ON THE INTERSECTIONS OF SYLOW SUBGROUPS IN ALMOST SIMPLE GROUPS

TIMOTHY C. BURNESS AND HONG YI HUANG

Dedicated to Professor Viktor Zenkov

ABSTRACT. Let G be a finite almost simple group and let H be a Sylow p-subgroup of G. As a special case of a theorem of Zenkov, there exist $x, y \in G$ such that $H \cap H^x \cap H^y = 1$. In fact, if G is simple, then a theorem of Mazurov and Zenkov reveals that $H \cap H^x = 1$ for some $x \in G$. However, it is known that the latter property does not extend to all almost simple groups. For example, if $G = S_8$ and $p = 2$, then $H \cap H^x \neq 1$ for all $x \in G$. Further work of Zenkov in the 1990s shows that such examples are rare (for instance, there are no such examples if $p \geqslant 5$) and he reduced the classification of all such pairs to the situation where $p = 2$ and G is an almost simple group of Lie type defined over a finite field $\mathbb{F}_q$ and either $q = 9$ or q is a Mersenne or Fermat prime. In this paper, by adopting a probabilistic approach based on fixed point ratio estimates, we complete Zenkov's classification.

1. INTRODUCTION

This paper is a contribution to an extensive and expanding literature on problems concerning the intersections of nilpotent subgroups in finite groups, which stretches back several decades. In general terms, our main problem of interest can be stated as follows: given a finite group G and a collection of nilpotent subgroups $H_1, \ldots, H_k$, can we find elements $x_i \in G$ such that the intersection of the conjugate subgroups $\bigcap_i H_i^{x_i}$ is as small as possible, in some natural sense? For example, a theorem of Passman [30] from the 1960s states that if G is p-soluble and H is a Sylow p-subgroup of G for some prime p, then there exist elements $x, y \in G$ such that

$$H \cap H^x \cap H^y = O_p(G),$$

where $O_p(G)$ denotes the largest normal p-subgroup of G (and is therefore contained in every conjugate of H).

In more recent years, Passman's theorem has been extended and generalised in various directions. For example, Zenkov uses the Classification of Finite Simple Groups in [43] to extend Passman's theorem to all finite groups, without any assumption on the p-solubility of G. And in [19], Dolfi proves that if G is π-soluble and H is a Hall π-subgroup, with π any set of primes, then $H \cap H^x \cap H^y = O_\pi(G)$ for some $x, y \in G$ (here Passman's theorem is the special case $\pi = \{p\}$). In a different direction, Zenkov [33] shows that if G is a finite group with nilpotent subgroups A, B, C, then there exist $x, y \in G$ such that

$$A \cap B^x \cap C^y \leqslant F(G),$$

where $F(G)$ is the Fitting subgroup of G. It is not too difficult to see that the latter statement is false if we only consider two nilpotent subgroups. For example, if $G = S_8$ is the symmetric group of degree 8 and $A = B$ is a Sylow 2-subgroup, then $F(G) = 1$ and $A \cap B^x \neq 1$ for all $x \in G$. We refer the reader to [36, 43, 44] for some further variations on this theme.

In this paper, we will focus on the intersections of Sylow subgroups. So let us fix a finite group G and let H be a Sylow p-subgroup of G, where p is a prime divisor of $|G|$. Let us assume that $O_p(G) = 1$, which means that H is a *core-free* subgroup of G. In particular, it follows that G acts faithfully on the set $\Omega = G/H$ of cosets of H in G and this allows us to view $G \leqslant \mathrm{Sym}(\Omega)$ as a transitive permutation group on Ω with point stabiliser H. In this

Date: November 11, 2025.

setting, we recall that a *base* for G is a subset B of Ω with the property that the pointwise stabiliser of B in G is trivial. And then the *base size* of G, denoted $b(G,H)$, is defined to be the minimal size of a base and we note that

$$b(G,H) = \min\left\{ |S| \,:\, S \subseteq G,\ \bigcap_{x\in S} H^x = 1 \right\}.$$

Determining the base size of a given group is a fundamental problem in permutation group theory and there is a vast literature on this topic, dating back more than a century, with bases finding natural connections and applications across many different areas of group theory and combinatorics. We refer the reader to the survey articles [2, 27] and [11, Section 5] for further details and references on bases and their applications.

In the language of bases, Zenkov's aforementioned theorem from [33] implies that if G is a finite transitive permutation group with $F(G) = 1$ and a nilpotent point stabiliser H, then $b(G,H) \leqslant 3$ and this bound is best possible (for instance, if $G = S_8$ and H is a Sylow 2-subgroup, then $b(G,H) = 3$). The analogous problem for transitive groups with soluble point stabilisers is less well understood. Here the main conjecture is due to Vdovin, which asserts that $b(G,H) \leqslant 5$ if $R(G) = 1$, where $R(G)$ is the soluble radical of G (see Problem 17.41(b) in the *Kourovka Notebook* [28]). In other words, if G is a finite group with $R(G) = 1$ and H is a soluble subgroup, then it is conjectured that there exist elements $x_1, \ldots, x_4 \in G$ such that

$$H \cap H^{x_1} \cap H^{x_2} \cap H^{x_3} \cap H^{x_4} = 1.$$

Once again, examples show that this proposed upper bound is optimal (for instance, if $G = S_8$ and $H = S_4 \wr S_2$, then $b(G,H) = 5$). This conjecture remains open, although there is a reduction to almost simple groups due to Vdovin [31], and there is a further reduction to groups of Lie type [5, 9], with recent progress on classical groups due to Baykalov [4]. The conjecture in the special case where H is a soluble maximal subgroup of G is proved in [10] and we refer the reader to [1, Section 1] for various extensions of a similar flavour.

Let us now focus our attention on the case where G is a finite almost simple group with socle G_0. Here G_0, which is the unique minimal normal subgroup of G, is a non-abelian simple group and by identifying G_0 with its group of inner automorphisms we have

$$G_0 \trianglelefteqslant G \leqslant \mathrm{Aut}(G_0).$$

Let H be a non-trivial nilpotent subgroup of G. Then $b(G,H) \leqslant 3$ by Zenkov's theorem [33] and we highlight the following conjecture in the special case where G is simple (see Problem 15.40 in [28]):

Conjecture 1 (Vdovin [28], 2002)**.** *If G is a finite non-abelian simple group and H is a non-trivial nilpotent subgroup, then $b(G,H) = 2$.*

This conjecture has been resolved in various special cases (see [24, 35] for alternating and sporadic groups, for example), but it remains open for simple groups of Lie type. We refer the reader to Remarks 5 and 6 for a brief discussion of some related open problems.

The case where H is a Sylow p-subgroup of G for some prime divisor p of $|G|$ is of course a natural special case of Conjecture 1. In this setting, the conjecture was proved by Mazurov and Zenkov [45] in 1996. It is interesting to note that their proof for groups of Lie type relies on several deep results in representation theory. More precisely, a theorem of Green [22] from 1962 reveals that if G is a finite group, H is a Sylow p-subgroup and D is the defect group of a p-block for G, then $H \cap H^x = D$ for some $x \in G$. This key observation is then combined with later work of Michler [29] and Willems [32] in the 1980s, which shows that every finite simple group of Lie type has a p-block of defect zero for every prime divisor p of $|G|$, whence $D = 1$ is trivial and Green's theorem implies that $b(G,H) = 2$.

As noted above, there exist almost simple groups G with a Sylow p-subgroup H such that $b(G,H) = 3$. So it is natural to seek a complete classification of the pairs (G,p) with this property. This challenge was taken up by Zenkov in [43], which was published in 1996. In

p	G	Conditions
3	$\mathrm{P}\Omega_8^+(3).X$	$X \in \{C_3, S_3\}$
2	$\mathrm{L}_2(9).2^2$	
	$\mathrm{L}_2(q).2$	$q \geqslant 7$ is a Mersenne prime
	$\mathrm{L}_3(4).X$	$X \in \{C_2, C_2^2\}$, $\gamma \in G$
	$\mathrm{L}_n(2).2$	$n \geqslant 4$
	$\Omega_n^+(2).2$	$n \geqslant 8$
	$F_4(2).2$	
	$E_6(2).2$	

TABLE 1. The almost simple groups G with $b(G,H) = 3$ for $H \in \mathrm{Syl}_p(G)$

this substantial 92-page paper, Zenkov proves a number of remarkable results, culminating in the following major reduction of the original problem.

Theorem 2 (Zenkov [43], 1996)**.** *Let G be an almost simple group with socle G_0 and let H be a Sylow p-subgroup of G, where p is a prime divisor of $|G|$. Then $b(G,H) \leqslant 3$, with equality possible only if $p \in \{2,3\}$ and one of the following holds:*

(i) *(p,G) is recorded in Table 1, in which case $b(G,H) = 3$; or*

(ii) *$p = 2$ and G_0 is a simple group of Lie type over $\mathbb{F}_q$, where $q = 9$ or q is a Mersenne or Fermat prime.*

Remark 3. Note that in Table 1 we have not listed the groups $\mathrm{L}_3(2).2$ and S_8 with $p = 2$. This is simply to avoid a repetition of cases, noting that $\mathrm{L}_3(2).2 \cong \mathrm{L}_2(7).2$ and $S_8 \cong \mathrm{L}_4(2).2$. And in the row for $G = \mathrm{L}_3(4).X$ we write '$\gamma \in G$' to record the fact that G must contain an involutory graph automorphism of $\mathrm{L}_3(4)$.

In fact, Theorem 2 is a special case of a more general result (see [43, Theorem B]) concerning the structure of an arbitrary finite group G with a Sylow p-subgroup H such that $H \cap H^x \neq O_p(G)$ for all $x \in G$. We refer the reader to Remark 3.1 for a brief overview of the main steps in the proof of Zenkov's result in the almost simple setting.

Some of the open cases arising in part (ii) of Theorem 2 have been handled in more recent work. More specifically, the groups with socle $\mathrm{L}_2(q)$ are treated in [43, Lemma 3.18] (in fact, the main theorem of [40] determines all the pairs of nilpotent subgroups A, B with $A \cap B^x \neq 1$ for all $x \in G$), and those with socle $\mathrm{L}_3(q)$ or $\mathrm{U}_3(q)$ are dealt with in [34]. In addition, the main theorem of [42] handles all the almost simple exceptional groups of Lie type over $\mathbb{F}_3$.

Our main result is Theorem A below. This shows that $b(G,H) = 2$ for all of the open cases in part (ii) of Theorem 2, thereby completing the classification of the almost simple groups G with a Sylow p-subgroup H such that $H \cap H^x \neq 1$ for all $x \in G$. In addition, Theorem A resolves Problem 20.121 in the *Kourovka Notebook* [28].

Theorem A. *Let G be an almost simple group and let H be a Sylow p-subgroup of G, where p is a prime divisor of $|G|$. Then $b(G,H) \leqslant 3$, with equality if and only if (p,G) is one of the cases recorded in Table 1.*

In view of Theorem 2, we may assume G is an almost simple group of Lie type over $\mathbb{F}_q$ with socle G_0, and either $q = 9$ or q is a Mersenne or Fermat prime. In addition, we may assume H is a Sylow 2-subgroup and $G_0 \neq \mathrm{L}_2(q)$, $\mathrm{L}_3(q)$ or $\mathrm{U}_3(q)$. And in view of the main theorem in [45] for simple groups, we can also assume that $|G : G_0|$ is even. As discussed above, we may view $G \leqslant \mathrm{Sym}(\Omega)$ as a transitive permutation group on $\Omega = G/H$ and our goal is to show that $b(G,H) = 2$.

To prove Theorem A, we adopt a completely different approach to the problem, utilising a powerful probabilistic technique first introduced by Liebeck and Shalev [25]. This method

p	G	(A,B)	Conditions	Reference
3	$\mathrm{P}\Omega_8^+(3).X$	$K \leqslant A, B \leqslant H$	$X \in \{C_3, S_3\}$	[47, Theorem 1]
2	$\mathrm{L}_2(9).2^2$	(H,K)		[40, Theorem 2]
	$\mathrm{L}_3(4).X$	See Remark 4(a)	$X \in \{C_2, C_2^2\}$, $\gamma \in G$	[37, Theorem 1]
	$\mathrm{L}_n(2).2$	$K \leqslant A, B \leqslant H$	$n \geqslant 4$ even	[37, Theorem 1]
	$\Omega_n^+(2).2$	$K \leqslant A, B \leqslant H$	$n \geqslant 8$	[38, Theorem 1]
	$F_4(2).2$	(H,K)		[46, Theorem 2]
	$E_6(2).2$	$K \leqslant A, B \leqslant H$		[39, Theorem 5]

TABLE 2. The pairs (A,B) in part (ii) of Corollary B

has been extensively applied in recent years for studying bases for almost simple primitive permutation groups.

This approach relies on the elementary observation that if $Q(G,H)$ is the probability that a uniformly random pair of points in Ω do not form a base for G, then

$$Q(G,H) \leqslant \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i, G/H)^2 =: \widehat{Q}(G,H),$$

where $\{x_1, \ldots, x_k\}$ is a complete set of representatives of the conjugacy classes in G of elements of prime order, and

$$\mathrm{fpr}(x_i, G/H) = \frac{|x_i^G \cap H|}{|x_i^G|}$$

is the fixed point ratio of x_i on G/H, which is simply the proportion of cosets in G/H fixed by x_i. In particular, if $\widehat{Q}(G,H) < 1$ then $b(G,H) = 2$. And of course, in the setting we are interested in, with H a Sylow 2-subgroup of G, we only need to consider fixed point ratios for involutions.

The main challenge in applying this method involves bounding the number of involutions in H that are contained in 'small' conjugacy classes in G. To do this, it is often helpful to identify an appropriate subgroup $L < G$ containing H, where it may be easier to bound the number of involutions in L of a given type, rather than in H directly. For the remaining classes x_i^G of involutions, we can often work with the trivial upper bound $|x_i^G \cap H| < |H|$, which greatly simplifies the analysis.

By combining Theorem A with more recent work of Zenkov [37, 38, 39, 40, 46, 47] we immediately obtain Corollary B below, which gives a precise description of the triples (G,A,B), where G is almost simple and A, B are primary subgroups (that is to say, A and B have prime power order) with the property that $A \cap B^x \neq 1$ for all $x \in G$. Note that the subgroup K defined in part (ii) is denoted by $\min_G(H,H)$ in Zenkov's papers.

Corollary B. *Let G be an almost simple group and let A and B be primary subgroups of G. Then $A \cap B^x \neq 1$ for all $x \in G$ if and only if (p,G) is one of the cases in Table 1, and A, B are p-subgroups such that*

(i) *A and B are both Sylow p-subgroups of G; or*

(ii) *(A,B) is recorded in Table 2, up to conjugacy and ordering, where H is a Sylow p-subgroup of G and*

$$K = \langle H \cap H^x \,:\, x \in G, |H \cap H^x| = m \rangle$$

with $m = \min\{|H \cap H^x| \,:\, x \in G\}$.

Remark 4. Some comments on the statement of Corollary B are in order.

(a) Suppose $p = 2$ and $G_0 = \mathrm{L}_3(4)$ as in Table 2. Here $G = G_0.2$ or $G_0.2^2$ contains an involutory graph automorphism γ and we set $G_1 = G_0.\langle\gamma\rangle$. Then according to [37, Theorem 1], if A and B are a pair of primary subgroups of G, then $A \cap B^x \neq 1$ for all $x \in G$ if and only if $K < A \cap B \cap G_1$ and either $L \leqslant A$ or $L \leqslant B$, where $L = \langle A \cap B^x \,:\, x \in \mathcal{M}\rangle$ and $\mathcal{M}$ is the set of elements $x \in G$ such that $A \cap B^x$ is inclusion-minimal in the set $\{A \cap B^g \,:\, g \in G\}$. It is straightforward to construct all of the relevant pairs (A, B) using Magma [7].

(b) In each of the remaining cases, the description of the relevant pairs (A, B) is easier to state and it just depends on the subgroup K of H defined in part (ii) of the corollary. This subgroup K is given in the relevant reference listed in the final column of Table 2, but for the reader's convenience we provide a brief description here:

- $G = \mathrm{P}\Omega_8^+(3).X$: $K = O_3(N_G(P))$, where $P = P_{1,3,4}$ is a parabolic subgroup of G_0 corresponding to the central node in the Dynkin diagram of type D_4. We note that $|H : K| = 3$.
- $G = \mathrm{L}_2(9).2^2$: $K = D_{16}$ and $|H : K| = 2$.
- $G = \mathrm{L}_n(2).2$, $n \geqslant 4$ even: $K = O_2(N_G(P))$, where P is a parabolic subgroup of G_0 corresponding to the central node of the Dynkin diagram of type A_{n-1}. Here $P = [2^a].\mathrm{L}_2(2)$ with $a = n(n-1)/2 - 1$ and thus $|H : K| = 2$.
- $G = \Omega_n^+(2).2 = \mathrm{O}_n^+(2)$, $n \geqslant 8$: $K = O_2(P)$ is the unipotent radical of a maximal parabolic subgroup P of G. In the notation of [23], we have $P = P_k$ with $k = n/2 - 1$, which we can view as the stabiliser in G of a k-dimensional totally singular subspace of the natural module for G. In particular, $|H : K| = 2^a$ with $a = (n^2 - 6n + 8)/8$.
- $G = F_4(2).2$: $K = O_2(P).D_{16}$, where $P = P_{1,4}$ is a maximal parabolic subgroup of G with Levi subgroup of type B_2. Note that $|H : K| = 2$.
- $G = E_6(2).2$: $K = O_2(P).(O_2(Q).2)$, where $O_2(P)$ is the unipotent radical of a maximal parabolic subgroup $P = [2^{24}].\mathrm{O}_8^+(2)$ of G of type $P_{1,6}$, and $O_2(Q)$ is the unipotent radical of a maximal parabolic subgroup $Q = 2^{3+6}.\mathrm{L}_3(2)$ of $\Omega_8^+(2)$ of type P_1. In particular, $|O_2(P)| = 2^{24}$ and $|O_2(Q)| = 2^9$, whence $|H : K| = 2^3$.

(c) Note that if $G = \mathrm{L}_n(2).2$ with $n \geqslant 5$ odd, then [37, Theorem 1] implies that $A \cap B^x \neq 1$ for all $x \in G$ if and only if A and B are both Sylow 2-subgroups of G. This explains why n is even for $G = \mathrm{L}_n(2).2$ in Table 2. And by [40, Theorem 2], the same conclusion holds when $G = \mathrm{L}_2(q).2$ and $q \geqslant 7$ is a Mersenne prime.

In order to conclude the introduction, we present several remarks describing some related open problems.

Remark 5. Let G be a finite group and let P_i be a Sylow p_i-subgroup of G, where $p_1, \ldots, p_n$ are the distinct prime divisors of $|G|$. In a recent preprint [26], Lisi and Sabatini conjecture that there exists an element $x \in G$ such that for each i, $P_i \cap P_i^x$ is inclusion-minimal in the set $\{P_i \cap P_i^g \,:\, g \in G\}$. So for a simple group G, in view of the main theorem of [45], this conjecture asserts that there is an element $x \in G$ such that $P_i \cap P_i^x = 1$ for all i. In particular, if H is a nilpotent subgroup of G (with G simple), then $H \cap H^x = 1$ and so [26, Conjecture A] immediately implies Conjecture 1. The Lisi-Sabatini conjecture is proved in [26] for all metanilpotent groups of odd order, as well as all sufficiently large symmetric and alternating groups. The latter asymptotic result relies on a probabilistic argument, which applies recent work of Diaconis et al. [18] and Eberhard [20].

Remark 6. Let G be a finite non-abelian simple group and let H be a nilpotent subgroup. Recall that Conjecture 1 asserts that $H \cap H^x = 1$ for some $x \in G$. In fact, in several special cases, it has been shown that if A and B are any nilpotent subgroups of G, then $A \cap B^x = 1$ for some $x \in G$. This is proved in [35, 41] for alternating and sporadic groups, and we refer

the reader to [34, 40] for the low-rank Lie type groups $\mathrm{L}_2(q), \mathrm{L}_3(q)$ and $\mathrm{U}_3(q)$. Given these results, it seems reasonable to speculate that this property holds for all simple groups, which can be viewed as a natural generalisation of Conjecture 1.

Remark 7. Let G be a finite group and let H be a proper subgroup. In 2011, Boltje, Danz and Külshammer [6] introduced and studied the *depth* of H, denoted $d_G(H)$, which is a positive integer defined in terms of the inclusion of complex group algebras $\mathbb{C}H \subseteq \mathbb{C}G$ (we refer the reader to [6] for the formal definition). This notion has been the focus of numerous papers and there has been a particular interest in studying the depth of subgroups of simple and almost simple groups (see [8] and the references therein). In this setting, if G is almost simple and $H \neq 1$ is core-free, then we have

$$3 \leqslant d_G(H) \leqslant 2b(G,H) - 1 \tag{1}$$

(see [8, Propositions 2.2 and 2.6], for example). In particular, if $b(G,H) = 2$ then $d_G(H) = 3$, so the main theorem of [45] implies that every (non-trivial) Sylow subgroup of a simple group has depth 3 (and Conjecture 1 asserts that every non-trivial nilpotent subgroup has depth 3). In view of Theorem A, in order to determine the depth of every Sylow subgroup of an almost simple group, it just remains to consider the pairs (G,H) recorded in Table 1. Since $b(G,H) = 3$, the bounds in (1) imply that $d_G(H) \in \{3,4,5\}$ and further work is needed in order to determine the precise depth of H:

(a) As noted in [8, Remark 8(b)], if $G = \mathrm{PGL}_2(q)$ and H is a Sylow 2-subgroup of G, where q is a Mersenne prime, then $d_G(H) = 5$.

(b) The relevant groups with socle $\mathrm{P}\Omega_8^+(3)$, $\mathrm{L}_4(2)$, $\mathrm{L}_3(4)$ and $\mathrm{L}_2(9)$ can be handled using Magma and the character-theoretic approach for calculating $d_G(H)$, which is explained in [8, Section 2.1.1]. In every case, we get $d_G(H) = 5$.

(c) It remains an open problem to determine $d_G(H)$ for the remaining cases in Table 1, where $p = 2$ and $G = F_4(2).2$, $E_6(2).2$, $\mathrm{L}_n(2).2$ or $\mathrm{O}_n^+(2)$. We have used Magma to check that $d_G(H) = 5$ for $G = \mathrm{L}_n(2).2$ with $3 \leqslant n \leqslant 7$, and for $G = \mathrm{O}_n^+(2)$ with $n = 8$ or 10.

So there is some evidence to suggest that if G is almost simple and H is a Sylow p-subgroup of G, where p is a prime divisor of $|G|$, then either $d_G(H) = 3$, or (G,H) is one of the cases in Table 1 and $d_G(H) = 5$.

Remark 8. Let G be an almost simple group and set $N = N_G(H)$, where H is a Sylow p-subgroup of G and p is a prime divisor of $|G|$. Then we can identify G/N with the set of Sylow p-subgroups of G and we can think of $b(G,N)$ as the base size with respect to the natural transitive action of G by conjugation on the set of Sylow p-subgroups of G. Of course, if $N = H$, then $b(G,N)$ is given in Theorem A. However, it remains an open problem to determine $b(G,N)$ when $N \neq H$. Here we speculate that the upper bound $b(G,N) \leqslant 4$ is best possible, noting that equality holds when $G = S_6$ and $p = 3$ (in which case, $N = S_3 \wr S_2$ is a maximal subgroup of G). Let us also observe that there are examples where $b(G,N) > 2$ and p is arbitrarily large (in contrast to the situation for $b(G,H)$, where Theorem 2 shows that $b(G,H) > 2$ only if $p = 2$ or 3). For example, if $G = \mathrm{L}_2(p)$ with $p \geqslant 5$, then N is a Borel subgroup of G and we have $b(G,N) = 3$ (see [10, Proposition 4.1]).

Note added in press. In a recent preprint [15], we have used a probabilistic approach to prove the Lisi-Sabatini conjecture for all non-alternating simple groups (see Remark 5). And by combining the main result in [15] with earlier work of Kurmazov [24], we are able to complete the proof of Vdovin's conjecture on nilpotent subgroups of simple groups (see Conjecture 1). In fact, we have established the stronger form of the conjecture alluded to in Remark 6: if G is simple and A, B are nilpotent subgroups of G, then $A \cap B^x = 1$ for some $x \in G$.

Notation. For a finite group G and positive integer n, we 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 $G{:}H$. If X is a subset of G, then we will write $i_2(X)$ for the number of involutions in X. And if p is a prime, then $\mathrm{Syl}_p(G)$ is the set of Sylow p-subgroups of G. We will 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 [23] and we write (a, b) for the highest common factor of the positive integers a and b.

Acknowledgements. The second author thanks the London Mathematical Society for their support as an LMS Early Career Research Fellow at the University of St Andrews.

2. Preliminaries

In this section we record several preliminary results, which will be needed in the proof of Theorem A. We begin by briefly recalling the probabilistic method for bounding the base size of a finite permutation group, which is at the heart of our proof.

2.1. **Bases.** Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group on a finite set Ω with point stabiliser $H \neq 1$. Recall that a subset B of Ω is a *base* for G if the pointwise stabiliser of B in G is trivial. We write $b(G, H)$ for the minimal size of a base, which we refer to as the *base size* of G. Notice that this coincides with the minimal number of conjugates of H with trivial intersection.

Next let

$$Q(G,H) = \frac{|\{(\alpha,\beta) \in \Omega^2 \,:\, G_\alpha \cap G_\beta \neq 1\}|}{|\Omega|^2} \tag{2}$$

be the probability that a random pair of points in Ω is not a base for G, which means that $b(G, H) = 2$ if and only if $Q(G, H) < 1$. Then as explained in the proof of [25, Theorem 1.3] (see [25, Section 2]), we have

$$Q(G,H) \leqslant \widehat{Q}(G,H) = \sum_{i=1}^{k} |x_i^G| \cdot \left(\frac{|x_i^G \cap H|}{|x_i^G|}\right)^2, \tag{3}$$

where $x_1, \ldots, x_k$ is a complete set of representatives of the conjugacy classes in G of elements of prime order. The following result is an immediate consequence.

Lemma 2.1. *If $\widehat{Q}(G, H) < 1$ then $b(G, H) = 2$.*

Remark 2.2. In the proof of Theorem A, we are interested in the case where H is a Sylow 2-subgroup of G. Since $|x^G \cap H| = 0$ for all $x \in G$ of odd order, we have

$$\widehat{Q}(G,H) = \sum_{i=1}^{\ell} |y_i^G| \cdot \left(\frac{|y_i^G \cap H|}{|y_i^G|}\right)^2,$$

where $y_1, \ldots, y_\ell$ is a set of representatives of the conjugacy classes of involutions in G.

The next elementary lemma is useful for obtaining an upper bound on $\widehat{Q}(G, H)$.

Lemma 2.3. *Suppose $x_1, \ldots, x_m$ represent distinct G-classes such that $\sum_i |x_i^G \cap H| \leqslant a$ and $|x_i^G| \geqslant b$ for all i. Then*

$$\sum_{i=1}^{m} |x_i^G| \cdot \left(\frac{|x_i^G \cap H|}{|x_i^G|}\right)^2 \leqslant a^2 b^{-1}.$$

Proof. See [12, Lemma 2.1]. □

G_0	$\lvert H_0\rvert$	Conditions
$\mathrm{L}_n^{\varepsilon}(q)$	$\alpha^m((q-\varepsilon)_2)^m(m!)_2$	$n = 2m+1 \geqslant 3$
	$\frac{1}{d_2}\alpha^m((q-\varepsilon)_2)^{m-1}(m!)_2$	$n = 2m \geqslant 2$, $d = (n, q-\varepsilon)$
$\mathrm{PSp}_n(q)$	$\frac{1}{2}\alpha^m(m!)_2$	$n = 2m \geqslant 2$
$\Omega_n(q)$	$\frac{1}{2}\alpha^m(m!)_2$	$n = 2m+1 \geqslant 3$
$\mathrm{P}\Omega_n^+(q)$	$\frac{1}{2d}\alpha^m(m!)_2$	$n = 2m$, $m \geqslant 4$ even, $d = (4, q^m-1)$
	$\frac{1}{d}\alpha^{m-1}(q-1)_2((m-1)!)_2$	$n = 2m$, $m \geqslant 3$ odd, $d = (4, q^m-1)$
$\mathrm{P}\Omega_n^-(q)$	$\alpha^{m-1}((m-1)!)_2$	$n = 2m$, $m \geqslant 4$ even
	$\frac{1}{d}\alpha^{m-1}(q+1)_2((m-1)!)_2$	$n = 2m$, $m \geqslant 3$ odd, $d = (4, q^m+1)$
$E_8(q)$	$2^6\alpha^8$	
$E_7(q)$	$2^2\alpha^7$	
$E_6^{\varepsilon}(q)$	$2^3\alpha^4((q-\varepsilon)_2)^2$	
$F_4(q)$	$2^3\alpha^4$	
${}^3D_4(q)$	α^2	
$G_2(q)$, $q \geqslant 5$	α^2	
${}^2G_2(q)$, $q \geqslant 27$	α	

TABLE 3. The order of $H_0 \in \mathrm{Syl}_2(G_0)$ with q odd, $\alpha = (q^2-1)_2$

2.2. **Sylow subgroups.** We will need information of the orders of Sylow 2-subgroups in almost simple groups of Lie type in odd characteristic. To this end, the following number-theoretic result will be useful. Here and throughout the paper, we write $(m)_2$ for the largest power of 2 dividing the positive integer m (so for example, $(24)_2 = 8$).

Lemma 2.4. *Let q be an odd prime power, let d be a positive integer and let $\varepsilon \in \{-1, 1\}$. Then*

$$(q^d-\varepsilon)_2 = \begin{cases} (q-\varepsilon)_2 & \text{if } d \text{ is odd} \\ (q^2-1)_2(d/2)_2 & \text{if } d \text{ is even and } \varepsilon = 1 \\ 2 & \text{otherwise.} \end{cases}$$

Proof. This is [3, Lemma 2.1(i)]. □

We will also need the following elementary result concerning factorials.

Lemma 2.5. *Let m be a positive integer. Then $2^m(m!)_2 = ((2m)!)_2$ and $(m!)_2 < 2^m$.*

Proof. The first statement is trivial. And for the inequality, set $(m!)_2 = 2^{\ell}$ and note that

$$\ell = \sum_{i=1}^{\infty} \left\lfloor \frac{m}{2^i} \right\rfloor < m \sum_{i=1}^{\infty} 2^{-i} = m.$$

The result follows. □

Our main result is the following.

Proposition 2.6. *Let G be an almost simple group of Lie type over $\mathbb{F}_q$ with socle G_0 and assume q is odd. Let H be a Sylow 2-subgroup of G and set $H_0 = H \cap G_0$. Then we have $|H| = |H_0||G : G_0|_2$, where $|H_0|$ is recorded in Table 3.*

Proof. This is a routine exercise, working with Lemma 2.4 and the order of G_0, which is conveniently recorded in [23, Tables 5.1.A, 5.1.B]. □

2.3. **Involutions.** Our proof of Theorem A will rely on Lemma 2.1, which means that we will need to compute an appropriate upper bound on $\widehat{Q}(G,H)$. And to do this, we will make use of Lemma 2.3. Let $\mathcal{I} = \{y_1, \ldots, y_\ell\}$ be a set of representatives of the conjugacy classes in G of involutions.

Typically, we will proceed by partitioning $\mathcal{I}$ into two or three disjoint subsets, say

$$\mathcal{I} = \mathcal{I}_1 \cup \cdots \cup \mathcal{I}_m \text{ with } \mathcal{I}_j = \{y_{j,1}, \ldots, y_{j,k_j}\},$$

and for each j we will establish bounds of the form

$$\sum_{i=1}^{k_j} |y_{j,i}^G \cap H| \leqslant a_j, \;\; \min\{|y_{j,i}^G| \,:\, 1 \leqslant i \leqslant k_j\} \geqslant b_j.$$

Then Lemma 2.3 yields

$$\widehat{Q}(G,H) \leqslant \sum_{j=1}^{m} a_j^2 b_j^{-1}$$

and our aim is to use this upper bound to force $\widehat{Q}(G,H) < 1$.

In order to effectively apply this approach, we need some information on the 'small' conjugacy classes of involutions in almost simple groups of Lie type in odd characteristic. For the exceptional groups, it turns out that we will only require a lower bound on $|x^G|$ that is valid for every involution $x \in G$ and we can refer to [16, Proposition 2.11] for this information (see (4) in the proof of Proposition 3.3). However, for classical groups, we will usually need to know the sizes of the two or three smallest conjugacy classes and with this aim in mind we present the following technical result. In the statement, we refer to the notation for involutions from [21, Table 4.5.1].

Proposition 2.7. *Let G be an almost simple classical group over $\mathbb{F}_q$ with socle G_0, where q is odd. Let $x \in G$ be an involution.*

(i) *If $G_0 = \mathrm{L}_n^\varepsilon(q)$ with $n \geqslant 5$, then either x is a t_1-type involution and*

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

or $|x^G| \geqslant f(n,q)$ with

$$f(n,q) = \begin{cases} \frac{|G_0|}{|\mathrm{SU}_5(q_0)|} = \frac{1}{d}q^5(q+1)(q^{3/2}-1)(q^2+1)(q^{5/2}-1) & \text{if } (\varepsilon,n,q) = (+,5,q_0^2) \\ \frac{|G_0|}{|\mathrm{PSp}_6(q)|} = \frac{2}{d}q^6(q^3-\varepsilon)(q^5-\varepsilon) & \text{if } n = 6 \\ \frac{|\mathrm{GL}_n^\varepsilon(q)|}{|\mathrm{GL}_{n-2}^\varepsilon(q)||\mathrm{GL}_2^\varepsilon(q)|} = \frac{q^{2n-4}(q^{n-1}-\varepsilon^{n-1})(q^n-\varepsilon^n)}{(q^2-1)(q-\varepsilon)} & \text{otherwise,} \end{cases}$$

where $d = (n, q-\varepsilon)$.

(ii) *If $G_0 = \mathrm{L}_4^\varepsilon(q)$, then either x is a γ_1 graph automorphism and*

$$|x^G| \geqslant \frac{|G_0|}{|\mathrm{PSp}_4(q)|} \geqslant \frac{1}{2}q^2(q^3 - \varepsilon),$$

or

$$|x^G| \geqslant \frac{|\mathrm{GL}_4^\varepsilon(q)|}{|\mathrm{GL}_3^\varepsilon(q)||\mathrm{GL}_1^\varepsilon(q)|} = \frac{q^3(q^4-1)}{q-\varepsilon}.$$

(iii) *If $G_0 = \mathrm{PSp}_n(q)$ with $n \geqslant 6$, then either x is a t_1-type involution and*

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

or $|x^G| \geqslant f(n,q)$ *with*

$$f(n,q) = \begin{cases} \frac{|G_0|}{|\mathrm{Sp}_6(q_0)|} = \frac{1}{2}q^{9/2}(q+1)(q^2+1)(q^3+1) & \text{if } (n,q) = (6,q_0^2) \\ \frac{|G_0|}{|\mathrm{GU}_3(q)|} = \frac{1}{2}q^6(q-1)(q^2+1)(q^3-1) & \text{if } n = 6,\ q \neq q_0^2 \\ \frac{|G_0|}{|\mathrm{Sp}_4(q^2)|} = \frac{1}{2}q^8(q^2-1)(q^6-1) & \text{if } n = 8 \\ \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_{n-4}(q)||\mathrm{Sp}_4(q)|} = \frac{q^{2n-4}(q^{n-2}-1)(q^n-1)}{(q^4-1)(q^2-1)} & \text{otherwise.} \end{cases}$$

(iv) *If* $G_0 = \mathrm{PSp}_4(q)$*, then either* x *is a* t_2*-type or* t_2'*-type involution and*

$$|x^G| \geqslant \frac{|G_0|}{|\mathrm{Sp}_2(q^2)|} = \frac{1}{2}q^2(q^2-1),$$

or $|x^G| \geqslant f(n,q)$ *with*

$$f(n,q) = \begin{cases} \frac{|G_0|}{|\mathrm{Sp}_4(q_0)|} = \frac{1}{2}q^2(q+1)(q^2+1) & \text{if } q = q_0^2 \\ \frac{|G_0|}{|\mathrm{GU}_2(q)|} = \frac{1}{2}q^3(q-1)(q^2+1) & \text{otherwise.} \end{cases}$$

(v) *If* $G_0 = \Omega_n(q)$ *with* $n = 2m+1 \geqslant 7$*, then either* x *is a* t_m*-type or* t_m'*-type involution and*

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

or

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

(vi) *If* $G_0 = \mathrm{P}\Omega_n^\varepsilon(q)$ *with* $n = 2m \geqslant 8$*, then either* x *is a* γ_1 *graph automorphism and*

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

or

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

Proof. This is a straightforward exercise, working with the detailed information on conjugacy classes of semisimple involutions and involutory graph automorphisms presented in [21, Table 4.5.1] (also see [14, Chapter 3]).

For example, suppose $G_0 = \mathrm{PSp}_n(q)$ with $n = 2m \geqslant 10$ and let $x \in G$ be an involution. If $x \in G$ is a field automorphism, then $q = q_0^2$ and [14, Proposition 3.4.15] gives

$$|x^G| \geqslant \frac{|G_0|}{|\mathrm{Sp}_n(q_0)|} > \frac{1}{2}q^{n(n+1)/4}.$$

Otherwise, $x \in \mathrm{PGSp}_n(q)$ is semisimple and we can read off $|x^G|$ from [21, Table 4.5.1] (or [14, Table B.5]). Then either x is an involution of type t_m, t_m', $t_{m/2}$ or $t_{m/2}'$ (in the notation of [21, Table 4.5.1]), in which case

$$|x^G| \geqslant \frac{|G_0|}{|\mathrm{Sp}_m(q^2)|} > \frac{1}{4}q^{n^2/4},$$

or x is an involution of type t_i with $1 \leqslant i < m/2$ and we have

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

By comparing the above expressions, we deduce that $|x^G|$ is minimal when x is a t_1-type involution. And for all other involutions, $|x^G|$ is minimal when x is of type t_2, which gives the result recorded in part (iii). Note that the latter statement is false when $n = 8$ since

$$\frac{|\mathrm{Sp}_8(q)|}{2|\mathrm{Sp}_4(q)|^2} > \frac{|\mathrm{Sp}_8(q)|}{2|\mathrm{Sp}_4(q^2)|},$$

which explains why the expression for $f(n,q)$ in (iii) has a different form when $n = 8$ (and similarly when $n = 6$).

A very similar argument applies in each of the remaining cases and we omit the details. □

2.4. **Computational methods.** In the proof of Theorem A, it will be convenient to use direct computation to handle certain low rank groups of Lie type defined over small fields. For all the computations, we will use Magma [7] (version V2.28-21).

In order to state our main result, let us define $\mathcal{A}$ to be the following collection of simple groups of Lie type, recalling that we use the notation for simple groups from [23]:

$$\begin{array}{l}\mathrm{L}_4^{\varepsilon}(3),\ \mathrm{L}_4^{\varepsilon}(5),\ \mathrm{L}_4^{\varepsilon}(7),\ \mathrm{L}_4^{\varepsilon}(9),\ \mathrm{L}_4^{\varepsilon}(17),\ \mathrm{L}_4(31),\ \mathrm{L}_4(127),\ \mathrm{U}_5(3),\ \mathrm{L}_5(9),\ \mathrm{L}_6^{\varepsilon}(3),\ \mathrm{L}_6(9),\ \mathrm{L}_8^{\varepsilon}(3),\\ \mathrm{PSp}_4(3),\ \mathrm{PSp}_4(5),\ \mathrm{PSp}_4(7),\ \mathrm{PSp}_4(9),\ \mathrm{PSp}_4(17),\ \mathrm{PSp}_6(3),\ \mathrm{PSp}_8(3), \mathrm{PSp}_{10}(3),\\ \Omega_7(3),\ \Omega_9(3),\ \Omega_{11}(3),\ \Omega_{13}(3),\ \mathrm{P}\Omega_8^{\pm}(3),\ \mathrm{P}\Omega_{10}^{\pm}(3),\ \mathrm{P}\Omega_{12}^{\pm}(3),\ G_2(3)\end{array}$$

Proposition 2.8. *Let G be an almost simple group with socle $G_0 \in \mathcal{A}$ and let H be a Sylow 2-subgroup of G. Then $b(G,H) = 2$.*

Proof. To begin with, assume $G_0 \neq \mathrm{P}\Omega_8^+(3)$. We first construct the full automorphism group $L = \mathrm{Aut}(G_0)$ as a permutation group, using the function `AutomorphismGroupSimpleGroup`, and we take a Sylow 2-subgroup J of L. In every case, we note that L/G_0 is a 2-group and we can use random search to find an element $x \in L$ such that $J \cap J^x = 1$. This means that J has a regular orbit on L/J, which in turn implies that H has a regular orbit on G/H and thus $b(G,H) = 2$.

Finally, suppose $G_0 = \mathrm{P}\Omega_8^+(3)$. Here $|\mathrm{Out}(G_0)| = 24$ and we can use Magma to construct the index-three subgroup $L = \mathrm{PGO}_8^+(q) = G_0.D_8$ of $\mathrm{Aut}(G_0)$ as a permutation group of degree 3360. We can then proceed as before, taking a Sylow 2-subgroup J of L and using random search to find an element $x \in L$ such that $J \cap J^x = 1$. The result follows. □

3. Proof of Theorem A

We are now ready to prove Theorem A. Our starting point is Zenkov's main reduction theorem for almost simple groups from [43], which we stated as Theorem 2 in Section 1. For the reader's convenience, in the following remark we provide a brief overview of Zenkov's proof.

Remark 3.1. Let G be an almost simple group with socle G_0 and let H be a Sylow p-subgroup of G, where p is a prime divisor of $|G|$.

(a) A starting point is the main theorem from [45] on simple groups, which allows us to assume that p divides $|G : G_0|$. In particular, $p = 2$ when G_0 is an alternating or sporadic group; the argument for symmetric groups is given in [45] and the 12 sporadic groups of the form $G = G_0.2$ are handled case-by-case in [43, Section 3] (the result for sporadic groups can also be verified very easily using Magma [7], proceeding as in the proof of Proposition 2.8).

(b) Now assume G_0 is a simple group of Lie type over $\mathbb{F}_q$. For p odd, a long and technical argument, based on the elimination of a counterexample of minimal order, is presented in [43, Section 6]. Here the main result is [43, Theorem 6.1], which shows that $b(G,H) = 3$ if and only if $p = 3$ and $G_0 = \mathrm{P}\Omega_8^+(3)$, with G recorded in Table 1. It is worth noting that it is easy to use Magma to verify that $b(G,H) = 3$ for the two relevant groups with $G_0 = \mathrm{P}\Omega_8^+(3)$.

(c) The analysis for $p = 2$ divides naturally into two cases, according to whether or not q is odd or even, and the main details are given in Sections 4 and 5 of [43], respectively. For q odd, the main result is [43, Theorem 4.1], which implies that $b(G,H) = 2$ unless $q = 9$ or q is a Mersenne or Fermat prime. The proof relies on a detailed analysis

of a minimal counterexample, with [43, Lemma 4.3] as a key tool. The latter states that if G is a minimal counterexample, then $O_2(C) \cap H^x \neq 1$ for all $x \in G$, where $C = C_G(z)$ is the centraliser of an involution $z \in Z(H) \cap G_0$. Then by studying the structure of involution centralisers in G, in many cases Zenkov is able to reach a contradiction by establishing the existence of an element $x \in G$ with $O_2(C) \cap H^x = 1$.

(d) In [43, Lemma 3.18], Zenkov proves that $b(G,H) = 3$ when $p = 2$ and either $G = \mathrm{Aut}(\mathrm{L}_2(9)) = \mathrm{L}_2(9).2^2 \cong A_6.2^2$ or $G = \mathrm{PGL}_2(q)$ with $q \geqslant 7$ a Mersenne prime.

(e) Finally, suppose $p = 2$ and q is even. Here the first main result is [43, Theorem 5.1], which tells us that $b(G,H) = 3$ only if G_0 is one of the following (here we exclude $\mathrm{L}_3(2).2 \cong \mathrm{PGL}_2(7)$, $\mathrm{L}_4(2).2 \cong S_8$ and $\mathrm{PSp}_4(2)'.2^2 \cong \mathrm{L}_2(9).2^2$):

$$\mathrm{L}_3(4),\ \mathrm{L}_n(2)\ (n \geqslant 5),\ \Omega_n^{\pm}(2)\ (n \geqslant 8),\ E_6(2),\ F_4(2),\ {}^2F_4(2)',\ G_2(2)'.$$

As before, the proof proceeds by studying the structure of a minimal counterexample, using the fact that $N_G(H)$ is a Borel subgroup of G.

And then it remains to determine which of these possibilities lead to the genuine examples with $b(G,H) = 3$ recorded in Table 1. For instance, suppose $G = \mathrm{L}_n(2).2$, $\Omega_n^+(2).2$, $E_6(2).2$ or $F_4(2).2$ and set $H_0 = H \cap G_0$. By [43, Lemma 3.13], H_0 has a unique regular orbit on $\mathrm{Syl}_2(G_0)$ with respect to the usual conjugation action. And since $N_{G_0}(H_0) = H_0$, it follows that H_0 has a unique regular orbit on G_0/H_0 and this implies that $b(G,H) > 2$ (indeed, if $b(G,H) = 2$ then H_0 would have at least $|H : H_0| = 2$ regular orbits on G_0/H_0).

By combining Zenkov's main theorem for almost simple groups in [43] (see Theorem 2 in Section 1) with [43, Lemma 3.18] (socle $\mathrm{L}_2(q)$) and the main results in [34] (socle $\mathrm{L}_3(q)$ or $\mathrm{U}_3(q)$) and [45] (simple groups), we see that it suffices to prove the following result.

Theorem 3.2. *Let G be an almost simple group of Lie type over $\mathbb{F}_q$ with socle G_0 and let H be a Sylow 2-subgroup of G. Assume that*

(i) *G_0 is not isomorphic to $\mathrm{L}_2(q)$, $\mathrm{L}_3(q)$ or $\mathrm{U}_3(q)$;*

(ii) *$|G : G_0|$ is even; and*

(iii) *Either $q = 9$, or q is a Mersenne or Fermat prime.*

Then $b(G,H) = 2$.

3.1. **Exceptional groups.**

Proposition 3.3. *The conclusion to Theorem 3.2 holds when G is an exceptional group of Lie type.*

Proof. First observe that the hypotheses in parts (ii) and (iii) of Theorem 3.2 imply that

$$G_0 \neq {}^2B_2(q),\ {}^2G_2(q)',\ {}^2F_4(q)'.$$

Set $\alpha = (q^2-1)_2$ and $\beta = \delta_{9,q}$ (so $\beta = 1$ if $q = 9$, otherwise $\beta = 0$). Note that $\alpha \leqslant 2(q+1)$.

Let $x \in G$ be an involution. Then by appealing to [16, Proposition 2.11], we see that $|x^G| > f_G(q)$, where $f_G(q)$ is defined as follows (with $\gamma = (q-1)/q$ and $\delta = (3, q-\varepsilon)^{-1}$):

G_0	$E_8(q)$	$E_7(q)$	$E_6^{\varepsilon}(q)$	$F_4(q)$	${}^3D_4(q)$	$G_2(q)$
$f_G(q)$	q^{112}	$\frac{1}{2}\gamma q^{54}$	$\gamma\delta q^{26}$	q^{16}	q^{14}	q^7

(4)

Let H be a Sylow 2-subgroup of G and set $H_0 = H \cap G_0$. As in (2), let $Q(G,H)$ be the probability that two random elements in $\Omega = G/H$ form a base for G and recall that $Q(G,H) \leqslant \widehat{Q}(G,H)$ as in (3), so it suffices to show that $\widehat{Q}(G,H) < 1$.

First assume $G_0 = E_8(q)$. Here Proposition 2.6 gives $|H_0| = 2^6\alpha^8$ and we deduce that $|H| \leqslant 2^{14+\beta}(q+1)^8 = a$. Since $|x^G| > f_G(q)$ for every involution $x \in G$, Lemma 2.3 implies that

$$\widehat{Q}(G,H) \leqslant a^2 f_G(q)^{-1} \tag{5}$$

and it is easy to check that this upper bound is less than 1 for all $q \geqslant 3$. Similarly, (5) holds in each of the remaining cases, where $f_G(q)$ is given in (4) and $a = 2^{c+\beta}(q+1)^d$ with

$$(c,d) = (10,7),\ (8,6),\ (7,4),\ (2,2),\ (3,2)$$

for $G_0 = E_7(q), E_6^{\varepsilon}(q), F_4(q), {}^3D_4(q), G_2(q)$, respectively. It is now a routine exercise to check that the upper bound in (5) is sufficient unless $G_0 = F_4(3)$, $G_2(5)$ or $G_2(3)$. Here the first two possibilities can be discarded since G is simple (recall that we may assume $|G : G_0|$ is even), while the latter case was handled in Proposition 2.8. □

3.2. **Classical groups.** In this section we complete the proof of Theorem A by establishing Theorem 3.2 for classical groups. Throughout, we will adopt the standard notation for classical groups given in [23]. In particular, we denote the simple orthogonal groups by $\mathrm{P}\Omega_n^{\varepsilon}(q)$, which differs from the notation for orthogonal groups used in the Atlas [17], for example.

Let G be an almost simple classical group over $\mathbb{F}_q$ as in the statement of Theorem 3.2. By combining the hypotheses of the theorem with the existence of well-known isomorphisms among some of the low-dimensional classical groups (see [23, Proposition 2.9.1], for example), we may assume G_0 is one of the following:

$\mathrm{L}_n(q)$, $\mathrm{U}_n(q)$	$n \geqslant 4$
$\mathrm{PSp}_n(q)$	$n \geqslant 4$ even
$\Omega_n(q)$	$n \geqslant 7$ odd, q odd
$\mathrm{P}\Omega_n^+(q)$, $\mathrm{P}\Omega_n^-(q)$	$n \geqslant 8$ even

We will sometimes refer to the 'type' of a subgroup L of G, which is intended to provide an approximate description of the structure of L. For example, if $G_0 = \mathrm{P}\Omega_{10}^+(q)$ then we may refer to a subgroup L of type $(\mathrm{O}_2^-(q) \wr S_4) \perp \mathrm{O}_2^+(q)$, which indicates that L is the stabiliser in G of an orthogonal decomposition

$$V = U \perp W = (U_1 \perp U_2 \perp U_3 \perp U_4) \perp W$$

of the natural module V for G_0, where each U_i is a 2-dimensional non-degenerate subspace of minus-type, and W is a non-degenerate 2-space of plus-type (recall that if $m = 2\ell$ is even, then an orthogonal m-space is of *plus-type* if it contains a totally singular ℓ-space, otherwise it is a *minus-type* space).

Finally, we refer the reader to [21, Table 4.5.1] and [14, Chapter 3] for detailed information on the conjugacy classes of involutions in $\mathrm{Aut}(G_0)$. As in the statement of Proposition 2.7, we will freely adopt the notation for involutions given in [21, Table 4.5.1].

Proposition 3.4. *The conclusion to Theorem 3.2 holds if* $G_0 = \mathrm{L}_n(q)$.

Proof. Let H be a Sylow 2-subgroup of G and set $H_0 = H \cap G_0$ and $\alpha = (q^2-1)_2$ as before. In addition, set $d = (n, q-1)$ and $\beta = \delta_{9,q}$.

Given an integer $1 \leqslant k \leqslant n/2$, we say that an involution $x \in G$ is of type t_k if it is conjugate in $\mathrm{PGL}_n(q)$ to $y = \hat{y}Z$, where $\hat{y} = (-I_k, I_{n-k}) \in \mathrm{GL}_n(q)$ is a diagonal matrix and Z is the centre of $\mathrm{GL}_n(q)$. This notation is consistent with [21, Table 4.5.1].

Case 1. n odd, $q \equiv 1 \pmod 4$

Here $n = 2m+1 \geqslant 5$ and either $q = 9$ or $q \in \{5, 17, 257, 65537, \ldots\}$ is a Fermat prime. In particular, $q-1$ is a 2-power and $\alpha = 2(q-1)$. As recorded in Table 3, we have

$$|H_0| = \alpha^m((q-1)_2)^m(m!)_2 = (q-1)^{n-1}((n-1)!)_2 = (q-1)^{n-1}(n!)_2$$

and it follows that H is contained in a subgroup L of G of type $\mathrm{GL}_1(q) \wr S_n$. The case $(n,q) = (5,9)$ was handled in Proposition 2.8, so we may assume $n \geqslant 7$ if $q = 9$.

Suppose $x \in G$ is a t_1-involution. Then

$$|x^G| = \frac{|\mathrm{GL}_n(q)|}{|\mathrm{GL}_{n-1}(q)||\mathrm{GL}_1(q)|} = \frac{q^{n-1}(q^n-1)}{q-1} = b_1 \tag{6}$$

and we claim that H contains at most $a_1 = n + \binom{n}{2}(q-1)$ such elements. To justify the claim, we will count the number of involutions of type $(I_1, -I_{n-1})$ in the subgroup $J = \mathrm{GL}_1(q) \wr S_n$ of $\mathrm{GL}_n(q)$. Visibly, there are $\binom{n}{1} = n$ such elements in the base group $B = \mathrm{GL}_1(q)^n$ of J. And if $x \in B\pi$ with $1 \neq \pi \in S_n$, then π is a transposition, x is B-conjugate to π and we have $|C_B(x)| = |\mathrm{GL}_1(q)|^{n-1}$. Since S_n contains $\binom{n}{2}$ transpositions, it follows that there are exactly $\binom{n}{2}(q-1)$ such involutions in $J \setminus B$, whence a_1 in J in total.

By Proposition 2.7, if $x \in G$ is a non-t_1 involution then

$$|x^G| \geqslant \frac{|\mathrm{GL}_n(q)|}{|\mathrm{GL}_{n-2}(q)||\mathrm{GL}_2(q)|} = \frac{q^{2n-4}(q^{n-1}-1)(q^n-1)}{(q^2-1)(q-1)} = b_2 \tag{7}$$

(minimal if x is a t_2-involution, using the fact that $(n,q) \neq (5,9)$) and we note that

$$|H| = |H_0||G:G_0|_2 \leqslant (q-1)^{n-1}((n-1)!)_2 2^{1+\beta} < 2^{n+\beta}(q-1)^{n-1} = a_2,$$

since $((n-1)!)_2 < 2^{n-1}$ by Lemma 2.5.

Then by applying Lemmas 2.1 and 2.3, we deduce that

$$Q(G,H) < a_1^2 b_1^{-1} + a_2^2 b_2^{-1} \tag{8}$$

and it is routine to check that this upper bound yields $Q(G,H) < 1$ and thus $b(G,H) = 2$.

Case 2. n odd, $q \equiv 3 \pmod 4$

Here $n = 2m+1 \geqslant 5$ and $q \in \{3, 7, 31, 127, 8191, \ldots\}$ is a Mersenne prime. Note that $q+1$ is a 2-power and $\alpha = 2(q+1)$. By inspecting Table 3,

$$|H_0| = \alpha^m((q-1)_2)^m(m!)_2 = (2\alpha)^m(m!)_2$$

and we deduce that H is contained in a subgroup L of G of type $(\mathrm{GL}_2(q) \wr S_m) \oplus \mathrm{GL}_1(q)$. Here L is the stabiliser in G of a direct sum decomposition of the natural module of the form

$$V = U \oplus W = (U_1 \oplus \cdots \oplus U_m) \oplus W,$$

where $\dim W = 1$ and each U_i is 2-dimensional. The case $(n,q) = (5,3)$ was handled in Proposition 2.8, so we may assume $q \geqslant 7$ when $n = 5$.

As in Case 1, if $x \in G$ is a t_1-involution then $|x^G| = b_1$ as in (6) and by counting the number of such elements in L we deduce that there are at most

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

such involutions in H. And for any other involution $x \in G$ we see that (7) holds and we note that $|H| \leqslant 2^{3m+1}(q+1)^m = a_2$. As before, the result now follows via the upper bound in (8).

Case 3. n even, $q \equiv 1 \pmod 4$

Here $n = 2m \geqslant 4$ and either $q = 9$ or q is a Fermat prime. From Table 3 we read off

$$|H_0| = \frac{1}{d}\alpha^m(q-1)^{m-1}(m!)_2 = \frac{1}{d}(q-1)^{n-1}(n!)_2$$

and we see that H is contained in a subgroup L of type $\mathrm{GL}_1(q) \wr S_n$.

For $n \geqslant 8$, we can now proceed as in Case 1 and we deduce that (8) holds, where a_1, b_1 and b_2 are defined as in Case 1, and we set $a_2 = 2^{n+1+\beta}(q-1)^{n-1}$. It is easy to check that the bound in (8) implies that $Q(G,H) < 1$ for all $n \geqslant 8$ and $q \geqslant 5$, so for the remainder of Case 3 we may assume $n = 4$ or 6.

Suppose $n = 6$ and note that $d = (n, q-1) = 2$. In view of Proposition 2.8, we may assume $q \geqslant 17$. As above, the contribution to $\widehat{Q}(G,H)$ from t_1-involutions is at most $a_1^2 b_1^{-1}$, where a_1 and b_1 are defined as before. As recorded in Proposition 2.7, if $x \in G$ is any other

involution then $|x^G|$ is minimal when x is a γ_1-type graph automorphism (rather than a t_2-involution) and thus

$$|x^G| \geqslant \frac{|G_0|}{|\mathrm{PSp}_6(q)|} = q^6(q^3-1)(q^5-1) = b_2.$$

In addition, we have $|H| \leqslant 2^{1+\beta}(q-1)^5(6!)_2 = 2^{5+\beta}(q-1)^5 = a_2$. It is now routine to check that the upper bound in (8) is sufficient.

Finally, let us assume $n = 4$. The groups with $q \in \{5, 9, 17\}$ were handled in Proposition 2.8, so we may assume $q \geqslant 257$. As usual, the contribution to $\widehat{Q}(G, H)$ from t_1-involutions is at most $a_1^2 b_1^{-1}$. If $x \in G$ is a γ_1 graph automorphism, then

$$|x^G| \geqslant \frac{|G_0|}{|\mathrm{PSp}_4(q)|} = \frac{1}{2}q^2(q^3-1) = b_2$$

and the proof of [13, Proposition 2.7] indicates that there are at most

$$a_2 = \frac{4!}{2!2^2}|\mathrm{GL}_1(q)| = 3(q-1)$$

such elements in L. And since q is a prime, we see that

$$|x^G| \geqslant \frac{|\mathrm{GL}_4(q)|}{2|\mathrm{GL}_2(q^2)|} = \frac{1}{2}q^4(q-1)(q^3-1) = b_3$$

for all other involutions $x \in G$. Now $|H| \leqslant 2^{1+\beta}(q-1)^3(4!)_2 = 2^{4+\beta}(q-1)^3 = a_3$, so

$$Q(G, H) < a_1^2 b_1^{-1} + a_2^2 b_2^{-1} + a_3^2 b_3^{-1} \tag{9}$$

and it is straightforward to check that this upper bound is less than 1 for all $q \geqslant 257$.

Case 4. n even, $q \equiv 3 \pmod 4$

Write $n = 2m \geqslant 4$ and note that q is a Mersenne prime. From Table 3 we read off

$$|H_0| = \frac{1}{2}\alpha^m(q-1)^{m-1}(m!)_2,$$

which allows us to conclude that H is contained in a subgroup L of type $\mathrm{GL}_2(q) \wr S_m$.

Let $x \in G$ be a t_1-involution and note that $|x^G| = b_1$, where b_1 is defined as in (6). We calculate that there are at most

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

such elements in L. If we now assume $n \geqslant 8$, then any other involution $x \in G$ satisfies the bound $|x^G| \geqslant b_2$ as in (7). So for $n \geqslant 8$ it follows that (8) holds with $a_2 = 2^{3m}(q+1)^m$ and we check that this bound yields $Q(G, H) < 1$ unless $(n, q) = (8, 3)$. But the latter case was handled in Proposition 2.8, so the proof is complete for $n \geqslant 8$.

Now assume $n = 6$. If $x \in G$ is a non-t_1 involution then $|x^G| \geqslant q^6(q^3-1)(q^5-1) = b_2$ as in Case 3. If we now take a_1 and b_1 as above, noting that $|H| \leqslant 2^7(q+1)^3 = a_2$ since $(3!)_2 = 2$, then the bound in (8) yields $Q(G, H) < 1$ for all $q \geqslant 7$ and we recall that the case $q = 3$ was treated in Proposition 2.8.

Finally, let us assume $n = 4$. Define a_1 and b_1 as above and set $b_2 = \frac{1}{2}q^2(q^3-1)$ as in Case 3 (for $n = 4$). Since $|H| \leqslant 2^5(q+1)^2 = a_2$, it follows that (8) holds and one checks that this upper bound yields $Q(G, H) < 1$ for all $q > 127$ (recall that q is a Mersenne prime, so the bound $q > 127$ implies that $q \geqslant 8191$). Finally, the result for $q \in \{3, 7, 31, 127\}$ can be checked computationally (see Proposition 2.8). □

Proposition 3.5. *The conclusion to Theorem 3.2 holds if $G_0 = \mathrm{U}_n(q)$.*

Proof. As in the proof of the previous proposition, let H be a Sylow 2-subgroup of G and set $H_0 = H \cap G_0$ and $\alpha = (q^2-1)_2$. Write $d = (n, q+1)$ and $\beta = \delta_{9,q}$.

For an integer $1 \leqslant k \leqslant n/2$, we say that $x \in G$ is of type t_k if it is conjugate in $\mathrm{PGU}_n(q)$ to $y = \hat{y}Z$, where $\hat{y} = (-I_k, I_{n-k}) \in \mathrm{GU}_n(q)$ is a diagonal matrix (with non-degenerate eigenspaces) and Z is the centre of $\mathrm{GU}_n(q)$. As before, this notation is consistent with [21, Table 4.5.1].

Case 1. n odd, $q \equiv 1 \pmod 4$

Write $n = 2m+1 \geqslant 5$ and note that $\alpha = 2(q-1)$. By inspecting Table 3, we see that

$$|H_0| = \alpha^m((q+1)_2)^m(m!)_2 = 2^{n-1}(q-1)^m(m!)_2$$

and hence H is contained in a subgroup L of G of type $(\mathrm{GU}_2(q) \wr S_m) \perp \mathrm{GU}_1(q)$. Here the notation indicates that L is the stabiliser in G of an orthogonal decomposition

$$V = U \perp W = (U_1 \perp \cdots \perp U_m) \perp W$$

of the natural module V for G_0, where W is a non-degenerate 1-space and each U_i is a non-degenerate 2-space.

Suppose $x \in G$ is a t_1-involution. Then

$$|x^G| = \frac{|\mathrm{GU}_n(q)|}{|\mathrm{GU}_{n-1}(q)||\mathrm{GU}_1(q)|} = \frac{q^{n-1}(q^n-(-1)^n)}{q+1} = b_1 \tag{10}$$

and by arguing as in the proof of Proposition 3.4 (see Case 2), we can show that there are at most

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

such involutions in L (and therefore at most a_1 in H itself). And if $x \in G$ is any other type of involution, then Proposition 2.7 gives

$$|x^G| \geqslant \frac{|\mathrm{GU}_n(q)|}{|\mathrm{GU}_{n-2}(q)||\mathrm{GU}_2(q)|} = \frac{q^{2n-4}(q^{n-1}-(-1)^{n-1})(q^n-(-1)^n)}{(q^2-1)(q+1)} = b_2 \tag{11}$$

(minimal if x is a t_2-involution). In addition, since $|G : G_0|_2 \leqslant 2^{1+\beta}$, we compute

$$|H| \leqslant 2^{n+\beta}(q-1)^m(m!)_2 < 2^{n+m+\beta}(q-1)^m = a_2.$$

Then the upper bound in (8) holds and it is easy to check that this gives $Q(G,H) < 1$ in all cases.

Case 2. n odd, $q \equiv 3 \pmod 4$

Here $n = 2m+1 \geqslant 5$, $\alpha = 2(q+1)$ and we note that

$$|H_0| = \alpha^m((q+1)_2)^m(m!)_2 = 2^m(q+1)^{n-1}(m!)_2 = (q+1)^{n-1}(n!)_2$$

(see Table 3). In particular, we deduce that H is contained in a subgroup L of G of type $\mathrm{GU}_1(q) \wr S_n$.

If $x \in G$ is a t_1-involution then (10) holds and by arguing as in the proof of Proposition 3.4 (see Case 1), we deduce that there are at most $a_1 = n + \binom{n}{2}(q+1)$ such involutions in H. And if $x \in G$ is any other type of involution, then (11) holds and we note that $|H| \leqslant 2^n(q+1)^{n-1} = a_2$. By defining b_1 and b_2 as in Case 1, we deduce that (8) holds and this gives $Q(G,H) < 1$ unless $(n,q) = (5,7)$, or if $q = 3$ and $n \leqslant 25$.

So to complete the proof in Case 2, we may assume $(n,q) = (5,7)$, or $q = 3$ and $5 \leqslant n \leqslant 25$. Firstly, by setting $a_2 = 2(q+1)^{n-1}(n!)_2$ we find that the upper bound in (8) is sufficient unless $q = 3$ and $n \leqslant 17$. In addition, we recall that the case $(n,q) = (5,3)$ was handled in Proposition 2.8, so we may assume $q = 3$ and $7 \leqslant n \leqslant 17$ is odd. To deal with the remaining cases, define a_1, b_1 and b_2 as above, and observe that there are no more than

$$\begin{aligned} a_2 &= \binom{n}{2} + \binom{n}{2}|\mathrm{GU}_1(q)| \cdot \binom{n-2}{1} + \frac{n!}{2!(n-4)!2^2}|\mathrm{GU}_1(q)|^2 \\ &= \frac{1}{2}n(n-1)\left(1 + (n-2)(q+1) + \frac{1}{4}(n-2)(n-3)(q+1)^2\right) \end{aligned} \tag{12}$$

involutions of type t_2 in L. By inspecting [21, Table 4.5.1], we note that if $x \in G$ is any other involution (that is to say, x is not a t_k-involution with $k = 1, 2$) then

$$|x^G| \geqslant \frac{|\mathrm{GU}_n(q)|}{|\mathrm{GU}_{n-3}(q)||\mathrm{GU}_3(q)|} > \frac{1}{2}\left(\frac{q}{q+1}\right) q^{6n-18} = b_3. \tag{13}$$

It follows that (9) holds with $a_3 = 2(q+1)^{n-1}(n!)_2$ and one checks that this upper bound is sufficient for all $n \geqslant 7$.

Case 3. n even, $q \equiv 1 \pmod 4$

Write $n = 2m \geqslant 4$ and note that $d = (n, q+1) = 2$. Then $\alpha = 2(q-1)$ and from Table 3 we get

$$|H_0| = \frac{1}{2}\alpha^m((q+1)_2)^{m-1}(m!)_2,$$

which means that H is contained in a subgroup L of G of type $\mathrm{GU}_2(q) \wr S_m$. Note that if $x \in G$ is a t_1-involution then (10) holds and by arguing as in the proof of Proposition 3.4 (see Case 4), we deduce that there are at most

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

such elements in H.

For now, let us assume $n \geqslant 8$. Then Proposition 2.7 implies that $|x^G| \geqslant b_2$ if x is any other involution in G, where b_2 is defined in (11). And since $|H| \leqslant 2^{3m+\beta}(q-1)^m = a_2$, we deduce that (8) holds, which in turn allows us to conclude that $Q(G, H) < 1$.

Now suppose $n = 6$. If $x \in G$ is a non-t_1 involution, then $|x^G| \geqslant b_2$, where

$$b_2 = \frac{|G_0|}{|\mathrm{Sp}_6(q)|} = q^6(q^3+1)(q^5+1) \tag{14}$$

(with equality possible if x is a γ_1 graph automorphism). It follows that (8) holds with $a_2 = 2^{2+\beta}|H_0| = 2^{7+\beta}(q-1)^3$ and one checks that this upper bound yields $Q(G, H) < 1$.

Finally, let us assume $n = 4$. The cases $q \in \{5, 9, 17\}$ were handled in Proposition 2.8, so we may assume $q \geqslant 257$ is a Fermat prime. Here $|H| \leqslant 2^5(q-1)^2 = a_2$ and we note that

$$|x^G| \geqslant \frac{|G_0|}{|\mathrm{Sp}_4(q)|} = \frac{1}{2}q^2(q^3+1) = b_2$$

for every non-t_1 involution $x \in G$ (see Proposition 2.7). It follows that (8) holds and we get $Q(G, H) < 1$ for all $q > 257$ (recall that q is a Fermat prime, so the bound $q > 257$ implies that $q \geqslant 65537$).

So to complete the argument, suppose $G_0 = \mathrm{U}_4(q)$ with $q = 257$. Without loss of generality, we may assume $G = \mathrm{Aut}(G_0) = G_0.2^2$. As before, the contribution to $\widehat{Q}(G, H)$ from t_1-involutions is at most $a_1^2 b_1^{-1}$, where a_1 and b_1 are defined as above. Also observe that if $x \in G$ is an involution, which is not of type t_1 nor γ_1, then

$$|x^G| \geqslant \frac{|\mathrm{GU}_4(q)|}{2|\mathrm{GU}_2(q)|^2} = \frac{1}{2}q^4(q^2-q+1)(q^2+1) = f(q) \tag{15}$$

(minimal if x is a t_2-involution). Set $G_1 = \mathrm{PGU}_4(q) = G_0.2$ and $H_1 = H \cap G_1$, so we have $|H : H_1| = 2$. If $x \in H$ is a γ_1 graph automorphism, then $|x^G| = q^2(q^3+1) = b_2$ and we note that every graph automorphism in H is contained in the coset $H_1 x$, so there are at most $|H_1| = 2^{20} = a_2$ such elements in H. Then by setting $a_3 = |H| = 2^{21}$ and $b_3 = f(q)$, we deduce that (9) holds and this is good enough to force $Q(G, H) < 1$.

Case 4. n even, $q \equiv 3 \pmod 4$

Here we have $n = 2m \geqslant 4$, $\alpha = 2(q+1)$ and by inspecting Table 3 we get

$$|H_0| = \frac{1}{d}\alpha^m(q+1)^{m-1}(m!)_2 = \frac{1}{d}(q+1)^{n-1}(n!)_2.$$

Then H is contained in a subgroup L of G of type $\mathrm{GU}_1(q) \wr S_n$. As usual, if $x \in G$ is a t_1-involution then $|x^G| = b_1$, where b_1 is given in (10), and it is easy to check that there are at most $a_1 = n + \binom{n}{2}(q+1)$ such elements in L (and therefore in H as well).

Suppose $n \geqslant 10$. If $x \in G$ is a t_2-involution then $|x^G| = b_2$, where b_2 is defined in (11), and we see that there are at most a_2 such elements in H, where a_2 is defined in (12). And if $x \in G$ is any other involution (that is, if x is not a t_k-involution for $k = 1$ or 2) then $|x^G|$ is minimal when x is a t_3-involution and thus $|x^G| > b_3$, where b_3 is defined in (13). Then by setting $a_3 = 2^{n+1}(q+1)^{n-1}$ we deduce that (9) holds and the result follows.

The case $n = 8$ is entirely similar. The only difference is that if $x \in G$ is an involution, which is not of type t_1 or t_2, then $|x^G|$ is minimal when x is a γ_1 graph automorphism. This means that

$$|x^G| \geqslant \frac{|G_0|}{|\mathrm{Sp}_8(q)|} \geqslant \frac{1}{8}q^{12}(q^3+1)(q^5+1)(q^7+1) = b_3$$

and one checks that the upper bound in (9) is sufficient for all $q \geqslant 7$. This completes the argument because the case $G_0 = \mathrm{U}_8(3)$ was handled in Proposition 2.8.

Next assume $n = 6$. The case $q = 3$ is treated in Proposition 2.8, so we may assume $q \geqslant 7$. As usual, the contribution to $\widehat{Q}(G,H)$ from t_1-involutions is at most $a_1^2 b_1^{-1}$, where a_1 and b_1 are defined as above. And if $x \in G$ is any other involution, then $|x^G| \geqslant b_2$, where b_2 is defined in (14). Since $|H| \leqslant 2^5(q+1)^5 = a_2$, we deduce that (8) holds and the result follows for all $q \geqslant 31$.

So to complete the proof for $G_0 = \mathrm{U}_6(q)$, we may assume $q = 7$. If $x \in G$ is a γ_1 involution then $|x^G| = b_2$ as in (14) and by appealing to the proof of [13, Proposition 2.7] we deduce that there are at most

$$a_2 = \frac{6!}{3!2^3} \cdot |\mathrm{GU}_1(q)|^2 = 15(q+1)^2$$

such elements in L (and hence at most this number in H). And if $x \in G$ is an involution, which is not of type t_1 or γ_1, then $|x^G|$ is minimal when x is of type t_2 and thus

$$|x^G| \geqslant \frac{|\mathrm{GU}_6(q)|}{|\mathrm{GU}_4(q)||\mathrm{GU}_2(q)|} = \frac{q^8(q^5+1)(q^6-1)}{(q^2-1)(q+1)} = b_3.$$

Since $|H_0| = 2^{18}$ it follows that $|H| \leqslant 2^{20} = a_3$ and the bound in (9) is satisfied. This forces $Q(G,H) < 1$ and the result follows.

Finally, let us assume $n = 4$ and define a_1 and b_1 as above. If $x \in G$ is a γ_1 involution, then $|x^G| \geqslant \frac{1}{2}q^2(q^3+1) = b_2$ and by inspecting the proof of [13, Proposition 2.7] we calculate that there are no more than $a_2 = 3(q+1)$ such elements in H. And if $x \in G$ is any other involution (neither a t_1 nor a γ_1 involution), then $|x^G| \geqslant b_3 = f(q)$ as defined in (15) and we note that $|H| \leqslant 2^4(q+1)^3 = a_3$. Then (9) holds and the reader can check that this bound gives $Q(G,H) < 1$ for all $q \geqslant 31$. This completes the proof since the cases $q = 3, 7$ were handled in Proposition 2.8. □

Proposition 3.6. *The conclusion to Theorem 3.2 holds if* $G_0 = \mathrm{PSp}_n(q)$.

Proof. Here $n = 2m \geqslant 4$ and we set $H_0 = H \cap G_0$ and $\alpha = (q^2-1)_2$ as before, where H is a Sylow 2-subgroup of G. As in [21, Table 4.5.1], we say that an involution $x \in G$ is of type t_1 if it is G_0-conjugate to $y = \hat{y}Z$, where $\hat{y} = (-I_2, I_{n-2}) \in \mathrm{Sp}_n(q)$ is a diagonal matrix (with non-degenerate eigenspaces) and Z is the centre of $\mathrm{Sp}_n(q)$. As usual, set $\beta = \delta_{9,q}$.

Case 1. $n \geqslant 6$

By inspecting Table 3, we see that $|H_0| = \frac{1}{2}\alpha^m(m!)_2$ and thus H is contained in a subgroup L of G of type $\mathrm{Sp}_2(q) \wr S_m$. In particular, if x is a t_1-involution, 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 at most

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

such elements in H.

First assume $n \geqslant 10$. If $x \in G$ is a non-t_1 involution, then Proposition 2.7 implies that

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

In addition, $|H| \leqslant 2^{n+\beta}(q+1)^m = a_2$ and one can check that the upper bound in (8) is good enough unless $(n,q) = (10,3)$. But the latter case was handled in Proposition 2.8, so the result follows.

Similarly, if $n = 8$ and x is a non-t_1 involution, then

$$|x^G| \geqslant \frac{|\mathrm{Sp}_8(q)|}{2|\mathrm{Sp}_4(q^2)|} = \frac{1}{2}q^8(q^2-1)(q^6-1) = b_2$$

and we have $|H| \leqslant 2^{7+\beta}(q+1)^4 = a_2$. Then (8) holds and we immediately deduce that $Q(G,H) < 1$ if $q \geqslant 5$. This completes the argument since we treated the case $G_0 = \mathrm{PSp}_8(3)$ in Proposition 2.8.

Next assume $n = 6$. If x is a non-t_1 involution, then

$$|x^G| \geqslant \frac{|\mathrm{Sp}_6(q)|}{2|\mathrm{GU}_3(q)|} = \frac{1}{2}q^6(q-1)(q^2+1)(q^3-1) = b_2$$

(see Proposition 2.7) and we note that $|H| \leqslant 2^{4+\beta}(q+1)^3 = a_2$. Then (8) holds and we deduce that $Q(G,H) < 1$ for all $q \geqslant 5$. This just leaves the case $G_0 = \mathrm{PSp}_6(3)$, which was handled in Proposition 2.8.

Case 2. $n = 4$

For the remainder of the proof, we may assume $n = 4$. The groups with $q \leqslant 17$ can be handled using Magma (see Proposition 2.8), so we may assume $q \geqslant 31$ is a Fermat or Mersenne prime. In particular, $G = \mathrm{PGSp}_4(q) = G_0.2$. Write $G_0 = L/Z$ and $H_0 = J/Z$, where Z is the centre of $L = \mathrm{Sp}_4(q)$, and note that

$$J = Q_{2(q-\varepsilon)} \wr S_2 < \mathrm{Sp}_2(q) \wr S_2$$
$$H = D_{2(q-\varepsilon)} \wr S_2,$$

where $\varepsilon = 1$ if $q \equiv 1 \pmod 4$, otherwise $\varepsilon = -1$ (here $Q_{2(q-\varepsilon)}$ denotes the quaternion group of order $2(q-\varepsilon)$). In particular, $|H| = 8(q-\varepsilon)^2$. Given a finite group X, we recall that $i_2(X)$ denotes the number of involutions in X.

To begin with, we will assume $q \equiv 1 \pmod 4$, so $q \geqslant 257$ is a Fermat prime and

$$i_2(H) = (q+1)^2 - 1 + 2(q-1) = q^2 + 4q - 2.$$

There are four G-classes of involutions, with representatives labelled t_1, t_2, t_1' and t_2' in [21, Table 4.5.1]. Here $t_1, t_2 \in G_0$ and $t_1', t_2' \in G \setminus G_0$. It will be useful to note that the involutions of type t_1 lift to involutions in L, whereas those of type t_2 lift to elements of order 4.

Suppose $x \in G$ 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 we note that $x = \hat{x}Z \in L/Z$ with $\hat{x} \in L$ an involution of type $(-I_2, I_2)$. Now

$$i_2(J) = 2q + |Z| - 1 = 2q + 1$$

since $Q_{2(q-1)}$ has a unique involution, and we deduce that exactly q involutions in H_0 lift to an involution in J. This means that H contains $a_1 = q$ involutions of type t_1. Similarly, we calculate that there are precisely $q^2 + 4q - 1$ elements $y \in J$ of order 4 with $y^2 \in Z$ and this allows us to conclude that H contains $(q^2 + 4q - 1)/2$ involutions of type t_2.

Now let $x \in G$ be an involution of type t_1' in the notation of [21, Table 4.5.1]. Here $x \in G \setminus G_0$ and

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

Moreover, our previous calculations show that there are at most

$$a_2 = i_2(H) - q - \frac{1}{2}(q^2+4q-1) = \frac{1}{2}(q^2+2q-3)$$

such involutions in H.

Now, if $x \in G$ is an involution of type t_2 or t_2', then

$$|x^G| \geqslant \frac{|\mathrm{Sp}_4(q)|}{2|\mathrm{GU}_2(q)|} = \frac{1}{2}q^3(q-1)(q^2+1) = b_3$$

and we note that $|H| = 8(q-1)^2 = a_3$. It follows that (9) holds and we conclude that $Q(G,H) < 1$ for all $q \geqslant 257$.

A very similar argument applies when $q \equiv 3 \pmod 4$. Here the involutions in G of type t_1 and t_2' are contained in G_0, whereas those of type t_1' and t_2 are in $G \setminus G_0$. Since $H = D_{2(q+1)} \wr S_2$ we compute

$$i_2(H) = (q+3)^2 - 1 + 2(q+1) = q^2 + 8q + 10$$

and as before we calculate that H contains $a_1 = q+2$ involutions of type t_1. By counting the elements $y \in J$ of order 4 with $y^2 \in Z$, we deduce that there are $(q^2+8q+11)/2$ involutions of type t_2' in H. As a consequence, it follows that H contains at most

$$a_2 = i_2(H) - (q+2) - \frac{1}{2}(q^2+8q+11) = \frac{1}{2}(q^2+6q+5)$$

involutions of type t_1'. Putting this together, we deduce that (9) holds with $a_3 = 8(q+1)^2$ and a_1, a_2, b_1, b_2, b_3 defined as above. It is now easy to check that this upper bound on $Q(G,H)$ is less than 1 for all $q \geqslant 31$. □

Proposition 3.7. *The conclusion to Theorem 3.2 holds if $G_0 = \Omega_n(q)$.*

Proof. Here $n = 2m+1 \geqslant 7$ and we set $H_0 = H \cap G_0$, where H is a Sylow 2-subgroup of G. For $k \in \{1,2\}$, we will say that an involution $x \in \mathrm{SO}_n(q) = G_0.2$ is of type s_k if it is conjugate to an element of the form $(-I_{n-1}, I_1)$ for $k=1$, or $(-I_2, I_{n-2})$ for $k=2$ (in the notation of [21, Table 4.5.1], these are the involutions of type t_m or t_m' (for $k=1$), and type t_1 or t_1' (for $k=2$)). Note that if $x \in G$ is an involution of type s_1 then

$$|x^G| \geqslant \frac{|\mathrm{SO}_n(q)|}{2|\mathrm{SO}^-_{n-1}(q)|} = \frac{1}{2}q^m(q^m-1) = b_1. \tag{16}$$

And similarly, if x is an s_2-type involution then

$$|x^G| \geqslant \frac{|\mathrm{SO}_n(q)|}{2|\mathrm{SO}_{n-2}(q)||\mathrm{SO}^-_2(q)|} = \frac{q^{n-2}(q^{n-1}-1)}{2(q+1)} = b_2. \tag{17}$$

As recorded in Table 3, we have $|H_0| = \frac{1}{2}\alpha^m(m!)_2$, where $\alpha = (q^2-1)_2$. Let V be the natural module for G_0. As before, set $\beta = \delta_{9,q}$.

Case 1. $q \equiv 1 \pmod 4$

First we assume $q \equiv 1 \pmod 4$, so $|H_0| = \frac{1}{2}(2(q-1))^m(m!)_2$ and we note that H is contained in a subgroup L of G of type

$$(\mathrm{O}^+_2(q) \wr S_m) \perp \mathrm{O}_1(q) < \mathrm{O}^+_{2m}(q) \perp \mathrm{O}_1(q).$$

Note that L is the stabiliser in G of an orthogonal decomposition of the form

$$V = U \perp W = (U_1 \perp U_2 \perp \cdots \perp U_m) \perp W,$$

where each U_i is a 2-dimensional non-degenerate orthogonal space of plus-type and W is a non-degenerate 1-space (recall that a 2-dimensional orthogonal space is of *plus-type* if

it contains a non-zero singular vector with respect to the defining quadratic form). In particular, if $G = \mathrm{SO}_n(q) = G_0.2$, then

$$L = D_{2(q-1)} \wr S_m = \mathrm{O}_2^+(q) \wr S_m < \mathrm{O}_{2m}^+(q) < G.$$

Let $x \in G$ be an s_1-type involution, so $|x^G| \geqslant b_1$ as in (16). Working in L, and noting that $D_{2(q-1)}$ has exactly $q-1$ non-central involutions, we calculate that H contains at most

$$a_1 = \binom{m}{1}(q-1) + 1 = m(q-1) + 1$$

such elements. And if $x \in G$ is any other type of involution, then Proposition 2.7 implies that $|x^G| \geqslant b_2$ with b_2 defined as in (17) and we note that $|H| \leqslant 2^{n-1+\beta}(q-1)^m = a_2$. It follows that $Q(G,H)$ satisfies the upper bound in (8) and this allows us to deduce that $Q(G,H) < 1$ unless $(n,q) \in \{(7,5),(7,9),(9,5)\}$. In the latter cases, by setting $a_2 = 2^{m+\beta}(q-1)^m(m!)_2$, one can check that (8) is sufficient.

Case 2. $q \equiv 3 \pmod 4$

Here $|H_0| = \frac{1}{2}(2(q+1))^m(m!)_2$ and H is contained in a subgroup L of G of type

$$(\mathrm{O}_2^-(q) \wr S_m) \perp \mathrm{O}_1(q) < \mathrm{O}_{2m}^\varepsilon(q) \perp \mathrm{O}_1(q),$$

where $\varepsilon = +$ if m is even, otherwise $\varepsilon = -$. By arguing as in Case 1, we deduce that the contribution to $\widehat{Q}(G,H)$ from s_1-involutions is at most $a_1^2 b_1^{-1}$, where $a_1 = m(q+1)+1$ and b_1 is defined in (16). And if $x \in G$ is an s_2-type involution, then $|x^G| \geqslant b_2$ as above and we note that $|H| \leqslant 2^{n-1}(q+1)^m = a_2$. Then as in Case 1, we deduce that (8) holds and for $q \geqslant 7$ we check that this bound is sufficient unless $q = 7$ and $n \in \{7,9,11\}$. But in each of these cases, by setting $a_2 = 2^m(q+1)^m(m!)_2$, we obtain $Q(G,H) < 1$ via (8).

Now suppose $q = 3$. In view of Proposition 2.8, we may assume $n \geqslant 15$. Here we need a more accurate estimate for the number of s_2-involutions in H. By working in L, we calculate that there are at most a_2 such elements, where

$$\begin{aligned} a_2 &= \binom{m}{1} + \binom{m}{1}(q+1) + \binom{m}{2}(q+1)^2 + \binom{m}{2}|\mathrm{O}_2^-(q)| \\ &= m(q+2) + \frac{1}{2}m(m-1)\left((q+1)^2 + 2(q+1)\right). \end{aligned}$$

And if $x \in G$ is an involution, which is not of type s_1 or s_2, then it is easy to see that

$$|x^G| \geqslant \frac{|\mathrm{SO}_n(q)|}{2|\mathrm{SO}_{n-3}^-(q)||\mathrm{SO}_3(q)|} > \frac{1}{4}q^{3n-9} = b_3.$$

Setting $a_3 = 2^{n-1}(q+1)^m$, it follows that (9) holds and one can check that this upper bound is sufficient if $n \geqslant 17$. Finally, if $n = 15$ then $(m!)_2 = 2^4$ and so we can set $a_3 = 2^{11}(q+1)^7$ in (9) and we deduce that $Q(G,H) < 1$ as required. □

Proposition 3.8. *The conclusion to Theorem 3.2 holds if* $G_0 = \mathrm{P}\Omega_n^+(q)$.

Proof. Here $n = 2m \geqslant 8$ and as usual we set $H_0 = H \cap G_0$, where H is a Sylow 2-subgroup of G. Set $d = (4, q^m - 1)$ and $\beta = \delta_{9,q}$.

For $k \in \{1,2\}$, we say that an involution $x \in \mathrm{PO}_n^+(q)$ is of type s_k if it lifts to an involution in $\mathrm{O}_n^+(q)$ of the form $(-I_{n-k}, I_k)$. If x is an s_1-type involution, then $x \in \mathrm{PO}_n^+(q) \setminus \mathrm{PSO}_n^+(q)$ is an involutory graph automorphism of G_0 (of type γ_1 in [21, Table 4.5.1]) and we have

$$|x^G| \geqslant \frac{|\mathrm{SO}_n^+(q)|}{2|\mathrm{SO}_{n-1}(q)|} = \frac{1}{2}q^{m-1}(q^m - 1) = b_1. \tag{18}$$

Similarly, if x is an s_2-involution then

$$|x^G| \geqslant \frac{|\mathrm{SO}_n^+(q)|}{2|\mathrm{SO}_{n-2}^-(q)||\mathrm{SO}_2^-(q)|} = \frac{q^{n-2}(q^m-1)(q^{m-1}-1)}{2(q+1)} = b_2. \tag{19}$$

Recall that $\mathrm{Inndiag}(G_0)$ is the index-two subgroup of $\mathrm{PGO}_n^+(q)$ generated by the inner and diagonal automorphisms of G_0.

Case 1. $q \equiv 1 \pmod 4$

Here $d = 4$ and we first observe that

$$|H_0| = \frac{1}{8}(2(q-1))^m (m!)_2,$$

which means that H is contained in a subgroup L of G of type $\mathrm{O}_2^+(q) \wr S_m$.

To begin with, let us assume $n \geqslant 10$. If $x \in G$ is an s_1-type involution, then $|x^G| \geqslant b_1$ as in (18) and by counting in L we deduce that there are at most $a_1 = m(q-1)$ such elements in H. Similarly, if x is an s_2-type involution, then $|x^G| \geqslant b_2$ (see (19)) and we calculate that H contains no more than a_2 such involutions, where

$$a_2 = \binom{m}{1} + \binom{m}{2}(q-1)^2 + \binom{m}{2}|\mathrm{O}_2^+(q)| = m + \frac{1}{2}m(m-1)((q-1)^2 + 2(q-1)).$$

And if $x \in G$ is any other type of involution, then by inspecting [21, Table 4.5.1] we deduce that $|x^G|$ is minimal when x is an involutory graph automorphism of type $(-I_3, I_{n-3})$. So in this situation we get

$$|x^G| \geqslant \frac{|\mathrm{SO}_n^+(q)|}{2|\mathrm{SO}_{n-3}(q)||\mathrm{SO}_3(q)|} > \frac{1}{4}q^{3n-9} = b_3 \tag{20}$$

and we note that $|H| \leqslant 2^{n+\beta}(q-1)^m = a_3$. Putting all of this together, we deduce that (9) holds and this implies that $Q(G,H) < 1$. The result follows.

Now assume $n = 8$ and $q \equiv 1 \pmod 4$. To begin with, we will assume $q \geqslant 5$ is a Fermat prime, noting that a separate argument for $q = 9$ will be given below.

As above, the contribution to $\widehat{Q}(G,H)$ from s_1-involutions is at most $a_1^2 b_1^{-1}$. Next suppose $x \in G$ is an s_2-involution and recall that $|x^G| \geqslant b_2$. If $C_G(x)$ is of type $\mathrm{O}_6^\varepsilon(q) \times \mathrm{O}_2^\varepsilon(q)$, then x is conjugate under a triality graph automorphism τ of G_0 to an involution y with $C_G(y)$ of type $\mathrm{GL}_4^\varepsilon(q)$. And in turn, $z = y^\tau$ is contained in a second $\mathrm{Inndiag}(G_0)$-class of involutions with $C_G(z)$ of type $\mathrm{GL}_4^\varepsilon(q)$. Since the number of s_2-involutions in H is at most $4 + 6(q-1)^2 + 12(q-1)$, as noted above, it follows that there are no more than

$$a_2 = 3(4 + 6(q-1)^2 + 12(q-1))$$

involutions $x \in H$ with $C_G(x)$ of type $\mathrm{O}_6^\varepsilon(q) \times \mathrm{O}_2^\varepsilon(q)$ or $\mathrm{GL}_4^\varepsilon(q)$ for $\varepsilon = \pm$. And if x is any other involution, then the fact that q is a prime (so G does not contain any involutory field or graph-field automorphisms) implies that

$$|x^G| \geqslant \frac{|\mathrm{SO}_8^+(q)|}{2|\mathrm{SO}_5(q)||\mathrm{SO}_3(q)|} = \frac{1}{2}q^7(q^2+1)(q^6-1) = b_3 \tag{21}$$

as in (20). Finally, since $|H| \leqslant 2^7(q-1)^4 = a_3$ we deduce that (9) holds and this upper bound yields $Q(G,H) < 1$, as required.

To complete the proof for $n = 8$ with $q \equiv 1 \pmod 4$, we may assume $q = 9$. The analysis of this case is complicated by the fact that G may contain involutory field or graph-field automorphisms. Using Magma [7], we begin by constructing $L = \mathrm{Aut}(G_0) = G_0.[48]$ as a permutation group of degree 1795800 and we construct a Sylow 2-subgroup J of L. We then take a set of representatives of the conjugacy classes of involutions in J and we deduce that $i_2(J) = 14495$. In addition, by computing $|x^L|$ for each involution $x \in J$, we find that J contains exactly $a_1 = 32$ involutions of type s_1. As before, if x is any other involution in G, then $|x^G| \geqslant b_2$ as in (19). So by applying Lemma 2.3, we see that (8) holds with b_1 defined in (18) and $a_2 = 14463$. It is easy to check that this estimate gives $Q(G,H) < 1$ and the result follows.

Case 2. $q \equiv 3 \pmod 4$

First assume m is even and note that

$$|H_0| = \frac{1}{2d}(2(q+1))^m(m!)_2.$$

It follows that H is contained in a subgroup L of G of type $\mathrm{O}_2^-(q) \wr S_m$, which means that the analysis of this case is almost identical to our previous work in Case 1.

First assume $n \geqslant 12$. Here we see that (9) holds, where

$$a_1 = m(q+1),\ a_2 = \frac{1}{2}m(m-1)((q+1)^2 + 2(q+1)) + m,\ a_3 = 2^n(q+1)^m$$

and b_1, b_2 and b_3 are defined in (18), (19) and (20), respectively. Then one can check that this upper bound is sufficient unless $q = 3$ and $n \in \{12, 16, 20\}$. The case $(n, q) = (12, 3)$ was handled in Proposition 2.8. For $(n, q) = (20, 3)$ we have $|H| \leqslant 2^{18}4^{10}$ since $(10!)_2 = 2^8$ and by setting $a_3 = 2^{18}4^{10}$ we check that the revised bound in (9) is good enough.

Finally, suppose $(n, q) = (16, 3)$. We may assume $G = \mathrm{PGO}_{16}^+(3) = G_0.D_8$. Set $H_1 = H \cap \mathrm{Inndiag}(G_0)$ and note that $|H : H_1| = 2$. If $x \in H$ is an involutory graph automorphism of type $(-I_3, I_{13})$, then

$$|x^G| \geqslant \frac{|\mathrm{SO}_{16}^+(3)|}{2|\mathrm{SO}_{13}(3)||\mathrm{SO}_3(3)|} = 2279214355760562960 = b_3$$

and we note that all such involutions are contained in the coset H_1x, so there are at most $|H_1| = 2^{30} = a_3$ such elements in H. And if $x \in G$ is an involution that is not of type s_1 or s_2, nor a graph automorphism of type $(-I_3, I_{13})$, then

$$|x^G| \geqslant \frac{|\mathrm{SO}_{16}^+(3)|}{2|\mathrm{SO}_{12}^-(3)||\mathrm{SO}_4^-(3)|} = 40320213639146662987584 = b_4.$$

We deduce that

$$Q(G, H) < a_1^2b_1^{-1} + a_2^2b_2^{-1} + a_3^2b_3^{-1} + a_4^2b_4^{-1} < 1,$$

where $a_4 = |H| = 2^{31}$, and the result follows.

Now assume $n = 8$. In view of Proposition 2.8, we are free to assume that $q \geqslant 7$. Then by arguing as in Case 1, we deduce that (9) holds, where b_1 and b_2 are defined as above, b_3 is given in (21), and we set

$$a_1 = 4(q+1),\ a_2 = 18((q+1)^2 + 2(q+1)) + 12,\ a_3 = 2^7(q+1)^4,$$

noting that $|H| \leqslant a_3$. It is easy to check that this yields $Q(G, H) < 1$ for all $q \geqslant 7$ and the result follows.

To complete the proof, we may assume $m \geqslant 5$ is odd. Here

$$|H_0| = (2(q+1))^{m-1}((m-1)!)_2$$

and we deduce that H is contained in a subgroup L of G of type

$$(\mathrm{O}_2^-(q) \wr S_{m-1}) \perp \mathrm{O}_2^+(q) < \mathrm{O}_{n-2}^+(q) \perp \mathrm{O}_2^+(q).$$

If $x \in G$ is an s_1-involution, then $|x^G| \geqslant b_1$ as in (18) and by working in L we deduce that there are at most

$$a_1 = \binom{m-1}{1}(q+1) + q - 1 = m(q+1) - 2$$

such elements in H. Similarly, if x is an s_2-involution then $|x^G| \geqslant b_2$ with b_2 defined as in (19) and we calculate that H contains no more than a_2 such elements, where

$$\begin{aligned} a_2 &= \binom{m-1}{1} + \binom{m-1}{1}(q+1)(q-1) + \binom{m-1}{2}(q+1)^2 + \binom{m-1}{2}|\mathrm{O}_2^-(q)| + 1 \\ &= \frac{1}{2}(m-1)(m-2)((q+1)^2 + 2(q+1)) + (m-1)q^2 + 1. \end{aligned}$$

And if $x \in G$ is any other type of involution, then as in (20) we have $|x^G| > \frac{1}{4}q^{3n-9} = b_3$ and we note that $|H| \leqslant 2^n(q+1)^{m-1} = a_3$. Then one checks that the upper bound in (9) is

sufficient unless $q = 3$ and $n \in \{10, 14\}$. The case $(n, q) = (10, 3)$ was handled in Proposition 2.8. And for $(n, q) = (14, 3)$ we have $|H| \leqslant 2^{24}$; by setting $a_3 = 2^{24}$ we find that the bound in (9) is good enough and the proof is complete. □

Proposition 3.9. *The conclusion to Theorem 3.2 holds if* $G_0 = \mathrm{P}\Omega_n^-(q)$.

Proof. Here $n = 2m \geqslant 8$ is even. Let H be a Sylow 2-subgroup of G and set $H_0 = H \cap G_0$, $d = (4, q^m + 1)$ and $\beta = \delta_{9,q}$.

For $k \in \{1, 2\}$, we define an involution $x \in \mathrm{PO}_n^-(q)$ to be of type s_k if it lifts to an involution in $\mathrm{O}_n^-(q)$ of the form $(-I_{n-k}, I_k)$. If x is of type s_1, then

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

and we get

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

if x is of type s_2. As in the proof of the previous proposition, we divide the analysis into two cases, according to whether or not $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$.

Case 1. $q \equiv 1 \pmod 4$

Here $d = 2$ and

$$|H_0| = (2(q - 1))^{m-1}((m - 1)!)_2,$$

which means that $H < L < G$, where L is of type

$$(\mathrm{O}_2^+(q) \wr S_{m-1}) \perp \mathrm{O}_2^-(q) < \mathrm{O}_{n-2}^+(q) \perp \mathrm{O}_2^-(q).$$

Then by arguing as in Case 2 (with m odd) in the proof of Proposition 3.8, we calculate that H contains at most $a_1 = m(q - 1) + 2$ involutions of type s_1 and at most

$$a_2 = \frac{1}{2}(m - 1)(m - 2)((q - 1)^2 + 2(q - 1)) + (m - 1)q^2 + 1$$

involutions of type s_2. And if $x \in G$ is any other type of involution, then $|x^G| > \frac{1}{4}q^{3n-9} = b_3$ as in (20) and we note that $|H| \leqslant 2^{n+\beta}(q - 1)^{m-1} = a_3$. It is now routine to check that the upper bound in (9) is sufficient.

Case 2. $q \equiv 3 \pmod 4$

First assume m is even. Here $|H_0| = (2(q + 1))^{m-1}((m - 1)!)_2$ and thus H is contained in a subgroup of type

$$(\mathrm{O}_2^-(q) \wr S_{m-1}) \perp \mathrm{O}_2^+(q) < \mathrm{O}_{n-2}^-(q) \perp \mathrm{O}_2^+(q).$$

Then by arguing as in Case 1, setting b_1, b_2 and b_3 as above, we deduce that (9) holds with

$$a_1 = m(q + 1) - 2,\ a_2 = \frac{1}{2}(m - 1)(m - 2)((q + 1)^2 + 2(q + 1)) + (m - 1)q^2 + 1$$

and $a_3 = 2^{n-1}(q + 1)^{m-1}$. It is easy to check that this bound is sufficient unless $q = 3$ and $n \in \{8, 12\}$. The latter two cases were handled in Proposition 2.8 and the result follows.

Finally, suppose m is odd. In this case we have

$$|H_0| = \frac{1}{8}(2(q + 1))^m(m!)_2$$

and thus $H < L < G$ with L of type $\mathrm{O}_2^-(q) \wr S_m$. And so by arguing as in Case 2 (with m even) in the proof of Proposition 3.8, we deduce that (9) holds, where b_1, b_2, b_3 are defined as above and

$$a_1 = m(q + 1),\ a_2 = \frac{1}{2}m(m - 1)((q + 1)^2 + 2(q + 1)) + m,\ a_3 = 2^{n-1}(q + 1)^m.$$

We then check that this bound is sufficient unless $q = 3$ and $n \in \{10, 14, 18\}$. For $(n, q) = (10, 3)$ we can appeal to Proposition 2.8. And in the two remaining cases, by setting $a_3 = 2^{3m}(m!)_2$, we can check that the bound in (9) is good enough. The result follows. □

This completes the proof of Theorem 3.2. By combining this result with Theorem 2, we conclude that the proof of Theorem A is complete.

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] R.F. Bailey and P.J. Cameron, *Base size, metric dimension and other invariants of groups and graphs*, Bull. Lond. Math. Soc. **43** (2011), 209–242.

[3] 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.

[4] A.A. Baykalov, *Base sizes for finite linear groups with solvable stabilisers*, J. Group Theory **28** (2025), 1003–1077.

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

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

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

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

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

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

[11] T.C. Burness, *Simple groups, fixed point ratios and applications*, in Local representation theory and simple groups, 267–322, EMS Ser. Lect. Math., Eur. Math. Soc., Zürich, 2018.

[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 of finite classical groups, III*, J. Algebra **314** (2007), 693–748.

[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 H.Y. Huang, *On the intersections of nilpotent subgroups in simple groups*, submitted (arXiv:2508.03479), 2025.

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

[17] 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.

[18] 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*, J. Algebra **689** (2026), 62–86.

[19] S. Dolfi, *Large orbits in coprime actions of solvable groups*, Trans. Amer. Math. Soc. **360** (2008), 135–152.

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

[21] 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.

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

[23] 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.

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

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

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

[27] A. Maróti, *Minimal degree, base size, order: selected topics on primitive permutation groups*, Arch. Math. **121** (2023), 485–493.

[28] V.D. Mazurov and E.I. Khukhro, *Unsolved problems in group theory: The Kourovka notebook, no. 20*, (arXiv:1401.0300v38), 2025.

[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* $\mathrm{L}_3(q)$ *or* $\mathrm{U}_3(q)$, 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 Abelian and nilpotent subgroups in finite groups, II*, Math. Notes **105** (2019), 366–375.
[37] V.I. Zenkov, *On intersections of primary subgroups in unsolvable finite groups with a socle isomorphic to* $\mathrm{L}_n(2^m)$, Sib. Math. J. **59** (2018), 264–269.
[38] V.I. Zenkov, *On intersections of pairs of primary subgroups in a finite group with socle* $\Omega^+_{2n}(2^m)$, Sib. Èlektron. Mat. Izv. **15** (2018), 728–732.
[39] V.I. Zenkov, *On the intersection of two nilpotent subgroups in a finite group with socle* $\Omega^+_8(2)$, $E_6(2)$ *or* $E_7(2)$, Sib. Èlektron. Mat. Izv. **14** (2017), 1424–1433.
[40] V.I. Zenkov, *On intersections of two nilpotent subgroups in finite groups with socle* $\mathrm{L}_2(q)$, Sib. Math. J. **57** (2016), 1002–1010.
[41] V.I. Zenkov, *On intersections of nilpotent subgroups in finite symmetric and alternating groups*, Proc. Steklov Inst. Math. **285** (2014), S203–S208.
[42] V.I. Zenkov, *On the intersections of Sylow 2-subgroups in finite groups, II*, Sib. Èlektron. Mat. Izv. **7** (2010), 42–51.
[43] V.I. Zenkov, *Intersections of nilpotent subgroups in finite groups*, Fundam. Prikl. Mat. **2** (1996), 1–92.
[44] V.I. Zenkov, *Intersections of abelian subgroups in finite groups*, Math. Notes **56** (1994), 869–871.
[45] V.I. Zenkov and V.D. Mazurov, *On the intersection of Sylow subgroups in finite groups*, Algebra and Logic **35** (1996), 236–240.
[46] V.I. Zenkov and Y.N. Nuzhin, *On intersection of primary subgroups in the group* $\mathrm{Aut}(F_4(2))$, Zh. Sib. Fed. Univ. Mat. Fiz. **11** (2018), 171–177.
[47] V.I. Zenkov and Y.N. Nuzhin, *On intersections of primary subgroups of odd order in almost simple groups*, J. Math. Sci. (N.Y.) **221** (2017), 384–390.

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
Current address: Department of Mathematics, Southern University of Science and Technology, Shenzhen 518055, Guangdong, P. R. China
Email address: 11612012@mail.sustech.edu.cn