Rapid growth in finite simple groups

Martin W. Liebeck, Gili Schul, Aner Shalev

March 1, 2016

Abstract

We show that small normal subsets A of finite simple groups grow very rapidly – namely, $|A^2| \geq |A|^{2-\epsilon}$, where $\epsilon > 0$ is arbitrarily small. Extensions, consequences, and a rapid growth result for simple algebraic groups are also given.

The first and third authors acknowledge the support of EPSRC Mathematics Platform grant EP/I019111/1. The second and third authors acknowledge the support of an ERC advanced grant 247034 and of an Israel Science Foundation grant 1117/13. The third author acknowledges the support of the Vinik Chair of Mathematics which he holds.

2010 *Mathematics Subject Classification:* 20D06, 20F69

1 Introduction

In recent years there has been intense interest in the growth of powers of subsets of finite (nonabelian) simple groups. For example, the remarkable product theorem of [1, 12] states that if G is a simple group of Lie type, and A is any subset generating G, then either $A^3 = G$ or $|A^3| \geq |A|^{1+\epsilon}$, where $\epsilon > 0$ depends only on the rank of G. See also [6] for important earlier results in this direction, and [4, 5] for the groundbreaking results on $L_2(p)$ and $L_3(p)$.

The case where the subset A is a conjugacy class and G is an arbitrary finite simple group was considered in [13] before the product theorem was established. Theorem 2.7 of [13] shows that for any $\delta > 0$ there is $\epsilon > 0$ depending on δ such that $|A^3| \geq |A|^{1+\epsilon}$ for any class A of size at most $|G|^{1-\delta}$; here G is any finite simple group, and ϵ does not depend on its rank or degree.

While the above mentioned results establish 3-step growth, results on 2-step growth were also obtained. In [13, 10.4] it is shown that if A is a conjugacy class of a finite simple group G of Lie type, then $|A^2| \geq |A|^{1+\epsilon}$ where $\epsilon > 0$ now depends on the rank of G.

Subsequently, growth of normal subsets was also studied. Recall that a subset A of a group G is said to be *normal* if it is closed under conjugation, namely, it is a union of conjugacy classes of G. In [3, 1.5] it is shown that there are absolute constants $b \in \mathbb{N}$ and $\epsilon > 0$ such that for any normal subset A of a finite simple group G, either $A^b = G$ or $|A^2| \geq |A|^{1+\epsilon}$.

In this paper we obtain a stronger growth result for normal subsets, as follows.

Theorem 1.1. *Given any $\epsilon > 0$, there exists $b \in \mathbb{N}$ such that for any normal subset A of any finite simple group G, either $A^b = G$ or $|A^2| \geq |A|^{2-\epsilon}$.*

Obviously $|A^2| \leq |A|^2$, so the result says that small normal subsets of simple groups grow almost as fast as possible. Theorem 1.1 follows from the following result.

Theorem 1.2. *Given any $\epsilon > 0$, there exists $\delta > 0$ such that if A is a normal subset of a finite simple group G satisfying $|A| \leq |G|^{\delta}$, then $|A^2| \geq |A|^{2-\epsilon}$.*

Note that some upper bound on the size of A is needed in order for the above conclusion to be true. The study of the growth of large normal subsets requires different methods and will be carried out elsewhere.

We will deduce Theorem 1.2 from the following more general result.

Theorem 1.3. *Given any $\epsilon > 0$, there exists $\delta > 0$ such that if A_1, A_2 are normal subsets of a finite simple group G satisfying $|A_i| \leq |G|^{\delta}$ for $i = 1, 2$, then $|A_1 A_2| \geq (|A_1|\,|A_2|)^{1-\epsilon}$.*

Let us now briefly describe the strategy of the proof of Theorem 1.3.

The theorem holds vacuously for simple groups of bounded order, or of bounded Lie rank, since for these groups we may choose δ so small that $|A| > |G|^\delta$ for all nontrivial classes (see Lemma 2.3 below); this enables us to ignore the sporadic groups and the exceptional groups of Lie type. It therefore remains to prove Theorem 1.3 for simple classical groups of large rank, and for alternating groups of large degree.

Next, we reduce Theorem 1.3 to the case where the normal subsets $A_1, A_2 \subseteq G$ are single conjugacy classes. This is done using a certain zeta function encoding the class sizes, and showing that a normal subset must contain a conjugacy class of comparable size (see Theorem 2.2 below for the exact formulation).

Our proof of Theorem 1.3 for conjugacy classes is based on results from [9, 10, 11], together with some new results on the size of the conjugacy classes in classical groups and in symmetric groups; see e.g. Propositions 3.1 and 4.1 below. In fact, under the assumptions of Theorem 1.3, we establish a stronger conclusion: there exists a single conjugacy class $C \subseteq A_1A_2$ such that $|C| \geq (|A_1|\,|A_2|)^{1-\epsilon}$. The notion of the support of elements of G plays a key role in our arguments.

A similar result for k subsets follows inductively from Theorem 1.3:

Corollary 1.4. *Given $\epsilon > 0$ and $k \in \mathbb{N}$ there exists $\delta > 0$ such that if $A_1, \ldots, A_k \subseteq G$ are normal subsets of a finite simple group G with $|A_i| \leq |G|^\delta$, then $|A_1 \cdots A_k| \geq (|A_1| \cdots |A_k|)^{1-\epsilon}$. In particular, $|A^k| \geq |A|^{k-\epsilon}$ for every normal subset A of G satisfying $|A| \leq |G|^\delta$, where δ depends on ϵ and k.*

We also prove a result analogous to Theorem 1.3 for algebraic groups over algebraically closed fields:

Theorem 1.5. *Given any $\epsilon > 0$, there exists $\delta > 0$ such that if A_1, A_2 are conjugacy classes in a simple algebraic group G satisfying $\dim A_i \leq \delta \dim G$ for $i = 1, 2$, then the product A_1A_2 contains a conjugacy class of dimension at least $(1-\epsilon)(\dim A_1 + \dim A_2)$.*

The layout of the paper is as follows. In Section 2 we perform the reduction to conjugacy classes described above. Section 3 is devoted to classical groups of large rank. We study the size of conjugacy classes in these groups, and show that it is closely related to the support of the elements in the class; see Propositions 3.1 and 3.4 for more details. Section 3 concludes the proof of Theorem 1.3 for classical groups. Then, in Section 4, we prove Theorem 1.3 for symmetric and alternating groups, and derive some stronger results. Finally in Section 5 we deduce Theorems 1.1 and 1.5 as well as Corollary 1.4.

2 Reduction to conjugacy classes

We start with some notation. Throughout, finite simple groups G are assumed to be nonabelian, and for subsets $A_1, \ldots, A_k$ of G we define $A_1 \cdots A_k = \{a_1 \cdots a_k : a_i \in A_i\}$. The conjugacy class of $x \in G$ in G is denoted by x^G. We define the *rank* of a finite simple group to be its untwisted Lie rank if it is a group of Lie type, and to be its degree if it is an alternating group.

For a positive integer i and a finite group G, let $c_i(G)$ denote the number of conjugacy classes of G of size i. For $s \in \mathbb{R}$, the function

$$\eta^G(s) = \sum_{i \in \mathbb{N}} c_i(G) i^{-s} = \sum_C |C|^{-s}$$

(where the second sum is over conjugacy classes C), was defined in [11] and studied for simple groups G.

We need the following two results which are of independent interest.

Proposition 2.1. *For any $\epsilon > 0$ there exists N such that if G is a finite simple group of rank at least N, then for all $m \in \mathbb{N}$, G has at most m^ϵ conjugacy classes of size at most m.*

Proof. The alternating (and symmetric) case is covered in the proof of [10, 2.3]. So now assume that G is of Lie type. Choosing N large enough we may assume that G is a classical group. Let $\epsilon > 0$. Theorem 1.10(ii) of [11] shows that $\eta^G(\epsilon/2) \to 1$ as $\mathrm{rank}(G) \to \infty$. Hence there exists N such that for G of rank at least N we have $\sum_{i \geq 1} c_i(G) i^{-\epsilon/2} \leq 1 + \epsilon/2$, and it follows that $\sum_{i=1}^m c_i(G) \leq (1+\epsilon/2) m^{\epsilon/2}$. For $m \geq 3$ we have $1 + \epsilon/2 \leq e^{\epsilon/2} \leq m^{\epsilon/2}$, which implies $\sum_{i=1}^m c_i(G) \leq m^\epsilon$ as required. Finally, the last inequality holds trivially for $m = 1, 2$ (since $c_2(G) = 0$). The conclusion follows. ∎

The next result shows that normal subsets of finite simple groups of large rank contain a relatively large conjugacy class.

Theorem 2.2. *For any $\epsilon > 0$ there exists N such that if G is a finite simple group (or a symmetric group) of rank at least N, and A is a non-empty normal subset of G, then A contains a conjugacy class C such that $|C| \geq |A|^{1-\epsilon}$.*

Proof. Let $\epsilon > 0$, and let N be as in the conclusion of Proposition 2.1. Let G be a finite simple group of rank at least N, and A a normal subset of G. Denote by m the maximal size of a conjugacy class contained in A. Then A is a union of at most m^ϵ classes, each of size at most m, and hence $|A| \leq m^{1+\epsilon}$. This implies that $m \geq |A|^{1-\epsilon}$, and the result follows. ∎

Note that Theorem 2.2 improves [10, 2.4] in the case where the rank is unbounded.

We now reduce Theorem 1.3 to the case where the normal subsets in the theorem are single conjugacy classes. First we need

Lemma 2.3. *For any $N \in \mathbb{N}$, there exists $\delta > 0$ such that if a finite simple group G has a nontrivial conjugacy class of size at most $|G|^\delta$, then* $\mathrm{rank}(G) \geq N$.

Proof. The case of alternating groups is trivial, since the order of the group is then bounded in terms of the rank. Now suppose $G = G(q)$ is of Lie type over $\mathbb{F}_q$ of rank r. Since $|x^G| = |G : C_G(x)|$, the size of a nontrivial conjugacy class in G is at least the minimal index of a proper subgroup, which is at least cq^r, where $r = \mathrm{rank}(G)$ and $c > 0$ is a constant, as can be seen from [7, Tables 5.2A, 5.3A]. The result follows since $|G| < q^{4r^2}$. ∎

Lemma 2.4. *It suffices to prove Theorem* 1.3 *in the case where A_1, A_2 are single conjugacy classes.*

Proof. Assume the conclusion of Theorem 1.3 holds in the case of conjugacy classes. Namely, given $\epsilon > 0$, there exists $\delta_1 > 0$ such that if C_1, C_2 are conjugacy classes of finite simple group G of size at most $|G|^{\delta_1}$, then $|C_1C_2| \geq (|C_1|\,|C_2|)^{1-\epsilon/2}$.

Applying Theorem 2.2, choose N such that whenever A is a normal subset of a simple group G of rank at least N, then A contains a conjugacy class C such that $|C| \geq |A|^{1-\epsilon/2}$.

By Lemma 2.3, there exists $\delta_2 > 0$ such that if a finite simple group G has a nontrivial conjugacy class of size at most $|G|^{\delta_2}$, then $\mathrm{rank}(G) \geq N$. Define $\delta = \min(\delta_1, \delta_2)$.

Let G be a finite simple group, and let A_1, A_2 be normal subsets of G satisfying $|A_i| \leq |G|^\delta$ for $i = 1, 2$. Let C_i be a largest conjugacy class in A_i, so that $|C_i| \geq |A_i|^{1-\epsilon/2}$. Then

$$|A_1A_2| \geq |C_1C_2| \geq (|C_1|\,|C_2|)^{1-\epsilon/2} \geq (|A_1|\,|A_2|)^{(1-\epsilon/2)^2} \geq (|A_1|\,|A_2|)^{1-\epsilon},$$

as required. ∎

3 Classical groups

In this section we relate the size of a conjugacy class in a classical group to the support of the elements in the class; we then use our results to prove Theorem 1.3 for classical groups. By Lemma 2.3, we need only prove the result for classical groups of large dimension.

Let G be one of the classical groups $L_n^{\pm}(q)$, $PSp_n(q)$ or $P\Omega_n^{\pm}(q)$, and let $V = V_n(q^u)$ be the natural module for G with n large, where $u = 2$ if G is unitary and $u = 1$ otherwise. Let $\bar{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}_q$, and let $\bar{V} = V \otimes \bar{\mathbb{F}}$. Let $x \in G$, and let $\hat{x}$ be a preimage of x in $GL(V)$. Define

$$\nu(x) = \nu_{V,\bar{\mathbb{F}}}(x) = \min\{\operatorname{codim}\ker(\hat{x} - \lambda I) : \lambda \in \bar{\mathbb{F}}^*\}.$$

We shall refer to $\nu(x)$ as the *support* of x.

The following proposition, which is an extension of [9, 3.4], shows that $\nu(x)$ is closely related to the size of the conjugacy class of x. Define

$$a(G) = \begin{cases} 1, & \text{if } G = L_n^{\pm}(q) \\ \frac{1}{2}, & \text{otherwise} \end{cases}$$

Proposition 3.1. *Suppose that $\nu(x) = s < \frac{n}{2}$, and let $a = a(G)$. There are absolute constants $c, c' > 0$ such that*

$$cq^{2as(n-s-1)} \leq |x^G| \leq c'q^{as(2n-s+1)}.$$

Proof. In the case where x has prime order this is [9, 3.4], but the general case requires quite a bit more argument.

Write $\hat{x} = tu$, where t is the semisimple part and u the unipotent part.

First suppose that $G = L_n(q)$. Since $\nu(t) \leq \nu(x) = s < \frac{n}{2}$, the semisimple part t has an eigenvalue $\lambda \in \bar{\mathbb{F}}$ of multiplicity $n - s > \frac{n}{2}$. Then λ must lie in $\mathbb{F}_q^*$. Denote by V_λ the λ-eigenspace of t, and let u act on V_λ as $\sum_i J_i^{n_i}$, where J_i is a Jordan block of size i. Writing $k = n - \sum in_i$, we have

$$\hat{x} = \lambda \sum J_i^{n_i} \oplus K = x_1 \oplus K,$$

where $x_1 = \lambda \sum J_i^{n_i} \in GL_{n-k}(q)$, $K \in GL_k(q)$, and $n = k + \sum in_i = s + \sum n_i$. If we write

$$f = \sum_i in_i^2 + 2\sum_{i<j} in_i n_j, \tag{1}$$

then $|C_{GL_{n-k}(q)}(x_1)| \sim q^f$ (see [8, 3.1]), and hence

$$cq^{n^2-f-k^2} < |x^G| < c'q^{n^2-f-k}, \tag{2}$$

where $c, c' > 0$ are constants. Now $\nu(x_1) = n - k - \sum n_i = s - k$. So the inequalities labelled (1) and (2) in the proof of [9, 3.4(i)] show that

$$(n-s)^2 + s - k \leq f \leq (n-s)^2 + (s-k)^2.$$

Putting this into (2) gives the conclusion of the lemma for the case $G = L_n(q)$.

Next consider the unitary group $G = U_n(q)$. Again the semisimple part t has an eigenspace V_λ of dimension greater than $\frac{n}{2}$. Write $(\ ,\ )$ for the unitary form on V preserved by G, and $\alpha \to \bar{\alpha}$ for the involutory automorphism of the field $\mathbb{F}_{q^2}$. There is a nonsingular vector $v \in V_\lambda$, so $0 \neq (v,v) = (v\hat{x}, v\hat{x}) = \lambda\bar{\lambda}(v,v)$, and hence $\lambda\bar{\lambda} = 1$. Also V_λ is a non-degenerate subspace, since its radical must be contained in the radical of the whole space V. Hence, letting u acts on V_λ as $\sum_i J_i^{n_i}$, we have as above

$$\hat{x} = \lambda \sum J_i^{n_i} \perp K,$$

where $K \in GU_k(q)$ and $n = k + \sum in_i = s + \sum n_i$. Now we argue exactly as in the previous paragraph.

Next let $G = PSp_n(q)$. Here t has an eigenspace V_λ of dimension greater than $\frac{n}{2}$, and λ must be ± 1 and V_λ non-degenerate. So $\hat{x} = \lambda \sum J_i^{n_i} \perp K = x_1 \perp K$ with $K \in Sp_k(q)$ and $n = k + \sum in_i = s + \sum n_i$.

Suppose q is odd. Then by [8, 3.1] we have $|C_{Sp_{n-k}(q)}(x_1)| \sim q^{g/2}$, where

$$g = \sum_i in_i^2 + 2\sum_{i<j} in_i n_j + \sum_{i\ odd} n_i. \tag{3}$$

As $|Sp_n(q)| \sim q^{\frac{1}{2}(n^2+n)}$, it follows that

$$cq^{\frac{1}{2}(n^2+n-g-k^2-k)} < |x^G| < c'q^{\frac{1}{2}(n^2+n-g-k)}. \tag{4}$$

The inequalities labelled (1) and (2) in the proof of [9, 3.4(ii)] show that

$$(n-s)^2 + n - s \leq g \leq (n-s)^2 + (s-k)^2 + n - k.$$

Putting this into (4) gives the conclusion of the lemma for $G = PSp_n(q)$ with q odd.

Now suppose q is even. This is slightly more complicated, as in general there can be many unipotent classes in a symplectic group having the same Jordan form. The general form of a unipotent element, and its centralizer, is given by [8, 6.2, 7.3], from which it can be seen that $|C_{Sp_{n-k}(q)}(x_1)| \sim q^{\frac{1}{2}g'}$, where

$$g \leq g' \leq g + 2\sum_{i, n_i\ even} n_i$$

and g is as above. Then $g' \geq g \geq (n-s)^2 + n - s$, and the lower bound for $|x^G|$ follows as before. As for the upper bound, observe that

$$\begin{aligned}(s-k)^2 + n - k &= (\textstyle\sum (i-1)n_i)^2 + \sum in_i \\ &\geq \textstyle\sum (i-1)n_i^2 + 2\sum_{i<j}(i-1)n_i n_j + \sum_{i\ odd} n_i + 2\sum_{i\ even} n_i \\ &= g + 2\textstyle\sum_{i\ even} n_i - (n-s)^2 \\ &\geq g' - (n-s)^2.\end{aligned}$$

Hence $g' \leq (n-s)^2 + (s-k)^2 + n - k$, and the upper bound for $|x^G|$ follows as before. This completes the proof for the symplectic groups.

The argument for orthogonal groups is very similar: again we have $\hat{x} = \lambda \sum J_i^{n_i} \perp K = x_1 \perp K \in O_{n-k}(q) \times O_k(q)$, where $\lambda = \pm 1$, $k < \frac{n}{2}$ and $n = k + \sum in_i = s + \sum n_i$. If we define

$$h = \sum_i in_i^2 + 2\sum_{i<j} in_i n_j - \sum_{i \ odd} n_i,$$

then for q odd we have $|C_{O_{n-k}(q)}(x_1)| \sim q^{h/2}$, and for q even we have $|C_{O_{n-k}(q)}(x_1)| \sim q^{h'/2}$, where $h - 2\sum_{i,n_i \ even} n_i \leq h' \leq h$ (see [8, 3.1, 6.2, 7.3]). Arguing as for the symplectic case, we see that

$$(n-s)^2 - (n-k) - (s-k) \leq h' \leq (n-k)^2 + (s-k)^2 + 2(s-k) - n,$$

and the conclusion follows. ∎

Lemma 3.2. *Let $x \in G$ with $\nu(x) = s$, and suppose that $|x^G| \leq |G|^{\frac{1}{4}}$. Then $s < \frac{n}{2} - 1$.*

Proof. First suppose $G = L_n(q)$, and write $\hat{x} = tu$ as in the previous proof. Recall our assumption that n is large. The centralizer of t in $GL_n(q)$ is of the form $C = \prod GL_{n_i}(q^{a_i})$, where $\sum n_i a_i = n$. Since this must have order greater than $|G|^{\frac{3}{4}}$, it follows that the largest factor of C is $GL_r(q)$, where $r > \frac{n}{2}$ and $q^{r^2+(n-r)^2} > |G|^{\frac{3}{4}}$. Hence in fact $r > \alpha n$, where $\alpha = 0.85$. Let V_r be the r-dimensional eigenspace for t, and let u act on V_r as $\sum J_i^{n_i}$. So as in the previous proof we have

$$\hat{x} = \lambda \sum J_i^{n_i} \oplus K = x_1 \oplus K \in GL_r(q) \times GL_{n-r}(q).$$

Let $s_1 = \nu(x_1)$, so that $s \leq s_1 + n - r$. Define f as in (1) in the previous proof.

Suppose $s_1 > \frac{r}{2}$. Then the inequality (3) in the proof of [9, 3.4(i)] shows that $f \leq r(r - s_1)$. Therefore $|x^G| \geq |x_1^{GL_r(q)}| \geq cq^{rs_1}$ (where c is a positive constant). Since by hypothesis $|x^G| \leq |G|^{\frac{1}{4}}$, it follows that $rs_1 \leq \frac{n^2}{4}$. Then

$$s \leq s_1 + n - r \leq \frac{n^2}{4r} + n - r, \tag{5}$$

which is less than $\frac{n}{2} - 1$ since $r > \alpha n$.

Now suppose $s_1 \leq \frac{r}{2}$. Then the inequality (2) in the proof of [9, 3.4(i)] shows that $f \leq (r - s_1)^2 + s_1^2$, and so $|x^G| \geq |x_1^{GL_r(q)}| \geq cq^{2s_1(r-s_1)}$. Thus $2s_1(r-s_1) \leq \frac{n^2}{4}$. Writing $\beta = \frac{s_1}{r}$ (so $0 < \beta < \frac{1}{2}$), this gives $2\beta(1-\beta)r^2 \leq \frac{n^2}{4}$, and hence

$$2\beta(1-\beta) \leq \frac{1}{8\alpha^2}. \tag{6}$$

Also $s \leq s_1 + n - r \leq n - (1-\beta)r \leq n(1-\alpha(1-\beta))$. Now check that for β satisfying (6), we have $\alpha(1-\beta) > \frac{1}{2}$, and the conclusion follows. This completes the proof for $G = L_n(q)$.

The proof for the other classical groups runs along entirely similar lines. We shall just give a sketch for the symplectic groups and leave the other cases to the reader. Let $G = PSp_n(q)$ with n large, and write $\hat{x} = tu$ as above. The centralizer of t in $Sp_n(q)$ is of the form $C = Sp_r(q) \times Sp_s(q) \times \prod GL_{n_i}^{\epsilon_i}(q^{a_i})$, where $n = r+s+2\sum n_i a_i$ and the first two factors correspond to the ± 1-eigenspaces. This has order greater than $|G|^{\frac{3}{4}}$, so C must have a factor $Sp_r(q)$, where $r > \frac{n}{2}$ and $|Sp_r(q) \times Sp_{n-r}(q)| \geq |G|^{\frac{3}{4}}$. As above it follows that for large n we have $r > \alpha n$ with $\alpha = 0.85$. As usual we can write

$$\hat{x} = \lambda \sum J_i^{n_i} \oplus K = x_1 \oplus K \in Sp_r(q) \times Sp_{n-r}(q),$$

where $\lambda = \pm 1$. As in the proof of the previous lemma we have $|C_{Sp_r(q)}(x_1)| \sim q^{\frac{1}{2}g'}$, where $g \leq g' \leq g + 2\sum_{i,n_i \ even}$ and g is as in (3). If $s_1 > \frac{r}{2}$ then $g' \leq (r-s_1)^2 + s_1(r-s_1) + r$, since

$$\begin{aligned}
(r-s_1)^2 + s_1(r-s_1) + r &= (\sum n_i)^2 + (\sum (i-1)n_i)(\sum n_i) + \sum i n_i \\
&\geq \sum n_i^2 + 2\sum_{i<j} n_i n_j + \sum (i-1)n_i^2 + \\
&\quad 2\sum_{i<j}(i-1)n_i n_j + \sum i n_i \\
&\geq g + 2\sum_{i \ even} n_i \\
&\geq g'.
\end{aligned}$$

Hence $|x^G| \geq |x_1^{Sp_r(q)}| \geq cq^{\frac{1}{2}(r^2+r-g')} \geq cq^{\frac{1}{2}rs_1}$. As $|x^G| \leq |G|^{\frac{1}{4}}$ it follows that $rs_1 \leq \frac{n^2+n}{4}$. Now the conclusion follows as in (5) above. Finally, if $s_1 \leq \frac{r}{2}$ then we similarly deduce that $g' \leq (r-s_1)^2 + s_1^2 + r$, which implies that $|x^G| \geq cq^{s_1(r-s_1)}$. Hence $s_1(r-s_1) \leq \frac{n^2+n}{4}$ and now we argue as in the $L_n(q)$ case above. ∎

Lemma 3.3. *Let $x \in G$ with $\nu(x) = s$, and let $0 < \delta \leq \frac{1}{4}$. There is a constant d such that if $|x^G| \leq |G|^\delta$, then $s \leq 2\delta n + \frac{d}{n}$.*

Proof. Let $C = x^G$ and suppose $|C| \leq |G|^\delta$. By Lemma 3.2 and Proposition 3.1 we have

$$cq^{2as(n-s-1)} \leq |C| \leq |G|^\delta < q^{n^2\delta},$$

Writing $d' = \log_2 \frac{1}{c}$, this gives $q^{2as(n-s-1)} < q^{n^2\delta + d'}$. Since $s \leq \frac{n}{2} - 1$, this implies $ans < \delta n^2 + d'$. ∎

The next result shows that the size of a small conjugacy class x^G of a finite simple classical group G is almost determined by the support $\nu(x)$ of x.

Proposition 3.4. *For any $\epsilon_1 > 0$, there exists $\delta > 0$ such that if $x \in G$ with $\nu(x) = s$ and $|x^G| \leq |G|^\delta$, then*

$$q^{(2a-\epsilon_1)ns} \leq |x^G| \leq q^{(2a+\epsilon_1)ns}.$$

Proof. We may assume that $\epsilon_1 < \frac{2}{3}$. Choose $\delta = \frac{\epsilon_1}{4}$. Now $s \leq 3\delta n$ for large n, by Lemma 3.3. Since $s < \frac{n}{2}$, we may apply Proposition 3.1. We have $\epsilon_1 n \geq 3\delta n + 1 \geq s + 1$, so Proposition 3.1 gives the conclusion. ∎

Now let $x_1, x_2 \in G$, and assume that $\nu(x_i) = s_i$ with $s_i < \frac{1}{4}n$ for $i = 1, 2$. The largest eigenspace of $\hat{x}_i$ on $\bar{V}$ has dimension $n - s_i > \frac{3}{4}n$, and it follows that the corresponding eigenvalue λ_i lies in $\mathbb{F}_{q^u}$, and also that $\lambda_i\bar{\lambda}_i = 1$ in the unitary case, and $\lambda_i = \pm 1$ in the symplectic and orthogonal cases. As in the proof of Proposition 3.1 we have $\hat{x} = \lambda \sum J_i^{n_i} \perp K$, and separating the Jordan blocks of size 1, we can write

$$\hat{x}_i = \lambda_i I_{t_i} \perp \sum_{j=1}^{r_i} J_{n_{ji}}(\lambda_i) \perp K_i,$$

where $J_{n_{ji}}(\lambda_i)$ denotes a single Jordan block of size $n_{ji} \geq 2$ for each j, and K_i has no eigenvalue equal to λ_i; moreover the subspaces on which the three summands act are non-degenerate and mutually perpendicular in the case $G \neq L_n(q)$.

Now $s_i = n - (t_i + r_i)$ and $n \geq t_i + 2r_i$, hence $t_i > n - s_i - \frac{1}{2}(n - t_i)$. Since $s_i < \frac{1}{4}n$ it follows that $t_i > \frac{1}{2}n$, and

$$\hat{x}_i = \lambda_i I_{t_i} \perp L_i,$$

where $L_i = \sum_j J_{n_{ji}}(\lambda_i) \perp K_i$. Now define

$$\hat{y} = \lambda_1\lambda_2 I_{t_1+t_2-n} \perp \lambda_2 L_1 \perp \lambda_1 L_2,$$

and let y be the image of $\hat{y}$ in G. Write $y = x_1 * x_2$ (defined only up to conjugacy).

Lemma 3.5. *Let $y = x_1 * x_2$ as above. Then $y \in x_1^G x_2^G$, and $\nu(y) = \nu(x_1) + \nu(x_2)$.*

Proof. There are conjugates of $\hat{x}_1, \hat{x}_2$ of the form $\lambda_1 I_{t_1+t_2-n} \perp L_1 \perp \lambda_1 I_{n-t_2}$ and $\lambda_2 I_{t_1+t_2-n} \perp \lambda_2 I_{n-t_1} \perp L_2$ respectively, and their product is equal to $\hat{y}$. Also, from the definition of $\hat{y}$ we have

$$\nu(y) = n - (t_1 + t_2 - n) - r_1 - r_2 = 2n - (t_1 + r_1) - (t_2 + r_2) = s_1 + s_2,$$

as required. ∎

Lemma 3.6. *Given $\epsilon > 0$, there exists $\delta > 0$ such that the following holds. If x_1^G, x_2^G are classes in G with $|x_i^G| \leq |G|^\delta$ for $i = 1, 2$, and $y = x_1 * x_2$, then $|y^G| \geq (|x_1^G|\,|x_2^G|)^{1-\epsilon}$.*

Proof. By Lemma 3.3 and Proposition 3.4, there exists $\delta > 0$ such that if x^G is a class such that $|x^G| \leq |G|^\delta$, then $\nu(x) < \frac{n}{4}$ and also the conclusion of Proposition 3.4 holds with $\epsilon_1 = \frac{\epsilon}{2}$.

Now let x_1^G, x_2^G be classes in G with $|x_i^G| \leq |G|^\delta$. Then $s_i := \nu(x_i) < \frac{n}{4}$ for $i = 1, 2$, so we can define $y = x_1 * x_2$. Moreover $\nu(y) = s_1 + s_2$ by Lemma 3.5, so Proposition 3.4 gives

$$|y^G| \geq q^{(2a-\epsilon_1)n(s_1+s_2)}, \quad |x_1^G|\,|x_2^G| \leq q^{(2a+\epsilon_1)n(s_1+s_2)}.$$

The conclusion follows, since $\frac{2a-\epsilon_1}{2a+\epsilon_1} \geq 1 - \epsilon$. ∎

Theorem 1.3 for classical groups now follows from Lemmas 3.5 and 3.6, together with Lemma 2.4.

4 Symmetric and alternating groups

We now prove Theorem 1.3 for alternating groups. Recall that it suffices to prove it for conjugacy classes. We start with symmetric groups S_n.

Let $\pi \in S_n$ and let s be the support of π, namely

$$s = |\{1 \leq j \leq n : \pi(j) \neq j\}|.$$

As in the previous section, we shall relate the size of the conjugacy class of an element $\pi \in S_n$ to the support s of π. However, in this case it is not true that the support almost determines the class size as in Proposition 3.4 for classical groups.

For $i \geq 2$ let c_i denote the number of cycles of length i in π. Then $s = \sum_{i \geq 2} i c_i$ and π has $n - s$ fixed points. Let C be the conjugacy class of π in S_n. It is well known that

$$|C| = \frac{n!}{(n-s)! \prod_{i \geq 2} i^{c_i} \prod_{i \geq 2} c_i!}.$$

The following result provides best possible bounds on the size of a conjugacy class $C \subseteq S_n$ in terms of its support s.

Proposition 4.1. *With the above notation, if $s \neq 3$ we have*

$$\frac{n!}{(n-s)! 2^{s/2} \left\lfloor \frac{s}{2} \right\rfloor !} \leq |C| \leq \frac{n!}{(n-s)! s}.$$

The right hand inequality holds also for $s = 3$.

Proof. For the upper bound we need to prove $\prod_{i\geq 2} i^{c_i} \prod_{i\geq 2} c_i! \geq s$. This inequality holds since $\prod_{i\geq 2} i^{c_i} \geq \prod_{i\geq 2} ic_i = s$.

For the lower bound we need to prove

$$\prod_{i\geq 2} i^{c_i} \prod_{i\geq 2} c_i! \leq 2^{s/2} \left\lfloor \frac{s}{2} \right\rfloor !. \tag{7}$$

Since $\sum_{i\geq 2} ic_i = s$, we have $\sum_{i\geq 2} c_i \leq \lfloor \frac{s}{2} \rfloor$. This implies $\prod_{i\geq 2} c_i! \leq \lfloor \frac{s}{2} \rfloor !$. Also for $i \neq 3$, $i \leq 2^{i/2}$. Therefore

$$\prod_{3\neq i\geq 2} i^{c_i} \leq \prod_{3\neq i\geq 2} 2^{ic_i/2} = 2^{(s-3c_3)/2}.$$

Hence if $c_3 = 0$ the inequality (7) follows.

Now suppose that $c_3 > 1$. Then

$$c_3! = (\lfloor 3c_3/2 \rfloor - \lfloor c_3/2 \rfloor)! \leq \frac{1}{2^{\lfloor c_3/2 \rfloor}} \lfloor 3c_3/2 \rfloor !.$$

Also $3 < 2^{3/2} \cdot 2^{1/4}$, so

$$3^{c_3} \leq 2^{3c_3/2} \cdot 2^{c_3/4} \leq 2^{3c_3/2} \cdot 2^{\lfloor c_3/2 \rfloor}.$$

Thus $3^{c_3} c_3! \leq 2^{3c_3/2} \lfloor 3c_3/2 \rfloor !$. Note that

$$\prod_{3\neq i\geq 2} i^{c_i} \prod_{3\neq i\geq 2} c_i! \leq 2^{(s-3c_3)/2} \left\lfloor \frac{s-3c_3}{2} \right\rfloor !.$$

It follows that

$$\prod_{i\geq 2} i^{c_i} \prod_{i\geq 2} c_i! \leq 2^{3c_3/2} \lfloor 3c_3/2 \rfloor ! 2^{(s-3c_3)/2} \left\lfloor \frac{s-3c_3}{2} \right\rfloor ! \leq 2^{s/2} \left\lfloor \frac{s}{2} \right\rfloor !.$$

(We used the fact that $\lfloor \frac{k}{2} \rfloor ! \lfloor \frac{n}{2} \rfloor ! \leq \lfloor \frac{k+n}{2} \rfloor !$.) This completes the proof for $c_3 > 1$.

Finally, suppose $c_3 = 1$. Then since we are assuming $s \neq 3$, we have $\lfloor s/2 \rfloor \geq 2$. So $\lfloor (s-3)/2 \rfloor ! \leq \frac{1}{2} \lfloor s/2 \rfloor !$. We also have $3^{c_3} c_3! = 3 \leq 2^{3/2} \cdot 2$. Thus

$$\begin{aligned} 3^{c_3} c_3! \cdot \textstyle\prod_{3\neq i\geq 2} i^{c_i} \prod_{3\neq i\geq 2} c_i! &\leq 3 \cdot 2^{(s-3)/2} \lfloor (s-3)/2 \rfloor ! \\ &\leq 2^{3/2} \cdot 2 \cdot 2^{(s-3)/2} \cdot 1/2 \lfloor s/2 \rfloor ! = 2^{s/2} \lfloor s/2 \rfloor !, \end{aligned}$$

which completes the proof. ∎

Remark. Note that if $s = 3$ then C is the class of 3-cycles, and the lower bound in Proposition 4.1 does not hold; however it holds if we replace $\lfloor s/2 \rfloor !$ by $\lceil s/2 \rceil !$.

Note also that the lower bound in Proposition 4.1 is best possible, as shown by the case $\pi = (12)(34)\dots(s-1\,s)$ (s even). The upper bound is also best possible, as shown by $\pi = (12\dots s)$.

We fix some notation for the rest of this section. Let $\pi_1, \pi_2 \in S_n$ be permutations of supports s_1, s_2 respectively. For $i = 1, 2$ let C_i denote the conjugacy class of π_i in S_n.

Suppose $s_1 + s_2 \leq n$. Then there exists a permutation, which we denote by π_2', that has the same cycle structure as π_2, such that the points moved by π_2' are fixed points of π_1. Define the conjugacy class

$$C_1 * C_2 = (\pi_1 \pi_2')^{S_n} \subseteq C_1 C_2. \tag{8}$$

Note that the elements of $C_1 * C_2$ have support $s_1 + s_2$. We shall prove that $|C_1 C_2|$ is large by providing lower bounds on the size of $|C_1 * C_2|$.

We start by showing that the conclusion of Theorem 1.3 holds for conjugacy classes C_1, C_2 of bounded support.

Lemma 4.2. *Let s_1, s_2 be positive integers, and let $\epsilon > 0$. There exists an integer $N = N(\epsilon, s_1, s_2)$ such that if $n \geq N$ and C_1, C_2 are classes in S_n of support s_1, s_2 respectively, then*

$$|C_1 C_2| \geq (|C_1|\,|C_2|)^{1-\epsilon}.$$

Proof. We shall choose $N \geq s_1 + s_2$ so the conjugacy class $C_1 * C_2$ may be constructed. It follows from Proposition 4.1 and the remark following it, that for this class (whose support is $s_1 + s_2$) we obtain

$$|C_1 C_2| \geq |C_1 * C_2| \geq \frac{n!}{(n - s_1 - s_2)! 2^{s_1 + s_2} (s_1 + s_2)!} := f(n).$$

By the same proposition we also have

$$(|C_1|\,|C_2|)^{1-\epsilon} \leq \left(\frac{n!}{(n - s_1)!} \cdot \frac{n!}{(n - s_2)!} \right)^{1-\epsilon} := g(n)^{1-\epsilon}. \tag{9}$$

Since $f(n)$ and $g(n)$ are polynomials in n of degree $s_1 + s_2$, there exists $N = N(\epsilon, s_1, s_2)$ such that $f(n) \geq g(n)^{1-\epsilon}$ for $n \geq N$, and the conclusion follows. ∎

In Proposition 4.6 below we will derive a similar conclusion assuming only $s_1, s_2 \leq \frac{n}{2}$. We need some preparations.

We will need Stirling's approximation which holds for all $n \geq 1$ (see [2, §2.9]):

$$e^{1/(12n+1)} \sqrt{2\pi n} \left(\frac{n}{e} \right)^n \leq n! \leq e^{1/(12n)} \sqrt{2\pi n} \left(\frac{n}{e} \right)^n.$$

In fact, we will only need the following weaker inequality

$$\sqrt{2\pi n} \left(\frac{n}{e} \right)^n \leq n! \leq 1.1 \sqrt{2\pi n} \left(\frac{n}{e} \right)^n. \tag{10}$$

Lemma 4.3. *Suppose $s_1, s_2 \le n/2$, and define $f_1(n, s_1, s_2) = \frac{n!}{(n-s_1-s_2)!}$ and $f_2(n, s_1, s_2) = \frac{n!^2}{(n-s_1)!(n-s_2)!}$. Then*

$$\frac{f_1(n, s_1, s_2)}{f_2(n, s_1, s_2)} \ge \frac{1}{1.1^2} \left(\frac{1}{2}\right)^{s_1+s_2}.$$

Proof. If $s_1 + s_2 < n$ use (10) to obtain

$$\begin{aligned}
\tfrac{f_1(n,s_1,s_2)}{f_2(n,s_1,s_2)} &= \tfrac{(n-s_1)!(n-s_2)!}{n!(n-s_1-s_2)!} \\
&\ge \tfrac{1}{1.1^2} \sqrt{\tfrac{2\pi(n-s_1)\cdot 2\pi(n-s_2)}{2\pi n \cdot 2\pi(n-s_1-s_2)}} \cdot \tfrac{e^n e^{n-s_1-s_2}}{e^{n-s_1} e^{n-s_2}} \cdot \tfrac{(n-s_1)^{n-s_1}(n-s_2)^{n-s_2}}{n^n (n-s_1-s_2)^{n-s_1-s_2}} \\
&= \tfrac{1}{1.1^2} \sqrt{\tfrac{(n-s_1)(n-s_2)}{n(n-s_1-s_2)}} \cdot \tfrac{(n-s_1)^{n-s_1}(n-s_2)^{n-s_2}}{n^n (n-s_1-s_2)^{n-s_1-s_2}} \\
&\ge \tfrac{1}{1.1^2} \tfrac{(n-s_1)^{n-s_1}(n-s_2)^{n-s_2}}{n^n (n-s_1-s_2)^{n-s_1-s_2}} \\
&= \tfrac{1}{1.1^2} \left(\tfrac{n-s_1}{n}\right)^{s_2} \left(\tfrac{n-s_2}{n}\right)^{s_1} \left(\tfrac{(n-s_1)(n-s_2)}{n(n-s_1-s_2)}\right)^{n-s_1-s_2} \\
&\ge \tfrac{1}{1.1^2} \left(\tfrac{1}{2}\right)^{s_1+s_2}.
\end{aligned}$$

(We used the fact that $\frac{(n-s_1)(n-s_2)}{n(n-s_1-s_2)} \ge 1$ and that $\frac{n-s_i}{n} \ge \frac{1}{2}$.)

If $s_1 = s_2 = n/2$ then $\frac{f_1(n,s_1,s_2)}{f_2(n,s_1,s_2)} = \frac{(n/2)!(n/2)!}{n!} \ge \left(\frac{1}{2}\right)^n = \left(\frac{1}{2}\right)^{s_1+s_2}$. ∎

As above let $\pi_1, \pi_2 \in S_n$ have supports s_1, s_2 respectively. For $i \ge 2$ let c_i be the number of cycles of length i in π_1, and d_i the number of cycles of length i in π_2.

Lemma 4.4. *We have*

$$\frac{\prod_{i\ge 2} c_i! \prod_{i\ge 2} d_i!}{\prod_{i\ge 2} (c_i + d_i)!} \ge 2^{-(s_1+s_2)/2}.$$

Proof. Observe that

$$\frac{c_i! d_i!}{(c_i + d_i)!} = \frac{1}{\binom{c_i+d_i}{c_i}} \ge \frac{1}{2^{c_i+d_i}}.$$

Combining this with the inequalities $\sum c_i \le \sum \frac{i}{2} c_i = \frac{s_1}{2}$ and $\sum d_i \le \frac{s_2}{2}$ we obtain

$$\frac{\prod c_i! \prod d_i!}{\prod (c_i + d_i)!} \ge 2^{-\sum c_i - \sum d_i} \ge 2^{-\frac{s_1+s_2}{2}}.$$

∎

Recall that $C_i = \pi_i^{S_n}$ for $i = 1, 2$.

Lemma 4.5. *Suppose $s_1 \le \frac{n}{2}$. Then $|C_1| \ge s_1^{s_1/2}$.*

Proof. Applying Proposition 4.1, we obtain for $s_1 \neq 3$

$$\begin{aligned} |C_1| &\geq \frac{n!}{(n-s_1)!\cdot 2^{s_1/2}\lfloor s_1/2\rfloor!} \\ &\geq \frac{(n-s_1)^{s_1}}{2^{s_1/2}\left(\frac{s_1}{2}\right)^{s_1/2}} \geq \frac{s_1^{s_1}}{2^{s_1/2}\left(\frac{s_1}{2}\right)^{s_1/2}} = s_1^{s_1/2}. \end{aligned}$$

For $s_1 = 3$, we have $|C_1| = \frac{n(n-1)(n-2)}{3} \geq \frac{6\cdot 5\cdot 4}{3} \geq 3^{3/2}$. ∎

Proposition 4.6. *For any $\epsilon > 0$ there exists $N = N(\epsilon)$ such that if $n \geq N$ and $s_1, s_2 \leq \frac{n}{2}$, then $|C_1C_2| \geq (|C_1|\,|C_2|)^{1-\epsilon}$.*

Proof. We have

$$\begin{aligned} &|C_1| = \tfrac{n!}{(n-s_1)!\prod i^{c_i}\prod c_i!},\ |C_2| = \tfrac{n!}{(n-s_2)!\prod i^{d_i}\prod d_i!},\ \text{and} \\ &|C_1 * C_2| = \tfrac{n!}{(n-s_1-s_2)!\prod i^{c_i+d_i}\prod (c_i+d_i)!}. \end{aligned}$$

Hence, taking f_1, f_2 as in Lemma 4.3,

$$\frac{|C_1 * C_2|}{|C_1|\,|C_2|} = \frac{f_1(n,s_1,s_2)}{f_2(n,s_1,s_2)}\frac{\prod (c_i!)\prod (d_i!)}{\prod (c_i+d_i)!}.$$

It follows using Lemmas 4.3, 4.4 and 4.5 that

$$\begin{aligned} \tfrac{|C_1C_2|}{(|C_1|\,|C_2|)^{1-\epsilon}} &= \tfrac{|C_1C_2|}{|C_1|\,|C_2|}|C_1|^{\epsilon}|C_2|^{\epsilon} \\ &\geq \tfrac{|C_1*C_2|}{|C_1|\,|C_2|}|C_1|^{\epsilon}|C_2|^{\epsilon} \\ &\geq \tfrac{1}{1.1^2}\cdot 2^{-(s_1+s_2)}2^{-(s_1+s_2)/2}s_1^{s_1\epsilon/2}s_2^{s_2\epsilon/2} \\ &= \tfrac{1}{1.1^2}\cdot 2^{-\frac{3}{2}(s_1+s_2)}s_1^{s_1\epsilon/2}s_2^{s_2\epsilon/2}. \end{aligned}$$

Let $S_0 = S_0(\epsilon)$ be such that $\frac{1}{1.1^2}\cdot 2^{-\frac{3}{2}(s_1+s_2)}s_1^{s_1\epsilon/2}s_2^{s_2\epsilon/2} \geq 1$ provided $s_1 \geq S_0$ or $s_2 \geq S_0$. If one of the latter inequalities holds, we deduce that $|C_1C_2| \geq (|C_1|\,|C_2|)^{1-\epsilon}$. Otherwise we have $s_1, s_2 \leq S_0$, and we let $N_0 = N_0(\epsilon, S_0, S_0) = N(\epsilon)$ be such that for $n \geq N_0$, $|C_1C_2| \geq (|C_1|\,|C_2|)^{1-\epsilon}$ (such N_0 exists by Lemma 4.2). ∎

The next result provides a lower bound close to $n^{s/2}$ for the size of a conjugacy class of support s.

Lemma 4.7. *If $C \subseteq S_n$ is a conjugacy class with support s, then*

$$|C| \geq \frac{1}{\sqrt{\pi n}}n^{\frac{s}{2}}e^{-\frac{s}{2}}.$$

Proof. Using Proposition 4.1 and (10), we obtain for $s \neq 3$ and $s < n$

$$\begin{aligned} |C| &\geq \tfrac{n!}{(n-s)!2^{s/2}\lfloor s/2\rfloor!} \geq \tfrac{1}{1.1^2}\cdot\tfrac{\sqrt{2\pi n}}{\sqrt{2\pi(n-s)\cdot 2\pi s/2}}\cdot\tfrac{n^n}{(n-s)^{(n-s)}(s/2)^{s/2}}e^{-s/2}2^{-s/2} \\ &= \tfrac{1}{1.1^2}\cdot\tfrac{\sqrt{n}}{\sqrt{\pi(n-s)s}}\cdot\tfrac{n^n}{(n-s)^{(n-s)}s^{s/2}}e^{-s/2} \geq \tfrac{1}{1.1^2}\cdot\tfrac{\sqrt{n}}{\sqrt{\pi n^2/2}}\cdot\tfrac{n^n}{n^{(n-s)}n^{s/2}}e^{-s/2} \\ &= \tfrac{\sqrt{2}}{1.1^2}\cdot\tfrac{1}{\sqrt{\pi n}}n^{\frac{s}{2}}e^{-\frac{s}{2}} \geq \tfrac{1}{\sqrt{\pi n}}n^{\frac{s}{2}}e^{-\frac{s}{2}}, \end{aligned}$$

as required.

For $s = 3$, we have

$$|C| = \frac{n(n-1)(n-2)}{3} \geq \frac{2}{3}n \geq \frac{1}{\sqrt{\pi}}ne^{-\frac{3}{2}} = \frac{1}{\sqrt{\pi n}}n^{\frac{3}{2}}e^{-\frac{3}{2}}.$$

Finally, if $s = n$ we obtain

$$\begin{aligned} |C| &\geq \tfrac{n!}{2^{n/2}\lfloor n/2 \rfloor!} \geq \tfrac{1}{1.1} \cdot \tfrac{\sqrt{2\pi n}}{\sqrt{2\pi n/2}} \cdot \tfrac{e^{n/2}}{e^n} \cdot \tfrac{n^n}{(n/2)^{n/2}} \cdot \tfrac{1}{2^{n/2}} \\ &= \tfrac{\sqrt{2}}{1.1} \cdot \tfrac{1}{e^{n/2}} \cdot n^{n/2} \geq n^{n/2}e^{-n/2}. \end{aligned}$$

This completes the proof. ∎

Proposition 4.8. *For any $\epsilon > 0$ there exists $N = N(\epsilon)$ such that, if $n \geq N$, and C_1, C_2 are conjugacy classes of $G = S_n$ satisfying $|C_1|, |C_2| \leq |G|^{\frac{1}{4}-\epsilon}$, then $|C_1C_2| \geq (|C_1||C_2|)^{1-\epsilon}$.*

In particular, Theorem 1.3 *holds for conjugacy classes in S_n.*

Proof. We will first show that there exists $N_0 = N_0(\epsilon)$, such that if $n \geq N_0$ and $C \subset G = S_n$ is a class of support s satisfying $|C| \leq |G|^{\frac{1}{4}-\epsilon}$, then $s \leq \frac{n}{2}$.

Let C be such a class. By Lemma 4.7 and (10),

$$\frac{1}{\sqrt{\pi n}}n^{\frac{s}{2}}e^{-\frac{s}{2}} \leq |C| \leq |G|^{\frac{1}{4}-\epsilon} = (n!)^{\frac{1}{4}-\epsilon} \leq \left(1.1\sqrt{2\pi n} \cdot n^n e^{-n}\right)^{\frac{1}{4}-\epsilon}.$$

Thus

$$\frac{1}{\sqrt{\pi n}}\left(\frac{n}{e}\right)^{\frac{s}{2}} \leq \left(1.1\sqrt{2\pi n}\right)^{\frac{1}{4}} \cdot \left(\frac{n}{e}\right)^{\frac{n}{4}-n\epsilon},$$

and so

$$\left(\frac{n}{e}\right)^{\frac{s}{2}-\frac{n}{4}+n\epsilon} \leq cn^{\frac{5}{8}},$$

where $c = 1.1^{\frac{1}{4}}2^{\frac{1}{8}}\pi^{\frac{5}{8}}$. Suppose $s \geq \frac{n+1}{2}$. Then $\frac{s}{2} - \frac{n}{4} \geq \frac{1}{4}$, so

$$\left(\frac{n}{e}\right)^{\frac{1}{4}+n\epsilon} \leq cn^{\frac{5}{8}},$$

and

$$\left(\frac{n}{e}\right)^{n\epsilon} \leq ce^{\frac{1}{4}}n^{\frac{3}{8}} \leq 3n^{\frac{3}{8}},$$

which is a contradiction for $n \geq N_0(\epsilon)$. Hence $s \leq \frac{n}{2}$ for $n \geq N_0$.

Now let C_1, C_2 be classes as in the statement of the proposition, with supports s_1, s_2. By the above $s_1, s_2 \leq \frac{n}{2}$, so we can take $N = N(\epsilon)$ as in Proposition 4.6. Then if $n \geq \max\{N, N_0\}$ we have $|C_1C_2| \geq (|C_1|\,|C_2|)^{1-\epsilon}$. This completes the proof. ∎

We finally turn to alternating groups, proving

Lemma 4.9. *Proposition* 4.8 *holds for conjugacy classes in* $G = A_n$.

Proof. If $\pi \in A_n$ then $\pi^{A_n} = \pi^{S_n}$ or $\left|\pi^{A_n}\right| = \frac{1}{2}\left|\pi^{S_n}\right|$. Also if $s \leq n/2$, then $\pi^{A_n} = \pi^{S_n}$. So the results leading to the proof of Proposition 4.8 can easily be adjusted to handle $G = A_n$. ∎

This completes the proof of Theorem 1.3 for alternating groups $G = A_n$ in a somewhat stronger form: it suffices to assume that the normal subsets have size at most $|G|^{1/4-\epsilon}$ and that $n \geq N(\epsilon)$.

5 Final deductions

Deduction of Theorem 1.1

Let $\epsilon > 0$ and let $\delta > 0$ be as in the conclusion of Theorem 1.2. Theorem 1.1 of [10] states that there is an absolute constant c such that for every nontrivial normal subset A of a finite simple group G, we have $A^m = G$ for any $m \geq c\frac{\log|G|}{\log|A|}$. Define $b = \lceil \frac{c}{\delta} \rceil$.

Now let A be a normal subset of a finite simple group G. If $|A| \geq |G|^{\delta}$ then the previous paragraph shows that $A^b = G$. Otherwise, Theorem 1.2 shows that $|A^2| \geq |A|^{2-\epsilon}$. This completes the proof. ∎

Deduction of Corollary 1.4

We argue by induction on $k \geq 2$. The case $k = 2$ is Theorem 1.3. Suppose $k \geq 3$. By induction, given $\epsilon > 0$ and $2 \leq m < k$, there exists $\delta(\epsilon, m) > 0$ such that if $A_1, \ldots, A_m \subseteq G$ are normal subsets with $|A_i| \leq |G|^{\delta(\epsilon,m)}$ then $|A_1 \cdots A_m| \geq (|A_1| \cdots |A_m|)^{1-\epsilon}$.

Define $\delta(\epsilon, k) = \min\{\delta(\epsilon/2, 2)/(k-1), \delta(\epsilon/2, k-1)\}$.

Now let $\delta = \delta(\epsilon, k)$ and suppose $A_1, \ldots, A_k$ are normal subsets of G of size at most $|G|^{\delta}$. By induction it follows that

$$|A_1 \cdots A_{k-1}| \geq (|A_1| \cdots |A_{k-1}|)^{1-\epsilon/2}.$$

Note that $|A_1 \cdots A_{k-1}| \leq |G|^{(k-1)\delta} \leq |G|^{\delta(\epsilon/2,2)}$, and so the case $k = 2$ yields

$$|A_1 \cdots A_k| \geq (|A_1 \cdots A_{k-1}||A_k|)^{1-\epsilon/2} \geq ((|A_1| \cdots |A_{k-1}|)^{1-\epsilon/2}|A_k|)^{1-\epsilon/2},$$

which is at least $(|A_1| \cdots |A_k|)^{1-\epsilon}$. The result follows. ∎

Deduction of Theorem 1.5

The proof is virtually the same as that of Theorem 1.3. As in Lemma 2.3, since every conjugacy class in a simple algebraic group G has dimension at least $r = \mathrm{rank}(G)$, we need only consider classical groups of large dimension. So let $G = SL_n(K)$, $Sp_n(K)$ or $SO_n(K)$ where K is algebraically closed and n is large, and define $a := a(G) = 1$, $\frac{1}{2}$ or $\frac{1}{2}$, respectively. Let $x \in G$ and define $s = \nu(x)$ as in Section 3. The proof of Lemma 3.1 gives

$$2as(n - s - 1) \leq \dim x^G \leq as(2n - s + 1),$$

and there are similar dimensional analogues of Lemma 3.2, Lemma 3.3 and Proposition 3.4, with the same proofs. For $x_1, x_2 \in G$ with $s_i = \nu(x_i) < \frac{n}{4}$ we can define $y = x_1 * x_2$ as before, and $\nu(y) = s_1 + s_2$ as in Lemma 3.5. Now the theorem follows as in the proof of Lemma 3.6. ∎

References

[1] E. Breuillard, B. Green and T. Tao, Approximate subgroups of linear groups, *Geom. Funct. Anal.* **21** (2011), 774–819.

[2] W. Feller, *An Introduction to Probability Theory and Its Applications*, Vol. 1, 3rd ed., Wiley, New York, 1968.

[3] N. Gill, L. Pyber, I. Short, E. Szabò, On the product decomposition conjecture for finite simple groups, *Groups Geom. Dyn.* **7** (2013), 867–882.

[4] H.A. Helfgott, Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$, *Annals of Math.* **167** (2008), 601–623.

[5] H.A. Helfgott, Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$, *J. Eur. Math. Soc.* **13** (2011), 761–851.

[6] E. Hrushovski, Stable group theory and approximate subgroups, *J. Amer. Math. Soc.* **25** (2012), 189-243.

[7] P. Kleidman and M.W. Liebeck, *The subgroup structure of the finite classical groups*, London Math. Soc. Lecture Note Series **129**, Cambridge Univ. Press, 1990.

[8] M.W. Liebeck and G.M. Seitz, *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, Mathematical Surveys and Monographs, Vol.180, American Math. Soc., Providence, RI, 2012.

[9] M. W. Liebeck and A. Shalev, Simple groups, permutation groups, and probability, *J. Amer. Math. Soc.* **12** (1999), 497–520.

[10] M. W. Liebeck and A. Shalev, Diameters of finite simple groups: sharp bounds and applications, *Annals of Math.* **154** (2001), 383–406.

[11] M. W. Liebeck and A. Shalev, Character degrees and random walks in finite groups of Lie type, *Proc. London Math. Soc.* **90** (2005), 61–86.

[12] L. Pyber and E. Szabò, Growth in finite simple groups of Lie type, *J. Amer. Math. Soc.*, to appear.

[13] A. Shalev, Word maps, conjugacy classes, and a noncommutative Waring-type theorem, *Annals of Math.* **170** (2009), 1383–1416.

M. W. Liebeck, Department of Mathematics, Imperial College, London SW7 2AZ, UK

G. Schul, Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel

A. Shalev, Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel