5-\epsilon}$ cycles, we have $(\sigma^{S_n})^2 = A_n$.*

Theorem 1.4. *For any $\epsilon > 0$, there exists an integer n_0 , such that for any $n > n_0$ and for any normal subset $A \subset S_n$ with $\mu(A) \geq e^{-n^{2/5-\epsilon}}$, we have $A^2 \supseteq A_n$.*

We also prove a similar strengthening of the corresponding result for subsets of A_n that was recently proved by Larsen and Tiep [25].

Theorem 1.5. *For any $\epsilon > 0$, there exists an integer n_0 , such that for any $n > n_0$ and for any normal subset $A \subset A_n$ with $\mu(A) \geq e^{-n^{2/5-\epsilon}}$, we have $A^2 \supseteq A_n \setminus \{1\}$.*

Theorem 1.5 significantly improves over a recent result of Lifshitz and Marmor [28, Corollary 2.11], which achieves the weaker conclusion $A^3 = A_n$ under the stronger assumption $\mu(A) \geq e^{-n^{1/3-\epsilon}}$.

In terms of techniques, Larsen and Shalev [23, 24] obtained their results by establishing upper bounds for the values of irreducible characters. Those character bounds have grown out to be fundamental to the study of covering numbers and have found various applications in other areas of mathematics. Our new results demonstrate the surprising role of a very different new tool – the recent result of Keevash and Lifshitz [16] on hypercontractivity for global functions over symmetric groups.

Regarding tightness of our results, we believe that the minimal density of A which guarantees $A^2 \supseteq A_n$ is significantly smaller than $e^{-n^{2/5-\epsilon}}$. In this context, it is worth noting that Garonzi and Maróti [10] conjectured that there exists an absolute constant $c > 0$, such that if A, B, C are normal subsets of an alternating group $G = A_n$ of density $\geq |G|^{-c}$, then $ABC = G$. They achieved an essentially best possible result for four sets by showing that for any $\epsilon > 0$, there exists $n_0 = n_0(\epsilon)$, such that if $n > n_0$ and A, B, C, D are normal sets of density $\geq |G|^{-1/2+\epsilon}$, then $ABCD = G$. Lifshitz and Marmor [28] speculated that a far-reaching generalization of Theorem 1.4 holds: If A is a normal subset of S_n of density $\geq (n!)^{-c}$, then $A^2 \supseteq A_n$.

1.2. Independent sets in normal Cayley graphs

Theorem 1.2 can be restated in a graph theoretic terminology. Recall that a subset of the vertices of a graph is *independent* if it does not contain any edges. The largest size of an independent set in a graph is called its *independence number*. A Cayley graph $\text{Cay}(G, A)$ is said to be *normal* if the set A is normal. For a set $I \subseteq S_n$ and for $\tau \in S_n$, it is easy to see that $\tau \notin I^{-1}I$ if and only if I is an independent set in the Cayley graph $\text{Cay}(S_n, \tau^{S_n})$. Since for a normal set $I \subseteq S_n$, we have $I^{-1}I = I^2$, it is clear that the following theorem is a restatement of Theorem 1.2.

Theorem 1.6 (Theorem 1.2 restated). *For any $\epsilon > 0$, there exists an integer n_0 , such that for any $n > n_0$ and for any $\tau \in A_n \setminus \{1\}$, the largest normal independent set in the Cayley graph $\text{Cay}(A_n, \tau^{S_n})$ has size at most $e^{-n^{1/4-\epsilon}}$.*

The size of the largest normal independent set in $\text{Cay}(A_n, \tau^{S_n})$ is clearly bounded by the independence number of $\text{Cay}(A_n, \tau^{S_n})$. A subfield of extremal combinatorics known as Erdős–Ko–Rado type theorems (see the book [11] and the thesis [7]) is mostly devoted to the study of the independence numbers of graphs that have a large group of symmetries. One breakthrough in this direction is the work of Ellis, Friedgut and Pilpel [4] concerning the independence number of the Cayley graph $\text{Cay}(S_n, A)$, where A is the set of permutations with at most $t - 1$ fixed points. Independent sets I in $\text{Cay}(A_n, A)$ are called *t-intersecting*, as in such a set I , any two permutations agree on at least t coordinates.

Ellis, Friedgut and Pilpel showed that for any $n > n_0(t)$, the largest t -intersecting sets in S_n are the *t-umvirates*, which are cosets of the subgroup of all permutations that fix a given set of size t . The minimal possible value of $n_0(t)$ was improved by Ellis and Lifshitz [6], then by Kupavskii and Zakharov [22], and finally by Keller, Lifshitz, Minzer and Sheinfeld [20] who showed that $n_0(t)$ can be taken to be linear in t . Furthermore, the authors of [6, 22] showed that the results of Ellis, Friedgut and Pilpel extend to the sparser Cayley graph $\text{Cay}(G, A')$, where A' consists only of the permutations that have exactly $t - 1$ fixed points (though, starting at a larger value of $n_0(t)$). The latter setting is known as the ‘forbidding one intersection’ problem; see [5].

When removing edges from a Cayley graph, its family of independent sets widens, making it increasingly challenging to establish effective upper bounds on the independence number. We prove the following result regarding the independence number of significantly sparser Cayley graphs, in which the generating set is a single conjugacy class.¹ In order to avoid sign issues, we restrict our attention to the alternating group A_n .

Theorem 1.7. *For any $\epsilon > 0$, there exist δ, n_0 , such that the following holds for any $t \in \mathbb{N}$ and $n > n_0 + t$. Let $\sigma \in A_n$ be a permutation with t fixed points. Then the largest independent set in the Cayley graph $\text{Cay}(A_n, \sigma^{S_n})$ has density of at most $\max(e^{-(n-t)^{1/3-\epsilon}}, (n-t)^{-\delta t}$.*

For $t < n^{1/3-\epsilon}$, Theorem 1.7 implies that the independence number of the Cayley graph $\text{Cay}(A_n, \sigma^{S_n})$ is $n^{-\Theta(t)}$, as in this range, the assertion matches the trivial lower bound implied by the t -umvirates. Thus, the theorem shows that in terms of the order of magnitude, the results of [6, 22] for the ‘forbidding one intersection’ problem extend to the much sparser setting where only intersection inside a single conjugacy class is forbidden.

For larger values of t , our bound improves upon the bound of Larsen and Shalev in two ways. First, our bound holds for all independent sets, while their bound applies only to normal independent sets. Moreover, even in the broader context of arbitrary independent sets in normal Cayley graphs, we improve the $1/4$ in the double exponent to $1/3$.

Our main tool, which is interesting for its own sake, is the following stability result which says that a mild lower bound on the density of an independent set suffices to imply that it is heavily correlated with a t -umvurate. Given a set A , we write μ_A for the uniform measure on A .

¹We note that in the specific case of the Cayley graph $\text{Cay}(G, B)$, where B consists of all permutations that have a single cycle of length > 1 and arbitrarily many fixed points (which is a union of $n - 1$ conjugacy classes), significantly stronger bounds on the independence number were obtained in [3, 15]. These results, which have important applications to coding theory, are incomparable with our results.

Theorem 1.8. *For any $\epsilon > 0$, there exist δ, n_0 , such that the following holds for any $t \in \mathbb{N}$ and $n > n_0 + t$. Let $\sigma \in A_n$ be a permutation with t fixed points. Suppose that I is an independent set in the Cayley graph $\text{Cay}(A_n, \sigma^{S_n})$ of density $\geq e^{-n^{1/2 - \frac{\log n \cdot t}{2} - \epsilon}}$. Then there exists $\ell > 0$ and an ℓ -umvirate U , such that*

$$\mu_U(I) \geq n^{\delta \ell} \mu_{A_n}(I).$$

1.3. Our methods: Hypercontractivity and bounds for the isotypic projections

Our proof combines character bounds with a recent tool known as ‘sharp hypercontractivity in the symmetric group’ due to Keevash and Lifshitz [16], which improves upon the earlier work of Filmus, Kindler, Lifshitz and Minzer [8].

The covering results of Larsen and Shalev are based upon character bounds. These can be used to show that conjugacy classes behave (in some senses) like random sets of the same density. Hypercontractivity serves a similar role to the character bounds for functions that are not necessarily class functions. We make use of this by applying it to study the restrictions of the conjugacy classes to the ℓ -umvirates (for various values of ℓ). These restrictions satisfy the following *spreadness* notion (see [22]), which is also known as globalness or quasiregularity in the literature (see [17, 18]).

Let $\delta > 0$. We say that a set $A \subseteq S_n$ is δ -spread if for each $\ell \geq 1$ and for each ℓ -umvirate U ,

$$\mu_U(A) \leq n^{\delta \ell} \mu_{S_n}(A).$$

In words, this means that no restriction to an ℓ -umvirate increases the density of A significantly.

Theorem 1.8 can be restated as an upper bound on the size of δ -spread independent sets in normal Cayley graphs. It lies in the heart of the paper, and the rest of our theorems are reduced to it by combinatorial arguments.

Sketch of proof for Theorem 1.8

For functions f, g on a finite group G , we write

$$f * g(y) = \mathbb{E}_{x \sim G} [f(x)g(x^{-1}y)],$$

where $x \sim A$ denotes that x is chosen uniformly out of A . Denote by \hat{G} the set of irreducible characters on G . For $\chi \in \hat{G}$, we write $f^{\chi} = \chi(1)f * \chi$. It is well known that f can be orthogonally decomposed as $f = \sum_{\chi \in \hat{G}} f^{\chi}$. We denote the space of functions of the form f^{χ} by W_{χ} .

Fix $\sigma \in A_n$ and write $f = \frac{1_{(\sigma^{S_n})}}{\mu_{A_n}(\sigma^{S_n})}$. It was known already to Frobenius that since f is a class function, for any $\chi \in \hat{G}$, the space W_{χ} is an eigenspace of the convolution operator $g \mapsto f * g$, which corresponds to the eigenvalue $\frac{\chi(\sigma)}{\chi(1)}$.

Let $g = \frac{1_I}{\mu_{A_n}(I)}$ be the normalized indicator of an independent set I in the Cayley graph $\text{Cay}(A_n, \sigma^{S_n})$. Then one can decompose

$$0 = \langle f * g, g \rangle = \sum_{\chi \in \hat{A}_n} \frac{\chi(\sigma)}{\chi(1)} \|g^{\chi}\|_2^2. \tag{1.1}$$

The ‘main term’ of the above sum comes from the trivial representation $\chi = 1$, which contributes $\langle g, 1 \rangle = \mathbb{E}[g] = 1$ to the sum. We proceed by showing that if σ has t fixed points and I is ‘large’ (as a function of t) and δ -spread, then the other terms are negligible compared to the main term, leading to a contradiction.

Our proof is divided into two parts – upper bounding the terms $\left| \frac{\chi(\sigma)}{\chi(1)} \right|$ and upper bounding the terms $\|g^{\chi}\|_2^2$, for all $\chi \in \hat{A}_n \setminus \{1\}$. To upper bound the terms $\left| \frac{\chi(\sigma)}{\chi(1)} \right|$, we use the character bounds of

Larsen–Shalev [23] and Larsen–Tiep [25] that take the form $\chi(\sigma) \leq \chi(1)^\beta$, where β depends only on σ and not on χ . The main novel tool that we introduce in this paper is the following proposition which allows upper bounding the terms $\|g^{=x}\|_2^2$.

Proposition 1.9. *For any $\epsilon > 0$, there exist $\delta, n_0 > 0$, such that the following holds for all $n > n_0$. Let $\alpha < 1 - \epsilon$ and let $A \subseteq S_n$ be a δ -spread set of density $\geq e^{-n^\alpha}$. Write $g = \frac{1_A}{\mu(A)}$. Then $\|g^{=x}\|_2^2 \leq \chi(1)^{\alpha+\epsilon}$ for any $\chi \in \widehat{G}$.*

We prove Proposition 1.9 by appealing to the hypercontractivity theorem of Keevash and Lifshitz [16].

Combining the Larsen–Shalev and Larsen–Tiep bounds with ours, while choosing α appropriately, we obtain that $|\langle f * g, g \rangle - 1| \leq \sum_{\chi \in \widehat{A_n} \setminus 1} \chi(1)^{-s}$ for an absolute constant $s > 0$. At this point, we apply the Witten zeta function estimates of Liebeck and Shalev. For a finite group G , the Witten zeta function is given by $\zeta_G(s) = \sum_{\chi \in \widehat{G}} \chi(1)^{-s}$. Liebeck and Shalev [27] showed that $\zeta_{A_n}(s) = 1 + o(1)$ for any fixed $s > 0$, as n tends to infinity. This estimate yields $|\langle f * g, g \rangle - 1| = o(1)$ in contradiction to Equation (1.1), thus completing the proof.²

We deduce Theorems 1.3, 1.4 and 1.5 from Proposition 1.9 by proving that certain restricted conjugacy classes are δ -spread for an absolute constant $\delta > 0$, and then following a similar route to the above sketch.

Structure of the paper

In Section 2, we present results from works of Larsen–Shalev [23], Larsen–Tiep [25] and Liebeck–Shalev [27] that will be used in the sequel.

In Section 3, we prove Proposition 1.9. In Section 4, we prove a key theorem (Theorem 4.2) and deduce from it Theorems 1.7 and 1.8. In Section 5, we prove that certain restricted conjugacy classes admit some form of spreadness. In Section 6, we prove Theorems 1.3, 1.4 and 1.5.

2. Preliminaries from the Works of Larsen–Shalev, Larsen–Tiep, and Liebeck–Shalev

2.1. Character bounds using the parameter $E(\sigma)$

Recall that given a finite group G , we write \widehat{G} for the set of its irreducible complex characters. Larsen and Shalev [23] introduced the parameter $E(\sigma)$, defined as follows.

Definition 2.1. For $\sigma \in S_n$, let $f_\sigma(i)$ be the number of i -cycles in its cycle decomposition. Define the orbit growth sequence e_1, e_2, \dots, e_n via the equality

$$e_1 + \dots + e_k := \max \left(\frac{\log \left(\sum_{i=1}^k i \cdot f_\sigma(i) \right)}{\log n}, 0 \right),$$

for each $1 \leq k \leq n$. The function $E(\sigma)$ is defined by

$$E(\sigma) := \sum_{i=1}^n \frac{e_i}{i}.$$

The main result of Larsen and Shalev [23] is the following character bound.

Theorem 2.2 [23, Theorem 1.1]. *For any $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$, such that the following holds. Let $n > n_0$, let χ be an irreducible character of S_n , and let $\sigma \in S_n$. Then*

$$|\chi(\sigma)| \leq \chi(1)^{E(\sigma)+\epsilon}.$$

We also make use of the following character bound of Larsen and Tiep [25].

²We note that the Witten zeta function originates in the representation theory of compact Lie groups, where $\zeta_{\text{SU}(2)}$ is the Riemann zeta function. We define it here only for finite groups for simplicity.

Theorem 2.3 [25, Theorem 2]. *For any $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$ such that the following holds. Let $n > n_0$ and suppose that $\sigma \in A_n$ satisfies $\sigma^{A_n} \neq \sigma^{S_n}$. Then for every character χ of A_n , we have $|\chi(\sigma)| \leq \chi(1)^\epsilon$.*

These bounds combine to yield the following variant of Theorem 2.2 for A_n .

Theorem 2.4. *For any $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$, such that the following holds. Let $n > n_0$, let χ be an irreducible character of A_n , and let $\sigma \in A_n$. Then*

$$|\chi(\sigma)| \leq \chi(1)^{E(\sigma)+\epsilon}.$$

Proof. Recall from the representation theory of S_n and A_n that every irreducible character χ of S_n is either irreducible when restricted to A_n or is the sum of two irreducible characters χ_1, χ_2 , such that $\chi_2(\sigma) = \chi_1((12)\sigma(12))$ for all $\sigma \in A_n$. Moreover, any irreducible character of A_n can be obtained from an irreducible character of S_n in one of these two ways.

It follows that whenever $\sigma^{A_n} = \sigma^{S_n}$, we have $\chi_1(\sigma) = \chi_2(\sigma) = \chi(\sigma)/2$, and the assertion follows from Theorem 2.2. Otherwise, by Theorem 2.3, we have $|\chi(\sigma)| \leq \chi(1)^\epsilon$, which implies the assertion. □

2.2. Upper bounds for $E(\sigma)$

We now give several simple estimates for $E(\sigma)$. First, we treat the case where σ has t fixed points.

Lemma 2.5. *For any $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$ such that the following holds for all $n > n_0$. Suppose that $\sigma \in S_n$ has t fixed points. Then $E(\sigma) \leq \frac{1+\log_n t}{2}$.*

Proof. Let e_i be as in the definition of $E(\sigma)$. We have

$$E(\sigma) = \sum_{i=1}^n e_i/i = e_1 + \sum_{i=2}^n e_i/i \leq e_1 + \frac{\sum_{i=2}^n e_i}{2} = e_1 + \frac{1 - e_1}{2} = \frac{1 + e_1}{2} = \frac{1 + \log_n t}{2}.$$

□

We now treat the case where σ has $n^{o(1)}$ i -cycles for each ‘small’ i .

Lemma 2.6. *For any $\epsilon > 0$ and any $m \in \mathbb{N}$, there exist $\delta > 0$ and $n_0 \in \mathbb{N}$ such that the following holds. Let $n > n_0$ and suppose that $\sigma \in S_n$ has at most n^δ i -cycles for each $i < m$. Then $E(\sigma) \leq 1/m + \epsilon$.*

Proof. We have

$$\begin{aligned} E(\sigma) &= \sum_{i=1}^n e_i/i = \sum_{i=1}^{m-1} e_i/i + \sum_{i=m}^n e_i/i \leq \sum_{i=1}^{m-1} \frac{\delta + \frac{i}{\log n}}{i} + \frac{\sum_{i=m}^n e_i}{m} \\ &\leq \delta \cdot 2 \log(m) + m/\log n + 1/m \leq 1/m + \epsilon. \end{aligned}$$

□

Another estimate for $E(\sigma)$ that we need is the following.

Lemma 2.7. *For any $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$, such that the following holds for all $n > n_0$. Let $0 < \alpha < 1$. Suppose that $\sigma \in S_n$ has no fixed points and has at most n^α cycles of length at most $\lceil 2/\epsilon \rceil$. Then $E(\sigma) \leq \alpha/2 + \epsilon/2 + \frac{\log(2/\epsilon)}{\log(n)}$.*

Proof. We have

$$E(\sigma) = \sum_{i=1}^n e_i/i = \sum_{i=2}^{\lfloor 2/\epsilon \rfloor} e_i/i + \sum_{i=\lfloor 2/\epsilon \rfloor+1}^n e_i/i \leq \frac{\sum_{i=2}^{\lfloor 2/\epsilon \rfloor} e_i}{2} + \frac{\sum_{i=\lfloor 2/\epsilon \rfloor+1}^n e_i}{2/\epsilon} \leq \frac{\alpha}{2} + \frac{\log(2/\epsilon)}{\log(n)} + \frac{\epsilon}{2},$$

where the last inequality holds since $e_2 + \dots + e_{\lfloor 2/\epsilon \rfloor} \leq \alpha + \frac{\log(2/\epsilon)}{\log(n)}$. □

A similar argument yields the following lemma:

Lemma 2.8. *For any $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$, such that the following holds for all $n > n_0$. Let $\alpha > 0$. Suppose that $\sigma \in S_n$ has at most n^α cycles. Then $E(\sigma) \leq \alpha + \epsilon$.*

Proof. We have

$$E(\sigma) = \sum_{i=1}^n e_i/i \leq \sum_{i=1}^{\lfloor n^{\epsilon/2} \rfloor} e_i + \sum_{i=\lfloor n^{\epsilon/2} \rfloor+1}^n e_i/n^{\epsilon/2} \leq \alpha + \epsilon/2 + n^{-\epsilon/2} \leq \alpha + \epsilon. \quad \square$$

2.3. Squares of conjugacy classes

We use several results on squares of conjugacy classes in A_n and in S_n , of Larsen and Shalev [23] and of Larsen and Tiep [25].

Theorem 2.9 [25, Theorem 3]. *There exists $n_0 \in \mathbb{N}$, such that the following holds for all $n > n_0$. Suppose that $\sigma \in A_n$ satisfies $\sigma^{A_n} \neq \sigma^{S_n}$. Then*

$$(\sigma^{A_n})^2 \supseteq A_n \setminus \{1\}.$$

Theorem 2.10 [23, Theorem 5.1]. *For any $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$ such that the following holds for all $n > n_0$. Suppose that for some $\sigma \in S_n, \tau \in A_n$, we have $2E(\sigma) + E(\tau) < 1 - \epsilon$. Then $\tau \in (\sigma^{S_n})^2$.*

Theorem 2.11 [23, Theorem 1.10]. *For any $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$ such that the following holds for all $n > n_0$. Suppose that $\sigma \in S_n$ has no fixed points, at most $n^{1-\epsilon}$ 2-cycles and at most $(1/4 - \epsilon)n$ cycles overall. Then $(\sigma^{S_n})^2 = A_n$.*

For integers n, m such that $m|n$, we denote by $(m^{n/m})$ the conjugacy class of all $\sigma \in S_n$ that consist of n/m m -cycles.

Theorem 2.12 [23, Theorem 1.12]. *There exists $n_0 \in \mathbb{N}$ such that for any $n > n_0$ and for any $m \geq 4$ that divides n , we have $(m^{n/m})^2 = A_n$.*

We also make use of the following result due to Vishne [32].

Theorem 2.13 [32, Theorem 3.2]. *For any even $n \in \mathbb{N}$, the set $(2^{n/2})^2$ consists of the permutations that have an even number of i -cycles for each i .*

2.4. The Witten zeta function

As was described in the introduction, we apply a result of Liebeck and Shalev [27] concerning the Witten zeta function.

Recall that the Witten zeta function for a finite group G is defined by

$$\zeta(s) = \zeta_G(s) = \sum_{\chi \in \hat{G}} \chi(1)^{-s}.$$

Theorem 2.14 [27, Theorem 1.1, Corollary 2.7]. *For any $\epsilon, s > 0$, there exists n_0 such that for any $n > n_0$, we have*

$$2 - \epsilon \leq \sum_{\chi \in \widehat{S}_n} \chi(1)^{-s} \leq 2 + \epsilon, \quad \text{and} \quad 1 - \epsilon \leq \sum_{\chi \in \widehat{A}_n} \chi(1)^{-s} \leq 1 + \epsilon.$$

3. From hypercontractivity to bounds for the finer isotypic decomposition

In this section, we prove Proposition 1.9. Let us recall its statement.

Proposition 1.9. *For any $\epsilon > 0$, there exist $\delta, n_0 > 0$, such that the following holds for all $n > n_0$. Let $\alpha < 1 - \epsilon$ and let $A \subseteq S_n$ be a δ -spread set of density $\geq e^{-n^\alpha}$. Write $g = \frac{1_A}{\mu(A)}$. Then $\|g^{\otimes \chi}\|_2^2 \leq \chi(1)^{\alpha + \epsilon}$ for any $\chi \in \widehat{S}_n$.*

In the proof, we use a hypercontractive inequality of Keevash and Lifshitz for global functions over symmetric groups, as well as standard estimates for the dimensions of the characters.

3.1. The level- d inequality of Keevash and Lifshitz

Level- d inequalities bound the L_2 norm of certain ‘chunks’ of the orthogonal decomposition of a function, using hypercontractivity. The first level- d inequality was obtained in 1988 by Kahn, Kalai and Linial [14], for Boolean functions over the discrete cube $\{-1, 1\}^n$ endowed with the uniform measure. It asserts that for any $f : \{-1, 1\}^n \rightarrow \{0, 1\}$ with $\mathbb{E}[f] = \alpha$ and for any $d \leq 2 \ln(1/\alpha)$, the coefficients of the Fourier-Walsh expansion of f (namely, $f = \sum_{S \subseteq [n]} \hat{f}(S)\chi_S$) satisfy $\|\sum_{|S|=d} \hat{f}(S)\chi_S\|_2^2 \leq (2e/d)^d \alpha^2 \ln(1/\alpha)^d$ (see [29, Chapter 9]). Level- d inequalities turned out to be very useful, and have diverse applications.

In [17], Keevash, Lifshitz, Long and Minzer (see also Khot, Minzer and Safra [21]) showed that level- d inequalities can be obtained in much more general settings under the additional assumption that the function is ‘global’ (or ‘spread’) – i.e., that no restriction of $O(1)$ coordinates can increase its L_2 -norm significantly. Filmus, Kindler, Lifshitz and Minzer [8] were the first to use the technique of Keevash et al. to obtain a level- d inequality for global functions over symmetric groups. Here, we use a sharp level- d inequality which was recently proved by Keevash and Lifshitz [16], building upon a sharp version of the inequality of Keevash et al. that was obtained by Keller, Lifshitz and Marcus [19].

In order to state the level- d inequality due to Keevash and Lifshitz [16], we need a few more notations. The terminology we use follows [4] in providing a *degree decomposition* for the symmetric group, which corresponds to the decomposition of the Fourier-Walsh expansion over the discrete cube into ‘degree levels’ $f^{\otimes d} = \sum_{|S|=d} \hat{f}(S)\chi_S$ that appears in the original level- d inequality.

A *dictator* $U_{i \rightarrow j}$ is the set of permutations that send i to j . The intersection of d distinct dictators is called a d -umvirate if it is nonempty. The d -umvirates correspond to pairs of d -tuples I, J and we denote by $U_{I \rightarrow J}$ the set of permutations sending the tuple I to the tuple J . The restriction of a function f to a d -umvirate $U_{I \rightarrow J}$ is denoted by $f_{I \rightarrow J}$ and is called a d -restriction. We write $\|f_{I \rightarrow J}\|_p$ for the L_p -norm of f with respect to the uniform measure on the d -umvirate $U_{I \rightarrow J}$.

A function f is said to be r -global if $\|f_{I \rightarrow J}\|_2 \leq r^{|I|} \|f\|_2$ for all d -restrictions $f_{I \rightarrow J}$, for all values of d . A set A is r -global if its indicator function is r -global. Note that a set A is δ -spread if and only if it is n^δ -global.³

For a partition $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r) \vdash n$, the *strict level* of a representation V_λ that corresponds to λ is $n - \lambda_1$. The *level* of V_λ is the minimum between the strict levels of V_λ and $V_{\lambda'}$, where λ' is the conjugate partition of n . The *space of matrix coefficients* of an irreducible representation V is the space spanned

³For the sake of compliance with the notations of [16], we use the term ‘global’ below and in Section 5 where the results of [16] are applied. In the rest of the paper, we use the term ‘spread’.

by the functions $f_{v,\varphi}: G \rightarrow \mathbb{C}$ indexed by $v \in V, \varphi \in V^*$ that are given by

$$f_{v,\varphi}(g) = \varphi g(v).$$

We write W_d for the sum of the spaces of matrix coefficients for all representations of level d , and denote by $f^{\approx d}$ the projection of f onto W_d .

Keevash and Lifshitz proved the following:

Theorem 3.1 [16, Theorem 4.1]. *There exists $C > 0$, such that for any $n \in \mathbb{N}$ and for any $r > 1$, if $A \subseteq S_n$ is r -global and $d \leq \min(\frac{1}{8} \log(1/\mu(A)), 10^{-5}n)$, then*

$$\|1_A^{\approx d}\|_2^2 \leq \mu(A)^2 \left(Cr^4 d^{-1} \log(1/\mu(A)) \right)^d.$$

3.2. Proof of Proposition 1.9

Recall that any irreducible character χ is the trace of a unique irreducible representation ρ , and that we have $\chi(1) = \dim(\rho)$. We say that the *level* of an irreducible character χ is the level of the unique irreducible representation that corresponds to it.

In the proof, we use the following lower bounds on the dimensions of low level irreducible representations.

Lemma 3.2 [4, Claim 1 and Theorem 19]. *There exists $n_0 \in \mathbb{N}$, such that the following holds for all $n > n_0$. Let $d \leq n/200$ and let χ be an irreducible character of S_n of level $\geq d$. Then $\chi(1) \geq (\frac{n}{ed})^d$.*

Proof of Proposition 1.9. Let $A \subseteq S_n$ be a δ -spread set of density $\geq e^{-n^\alpha}$, let $g = \frac{1_A}{\mu(A)}$, and let χ be a character of level d . We may assume w.l.o.g. that $\mu(A) = e^{-n^\alpha}$. We consider two cases:

1. $d \geq \min(10^{-5}n, \frac{1}{8}n^\alpha)$. In this case, we may upper bound $\|g^{\approx \chi}\|_2 \leq \|g\|_2 = e^{n^\alpha} \leq e^{n^{1-\epsilon}}$, while by Lemma 3.2, for a sufficiently large n , we have $\chi(1) \geq \min((\frac{n}{ed})^d, (\frac{200}{e})^{n/200})$. This implies that the statement of the proposition holds provided that n_0 is sufficiently large.
2. $d \leq \min(10^{-5}n, \frac{1}{8}n^\alpha)$. In this case, we may apply Theorem 3.1 to obtain

$$\|g^{\approx \chi}\|_2^2 \leq \mu(A)^2 \left(Cn^{4\delta} d^{-1} \log(1/\mu(A)) \right)^d \leq \left(Cd^{-1} n^{\alpha+4\delta} \right)^d,$$

and by Lemma 3.2, the right-hand side is smaller than $\chi(1)^{\alpha+\epsilon}$, provided that δ is sufficiently small and n_0 is sufficiently large.

This completes the proof. □

3.3. Bounds for the finer isotypic decomposition over A_n

We shall make use also of the following variant of Proposition 1.9 for A_n .

Proposition 3.3. *For any $\epsilon > 0$, there exist $\delta, n_0 > 0$, such that the following holds for all $n > n_0$. Let $\alpha < 1 - \epsilon$ and let $A \subseteq A_n$ be a δ -spread set of density $\mu_{A_n}(A) \geq e^{-n^\alpha}$. Write $g = \frac{1_A}{\mu_{A_n}(A)}$. Then $\|g^{\approx \chi}\|_2^2 \leq \chi(1)^{\alpha+\epsilon}$ for any $\chi \in \widehat{A_n}$.*

Proof. For a partition λ , let us write λ' for the conjugate partition obtained by replacing the roles of the rows and the columns in its Young diagram. Recall that the corresponding characters satisfy $\chi_\lambda = \chi_{\lambda'} \cdot \text{sign}$.

It is well known that all irreducible characters of A_n are obtained from characters of S_n , in one of two possible ways:

1. Characters that correspond to partitions λ with $\lambda \neq \lambda'$: In this case, the characters χ_λ and $\chi_{\lambda'}$ restrict to the same irreducible character of A_n .
2. Characters that correspond to partitions λ with $\lambda = \lambda'$. In this case, the restriction of χ_λ to A_n splits to the sum of two irreducible characters, which we denote by χ_{λ_1} and χ_{λ_2} , that have the same dimension.

To handle the characters of the second type, we note that for any such λ , the level of χ_λ is necessarily $\geq n/2 - 1$. Therefore, by Lemma 3.2, we have

$$\chi_{\lambda_1}(1) = \chi_{\lambda_2}(1) \geq \frac{1}{2} \left(\frac{200}{e} \right)^{n/200},$$

which implies that

$$\|g^{\chi_\lambda}\|_2^2 \leq \|g\|_2^2 \leq e^{n^\alpha} \leq \chi(1)^{\alpha+\epsilon},$$

provided that n is sufficiently large with respect to ϵ .

We now handle the characters of the first type. Let h be the extension of g to S_n whose value on the odd permutations is 0. Write $h = \sum_{\lambda \vdash n} h^{\chi_\lambda}$. Let $\lambda \neq \lambda'$ and let χ be the restriction of χ_λ to A_n . Then $g^{\chi_\lambda} = \chi(1)g * \chi$. We would like to write this convolution in terms of convolutions over S_n to which we will be able to apply Proposition 1.9.

Let $\tilde{\chi} = \chi_\lambda + \chi_{\lambda'}$. Then we have $\tilde{\chi}(\sigma) = 2\chi(\sigma)$ for all $\sigma \in A_n$ and $\tilde{\chi}(\sigma) = 0$ for all $\sigma \in S_n \setminus A_n$. Therefore, the functions $g * \chi$ and $h * \tilde{\chi}$ agree on A_n (note that the first convolution takes place in A_n and the second takes place in S_n). Hence,

$$g^{\chi_\lambda} = \chi(1)g * \chi = \chi(1)(h * \chi_\lambda + h * \chi_{\lambda'})|_{A_n} = (h^{\chi_\lambda} + h^{\chi_{\lambda'}})|_{A_n}.$$

The desired upper bound on g^{χ_λ} now follows from the triangle inequality, when applying Proposition 1.9 to h . □

4. Upper bounding spread independent sets in normal Cayley graphs

In this section, we prove Theorem 1.8, as well as several related results. We begin with a proposition that explains how to combine character bounds with hypercontractivity to upper bound the size of spread independent sets.

Recall that any class function $h : A_n \rightarrow \mathbb{C}$ can be uniquely represented as a linear combination of irreducible characters: $h = \sum_{\chi \in \widehat{A_n}} h_\chi \chi$. The coefficient of χ in this expansion is denoted by $\hat{h}(\chi)$. Note that if $A = \sigma^{S_n}$ for some $\sigma \in A_n$ and $h = 1_A$, then for any $\chi \in \widehat{A_n}$, we have $\hat{h}(\chi) = \mu_{A_n}(A)\chi(\sigma)$.

Proposition 4.1. *For any $\epsilon > 0$, there exist $n_0 \in \mathbb{N}$ and $\delta > 0$ such that the following holds for all $n > n_0$ and all $0 < \alpha < 1 - \epsilon$. Suppose that $I, I' \subseteq G$ are δ -spread subsets of A_n , such that $\mu_{A_n}(I), \mu_{A_n}(I') > e^{-n^{1-\alpha-\epsilon}}$. Suppose additionally that $A \subseteq A_n$ is a normal set with*

$$\frac{\widehat{1_A}(\chi)}{\mu_{A_n}(A)} < \chi(1)^\alpha$$

for every irreducible character χ of A_n . Then the sets I, I' span at least one edge in the Cayley graph $\text{Cay}(A_n, A)$.

Proof. Write $h = \frac{1_A}{\mu_{A_n}(A)}$. Let T_A be the operator associated with the Cayley graph generated by A (i.e., $T_A g = h * g$). Let $W_\chi := \text{span}\{g\chi\}_{g \in A_n}$ (where $g\chi$ is defined as $1_g * \chi$) be the isotypic component of χ . Each W_χ consists of the union of all the irreducible representations ρ_χ that correspond to χ in $L^2(A_n)$. Hence, it follows from the Peter-Weyl theorem that each W_χ is an irreducible $A_n \times A_n$ representation appearing in $L^2(A_n)$ exactly once. The operator T_A commutes with the action of $A_n \times A_n$,

and thus, it follows from Schur’s lemma that the restriction of T_A to W_χ is multiplication by a scalar. To compute the scalar it is sufficient to compute $T_A\chi$. By Frobenius, we therefore obtain that the eigenvalue corresponding to W_χ is given by $\frac{\widehat{h}(\chi)}{\chi(1)}$. Write $f = \frac{1_I}{\mu_G(I)}$ and $g = \frac{1_{I'}}{\mu_G(I')}$. We have

$$\langle T_A f, g \rangle = \sum_{\chi} \frac{\widehat{h}(\chi)}{\chi(1)} \langle f^{=\chi}, g^{=\chi} \rangle. \tag{4.1}$$

By Proposition 3.3, applied with $\epsilon/2$ in place of ϵ , and Theorem 2.14, we therefore have

$$|\langle T_A f, g \rangle - 1| \leq \sum_{\chi \in \widehat{A_n} \setminus \{triv\}} \chi(1)^{\alpha-1} \|f^{=\chi}\|_2 \|g^{=\chi}\|_2 \leq \sum_{\chi \in \widehat{A_n} \setminus \{triv\}} \chi(1)^{-\epsilon/2} = o(1).$$

Hence, we have $\langle T_A f, g \rangle \neq 0$, provided that n is sufficiently large, which implies that there exists an edge between I and I' . □

The following theorem follows by combining Proposition 4.1 with the results of Larsen–Shalev [23] and Larsen–Tiep [25] presented in Section 2.

Theorem 4.2. *For any $\epsilon > 0$, there exist $n_0 \in \mathbb{N}$ and $\delta > 0$, such that the following holds for all $n > n_0$. Let $\sigma \in A_n$ and write $E(\sigma) = \alpha$. Then every δ -spread independent set in the Cayley graph $\text{Cay}(A_n, \sigma^{S_n})$ has density $\leq e^{-n^{1-\alpha-\epsilon}}$.*

Proof. Let $A = \sigma^{S_n}$. As $E(\sigma) = \alpha$, we may apply Theorem 2.4 to deduce that for any character χ of A_n ,

$$\frac{\widehat{1_A}(\chi)}{\mu_{A_n}(A)} = \chi(\sigma) \leq \chi(1)^{\alpha+\epsilon/2}.$$

The assertion now follows from Proposition 4.1, when substituting $\alpha + \epsilon/2$ in place of α and $\epsilon/2$ in place of ϵ . □

Now we are ready to present the proofs of Theorems 1.7 and 1.8.

Proof of Theorem 1.8. The theorem follows immediately by combining Theorem 4.2 with Lemma 2.5. □

Proof of Theorem 1.7. Let $\epsilon > 0$, let δ, n_0 (depending on ϵ) be determined below, and let I be an independent set in $\text{Cay}(A_n, \sigma^{S_n})$, where $n \geq n_0 + t$ and $\sigma \in A_n$ is a permutation with t fixed points. Assume on the contrary that $\mu_{A_n}(I) > \max(e^{-(n-t)^{1/3-\epsilon}}, (n-t)^{-\delta t})$. We obtain a contradiction in a three-step argument.

Step 1: Reducing to the case $t \leq n^{1/3}$. We use the following observation. Let $1 \leq \ell \leq t$ and let σ' be obtained from σ by deleting ℓ of its fixed points. For each ℓ -umvirate τU , with U the subgroup of all permutations that fix a given set of size ℓ , the set $I' = \tau^{-1}I \cap U$ is independent in the Cayley graph $\text{Cay}(U, (\sigma')^U)$ which is isomorphic to $\text{Cay}(A_{n-\ell}, (\sigma')^{S_{n-\ell}})$.

If $t > n^{1/3}$, we may reduce the number of fixed points by applying this process with $\ell = \lceil t - (n-t)^{1/3} \rceil$, choosing an ℓ -umvirate τU such that $\frac{\mu(I \cap \tau U)}{\mu(U)} \geq \mu_{A_n}(I)$. The resulting set I' is independent in the Cayley graph $\text{Cay}(A_{n'}, (\sigma')^{A_{n'}}$ with $n' = n - \ell$, where the number $t' = \lfloor (n-t)^{1/3} \rfloor$ of fixed points of σ' satisfies $(n')^{1/3-\epsilon/2} \leq t' \leq (n')^{1/3}$, provided that n_0 is sufficiently large as a function of ϵ .

To see that $\mu_{A_{n'}}(I') > \max(e^{-(n'-t')^{1/3-\epsilon}}, (n'-t')^{-\delta t'})$, note that for any $\epsilon, \delta > 0$, for any sufficiently large n_0 (depending on ϵ, δ), and for any n, t such that $t \gg n^{1/3-\epsilon}$ and $n-t \geq n_0$, we have $e^{-(n-t)^{1/3-\epsilon}} \gg$

$(n - t)^{-\delta t}$. Hence,

$$\begin{aligned} \mu_{A_{n'}}(I') &\geq \mu_{A_n}(I) > \max(e^{-(n-t)^{1/3-\epsilon}}, (n - t)^{-\delta t}) = e^{-(n-t)^{1/3-\epsilon}} = e^{-(n'-t')^{1/3-\epsilon}} \\ &= \max(e^{-(n'-t')^{1/3-\epsilon}}, (n' - t')^{-\delta t'}), \end{aligned}$$

where the last equality holds since $t' \geq (n')^{1/3-\epsilon/2}$. Therefore, I' satisfies the ‘contrary assumption’ for (n', t') in place of (n, t) . This shows that we may assume w.l.o.g. that $t \leq n^{1/3}$.

Step 2: Reducing to the case where I is δ -spread. Similarly to the first step, we may also assume that I is δ -spread, as otherwise we may iteratively find ℓ -umvirates in which the density of A is $\geq \mu(A)n^{\delta\ell}$ until we are stuck. The set I'' we obtain at the end of this process is an independent δ -spread set in the Cayley graph $\text{Cay}(A_{n''}, (\sigma'')^{A_{n''}})$, where σ'' has t'' fixed points and $n'' = n - (t - t'')$. Its measure satisfies $\mu_{A_{n''}}(I'') \geq \max(e^{-(n''-t'')^{1/3-\epsilon}}, (n'' - t'')^{-\delta t''})$, as in the transition from (n, t) to (n'', t'') , the left term remains unchanged and the increase of the right term is less than the density increase by a factor of $n^{\delta\ell}$ which we obtain in each ℓ -restriction. This shows that we may assume w.l.o.g. that I is δ -spread.

Step 3: Applying Theorem 1.8. Assuming that $t \leq n^{1/3}$ and that I is δ -spread, we can apply Theorem 1.8, with the same value of ϵ , to deduce that

$$\mu(I) < e^{-n^{1/2 - \frac{\log n}{2}t - \epsilon}} \leq e^{-n^{1/3-\epsilon}},$$

which contradicts the assumption $\mu_{A_n}(I) > \max(e^{-(n-t)^{1/3-\epsilon}}, (n - t)^{-\delta t})$. This completes the proof (with δ being the same as in Theorem 1.8 and n_0 being sufficiently large). \square

5. The spreadness of conjugacy classes and their restrictions

In this section, we prove that ‘large’ conjugacy classes of permutations with not-too-many short cycles are spread and that the same holds for their restrictions inside t -umvirates (under certain additional conditions). In order to state our goal more precisely, we introduce some more terminology.

A d -restriction of a function is its restriction to a d -umvurate $U_{I \rightarrow J}$ with $|I| = d$. A k -chain is a restriction of the form $i_1 \rightarrow i_2 \rightarrow \dots \rightarrow i_{k+1}$ (i.e., $i_1 \rightarrow i_2, i_2 \rightarrow i_3, \dots, i_k \rightarrow i_{k+1}$), where i_1, \dots, i_{k+1} are all different. In other words, a k -chain is the restriction to the k -umvurate $U_{I \rightarrow J}$, where $I = (i_1, \dots, i_k)$, and $J = (i_2, \dots, i_{k+1})$. We say that a k_1 -chain $(i_1 \rightarrow i_2 \rightarrow \dots \rightarrow i_{k_1+1})$ and k_2 -chain $(j_1 \rightarrow j_2 \rightarrow \dots \rightarrow j_{k_2+1})$ are *disjoint* if all the coordinates $i_1, \dots, i_{k_1+1}, j_1, \dots, j_{k_2+1}$ are different. We say that the *length* of a k_1 -chain is k_1 . A k -restriction is a k -cycle if it takes the form $i_1 \rightarrow i_2 \rightarrow \dots \rightarrow i_k \rightarrow i_1$. Every d -restriction can be decomposed to disjoint cycles and k -chains that we call the *parts* of the restriction.

We prove the following lemma, as well as a variant of it (Lemma 5.3 below) that will be used in the sequel. For the sake of convenience, we use the term ‘globalness’ throughout this section. Recall that a set is δ -spread if and only if it is n^δ -global.

Lemma 5.1. *There exists $n_0 > 0$ such that the following holds for all $n > n_0$. Let $r \geq 25$, and let $A \subseteq S_n$ be a conjugacy class of density at least e^{-n} , such that all the permutations in A have at most $(r/2)^\ell$ ℓ -cycles for each ℓ . Then A is r -global.*

In order to prove the lemma, we first prove the following claim which calculates the measure of restrictions without cycles.

Claim 5.2. *Let A be a normal set. Let $d > 0$ and let $A_{I \rightarrow J}$ be a d -restriction that consists of t chains. Denote the chain lengths of $A_{I \rightarrow J}$ by $i_1 - 1, \dots, i_t - 1$. Let P be the probability that for a random permutation $\tau \sim A$, and for all $1 \leq \ell \leq t$, the length of the cycle containing ℓ in τ is at least i_ℓ . Then*

$$\mu(A_{I \rightarrow J}) = \mu(A) \cdot P \cdot \left[\left(1 - \frac{t}{n}\right) \left(1 - \frac{t}{n-1}\right) \cdots \left(1 - \frac{t}{n+1-|I|}\right) \right]^{-1}.$$

Proof. Decompose the d -restriction $A_{I \rightarrow J}$ into its chain parts

$$\begin{aligned} a_{11} &\rightarrow a_{12} \rightarrow \dots \rightarrow a_{1i_1}, \\ a_{21} &\rightarrow \dots \rightarrow a_{2i_2}, \\ &\vdots \\ a_{t1} &\rightarrow \dots \rightarrow a_{ti_t}. \end{aligned}$$

Consider the family of d -umvirates $U_{\sigma(I) \rightarrow \sigma(J)} = \sigma U_{I \rightarrow J} \sigma^{-1}$, for all permutations $\sigma \in S_n$ that fix each of a_{11}, \dots, a_{t1} . It is clear that any two non-equal d -umvirates of this form are pairwise disjoint (as sets of permutations). Moreover, since A is normal, the measure of A inside each such d -umvirate is the same.

Without loss of generality, we may assume $a_{11} = 1, \dots, a_{t1} = t$. Observe that $A \cap (\bigcup_{\sigma \in U_{(1, \dots, t) \rightarrow (1, \dots, t)}} U_{\sigma(I) \rightarrow \sigma(J)})$ consists of all the permutations in A for which for all $1 \leq \ell \leq t$, the length of the cycle that contains ℓ is $\geq i_\ell$. Hence, we have

$$\mu(A)P = \mu(A_{I \rightarrow J})\mu(U_{I \rightarrow J})\#\{U_{\sigma(I) \rightarrow \sigma(J)} : \sigma \in U_{(1, \dots, t) \rightarrow (1, \dots, t)}\}$$

Therefore, in order to prove the claim, all that remains is computing the orbit of $U_{I \rightarrow J}$ with respect to the action of the group $U_{(1, \dots, t) \rightarrow (1, \dots, t)}$ on S_n by conjugation. By the orbit stabilizer theorem, its size is

$$\frac{(n - t)!}{(n - i_1 - i_2 - \dots - i_t)!}.$$

As $\mu(U_{I \rightarrow J}) = [n(n - 1) \cdot \dots \cdot (n - i_1 - i_2 - \dots - i_t + t + 1)]^{-1}$, the claim follows by rearranging. \square

Proof of Lemma 5.1. Given a restriction $A_{I \rightarrow J}$ of A , we view it as a composition of two restrictions, denoted by $I_1 \rightarrow J_1$ and $I_2 \rightarrow J_2$, where the restriction $I_1 \rightarrow J_1$ consists of all the cycle parts of $I \rightarrow J$, and the restriction $I_2 \rightarrow J_2$ consists of the chain parts. Let us consider each restriction separately.

Density increase in a restriction consisting of cycles. By the orbit stabilizer theorem, if σ has $f_\sigma(i)$ cycles of length i for each i , then the density of its conjugacy class σ^{S_n} in S_n is $1/\prod(i^{f_\sigma(i)} \cdot f_\sigma(i)!)$. Therefore, when removing a cycle of size ℓ from σ , the measure of the corresponding conjugacy class increases by a factor of $\ell \cdot f_\sigma(\ell)$. By assumption, we have $f_\sigma(\ell) \leq (r/2)^\ell$, and hence, when deleting an ℓ -cycle from σ , the density of the corresponding conjugacy class increases by a factor of $\leq (\ell^{1/\ell} r/2)^\ell$. Set $A' = A_{I_1 \rightarrow J_1}$, and write $k = |I_1|, n' = n - k$. We obtain that $\mu(A'_{I_1 \rightarrow J_1}) \leq r^k \mu(A)$, by sequentially removing cycles from σ and taking into account the measure increment at each step.

Density increase in a restriction consisting of chains. Denote the lengths of the chains in the restriction by $i_1 - 1, i_2 - 1, \dots, i_t - 1$. Note that we may assume that $(i_1 - 1) + \dots + (i_t - 1) < n/3$, for otherwise, the lemma holds trivially. Hence, we have $1 - \frac{t}{n+1-|I|} > 1/2$, and consequently,

$$\left[\left(1 - \frac{t}{n}\right) \left(1 - \frac{t}{n-1}\right) \dots \left(1 - \frac{t}{n+1-|I|}\right) \right]^{-1} \leq 2^n.$$

Therefore, the upper bound $\mu(A_{I \rightarrow J}) = \mu(A'_{I_2 \rightarrow J_2}) \leq 2^{|I_2|} \mu(A') \leq r^{|I|} \mu(A)$ follows immediately from Claim 5.2, applied with A' in place of A . \square

Lemma 5.3. *There exist $n_0 \in \mathbb{N}$ and $C > 0$, such that the following holds for all $n > n_0$ and all $r \geq 20$. Let $\sigma \in S_n$ be a permutation that has at most $r/20$ fixed points and 2-cycles, and at most $(r/20)^{\ell/3}$ ℓ -cycles for each $\ell \geq 3$. Suppose in addition that $A = \sigma^{S_n}$ has density $\geq e^{-\sqrt{n/C}}$. Let $d \leq \frac{\sqrt{n}}{rC}$ and suppose*

that $A_{I \rightarrow J}$ is a d -restriction of A whose parts consist only of 1-chains and 2-chains. Then $A_{I \rightarrow J}$ is r -global.

Proof. Let A be a conjugacy class that satisfies the assumptions of the lemma, and let $A_{I \rightarrow J}$ be a d -restriction of A . Let $A_{I' \rightarrow J'}$ be an ℓ -restriction of $A_{I \rightarrow J}$. Our goal is to show that $\mu(A_{I' \rightarrow J'}) \leq r^\ell \mu(A_{I \rightarrow J})$.

Similarly to the proof of Lemma 5.1, we view the restriction $I' \rightarrow J'$ as a composition of two restrictions, denoted by $I_1 \rightarrow J_1$ and $I_2 \rightarrow J_2$, where the restriction $I_1 \rightarrow J_1$ consists of all the cycle parts, and the restriction $I_2 \rightarrow J_2$ consists of the chain parts. We will show that

$$\frac{\mu(A_{I' \rightarrow J'})}{\mu(A_{I \rightarrow J})} = \frac{\mu(A_{I_1 \rightarrow J_1})}{\mu(A_{(I \cap I_1) \rightarrow (J \cap J_1)})} \cdot \frac{\mu(A_{I' \rightarrow J'}) / \mu(A_{I_1 \rightarrow J_1})}{\mu(A_{I \rightarrow J}) / \mu(A_{(I \cap I_1) \rightarrow (J \cap J_1)})} \leq r^\ell, \tag{5.1}$$

by considering each restriction separately.

Density increase in the restriction $I_1 \rightarrow J_1$ consisting of cycles. Here, we have to bound the density increase $\frac{\mu(A_{I_1 \rightarrow J_1})}{\mu(A_{(I \cap I_1) \rightarrow (J \cap J_1)})}$. It will be more convenient for us to bound the density increase $\mu(A_{I_1 \rightarrow J_1}) / \mu(A)$ instead. To see that this is sufficient, note that by Claim 5.2, we have

$$\mu(A_{(I \cap I_1) \rightarrow (J \cap J_1)}) \geq \mu(A) / 2.$$

Indeed, denoting the lengths of the chains in the restriction $(A_{(I \cap I_1) \rightarrow (J \cap J_1)})$ by $i_1 - 1, i_2 - 1, \dots, i_s - 1$, the claim implies that $\mu(A_{(I \cap I_1) \rightarrow (J \cap J_1)}) \geq \mu(A) \cdot P$, where P is the probability that for a randomly chosen $\tau \sim A$, for all $j = 1, \dots, s$, the length of the cycle containing j in τ is at least i_j . By assumption, $i_j \leq 2$ for all j , the permutations in A have at most $3r/20$ elements in cycles of length ≤ 2 , and we have $s \leq d \leq \frac{n}{rC}$. Hence,

$$P \geq \left(1 - \frac{3r}{20n}\right)^s \geq \left(1 - \frac{3r}{20n}\right)^{\sqrt{n}/rC} > 1/2,$$

provided that C is sufficiently large.

In order to bound $\mu(A_{I_1 \rightarrow J_1}) / \mu(A)$, we observe that as the ‘old’ restriction $I \rightarrow J$ consists only of 1-chains and 2-chains, each cycle of length $l \geq 3$ in $I_1 \rightarrow J_1$ contains at least $l/3$ elements from the ‘new’ restriction $I_1 \setminus I \rightarrow J_1 \setminus J$. Similarly, each cycle of length 1 or 2 in $I_1 \rightarrow J_1$ contains at least one element from the restriction $I_1 \setminus I \rightarrow J_1 \setminus J$. As was shown in the proof of Lemma 5.1, the density increase when removing a single cycle of length l from the conjugacy class of $\sigma \in S_n$ is at most $l \cdot f_\sigma(l)$. By assumption, we have $f_\sigma(l) \leq (r/20)^{l/3}$ for all $l \geq 3$, and also $f_\sigma(l) \leq (r/20)^{l/2}$ for $l = 2$ and $f_\sigma(l) \leq (r/20)^l$ for $l = 1$. It follows that the density increase when removing a cycle that contains l' ‘new’ coordinates is at most $3l' \cdot (r/20)^{l'} \leq (r/8)^{l'}$. Since the number of ‘new’ coordinates is $|I_1 \setminus I| \leq \ell$, by sequentially removing cycles from σ and taking into account the measure increment at each step, we obtain

$$\frac{\mu(A_{I_1 \rightarrow J_1})}{\mu(A_{(I \cap I_1) \rightarrow (J \cap J_1)})} \leq 2 \cdot \frac{\mu(A_{I_1 \rightarrow J_1})}{\mu(A)} \leq 2(r/8)^\ell \leq r^\ell / 4. \tag{5.2}$$

Density increase in the restriction $I_2 \rightarrow J_2$ consisting of chains. Here, we have to bound the ratio between the density increases of the restrictions $A_{I_1 \rightarrow J_1} \rightarrow A_{I_1 \cup I_2 \rightarrow J_1 \cup J_2}$ and $A_{(I \cap I_1) \rightarrow (J \cap J_1)} \rightarrow A_{I \rightarrow J}$. As these restrictions consist only of chains, we can estimate and compare their density increases using Claim 5.2.

As the restriction $I \rightarrow J$ consists only of 1 chains and 2 chains, the value P that corresponds to it in Claim 5.2 is at least $1/2$. Therefore, we may assume that $\ell = |I' \setminus I| \leq 4\sqrt{n}/C$, as otherwise, we have $\mu(A_{I' \rightarrow J'}) \leq 1 \leq 4^\ell \frac{1}{2} \mu(A) \leq 4^\ell \mu(A_{I \rightarrow J})$. We also have $|I| \leq 4\sqrt{n}/C$ by hypothesis.

Denote the chain lengths of the restrictions $I_2 \rightarrow J_2$ and $(I \cap I_2) \rightarrow (J \cap J_2)$ by $i'_1 - 1, \dots, i'_{s'} - 1$ and $i''_1 - 1, \dots, i''_{s''} - 1$, respectively, where $i'_j \geq i''_j$ for any $1 \leq j \leq s''$ and $s' \geq s''$. Note that

$s'' \leq |I \cap I_2| \leq \frac{4\sqrt{n}}{C}$ and that $s' - s'' \leq |I_2 \setminus I| \leq \ell \leq \frac{4\sqrt{n}}{C}$. Let $n' = n - |I_1| \geq n - d - \ell$ and $n'' = n - |I \cap I_1| \geq n - d$.

As the corresponding value of P for the restriction $I \cap I_2 \rightarrow J \cap J_2$ is also $\geq \frac{1}{2}$, we may apply Claim 5.2 to obtain that

$$\frac{\mu(A_{I' \rightarrow J'})/\mu(A_{I_1 \rightarrow J_1})}{\mu(A_{I \rightarrow J})/\mu(A_{(I \cap I_1) \rightarrow (J \cap J_1)})} \leq 2 \frac{\left(1 - \frac{s''}{n'}\right)\left(1 - \frac{s''}{n''-1}\right) \cdots \left(1 - \frac{s''}{n''+1-|I \cap I_2|}\right)}{\left(1 - \frac{s'}{n'}\right)\left(1 - \frac{s'}{n'-1}\right) \cdots \left(1 - \frac{s'}{n'+1-|I_2|}\right)} \leq 4,$$

provided that C is sufficiently large. Combining this with (5.1) and (5.2) completes the proof of the lemma. □

6. Proof of Theorems 1.3, 1.4 and 1.5

In this section, we prove Theorem 1.3, which states that for a sufficiently large n , for any $\sigma \in S_n$ with less than $n^{2/5-\epsilon}$ cycles, we have $(\sigma^{S_n})^2 = A_n$. Then, we deduce from it Theorems 1.4 and 1.5.

The proof of Theorem 1.3 proceeds in two stages. First, we show that we may strengthen the hypothesis of the theorem by adding the assumption that σ has only a few short cycles, and at the same time weaken the assertion to claiming that $(\sigma^{S_n})^2$ contains any fixed-point free $\tau \in A_n$. Afterward, we prove the ‘reduced’ statement.

Formally, in Sections 6.1 and 6.2, we show that it is sufficient to prove the following lemma.

Lemma 6.1. *For any $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$ such that the following holds for all $n > n_0$. Let $\tau \in A_n$ be a permutation with no fixed points. Suppose that $\sigma \in S_n$ has at most $n^{2/5-\epsilon}$ cycles overall and less than 10 cycles of length ℓ for each $2 \leq \ell \leq \log n$. Then $\tau \in (\sigma^{S_n})^2$.*

The proof of Lemma 6.1 is presented in Section 6.3. The proofs of Theorems 1.4 and 1.5 is presented in Section 6.4.

6.1. Explicit computations

For $\sigma \in S_m$ and $\tau \in S_{n-m}$, we write $\sigma \oplus \tau$ for the element in S_n obtained by letting σ act on the first m elements and τ act on the last $n - m$ elements. For a conjugacy class C_1 of S_m and a conjugacy class C_2 of S_{n-m} , we write $C_1 \oplus C_2$ for the conjugacy class obtained by concatenating their cycle decompositions.

Lemma 6.2. *Let C_1, C'_1, C''_1 be conjugacy classes of S_m with $C''_1 \subseteq C_1 \cdot C'_1$, and let C_2, C'_2, C''_2 be conjugacy classes of S_{n-m} with $C''_2 \subseteq C_2 \cdot C'_2$. Then the set $(C_1 \oplus C_2) \cdot (C'_1 \oplus C'_2)$ contains $C''_1 \oplus C''_2$.*

Proof. Let $\pi_1 \in C''_1$ and write $\pi_1 = \sigma_1 \tau_1$ for $\sigma'_1 \in C_1, \tau_1 \in C'_1$. Let $\pi_2 \in C''_2$ and let σ_2, τ_2 be defined similarly. We have $(\sigma_1 \oplus \sigma_2)(\tau_1 \oplus \tau_2) = (\pi_1 \oplus \pi_2)$. □

Lemma 6.3. *There exists $n_0 \in \mathbb{N}$ such that the following holds for any $n > n_0$. Let r, m be integers dividing n , with $r > 1$ and n/m even. Then $(r^{n/r})^2 \supseteq (m^{n/m})$.*

Proof. Let $B = (r^{n/r})$. For $r \geq 4$, by Theorem 2.12, we have $B^2 = A_n$. For $r = 2$, we may apply Theorem 2.13 which says that B^2 contains all the permutations that have an even number of cycles of each length. As n/m is even by hypothesis, this proves the claim.

It now remains to treat the case $r = 3$. For all $m \geq 4$, we may apply Theorem 2.10 to prove our assertion, as $E(m^{n/m}) = 1/m$ by definition. The case $m = 3$ is straightforward, as when squaring a permutation of cycle type $(3^{n/3})$, we obtain a permutation of the same cycle type. Finally, when $m = 2$ and $r = 3$, we use the fact that in S_{12} , we have

$$\begin{aligned} (2, 7, 5)(3, 8, 6)(1, 9, 4)(12, 11, 10) \cdot (1, 2, 3)(7, 4, 11)(8, 5, 12)(9, 6, 10) &= \\ &= (1, 7)(2, 8)(3, 9)(4, 10)(5, 11)(6, 12). \end{aligned}$$

We now write $(3^{n/3}) = C_1 \oplus \dots \oplus C_{n/12}$, where each C_i is the conjugacy class of $(1, 2, 3)(4, 5, 6)(7, 8, 9)(10, 11, 12)$, and write $(2^{n/2}) = D_1 \oplus \dots \oplus D_{n/12}$, where each D_i is the conjugacy class of $(1, 2)(3, 4)(5, 6)(7, 8), (9, 10), (11, 12)$. (Note that in this case, n is indeed divisible by 12 since by assumption, $r = 3$ divides n and $n/m = n/2$ is even). Lemma 6.2 now completes the proof. \square

6.2. Reducing to Lemma 6.1

In this subsection, we reduce the statement of Theorem 1.3 to the statement of Lemma 6.1.

Proof of Theorem 1.3, assuming Lemma 6.1. Our goal is to show that for a sufficiently large n , for any $\sigma \in S_n$ with at most $n^{2/5-\epsilon}$ cycles, the conjugacy class $I = \sigma^{S_n}$ satisfies $I^2 = A_n$. Equivalently, we have to show that $I^2 \cap \tau^{S_n} \neq \emptyset$ for each $\tau \in A_n$. Fix such a τ and write $A = \tau^{S_n}$. We split the proof into two cases:

- o Case 1: The number of fixed points of σ is at most the number of fixed points of τ .
- o Case 2: The number of fixed points of σ is larger than the number of fixed points of τ .

Case 1: σ has no more fixed points than τ . Write t for the number of fixed points in σ . We may restrict both I and A to the t -umvirate $U = U_{[t] \rightarrow [t]}$ to obtain the conjugacy classes I', A' obtained by removing t fixed points from σ, τ . It is clearly sufficient to show that $(I')^2 \supseteq A'$. We may therefore assume that σ is fixed points free. As σ has less than $n^{2/5}$ cycles overall, the assertion now follows from Theorem 2.11.

Case 2: σ has more fixed points than τ . By the same argument as in Case 1, we may assume without loss of generality that τ has no fixed points. By Lemma 2.8 (applied with $\epsilon/3$ in place of ϵ), we have $E(\sigma) \leq 2/5 - 2\epsilon/3$. Theorem 2.10 now completes the proof if $E(\tau) < 1/5$. Suppose on the contrary that $E(\tau) \geq 1/5$. By Lemma 2.6, applied with $m = 6$ and $\epsilon = 1/60$, this implies that for some $i \leq 5$, τ has at least n^δ i -cycles, for some explicit $\delta > 0$. (Actually, this holds for all $n > n_0$, but we may absorb this into our assumption that n is sufficiently large).

Suppose that σ has at least 10 ℓ -cycles for some $2 \leq \ell \leq \log n$, as otherwise, we are done by Lemma 6.1. We may write $\sigma = \sigma_1 \oplus \sigma'_1$ and $\tau = \tau_1 \oplus \tau'_1$, where τ'_1 consists of 2ℓ i -cycles and σ'_1 consists of $2i$ ℓ -cycles. (Note that as $i \leq 5$, σ contains at least $10 \geq 2i$ ℓ -cycles, and as $\ell \leq \log n$, τ contains at least $n^\delta \geq 2\ell$ i -cycles, assuming n is sufficiently large. Hence, the decomposition is possible). By Lemma 6.3, we have $((\sigma'_1)^{S_n})^2 \supseteq (\tau'_1)^{S_n}$. Hence, by Lemma 6.2, it is sufficient to show that $(\sigma_1^{S_n})^2 \supseteq \tau_1^{S_n}$.

We can repeat the deletion process to obtain a sequence of restrictions $\sigma_1, \dots, \sigma_j$ and τ_1, \dots, τ_j , until either $E(\tau_j) < 1/5$ or σ_j has less than 10 ℓ -cycles for all $2 \leq \ell \leq \log n$. (Note that as σ contains at most $n^{2/5}$ cycles, the process terminates when σ_j, τ_j are permutations on at least $n - 10n^{2/5} \log n$ coordinates, and thus, for all $1 \leq l \leq j$, we have $E(\sigma_l) < 2/5 - \epsilon/2$, provided that n is sufficiently large). In the former case, we are done by Theorem 2.10. In the latter case, we are done by Lemma 6.1. This completes the proof. \square

6.3. Proving Lemma 6.1

Proof of Lemma 6.1. The proof consists of four steps.

Step 1: Reducing to the case where τ has many short cycles. If τ has at most $n^{2/5-\epsilon/3}$ cycles of length less than $\frac{10}{\epsilon}$, then by Lemma 2.7, we have $E(\tau) \leq 1/5 - \epsilon/12$ (provided that n is sufficiently large). As $E(\sigma) \leq 2/5 - \epsilon/2$ by Lemma 2.8, Theorem 2.10 implies that $\tau \in (\sigma^{S_n})^2$, completing the proof.

Hence, we may assume that τ has at least $n^{2/5-\epsilon/3}$ cycles of length less than $\frac{10}{\epsilon}$. In particular, there exists $m \leq \frac{10}{\epsilon}$, such that τ has at least $\frac{\epsilon}{10} n^{2/5-\epsilon/3} > n^{2/5-\epsilon/2}$ m -cycles. We fix such an m and proceed with it.

We note that this step, which allows us to assume that τ has more short cycles of a fixed length than the total number of fixed points of σ , is the only step where we crucially use the bound $n^{2/5-\epsilon}$ on the number of cycles in σ . The other steps can be adapted to work with up to $n^{1/2-\epsilon}$ cycles in σ .

Step 2: Removing almost all fixed points of σ by restrictions. We perform a sequence of $2m$ -restrictions intended for removing almost all fixed points of σ , in exchange for removing m -cycles of τ . The restrictions are of the form $I_{S' \rightarrow T'}$, $I_{S' \rightarrow W'}$, and $A_{T' \rightarrow W'}$, for appropriately chosen sets S', T', W' . The way in which these restrictions are used is explained at the next step.

Assume for simplicity that m is even. Each $2m$ -restriction involves $4m$ coordinates denoted by

$$x_1, x_2, \dots, x_m, y_1, \dots, y_m, x'_1, \dots, x'_m, y'_1, \dots, y'_m,$$

where $x_i = y_i$ and $x'_i = y'_i$ for all odd i , and except for this, all the coordinates are pairwise distinct. We define the restrictions by setting

$$S' = (x_1, x_2, \dots, x_m, x'_1, x'_2, \dots, x'_m), \quad T' = (y_1, y_2, \dots, y_m, y'_m, y'_1, \dots, y'_{m-1}),$$

$$W' = (y_m, y_1, \dots, y_{m-1}, y'_1, y'_2, \dots, y'_m).$$

As a result, each of the restrictions $I_{S' \rightarrow T'}$, $I_{S' \rightarrow W'}$ consists of $m/2$ 1-cycles, $m/2$ 1-chains and $m/2$ 2-chains, while the restriction $A_{T' \rightarrow W'}$ consists of the two m -cycles $(y_1, y_2, \dots, y_m, y_1)$ and $(y'_1, y'_2, \dots, y'_m, y'_1)$.

We perform $s = \lfloor \frac{2f_\sigma}{m} \rfloor$ such $2m$ -restrictions, where f_σ is the number of fixed points of σ . As a result, all fixed points of σ , except for at most $m/2 - 1$, are removed. (Note that we do not ‘get stuck’ on the side of A since the number of m -cycles in τ is much larger than the number of fixed points of σ , bounded by $n^{2/5-\epsilon}$). We let $I_{S \rightarrow T}$, $I_{S \rightarrow W}$ and $A_{T \rightarrow W}$ be the sets obtained at the end of the process.

Step 3: Reducing to edges between vertex sets in a Cayley graph. First, we perform a simple shifting procedure which allows us to ‘get rid’ of the coordinates in S, T and W . We let π_1 be the permutation that fixes the set of coordinates not appearing in W and sends the tuple W to the tuple T . The permutation π_1 consists of $2s$ m -cycles on the elements appearing in W . Let π_2 be an arbitrary permutation that sends S to W . Consider the sets $B_1 = \pi_2 I \pi_1, B_2 = \pi_2 I, B_3 = A \pi_1$. As $(B_2)^{-1} B_1 = I^{-1} I \pi_1$ and $I^{-1} I = I^2$; it is sufficient to prove that $(B_2)^{-1} B_1$ has a nonempty intersection with $B_3 = A \pi_1$. In fact, we show that $(B_2^{-1})_{W \rightarrow W} (B_1)_{W \rightarrow W}$ has a nonempty intersection with $(B_3)_{W \rightarrow W}$.

Assume without loss of generality that $W = \{(n - 2sm + 1, \dots, n)\}$ and identify S_{n-2ms} with the set of permutations in S_n fixing W . Then $(A \pi_1)_{W \rightarrow W}$ is the conjugacy class $(\tau')^{S_{n-2ms}}$ of S_{n-2ms} , obtained by deleting $2s$ m -cycles from τ . Our goal is showing that the sets $(B_2)_{W \rightarrow W}, (B_1)_{W \rightarrow W}$ span an edge in the Cayley graph $\text{Cay}(S_n, (\tau')^{S_{n-2ms}})$. Furthermore, we can reduce the problem to A_{n-2ms} (i.e., assume w.l.o.g. that B_2, B_3 are contained in A_{n-2ms} by multiplying all odd permutations in B_2 by some fixed permutation and multiplying all odd permutations in B_3 by its inverse).

Step 4: Completing the proof using Proposition 4.1. The sets $(B_1)_{W \rightarrow W}, (B_2)_{W \rightarrow W}$ are shifts of the sets $I_{S \rightarrow T}, I_{S \rightarrow W}$, and therefore inherit their spreadness. In order to apply Proposition 4.1, we establish the δ -spreadness of $I_{S \rightarrow T}$ and $I_{S \rightarrow W}$. We may view the restrictions $I_{S \rightarrow T}$ and $I_{S \rightarrow W}$ as a composition of two restrictions – a restriction that removes all fixed points except for at most $m/2 - 1$ and a restriction that consists only of 1-chains and 2-chains. By the assumption on σ , this allows us to apply Lemma 5.3, with any constant $r > \max(10m, 200)$, to deduce that the sets B_2 and B_3 are r -global. It follows that B_2, B_3 are δ -spread for an arbitrarily small $\delta > 0$, provided that n is sufficiently large.

As follows from Claim 5.2, a restriction that consists of 1-cycles, 1-chains and 2-chains cannot decrease the measure of a conjugacy class by more than a factor of 2, and hence, we have $\mu(I'), \mu(I'') \geq e^{-n^{2/5-2\epsilon}}$. Furthermore, τ' is fixed-point free, and hence, by Lemma 2.5, we have $E(\tau') \leq 1/2$. Consequently, by Theorem 2.2, we have

$$\frac{\widehat{1}_{A'}(\chi)}{\mu(A')} = \chi(\tau') < \chi(1)^{1/2+\epsilon},$$

for any $\chi \in \widehat{A_{n-2ms}}$, provided that n is sufficiently large. Hence, Proposition 4.1, applied with $\alpha = 1/2+\epsilon$, implies that the sets I', I'' span an edge in the Cayley graph $\text{Cay}(A_{n-2ms}, A')$, completing the proof. \square

6.4. Proving Theorems 1.4 and 1.5

In the proof of Theorem 1.4, we use the following standard fact regarding the cycle structure of random permutations. For $\sigma \in S_n$, denote by $C(\sigma)$ the total number of cycles in σ .

Proposition 6.4 [9, Corollary 1.6]. *For any $n \in \mathbb{N}$ and any $0 \leq m \leq n$, we have $\Pr_{\sigma \sim S_n}[C(\sigma) = m] \leq \frac{(2 \log(n))^{m-1}}{(m-1)!}$.*

Proof of Theorem 1.4. Let A be a normal set with $\mu(A) \geq e^{-n^{2/5-\epsilon}}$. We claim that for a sufficiently large n , A contains a conjugacy class $C = \sigma^{S_n}$ with $\mu(C) \geq e^{-n^{2/5-\epsilon/3}}$. Once we show this, the assertion of the theorem follows by applying Theorem 1.3 to C .

It is clearly sufficient to show that for a sufficiently large n , the union of all conjugacy classes $C' = (\sigma')^{S_n}$ with $\mu(C') < e^{-n^{2/5-\epsilon/3}}$ has measure $< e^{-n^{2/5-\epsilon}}$.

Recall that $\mu(C') = [\prod_{i=1}^n (i^{f_{\sigma'}(i)} \cdot f_{\sigma'}(i)!)]^{-1}$. Hence, by taking logarithms, the assumption $\mu(C') < e^{-n^{2/5-\epsilon/3}}$ implies

$$\sum_{i=1}^n f_{\sigma'}(i) \log(i) + f_{\sigma'}(i) \log(f_{\sigma'}(i)) \geq n^{2/5-\epsilon/3},$$

and subsequently, $C(\sigma') = \sum_{i=1}^n f_{\sigma'}(i) \geq n^{2/5-2\epsilon/3}$, provided that n is sufficiently large. By Proposition 6.4, the probability that a random σ' satisfies this condition is less than $e^{-n^{2/5-\epsilon}}$, provided that n is sufficiently large. The assertion follows. \square

Proof of Theorem 1.5. Let A be a normal subset of A_n of density $\geq e^{-n^{2/5-\epsilon}}$. If A is a normal subset of S_n as well, then the statement follows from Theorem 1.4. Otherwise, A contains a permutation σ with $\sigma^{A_n} \neq \sigma^{S_n}$, in which case the statement follows from Theorem 2.9. \square

Acknowledgements. This work was done while N. L. and O. S. were visiting the Simons Institute for the Theory of Computing.

Competing interest. The authors certify that there are no actual or potential competing interest.

Financial support. N. K. is supported by the Israel Science Foundation (grant no. 2669/21). N. L. is supported by the Israel Science Foundation (grant no.1980/22).

References

- [1] E. Bertram, ‘Even permutations as a product of two conjugate cycles’, *J. Combin. Theory, Ser. A* **12**(3) (1972), 368–380.
- [2] J. L. Brenner, ‘Covering theorems for finite nonabelian simple groups. IX. How the square of a class with two nontrivial orbits in S_n covers A_n ’, *Ars Combin.* **4** (1977), 151–176.
- [3] L. N. Coregliano and F. G. Jeronimo, ‘Tighter bounds on the independence number of the Birkhoff graph’, *European J. Combin.* **105**(Paper No. 103564) (2022), 29.
- [4] D. Ellis, E. Friedgut and H. Pilpel, ‘Intersecting families of permutations’, *J. Amer. Math. Soc.* **24**(3) (2011), 649–682.
- [5] D. Ellis, N. Keller and N. Lifshitz, ‘Stability for the Complete Intersection Theorem, and the forbidden intersection problem of Erdős and Sós’, *J. Eur. Math. Soc.* **26**(5) (2020), 1611–1654.
- [6] D. Ellis and N. Lifshitz, ‘Approximation by juntas in the symmetric group, and forbidden intersection problems’, *Duke Math. J.* **171**(7) (2022), 1417–1467.
- [7] Y. Filmus, ‘Spectral methods in extremal combinatorics’, PhD thesis, University of Toronto, 2013.
- [8] Y. Filmus, G. Kindler, N. Lifshitz and D. Minzer, ‘Hypercontractivity on the symmetric group’, *Forum Math. Sigma* **12** (2024), e6.
- [9] K. Ford, ‘Cycle type of random permutations: A toolkit’, *Discrete Anal.* **2022** (2022), 9.
- [10] M. Garonzi and A. Maróti, ‘Alternating groups as products of four conjugacy classes’, *Arch. Math.* **116** (2021), 121–130.
- [11] C. Godsil and K. Meagher, *Erdos-Ko-Rado Theorems: Algebraic Approaches* (Cambridge University Press, 2016).
- [12] R. M. Guralnick, M. Larsen and P. H. Tiep, ‘Character levels and character bounds’, in *Forum of Mathematics, Pi* vol. 8 (Cambridge University Press, 2020), e2.
- [13] D. H. Husemoller, ‘Ramified coverings of Riemann surfaces’, *Duke Math. J.* **29**(1) (1962), 167–174.

- [14] J. Kahn, G. Kalai and N. Linial, 'The influence of variables on boolean functions', in *29th Annual Symposium on Foundations of Computer Science* (IEEE, 1988), 68–80.
- [15] D. Kane, S. Lovett and S. Rao, 'The independence number of the Birkhoff polytope graph, and applications to maximally recoverable codes', *SIAM J. Comput.* **48**(4) (2019), 1425–1435.
- [16] P. Keevash and N. Lifshitz, 'Sharp hypercontractivity for symmetric groups and its applications', Preprint, 2023, [arXiv:2307.15030](https://arxiv.org/abs/2307.15030).
- [17] P. Keevash, N. Lifshitz, E. Long and D. Minzer, 'Hypercontractivity for global functions and sharp thresholds', *J. Amer. Math. Soc.* **37** (2024), 245–279.
- [18] N. Keller and N. Lifshitz, 'The junta method for hypergraphs and the Erdős-Chvátal simplex conjecture', *Adv. Math.* **392** (2021), 107991.
- [19] N. Keller, N. Lifshitz and O. Marcus, 'Sharp hypercontractivity for global functions', Preprint, 2023, [arXiv:2307.01356](https://arxiv.org/abs/2307.01356).
- [20] N. Keller, N. Lifshitz, D. Minzer and O. Sheinfeld, 'On t -intersecting families of permutations', *Adv. Math.* **445** (2024), 109650.
- [21] S. Khot, D. Minzer and M. Safra, 'Pseudorandom sets in Grassmann graph have near-perfect expansion', *Ann. of Math.* **198** (1) (2023), 1–92.
- [22] A. Kupavskii and D. Zakharov, 'Spread approximations for forbidden intersections problems', *Adv. Math.* **445** (2024), 109653.
- [23] M. Larsen and A. Shalev, 'Characters of symmetric groups: sharp bounds and applications', *Invent. Math.* **174** (2008), 645–687.
- [24] M. Larsen and A. Shalev, 'Word maps and Waring type problems', *J. Amer. Math. Soc.* **22**(2) (2009), 437–466.
- [25] M. Larsen and P. H. Tiep, 'Squares of conjugacy classes in alternating groups', Preprint, 2023, [arXiv:2305.04806](https://arxiv.org/abs/2305.04806).
- [26] M. W. Liebeck and A. Shalev, 'Diameters of finite simple groups: sharp bounds and applications', *Ann. of Math.* (2001), 383–406.
- [27] M. W. Liebeck and A. Shalev, 'Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks', *J. Algebra* **276**(2) (2004), 552–601.
- [28] N. Lifshitz and A. Marmor, 'Bounds for characters of the symmetric group: A hypercontractive approach', Preprint, 2023, [arXiv:2308.08694](https://arxiv.org/abs/2308.08694).
- [29] R. O'Donnell, *Analysis of Boolean Functions* (Cambridge University Press, 2014).
- [30] A. Shalev, 'Word maps, conjugacy classes, and a noncommutative Waring-type theorem', *Ann. of Math.* (2009), 1383–1416.
- [31] A. Shalev, 'Covering and growth for group subsets and representations', in *European Congress of Mathematics* (EMS Press, Berlin, 2023), 465–487.
- [32] U. Vishne, 'Mixing and covering in the symmetric groups', *J. Algebra* **205**(1) (1998), 119–140.