ON THE INTERSECTIONS OF NILPOTENT SUBGROUPS IN SIMPLE GROUPS

TIMOTHY C. BURNESS AND HONG YI HUANG

ABSTRACT. Let G be a finite group and let H_p be a Sylow p-subgroup of G. A very recent conjecture of Lisi and Sabatini asserts the existence of an element $x \in G$ such that $H_p \cap H_p^x$ is inclusion-minimal in the set $\{H_p \cap H_p^g \ : \ g \in G\}$ for every prime p. This has been proved in several special cases, including all sufficiently large symmetric and alternating groups. For a simple group G, in view of a theorem of Mazurov and Zenkov from 1996, the conjecture implies the existence of an element $x \in G$ with $H_p \cap H_p^x = 1$ for all p. In turn, this statement implies a conjecture of Vdovin from 2002, which asserts that if G is simple and H is a nilpotent subgroup, then $H \cap H^x = 1$ for some $x \in G$.

In this paper, we adopt a probabilistic approach to prove the Lisi-Sabatini conjecture for all non-alternating simple groups. By combining this with earlier work of Kurmazov on nilpotent subgroups of alternating groups, we complete the proof of Vdovin's conjecture. Moreover, by combining our proof for groups of Lie type with earlier work of Zenkov on alternating and sporadic groups, we are able to establish a stronger form of Vdovin's conjecture: if G is simple and A, B are nilpotent subgroups, then $A \cap B^x = 1$ for some $x \in G$. In addition, we study the asymptotic probability that a random pair of Sylow p-subgroups in a simple group of Lie type intersect trivially, complementing recent work of Diaconis et al. and Eberhard on symmetric and alternating groups.

1. INTRODUCTION

Let G be a finite group and let H be a nilpotent subgroup of G. By a theorem of Zenkov [33], there exist elements $x, y \in G$ such that

$$H \cap H^x \cap H^y \leqslant F(G),$$

where $F(G)$ is the Fitting subgroup of G. This result is optimal in the sense that there exist examples $H < G$ with the property that the intersection of any two conjugates of H is not contained in $F(G)$ (for instance, if $G = S_8$ and H is a Sylow 2-subgroup of G, then $H \cap H^x \neq 1$ for all $x \in G$). Zenkov's theorem is just one of many results in a substantial literature on the intersections of nilpotent subgroups of finite groups, which can be traced all the way back to work of Passman [30] in the 1960s.

In this paper, we are interested in the special case where G is a (non-abelian) finite simple group. Since the Fitting subgroup of G is trivial, Zenkov's theorem implies that for any nilpotent subgroup H we have $H \cap H^x \cap H^y = 1$ for some $x, y \in G$. In fact, Vdovin has proposed the following conjecture, which is stated as Problem 15.40 in the *Kourovka Notebook* [28]. Here and throughout the paper, whenever we refer to a simple group, we implicitly assume the group is non-abelian.

Conjecture 1 (Vdovin [28], 2002). *Let G be a finite simple group and let H be a nilpotent subgroup of G. Then $H \cap H^x = 1$ for some $x \in G$.*

This conjecture has been resolved for alternating groups [24] and sporadic groups [35]. In addition, there are some partial results for certain low rank groups of Lie type (for example, see [36] for the 2-dimensional linear groups $L_2(q)$, and [34] for $L_3(q)$ and $U_3(q)$). But in general, the conjecture remains open for groups of Lie type.

An important special case of Conjecture 1 was established in earlier work of Mazurov and Zenkov [39].

Theorem 2 (Mazurov & Zenkov [39], 1996). *Let G be a finite simple group and let H be a Sylow p-subgroup of G. Then $H \cap H^x = 1$ for some $x \in G$.*

In [39], the proof of Theorem 2 for groups of Lie type rests on a representation-theoretic result of Green [23], which states that if a p-block for a finite group G has defect group D and H is a Sylow p-subgroup of G, then $H \cap H^x = D$ for some $x \in G$. This can then be combined with later work of Michler [29] and Willems [32] in the 1980s, who showed that every finite simple group of Lie type has a p-block with trivial defect group, for every prime divisor p of the order of the group.

Remark 3. Recall that a finite group G is *almost simple* if $G_0 \trianglelefteq G \leqslant \mathrm{Aut}(G_0)$ for some non-abelian simple group G_0, where we identify G_0 with its group of inner automorphisms. It turns out that Theorem 2 does not extend to almost simple groups and we refer the reader to our recent paper [16], where we extend earlier work of Zenkov to determine all the pairs (G, H), where G is almost simple, H is a Sylow p-subgroup and $H \cap H^x \neq 1$ for all $x \in G$. This of course includes the example highlighted above, where $G = S_8$ and H is a Sylow 2-subgroup.

Remark 4. The statements of Conjecture 1 and Theorem 2 can be rephrased in several different ways, providing natural connections to other well studied problems.

(a) Let G be a finite group and let H be a core-free subgroup, which allows us to view G as a transitive permutation group $G \leqslant \mathrm{Sym}(\Omega)$ on the set $\Omega = G/H$ of cosets of H in G. Then the *base size* of G, denoted $b(G, H)$, is defined to be the minimal size of a subset of Ω with trivial pointwise stabiliser in G. This is a fundamental and intensively studied invariant in permutation group theory, with an extensive literature stretching all the way back to the 19th century. In the language of bases, Zenkov's main theorem in [33] reveals that $b(G, H) \leqslant 3$ for every finite transitive group G with $F(G) = 1$ and nilpotent point stabiliser H. And similarly, Conjecture 1 asserts that $b(G, H) = 2$ for every finite simple transitive group G with a nilpotent point stabiliser $H \neq 1$.

(b) The previous observation connects with another well-known conjecture of Vdovin, which is stated as Problem 17.41(b) in [28]. This asserts that $b(G, H) \leqslant 5$ for every transitive permutation group G with trivial soluble radical and soluble point stabiliser H (the example $G = S_8$ and $H = S_4 \wr S_2$ shows that the purported bound is best possible). This conjecture is proved for primitive groups in [11], and Vdovin gives a reduction of the general problem to almost simple groups in [31]. Further work [3, 10] reduces the problem to groups of Lie type, and Baykalov [4] has made recent progress towards a proof for the classical groups. But the general problem remains open, including the special case where G is a simple group.

(c) It also worth highlighting a connection with the notion of the *depth* of a subgroup H of a finite group G, denoted $d_G(H)$, which was introduced in a 2011 paper by Boltje, Danz and Külshammer [5]. This is a positive integer defined in terms of the inclusion of complex group algebras $\mathbb{C}H \subseteq \mathbb{C}G$ and there has been a focus on studying the depth of subgroups of simple and almost simple groups (see [9] and the references therein). The relevant connection arises from the observation that if H is core-free and $b(G, H) = 2$, then $d_G(H) = 3$ (see [8, Theorem 6.9]). So in the language of subgroup depth, Conjecture 1 asserts that every non-trivial nilpotent subgroup of a simple group has depth 3.

A renewed interest in Conjecture 1 stems from a recent paper of Lisi and Sabatini [27], where they propose the following far reaching generalisation. In the statement, we write $\pi(G)$ for the set of distinct prime divisors of $|G|$.

Conjecture 5 (Lisi & Sabatini [27], 2025). *Let G be a finite group with $\pi(G) = \{p_1, \ldots, p_k\}$ and let P_i be a Sylow p_i-subgroup of G. Then there exists an element $x \in G$ such that for each i, $P_i \cap P_i^x$ is inclusion-minimal in the set $\{P_i \cap P_i^g : g \in G\}$.*

In [27], the conjecture is proved for all metanilpotent groups of odd order, as well as all sufficiently large alternating and symmetric groups. In view of Theorem 2, Conjecture 5 takes the following striking form for simple groups.

Conjecture 6. *Let G be a finite simple group and let H_p be a Sylow p-subgroup of G. Then there exists an element $x \in G$ such that $H_p \cap H_p^x = 1$ for all $p \in \pi(G)$.*

Since every finite nilpotent group is the direct product of its Sylow subgroups, we immediately observe that Conjecture 6 implies Conjecture 1. As noted above, Conjecture 6 is proved in [27] for all sufficiently large alternating groups. Our main goal in this paper is to prove it for all simple groups of Lie type and all simple sporadic groups, without any conditions on the order of the group.

Theorem A. *Conjecture 6 is true for all non-alternating finite simple groups.*

By combining this result with the main theorem of [24], we immediately obtain the following result, which resolves Vdovin's conjecture on nilpotent subgroups of simple groups.

Corollary B. *Conjecture 1 is true.*

And in view of the connections highlighted in Remark 4, we get the following corollary, which may be of independent interest.

Corollary C. *Let G be a finite simple group. Then $b(G, H) = 2$ and $d_G(H) = 3$ for every non-trivial nilpotent subgroup H of G.*

Remark 7. As noted above, Lisi and Sabatini [27, Theorem 1.4] prove Conjecture 6 for all sufficiently large alternating groups and their argument relies on recent asymptotic results due to Diaconis et al. [20] and Eberhard [21]. So in view of Theorem A, we have a proof of Conjecture 6 for all simple groups, apart from the alternating groups $G = A_n$ with $n \leqslant N$ for some unspecified constant N. It is straightforward to verify the conjecture computationally for all $G = A_n$ with $n \leqslant 500$, but it remains an open problem to prove it for all alternating groups.

Our proof of Theorem A involves a combination of probabilistic and computational methods. In order to outline our approach, let G be a non-alternating finite simple group and let H_p be a Sylow p-subgroup of G for each $p \in \pi(G)$.

Let us first assume G admits a suitable permutation representation from a computational perspective, which means that the order of G and the degree n of the representation are not prohibitively large. In this situation, it is entirely straightforward to verify the desired result by direct computation in MAGMA [6]. To do this, we work with the given permutation representation of G and for each $p \in \pi(G)$ we construct a Sylow p-subgroup H_p of G. And then by random search, we identify an element $x \in G$ such that $H_p \cap H_p^x = 1$ for all p. For instance, this direct approach turns out to be effective for 21 of the 26 sporadic simple groups (see the proof of Theorem 3.1).

In the general setting, our proof of Theorem A relies on a probabilistic argument. Let

$$Q(G) = \frac{|\{x \in G : H_p \cap H_p^x \neq 1 \text{ for some } p \in \pi(G)\}|}{|G|}$$

be the probability that a uniformly random element $x \in G$ does not satisfy the condition in Conjecture 6. So our goal is to show that $Q(G) < 1$. To do this, first observe that

$$Q(G) \leqslant \sum_{p \in \pi(G)} Q_p(G),$$

where $Q_p(G)$ is the probability that $H_p \cap H_p^x \neq 1$ for a uniformly random $x \in G$. For each $p \in \pi(G)$, we may view G as a transitive permutation group on $\Omega = G/H_p$, in which case $Q_p(G)$ coincides with the probability that two randomly chosen points in Ω do not form a base for G. In turn, this implies that

$$Q_p(G) \leqslant \sum_{i=1}^{k} |x_i^G| \cdot \left(\frac{|x_i^G \cap H_p|}{|x_i^G|} \right)^2 =: \widehat{Q}_p(G),$$

where $\{x_1, \ldots, x_k\}$ is a complete set of representatives of the conjugacy classes in G of elements of order p (a more general version of this upper bound was first introduced by Liebeck and Shalev in their proof of [26, Theorem 1.3]).

In this way, the problem is essentially reduced to the derivation of an appropriate upper bound on $\widehat{Q}_p(G)$ for each $p \in \pi(G)$. To do this, we can appeal to the extensive literature on conjugacy classes of prime order elements in simple groups, which reduces the problem further to estimating $|x_i^G \cap H_p|$. For most classes, we will show that the trivial upper bound $|x_i^G \cap H_p| < |H_p|$ is good enough. But further work is often required when x_i^G is one of the smallest conjugacy classes of elements of order p and in these cases we typically proceed by embedding H_p in a specific subgroup L of G, which allows us to work with the upper bound $|x_i^G \cap H_p| \leqslant |x_i^G \cap L|$. Here the subgroup L is chosen so that it is easier to count the appropriate number of elements of order p in L than in H_p itself.

In the critical case where G is a group of Lie type in characteristic r, the prime divisor $p = r$ requires special attention. Here $N_G(H_r)$ is a Borel subgroup of G with unipotent radical H_r and by considering the opposite Borel subgroup it is easy to see that $H_r \cap H_r^x = 1$ for some $x \in G$. In turn, this implies that

$$Q_r(G) \leqslant 1 - \frac{|H_r||N_G(H_r)|}{|G|}.$$

Then by setting $\pi'(G) = \pi(G) \setminus \{r\}$, it just remains to show that

$$\sum_{p \in \pi'(G)} \widehat{Q}_p(G) < \frac{|H_r||N_G(H_r)|}{|G|}$$

and this is how we proceed. In particular, this approach allows us to focus entirely on semisimple elements of prime order.

Remark 8. It is worth noting that our proof of Theorem A is independent of Theorem 2. In particular, we obtain a new proof of Theorem 2 for simple groups of Lie type, which does not rely on the earlier work in [23, 29, 32] concerning p-blocks and defect groups. Moreover, our new proof is quantitative, in the sense that it allows us to draw conclusions concerning the proportion of elements $x \in G$ with $H \cap H^x = 1$, which is not possible via the original existence proof in [39].

Remark 9. Let $G = A_n$ be an alternating group. Here the main result is [27, Proposition 4.1], which in terms of the above notation gives $Q_2(G) \leqslant 0.99$ and $Q_p(G) = O(n^{-1})$ for all large n and all odd primes p (in fact, the main theorem of [21] reveals that $Q_2(G) \to 1 - \frac{3}{2}e^{-1/2}$ as n tends to infinity; see Theorem 10 below). Then an easy application of the Prime Number Theorem yields

$$\sum_{p \in \pi(G)} Q_p(G) < 1 \tag{1}$$

for $n \gg 0$ and this completes the proof of Conjecture 6 for all sufficiently large alternating groups. Proving a non-asymptotic version of Conjecture 6 using a probabilistic approach seems to be a difficult problem and we intend to return to this in future work.

The asymptotic behaviour of the probability $Q_p(G)$ is studied in recent papers by Diaconis et al. [20] and Eberhard [21] in the special case where G is a symmetric or alternating

group, with several interesting applications highlighted in [20]. Here the main results can be summarised as follows (part (i) is [20, Theorem 1.1(a)], while (ii) is [21, Theorem 1]).

Theorem 10 (Diaconis et al. [20]; Eberhard [21], 2025)**.** *Let p be a prime and let $G = S_n$ or A_n.*

    (i) *If $p > 2$, then $Q_p(G) \to 0$ as $n \to \infty$.*

    (ii) *If $p = 2$, then $Q_p(G) \to 1 - \alpha e^{-1/2}$ as $n \to \infty$, where $\alpha = 1$ if $G = S_n$ and $\alpha = \frac{3}{2}$ if $G = A_n$.*

Our probabilistic proof of Theorem A allows us to establish a strong version of Theorem 10 for groups of Lie type (see the asymptotic statements in Theorems 4.1 and 5.1).

Theorem D. *Let G be a finite simple group of Lie type over a field $\mathbb{F}_q$ of characteristic r and set*

$$\beta(G) = \sum_{p \in \pi(G) \setminus \{r\}} Q_p(G), \quad \gamma(G) = \sum_{p \in \pi(G) \setminus \{2, r\}} Q_p(G).$$

Then $\gamma(G) \to 0$ as $|G| \to \infty$. In addition, if $G \neq \mathrm{L}_2(q)$ then $\beta(G) \to 0$ as $|G| \to \infty$.

By combining this with Theorem 10, we obtain the following corollary.

Corollary E. *Let (G_i, p_i) be a sequence of pairs, where G_i is a finite simple group, p_i is a prime and $|G_i| \to \infty$. Then either*

$$Q_{p_i}(G_i) \to 0 \ as \ i \to \infty,$$

or there exists a subsequence of pairs (G_{i_k}, p_{i_k}) such that one of the following holds for all k:

    (a) $G_{i_k} = A_{n_k}$ *and* $p_{i_k} = 2$;

    (b) $G_{i_k} = \mathrm{L}_2(q_k)$, q_k *is odd and* $p_{i_k} = 2$;

    (c) G_{i_k} *is a group of Lie type defined over a field of characteristic* p_{i_k}.

Remark 11. Let us briefly comment on the special subsequences arising in the statement of Corollary E. For (a), we refer to Theorem 10(ii). And for (b), observe that if $G = \mathrm{L}_2(q)$ and q is a Mersenne prime, then

$$Q_2(G) = 1 - \frac{s|H_2|}{|G : H_2|},$$

where s is the number of regular orbits of $H_2 = D_{q+1}$ on G/H_2. By [15, Lemma 7.9] we have $s = (q - 3)/4$ and thus

$$Q_2(G) = \frac{1}{2} + \frac{q + 3}{2q(q - 1)}.$$

In particular, if there are infinitely many Mersenne primes (as expected), then there exists a sequence of groups $G_i = \mathrm{L}_2(q_i)$ such that $|G_i| \to \infty$ and $Q_2(G_i) \to \frac{1}{2}$ as i tends to infinity. Finally, in case (c) we refer to [38, Lemma 3.13], which implies that if G is a simple group of Lie type in characteristic r, and $G \neq \mathrm{Sp}_4(2)'$, $G_2(2)'$, ${}^2G_2(3)'$ or ${}^2F_4(2)'$, then

$$Q_r(G) = 1 - \frac{|H_r||N_G(H_r)|}{|G|}.$$

So for example, if $G = \mathrm{L}_n(q)$ and $q = r^f$ then $|N_G(H_r) : H_r| = \frac{1}{d}(q-1)^{n-1}$ with $d = (n, q-1)$ and thus

$$Q_r(G) = 1 - \frac{q^{n(n-1)/2}(q-1)^{n-1}}{\prod_{i=2}^{n}(q^i - 1)} \to 1$$

if q is fixed and n tends to infinity.

Another interesting feature of our proof of Theorem A is that it allows us to show that (1) holds for every finite simple group of Lie type, with the single exception of $U_4(2) \cong \mathrm{PSp}_4(3)$ (see Theorems 4.1 and 5.1). Putting the special case $U_4(2)$ to one side, this immediately settles Conjecture 6, and hence Conjecture 1, for groups of Lie type. In addition, it allows us to establish the following generalisation of Conjecture 1 (the conclusion can be checked directly for $U_4(2)$).

Theorem F. *Let G be a simple group of Lie type and let A and B be nilpotent subgroups of G. Then $A \cap B^x = 1$ for some $x \in G$.*

To see this, let A and B be nilpotent subgroups of G and for each $p \in \pi(G)$ let A_p and B_p be the unique Sylow p-subgroups of A and B, respectively. Setting

$$R_p(A, B) = \frac{|\{x \in G \,:\, A_p \cap B_p^x \neq 1\}|}{|G|}$$

we observe that $A \cap B^x = 1$ for some $x \in G$ if $\sum_p R_p(A, B) < 1$. Now if we embed $A_p \leqslant H_p$ and $B_p \leqslant K_p$, where H_p and K_p are Sylow p-subgroups of G, then

$$R_p(A, B) \leqslant \frac{|\{x \in G \,:\, H_p \cap K_p^x \neq 1\}|}{|G|} = Q_p(G)$$

and so the inequality in (1) yields $A \cap B^x = 1$ for some $x \in G$.

By combining Theorem F with earlier work of Zenkov for alternating groups [37] and sporadic groups [35] (see Remark 3.3), we obtain the following corollary which can be viewed as a natural generalisation of Theorem 2 and Corollary B. In the language of [1], this shows that every pair of nilpotent subgroups of a simple group is regular.

Corollary G. *Let G be a finite simple group and let A and B be nilpotent subgroups of G. Then $A \cap B^x = 1$ for some $x \in G$.*

Remark 12. In view of Conjecture 6, it is natural to ask if there is a stronger form of Corollary G. For example, if G is simple and $\{N_1, \ldots, N_k\}$ is a complete set of representatives of the conjugacy classes of non-trivial nilpotent subgroups of G, then is there an element $x \in G$ such that $N_i \cap N_j^x = 1$ for all i, j? The answer is no, in general. For example, $G = A_6$ has 9 conjugacy classes of non-trivial nilpotent subgroups, with representatives as follows:

$$
\begin{aligned}
N_1 &= \langle (1,3)(4,5) \rangle & N_2 &= \langle (1,4,3) \rangle \\
N_3 &= \langle (1,3,2)(4,6,5) \rangle & N_4 &= \langle (1,6,4,5,3) \rangle \\
N_5 &= \langle (1,2)(3,4), (1,3)(2,4) \rangle & N_6 &= \langle (3,4,5), (1,2,6) \rangle \\
N_7 &= \langle (1,4,3,2)(5,6), (1,3)(2,4) \rangle & N_8 &= \langle (1,2)(3,6), (3,6)(4,5) \rangle \\
N_9 &= \langle (2,5)(3,4), (1,6)(3,4), (1,3)(4,6) \rangle.
\end{aligned}
$$

With the aid of MAGMA, it is easy to check that there is no element $x \in G$ such that $N_i \cap N_j^x = 1$ for all i, j. In particular, this example shows that the answer may depend on the choice of conjugacy class representatives. We are not aware of the existence of a simple group G that does not have an element $x \in G$ and a set of representatives $\{N_1, \ldots, N_k\}$ of the conjugacy classes of nilpotent subgroups of G such that $N_i \cap N_j^x = 1$ for all i, j.

Notation. Let G be a finite group and let n be a positive integer. We will write C_n, or just n, for a cyclic group of order n and G^n for the direct product of n copies of G. An unspecified extension of G by a group H will be denoted by $G.H$; if the extension splits then we may write $G{:}H$. We will use $i_n(G)$ for the number of elements of order n in G, and we will sometimes write $[n]$ for an unspecified soluble group of order n. Throughout the paper, we adopt the standard notation for simple groups of Lie type from [25]. In addition, we write (a, b) for the highest common factor of the positive integers a and b. And for a prime p, we use $(n)_p$ to denote the p-part of n. All logarithms in this paper are base 2.

2. Preliminaries

In this section we present a collection of preliminary results, which will be needed in the proofs of our main theorems.

2.1. **Number theory.** We will require one or two basic number-theoretic results. Given a positive integer m and a prime number p, we write $(m)_p$ for the largest power of p dividing m (so for example, $(18)_3 = 9$).

Lemma 2.1. *Let t be a prime power, let d be a positive integer and let p be a prime divisor of $t - \varepsilon$, where $\varepsilon = \pm 1$.*

  (i) *If $p = 2$, then*
$$(t^d - \varepsilon)_p = \begin{cases} (t - \varepsilon)_p & \text{if } d \text{ is odd} \\ (t^2 - 1)_p(d/2)_p & \text{if } d \text{ is even and } \varepsilon = 1 \\ 2 & \text{if } d \text{ is even and } \varepsilon = -1. \end{cases}$$

  (ii) *If p is odd, then*
$$(t^d - \varepsilon)_p = \begin{cases} 1 & \text{if } d \text{ is even and } \varepsilon = -1 \\ (t - \varepsilon)_p(d)_p & \text{otherwise} \end{cases}$$
$$(t^d + \varepsilon)_p = \begin{cases} (t - \varepsilon)_p(d)_p & \text{if } d \text{ is even and } \varepsilon = -1 \\ 1 & \text{otherwise.} \end{cases}$$

Proof. This is [2, Lemma 2.1(i)]. $\qquad\square$

We will also need the following results concerning factorials and odd prime divisors.

Lemma 2.2. *Let m be a positive integer and let p be a prime. Then $p^m(m!)_p = ((pm)!)_p$ and $(m!)_p < p^k$, where $k = m/(p-1)$.*

Proof. The first claim is clear. For the second statement, set $(m!)_p = p^\ell$ and note that
$$\ell = \sum_{i=1}^{\infty} \left\lfloor \frac{m}{p^i} \right\rfloor < m \sum_{i=1}^{\infty} p^{-i} = \frac{m}{p-1}. \qquad\square$$

Lemma 2.3. *Let d be a positive integer. Then $d + 1$ has at most $\log d$ distinct odd prime divisors.*

Proof. We may assume $d + 1$ is divisible by an odd prime, so we can write
$$d + 1 = 2^a p_1^{a_1} \cdots p_k^{a_k},$$
where the p_i are distinct odd primes and we have $a \geqslant 0$ and $a_i \geqslant 1$ for all i. Setting $b = \sum_i a_i$, we see that $d \geqslant 2^{a+b}$ and thus $k \leqslant b \leqslant \log d$ as required. $\qquad\square$

2.2. **Probability.** Let G be a finite simple group and let $\pi(G)$ be the set of prime divisors of $|G|$. Fix a prime $p \in \pi(G)$ and let H_p be a Sylow p-subgroup of G. In view of Theorem A, we are interested in the following property:

$$\text{There exists an element } x \in G \text{ such that } H_p \cap H_p^x = 1 \text{ for all } p \in \pi(G) \qquad (\star)$$

and our main goal is to show that $(\star)$ holds for all non-alternating simple groups.

Let
$$Q_p(G) = \frac{|\{x \in G : H_p \cap H_p^x \neq 1\}|}{|G|}$$
be the probability that $H_p \cap H_p^x \neq 1$ for a uniformly random element $x \in G$ and note that $Q_p(G) < 1$ by Theorem 2. In fact, the existence of an element $x \in G$ with $H_p \cap H_p^x = 1$ implies that $N_G(H_p)$ has a regular orbit on G/H_p and thus
$$Q_p(G) \leqslant 1 - \frac{|H_p||N_G(H_p)|}{|G|}. \qquad (2)$$

The following observation is immediate.

Lemma 2.4. *Property* $(\star)$ *holds if* $\displaystyle\sum_{p \in \pi(G)} Q_p(G) < 1$.

For a given prime $p \in \pi(G)$, let us observe that $Q_p(G)$ coincides with the probability that a random pair of cosets in G/H_p do not form a base for G. Then by arguing as in the proof of [26, Theorem 1.3], it follows that

$$Q_p(G) \leqslant \widehat{Q}_p(G) := \sum_{i=1}^{k} \frac{|x_i^G \cap H_p|^2}{|x_i^G|},$$

where $\{x_1, \ldots, x_k\}$ is a complete set of representatives of the conjugacy classes in G of elements of order p. In particular, $(\star)$ holds if

$$\sum_{p \in \pi(G)} \widehat{Q}_p(G) < 1. \tag{3}$$

Remark 2.5. Let us record several observations on the above set-up.

(a) We have

$$Q_p(G) = 1 - \frac{s|H_p|}{|G : H_p|},$$

where s is the number of regular H_p-orbits on G/H_p. Equivalently, s is the number of (H_p, H_p) double cosets in G of size $|H_p|^2$.

(b) Let G be a finite simple group of Lie type defined over a field $\mathbb{F}_q$ of characteristic r. If we exclude the special cases $\mathrm{Sp}_4(2)'$, $G_2(2)'$, ${}^2G_2(3)'$ and ${}^2F_4(2)'$, then a result of Zenkov [38, Lemma 3.13] shows that

$$Q_r(G) = 1 - \frac{|H_r||N_G(H_r)|}{|G|},$$

so the upper bound in (2) is in fact an equality in this situation.

In addition, for each prime divisor $p \neq r$ of $|G|$ we will derive an explicit upper bound of the form

$$\widehat{Q}_p(G) \leqslant f_p(t, q),$$

where t is the rank of G. Then by combining these estimates, we get

$$\sum_{p \in \pi(G) \setminus \{r\}} \widehat{Q}_p(G) \leqslant f(t, q),$$

which we can use with the upper bound in (2) (with $p = r$) in order to verify the inequality in (3), with the possible exception of a handful of special cases that can be treated directly. This is our basic approach to the proof of Theorem A for groups of Lie type. In addition, we will see that $f(t, q) \to 0$ as t or q tends to infinity (unless $G = \mathrm{L}_2(q)$ and q is odd) and this is how we will prove Theorem D.

(c) As noted in Section 1, the key inequality $\sum_p Q_p(G) < 1$ in Lemma 2.4 implies that if A and B are nilpotent subgroups of G, then $A \cap B^x = 1$ for some $x \in G$. So a detailed analysis of $\sum_p Q_p(G)$ for groups of Lie type plays an essential role in our proof of Theorem F.

The following elementary result will be useful for computing an upper bound on $\widehat{Q}_p(G)$.

Lemma 2.6. *Suppose* $x_1, \ldots, x_m$ *represent distinct G-classes such that* $\sum_i |x_i^G \cap H_p| \leqslant a$ *and* $|x_i^G| \geqslant b$ *for all i. Then*

$$\sum_{i=1}^{m} \frac{|x_i^G \cap H_p|^2}{|x_i^G|} \leqslant a^2 b^{-1}.$$

Proof. This is [12, Lemma 2.1]. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

3. Sporadic groups

In this section we prove Theorem A for sporadic groups.

Theorem 3.1. *Theorem A holds for all sporadic groups.*

Proof. Let G be a simple sporadic group and for now let us assume $G \notin \mathcal{A}$, where

$$\mathcal{A} = \{\mathrm{J}_4, \mathrm{Ly}, \mathrm{Th}, \mathbb{B}, \mathbb{M}\}. \tag{4}$$

In each case, it is entirely straightforward to verify the desired property with the aid of MAGMA [6] (working with version V2.28-21). In order to do this, we first use the function `AutomorphismGroupSimpleGroup` to construct $L = \mathrm{Aut}(G)$ as a permutation group of degree n, obtaining G as the socle of L. We then construct a Sylow p-subgroup H_p of G for each $p \in \pi(G)$ and by random search it is very easy to find an element $x \in G$ satisfying $(\star)$, as required. To give some indication of timing and memory usage, if $G = \mathrm{HN}$ is the Harada-Norton sporadic simple group, then $|G| = 273030912000000$, $n = 1140000$ and the entire computation takes about 2 minutes, using less than 1GB of memory. For the remainder, we may assume $G \in \mathcal{A}$.

Let $\pi'(G)$ be the set of odd prime divisors of $|G|$ and note that Lemma 2.6 gives

$$\sum_{p \in \pi'(G)} \widehat{Q}_p(G) < \sum_{p \in \pi'(G)} a_p^2 b_p^{-1} < \eta(G),$$

where $a_p = |H_p|$, $b_p = \min\{|x^G| : x \in G, |x| = p\}$ and

$$\eta(G) = \begin{cases} 0.26 & \text{if } G = \mathrm{Ly} \\ 0.49 & \text{if } G = \mathrm{Th} \\ 6.8 \times 10^{-10} & \text{if } G = \mathrm{J}_4 \\ 2.4 \times 10^{-7} & \text{if } G = \mathbb{B} \\ 5.7 \times 10^{-11} & \text{if } G = \mathbb{M}. \end{cases}$$

So to complete the proof, it suffices to show that $\widehat{Q}_2(G) < 1 - \eta(G)$.

For $G = \mathrm{Ly}$ we have $|H_2| = 2^8$ and $|x^G| = 1296826875$ for every involution $x \in G$, so Lemma 2.6 implies that

$$\widehat{Q}_2(G) < 2^{16}(1296826875)^{-1} < 5.1 \times 10^{-5} < 1 - \eta(G)$$

as required. Next assume $G = \mathrm{J}_4$. Here G has two conjugacy classes of involutions, labelled 2A and 2B in [19], where

$$|\text{2A}| = 3980549947 = d_1, \quad |\text{2B}| = 47766599364 = d_2.$$

We can embed H_2 in a maximal subgroup $L = 2^{3+12}.(S_5 \times \mathrm{L}_3(2))$ of G, noting that the character tables of G and L are available in the GAP Character Table Library [7], together with the fusion map from L-classes to G-classes. This allows us to compute

$$|\text{2A} \cap L| = 43067 = c_1, \quad |\text{2B} \cap L| = 131524 = c_2$$

and by appealing to Lemma 2.6 once again we deduce that

$$\widehat{Q}_2(G) \leqslant c_1^2 d_1^{-1} + c_2^2 d_2^{-1} < 0.83.$$

Similarly, $G = \mathrm{Th}$ has a unique class of involutions, labelled 2A in [19], and we can embed H_2 in a maximal subgroup $L = 2^5.\mathrm{L}_5(2)$ of G. We then compute

$$|\text{2A} \cap L| = i_2(L) = 7471 = c_1,$$

which gives $\widehat{Q}_2(G) \leqslant c_1^2 d_1^{-1} < 0.06$, where $d_1 = |\text{2A}| = 976841775$.

Next suppose $G = \mathbb{B}$. Here G has four classes of involutions and we can embed H_2 in a maximal subgroup $L = [2^{35}].(S_5 \times L_3(2))$. By working with [7], we compute

$$
\begin{array}{ll}
|\mathtt{2A}| = 13571955000 = d_1 & |\mathtt{2A} \cap L| = 51512 = c_1 \\
|\mathtt{2B}| = 11707448673375 = d_2 & |\mathtt{2B} \cap L| = 1172575 = c_2 \\
|\mathtt{2C}| = 156849238149120000 = d_3 & |\mathtt{2C} \cap L| = 131022848 = c_3 \\
|\mathtt{2D}| = 355438141723665000 = d_4 & |\mathtt{2D} \cap L| = 313463400 = c_4
\end{array}
$$

which gives $\widehat{Q}_2(G) \leqslant \sum_i c_i^2 d_i^{-1} < 0.7 < 1 - \eta(G)$. Similarly, $G = \mathbb{M}$ has two classes of involutions with

$$|\mathtt{2A}| = 97239461142009186000 = d_1, \quad |\mathtt{2B}| = 579174806851198263694 4259375 = d_2.$$

We can embed H_2 in a maximal subgroup $L = 2^{3+6+12+18}.(3S_6 \times L_3(2))$ of G, noting that [17, Proposition 3.9] gives

$$|\mathtt{2A} \cap L| = 3573456 = c_1, \quad |\mathtt{2B} \cap L| = 4026530095 = c_2.$$

This yields $\widehat{Q}_2(G) \leqslant c_1^2 d_1^{-1} + c_2^2 d_2^{-1} < 1.4 \times 10^{-7}$ and the result follows. $\qquad\square$

Remark 3.2. In the same way, it is entirely straightforward to verify Conjecture 6 for all almost simple sporadic groups.

Remark 3.3. Let G be an almost simple sporadic group and set

$$\alpha(G) = \sum_{p \in \pi(G)} Q_p(G).$$

Our proof of Theorem 3.1 shows that $\alpha(G) < 1$ for the groups $G \in \mathcal{A}$ (see (4)) and it is not difficult to extend this to all almost simple sporadic groups. For example, if

$$G \in \{\mathrm{M}_{11}, \mathrm{M}_{12}.c, \mathrm{M}_{22}.c, \mathrm{M}_{23}, \mathrm{M}_{24}, \mathrm{J}_1, \mathrm{J}_2.c, \mathrm{HS}.c, \mathrm{He}.c\}$$

with $c \in \{1, 2\}$, then for each $p \in \pi(G)$ we can use MAGMA to compute

$$Q_p(G) = 1 - \frac{s|H_p|}{|G : H_p|},$$

where s is the number of (H_p, H_p) double cosets in G of size $|H_p|^2$, and we immediately deduce that $\alpha(G) < 1$. Similarly, for

$$G \in \{\mathrm{J}_3.c, \mathrm{He}.c, \mathrm{McL}.c, \mathrm{Suz}.c, \mathrm{Ru}, \mathrm{Fi}_{22}, \mathrm{Fi}_{23}, \mathrm{Co}_1, \mathrm{Co}_3\}$$

we can compute $\widehat{Q}_p(G)$ precisely for each p (to do this, we can use the approach described in the proof of Lemma 4.2) and we get $\sum_p \widehat{Q}_p(G) < 1$. The latter inequality does not hold for the groups $G \in \{\mathrm{Co}_2, \mathrm{Fi}_{22}.2\}$, but here one checks that

$$Q_2(G) + \sum_{p \in \pi'(G)} \widehat{Q}_p(G) < 1,$$

where $\pi'(G)$ is the set of odd prime divisors of $|G|$. For all of the remaining groups we can work with the GAP Character Table Library [7] to show that

$$\sum_{p \in \pi(G)} \widehat{Q}_p(G) \leqslant \sum_{p \in \pi(G)} \sum_{i=1}^{k_p} a_{p,i}^2 b_{p,i}^{-1} < 1,$$

where

$$a_{p,i} = \min\{|H_p|, |x_i^G \cap L| \,:\, L \in \mathcal{M}_p\}, \quad b_{p,i} = |x_i^G|$$

with respect to a complete set $\{x_1, \ldots, x_{k_p}\}$ of representatives of the conjugacy classes in G of elements of order p and a set $\mathcal{M}_p$ of representatives of the conjugacy classes of maximal overgroups of H_p in G.

This provides an alternative way to prove Theorem A for sporadic groups. In addition, as explained in the discussion following Theorem F in Section 1, the bound $\alpha(G) < 1$ also

gives the conclusion in Corollary G: if A, B are nilpotent subgroups of G, then $A \cap B^x = 1$ for some $x \in G$. In this way, we obtain a new proof of the main theorem of [35].

4. EXCEPTIONAL GROUPS OF LIE TYPE

In this section we will prove Theorems A, D and F for all simple exceptional groups of Lie type; the proofs will be completed in Section 5, where we deal with the classical groups. We begin by setting up some general notation that we will use for all simple groups of Lie type.

Let G be a finite simple group of Lie type over $\mathbb{F}_q$, where $q = r^f$ for some prime r and integer f. As before, let $\pi(G)$ be the set of prime divisors of $|G|$ and set

$$\pi'(G) = \pi(G) \setminus \{r\}.$$

Let H_r be a Sylow r-subgroup of G, which means that $B = N_G(H_r)$ is a Borel subgroup of G with unipotent radical H_r. By choosing $x \in G$ so that B^x is the opposite Borel subgroup, we deduce that $H_r \cap H_r^x = 1$ (without appealing to Theorem 2). So in view of (2) and Lemma 2.4, we observe that $(\star)$ holds (see Section 2.2) if $\Sigma(G) < 1$, where

$$\Sigma(G) = 1 - \frac{|H_r||N_G(H_r)|}{|G|} + \sum_{p \in \pi'(G)} \widehat{Q}_p(G). \tag{5}$$

The main result of this section is the following, which immediately yields Theorems A, D and F for exceptional groups.

Theorem 4.1. *Let G be a finite simple exceptional group of Lie type and set*

$$\alpha(G) = \sum_{p \in \pi(G)} Q_p(G), \quad \beta(G) = \sum_{p \in \pi'(G)} Q_p(G).$$

Then $\alpha(G) < 1$. In addition, $\beta(G) \to 0$ as $|G| \to \infty$.

It is convenient to handle certain low rank groups defined over small fields by direct computation in MAGMA [6]. This is recorded in the following result.

Lemma 4.2. *The conclusion to Theorem 4.1 holds when G is one of the following:*

$$G_2(2)', \ G_2(3), \ G_2(4), \ {}^2G_2(3)', \ {}^2F_4(2)'.$$

Proof. Let r be the defining characteristic. As in the proof of Theorem 3.1, we begin by using the function `AutomorphismGroupSimpleGroup` to construct G as a permutation group of degree n (note that $G_2(2)' \cong U_3(3)$ and ${}^2G_2(3)' \cong L_2(8)$, so we can work directly with the classical groups $U_3(3)$ and $L_2(8)$ in these two special cases). Then for each prime $p \in \pi(G)$ we construct a Sylow p-subgroup H_p of G. In addition, if $p \neq r$ then we construct a set of representatives $\mathcal{C} = \{y_1, \ldots, y_s\}$ of the conjugacy classes in H_p of elements of order p, which we then partition $\mathcal{C} = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_\ell$ so that y_i and y_j are in the same subset if and only if they are conjugate in G. Write $\mathcal{C}_i = \{y_{i,1}, \ldots, y_{i,k_i}\}$ for $i = 1, \ldots, \ell$. Then

$$\widehat{Q}_p(G) = \sum_{i=1}^{\ell} |y_{i,1}^G|^{-1} \left(\sum_{j=1}^{k_j} |y_{i,j}^{H_p}| \right)^2$$

and in each case we verify the bound $\Sigma(G) < 1$. For example, if $G = {}^2F_4(2)'$ then $n = 1755$ and we compute

$$\Sigma(G) = \frac{346991}{449280},$$

with the computation taking roughly 1 second and 30MB of memory. $\qquad\square$

The following result from [18] will be a useful tool.

Lemma 4.3. *Let $G \neq G_2(2)', {}^2F_4(2)', {}^2G_2(3)'$ be a simple exceptional group of Lie type over $\mathbb{F}_q$. Let $x_2 \in G$ be a semisimple element of odd prime order. In addition, if q is odd then let $x_1 \in G$ be an involution. Then $|x_i^G| > \ell_i$, where ℓ_1 and ℓ_2 are given in Table 1.*

G	ℓ_1	ℓ_2			
$E_8(q)$	q^{112}	$(q-1)q^{113}$	$G_2(q), q \geqslant 3$	q^8	$(q-1)q^5$
$E_7(q)$	$\frac{1}{2}(q-1)q^{53}$	$(q-1)q^{53}$	$^3D_4(q)$	q^{16}	$(q-1)q^{17}$
$E_6(q)$	q^{32}	q^{32}	$^2F_4(q), q \geqslant 8$	$-$	$(q-1)q^{17}$
$^2E_6(q)$	$(q-1)q^{31}$	$(q-1)q^{31}$	$^2G_2(q), q \geqslant 27$	$(q-1)q^3$	$\frac{1}{2}q^6$
$F_4(q)$	q^{16}	$(q-1)q^{29}$	$^2B_2(q)$	$-$	$\frac{1}{2}q^4$

TABLE 1. The lower bounds $|x_i^G| > \ell_i$ in Lemma 4.3

Proof. This is a special case of [18, Proposition 2.11]. $\qquad\square$

We are now ready to prove Theorem 4.1.

Proof of Theorem 4.1. Let G be a finite simple exceptional group of Lie type over $\mathbb{F}_q$, where $q = r^f$ is a power of the prime r. Since a very similar argument applies in each case, we will only give details for the groups $^2E_6(q)$, $F_4(q)$ and $G_2(q)'$. It will be convenient to define

$$\widehat{\beta}(G) = \sum_{p \in \pi'(G)} \widehat{Q}_p(G).$$

Case 1. $G = {}^2E_6(q)$

First assume $G = {}^2E_6(q)$ and note that

$$|G| = \frac{1}{d}q^{36}(q^2-1)(q^5+1)(q^6-1)(q^8-1)(q^9+1)(q^{12}-1),$$

where $d = (3, q+1)$. In addition, we have $|N_G(H_r) : H_r| = \frac{1}{d}(q^2-1)^2(q-1)^2$ and

$$\frac{|H_r||N_G(H_r)|}{|G|} = \frac{q^{72}(q^2-1)^2(q-1)^2}{d|G|} > \left(1 - q^{-1}\right)^6,$$

whence $\Sigma(G) < 1$ if

$$\widehat{\beta}(G) \leqslant \left(1 - q^{-1}\right)^6. \tag{6}$$

Fix a prime $p \in \pi'(G)$. For $p = 2$, Lemma 2.1(i) gives

$$|H_2| = 2^3((q^2-1)_2)^4((q+1)_2)^2 \leqslant 2^7(q+1)^6 = a_1$$

and Lemma 4.3 states that $|x^G| > (q-1)q^{31} = b_1$ for every involution $x \in G$. So by appealing to Lemma 2.6 we deduce that $\widehat{Q}_2(G) < a_1^2 b_1^{-1}$.

Now assume p is odd and let m be minimal such that p divides $q^m - 1$, in which case $m \in \{1, 2, 3, 4, 6, 8, 10, 12, 18\}$. By carefully considering each possibility for m in turn, it is straightforward to show that $|H_p| \leqslant 3^3(q+1)^6 = a_2$. For example, if $m = 6$ then $p \geqslant 7$ and

$$|H_p| = (q^6-1)_p(q^9+1)_p(q^{12}-1)_p = ((q^2-q+1)_p)^3.$$

Since $|x^G| > (q-1)q^{31} = b_2$ for all $x \in G$ of order p (see Lemma 4.3), Lemma 2.6 implies that $\widehat{Q}_p(G) < a_2^2 b_2^{-1}$. Moreover, since each $p \in \pi'(G)$ divides $n = (q^4+1)(q^5+1)(q^9+1)(q^{12}-1)$, it follows that $|\pi'(G)| < \log n < 31 \log q$ and thus

$$\widehat{\beta}(G) < (1 - \delta_{2,r})a_1^2 b_1^{-1} + 31 \log q \cdot a_2^2 b_2^{-1},$$

where $\delta_{2,r}$ is the usual Kronecker delta (so $\delta_{2,r} = 1$ if $r = 2$, otherwise $\delta_{2,r} = 0$).

This upper bound immediately implies that $\beta(G) \to 0$ as $q \to \infty$, so the asymptotic statement in Theorem 4.1 holds for $G = {}^2E_6(q)$. In addition, it is routine to check that the inequality in (6) is satisfied for all $q \geqslant 3$.

Finally, suppose $q = 2$ and $p \in \pi'(G)$. Here $|\pi'(G)| = 7$ and $|H_p| \leqslant 3^9 = a$. In addition, by inspecting the character table of G (see [7]) we observe that $|x^G| \geqslant 1319933815200 = b$ for all $x \in G$ of order p. Therefore, $\widehat{\beta}(G) \leqslant 7a^2 b^{-1} < 2^{-6}$ and the result follows.

Case 2. $G = F_4(q)$

Now suppose $G = F_4(q)$. Here

$$|G| = q^{24}(q^2 - 1)(q^6 - 1)(q^8 - 1)(q^{12} - 1)$$

and $|N_G(H_r) : H_r| = (q-1)^4$, whence $\Sigma(G) < 1$ if

$$\widehat{\beta}(G) \leqslant \left(1 - q^{-1}\right)^4. \tag{7}$$

Fix a prime $p \in \pi'(G)$. For $p = 2$ we compute

$$|H_2| = 2^3((q^2 - 1)_2)^4 \leqslant 2^7(q+1)^4 = a_1$$

and we note that $|x^G| > q^{16} = b_1$ for every involution $x \in G$ (see Lemma 4.3). This gives $\widehat{Q}_2(G) < a_1^2 b_1^{-1}$. On the other hand, if p is odd then $|H_p| \leqslant 3^2(q+1)^4 = a_2$ and Lemma 4.3 gives $|x^G| > (q-1)q^{29} = b_2$ for all $x \in G$ of order p, whence $\widehat{Q}_p(G) < a_2^2 b_2^{-1}$. In addition, since $|\pi'(G)| \leqslant 20 \log q$, it follows that

$$\widehat{\beta}(G) < (1 - \delta_{2,r})a_1^2 b_1^{-1} + 20 \log q \cdot a_2^2 b_2^{-1}.$$

Once again, it is clear from this bound that we have $\beta(G) \to 0$ as $q \to \infty$. One can also check that the inequality in (7) is satisfied for all $q \neq 3$.

Finally, suppose $q = 3$. Here $|\pi'(G)| = 6$ and by embedding H_2 in a maximal subgroup $L = 2.\Omega_9(3) = \mathrm{Spin}_9(3)$, we can use MAGMA to show that $i_2(H_2) = 1615$. The result now follows since

$$\widehat{\beta}(G) \leqslant 1615^2 b_1^{-1} + 5a_2^2 b_2^{-1} < \left(\frac{2}{3}\right)^4,$$

where b_1, a_2 and b_2 are defined as above.

Case 3. $G = G_2(q)'$

Finally, suppose $G = G_2(q)'$. In view of Lemma 4.2, we may assume $q \geqslant 5$. Since we have $|G| = q^6(q^2 - 1)(q^6 - 1)$ and $|N_G(H_r)| = q^6(q-1)^2$, it follows that $\Sigma(G) < 1$ if

$$\widehat{\beta}(G) \leqslant \left(1 - q^{-1}\right)^2. \tag{8}$$

Fix a prime $p \in \pi'(G)$. For $p = 2$ we have $|H_2| = ((q^2 - 1)_2)^2 \leqslant 2^2(q+1)^2 = a_1$ and $|x^G| = q^4(q^4 + q^2 + 1) = b_1$ for every involution $x \in G$, which yields $\widehat{Q}_2(G) \leqslant a_1^2 b_1^{-1}$. And for $p \geqslant 3$ we find that $|H_p| \leqslant 3(q+1)^2 = a_2$, while Lemma 4.3 shows that $|x^G| > (q-1)q^5 = b_2$ for all $x \in G$ of order p. Therefore, $\widehat{Q}_p(G) < a_2^2 b_2^{-1}$ and since $|\pi'(G)| \leqslant 6 \log q$ we deduce that

$$\widehat{\beta}(G) < (1 - \delta_{2,r})a_1^2 b_1^{-1} + 6 \log q \cdot a_2^2 b_2^{-1} < \left(1 - q^{-1}\right)^2$$

for all $q \geqslant 19$. In addition, we see that $\beta(G) \to 0$ as $q \to \infty$, so the desired asymptotic statement holds in this case.

Finally, suppose $5 \leqslant q \leqslant 17$. Here it is easy to improve the above estimates in order to verify the bound in (8). For example, suppose $q = 5$. Here $|H_2| = 2^6 = a_1$ and $|H_p| \leqslant 31 = a_2$ for all odd primes $p \in \pi'(G) = \{2, 3, 7, 31\}$. Therefore,

$$\widehat{\beta}(G) \leqslant a_1^2 b_1^{-1} + 3a_2^2 b_2^{-1} = \frac{1958753}{8137500} < \left(\frac{4}{5}\right)^2$$

as required, where b_1 and b_2 are defined as above. $\qquad\square$

5. CLASSICAL GROUPS

In this final section we complete the proofs of Theorems A, D and F by handling the classical groups. Let G be a finite simple classical group over $\mathbb{F}_q$, where $q = r^f$ for a prime r, and let V be the natural module for G. Due to the existence of exceptional isomorphisms between some of the low-dimensional classical groups (see [25, Proposition 2.9.1]), we may assume G is one of the following:

$$
\begin{array}{ll}
\mathrm{L}_n(q) & n \geqslant 2, \text{ with } q \geqslant 5 \text{ if } n = 2 \\
\mathrm{U}_n(q) & n \geqslant 3 \\
\mathrm{PSp}_n(q) & n \geqslant 4 \text{ even, } (n, q) \neq (4, 2) \\
\Omega_n(q) & n \geqslant 7 \text{ odd, } q \text{ odd} \\
\mathrm{P\Omega}_n^{\pm}(q) & n \geqslant 8 \text{ even.}
\end{array}
$$

As before, set $\pi'(G) = \pi(G) \setminus \{r\}$ and define

$$
\alpha(G) = \sum_{p \in \pi(G)} Q_p(G) \qquad \beta(G) = \sum_{p \in \pi'(G)} Q_p(G)
$$
$$
\gamma(G) = \sum_{p \in \pi'(G) \setminus \{2\}} Q_p(G) \qquad \widehat{\beta}(G) = \sum_{p \in \pi'(G)} \widehat{Q}_p(G)
\tag{9}
$$

In addition, define $\Sigma(G)$ as in (5) and recall that $\alpha(G) < 1$ if $\Sigma(G) < 1$. Our main result for classical groups is the following.

Theorem 5.1. *Let G be a finite simple classical group over $\mathbb{F}_q$.*

(i) *If $G \neq \mathrm{U}_4(2)$, then $\alpha(G) < 1$.*

(ii) *We have $\gamma(G) \to 0$ as $|G| \to \infty$.*

(iii) *If $G \neq \mathrm{L}_2(q)$, then $\beta(G) \to 0$ as $|G| \to \infty$.*

Remark 5.2. Let us record a couple of comments on the statement of Theorem 5.1.

(a) First note that the group $G = \mathrm{U}_4(2) \cong \mathrm{PSp}_4(3)$ in part (i) is a genuine exception. Indeed, we have $\pi(G) = \{2, 3, 5\}$ and using MAGMA we compute

$$
Q_2(G) = \frac{71}{135}, \; Q_3(G) = \frac{79}{160}, \; Q_5(G) = \frac{1}{1296},
$$

which means that $\alpha(G) = 2645/2592 > 1$.

(b) Suppose $G = \mathrm{L}_2(q)$ with q odd. Here the proof of Lemma 5.6 shows that $\gamma(G) \to 0$ as $q \to \infty$. However, the asymptotic behaviour of $Q_2(G)$ is rather different and we are not able to conclude that $Q_2(G) \to 0$ as $q \to \infty$. For example, as discussed in Remark 11, we have

$$
Q_2(G) = \frac{1}{2} + \frac{q+3}{2q(q-1)}
$$

if q is a Mersenne prime. This explains the condition $G \neq \mathrm{L}_2(q)$ in part (iii).

Remark 5.3. Let us briefly explain how we establish Theorems A and F in the special case $G = \mathrm{U}_4(2)$, where we have $\pi(G) = \{2, 3, 5\}$ and $\alpha(G) > 1$.

(a) In order to verify Conjecture 6, we first use MAGMA to construct G as a permutation group of degree 45. We fix a Sylow 5-subgroup H_5 of G and we construct the complete set Γ_p of Sylow p-subgroups of G for $p \in \{2, 3\}$. Then for each pair $(H_2, H_3) \in \Gamma_2 \times \Gamma_3$ we use random search to find an element $x \in G$ such that $H_p \cap H_p^x = 1$ for all $p \in \{2, 3, 5\}$. This is an entirely straightforward computation and it establishes Conjecture 6 for $G = \mathrm{U}_4(2)$.

(b) Similarly, to check Theorem F, we first use the function `NilpotentSubgroups` to construct a complete set of representatives of the conjugacy classes of nilpotent subgroups of G (there are 48 such classes). Then for each pair (A, B) of representatives

we use random search to identify an element $x \in G$ with $A \cap B^x = 1$. Once again, this is an easy calculation.

For a positive integer m we set

$$\mathcal{P}_m = \{p \in \pi'(G) : p \neq 2 \text{ is a primitive prime divisor of } q^m - 1\}, \tag{10}$$

which means that each $p \in \mathcal{P}_m$ divides $q^m - 1$, but it does not divide $q^i - 1$ for any $1 \leqslant i < m$. Since every prime divisor $p \neq r$ of $|G|$ is a primitive prime divisor of $q^m - 1$ for some m, it follows that

$$\widehat{\beta}(G) = (1 - \delta_{2,r})\widehat{Q}_2(G) + \sum_{m \geqslant 1} \sum_{p \in \mathcal{P}_m} \widehat{Q}_p(G)$$

and we define

$$\rho_0 = \widehat{Q}_2(G), \quad \rho_1 = \sum_{p \in \mathcal{P}_1} \widehat{Q}_p(G), \quad \rho_2 = \sum_{p \in \mathcal{P}_2} \widehat{Q}_p(G), \quad \rho_3 = \sum_{m \geqslant 3} \sum_{p \in \mathcal{P}_m} \widehat{Q}_p(G). \tag{11}$$

So in terms of this notation, we have

$$\widehat{\beta}(G) = (1 - \delta_{2,r})\rho_0 + \rho_1 + \rho_2 + \rho_3.$$

For each finite simple classical group G over $\mathbb{F}_q$, we will produce an explicit upper bound of the form $\rho_i \leqslant f_i(n,q)$ for each $i \in \{0,1,2,3\}$, where n is the dimension of the natural module for G. By combining these estimates, we will show that

$$\sum_{i=0}^{3} f_i(n,q) < \frac{|H_r||N_G(H_r)|}{|G|}$$

with the possible exception of a handful of special cases, which allows us to conclude that $\Sigma(G) < 1$ and thus $\alpha(G) < 1$, as in Theorem 5.1(i). In addition, it will be clear in every case that we have $f_i(n,q) \to 0$ as n or q tends to infinity (excluding the special case $i = 0$ with $G = L_2(q)$ and q odd) and this is how we establish the asymptotic statements in parts (ii) and (iii) of Theorem 5.1.

In order to derive suitable upper bounds $\rho_i \leqslant f_i(n,q)$, we need to study the conjugacy classes of prime order elements in G. With this aim in mind, fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p. We may view x as an element of $\mathrm{PGL}(V)$, where we recall that V is the natural module for G. In particular, we can write $x = \hat{x}Z$, where $\hat{x} \in \mathrm{GL}(V)$ and Z is the centre of $\mathrm{GL}(V)$, and it will be useful to define the positive integer

$$\nu(x) = \min\{\dim[\bar{V}, \lambda\hat{x}] : \lambda \in K^\times\}, \tag{12}$$

where K is the algebraic closure of $\mathbb{F}_q$ and $\bar{V} = V \otimes K$. Notice that $\nu(x)$ coincides with the codimension of the largest eigenspace of $\hat{x}$ on $\bar{V}$, which explains why it is sometimes referred to as the *support* of x, in analogy with the more familiar definition of support for permutations. Bounds on $|x^G|$ in terms of $\nu(x)$ are given in [13, Section 3]. In addition, we refer the reader to [14, Chapter 3] for detailed information on the conjugacy classes of semisimple elements in G of prime order.

We now consider each family of classical groups in turn, beginning with the linear groups. Throughout this section, we will repeatedly refer to the notation defined in (9), (10), (11) and (12).

5.1. **Linear groups.** In this section we assume $G = L_n(q)$ is a linear group. Note that the low-dimensional groups with $n \in \{2,3\}$ require special attention and they will be handled separately in Lemmas 5.5 and 5.6.

Lemma 5.4. *The conclusion to Theorem 5.1 holds when $G = L_n(q)$ and $n \geqslant 4$.*

Proof. Set $d = (n, q-1)$ and observe that

$$|G| = \frac{1}{d}q^{\frac{1}{2}n(n-1)}\prod_{i=2}^{n}(q^i - 1), \quad |N_G(H_r)| = \frac{1}{d}q^{\frac{1}{2}n(n-1)}(q-1)^{n-1}.$$

Therefore, the desired bound $\Sigma(G) < 1$ holds if

$$\widehat{\beta}(G) \leqslant (1 - q^{-1})^{n-1}. \tag{13}$$

Fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p. Define the integer $\nu(x)$ as in (12). We begin by handling the groups with $n \geqslant 5$.

Case 1. $n \geqslant 5$

First assume $p = 2$, so q is odd. By inspecting [14, Table B.1] we observe that

$$|x^G| \geqslant \frac{|\mathrm{GL}_n(q)|}{|\mathrm{GL}_{n-2}(q)||\mathrm{GL}_2(q)|} > \frac{1}{2}q^{4n-8} = b_2$$

if $\nu(x) \geqslant 2$, otherwise

$$|x^G| = \frac{|\mathrm{GL}_n(q)|}{|\mathrm{GL}_{n-1}(q)||\mathrm{GL}_1(q)|} = \frac{q^{n-1}(q^n - 1)}{q - 1} = b_1.$$

Suppose $q \equiv 1 \pmod 4$. By applying Lemmas 2.1(i) and 2.2 we compute

$$|H_2| = \frac{1}{(d)_2}((q-1)_2)^{n-1}(n!)_2 \leqslant 2^{n-1}(q-1)^{n-1} = a_2$$

and we deduce that $H_2 < L < G$, where L is a subgroup of type $\mathrm{GL}_1(q) \wr S_n$. That is to say, L is the stabiliser in G of a direct sum decomposition $V = V_1 \oplus \cdots \oplus V_n$ of the natural module for G, where each V_i is a 1-dimensional subspace. If $\nu(x) = 1$ then replacing x by a suitable conjugate if necessary, we may assume x lifts to a diagonal matrix $\hat{x} = \mathrm{diag}(-I_{n-1}, I_1)$ in $\mathrm{GL}_n(q)$. And then by counting the number of such involutions in the subgroup $\mathrm{GL}_1(q) \wr S_n < \mathrm{GL}_n(q)$, we deduce that there are no more than

$$a_1 = \binom{n}{1} + \binom{n}{2}|\mathrm{GL}_1(q)| = n + \frac{1}{2}n(n-1)(q-1)$$

involutions $x \in H_2$ with $\nu(x) = 1$. So Lemma 2.6 implies that $\rho_0 < a_1^2 b_1^{-1} + a_2^2 b_2^{-1}$.

Now assume $q \equiv 3 \pmod 4$. If $n = 2\ell$ is even then

$$|H_2| = \frac{1}{4}((q-1)_2(q^2-1)_2)^\ell(\ell!)_2 \leqslant 2^{3\ell-2}(q+1)^\ell = a_2$$

and we note that $(q-1)_2 \leqslant (n)_2$, which implies that $\nu(x) \geqslant 2$ (see [14, Table B.1]). It follows that $\rho_0 < a_2^2 b_2^{-1}$. On the other hand, if $n = 2\ell + 1$ is odd, then

$$|H_2| = ((q-1)_2(q^2-1)_2)^\ell(\ell!)_2 \leqslant 2^{3\ell}(q+1)^\ell = a_2$$

and H_2 is contained in a subgroup $L < G$ of type $(\mathrm{GL}_2(q) \wr S_\ell) \oplus \mathrm{GL}_1(q)$. By considering the number of involutions $x \in L$ with $\nu(x) = 1$, we deduce that $\rho_0 < a_1^2 b_1^{-1} + a_2^2 b_2^{-1}$, where

$$a_1 = 1 + \binom{\ell}{1}\frac{|\mathrm{GL}_2(q)|}{|\mathrm{GL}_1(q)|^2} = 1 + \ell q(q+1).$$

To complete the argument for $n \geqslant 5$ we may assume p is odd, in which case $p \in \mathcal{P}_m$ for some positive integer $m \leqslant n$. Set $k = \lfloor n/m \rfloor$ and write $\gamma = (4, q-1)$ and $\delta = (4, q+1)$.

First assume $m \geqslant 3$, in which case $p \geqslant 5$. By inspecting [14, Section 3.2.1], we see that

$$|x^G| \geqslant \begin{cases} \frac{|\mathrm{GL}_n(q)|}{|\mathrm{GL}_{n-3}(q)||\mathrm{GL}_1(q^3)|} & \text{if } n \neq 6 \\ \frac{|\mathrm{GL}_6(q)|}{|\mathrm{GL}_2(q^3)|} & \text{if } n = 6 \end{cases}$$

and thus $|x^G| > \frac{1}{2}q^{6n-12} = b_3$ for all $n \geqslant 5$. In addition, by applying Lemmas 2.1(ii) and 2.2, we observe that

$$|H_p| = \prod_{i=1}^k (q^{mi} - 1)_p = ((q^m - 1)_p)^k(k!)_p < q^{5n/4} = a_3$$

since $(k!)_p < p^{k/(p-1)} < q^{m(n/4m)} = q^{n/4}$. This yields $\widehat{Q}_p(G) < a_3^2 b_3^{-1}$. Since there are $n-2$ possibilities for m in the range $3 \leqslant m \leqslant n$, and since each $q^m - 1$ has at most $n \log q$ distinct prime divisors, we deduce that

$$\rho_3 < n(n-2) \log q \cdot a_3^2 b_3^{-1}.$$

Next assume $p \in \mathcal{P}_2$, so p divides $(q+1)/\delta$. Here

$$|x^G| \geqslant \frac{|\mathrm{GL}_n(q)|}{|\mathrm{GL}_{n-2}(q)||\mathrm{GL}_1(q^2)|} > \frac{1}{2} q^{4n-6} = b_4$$

and

$$|H_p| = ((q+1)_p)^k (k!)_p \leqslant \left(\frac{1}{\delta}(q+1) \right)^{3n/4} = a_4,$$

which means that $\widehat{Q}_p(G) < a_4^2 b_4^{-1}$ and $\rho_2 < \log((q+1)/\delta) \cdot a_4^2 b_4^{-1}$.

Finally, suppose $p \in \mathcal{P}_1$. Here p divides $(q-1)/\gamma$ and

$$|H_p| = \frac{1}{(d)_p}((q-1)_p)^{n-1}(n!)_p \leqslant \left(\frac{1}{\gamma}(q-1) \right)^{3n/2-1} = a_6.$$

In particular, we notice that H_p is contained in a subgroup $L < G$ of type $\mathrm{GL}_1(q) \wr S_n$. If $\nu(x) \geqslant 2$, then $|x^G| > \frac{1}{2} q^{4n-8} = b_6$. Now assume $\nu(x) = 1$, which means that some G-conjugate of x lifts to a diagonal matrix of the form $\hat{x} = \mathrm{diag}(\lambda, I_{n-1}) \in \mathrm{GL}_n(q)$, where $\lambda \in \mathbb{F}_q^\times$ has order p. It follows that

$$|x^G| = \frac{|\mathrm{GL}_n(q)|}{|\mathrm{GL}_{n-1}(q)||\mathrm{GL}_1(q)|} = \frac{q^{n-1}(q^n-1)}{q-1} = b_5$$

and by counting in L we deduce that there are no more than

$$\binom{n}{1}(p-1) \leqslant n((q-1)/\gamma - 1) = a_5$$

such elements in H_p. This yields $\rho_1 < \log((q-1)/\gamma) \cdot \left(a_5^2 b_5^{-1} + a_6^2 b_6^{-1} \right)$.

It is clear in every case that the given upper bound on ρ_i tends to 0 as n or q tends to infinity, so the asymptotic statements in parts (ii) and (iii) of Theorem 5.1 hold when $G = \mathrm{L}_n(q)$ and $n \geqslant 5$. In addition, if $n \geqslant 7$ then it is routine to check that the given estimates imply that the inequality in (13) is satisfied unless (n, q) is one of the following:

$$(7,2), (7,3), (8,2), (8,3), (9,2), (9,3), (10,2), (10,3), (12,3). \tag{14}$$

Suppose $(n, q) = (7, 2)$. If $p \in \mathcal{P}_m$ with $m \geqslant 3$ then $|H_p| \leqslant 127$ and we note that $|\pi'(G)| = 5$, $\mathcal{P}_2 = \{3\}$, $\mathcal{P}_1 = \emptyset$ and $|H_3| = 3^4$. Therefore,

$$\widehat{\beta}(G) < 4a_3^2 b_3^{-1} + a_4^2 b_4^{-1} < 2^{-6}$$

where $a_3 = 127$, $a_4 = 3^4$ and b_3, b_4 are defined as above. Similarly, if $(n, q) = (7, 3)$ then $|\pi'(G)| = 6$, $\mathcal{P}_1 = \mathcal{P}_2 = \emptyset$ and $|H_2| = 2^{13}$. In addition, $|H_p| \leqslant 1093$ for all odd primes $p \in \pi'(G)$ and thus

$$\widehat{\beta}(G) < a_1^2 b_1^{-1} + a_2^2 b_2^{-1} + 5a_3^2 b_3^{-1} < \left(\frac{2}{3} \right)^6,$$

where $a_2 = 2^{13}$, $a_3 = 1093$ and a_1, b_1, b_2, b_3 are defined as above. All of the other cases in (14) can be handled in an entirely similar fashion.

Now assume $n \in \{5, 6\}$. Here we observe that $|H_p| \leqslant c((q-1)/\gamma)^{n-1}$ for all $p \in \mathcal{P}_1$, where $c = 5$ if $n = 5$ and $c = 9$ if $n = 6$ (since $(5!)_p \leqslant 5$ and $(6!)_p \leqslant 3^2$ for all odd primes p). Then by setting $a_6 = c((q-1)/\gamma)^{n-1}$, one can check that our previous bounds are sufficient unless (n, q) is one of the following:

$$(5,2), (5,3), (5,4), (5,5), (6,2), (6,3).$$

All of these special cases can be handled using MAGMA. For example, if $(n, q) = (5, 2)$ then we compute

$$\Sigma(G) = \frac{4483687}{4999680} < 1,$$

where $\Sigma(G)$ is defined in (5).

Case 2. $n = 4$

Now assume $n = 4$. If $p = 2$ and $q \equiv 1 \pmod 4$, then $\rho_0 \leqslant a_1^2 b_1^{-1} + a_2^2 b_2^{-1}$, where

$$a_1 = \binom{4}{1} + \binom{4}{2}(q - 1), \quad b_1 = \frac{|\mathrm{GL}_4(q)|}{|\mathrm{GL}_3(q)||\mathrm{GL}_1(q)|} = q^3(q + 1)(q^2 + 1)$$

and

$$a_2 = 2(q - 1)^3, \quad b_2 = \frac{|\mathrm{GL}_4(q)|}{2|\mathrm{GL}_2(q^2)|} = \frac{1}{2}q^4(q - 1)(q^3 - 1),$$

noting that $|H_2| \leqslant a_2$. Similarly, if $p = 2$ and $q \equiv 3 \pmod 4$, then $\nu(x) = 2$ (see [14, Table B.1]) and Lemma 2.6 implies that $\rho_0 \leqslant a_2^2 b_2^{-1}$, where $|H_2| \leqslant 8(q + 1)^2 = a_2$ and b_2 is defined as above.

Now suppose $p \geqslant 3$ is odd and define γ, δ as before. Note that $p \in \mathcal{P}_m$ with $m \in \{1, 2, 3, 4\}$. If $m \in \{3, 4\}$ then $|H_p| \leqslant q^2 + q + 1 = a_3$ and

$$|x^G| \geqslant \frac{|\mathrm{GL}_4(q)|}{|\mathrm{GL}_1(q^4)|} = q^6(q - 1)(q^2 - 1)(q^3 - 1) = b_3,$$

which means that

$$\rho_3 \leqslant 2\log(q^2 + q + 1) \cdot a_3^2 b_3^{-1}.$$

Similarly, if $m = 2$ then $|H_p| \leqslant ((q + 1)/\delta)^2 = a_4$ and

$$|x^G| \geqslant \frac{|\mathrm{GL}_4(q)|}{|\mathrm{GL}_2(q^2)|} = q^4(q - 1)(q^3 - 1) = b_4,$$

which yields $\rho_2 \leqslant \log((q + 1)/\delta) \cdot a_4^2 b_4^{-1}$.

Finally, suppose $m = 1$, so p divides $(q - 1)/\gamma$ and H_p is contained in a subgroup of type $\mathrm{GL}_1(q) \wr S_4$. In particular, $|H_p| \leqslant 3((q - 1)/\gamma)^3 = a_6$. If $\nu(x) = 1$ then

$$|x^G| = \frac{|\mathrm{GL}_4(q)|}{|\mathrm{GL}_3(q)||\mathrm{GL}_1(q)|} = q^3(q + 1)(q^2 + 1) = b_5$$

and by arguing as in Case 1 we see that there are no more than $a_5 = 4((q - 1)/\gamma - 1)$ such elements in H_p. For $\nu(x) \geqslant 2$ we have

$$|x^G| \geqslant \frac{|\mathrm{GL}_4(q)|}{|\mathrm{GL}_2(q)|^2} = q^4(q^2 + 1)(q^2 + q + 1) = b_6$$

and it follows that $\rho_1 \leqslant \log((q - 1)/\gamma) \cdot (a_5^2 b_5^{-1} + a_6^2 b_6^{-1})$.

As before, it is clear that each upper bound on ρ_i tends to 0 as q tends to infinity. In addition, for $q \geqslant 4$ we find that our bounds are good enough to give the desired inequality in (13) with $n = 4$. In the two remaining cases we compute $\Sigma(G) = 9799/10080$ when $q = 2$, whereas $\Sigma(G) = 388757/379080$ when $q = 3$. So this gives the result for $q = 2$, but further work is needed when $q = 3$. In the latter case, we have $\pi(G) = \{2, 3, 5, 13\}$ and for each $p \in \pi(G)$ we can use MAGMA to compute

$$Q_p(G) = 1 - \frac{s|H_p|}{|G : H_p|},$$

where s is the number of (H_p, H_p) double cosets in G of size $|H_p|^2$. This yields

$$Q_2(G) = \frac{829}{3645}, \quad Q_3(G) = \frac{1351}{2080}, \quad Q_5(G) = \frac{1}{75816}, \quad Q_{13}(G) = \frac{1}{155520}$$

and thus $\alpha(G) < 1$ as required. $\qquad\square$

To complete the proof of Theorem 5.1 for linear groups, it just remains for us to handle $L_3(q)$ and $L_2(q)$.

Lemma 5.5. *The conclusion to Theorem 5.1 holds when $G = L_3(q)$.*

Proof. First observe that $\Sigma(G) < 1$ if

$$\widehat{\beta}(G) < \frac{q^3}{(q+1)(q^2+q+1)}. \tag{15}$$

Fix a prime $p \in \pi'(G)$ and set $\gamma = (4, q-1)$ and $\delta = (4, q+1)$ as before. Let $x \in G$ be an element of order p.

First assume $p = 2$, so q is odd and $|x^G| = q^2(q^2+q+1) = b_1$ for every involution $x \in G$. If $q \equiv 1 \pmod 4$ then $|H_2| = 2((q-1)_2)^2$ and H_2 is contained in a subgroup $L < G$ of type $GL_1(q) \wr S_3$. By counting in L, we see that $i_2(H_2) \leqslant 3 + 3(q-1) = 3q = a_1$. And for $q \equiv 3 \pmod 4$ we have $|H_2| \leqslant 4(q+1) = a_1$. It follows that $\rho_0 \leqslant a_1^2 b_1^{-1}$ for all odd q.

Now assume $p \in \mathcal{P}_m$ with $m \in \{1, 2, 3\}$. If $m = 3$ then

$$|H_p| = (q^2+q+1)_p \leqslant q^2+q+1 = a_2, \quad |x^G| = q^3(q-1)(q^2-1) = b_2$$

and thus $\rho_3 \leqslant a_2^2 b_2^{-1} \log a_2$. Similarly, we have $\rho_2 \leqslant a_3^2 b_3^{-1} \log a_3$, where $a_3 = (q+1)/\delta$ and $b_3 = q^3(q^3-1)$. Finally, suppose $m = 1$. Here $|H_p| \leqslant 3((q-1)/\gamma)^2 = a_5$ and we note that H_p is contained in a subgroup of type $GL_1(q) \wr S_3$. If $\nu(x) = 1$ then $|x^G| = q^2(q^2+q+1) = b_4$ and there are at most $3((q-1)/\gamma - 1) = a_4$ of these elements in H_p. Otherwise, if $\nu(x) = 2$ then $|x^G| \geqslant \frac{1}{3}q^3(q+1)(q^2+q+1) = b_5$ and we deduce that

$$\rho_1 \leqslant \log((q-1)/\gamma) \cdot (a_4^2 b_4^{-1} + a_5^2 b_5^{-1}).$$

The above estimates show that $\beta(G) \to 0$ as $q \to \infty$, and they also imply that the inequality in (15) holds if $q \geqslant 9$. For $3 \leqslant q \leqslant 8$, we can use MAGMA to check that $\Sigma(G) < 1$. Finally, for $q = 2$ we compute $\Sigma(G) = 121/84$, so this case requires further attention. Here $\pi(G) = \{2, 3, 7\}$ and using MAGMA we get

$$Q_2(G) = \frac{13}{21}, \; Q_3(G) = \frac{1}{28}, \; Q_7(G) = \frac{1}{8},$$

which implies that $\alpha(G) < 1$. $\qquad\square$

Lemma 5.6. *The conclusion to Theorem 5.1 holds when $G = L_2(q)$.*

Proof. First observe that $|G| = \frac{1}{d}q(q^2-1)$ and $|N_G(H_r)| = \frac{1}{d}q(q-1)$, where $d = (2, q-1)$, so we have $\Sigma(G) < 1$ if

$$\widehat{\beta}(G) < \frac{q}{q+1}. \tag{16}$$

Fix a prime $p \in \pi'(G)$. For $p = 2$ we have $H_2 = D_{(q-\varepsilon)_2}$, where $q \equiv \varepsilon \pmod 4$ and $\varepsilon = \pm 1$, so $i_2(H_2) \leqslant \frac{1}{2}(q+3) = a_1$ and we note that $|x^G| \geqslant \frac{1}{2}q(q-1) = b_1$ for all involutions $x \in G$. It follows that

$$\rho_0 \leqslant a_1^2 b_1^{-1} = \frac{(q+3)^2}{2q(q-1)}.$$

Notice that this estimate does not imply that $Q_2(G) \to 0$ as q tends to infinity, which explains why $G = L_2(q)$ is excluded in part (iii) of Theorem 5.1. For example, if $q = 2^k - 1$ is a Mersenne prime, then $H_2 = D_{q+1}$ and by appealing to [15, Lemma 7.9] we compute

$$Q_2(G) = 1 - \frac{s|H_2|}{|G : H_2|} = \frac{1}{2} + \frac{q+3}{2q(q-1)},$$

where $s = (q-3)/4$ is the number of regular orbits of H_2 on G/H_2. In particular, we observe that $Q_2(G) > \frac{1}{2}$ for every Mersenne prime q (and of course, we expect that there are infinitely many such primes).

Now assume $p \geqslant 3$ and let $x \in G$ be an element of order p. Set $\gamma = (4, q-1)$ and $\delta = (4, q+1)$. First suppose p divides $q-1$. Now G has $(p-1)/2$ distinct conjugacy classes of such elements, with $|x^G| = q(q+1)$ and $|x^G \cap H_p| = 2$ for all $x \in G$ of order p, whence

$$\widehat{Q}_p(G) = \frac{1}{2}(p-1) \cdot \frac{4}{q(q+1)} = \frac{2(p-1)}{q(q+1)} \leqslant \frac{2(q-2)}{q(q+1)}.$$

Similarly, if p divides $q+1$, then $|x^G| = q(q-1)$, $|x^G \cap H_p| = 2$ and we get

$$\widehat{Q}_p(G) = \frac{1}{2}(p-1) \cdot \frac{4}{q(q-1)} \leqslant \frac{2}{q-1}.$$

It follows that

$$\gamma(G) \leqslant \log((q-1)/\gamma) \cdot \frac{2(q-2)}{q(q+1)} + \log((q+1)/\delta) \cdot \frac{2}{q-1}$$

and thus $\gamma(G) \to 0$ as $q \to \infty$. In addition, we get

$$\widehat{\beta}(G) \leqslant (1 - \delta_{2,r})\frac{(q+3)^2}{2q(q-1)} + \log((q-1)/\gamma) \cdot \frac{2(q-2)}{q(q+1)} + \log((q+1)/\delta) \cdot \frac{2}{q-1},$$

which implies that the inequality in (16) holds for all $q > 37$. The remaining groups with $5 \leqslant q \leqslant 37$ can be checked using MAGMA. Indeed, for $q \neq 7$ we compute $\Sigma(G) < 1$, while for $q = 7$ we have $G \cong \mathrm{L}_3(2)$ and so this case has already been handled in Lemma 5.5. $\qquad\square$

5.2. **Unitary groups.** We now turn to the proof of Theorem 5.1 for the unitary groups. So throughout this section we assume $G = \mathrm{U}_n(q)$ with $n \geqslant 3$ and $(n, q) \neq (3, 2)$. Our main result is the following (note that the 3-dimensional groups are handled separately in Lemma 5.8).

Lemma 5.7. *The conclusion to Theorem 5.1 holds when $G = \mathrm{U}_n(q)$ and $n \geqslant 4$.*

Proof. Set $d = (n, q+1)$ and first observe that

$$|N_G(H_r) : H_r| = \frac{1}{d}(q^2 - 1)^{\lfloor (n-1)/2 \rfloor}(q-1)^e,$$

where $e = 1$ if n is even, otherwise $e = 0$. It follows that $\Sigma(G) < 1$ if the bound in (13) is satisfied.

Case 1. $n \geqslant 5$

Fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p. First assume $p = 2$, so q is odd and we have

$$|x^G| = \frac{|\mathrm{GU}_n(q)|}{|\mathrm{GU}_{n-1}(q)||\mathrm{GU}_1(q)|} = \frac{q^{n-1}(q^n - (-1)^n)}{q+1} = b_1$$

if $\nu(x) = 1$ (see [14, Table B.1]). Similarly, $|x^G| > \frac{1}{2}(q+1)^{-1}q^{4n-7} = b_2$ if $\nu(x) = 2$ and we have $|x^G| > \frac{1}{4}(q+1)^{-1}q^{6n-17} = b_3$ if $\nu(x) \geqslant 3$. There are now four cases to consider, according to the parity of n and the congruence class of q modulo 4.

Suppose $n = 2\ell + 1$ is odd and $q \equiv 1 \pmod 4$. By appealing to Lemma 2.1(i) we compute

$$|H_2| = ((q+1)_2(q^2-1)_2)^\ell (\ell!)_2 \leqslant 2^{3\ell}(q-1)^\ell = a_2$$

and it follows that $H_2 < L < G$, where L is of type $(\mathrm{GU}_2(q) \wr S_\ell) \perp \mathrm{GU}_1(q)$. Here the notation indicates that L is the stabiliser in G of an orthogonal decomposition

$$V = U \perp W = U_1 \perp \cdots \perp U_\ell \perp W$$

of the natural module for V, where each U_i is a non-degenerate 2-space and W is a non-degenerate 1-space. By counting in L, we deduce that there are at most

$$a_1 = 1 + \binom{\ell}{1}\frac{|\mathrm{GU}_2(q)|}{|\mathrm{GU}_1(q)|^2} = 1 + \ell q(q-1)$$

involutions $x \in H_2$ with $\nu(x) = 1$, so Lemma 2.6 yields $\rho_0 < a_1^2 b_1^{-1} + a_2^2 b_2^{-1}$.

Next assume $n = 2\ell + 1$ and $q \equiv 3 \pmod 4$. Here

$$|H_2| = ((q+1)_2)^{n-1}(n!)_2 \leqslant 2^{n-1}(q+1)^{n-1} = a_3$$

and we see that $H_2 < L < G$ with L of type $\mathrm{GU}_1(q) \wr S_n$. Then by working in L, we calculate that the number of involutions $x \in H_2$ with $\nu(x) = 1$ is at most

$$a_1 = \binom{n}{1} + \binom{n}{2}|\mathrm{GU}_1(q)| = n + \frac{1}{2}n(n-1)(q+1). \tag{17}$$

Similarly, there are at most

$$
\begin{aligned}
a_2 &= \binom{n}{2} + \binom{n}{2}\binom{n-2}{1}|\mathrm{GU}_1(q)| + \frac{n!}{(n-4)!2!2^2}|\mathrm{GU}_1(q)|^2 \\
&= \frac{1}{2}n(n-1)\left(1 + (n-2)(q+1) + \frac{1}{4}(n-2)(n-3)(q+1)^2\right)
\end{aligned}
\tag{18}
$$

involutions in H_2 with $\nu(x) = 2$. This implies that

$$\rho_0 < a_1^2 b_1^{-1} + a_2^2 b_2^{-1} + a_3^2 b_3^{-1}. \tag{19}$$

Now assume $n = 2\ell$ is even. If $q \equiv 1 \pmod 4$ then $\nu(x) \geqslant 2$ (see [14, Table B.1]) and

$$|H_2| = \frac{1}{4}((q+1)_2(q^2-1)_2)^\ell(\ell!)_2 \leqslant 2^{3\ell-2}(q-1)^\ell = a_2,$$

whence Lemma 2.6 implies that $\rho_0 < a_2^2 b_2^{-1}$. Finally, suppose $q \equiv 3 \pmod 4$. Here

$$|H_2| = \frac{1}{(d)_2}((q+1)_2)^{n-1}(n!)_2 \leqslant 2^{n-1}(q+1)^{n-1} = a_3$$

and thus $H_2 < L < G$ with L of type $\mathrm{GU}_1(q) \wr S_n$. Then as above, we calculate that H_2 contains at most a_1 (respectively, a_2) involutions with $\nu(x) = 1$ (respectively, $\nu(x) = 2$), where a_1 and a_2 are defined in (17) and (18), and we conclude that (19) holds.

Now assume $p \geqslant 3$ is odd, so $p \in \mathcal{P}_m$ with $m \leqslant 2n$. Note that either $m \leqslant \lfloor n/2 \rfloor$ is odd, or $m \leqslant n$ is even, or $m = 2i$ with $n/2 < i \leqslant n$ odd. In particular, there are precisely n possibilities for m.

To begin with, let us assume $m \geqslant 3$ and note that $p \geqslant 5$. By considering the possibilities for $|C_G(x)|$ (see [14, Section 3.3.1]), we first observe that

$$|x^G| \geqslant \begin{cases} \dfrac{|\mathrm{GU}_n(q)|}{|\mathrm{GU}_{n-3}(q)||\mathrm{GU}_1(q^3)|} & \text{if } n \neq 6 \\[2mm] \dfrac{|\mathrm{GU}_6(q)|}{|\mathrm{GU}_2(q^3)|} & \text{if } n = 6 \end{cases}$$

and thus $|x^G| > \frac{1}{2}(q+1)^{-1}q^{6n-11} = b_4$.

We claim that

$$|H_p| \leqslant (q^3+1)^{\frac{11}{24}n+\frac{1}{3}} = a_4.$$

If $m \equiv 0 \pmod 4$, then by applying Lemmas 2.1(ii) and 2.2, we compute

$$|H_p| = \prod_{i=1}^k (q^{mi}-1)_p = ((q^{m/2}+1)_p)^k(k!)_p < (q^{m/2}+1)^{\frac{5n}{4m}} \leqslant (q^2+1)^{\frac{5}{16}n} < a_4,$$

where $k = \lfloor n/m \rfloor$. Similarly, if m is odd and $k = \lfloor n/2m \rfloor$ then

$$|H_p| = \prod_{i=1}^k (q^{2mi}-1)_p = ((q^m-1)_p)^k(k!)_p < q^{\frac{5}{8}n} < a_4.$$

Finally, suppose $m \equiv 2 \pmod 4$ and set $k = \lfloor (n-1+e)/m \rfloor$ and $\ell = \lfloor (n-e)/m + 1/2 \rfloor$, where $e = 1$ if n is even, otherwise $e = 0$. Then

$$|H_p| = \prod_{i=1}^k (q^{mi}-1)_p \cdot \prod_{i=1}^\ell (q^{m(2i-1)}-1)_p = ((q^{m/2}+1)_p)^{k+\ell}(k!)_p \prod_{i=1}^\ell (2i-1)_p$$

and we deduce that

$$|H_p| \leqslant (q^{m/2} + 1)^{\frac{5}{4}k + \ell + \frac{1}{4}(2\ell - 1)} \leqslant (q^3 + 1)^{\frac{11}{24}n + \frac{1}{3}} = a_4.$$

This justifies the claim. In addition, since there are $n - 2$ possibilities for m with $m \geqslant 3$ and since $|\mathcal{P}_m| < \frac{1}{2}n \log q$ for all m (see Lemma 2.3), it follows that

$$\rho_3 < \frac{1}{2}n(n - 2) \log q \cdot a_4^2 b_4^{-1}.$$

Next suppose $m = 2$, so p divides $(q + 1)/\delta$ and

$$|H_p| = \frac{1}{(d)_p}((q + 1)_p)^{n-1}(n!)_p \leqslant ((q + 1)/\delta)^{\frac{3}{2}n - 1} = a_7,$$

where $\delta = (4, q + 1)$. In particular, we have $H_p < L < G$ with L of type $\mathrm{GU}_1(q) \wr S_n$. If $\nu(x) = 1$ then

$$|x^G| = \frac{|\mathrm{GU}_n(q)|}{|\mathrm{GU}_{n-1}(q)||\mathrm{GU}_1(q)|} = \frac{q^{n-1}(q^n - (-1)^n)}{q + 1} = b_5$$

and by counting in L we deduce that there are at most

$$\binom{n}{1}(p - 1) \leqslant n((q + 1)/\delta - 1) = a_5$$

of these elements in H_p. Similarly, if $\nu(x) = 2$ then $|x^G| > \frac{1}{2}(q + 1)^{-1}q^{4n-7} = b_6$ and H_p contains no more than

$$\binom{n}{2}(p - 1)^2 + \delta_{3,p}\frac{n!}{(n - 3)!3}|\mathrm{GU}_1(q)|^2$$

such elements, which in turn is at most

$$a_6 = \frac{1}{2}n(n - 1)\left(((q + 1)/\delta - 1)^2 + \frac{2}{3}(n - 2)(q + 1)^2\right).$$

Since $|x^G| > \frac{1}{2}(q + 1)^{-1}q^{6n-17} = b_7$ if $\nu(x) \geqslant 3$, it follows that

$$\rho_2 < \log((q + 1)/\delta) \cdot (a_5^2 b_5^{-1} + a_6^2 b_6^{-1} + a_7^2 b_7^{-1}).$$

Finally, suppose $m = 1$ and set $\gamma = (4, q - 1)$ and $k = \lfloor n/2 \rfloor$. Then p divides $(q - 1)/\gamma$ and

$$|H_p| = ((q - 1)_p)^k(k!)_p \leqslant ((q - 1)/\gamma)^{\frac{3}{4}n} = a_8.$$

In addition, we have

$$|x^G| \geqslant \frac{|\mathrm{GU}_n(q)|}{|\mathrm{GU}_{n-2}(q)||\mathrm{GL}_1(q^2)|} > \frac{1}{2}\left(\frac{q}{q + 1}\right)q^{4n-6} = b_8$$

for all $x \in G$ of order p, which implies that

$$\rho_1 < \log((q - 1)/\gamma) \cdot a_8^2 b_8^{-1}.$$

For each i, it is clear that the above estimates $\rho_i < f_i(n, q)$ have the property that $f_i(n, q) \to 0$ as either n or q tends to infinity. In particular, $\beta(G) \to 0$ as $|G| \to \infty$.

So to complete the proof of the lemma for $n \geqslant 5$, it just remains to show that $\alpha(G) < 1$. To do this, it will be convenient to partition our analysis of the above bounds according to the parity of q.

First assume q is odd. Here it is straightforward to check that the bound

$$\widehat{\beta}(G) < \sum_{i=0}^{3} f_i(n, q)$$

shows that the inequality in (13) is satisfied unless (n, q) is one of the following:

$$(5, 3), \ (5, 5), \ (5, 7), \ (6, 3), \ (7, 3), \ (8, 3).$$

For $(n,q) = (5,3)$ we can use MAGMA to check that $\Sigma(G) < 1$. And in each of the remaining cases, we can adjust the above estimates to give the desired result. For example, if $(n,q) = (5,5)$ then we compute $i_2(H_2) = 51$ and $\pi'(G) = \{2,3,7,13,521\}$, which means that we can set $a_2 = 51$ in our previous upper bound on ρ_0 and we can replace the factor $\frac{1}{2}n(n-2)\log q$ in the expression for a_4 by 3. It is then straightforward to check that the modified bound is sufficient.

Now suppose q is even. The case $q = 2$ will require special attention, so for now let us assume $q \geqslant 4$. If $n \geqslant 7$ then the bound

$$\widehat{\beta}(G) < \sum_{i=1}^{3} f_i(n,q)$$

is sufficient unless $(n,q) = (7,4)$. In the latter case, we have $\mathcal{P}_2 = \{5\}$ and $|H_5| = 5^7$, so we can set $a_7 = 5^7$ in the expression for $f_2(n,q)$ and then check that the corresponding bound on $\widehat{\beta}(G)$ is sufficient.

Next assume $n \in \{5,6\}$ and $q \geqslant 4$. If $n = 6$ then $m \in \{1,2,3,4,6,10\}$ and for $m \geqslant 3$ we observe that $|H_p| \leqslant q^4 - q^3 + q^2 - q + 1 = a_4$ and p divides

$$(q^2 + 1)(q^2 + q + 1)(q^2 - q + 1)(q^4 - q^3 + q^2 - q + 1) < q^{10},$$

which implies that $\rho_3 < 10\log q \cdot a_4^2 b_4^{-1}$, where b_4 is defined as above. Similarly, if $m = 2$ then $|H_p| \leqslant 5(q+1)^5$, so we can set $a_7 = 5(q+1)^5$ in the definition of $f_2(n,q)$. With these modifications, it is easy to check that the corresponding upper bound on $\widehat{\beta}(G)$ is sufficient for all $q \geqslant 4$.

The case $n = 5$ is very similar. Here $\rho_3 < 8\log q \cdot a_4^2 b_4^{-1}$, where $a_4 = q^4 - q^3 + q^2 - q + 1$ and b_4 is defined as above. In addition, we can set $a_7 = c(q+1)^4$ in the definition of $f_2(n,q)$, where $c = 3$ if $q \equiv -1 \pmod 3$, otherwise $c = 1$. The reader can then check that the improved upper bound on $\widehat{\beta}(G)$ is sufficient for all $q \geqslant 8$. Finally, if $(n,q) = (5,4)$ then $\pi'(G) = \{3,5,13,17,41\}$ and thus

$$\widehat{\beta}(G) < 3a_4^2 b_4^{-1} + \sum_{i=5}^{8} a_i^2 b_i^{-1} < \left(\frac{3}{4}\right)^4$$

as required.

Finally, let us assume $q = 2$. If $n \in \{5,6,7,8\}$ then we can use MAGMA to check that $\Sigma(G) < 1$. For example, for $n = 5$ we get

$$\Sigma(G) = \frac{6566723}{6842880}.$$

So for the remainder, we may assume $n \geqslant 9$. To resolve this case, we need to improve the upper bound $\rho_2 \leqslant f_2(n,2)$ presented above, noting that $\mathcal{P}_2 = \{3\}$ and H_3 is contained in a subgroup L of type $\mathrm{GU}_1(2) \wr S_n$.

With this goal in mind, let $x \in G$ be an element of order 3 and observe that

$$|x^G| \geqslant \frac{|\mathrm{GU}_n(2)|}{|\mathrm{GU}_{n-4}(2)||\mathrm{GU}_4(2)|} > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{8n-32} = b_9$$

if $\nu(x) \geqslant 4$. Now, if $\nu(x) = 3$ then $|x^G| > \frac{1}{2}(q+1)^{-1}q^{6n-17} = b_7$ and by counting in L we deduce that there are no more than

$$a_7 = 2^3\binom{n}{3} + \frac{n!}{(n-3)!3}|\mathrm{GU}_1(2)|^2 \cdot 2\binom{n-3}{1} = \frac{2}{3}n(n-1)(n-2)(9n-25)$$

such elements in H_3. Since $|H_3| < 3^{3n/2-1} = a_9$, we deduce that

$$\rho_2 < a_5^2 b_5^{-1} + a_6^2 b_6^{-1} + a_7^2 b_7^{-1} + a_9^2 b_9^{-1},$$

where the terms a_5, b_5, a_6 and b_6 are defined as in the main argument above. By combining this revised estimate for ρ_2 with our previous bound on ρ_3, the reader can check that $\widehat{\beta}(G) < 1$ for all $n \geqslant 14$.

Finally, suppose $9 \leqslant n \leqslant 13$. Recall that

$$\frac{|H_2||N_G(H_2)|}{|G|} = \frac{2^{n(n-1)/2}3^{\lfloor(n-1)/2\rfloor}}{\prod_{i=2}^{n}(2^i - (-1)^i)} =: f(n)$$

and it suffices to show that $\widehat{\beta}(G) < f(n)$. One checks that our previous upper bound on $\widehat{\beta}(G)$ is sufficient if $n \in \{11, 12, 13\}$, so we may assume $n = 9$ or 10. Here we can improve the upper bound on ρ_2 by setting

$$a_9 = i_3(H_3) = \begin{cases} 104246 & \text{if } n = 10 \\ 28430 & \text{if } n = 9, \end{cases}$$

where we have computed the exact values using MAGMA. One can now check that the revised estimate for $\widehat{\beta}(G)$ is good enough.

Case 2. $n = 4$

To complete the proof of the lemma we may assume $n = 4$. In view of part (i) of Theorem 5.1, we may assume $q \geqslant 3$. And with the aid of MAGMA we check that $\Sigma(G) < 1$ when $q \in \{3, 4, 5\}$, so we can assume $q \geqslant 7$. Note that it suffices to show that

$$\widehat{\beta}(G) < \frac{|H_r||N_G(H_r)|}{|G|} = \frac{q^6}{(q^3 + 1)(q^2 + 1)(q + 1)}. \tag{20}$$

Fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p.

First assume $p = 2$. If $q \equiv 1 \pmod 4$ then $|H_2| \leqslant 8(q-1)^2 = a_2$ and $\nu(x) = 2$, so

$$|x^G| \geqslant \frac{|\mathrm{GU}_4(q)|}{2|\mathrm{GU}_2(q)|^2} = \frac{1}{2}q^4(q^2 - q + 1)(q^2 + 1) = b_2$$

and $\rho_0 \leqslant a_2^2 b_2^{-1}$. Now assume $q \equiv 3 \pmod 4$. Here $|H_2| = 2((q+1)_2)^3 \leqslant 2(q+1)^3 = a_2$ and H_2 is contained in a subgroup L of type $\mathrm{GU}_1(q) \wr S_4$. If $\nu(x) = 1$ then $|x^G| = q^3(q-1)(q^2+1) = b_1$ and by working in L we calculate that there are at most $a_1 = 6q + 10$ such elements in H_2, so it follows that $\rho_0 \leqslant a_1^2 b_1^{-1} + a_2^2 b_2^{-1}$.

Now assume p is odd, so $p \in \mathcal{P}_m$ with $m \in \{1, 2, 4, 6\}$. If $m \in \{4, 6\}$ then $|H_p| \leqslant q^2 + 1 = a_3$ and

$$|x^G| \geqslant \frac{|\mathrm{GU}_4(q)|}{|\mathrm{GU}_1(q)||\mathrm{GU}_1(q^3)|} = q^4(q^2 - 1)(q^4 - 1) = b_3,$$

which means that $\rho_3 \leqslant 2\log(q^2 + 1) \cdot a_3^2 b_3^{-1}$.

Now suppose $m = 2$, so p divides $(q+1)/\delta$ with $\delta = (4, q+1)$. Here

$$|H_p| = ((q+1)_p)^3(4!)_p \leqslant 3((q+1)/\delta)^3 = a_5$$

and we note that $H_p < L < G$, where L is a subgroup of type $\mathrm{GU}_1(q) \wr S_4$. If $\nu(x) \geqslant 2$ then

$$|x^G| \geqslant \frac{|\mathrm{GU}_4(q)|}{|\mathrm{GU}_2(q)|^2} = q^4(q^2 - q + 1)(q^2 + 1) = b_5,$$

otherwise $|x^G| = q^3(q-1)(q^2+1) = b_4$ and by counting in L we deduce that H_p contains at most $4(p-1) \leqslant 4((q+1)/\delta - 1) = a_4$ such elements. This implies that

$$\rho_2 \leqslant \log((q+1)/\delta) \cdot (a_4^2 b_4^{-1} + a_5^2 b_5^{-1}).$$

Finally, if $m = 1$ then $|H_p| \leqslant ((q-1)/\gamma)^2 = a_6$ and

$$|x^G| \geqslant \frac{|\mathrm{GU}_4(q)|}{|\mathrm{GL}_2(q^2)|} = q^4(q + 1)(q^3 + 1) = b_6,$$

where $\gamma = (4, q-1)$, and we deduce that $\rho_1 \leqslant \log((q-1)/\gamma) \cdot a_6^2 b_6^{-1}$.

Bringing all of these estimates together, it is straightforward to check that the inequality in (20) holds for all $q \geqslant 5$ with $q \neq 8$. And for $q = 8$ we have $\mathcal{P}_2 = \{3\}$, so we can replace the factor $\log((q+1)/\delta)$ in the upper bound on ρ_2 by 1, and then it is easy to check that the corresponding upper bound on $\widehat{\beta}(G)$ is sufficient. $\qquad\square$

Lemma 5.8. *The conclusion to Theorem 5.1 holds when $G = \mathrm{U}_3(q)$.*

Proof. This is very similar to the proof of Lemma 5.5. Note that $q \geqslant 3$ (since $\mathrm{U}_3(2)$ is soluble) and it suffices to show that

$$\widehat{\beta}(G) < \frac{q^3}{q^3 + 1}. \tag{21}$$

Fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p.

Suppose $p = 2$, so q is odd and $|x^G| = q^2(q^2 - q + 1) = b_1$ for every involution $x \in G$. If $q \equiv 3 \pmod 4$ then $|H_2| = 2((q+1)_2)^2$ and H_2 is contained in a subgroup $L < G$ of type $\mathrm{GU}_1(q) \wr S_3$. By counting in L, we see that there are no more than $3q + 6 = a_1$ such involutions in H_2. On the other hand, if $q \equiv 1 \pmod 4$ then $|H_2| \leqslant 4(q-1) = a_1$. It follows that $\rho_0 \leqslant a_1^2 b_1^{-1}$ for all odd q.

Now assume p is odd, so $p \in \mathcal{P}_m$ with $m \in \{1, 2, 6\}$. Set $\gamma = (4, q-1)$ and $\delta = (4, q+1)$. If $m = 6$ then

$$|H_p| = (q^2 - q + 1)_p \leqslant q^2 - q + 1 = a_2, \quad |x^G| = q^3(q+1)(q^2 - 1) = b_2$$

and thus $\rho_3 \leqslant a_2^2 b_2^{-1} \log a_2$. Similarly, $\rho_1 \leqslant a_3^2 b_3^{-1} \log a_3$, where $a_3 = (q-1)/\gamma$ and $b_3 = q^3(q^3 + 1)$. Finally, suppose $m = 2$ and note that

$$|H_p| = ((q+1)_p)^2 (3!)_p \leqslant 3((q+1)/\delta)^2 = a_5,$$

which means that H_p is contained in a subgroup of type $\mathrm{GU}_1(q) \wr S_3$. If $\nu(x) = 1$ then $|x^G| = q^2(q^2 - q + 1) = b_4$ and there are at most $3((q+1)/\delta - 1) = a_4$ such elements in H_p. Otherwise, $|x^G| \geqslant \frac{1}{3}q^3(q-1)(q^2 - q + 1) = b_5$ and we deduce that

$$\rho_2 \leqslant \log((q+1)/\delta) \cdot (a_4^2 b_4^{-1} + a_5^2 b_5^{-1}).$$

The above bounds imply that (21) holds if $q \geqslant 9$. And for $q \leqslant 8$ we can use MAGMA to show that $\Sigma(G) < 1$ in every case. The result follows. $\qquad\square$

5.3. Symplectic groups.

In this section we prove Theorem 5.1 for the symplectic groups. Recall that we may assume $G = \mathrm{PSp}_n(q)$, where $n \geqslant 4$ is even and $(n, q) \neq (4, 2)$ (the latter assumption is valid since $\mathrm{PSp}_4(2)' \cong \mathrm{L}_2(9)$). As before, we will work closely with the notation defined in (9), (10), (11) and (12).

Our main result is the following (the 4-dimensional symplectic groups will be handled separately in Lemma 5.10).

Lemma 5.9. *The conclusion to Theorem 5.1 holds when $G = \mathrm{PSp}_n(q)$ and $n \geqslant 6$.*

Proof. Write $n = 2\ell$ and set $d = (2, q-1)$. We have

$$|G| = \frac{1}{d} q^{\ell^2} \prod_{i=1}^{\ell} (q^{2i} - 1), \quad |N_G(H_r)| = \frac{1}{d} q^{\ell^2} (q-1)^{\ell}$$

and thus $\Sigma(G) < 1$ if

$$\widehat{\beta}(G) \leqslant \left(1 - q^{-1}\right)^{\ell}. \tag{22}$$

We divide the proof into a number of separate cases.

Case 1. $n \geqslant 10$

To begin with, we assume $n \geqslant 10$. Fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p. For now, let us assume $p = 2$, so q is odd and either $\nu(x)$ is even or $\nu(x) = \ell$. By appealing to Lemma 2.1(i), we compute

$$|H_2| = \frac{1}{2}((q^2 - 1)_2)^\ell (\ell!)_2 \leqslant 2^{n-1}(q+1)^\ell = a_2$$

and thus H_2 is contained in a subgroup L of type $\mathrm{Sp}_2(q) \wr S_\ell$. If $\nu(x) = 2$ then

$$|x^G| = \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_{n-2}(q)||\mathrm{Sp}_2(q)|} = \frac{q^{n-2}(q^n - 1)}{q^2 - 1} = b_1$$

and by counting in L we deduce that there are no more than

$$a_1 = \binom{\ell}{1} + \binom{\ell}{2}|\mathrm{Sp}_2(q)| = \ell + \frac{1}{2}\ell(\ell - 1)q(q^2 - 1)$$

of these involutions in H_2. And if $\nu(x) \geqslant 4$ then

$$|x^G| \geqslant \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_{n-4}(q)||\mathrm{Sp}_4(q)|} > \frac{1}{2}q^{4n-16} = b_2$$

and thus Lemma 2.6 implies that $\rho_0 < a_1^2 b_1^{-1} + a_2^2 b_2^{-1}$.

Now assume p is odd, so $p \in \mathcal{P}_m$ with $m \leqslant n/e$, where $e = 2$ if m is odd, otherwise $e = 1$. Set $k = \lfloor n/me \rfloor$. First assume $m = 4$, in which case p divides $q^2 + 1$ and

$$|x^G| \geqslant \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_{n-4}(q)||\mathrm{GU}_1(q^2)|} > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{4n-8} = b_3.$$

In addition, by appealing to Lemma 2.2 (noting that $p \geqslant 5$), we deduce that

$$|H_p| = ((q^4 - 1)_p)^k (k!)_p \leqslant (q^2 + 1)^k \cdot p^{\frac{k}{4}} \leqslant (q^2 + 1)^{\frac{5}{16}n} = a_3.$$

Now suppose $m \geqslant 3$ and $m \neq 4$. Here $|H_p| = ((q^m - 1)_p)^k (k!)_p$ and

$$|x^G| \geqslant \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_{n-6}(q)||\mathrm{GU}_1(q^3)|} > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{6n-18} = b_4.$$

If m is even, then p divides $q^{m/2} + 1$ and we get

$$|H_p| \leqslant (q^{m/2} + 1)^k \cdot p^{\frac{k}{4}} \leqslant (q^{m/2} + 1)^{\frac{5n}{4m}} \leqslant (q^3 + 1)^{\frac{5}{24}n} = a_4.$$

Similarly, if m is odd then $|H_p| \leqslant (q^m - 1)^{5n/8m} < a_4$.

Since there are at most $n - 3$ possibilities for m in the range $3 \leqslant m \leqslant n$ with $m \neq 4$, and Lemma 2.3 implies that $|\mathcal{P}_m| < \frac{1}{2}n \log q$ for all m, we deduce that

$$\rho_3 < \log(q^2 + 1) \cdot a_3^2 b_3^{-1} + \frac{1}{2}n(n - 3)\log q \cdot a_4^2 b_4^{-1}.$$

Next assume $m = 2$, so p divides $q + 1$ and $|H_p| = ((q + 1)_p)^\ell (\ell!)_p$, which means that H_p is contained in a subgroup L of type $\mathrm{GU}_1(q) \wr S_\ell$. If $\nu(x) = 2$ then

$$|x^G| = \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_{n-2}(q)||\mathrm{GU}_1(q)|} = \frac{q^{n-1}(q^n - 1)}{q + 1} = b_5$$

and by counting in L we see that there are no more than

$$\binom{\ell}{1}(p - 1) \leqslant \frac{1}{2}nq = a_5$$

such elements in H_p. Otherwise, we have $|x^G| > \frac{1}{2}(q + 1)^{-1}q^{4n-9} = b_6$ and we observe that $|H_p| < (q + 1)^{3n/4} = a_6$. This gives $\rho_2 < \log(q + 1) \cdot (a_5^2 b_5^{-1} + a_6^2 b_6^{-1})$.

The case $m = 1$ is very similar. Here $|H_p| = ((q-1)_p)^\ell (\ell!)_p < q^{3n/4} = a_8$ and thus H_p is contained in a subgroup of type $\mathrm{GL}_1(q) \wr S_\ell$. If $\nu(x) = 2$, then

$$|x^G| = \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_{n-2}(q)||\mathrm{GL}_1(q)|} = \frac{q^{n-1}(q^n - 1)}{q - 1} = b_7$$

and there are no more than $a_7 = n(q-2)/2$ of these elements in H_p. On the other hand, if $\nu(x) \geqslant 4$ then $|x^G| > \frac{1}{2} q^{4n-10} = b_8$ and thus $\rho_1 < \log(q-1) \cdot (a_7^2 b_7^{-1} + a_8^2 b_8^{-1})$.

For each $i \in \{0, 1, 2, 3\}$ it is clear that the explicit upper bound $\rho_i < f_i(n, q)$ presented above implies that $\rho_i \to 0$ as n or q tends to infinity. In particular, this means that $\beta(G) \to 0$ as $|G| \to \infty$. In addition, one can check that if $q \geqslant 3$ then the above estimates imply that the inequality in (22) is satisfied unless $(n, q) = (10, 3)$. To handle the latter case we can set $a_2 = |H_2| = 2^{17}$ in the upper bound on ρ_0 and then it is easy to check that the previous bounds are sufficient.

Now assume $q = 2$. Here $\mathcal{P}_1 = \emptyset$, $\mathcal{P}_2 = \{3\}$ and $\mathcal{P}_4 = \{5\}$, which means that

$$\widehat{\beta}(G) < a_3^2 b_3^{-1} + \frac{1}{2} n(n-3) a_4^2 b_4^{-1} + a_5^2 b_5^{-1} + a_6^2 b_6^{-1},$$

where the a_i, b_i terms are defined as above. One checks that this upper bound is sufficient unless $n = 10$, in which case we can use MAGMA to show that $\Sigma(G) < 1$.

Case 2. $n = 8$

Fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p. For $p = 2$ we have $|H_2| \leqslant 2^6 (q+1)^4 = a_2$ and

$$|x^G| \geqslant \frac{|\mathrm{Sp}_8(q)|}{2|\mathrm{Sp}_4(q)|^2} > \frac{1}{4} q^{16} = b_2$$

if $\nu(x) = 4$. So by arguing as in Case 1 we deduce that $\rho_0 < a_1^2 b_1^{-1} + a_2^2 b_2^{-1}$, where $a_1 = 4 + 6q(q^2 - 1)$ and $b_1 = q^6 (q^2 + 1)(q^4 + 1)$.

Now assume $p \geqslant 3$ is odd, so $p \in \mathcal{P}_m$ with $m \in \{1, 2, 3, 4, 6, 8\}$. For $m = 4$ we have $|H_p| \leqslant (q^2 + 1)^2 = a_3$ and $|x^G| > \frac{1}{2}(q+1)^{-1} q^{25} = b_3$. Similarly, if $m \in \{3, 6, 8\}$ then $|H_p| \leqslant q^4 + 1 = a_4$ and $|x^G| > \frac{1}{2}(q+1)^{-1} q^{31} = b_4$, which allows us to conclude that

$$\rho_3 < \log(q^2 + 1) \cdot a_3^2 b_3^{-1} + 3 \log(q^4 + 1) \cdot a_4^2 b_4^{-1}.$$

Next suppose $m = 2$, in which case $|H_p| = ((q+1)_p)^4 (4!)_p \leqslant 3(q+1)^4 = a_6$. If $\nu(x) = 2$ then $|x^G| = q^7 (q^8 - 1)/(q+1) = b_5$ and by arguing as in Case 1 we deduce that there are at most $a_5 = 4q$ such elements in H_p. And if $\nu(x) > 2$, then

$$|x^G| \geqslant \frac{|\mathrm{Sp}_8(q)|}{|\mathrm{GU}_4(q)|} > \frac{1}{2} \left(\frac{q}{q+1} \right) q^{20} = b_6$$

and thus $\rho_2 < \log(q+1) \cdot (a_5^2 b_5^{-1} + a_6^2 b_6^{-1})$. Similarly, $\rho_1 < \log(q-1) \cdot (a_7^2 b_7^{-1} + a_8^2 b_8^{-1})$, where

$$a_7 = 4(q-2), \ a_8 = 3(q-1)^4, \ b_7 = \frac{q^7(q^8 - 1)}{q - 1}, \ b_8 = \frac{1}{2} q^{20}.$$

Putting these estimates together, it is clear that $\beta(G) \to 0$ as $q \to \infty$. Furthermore, we deduce that (22) holds (with $\ell = 4$) if $q \geqslant 4$. Finally, for $q \in \{2, 3\}$ we can use MAGMA to check that $\Sigma(G) < 1$.

Case 3. $n = 6$

This is very similar to the previous case. As usual, fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p.

First assume $p = 2$ and note that $|H_2| \leqslant 2^3 (q+1)^3 = a_2$. If $\nu(x) = 3$ then

$$|x^G| \geqslant \frac{|\mathrm{Sp}_6(q)|}{2|\mathrm{GU}_3(q)|} > \frac{1}{4} \left(\frac{q}{q+1} \right) q^{12} = b_2,$$

otherwise $|x^G| = q^4(q^4 + q^2 + 1) = b_1$ and as in Case 1 we see that there are at most $a_1 = 3 + 3q(q^2 - 1)$ involutions $x \in H_2$ with $\nu(x) = 2$. Therefore, $\rho_0 < a_1^2 b_1^{-1} + a_2^2 b_2^{-1}$.

Now assume $p \geqslant 3$ is odd, so $p \in \mathcal{P}_m$ with $m \in \{1, 2, 3, 4, 6\}$. If $m = 4$ then $|H_p| \leqslant q^2 + 1 = a_3$ and $|x^G| > \frac{1}{2}(q+1)^{-1}q^{17} = b_3$. Similarly, if $m \in \{3, 6\}$ then $|H_p| \leqslant q^2 + q + 1 = a_4$ and $|x^G| > \frac{1}{2}(q+1)^{-1}q^{19} = b_4$, which allows us to conclude that

$$\rho_3 < \log(q^2 + 1) \cdot a_3^2 b_3^{-1} + 2\log(q^2 + q + 1) \cdot a_4^2 b_4^{-1}.$$

Next suppose $m = 2$, in which case $|H_p| = ((q+1)_p)^3 (3!)_p \leqslant 3(q+1)^3 = a_6$. If $\nu(x) = 2$ then

$$|x^G| = \frac{|\mathrm{Sp}_6(q)|}{|\mathrm{Sp}_4(q)||\mathrm{GU}_1(q)|} = \frac{q^5(q^6 - 1)}{q + 1} = b_5$$

and by arguing as in Case 1 we deduce that there are at most $a_5 = 3q$ such elements in H_p. Otherwise, we have $|x^G| > \frac{1}{2}(q+1)^{-1}q^{13} = b_6$ and we conclude that

$$\rho_2 < \log(q+1) \cdot (a_5^2 b_5^{-1} + a_6^2 b_6^{-1}).$$

Similarly, $\rho_1 < \log(q-1) \cdot (a_7^2 b_7^{-1} + a_8^2 b_8^{-1})$, where

$$a_7 = 3(q-2), \ a_8 = 3(q-1)^3, \ b_7 = \frac{q^5(q^6 - 1)}{q - 1}, \ b_8 = \frac{1}{2}q^{12}.$$

It is clear that each upper bound $\rho_i < f_i(q)$ given above has the property that $f_i(q) \to 0$ as $q \to \infty$, whence G satisfies the asymptotic statement in Theorem 5.1. In addition, one checks that the given estimates imply that $\Sigma(G) < 1$ if $q \geqslant 4$. Finally, for $q \in \{2, 3\}$ we can use MAGMA to show that $\Sigma(G) < 1$. $\qquad\square$

Lemma 5.10. *The conclusion to Theorem 5.1 holds when $G = \mathrm{PSp}_4(q)$.*

Proof. We may assume $q \geqslant 4$ since $\mathrm{PSp}_4(2)' \cong \mathrm{L}_2(9)$ and $\mathrm{PSp}_4(3) \cong \mathrm{U}_4(2)$. Note that we have $\Sigma(G) < 1$ if

$$\widehat{\beta}(G) < \frac{q^4}{(q+1)^2(q^2+1)}. \tag{23}$$

Fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p.

Suppose $p = 2$, so q is odd and G has two conjugacy classes of involutions; in the notation of [22, Table 4.5.1], x is either a type t_1 involution, or x is of type t_2 (if $q \equiv 1 \pmod 4$) or t_2' (if $q \equiv 3 \pmod 4$). If x is a t_1 involution, then

$$|x^G| = \frac{|\mathrm{Sp}_4(q)|}{2|\mathrm{Sp}_2(q)|^2} = \frac{1}{2}q^2(q^2 + 1) = b_1$$

and the proof of [16, Proposition 3.6] shows that there are at most $a_1 = q+2$ such involutions in H_2. On the other hand, if x is a t_2 or t_2' involution then

$$|x^G| \geqslant \frac{|\mathrm{Sp}_4(q)|}{2|\mathrm{GU}_2(q)|} = \frac{1}{2}q^3(q-1)(q^2 + 1) = b_2$$

and we note that $|H_2| \leqslant 4(q+1)^2 = a_2$. This implies that $\rho_0 \leqslant a_1^2 b_1^{-1} + a_2^2 b_2^{-1}$.

For the remainder, we may assume p is odd, in which case $p \in \mathcal{P}_m$ with $m \in \{1, 2, 4\}$. If $m = 4$ then p divides $q^2 + 1$ and we have $|H_p| \leqslant q^2 + 1 = a_3$ and

$$|x^G| = \frac{|\mathrm{Sp}_4(q)|}{|\mathrm{GU}_1(q^2)|} = q^4(q^2 - 1)^2 = b_3,$$

whence $\rho_3 \leqslant \log(q^2 + 1) \cdot a_3^2 b_3^{-1}$. Similarly, if $m = 2$ then we have $|H_p| \leqslant (q+1)^2 = a_4$ and $|x^G| \geqslant q^3(q-1)(q^2 + 1) = b_4$, while for $m = 1$ we see that $|H_p| \leqslant (q-1)^2 = a_5$ and $|x^G| \geqslant q^3(q+1)(q^2 + 1) = b_5$. Therefore,

$$\rho_2 \leqslant \log(q+1) \cdot a_4^2 b_4^{-1}, \ \ \rho_1 \leqslant \log(q-1) \cdot a_5^2 b_5^{-1}.$$

Bringing these estimates together, it is clear that $\beta(G) \to 0$ as $q \to \infty$. In addition, we deduce that the inequality in (23) holds if $q \geqslant 9$. Finally, for $q \in \{4, 5, 7, 8\}$ we can use MAGMA to verify the bound $\Sigma(G) < 1$. $\qquad\square$

5.4. **Orthogonal groups.** To complete the proof of Theorem 5.1, we may assume G is an orthogonal group. As before, we continue to work with the notation defined in (9), (10), (11) and (12).

We begin by handling the odd-dimensional groups of the form $G = \Omega_n(q)$, where $n \geqslant 7$ is odd and q is odd.

Lemma 5.11. *The conclusion to Theorem 5.1 holds when $G = \Omega_n(q)$ and $n \geqslant 7$.*

Proof. Write $n = 2\ell + 1$ and note that q is odd. It is easy to check that $\Sigma(G) < 1$ if (22) holds, so our main aim is to verify the bound in (22). Fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p.

Suppose $p = 2$ and write $q \equiv \varepsilon \pmod 4$ with $\varepsilon = \pm 1$. Then

$$|H_2| = 2^{\ell-1}((q-\varepsilon)_2)^\ell (\ell!)_2 \leqslant 2^{2\ell-1}(q+1)^\ell = a_3$$

and we note that $H_2 < L < G$, where L is of type $(O_2^\varepsilon(q) \wr S_\ell) \perp O_1(q)$. If $\nu(x) = 1$ then

$$|x^G| \geqslant \frac{|\mathrm{SO}_n(q)|}{2|\mathrm{SO}_{n-1}^-(q)|} = \frac{1}{2}q^\ell(q^\ell - 1) = b_1$$

and by counting in L we deduce that there are at most

$$1 + \binom{\ell}{1}(q - \varepsilon) \leqslant 1 + \ell(q+1) = a_1$$

such involutions in H_2. Similarly, if $\nu(x) = 2$ then

$$|x^G| \geqslant \frac{|\mathrm{SO}_n(q)|}{2|\mathrm{SO}_{n-2}(q)||\mathrm{SO}_2^-(q)|} = \frac{q^{n-2}(q^{n-1} - 1)}{2(q+1)} = b_2$$

and we see that H_2 contains no more than

$$\binom{\ell}{1}(1 + q - \varepsilon) + \binom{\ell}{2}(|O_2^\varepsilon(q)| + (q - \varepsilon)^2) \leqslant \ell(q+2) + \frac{1}{2}\ell(\ell-1)(q+1)(q+3) = a_2$$

such elements. Finally, if $\nu(x) \geqslant 3$ then

$$|x^G| \geqslant \frac{|\mathrm{SO}_n(q)|}{2|\mathrm{SO}_{n-3}^-(q)||\mathrm{SO}_3(q)|} = \frac{q^{\frac{1}{2}(3n-9)}(q^{\frac{1}{2}(n-3)} - 1)(q^{n-1} - 1)}{2(q^2 - 1)} = b_3$$

and we conclude that

$$\rho_0 \leqslant a_1^2 b_1^{-1} + a_2^2 b_2^{-1} + a_3^2 b_3^{-1}.$$

Now assume p is odd and write $p \in \mathcal{P}_m$. Note that $m \leqslant (n-1)/e$, where $e = 2$ if m is odd, otherwise $e = 1$. Set $k = \lfloor (n-1)/me \rfloor$. If $m = 4$ then p divides $(q^2 + 1)/2$ and we have

$$|H_p| = ((q^4 - 1)_p)^k (k!)_p \leqslant ((q^2 + 1)/2)^{\frac{5}{16}(n-1)} = a_4$$

and

$$|x^G| \geqslant \frac{|\mathrm{SO}_n(q)|}{|\mathrm{SO}_{n-4}(q)||\mathrm{GU}_1(q^2)|} > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{4n-12} = b_4.$$

Similarly, if $m \geqslant 3$ and $m \neq 4$, then $|\mathcal{P}_m| < \frac{1}{2}(n-1)\log q$ (see Lemma 2.3) and we compute

$$|H_p| = ((q^m - 1)_p)^k (k!)_p \leqslant ((q^3 + 1)/2)^{\frac{5}{24}(n-1)} = a_5$$

and

$$|x^G| \geqslant \frac{|\mathrm{SO}_n(q)|}{|\mathrm{SO}_{n-6}(q)||\mathrm{GU}_1(q^3)|} > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{6n-24} = b_5.$$

This implies that

$$\rho_3 < \log(q^2 + 1) \cdot a_4^2 b_4^{-1} + \frac{1}{2}(n-1)(n-3) \log q \cdot a_5^2 b_5^{-1}.$$

Now assume $m = 2$, so p divides $(q+1)/2$ and we have $k = \ell$. Here

$$|H_p| = ((q+1)_p)^\ell (\ell!)_p \leqslant ((q+1)/2)^{3\ell/2} = a_7$$

and we see that $H_p < L < G$, where L is a subgroup of type $(\mathrm{O}_2^-(q) \wr S_\ell) \perp \mathrm{O}_1(q)$. If $\nu(x) = 2$ then

$$|x^G| = \frac{|\mathrm{SO}_n(q)|}{|\mathrm{SO}_{n-2}(q)||\mathrm{GU}_1(q)|} = \frac{q^{n-2}(q^{n-1}-1)}{q+1} = b_6$$

and by counting in L we deduce that there are at most $a_6 = \ell q$ such elements in H_p. On the other hand, if $\nu(x) > 2$ then

$$|x^G| \geqslant \frac{|\mathrm{SO}_n(q)|}{|\mathrm{SO}_{n-4}(q)||\mathrm{GU}_2(q)|} > \frac{1}{2}\left(\frac{q}{q+1}\right) q^{4n-14} = b_7$$

and it follows that

$$\rho_2 < \log((q+1)/2) \cdot (a_6^2 b_6^{-1} + a_7^2 b_7^{-1}).$$

Similarly, we have $\rho_1 < \log((q-1)/2) \cdot (a_8^2 b_8^{-1} + a_9^2 b_9^{-1})$ with

$$a_8 = \ell(q-2), \ a_9 = ((q-1)/2)^{3\ell/2}, \ b_8 = \frac{q^{n-2}(q^{n-1}-1)}{q-1}, \ b_9 = \frac{1}{2}q^{4n-14}.$$

It is clear to see that the above estimates imply that $\beta(G) \to 0$ as $|G| \to \infty$. We also deduce that the inequality in (22) holds if $q \geqslant 5$, or if $q = 3$ and $n \geqslant 21$. If $q = 3$ and $11 \leqslant n \leqslant 19$ then by setting $a_3 = |H_2|$ it is easy to check that the above bounds are sufficient. Finally, for $(n, q) = (9, 3), (7, 3)$ we can use MAGMA to verify the bound $\Sigma(G) < 1$. $\qquad\square$

Lemma 5.12. *The conclusion to Theorem 5.1 holds when $G = \mathrm{P}\Omega_n^+(q)$ and $n \geqslant 10$.*

Proof. Write $n = 2\ell$ and set $d = (4, q^\ell - 1)$. Since $|N_G(H_r)| = \frac{1}{d}q^{\ell(\ell-1)}(q-1)^\ell$, it follows that $\Sigma(G) < 1$ if (22) holds. Fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p.

Suppose $p = 2$, so q is odd and either $\nu(x)$ is even or $\nu(x) = \ell$. Note that if $\nu(x) = 2$ then

$$|x^G| \geqslant \frac{|\mathrm{SO}_n^+(q)|}{2|\mathrm{SO}_{n-2}^-(q)||\mathrm{SO}_2^-(q)|} = \frac{q^{n-2}(q^{(n-2)/2}-1)(q^{n/2}-1)}{2(q+1)} = b_1,$$

otherwise we have

$$|x^G| \geqslant \frac{|\mathrm{SO}_n^+(q)|}{2|\mathrm{SO}_{n-4}^-(q)||\mathrm{SO}_4^-(q)|} > \frac{1}{4}q^{4n-16} = b_2$$

if $n \geqslant 14$, and

$$|x^G| \geqslant \frac{|\mathrm{SO}_n^+(q)|}{2|\mathrm{GU}_{n/2}(q)|} > \frac{1}{4}\left(\frac{q}{q+1}\right) q^{\frac{1}{4}(n^2-2n)} = b_2$$

if $n \in \{10, 12\}$.

First assume $q \equiv 1 \pmod 4$. Then by applying Lemma 2.1(i), we compute

$$|H_2| = \frac{1}{4}2^{\ell-1}((q-1)_2)^\ell(\ell!)_2 \leqslant 2^{n-3}(q-1)^\ell = a_2$$

and $H_2 < L < G$ with L of type $\mathrm{O}_2^+(q) \wr S_\ell$. By counting in L we deduce that there are at most

$$a_1 = \ell + \binom{\ell}{2}\left((q-1)^2 + 2(q-1)\right)$$

involutions $x \in H_2$ with $\nu(x) = 2$.

Now assume $q \equiv 3 \pmod 4$. If ℓ is even then

$$|H_2| = \frac{1}{4}2^{\ell-1}((q+1)_2)^\ell(\ell!)_2 \leqslant 2^{n-3}(q+1)^\ell = a_2$$

and $H_2 < L < G$ with L of type $O_2^-(q) \wr S_\ell$. And by working in L we calculate that H_2 contains no more than

$$a_1 = \ell + \binom{\ell}{2}\left((q+1)^2 + 2(q+1)\right)$$

involutions with $\nu(x) = 2$. Similarly, if ℓ is odd then

$$|H_2| = \frac{1}{2}2^{\ell-1}((q+1)_2)^{\ell-1}((\ell-1)!)_2.2 \leqslant 2^{n-2}(q+1)^{\ell-1} = a_2$$

and H_2 is contained in a subgroup L of type $(O_2^-(q) \wr S_{\ell-1}) \perp O_2^+(q)$. By counting in L, we calculate that the number of involutions $x \in H_2$ with $\nu(x) = 2$ is at most

$$a_1 = 1 + (\ell-1)((q^2-1)+1) + \binom{\ell-1}{2}\left((q+1)^2 + 2(q+1)\right).$$

So for all odd q we deduce that $\rho_0 < a_1^2 b_1^{-1} + a_2^2 b_2^{-1}$, where the precise expressions for a_1 and a_2 depend on the congruence classes of n and q modulo 4, as defined above.

Now assume $p \geqslant 3$ is odd, so $p \in \mathcal{P}_m$ for some $m \leqslant n-2$. Set $k = \lfloor (n-2)/me \rfloor$, where $e = 2$ if m is odd, otherwise $e = 1$. If $m = 4$ then p divides $q^2 + 1$ and we have

$$|x^G| \geqslant \frac{|\mathrm{SO}_n^+(q)|}{|\mathrm{SO}_{n-4}^-(q)||\mathrm{GU}_1(q^2)|} > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{4n-12} = b_3.$$

In addition, since $p \geqslant 5$ and $(q^{n/2} - 1)_p \leqslant \frac{1}{8}n(q^2+1)$ by Lemma 2.1, we compute

$$|H_p| = ((q^4-1)_p)^k (k!)_p \cdot (q^{n/2} - 1)_p \leqslant (q^2+1)^{\frac{5}{16}(n-2)} \cdot \frac{1}{8}n(q^2+1)$$

$$= \frac{1}{8}n(q^2+1)^{\frac{1}{16}(5n+6)} = a_3.$$

Similarly, if $m \geqslant 3$ and $m \neq 4$, then

$$|x^G| \geqslant \frac{|\mathrm{SO}_n^+(q)|}{|\mathrm{SO}_{n-6}^-(q)||\mathrm{GU}_1(q^3)|} > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{6n-24} = b_4$$

and

$$|H_p| = ((q^m-1)_p)^k (k!)_p \cdot (q^{n/2} - 1)_p.$$

If $m \geqslant 6$ is even, then p divides $q^{m/2} + 1$ and thus

$$|H_p| < (q^{m/2}+1)^{\frac{5(n-2)}{4m}} \cdot q^{\frac{1}{2}n} \leqslant (q^3+1)^{\frac{5}{24}(n-2)} \cdot q^{\frac{1}{2}n} = a_4,$$

while we get

$$|H_p| < q^{\frac{5}{4}mk+\frac{1}{2}n} = q^{\frac{5}{8}(n-2)+\frac{1}{2}n} < a_4$$

if $m \geqslant 3$ is odd. This allows us to conclude that

$$\rho_3 < \log(q^2+1) \cdot a_3^2 b_3^{-1} + \frac{1}{2}n(n-5)\log q \cdot a_4^2 b_4^{-1}.$$

Next assume $m = 2$, so p divides $q + 1$. First observe that if ℓ is even then

$$|H_p| = ((q+1)_p)^\ell (\ell!)_p \leqslant (q+1)^{\frac{3}{4}n} = a_6$$

and $H_p < L < G$ with L of type $O_2^-(q) \wr S_\ell$. Similarly, if ℓ is odd then

$$|H_p| = ((q+1)_p)^{\ell-1}((\ell-1)!)_p < a_6$$

and H_p is contained in a subgroup L of type $(O_2^-(q) \wr S_{\ell-1}) \perp O_2^+(q)$. If $\nu(x) = 2$ then

$$|x^G| = \frac{|\mathrm{SO}_n^+(q)|}{|\mathrm{SO}_{n-2}^-(q)||\mathrm{GU}_1(q)|} = \frac{q^{n-2}(q^{(n-2)/2}-1)(q^{n/2}-1)}{q+1} = b_5,$$

otherwise we have

$$|x^G| \geqslant \frac{|\mathrm{SO}_n^+(q)|}{|\mathrm{SO}_{n-4}^+(q)||\mathrm{GU}_2(q)|} > \frac{1}{2}\left(\frac{q}{q+1}\right)q^{4n-14} = b_6.$$

And by counting in L, we deduce that there are at most $a_5 = \ell q$ elements $x \in H_p$ of order p with $\nu(x) = 2$. It follows that $\rho_2 < \log(q+1) \cdot (a_5^2 b_5^{-1} + a_6^2 b_6^{-1})$.

Finally, suppose $m = 1$. Here

$$|H_p| = ((q-1)_p)^\ell (\ell!)_p \leqslant (q-1)^{\frac{3}{4}n} = a_8$$

and $H_p < L < G$ with L of type $\mathrm{O}_2^+(q) \wr S_\ell$. If $\nu(x) = 2$ then

$$|x^G| = \frac{|\mathrm{SO}_n^+(q)|}{|\mathrm{SO}_{n-2}^+(q)||\mathrm{GL}_1(q)|} = \frac{q^{n-2}(q^{(n-2)/2}+1)(q^{n/2}-1)}{q-1} = b_7$$

and by working in L we see that there are no more than $a_7 = \ell(q-2)$ of these elements in H_p. And for $\nu(x) > 2$ we have $|x^G| > \frac{1}{2}q^{4n-14} = b_8$, so $\rho_1 < \log(q-1) \cdot (a_7^2 b_7^{-1} + a_8^2 b_8^{-1})$.

It is easy to see that each of the above bounds $\rho_i < f_i(n,q)$ has the property that $f_i(n,q) \to 0$ as n or q tends to infinity. In particular, this implies that $\beta(G) \to 0$ as $|G| \to \infty$. In addition, the above estimates imply that $\Sigma(G) < 1$ unless (n,q) is one of the following:

$$(10,2), \ (10,3), \ (12,2), \ (12,3), \ (14,2).$$

For $(n,q) = (10,2)$ we can use MAGMA to compute

$$\Sigma(G) = \frac{11219267305357}{11749647974400} < 1$$

as required. And in each of the remaining cases, we can slightly modify our previous estimates in order to obtain the desired conclusion. For example, suppose $(n,q) = (10,3)$. Here we compute $i_2(H_2) = 2063$ and $\pi'(G) = \{5,7,11,13,41\}$, so we can set $a_2 = 2063$ in the upper bound on ρ_0, and we can also replace the term $\frac{1}{2}n(n-5)\log q$ in the upper bound on ρ_3 by 4. One can then check that the revised estimates imply that $\Sigma(G) < 1$. $\square$

Lemma 5.13. *The conclusion to Theorem 5.1 holds when $G = \mathrm{P}\Omega_8^+(q)$.*

Proof. As in the proof of the previous lemma, we observe that $\Sigma(G) < 1$ if the inequality in (22) holds (with $\ell = 4$). For $q = 3$, we can directly verify the bound $\Sigma(G) < 1$ with the aid of MAGMA. However, for $q = 2$ we get

$$\Sigma(G) = \frac{6518753}{6220800} > 1.$$

To resolve the latter case, we use MAGMA to compute

$$Q_p(G) = 1 - \frac{s|H_p|}{|G:H_p|}$$

for each $p \in \pi(G) = \{2,3,5,7\}$, where s is the number of (H_p, H_p) double cosets in G of size $|H_p|^2$. In this way, we obtain

$$Q_2(G) = \frac{38429}{42525}, \ Q_3(G) = \frac{4307}{89600}, \ Q_5(G) = \frac{31}{435456}, \ Q_7(G) = \frac{1}{4147200}$$

and thus $\alpha(G) < 1$ as required.

For the remainder, we may assume $q \geqslant 4$. As usual, fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p.

If $p = 2$ then $|H_2| \leqslant 16(q+1)^4 = a_1$ and

$$|x^G| \geqslant \frac{|\mathrm{SO}_8^+(q)|}{2|\mathrm{GU}_4(q)|} = \frac{1}{2}q^6(q-1)(q^2+1)(q^3-1) = b_1,$$

so we have $\rho_0 \leqslant a_1^2 b_1^{-1}$.

Now assume p is odd, so $p \in \mathcal{P}_m$ with $m \in \{1,2,3,4,6\}$. If $m \in \{3,4,6\}$ then we have $|H_p| \leqslant (q^2+1)^2 = a_2$ and

$$|x^G| \geqslant \frac{|\mathrm{SO}_8^+(q)|}{|\mathrm{GU}_2(q^2)|} = q^{10}(q^2-1)^2(q^6-1) = b_2,$$

which gives $\rho_3 \leqslant 3 \log(q^2 + q + 1) \cdot a_2^2 b_2^{-1}$. Similarly, if $m = 2$ then $|H_p| \leqslant 3(q+1)^4 = a_3$ and

$$|x^G| \geqslant \frac{|\mathrm{SO}_8^+(q)|}{|\mathrm{GU}_4(q)|} = q^6(q-1)(q^2+1)(q^3-1) = b_3,$$

whereas $|H_p| \leqslant 3(q-1)^4 = a_4$ and

$$|x^G| \geqslant \frac{|\mathrm{SO}_8^+(q)|}{|\mathrm{GL}_4(q)|} = q^6(q+1)(q^2+1)(q^3+1) = b_4$$

if $m = 1$. It follows that

$$\rho_2 \leqslant \log(q+1) \cdot a_3^2 b_3^{-1}, \quad \rho_1 \leqslant \log(q-1) \cdot a_4^2 b_4^{-1}.$$

It is clear from the above estimates that $\beta(G) \to 0$ as $q \to \infty$. Furthermore, we deduce that (22) holds (with $\ell = 4$) if $q \geqslant 8$, so it just remains to handle the groups with $q \in \{4, 5, 7\}$.

If $q = 7$ then using MAGMA we compute $i_2(H_2) = 2831$ and by setting $a_1 = 2831$ in the previous estimate for ρ_0 it is easy to check (22) holds. And similarly if $q = 5$, noting that $i_2(H_2) = 495$. Finally, suppose $q = 4$. Here $\pi'(G) = \{3, 5, 7, 13, 17\}$ with $\mathcal{P}_1 = \{3\}$ and $\mathcal{P}_2 = \{5\}$, so by defining a_i, b_i as above for $i \in \{2, 3, 4\}$ we get

$$\widehat{\beta}(G) \leqslant 3a_2^2 b_2^{-1} + a_3^2 b_3^{-1} + a_4^2 b_4^{-1} < \left(\frac{3}{4}\right)^4$$

and the result follows.   □

Lemma 5.14. *The conclusion to Theorem 5.1 holds when $G = \mathrm{P\Omega}_n^-(q)$ and $n \geqslant 8$.*

Proof. Write $n = 2\ell$, $d = (4, q^\ell + 1)$ and note that $|N_G(H_r) : H_r| = \frac{1}{d}(q^2 - 1)(q - 1)^{\ell-2}$, which means that $\Sigma(G) < 1$ if the bound in (22) is satisfied. Fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p. To begin with, we will assume $n \geqslant 10$.

Case 1. $n \geqslant 10$

First assume $p = 2$. If $\nu(x) = 2$ then

$$|x^G| \geqslant \frac{|\mathrm{SO}_n^-(q)|}{2|\mathrm{SO}_{n-2}^+(q)||\mathrm{SO}_2^-(q)|} = \frac{q^{n-2}(q^{(n-2)/2}+1)(q^{n/2}+1)}{2(q+1)} = b_1,$$

otherwise $|x^G| > b_2$, where $b_2 = \frac{1}{4}q^{4n-16}$ if $n \geqslant 14$ and $b_2 = \frac{1}{4}(q+1)^{-1}q^c$ if $n \in \{10, 12\}$, with $c = 21$ if $n = 10$ and $c = 31$ if $n = 12$.

Suppose $q \equiv 1 \pmod{4}$. Then

$$|H_2| = \frac{1}{2}2^{\ell-1}((q-1)_2)^{\ell-1}((\ell-1)!)_2.2 \leqslant 2^{n-2}(q-1)^{\ell-1} = a_2$$

and we observe that H_2 is contained in a subgroup $L < G$ of type $(\mathrm{O}_2^+(q) \wr S_{\ell-1}) \perp \mathrm{O}_2^-(q)$. By counting in L we see that there are no more than

$$a_1 = 1 + \binom{\ell-1}{1}\left(1 + (q^2-1)\right) + \binom{\ell-1}{2}\left((q-1)^2 + 2(q-1)\right)$$

involutions $x \in H_2$ with $\nu(x) = 2$.

Now assume $q \equiv 3 \pmod{4}$. If ℓ is even, then

$$|H_2| = \frac{1}{2}2^{\ell-1}((q+1)_2)^{\ell-1}((\ell-1)!)_2.2 \leqslant 2^{n-2}(q+1)^{\ell-1} = a_2$$

and thus $H_2 < L < G$ with L of type $(\mathrm{O}_2^-(q) \wr S_{\ell-1}) \perp \mathrm{O}_2^+(q)$. By working in L we deduce that H_2 contains at most

$$a_1 = 1 + \binom{\ell-1}{1}\left(1 + (q^2-1)\right) + \binom{\ell-1}{2}\left((q+1)^2 + 2(q+1)\right)$$

involutions x with $\nu(x) = 2$. Similarly, if ℓ is odd then

$$|H_2| = \frac{1}{4} 2^{\ell-1} ((q+1)_2)^\ell (\ell!)_2 \leqslant 2^{n-3} (q+1)^\ell = a_2$$

and H_2 is contained in a subgroup L of type $O_2^-(q) \wr S_\ell$, which allows us to see that the number of involutions $x \in H_2$ with $\nu(x) = 2$ is at most

$$a_1 = \binom{\ell}{1} + \binom{\ell}{2} \left((q+1)^2 + 2(q+1) \right).$$

So for all odd q, we conclude that $\rho_0 < a_1^2 b_1^{-1} + a_2^2 b_2^{-1}$, where the expressions for a_1 and a_2 depend on the congruence classes of n and q modulo 4, as defined above.

Now assume $p \geqslant 3$ is odd, so $p \in \mathcal{P}_m$ for some $m \leqslant n$. Set $k = \lfloor (n-2)/me \rfloor$, where $e = 2$ if m is odd, otherwise $e = 1$. If $m = 4$ then p divides $q^2 + 1$ and

$$|x^G| \geqslant \frac{|\mathrm{SO}_n^-(q)|}{|\mathrm{SO}_{n-4}^+(q)||\mathrm{GU}_1(q^2)|} > \frac{1}{2} \left(\frac{q}{q+1} \right) q^{4n-12} = b_3.$$

Since $p \geqslant 5$ and $(q^{n/2} + 1)_p \leqslant \frac{1}{4} n(q^2 + 1)$ (see Lemma 2.1), we compute

$$|H_p| = ((q^4 - 1)_p)^k (k!)_p \cdot (q^{n/2} + 1)_p \leqslant \frac{1}{4} n(q^2 + 1)^{\frac{1}{16}(5n+6)} = a_3.$$

Similarly, if $m \geqslant 3$ and $m \neq 4$, then $|x^G| > \frac{1}{2}(q+1)^{-1} q^{6n-23} = b_4$ and

$$|H_p| = ((q^m - 1)_p)^k (k!)_p \cdot (q^{n/2} + 1)_p \leqslant (q^3 + 1)^{\frac{1}{24}(9n-10)} = a_4.$$

This implies that

$$\rho_3 < \log(q^2 + 1) \cdot a_3^2 b_3^{-1} + \frac{1}{2} n(n-4) \log q \cdot a_4^2 b_4^{-1}.$$

Next suppose $m = 2$. If ℓ is odd then

$$|H_p| = ((q+1)_p)^\ell (\ell!)_p \leqslant (q+1)^{\frac{3}{4}n} = a_6$$

and $H_p < L < G$ with L of type $O_2^-(q) \wr S_\ell$. On the other hand, if ℓ is even, then

$$|H_p| = ((q+1)_p)^{\ell-1} ((\ell-1)!)_p < a_6$$

and H_p is contained in a subgroup L of type $(O_2^-(q) \wr S_{\ell-1}) \perp O_2^+(q)$. If $\nu(x) = 2$ then

$$|x^G| = \frac{|\mathrm{SO}_n^-(q)|}{|\mathrm{SO}_{n-2}^+(q)||\mathrm{GU}_1(q)|} = \frac{q^{n-2}(q^{(n-2)/2} + 1)(q^{n/2} + 1)}{q+1} = b_5,$$

otherwise we have $|x^G| > \frac{1}{2}(q+1)^{-1} q^{4n-13} = b_6$. By counting in L, we calculate that there are at most $a_5 = \ell q$ elements $x \in H_p$ of order p with $\nu(x) = 2$ and it follows that

$$\rho_2 < \log(q+1) \cdot (a_5^2 b_5^{-1} + a_6^2 b_6^{-1}).$$

Finally, suppose $m = 1$. Here

$$|H_p| = ((q-1)_p)^{\ell-1} ((\ell-1)!)_p \leqslant (q-1)^{\frac{3}{4}(n-2)} = a_8$$

and $H_p < L < G$ with L of type $(O_2^+(q) \wr S_{\ell-1}) \perp O_2^-(q)$. If $\nu(x) = 2$ then

$$|x^G| = \frac{|\mathrm{SO}_n^-(q)|}{|\mathrm{SO}_{n-2}^-(q)||\mathrm{GL}_1(q)|} = \frac{q^{n-2}(q^{(n-2)/2} - 1)(q^{n/2} + 1)}{q-1} = b_7,$$

and by working in L we see that there are no more than $a_7 = (\ell-1)(q-1)$ of these elements in H_p. Otherwise $|x^G| > \frac{1}{2} q^{4n-14} = b_8$ and we conclude that

$$\rho_1 < \log(q-1) \cdot (a_7^2 b_7^{-1} + a_8^2 b_8^{-1}).$$

The above estimates $\rho_i < f_i(n, q)$ immediately imply that $\beta(G) \to 0$ as $|G| \to \infty$. Moreover, we deduce that $\Sigma(G) < 1$ unless (n, q) is one of the following:

$$(10, 2), \ (10, 3), \ (12, 2), \ (12, 3), \ (14, 2).$$

For $(n, q) = (10, 2)$ we can use MAGMA to verify the bound $\Sigma(G) < 1$, and in the remaining cases we can modify our previous estimates. For example, suppose $(n, q) = (12, 2)$. Here $|\pi'(G)| = 7$, $|H_3| = 3^6$ and we see that $\mathcal{P}_1 = \emptyset$, $\mathcal{P}_2 = \{3\}$, $\mathcal{P}_4 = \{5\}$. Therefore,

$$\widehat{\beta}(G) < a_3^2 b_3^{-1} + 5a_4^2 b_4^{-1} + a_5^2 b_5^{-1} + a_6^2 b_6^{-1} < 2^{-6},$$

where $a_6 = 3^6$ and the remaining a_i, b_i are defined as above.

Case 2. $n = 8$

To complete the proof, we may assume $n = 8$. We can use MAGMA to show that $\Sigma(G) < 1$ when $q = 2, 3$, so we may assume $q \geqslant 4$. Fix a prime $p \in \pi'(G)$ and let $x \in G$ be an element of order p.

If $p = 2$ then $|H_2| \leqslant 16(q + 1)^3 = a_1$ and

$$|x^G| \geqslant \frac{|\mathrm{SO}_8^-(q)|}{2|\mathrm{SO}_6^+(q)||\mathrm{SO}_2^-(q)|} = \frac{1}{2}q^6(q^2 - q + 1)(q^4 + 1) = b_1,$$

so we have $\rho_0 \leqslant a_1^2 b_1^{-1}$.

Now assume p is odd, so $p \in \mathcal{P}_m$ with $m \in \{1, 2, 3, 4, 6, 8\}$. If $m \geqslant 3$ then $|H_p| \leqslant q^4 + 1 = a_2$ and

$$|x^G| \geqslant \frac{|\mathrm{SO}_8^-(q)|}{|\mathrm{SO}_4^+(q)||\mathrm{GU}_1(q^2)|} = q^{10}(q^4 + 1)(q^6 - 1) = b_2,$$

which gives $\rho_3 \leqslant 4\log(q^4 + 1) \cdot a_2^2 b_2^{-1}$. For $m = 2$ we observe that $|H_p| \leqslant 3(q + 1)^3 = a_3$ and

$$|x^G| \geqslant \frac{|\mathrm{SO}_8^-(q)|}{|\mathrm{SO}_6^+(q)||\mathrm{GU}_1(q)|} = q^6(q^2 - q + 1)(q^4 + 1) = b_3,$$

whereas $|H_p| \leqslant 3(q - 1)^3 = a_4$ and

$$|x^G| \geqslant \frac{|\mathrm{SO}_8^-(q)|}{|\mathrm{SO}_6^-(q)||\mathrm{GL}_1(q)|} = q^6(q^2 + q + 1)(q^4 + 1) = b_4$$

if $m = 1$. It follows that

$$\rho_2 \leqslant \log(q + 1) \cdot a_3^2 b_3^{-1}, \quad \rho_1 \leqslant \log(q - 1) \cdot a_4^2 b_4^{-1}.$$

It is clear that the above estimates imply that $\beta(G) \to 0$ as q tends to infinity. Furthermore, we deduce that (22) holds (with $\ell = 4$) for all $q \geqslant 4$. $\qquad\square$

This completes the proof of Theorem 5.1. In Remark 5.3(a) we checked that Conjecture 6 holds in the special case $G = \mathrm{U}_4(2)$, so by combining Theorem 5.1 with Theorems 3.1 and 4.1, we deduce that the proofs of Theorems A and D are complete. In addition, Corollary B follows by combining Theorem A with the main theorem of [24], and we note that Corollary C is an immediate consequence. In view of Theorem 10, Corollary E follows immediately from Theorem D. Similarly, Theorem F follows from Theorems 4.1 and 5.1 (referring to Remark 5.3(b) for the special case $G = \mathrm{U}_4(2)$), which we then combine with the main theorems of [35, 37] to deduce Corollary G.

REFERENCES

[1] M. Anagnostopoulou-Merkouri and T.C. Burness, *On the regularity number of a finite group and other base-related invariants*, J. Lond. Math. Soc. **110** (2024), no. 6, Paper No. e70035, 65 pp.

[2] B. Baumeister, T.C. Burness, R.M. Guralnick and H.P. Tong-Viet, *On the maximal overgroups of Sylow subgroups of finite groups*, Adv. Math. **444** (2024), Paper No. 109632, 65 pp.

[3] A.A. Baykalov, *Intersection of conjugate solvable subgroups in symmetric groups*, Algebra and Logic **56** (2017), 87–97.

[4] A.A. Baykalov, *Base sizes for finite linear groups with solvable stabilisers*, J. Group Theory, to appear.

[5] R. Boltje, S. Danz and B. Külshammer, *On the depth of subgroups and group algebra extensions*, J. Algebra **335** (2011), 258–281.

[6] W. Bosma, J. Cannon and C. Playoust, *The MAGMA algebra system I: The user language*, J. Symb. Comput. **24** (1997), 235–265.

[7] T. Breuer, *The GAP Character Table Library, Version 1.3.3*, GAP package, `http://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib`, 2022.

[8] S. Burciu, L. Kadison and B. Külshammer, *On subgroup depth*, Int. Electron. J. Algebra **9** (2011), 133–166.

[9] T.C. Burness, *On the depth of subgroups of simple groups*, submitted (arXiv:2503.23845), 2025.

[10] T.C. Burness, *On soluble subgroups of sporadic groups*, Israel J. Math. **254** (2023), 313–340.

[11] T.C. Burness, *Base sizes for primitive groups with soluble stabilisers*, Algebra Number Theory **15** (2021), 1755–1807.

[12] T.C. Burness, *On base sizes for actions of finite classical groups*, J. Lond. Math. Soc. **75** (2007), 545–562.

[13] T.C. Burness, *Fixed point ratios in actions in finite classical groups, II*, J. Algebra **309** (2007), 80–138.

[14] T.C. Burness and M. Giudici, *Classical groups, derangements and primes*, Australian Mathematical Society Lecture Series, vol. 25, Cambridge University Press, Cambridge, 2016.

[15] T.C. Burness and S. Harper, *Finite groups, 2-generation and the uniform domination number*, Israel J. Math. **239** (2020), 271–367.

[16] T.C. Burness and H.Y. Huang, *On the intersections of Sylow subgroups in almost simple groups*, submitted (arXiv:2506.19745), 2025.

[17] T.C. Burness, E.A. O'Brien and R.A. Wilson, *Base sizes for sporadic simple groups*, Israel J. Math. **177** (2010), 307–333.

[18] T.C. Burness and A.R. Thomas, *The classification of extremely primitive groups*, Int. Math. Res. Not. IMRN no. 13 (2022), 10148–10248.

[19] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R. A. Wilson, ATLAS *of finite groups*, Oxford University Press, Eynsham, 1985.

[20] P. Diaconis, E. Giannelli, R.M. Guralnick, S. Law, G. Navarro, B. Sambale and H. Spink, *On the number and sizes of double cosets of Sylow subgroups of the symmetric group*, submitted (arXiv:2504.01149), 2025.

[21] S. Eberhard, *Intersections of Sylow 2-subgroups in symmetric groups*, J. Group Theory, to appear.

[22] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups, Number 3*, Mathematical Surveys and Monographs, Amer. Math. Soc., Providence, RI, 1998.

[23] J.A. Green, *Blocks of modular representations*, Math. Z. **79** (1962), 100–115.

[24] R.K. Kurmazov, *On the intersection of conjugate nilpotent subgroups in permutation groups*, Sib. Math. J. **54** (2013), 73–77.

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

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

[27] F. Lisi and L. Sabatini, *Sylow subgroups for distinct primes and intersection of nilpotent subgroups*, submitted (arXiv:2505.21222), 2025.

[28] V.D. Mazurov and E.I. Khukhro, *Unsolved problems in group theory: The Kourovka notebook, no. 20*, (arXiv:1401.0300), 2022.

[29] G.O. Michler, *A finite simple group of Lie type has p-blocks with different defects, $p \neq 2$*, J. Algebra **104** (1986), 220–230.

[30] D.S. Passman, *Groups with normal solvable Hall p-subgroups*, Trans. Amer. Math. Soc. **123** (1966), 99–111.

[31] E.P. Vdovin, *On the base size of a transitive group with solvable point stabilizer*, J. Algebra Appl. **11** (2012), 1250015, 14 pp.

[32] W. Willems, *Blocks of defect zero in finite simple groups of Lie type*, J. Algebra **113** (1988), 511–522.

[33] V.I. Zenkov, *Intersections of three nilpotent subgroups in a finite group*, Sib. Math. J. **62** (2021), 621–637.

[34] V.I. Zenkov, *On the intersections of nilpotent subgroups in finite groups with socle $L_3(q)$ or $U_3(q)$*, Tr. Inst. Mat. Mekh. **27** (2021), 70–78.

[35] V.I. Zenkov, *On intersections of nilpotent subgroups in finite groups with a sporadic socle*, Algebra Logic **59** (2020), 313–321.

[36] V.I. Zenkov, *On intersections of two nilpotent subgroups in finite groups with socle $L_2(q)$*, Sib. Math. J. **57** (2016), 1002–1010.

[37] V.I. Zenkov, *On intersections of nilpotent subgroups in finite symmetric and alternating groups*, Proc. Steklov Inst. Math. **285** (2014), S203–S208.

[38] V.I. Zenkov, *Intersections of nilpotent subgroups in finite groups*, Fundam. Prikl. Mat. **2** (1996), 1–92.

[39] V.I. Zenkov and V.D. Mazurov, *On the intersection of Sylow subgroups in finite groups*, Algebra and Logic **35** (1996), 236–240.

T.C. Burness, School of Mathematics, University of Bristol, Bristol BS8 1UG, UK
Email address: t.burness@bristol.ac.uk

H.Y. Huang, School of Mathematics and Statistics, University of St Andrews, KY16 9SS, UK
Email address: hy.huang@st-andrews.ac.uk