BASE SIZES FOR $\mathcal{S}$-ACTIONS OF FINITE CLASSICAL GROUPS

TIMOTHY C. BURNESS, ROBERT M. GURALNICK, AND JAN SAXL

ABSTRACT. Let G be a permutation group on a set Ω. A subset B of Ω is a base for G if the pointwise stabilizer of B in G is trivial; the base size of G is the minimal cardinality of a base for G, denoted by $b(G)$. In this paper we calculate the base size of every primitive almost simple classical group with point stabilizer in Aschbacher's collection $\mathcal{S}$ of irreducibly embedded almost simple subgroups. In this situation we also establish strong asymptotic results on the probability that randomly chosen subsets of Ω form a base for G. Indeed, with some specific exceptions, we show that almost all pairs of points in Ω are bases.

1. INTRODUCTION

Let G be a permutation group on a finite set Ω. A subset B of Ω is a *base* for G if the pointwise stabilizer of B in G is trivial. The *base size* of G, denoted by $b(G)$, is the minimal cardinality of a base for G. Determining base sizes is a fundamental problem in permutation group theory, with a long history stretching back to the early days of group theory in the nineteenth century (see [4], for example). More recently, bases have played an important role in computational group theory (see [43, Chapter 4] for more details).

Let G be a finite almost simple primitive permutation group on a set Ω with socle G_0 and point stabilizer H. Roughly speaking, G is said to be *standard* if G_0 is a classical group and Ω is an orbit of subspaces of the natural G_0-module, or if $G_0 = A_n$ and Ω is an orbit of subsets or partitions of the natural G-set $\{1, \ldots, n\}$ (see [13, Definition 1.1] for the precise definition); if (G, Ω) is not of this form then G is *non-standard*. A well-known conjecture of Cameron and Kantor [21] asserts that there is a constant c such that $b(G) \leq c$ for any non-standard group G. (In general, if G is standard then $|G|$ is not bounded above by a fixed polynomial in $|\Omega|$, so the non-standard condition is necessary.) This conjecture was proved by Liebeck and Shalev [38, Theorem 1.3] with an undetermined constant c, using probabilistic methods. More recently, by combining the main theorems in [13, 17, 18, 14], it follows that the optimal constant in the conjecture is $c = 7$; more precisely, $b(G) \leq 7$ with equality if and only if $G = \mathrm{M}_{24}$ in its 5-transitive action on 24 points.

More detailed results have been obtained in some specific cases. If G_0 is a sporadic group then the exact value of $b(G)$ is calculated in [18] (see also [42]). Similarly, if $G_0 = A_n$ is an alternating group then $b(G) = 2$ if $n > 12$, and the precise base size has been computed for all non-standard groups with an alternating socle (see [14]). For non-standard classical groups, [13, Theorem 1.1] states that $b(G) \leq 5$, with equality if and only if $G = \mathrm{U}_6(2).2$ and $H = \mathrm{U}_4(3).2^2$, while the bound $b(G) \leq 6$ is established in [17] for groups of exceptional Lie type. In the latter case, it has recently been established that there are infinitely

Date: February 10, 2012.

2010 *Mathematics Subject Classification.* Primary 20B15, 20D06; Secondary 20P05.

Key words and phrases. Base size; finite classical groups; primitive permutation groups.

The authors would like to thank Dr. T. Breuer for his assistance with a computer calculation (see Lemma 5.5). They also thank Dr. C. Roney-Dougal for supplying the list of subgroups in $\mathcal{S}$ in the low dimensional classical groups (see Table 14), which is taken from the forthcoming book [7]. The first author was supported by EPSRC grant EP/I019545/1. The second author was partially supported by NSF grant DMS-1001962 and a Simons Foundation Fellowship.

many examples with $b(G) = 6$ (see [15, Theorem 8]). For example, we have $b(G) = 6$ if $(G, H) = (E_6(q), P_1)$, $(E_6(q), P_6)$ or $(E_7(q), P_7)$, where P_i denotes the standard maximal parabolic subgroup of G corresponding to the i-th node of the Dynkin diagram of G. However, in general the precise base size for Lie type groups has only been computed in a handful of special cases (for example, see [25] for the case $G_0 = \mathrm{L}_n(q)$ and H of type $\mathrm{Sp}_n(q)$, and also [13] for some additional specific cases); one of the outstanding problems in this area is to compute the precise base size of every non-standard primitive group of Lie type.

Let G be a finite almost simple classical group over $\mathbb{F}_q$ with socle G_0 and natural module V of dimension n. In [1], Aschbacher introduces eight *geometric* families of subgroups of G, denoted by $\mathcal{C}_i$ $(1 \leq i \leq 8)$, which are defined in terms of the underlying geometry of V. For example, these collections include the stabilizers of suitable subspaces of V, and the stabilizers of appropriate direct sum and tensor product decompositions of V. Essentially, Aschbacher's main theorem states that if H is a maximal subgroup of G with $HG_0 = G$ then either H is contained in one of the $\mathcal{C}_i$ collections, or H is almost simple and the socle of H acts absolutely irreducibly on V. Following [34], we refer to the latter family of almost simple subgroups as the $\mathcal{S}$ collection (see Definition 2.9). In studying finite primitive classical groups it is natural to make a distinction between the groups in which a point stabilizer belongs to one of the $\mathcal{C}_i$ collections, and those with a point stabilizer in $\mathcal{S}$. (Throughout this paper, we follow [34] in defining the various $\mathcal{C}_i$ collections.)

Our main result, Theorem 1 below, gives the precise value of $b(G)$ in the case where a point stabilizer belongs to the above $\mathcal{S}$ collection. Base sizes for the geometric $\mathcal{C}_i$-actions of classical groups are considered separately in the forthcoming paper [16]. (In [16] we also handle the small number of additional primitive groups corresponding to certain *novelty* subgroups of $G_0 = \mathrm{P}\Omega_8^+(q)$ and $\mathrm{PSp}_4(q)'$ (q even); this includes the case $(G, H) = (\mathrm{P}\Omega_8^+(q).3, G_2(q))$, for example.) A related result for simple algebraic groups over an algebraically closed field appears in [15].

Theorem 1. *Let G be a non-standard classical group with socle G_0 and point stabilizer $H \in \mathcal{S}$. Then either $b(G) = 2$, or $(G, H, b(G))$ is one of the cases listed in Table 1, where $H_0 = \mathrm{Soc}(H)$ denotes the socle of H.*

Corollary 1. *Let G be a non-standard classical group with socle G_0 and point stabilizer $H \in \mathcal{S}$. Let n be the dimension of the natural G_0-module. If $n > 8$ then either $b(G) = 2$, or one of the following holds:*

(i) *$b(G) = 4$ and $(G, H) = (O_{10}^-(2), S_{12})$.*

(ii) *$b(G) = 3$ and $(G, H) = (O_{14}^+(2), S_{16}), (\Omega_{12}^-(2), A_{13}), (O_{12}^-(2), S_{13})$ or $(\Omega_{10}^-(2), A_{12})$.*

In particular, if $n > 14$ then $b(G) = 2$.

Remark 1. In the statement of Theorem 1 and Corollary 1 (and also Theorem 2 below) we exclude any groups which are permutation isomorphic to a standard group. For example, the action of $G_0 = \mathrm{P}\Omega_8^+(q)$ on the cosets of an irreducible subgroup $\Omega_7(q)$ is equivalent to the standard action of G_0 on the set of non-singular 1-dimensional subspaces of the natural G_0-module. In addition, we exclude any groups which are permutation isomorphic to a classical group acting on the cosets of a $\mathcal{C}_i$-subgroup. In Table 2 we list all of the excluded groups which arise in this way (in the fourth line of the table, $\Lambda^2 V_4$ denotes the wedge square of the natural H_0-module V_4).

The proof of Theorem 1 uses probabilistic methods, based on fixed point ratio estimates. Recall that the *fixed point ratio* of $x \in G$, which we denote by $\mathrm{fpr}(x) = \mathrm{fpr}(x, \Omega)$, is the

$b(G)$	G_0	H_0	Conditions
5	$\mathrm{U}_6(2)$	$\mathrm{U}_4(3)$	$G = G_0.2$
4	$\Omega_{10}^-(2)$	A_{12}	$G = G_0.2$
	$\mathrm{P}\Omega_8^+(3)$	$\Omega_8^+(2)$	$G \neq G_0$
	$\Omega_8^+(2)$	A_9	
	$\Omega_7(q)$	$G_2(q)$	q odd
	$\mathrm{Sp}_6(q)$	$G_2(q)'$	q even
	$\mathrm{U}_6(2)$	$\mathrm{U}_4(3)$	$G \neq G_0.2$
	$\mathrm{Sp}_6(2)$	$\mathrm{U}_3(3)$	
	$\mathrm{U}_4(3)$	$\mathrm{L}_3(4)$	
	$\mathrm{U}_3(5)$	A_7	
	$\mathrm{U}_3(3)$	$\mathrm{L}_2(7)$	$G = G_0.2$
3	$\Omega_{14}^+(2)$	A_{16}	$G = G_0.2$
	$\Omega_{12}^-(2)$	A_{13}	
	$\Omega_{10}^-(2)$	A_{12}	$G = G_0$
	$\mathrm{Sp}_8(2)$	A_{10}	
	$\mathrm{P}\Omega_8^+(3)$	$\Omega_8^+(2)$	$G = G_0$
	$\Omega_7(3)$	$\mathrm{Sp}_6(2)$	
	$\Omega_7(3)$	A_9	
	$\mathrm{U}_6(2)$	M_{22}	
	$\mathrm{U}_4(3)$	A_7	
	$\mathrm{PSp}_4(q)$	$\mathrm{Sz}(q)$	$q = 2^{2a+1} > 2$
	$\mathrm{L}_3(4)$	A_6	
	$\mathrm{U}_3(5)$	A_6	
	$\mathrm{U}_3(5)$	$\mathrm{L}_2(7)$	$G = G_0.2$
	$\mathrm{U}_3(3)$	$\mathrm{L}_2(7)$	$G = G_0$
	$\mathrm{L}_2(19)$	A_5	
	$\mathrm{L}_2(11)$	A_5	

TABLE 1. $H \in \mathcal{S}$, $b(G) > 2$

G_0	H_0	Representation	Equivalent action
$\mathrm{P}\Omega_8^+(q)$	$\begin{cases} \Omega_7(q) & p > 2 \\ \mathrm{Sp}_6(q) & p = 2 \end{cases}$	spin module	$\mathcal{C}_1$-action on non-singular 1-spaces
$\mathrm{P}\Omega_8^+(q)$	$\mathrm{P}\Omega_8^-(q^{1/2})$	spin module	$\mathcal{C}_5$-action on cosets of $O_8^-(q^{1/2})$
$\mathrm{L}_6^\epsilon(q)$	$\mathrm{L}_4^\epsilon(q)$	$\Lambda^2 V_4$	$\mathcal{C}_8$-action on cosets of $O_6^\epsilon(q)$
$\mathrm{L}_4(2)$	A_7		A_8 on $\{1, \ldots, 8\}$
$\mathrm{L}_2(9)$	A_5		A_6 on $\{1, \ldots, 6\}$

TABLE 2. Some excluded $\mathcal{S}$-actions

proportion of points in Ω which are fixed by x. In other words, $\mathrm{fpr}(x)$ is the probability that a randomly chosen element of Ω is fixed by x. If G is transitive with point stabilizer H then it is easy to see that

$$\mathrm{fpr}(x) = \frac{|x^G \cap H|}{|x^G|}. \tag{1}$$

As originally observed in the proof of [38, Theorem 1.3], the connection between fixed point ratios and base sizes arises in the following way. For a positive integer c, let $P(G, c)$ be the probability that a randomly chosen c-tuple of points in Ω is a base for G, and let $Q(G, c) = 1 - P(G, c)$ denote the complementary probability. Note that G admits a base

of size c if and only if $Q(G,c) < 1$. Of course, a c-tuple in Ω fails to be a base if and only if it is fixed by an element $x \in G$ of prime order; further, the probability that a random c-tuple is fixed by x is at most $\mathrm{fpr}(x)^c$. If G is transitive then fixed point ratios are constant on conjugacy classes (see (1)), so

$$Q(G,c) \leq \sum_{x \in \mathcal{P}} \mathrm{fpr}(x)^c = \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i)^c =: \widehat{Q}(G,c), \tag{2}$$

where $\mathcal{P}$ is the set of elements of prime order in H, and $x_1, \ldots, x_k$ represent the distinct G-classes of elements in $\mathcal{P}$. Therefore $b(G) \leq c$ if $\widehat{Q}(G,c) < 1$, so we can use upper bounds on fixed point ratios to bound the base size. In particular, we observe that $b(G) = 2$ if

$$|H| \leq \min_{x \in \mathcal{P}} |x^G|^{1/2} \tag{3}$$

(see Corollary 2.3).

This probabilistic approach also allows us to establish strong asymptotic results on the abundance of bases in Ω of a given size. In [21], Cameron and Kantor prove that if $G = A_n$ or S_n is a non-standard permutation group on a set Ω then the probability that a random pair of points in Ω form a base for G tends to 1 as n tends to infinity. Similarly, if G is a non-standard classical group with natural module of dimension greater than 15 then Liebeck and Shalev prove that three randomly chosen points in Ω form a base with probability tending to 1 as $|G|$ tends to infinity (see [39, Theorem 1.11]). More generally, by [17, Theorem 2], the same property holds for six random points in any non-standard permutation group. Theorem 2 below gives the optimal asymptotic result for $\mathcal{S}$-actions of almost simple classical groups (see Remark 1).

Theorem 2. *Let G_i be a sequence of primitive almost simple classical groups with $|G_i|$ tending to infinity and each point stabilizer $H_i \in \mathcal{S}$. Then the probability that a random pair of points is a base for G_i tends to 1, unless there exists an infinite subsequence with*

(i) $(\mathrm{Soc}(G_i), \mathrm{Soc}(H_i)) = \begin{cases} (\Omega_7(q), G_2(q)) & q \text{ odd} \\ (\mathrm{Sp}_6(q), G_2(q)') & q \text{ even} \end{cases}$ *; or*

(ii) $(\mathrm{Soc}(G_i), \mathrm{Soc}(H_i)) = (\mathrm{PSp}_4(q)', \mathrm{Sz}(q))$, *$q$ even.*

For subsequences of type (i) or (ii), let c be minimal such that the probability that c random points form a base for G_i tends to 1. Then $c = 4$ in case (i), and $c = 3$ in (ii).

Let G be an almost simple classical group over $\mathbb{F}_q$ (where $q = p^f$ for a prime p) with natural module V of dimension n. Let H be a point stabilizer and suppose $H \in \mathcal{S}$ with socle H_0. In order to prove Theorems 1 and 2 we partition the collection $\mathcal{S}$ into several sub-collections, in a similar spirit to the proof of [12, Theorem 1.1]. First we define three collections of irreducible almost simple subgroups, denoted by the letters $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ (see Tables 3, 4 and 5, respectively). For instance, if $H \in \mathcal{A}$ then H_0 is an alternating group and V is the fully deleted permutation module for H_0 over $\mathbb{F}_p$. Now, if $n \geq 6$ and H is *not* in $\mathcal{A}$, $\mathcal{B}$ or $\mathcal{C}$ then we are in a position to apply two powerful theorems of Liebeck and Guralnick-Saxl (see Theorems 2.10 and 2.12). Together, these theorems imply that

(a) $|H| < q^{2n+4}$; and

(b) $\nu(x) > \max\{2, \frac{1}{2}\sqrt{n}\}$ for all nontrivial $x \in H \cap \mathrm{PGL}(V)$, where $\nu(x)$ denotes the codimension of the largest eigenspace of a lift $\hat{x} \in \mathrm{GL}(\bar{V})$ with $\bar{V} = V \otimes \bar{\mathbb{F}}_q$.

If $x \in H \cap \mathrm{PGL}(V)$ has prime order then the bound in (b) easily translates into a lower bound for $|x^G|$ (see Proposition 2.6, for example), and subsequently we can use the upper bound on $|H|$ in (a) to determine when the inequality in (3) holds. Indeed, in Proposition 6.1 we show that (3) holds for all $n \geq N$, where $N = 14$ if $G_0 = \mathrm{L}_n^\epsilon(q)$, otherwise $N = 64$. This reduces the problem to irreducible subgroups of small degree and

we can inspect explicit lists of these subgroups compiled by Lübeck [40] and Hiss-Malle [30]. The subsequent analysis yields two further sub-collections, denoted by $\mathcal{D}$ and $\mathcal{E}$ (see Tables 11 and 12). We deal case-by-case with the permutation groups in the collections $\mathcal{A}$–$\mathcal{E}$, working with the underlying irreducible representation to compute fixed point ratio estimates, which we use to estimate $\widehat{Q}(G,c)$ in (2). Finally, the remaining cases with $n < 6$ can be listed explicitly (see Table 14), and the desired result quickly follows.

Our main theorem has already been applied in two recent papers. A finite transitive permutation group G is said to be 3/2-*transitive* if all the nontrivial orbits of a point stabilizer have the same size, with this size being greater than 1. Clearly, if $b(G) = 2$ then a point stabilizer has a regular orbit and thus G is not 3/2-transitive. Consequently, Theorem 1 plays an important role in the analysis of $\mathcal{S}$-actions in [3], where the almost simple 3/2-transitive groups are classified.

In a similar spirit, Theorem 1 has also been used in joint work of the first author with Praeger and Seress [19]. A non-regular primitive permutation group is *extremely primitive* if a point stabilizer acts primitively on each of its nontrivial orbits. By a theorem of Mann, Praeger and Seress [41], every finite extremely primitive group is either almost simple or of affine type, and the extremely primitive almost simple classical groups are classified in [19] (the sporadic and alternating examples are determined in [20]). If G is an almost simple extremely primitive group then $b(G) > 2$, and once again Theorem 1 is a key tool in this classification.

Finally, some words on the organization of this paper. In Section 2 we present some preliminary results we will use in the proof of Theorems 1 and 2. In particular, we introduce the sub-collections denoted $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$, which we deal with next in Sections 3, 4 and 5, respectively. Two further sub-collections, denoted by $\mathcal{D}$ and $\mathcal{E}$, are then handled in Section 6. Finally, the proof of Theorems 1 and 2 is completed in Section 7, where we deal with the remaining low dimensional classical groups.

2. Preliminaries

2.1. **Notation.** Our notation for classical groups is mostly standard, following Kleidman-Liebeck [34]. In particular, we write $\mathrm{L}_n^+(q) = \mathrm{L}_n(q)$ and $\mathrm{L}_n^-(q) = \mathrm{U}_n(q)$ for $\mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$, respectively. The simple orthogonal groups are denoted by $\mathrm{P}\Omega_n^\epsilon(q)$, where $\epsilon = \pm$ if n is even, and $\epsilon = \circ$ when n is odd (in the latter case we write $\mathrm{P}\Omega_n^\circ(q) = \Omega_n(q)$). Our notation for matrices is also standard. With respect to a fixed basis of V, we use $[x_1, \ldots, x_t]$ to denote a block-diagonal matrix in $\mathrm{GL}_n(q) = \mathrm{GL}(V)$ with blocks x_i. Further, I_m denotes the identity $m \times m$ matrix, and J_m is the standard indecomposable unipotent Jordan block of size m.

If G is a finite group then $|x|$ denotes the order of an element $x \in G$. Also, if X is a subset of a finite group and m is a positive integer then $i_m(X)$ is the number of elements of order m in X. The greatest common divisor of the integers a and b is denoted by (a, b), while the symbol $\delta_{i,j}$ represents the familiar Kronecker delta. We reserve the symbol Q for the rational number $q/(q+1)$. Finally, if x is a real number and $\epsilon = \pm$ then $x - \epsilon$ denotes $x - \epsilon 1$.

2.2. **Probabilistic methods.** Let G be a transitive permutation group on a finite set Ω with point stabilizer H. Let B be a base for G. By definition, the elements of G are uniquely determined by their action on B, whence $|G| \leq |\Omega|^{|B|}$. This trivial observation yields the following useful lower bound:

Lemma 2.1. $b(G) \geq \log |G| / \log |\Omega|$.

As explained in the Introduction, fixed point ratio estimates can be used to derive an upper bound on $b(G)$. Indeed, recall that if $Q(G,c)$ is the probability that a randomly chosen c-tuple of points in Ω do *not* form a base for G then

$$Q(G,c) \leq \sum_{x \in \mathcal{P}} \mathrm{fpr}(x)^c = \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i)^c =: \widehat{Q}(G,c),$$

where $\mathcal{P}$ is the set of elements of prime order in H, and $x_1, \ldots, x_k$ represent the distinct G-classes of elements in $\mathcal{P}$. Therefore, $b(G) \leq c$ if $\widehat{Q}(G,c) < 1$. The next result provides an effective upper bound on $\widehat{Q}(G,c)$ (see [13, Lemma 2.1]).

Proposition 2.2. *Let G be a transitive permutation group on a finite set Ω with point stabilizer H. Suppose $x_1, \ldots, x_m$ represent distinct G-classes such that $\sum_i |x_i^G \cap H| \leq A$ and $|x_i^G| \geq B$ for $1 \leq i \leq m$. Then*

$$\sum_{i=1}^{m} |x_i^G| \cdot \mathrm{fpr}(x_i)^c \leq B(A/B)^c$$

for all positive integers c.

Corollary 2.3. *Suppose $|H|^2 \leq |x^G|$ for all $x \in H$ of prime order. Then $b(G) = 2$.*

Proof. Set $A = |H|$ and $B = \min_{x \in \mathcal{P}} |x^G|$. Then Proposition 2.2 yields $\widehat{Q}(G,2) < A^2/B$ and the result follows. □

The next proposition provides an alternative base-two criterion in the case where G is a finite almost simple classical group.

Proposition 2.4. *Let G be a transitive almost simple classical group with socle G_0, point stabilizer H, and natural G_0-module of dimension $n \geq 6$.*

(i) *If $\mathrm{fpr}(x) < |x^G|^{-\frac{2}{3}}$ for all $x \in H$ of prime order, then $b(G) = 2$.*

(ii) *Suppose (G_i, H_i) is a sequence of transitive almost simple classical groups, where $|G_i|$ tends to infinity and the dimension of each natural G_i-module is at least 6. If $\mathrm{fpr}(x) < |x^{G_i}|^{-\frac{2}{3}}$ for all $x \in H_i$ of prime order, then $P(G_i, 2)$ tends to 1.*

Proof. Following [13, Definition 3], let t be a real number, let χ be the set of G-classes of elements of prime order in G and define $\eta_G(t) = \sum_{C \in \chi} |C|^{-t}$. Fix $T_G \in (0,1)$ such that $\eta_G(T_G) = 1$. Then

$$\widehat{Q}(G,2) < \sum_{i=1}^{k} |x_i^G|^{-\frac{1}{3}} \leq \eta_G(1/3),$$

where $x_1, \ldots, x_k$ represent the distinct G-classes of elements of prime order in H. Finally, [13, Proposition 2.2] (and its proof) implies that $T_G < 1/3$, so $\widehat{Q}(G,2) < 1$ and thus $b(G) = 2$. For (ii), the proof of [13, Proposition 2.2] reveals that $\eta_{G_i}(1/3) \to 0$, so $Q(G_i, 2) \to 0$ and the result follows. □

2.3. **Conjugacy classes.** Let G be an almost simple classical group over $\mathbb{F}_q$ with socle G_0 and natural module V of dimension n. Write $q = p^f$ where p is a prime. Due to the existence of certain exceptional isomorphisms between some of the low dimensional classical groups (see [34, Proposition 2.9.1], for example), we may assume $n \geq 3$ if $G_0 = \mathrm{U}_n(q)$, $n \geq 4$ if $G_0 = \mathrm{PSp}_n(q)'$ and $n \geq 7$ if $G_0 = \mathrm{P}\Omega_n^{\epsilon}(q)$.

In order to estimate $\widehat{Q}(G,c)$ we need information on the conjugacy classes of elements of prime order in G. Let $x \in G$ be an element of prime order r. If $x \in G \cap \mathrm{PGL}(V)$ then x is either *unipotent* (if $r = p$) or *semisimple* (if $r \neq p$). There are three remaining possibilities:

(i) r divides $\log_p q$ and x is a *field automorphism* (induced by an automorphism of $\mathbb{F}_q$);
(ii) $r \leq 3$ and x is a *graph automorphism* (induced by an order r symmetry of the corresponding Dynkin diagram);
(iii) $r \leq 3$, r divides $\log_p q$ and x is a *graph-field automorphism* (a product of commuting graph and field automorphisms of order r).

Let $\bar{\mathbb{F}}_q$ denote the algebraic closure of $\mathbb{F}_q$ and set $\bar{V} = V \otimes \bar{\mathbb{F}}_q$. For each element $\hat{x} \in \mathrm{GL}(\bar{V})$ we define a subspace $[\bar{V}, \hat{x}] = \langle v - v\hat{x} \mid v \in \bar{V} \rangle$, which allows us to introduce the following important invariant. (Here a *lift* of x is an element $\hat{x} \in \mathrm{GL}(V)$ such that $x = \hat{x}Z$, where Z denotes the centre of $\mathrm{GL}(V)$.)

Definition 2.5. Let $x \in G \cap \mathrm{PGL}(V)$ and let $\hat{x} \in \mathrm{GL}(V)$ be a lift of x. We define

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

so $\nu(x)$ is equal to the codimension of the largest eigenspace of $\hat{x}$ on $\bar{V}$ (which is independent of the choice of lift $\hat{x}$).

In [11, Section 3], various bounds on $|x^G|$ are given in terms of $\nu(x)$. For the remainder of this subsection we set $Q = q/(q+1)$ and $a = \frac{1}{2}(1-\epsilon)$.

Proposition 2.6. *Let $x \in G \cap \mathrm{PGL}(V)$ be an element of prime order r with $\nu(x) = s$. Then $|x^G| > F(n, s, q)$, where F is defined in the following table.*

G_0	$s < n/2$	$s \geq n/2$
$\mathrm{L}_n^\epsilon(q)$	$\frac{1}{2}Q^a q^{2s(n-s)}$	$\frac{1}{2r}Q^{\frac{as}{n-s}} q^{ns}$
$\mathrm{PSp}_n(q)'$	$\frac{1}{4}Qq^{s(n-s)}$	$\frac{1}{4}Qq^{\frac{1}{2}ns}$
$\mathrm{P\Omega}_n^\epsilon(q)$	$\frac{1}{4}Qq^{s(n-s-1)}$	$\frac{1}{8}Q^{\frac{n}{2(n-s)}} q^{\frac{1}{2}n(s-1)}$

Proof. This follows from [11, Proposition 3.38]. □

Corollary 2.7. *If $n \geq 7$ and $\nu(x) \geq 3$ then $|x^G| > G(n, q)$, where $G(n,q) = \frac{1}{2}Qq^{6n-18}$ if $G_0 = \mathrm{L}_n^\epsilon(q)$, otherwise $G(n,q) = \frac{1}{4}Qq^{3n-12}$.*

Proposition 2.8. *If $x \in G \setminus \mathrm{PGL}(V)$ has prime order then $|x^G| > H(n, q)$, where*

G_0	$H(n,q)$
$\mathrm{L}_n^\epsilon(q)$	$\frac{1}{2}Q^a q^{\frac{1}{2}(n^2-n-4)}$
$\mathrm{PSp}_n(q)'$	$\frac{1}{4}q^{\frac{1}{4}n(n+1)}$
$\mathrm{P\Omega}_n^\epsilon(q)$	$\frac{1}{8}q^{\frac{1}{4}n(n-1)}$

Proof. This is [11, Corollary 3.49]. □

2.4. **The $\mathcal{S}$ collection.** Let G be an almost simple classical group over $\mathbb{F}_q$, acting primitively on a set Ω with point stabilizer H, socle G_0 and natural module V of dimension n. Write $q = p^f$ where p is a prime.

Recall that Aschbacher's theorem [1] states that either H is contained in one of eight geometric subgroup collections (denoted $\mathcal{C}_i$, $1 \leq i \leq 8$), or H belongs to a collection $\mathcal{S}$ of almost simple absolutely irreducible subgroups. Some additional properties of the subgroups in $\mathcal{S}$ are detailed in Definition 2.9 below (see [34, p.3]). Note that the conditions labelled (iii) – (vii) prevent a subgroup in $\mathcal{S}$ from being contained in a member of one of the geometric $\mathcal{C}_i$ families.

Definition 2.9. A subgroup H of G is in $\mathcal{S}$ if and only if the following hold:

(i) The socle H_0 of H is a nonabelian simple group, and $H_0 \ncong G_0$.

	d	p	G_0
$(\mathcal{A}1)$	$d \equiv 2 \pmod 4$	2	$\mathrm{Sp}_{d-2}(2)$
$(\mathcal{A}2)$	$d \equiv 0 \pmod 4$	2	$\begin{cases} \Omega^+_{d-2}(2) & \text{if } d \equiv 0 \pmod 8 \\ \Omega^-_{d-2}(2) & \text{if } d \equiv 4 \pmod 8 \end{cases}$
$(\mathcal{A}3)$	odd	2	$\begin{cases} \Omega^+_{d-1}(2) & \text{if } d \equiv \pm 1 \pmod 8 \\ \Omega^-_{d-1}(2) & \text{if } d \equiv \pm 3 \pmod 8 \end{cases}$
$(\mathcal{A}4)$	arbitrary	odd	$\begin{cases} \mathrm{P}\Omega^\epsilon_{d-1}(p) & \text{if } (d,p) = 1 \\ \mathrm{P}\Omega^\epsilon_{d-2}(p) & \text{otherwise} \end{cases}$

TABLE 3. The collection $\mathcal{A}$, $H_0 = A_d$ on the fully deleted permutation module

(ii) If $\widehat{H}_0$ is the full covering group of H_0, and if $\rho : \widehat{H}_0 \to \mathrm{GL}(V)$ is a representation of $\widehat{H}_0$ such that $\rho(\widehat{H}_0) = H_0$ (modulo scalars) then ρ is absolutely irreducible.

(iii) $\rho(\widehat{H}_0)$ cannot be realized over a proper subfield of $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_{q^2}$ if G_0 is unitary, otherwise $\mathbb{F} = \mathbb{F}_q$.

(iv) If $\rho(\widehat{H}_0)$ fixes a non-degenerate quadratic form on V then $G_0 = \mathrm{P}\Omega^\epsilon_n(q)$.

(v) If $\rho(\widehat{H}_0)$ fixes a non-degenerate symplectic form on V, but no non-degenerate quadratic form, then $G_0 = \mathrm{PSp}_n(q)$.

(vi) If $\rho(\widehat{H}_0)$ fixes a non-degenerate unitary form on V then $G_0 = \mathrm{U}_n(q)$.

(vii) If $\rho(\widehat{H}_0)$ does not satisfy the conditions in (iv), (v) or (vi) then $G_0 = \mathrm{L}_n(q)$.

In order to prove Theorems 1 and 2 we partition the subgroups in $\mathcal{S}$ into several subcollections. First let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ denote the irreducible almost simple subgroups listed in Tables 3, 4 and 5, respectively. In the tables, $M(\lambda)$ is the unique irreducible $\mathbb{F}_q\widehat{H}_0$-module of highest weight λ (up to quasi-equivalence), and we follow [6] in labelling the fundamental dominant weights λ_i. Note that if $H \in \mathcal{A}$ then H_0 is an alternating group, $q = p$ is prime and V is the fully deleted permutation module for H_0 over $\mathbb{F}_p$ (see [34, pp.185-187]). The collections $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ facilitate the statement of two key theorems.

Theorem 2.10. *If $H \in \mathcal{S}$ and $n \geq 6$ then one of the following holds:*

(i) *H_0 is an alternating group, embedded in G_0 as in $\mathcal{A}$;*

(ii) *H_0 is embedded in G_0 as in $\mathcal{B}$;*

(iii) $|H| < q^{2n+4}$.

Proof. If $G_0 \neq \mathrm{U}_n(q)$ then this follows immediately from [37, Theorem 4.2], so let us assume $G_0 = \mathrm{U}_n(q)$. Here [37, Theorem 4.2] gives the possibilities with $|H| \geq q^{4n+8}$; in order to extend this result we proceed as in the proof of [37, Theorem 4.1].

For example, suppose H_0 is a simple group of Lie type in characteristic p. Let $\widehat{H}_0$ be the full covering group of H_0, and let K be the algebraic closure of $\mathbb{F}_q$. Then $H_0 = \mathrm{L}^\epsilon_d(q^i)$, $\mathrm{P}\Omega^\epsilon_d(q^i)$ (with $d \equiv 2 \pmod 4$) or $E^\epsilon_6(q^i)$, and $n = \ell^i$ where ℓ is the dimension of a non-self dual irreducible $K\widehat{H}_0$-module (see [34, Section 5.4]). Suppose $H_0 = \mathrm{P}\Omega^\epsilon_d(q^i)$. Here $\ell \geq d \geq 10$ and

$$|H| \leq |\mathrm{Aut}(H_0)| < q^{\frac{1}{2}id(d-1)+i} < q^{2d^i+4} \leq q^{2n+4}$$

if $i \geq 2$. If $i = 1$ then we may assume $n > d$, so $n \geq \min\{2^{d/2-1}, d^2/2 - d/2 - 1\}$ (see [40]) and we deduce that $|H| \geq q^{2n+4}$ if and only if $(n,d) = (16,10)$, which corresponds to the case labelled $(\mathcal{B}4)$ in Table 4 with $\epsilon = -$. The other cases are very similar.

	H_0	G_0	Representation of H_0
$(\mathcal{B}1)$	$\mathrm{L}_d^\epsilon(q)$	$\mathrm{L}^\epsilon_{d(d-1)/2}(q)$	$\Lambda^2 V_d,\ d \geq 5$
$(\mathcal{B}2)$	$\begin{cases} \Omega_7(q) & p > 2 \\ \mathrm{Sp}_6(q) & p = 2 \end{cases}$	$\mathrm{P}\Omega^+_8(q)$	spin module
$(\mathcal{B}3)$	$\begin{cases} \Omega_9(q) & p > 2 \\ \mathrm{Sp}_8(q) & p = 2 \end{cases}$	$\mathrm{P}\Omega^+_{16}(q)$	spin module
$(\mathcal{B}4)$	$\mathrm{P}\Omega^\epsilon_{10}(q)$	$\mathrm{L}^\epsilon_{16}(q)$	spin module
$(\mathcal{B}5)$	$E_6^\epsilon(q)$	$\mathrm{L}^\epsilon_{27}(q)$	$M(\lambda_1)$
$(\mathcal{B}6)$	$E_7(q)$	$\begin{cases} \mathrm{PSp}_{56}(q) & p > 2 \\ \Omega^+_{56}(q) & p = 2 \end{cases}$	$M(\lambda_7)$
$(\mathcal{B}7)$	M_{24}	$\mathrm{L}_{11}(2)$	
$(\mathcal{B}8)$	J_3	$\mathrm{U}_9(2)$	
$(\mathcal{B}9)$	Suz	$\mathrm{U}_{12}(2)$	
$(\mathcal{B}10)$	Co_1	$\Omega^+_{24}(2)$	
$(\mathcal{B}11)$	$\mathrm{PSp}_6(3)$	$\mathrm{U}_{13}(2)$	
$(\mathcal{B}12)$	$\mathrm{U}_4(3)$	$\mathrm{U}_6(2)$	
$(\mathcal{B}13)$	M_{22}	$\mathrm{U}_6(2)$	

TABLE 4. The collection $\mathcal{B}$ from Theorem 2.10

If H_0 is a sporadic group then $n \geq N(H_0)$, where $N(H_0)$ is the lower bound on the minimal dimension of a faithful projective p-modular representation of H_0 given in [34, Proposition 5.3.8]. If $|H| \geq q^{2n+4}$ then we immediately deduce that $q = 2$ and (H_0, n) is one of the following:

H_0	M_{11}	M_{12}	M_{22}	M_{24}	J_2	J_3	Suz	Co_1
n	5	6	6, 7	11	6, 7, 8	9, 10, 11	$12, \ldots, 17$	$24, \ldots, 28$

By inspecting [29, Table 2], we see that the only possibilities are the cases labelled $(\mathcal{B}8)$, $(\mathcal{B}9)$, $(\mathcal{B}10)$ and $(\mathcal{B}13)$ in Table 4. We leave the reader to verify the theorem in the remaining cases. (As in the proof of [37, Theorem 4.1], we use Landazuri-Seitz [35] to derive a lower bound on n when H_0 is a group of Lie type in non-defining characteristic, and we use a combination of [45, 46, 47] and [31, Theorem 7] when H_0 is an alternating group.) □

Remark 2.11. In case $(\mathcal{B}1)$ of Table 4 we may assume $d \geq 5$. Indeed, if $d = 3$ then the underlying representation ρ is an isomorphism, while G is permutation isomorphic to a $\mathcal{C}_8$-action when $d = 4$ (see Table 2).

Theorem 2.12. *If $H \in \mathcal{S}$ and $n \geq 6$ then one of the following holds:*

(i) *H_0 is an alternating group, embedded in G_0 as in $\mathcal{A}$;*
(ii) *H_0 is embedded in G_0 as in $\mathcal{C}$;*
(iii) *$\nu(x) > \max\{2, \frac{1}{2}\sqrt{n}\}$ for all nontrivial $x \in H \cap \mathrm{PGL}(V)$.*

Proof. This follows from [28, Theorem 7.1]. □

Remark 2.13. In case $(\mathcal{C}19)$ of Table 5 we may assume $p \geq 3$; if $p = 2$ then condition (iii) in Definition 2.9 implies that $q = 4$, but H is non-maximal since $\mathrm{J}_2 < G_2(4) < \mathrm{Sp}_6(4)$. For completeness, we note that $b(G) = 2$ if $(G, H) = (\mathrm{Sp}_6(4), \mathrm{J}_2)$ or $(\mathrm{Sp}_6(4).2, \mathrm{J}_2.2)$.

Suppose $n \geq 6$ and $H \in \mathcal{S}$ is not one of the subgroups in $\mathcal{A}$, $\mathcal{B}$ or $\mathcal{C}$. If $x \in H \cap \mathrm{PGL}(V)$ has prime order then the lower bound on $\nu(x)$ in Theorem 2.12(iii) provides a lower bound

	H_0	G_0	Remarks
$(\mathcal{C}1)$	$\mathrm{L}_3^\epsilon(q)$	$\mathrm{L}_6^\epsilon(q)$	$p>2,\ S^2V_3$
$(\mathcal{C}2)$	$\begin{cases}\Omega_7(q) & p>2\\ \mathrm{Sp}_6(q) & p=2\end{cases}$	$\mathrm{P}\Omega_8^+(q)$	spin module
$(\mathcal{C}3)$	${}^3D_4(q_0)$	$\mathrm{P}\Omega_8^+(q)$	$q=q_0^3$, minimal module
$(\mathcal{C}4)$	$G_2(q)'$	$\begin{cases}\Omega_7(q) & p>2\\ \mathrm{Sp}_6(q) & p=2\end{cases}$	$M(\lambda_1)$
$(\mathcal{C}5)$	$G_2(q)$	$\Omega_7(q)$	$p=3,\ M(\lambda_2)$
$(\mathcal{C}6)$	A_6	$\mathrm{L}_6^\epsilon(p)$	$p\equiv\epsilon\,(\mathrm{mod}\ 3),\ p\geq 5$
$(\mathcal{C}7)$	A_7	$\mathrm{L}_6^\epsilon(p)$	$p\equiv\epsilon\,(\mathrm{mod}\ 3),\ p\geq 5$
$(\mathcal{C}8)$	$\mathrm{L}_3(4)$	$\mathrm{L}_6^\epsilon(p)$	$p\equiv\epsilon\,(\mathrm{mod}\ 3),\ p\geq 5$
$(\mathcal{C}9)$	$\mathrm{U}_3(3)$	$\mathrm{PSp}_6(p)$	$p\neq 3$
$(\mathcal{C}10)$	$\mathrm{U}_3(3)$	$\mathrm{L}_7^\epsilon(p)$	$p\equiv\epsilon\,(\mathrm{mod}\ 3),\ p\geq 5$
$(\mathcal{C}11)$	$\mathrm{U}_3(3)$	$\Omega_7(p)$	$p\geq 5$
$(\mathcal{C}12)$	$\mathrm{U}_4(3)$	$\mathrm{L}_6^\epsilon(p)$	$p\equiv\epsilon\,(\mathrm{mod}\ 3),\ p\geq 5$
$(\mathcal{C}13)$	$\mathrm{U}_4(3)$	$\mathrm{U}_6(2)$	
$(\mathcal{C}14)$	$\mathrm{U}_5(2)$	$\mathrm{PSp}_{10}(p)$	$p\geq 3$
$(\mathcal{C}15)$	$\mathrm{Sp}_6(2)$	$\Omega_7(p)$	$p\geq 3$
$(\mathcal{C}16)$	$\Omega_8^+(2)$	$\mathrm{P}\Omega_8^+(p)$	$p\geq 3$
$(\mathcal{C}17)$	M_{12}	$\mathrm{L}_6(3)$	
$(\mathcal{C}18)$	M_{22}	$\mathrm{U}_6(2)$	
$(\mathcal{C}19)$	J_2	$\mathrm{PSp}_6(q)$	$p\geq 3$

TABLE 5. The collection $\mathcal{C}$ from Theorem 2.12

for $|x^G|$ (via Proposition 2.6, for example). Next we can apply Corollary 2.3, using the upper bound on $|H|$ given in Theorem 2.10(iii). In this way, we quickly deduce that $b(G)=2$ for all $n\geq N$, where $N=14$ if $G_0=\mathrm{L}_n^\epsilon(q)$, otherwise $N=64$ (see Proposition 6.1). Similarly, if (G_i,H_i) is a sequence of primitive almost simple classical groups with $H_i\in\mathcal{S}\setminus(\mathcal{A}\cup\mathcal{B}\cup\mathcal{C})$, such that $|G_i|$ tends to infinity and the dimension of each natural G_i-module is at least N, then $P(G_i,2)$ tends to 1.

This reduces the proof of Theorems 1 and 2 to certain irreducible embeddings of small degree, which we can determine precisely by appealing to [30] and [40]. This analysis yields two further sub-collections, denoted by $\mathcal{D}$ and $\mathcal{E}$ (see Tables 11 and 12). These collections are dealt with in Section 6, while the remaining cases with $n<6$ are handled in Section 7.

We are now ready to begin the proof of Theorems 1 and 2. For the remainder of the paper, G denotes a finite almost simple classical group over $\mathbb{F}_q$, with socle G_0 and natural module V of dimension n, and Ω is a primitive G-set with point stabilizer $H\in\mathcal{S}$. As in Definition 2.9, H_0 denotes the (simple) socle of H and ρ is the underlying absolutely irreducible representation of the full covering group $\widehat{H}_0$. In addition, $\bar{G}$ denotes the ambient simple algebraic group defined over the algebraic closure $K=\bar{\mathbb{F}}_q$ (so that $G_0=(\bar{G}_\sigma)'$ for a suitable Frobenius morphism σ of $\bar{G}$).

3. The $\mathcal{A}$ collection

We begin the proof of Theorems 1 and 2 by dealing with the irreducible subgroups in the $\mathcal{A}$ collection (see Table 3). Recall that these embeddings are afforded by the fully deleted permutation module for A_d over $\mathbb{F}_p$.

$b(G)$	G_0	H_0	Conditions
4	$\Omega^-_{10}(2)$	A_{12}	$G = G_0.2$
	$\Omega^+_8(2)$	A_9	
3	$\Omega^+_{14}(2)$	A_{16}	$G = G_0.2$
	$\Omega^-_{12}(2)$	A_{13}	
	$\Omega^-_{10}(2)$	A_{12}	$G = G_0$
	$\mathrm{Sp}_8(2)$	A_{10}	
	$\Omega_7(3)$	A_9	

TABLE 6. $H \in \mathcal{A}$, $b(G) > 2$

Proposition 3.1. *Suppose $H \in \mathcal{A}$. Then either $b(G) = 2$, or $(G, H, b(G))$ is one of the cases listed in Table 6. Moreover, if (G_i, H_i) is a sequence of primitive almost simple classical groups, with $H_i \in \mathcal{A}$ and $|G_i|$ tending to infinity, then $P(G_i, 2)$ tends to 1.*

Lemma 3.2. *Proposition 3.1 holds for $(\mathcal{A}1)$.*

Proof. Here $G_0 = \mathrm{Sp}_{d-2}(2)$, $d \equiv 2 \pmod 4$ and we may assume $d \geq 10$ since $H_0 \cong G_0$ if $d = 6$. Suppose $d = 10$. Then $\log|G|/\log|\Omega| > 2$ so Lemma 2.1 implies that $b(G) \geq 3$. With the aid of MAGMA [5] (and the command MaximalSubgroups) we can construct G and H as permutation groups on 255 points, and by random search it is easy to find $x, y \in G$ such that $H \cap H^x \cap H^y = 1$, whence $b(G) = 3$ as required. Now assume $d = 14$. Here MAGMA stores G as a permutation group on 4095 points, but we have to construct $H = S_{14}$ directly. To do this, first observe that

$$S_{14} = \langle x, y \mid x \text{ is a transposition}, |y| = 13, |xy| = 14\rangle$$

(see [48]). Now G contains a unique class of elements of order 13, and since V is the fully deleted permutation module for H it follows that the transpositions in H act as transvections on V (so $|C_G(x)| = 4095$). By random search it is straightforward to find $x, y \in G$ satisfying the relations in the above presentation for S_{14}; we take $H = \langle x, y\rangle$ and a further random search provides an element $g \in G$ such that $H \cap H^g = 1$, whence $b(G) = 2$.

Next let us assume $d \geq 30$. Let $x \in H$ be an element of prime order r and recall that $\mathrm{fpr}(x) = |x^G \cap H|/|x^G|$ (see (1)). In view of Proposition 2.4, it suffices to show that

$$\mathrm{fpr}(x) < |x^G|^{-\frac{2}{3}}. \tag{4}$$

Let h be the number of r-cycles in the cycle-shape of x and observe that

$$|x^G \cap H| \leq |x^{S_d}| = \frac{d!}{h!(d-hr)!r^h} \tag{5}$$

(see the proof of [12, Proposition 2.5]). If $r = 2$ and $h < d/2$ then x is G_0-conjugate to either b_h or c_h (in the notation of [2]), the precise type depending on the parity of h. Therefore [11, Proposition 3.22] gives $|x^G| > 2^{h(d-h-1)-1}$ and thus (4) holds. Similarly, if $r = 2$ and $h = d/2$ then x is conjugate to $a_{d/2-1}$, so $|x^G| > 2^{d(d/2-2)/2-1}$ and the result follows as before. Now, if $r > 2$ then x is $\bar{G}$-conjugate to $[I_{d-2-h(r-1)}, \omega I_h, \ldots, \omega^{r-1} I_h]$, where $\omega \in K$ is a primitive r-th root of unity. Therefore $C_{\bar{G}}(x) \cong \mathrm{Sp}_{d-2-h(r-1)} \times \mathrm{GL}_h^{(r-1)/2}$, so

$$|x^G| > \frac{1}{2}\left(\frac{2}{3}\right)^{\frac{1}{2}(r-1)} 2^{\frac{1}{2}(r-1)(2dh-3h-h^2r)}$$

and once again (5) is sufficient. Therefore (4) holds and we conclude that $b(G) = 2$. Finally, suppose $18 \leq d \leq 26$ and define $\widehat{Q}(G,2)$ as in (2). Then direct calculation yields $\widehat{Q}(G,2) < 1$ and thus $b(G) = 2$. □

Lemma 3.3. *Proposition 3.1 holds for* $(\mathcal{A}2)$.

Proof. Here $d \equiv 0 \pmod 4$ and we may assume $d \geq 12$ since $A_8 \cong \Omega_6^+(2)$. If $d = 12$ then a straightforward Magma calculation yields $b(G) = 4$ if $G = O_{10}^-(2)$, otherwise $b(G) = 3$. Now assume $d \geq 16$. We claim that if $d \geq 32$ then (4) holds for all $x \in H$ of prime order, so $b(G) = 2$ by Proposition 2.4. (To obtain the desired asymptotic result, it suffices to show that (4) holds for all sufficiently large d (see Proposition 2.4), so this also follows from the claim.) To justify the claim, let $x \in H$ be an element of prime order r and let h be the number of r-cycles in the cycle-shape of x. If $r = 2$ and $h < d/2$ then $|x^G| > 2^{h(d-h-2)-1}$, while $|x^G| > 2^{(d/2-2)(d/2-1)-1}$ if $h = d/2$. In both cases, the bound in (5) is sufficient. If r is odd then

$$|x^G| > \frac{1}{2}\left(\frac{2}{3}\right)^{\frac{1}{2}(r+1)} 2^{\frac{1}{2}h(r-1)(2d-5-hr)}$$

and once again (5) is good enough. If $20 \leq d \leq 28$ then one can check that $\widehat{Q}(G,2) < 1$ and so $b(G) = 2$ in these cases too.

It remains to deal with the case $d = 16$. Now Magma stores $O_{14}^+(2)$ as a permutation group on 8255 points and by random search we can construct $H = N_G(\langle x, y\rangle)$, where $x, y \in G$ satisfy the relations in the following presentation of A_{16} (see [48])

$$A_{16} = \langle x, y \mid x \text{ is a 3-cycle, } y \text{ is a 15-cycle}, |xy| = 14, |xy^2| = 63\rangle.$$

(Note that $|x^G| = 10924032$ and $|y^G| = 150360513379815847152844 80$ if $x \in H$ is a 3-cycle and $y \in H$ is a 15-cycle.) By random search it is easy to see that $b(G) = 2$ when $G = \Omega_{14}^+(2)$ and $b(G) \leq 3$ when $G = O_{14}^+(2)$. To deduce that $b(G) = 3$ when $G = O_{14}^+(2)$ we use a Magma implementation of the 'double coset enumeration' technique described in [18, Section 2.3.3]. (The basic idea is to find a set of distinct (H,H) double cosets $\{Hx_iH \mid i \in I\}$ such that $|Hx_iH| < |H|^2$ and $\sum_{i\in I} |Hx_iH| > |G| - |H|^2$; this implies that H does not have a regular orbit on G/H and thus $b(G) > 2$.) □

Lemma 3.4. *Proposition 3.1 holds for* $(\mathcal{A}3)$.

Proof. Here d is odd and we may assume $d \geq 9$ since $G_0 \cong A_8$ when $d = 7$ (see Table 2), while $G_0 \cong H_0$ when $d = 5$. In addition, we note that the maximality of H in G implies that $d \equiv 1 \pmod 4$. If $d = 9$ then a Magma calculation yields $b(G) = 4$ (see the proof of [13, Proposition 3.2]) so let us assume $d \geq 13$. In the usual way, it is straightforward to show that (4) holds if $d \geq 29$, while a direct calculation yields $\widehat{Q}(G,2) < 1$ when $d = 17$, 21 or 25. Therefore $b(G) = 2$ if $d \geq 17$, and the asymptotic result follows immediately from the fact that (4) holds for all sufficiently large d (see Proposition 2.4). Finally, if $d = 13$ then Magma stores $O_{12}^-(3)$ as a subgroup of S_{2015} and by random search we can construct $H = N_G(\langle x, y\rangle)$, where $x, y \in G$ satisfy the relations in the presentation

$$A_{13} = \langle x, y \mid x \text{ is a 3-cycle, } |y| = 11, |xy| = 13\rangle$$

(see [48]; note that $|x^G| = 732160$ if $x \in H$ is a 3-cycle). By a further random search it is easy to check that $b(G) \leq 3$, while the double coset method employed in the proof of Lemma 3.3 yields $b(G) > 2$. □

Lemma 3.5. *Proposition 3.1 holds for* $(\mathcal{A}4)$.

Proof. We have $d \geq 8$ and p is odd. First assume $(d,p) = 1$, so $G_0 = \mathrm{P}\Omega_{d-1}^{\epsilon}(p)$ and the maximality of H in G implies that p does not divide $d+1$. Let $x \in H$ be an element of prime order r and let h be the number of r-cycles in the cycle-shape of x. Suppose $r = 2$

and assume $h < d/2 - 1$ if d is even. Then $|x^G| > \frac{1}{8}p^{h(d-1-h)}$ and by applying the upper bound on $|x^G \cap H|$ given in (5) we deduce that (4) holds unless $(d,p) \in A$, where

$$A = \{(16,3),(13,3),(10,3),(8,7),(8,5)\}.$$

Similarly, if $r = 2$, d is even and $h \geq d/2 - 1$ then

$$|x^G \cap H| \leq \frac{d!}{(d/2-1)!2^{d/2}} + \frac{d!}{(d/2)!2^{d/2}} = \frac{(d/2+1)d!}{(d/2)!2^{d/2}},$$

$|x^G| > \frac{1}{4}(p+1)^{-1}p^{d^2/4-d/2+1}$ and thus (4) holds unless $(d,p) = (10,3)$ or $(8,5)$. Now, if $r > 2$ and $(d,p) \notin A$ then (4) follows from the bounds in the proof of [12, Proposition 2.5], hence $b(G) = 2$ for all $(d,p) \notin A$ (and as usual, the desired asymptotic result follows from Proposition 2.4). If $(d,p) \in A$ and $(d,p) \neq (10,3)$ then it is easy to check that $\widehat{Q}(G,2) < 1$ and thus $b(G) = 2$ in each of these cases too. Finally, if $(d,p) = (10,3)$ then we use MAGMA to construct G and $H = N_G(\langle x,y\rangle)$ as permutation groups of degree 3280, where $x, y \in G$ satisfy the relations in the presentation

$$A_{10} = \langle x, y \mid x \text{ is a 3-cycle}, |y| = 9, |xy| = 8, |xy^2| = 12\rangle.$$

(Note that $|x^{G_0}| = 2302560$ and $|y^{G_0}| = 812157489561600$.) In this way we quickly deduce that $b(G) = 2$ by random search.

Finally let us assume p divides d, so $G_0 = \mathrm{P}\Omega^{\epsilon}_{d-2}(p)$ and $d \geq 9$. Arguing as before, we see that (4) holds unless $(d,p) \in B$ where

$$B = \{(18,3),(15,3),(12,3),(10,5),(9,3)\}.$$

If $(d,p) = (9,3)$ then $(G,H) = (\Omega_7(3), S_9)$, $\log|G|/\log|\Omega| > 2$ and an easy MAGMA calculation yields $b(G) = 3$. Next suppose $(d,p) = (12,3)$. Here $\epsilon = +$ and MAGMA stores G as a permutation group on 9922 points. By random search we can find $x, y \in G$ such that $H = N_G(\langle x,y\rangle)$, where x, y satisfy the relations in the presentation

$$A_{12} = \langle x, y \mid x \text{ is a 3-cycle}, |y| = 11, |xy| = 10, |xy^2| = 35\rangle.$$

(Note that $|x^G| = 21431520$ if $x \in H$ has order 3.) We quickly deduce that $b(G) = 2$. In each of the remaining cases, direct calculation yields $\widehat{Q}(G,2) < 1$ and therefore $b(G) = 2$. □

This completes the proof of Proposition 3.1.

4. The $\mathcal{B}$ collection

Next we establish Theorems 1 and 2 for the irreducible subgroups in the $\mathcal{B}$ collection (see Table 4). Note that we may exclude the case labelled ($\mathcal{B}2$) – see Table 2. Our main result is the following:

Proposition 4.1. *Suppose $H \in \mathcal{B}\backslash\mathcal{B}2$. Then either $b(G) = 2$, or $G_0 = \mathrm{U}_6(2)$, $H_0 = \mathrm{U}_4(3)$ and $b(G) = 4 + \alpha$, where $\alpha = 1$ if $G = G_0.2$, otherwise $\alpha = 0$. Moreover, if (G_i, H_i) is a sequence of primitive almost simple classical groups, with $H_i \in \mathcal{B} \setminus \mathcal{B}2$ and $|G_i|$ tending to infinity, then $P(G_i, 2)$ tends to 1.*

Lemma 4.2. *Proposition 4.1 holds for ($\mathcal{B}1$).*

Proof. Here $H \cap \mathrm{PGL}(V) \leqslant \mathrm{PGL}^{\epsilon}_d(q) = \tilde{H}$, $d \geq 5$ and ρ is quasi-equivalent to the representation afforded by the wedge square $\Lambda^2 V_d$, where V_d is the natural module for $\mathrm{SL}^{\epsilon}_d(q)$. Define $\widehat{Q}(G,2)$ as in (2). To prove the lemma it suffices to show that $\widehat{Q}(G,2) < F(d,q)$ for some function F, where $F(d,q) < 1$ and $F(d,q) \to 0$ as $d + q \to \infty$.

If $x \in H \cap \mathrm{PGL}(V)$ has prime order then the proof of [12, Lemma 2.9] gives $\nu(x) \geq d-2$ (see Definition 2.5), whence Proposition 2.6 yields $|x^G| > \frac{1}{2}Qq^{d^3-5d^2+10d-8} = b$ (with

$Q = q/(q+1)$) and the same bound also holds if $x \in H \setminus \mathrm{PGL}(V)$ (see Proposition 2.8). Since $|H| < 2\log_2 q.q^{d^2-1} = a$ we deduce that $\widehat{Q}(G,2) \leq a^2/b$, which is less than q^{-d} if $d \geq 6$.

To complete the proof, we may assume $d = 5$, so $n = 10$. We will estimate the contribution to $\widehat{Q}(G,2)$ from the various elements of prime order in H. Set $\tilde{G} = \mathrm{PGL}^{\epsilon}_{10}(q)$ and let $x \in H \cap \mathrm{PGL}(V)$ be an element of prime order r.

Suppose $r = p$, so x is unipotent. It is straightforward to calculate the Jordan form of x on $V = \Lambda^2 V_5$, and we deduce that if x is conjugate to $[J_2^3, I_4]$ then $|x^G \cap H| < 2q^8 = a_1$ and $|x^G| > \frac{1}{2}Qq^{42} = b_1$, otherwise $|x^G| > \frac{1}{2}Qq^{48} = b_2$. We note that $\tilde{H}$ contains fewer than $q^{20} = a_2$ elements of order p. Next suppose $r \neq p$. If $r = 2$ then x is conjugate to $[-I_4, I_6]$, so $|x^G \cap H| < 2q^{12} + 2q^8 = a_3$ and $|x^G| > \frac{1}{2}Qq^{48} = b_3$. Now assume $r > 2$. If $C_G(x)$ is of type $\mathrm{GL}^{\epsilon}_6(q) \times \mathrm{GL}^{\epsilon}_4(q)$ then r divides $q - \epsilon$ and $C_H(x)$ is of type $\mathrm{GL}^{\epsilon}_4(q) \times \mathrm{GL}^{\epsilon}_1(q)$, so $|x^{\tilde{G}} \cap H| < 2q^8 = a_4$ and $|x^G| > \frac{1}{2}Qq^{48} = b_4$. In addition, we note there are at most

$$\sum_{r \in \pi'} (r-1) \leq (q - \epsilon - 1)|\pi'| < q\log(q+1) = n_4$$

distinct $\tilde{G}$-classes of such elements, where π' is the set of odd prime divisors of $q - \epsilon$. In the remaining cases, a straightforward calculation with the module $\Lambda^2 V_5$ reveals that $|x^G| > \frac{1}{2}Q^2q^{54} = b_5$ and we note that $|\tilde{H}| < q^{24} = a_5$.

Finally suppose $x \in H \setminus \mathrm{PGL}(V)$ has prime order. If x is an involutory graph automorphism then $|x^G| > \frac{1}{2}Qq^{43} = b_6$ and we calculate that $|x^G \cap H| < 2q^{14} = a_6$ since x induces an involutory graph automorphism on H_0. Similarly, we have $|x^G \cap H| < 2q^{12} = a_7$ and $|x^G| > \frac{1}{2}q^{97/2} = b_7$ if $\epsilon = +$ and x is an involutory graph-field automorphism. If x is a field automorphism of prime order r then $|x^G \cap H| < 2q^{24(1-r^{-1})}$ and $|x^G| > \frac{1}{2}Qq^{99(1-r^{-1})-1} = f(r)$, so $\mathrm{fpr}(x) < 4(q+1)q^{-75(1-r^{-1})} = g(r)$. Clearly, G contains fewer than $\log_2 q.q^{99}$ field automorphisms, so by applying Proposition 2.2 we see that the contribution to $\widehat{Q}(G,2)$ from these elements is less than

$$\sum_{r \in \pi} (r-1) \cdot h(r) < h(2) + 2h(3) + \log_2 q.q^{99} g(5)^2,$$

where $h(r) = f(r)g(r)^2$ and π is the set of distinct prime divisors of $\log_p q$. Putting all this together, and using Proposition 2.2 once again, we conclude that

$$\widehat{Q}(G,2) < \sum_{i=1}^{7} n_i b_i (a_i/b_i)^2 + h(2) + 2h(3) + \log_2 q.q^{99} g(5)^2 < q^{-1},$$

where $n_i = 1$ for $i \neq 4$. The result follows. □

Lemma 4.3. *Proposition 4.1 holds for* ($\mathcal{B}3$).

Proof. Here ρ is the restriction to $\Omega_9(q)$ (or $\mathrm{Sp}_8(q)$ if q is even) of a spin representation which embeds $\Omega^+_{10}(q)$ in $\mathrm{SL}_{16}(q)$. As in the proof of the previous lemma, our aim is to derive a suitable upper bound for $\widehat{Q}(G,2)$. Let $x \in H \cap \mathrm{PGL}(V)$ be an element of prime order r.

First assume $r = p > 2$ and let λ be the partition of 16 corresponding to the Jordan form of x on V. If $\lambda \neq (2^8)$, $(3, 2^4, 1^5)$ or $(2^4, 1^8)$ then the proof of [12, Lemma 2.8] gives $|x^G| > \frac{1}{8}Q^2q^{70} = b_1$, and we note that $H \cap \mathrm{PGL}(V)$ contains fewer than $q^{32} = a_1$ elements of order p. For $\lambda = (2^8)$ we calculate that $|x^G \cap H| < 2q^{14} = a_2$ and $|x^G| > \frac{1}{4}q^{56} = b_2$. Similarly, $|x^G \cap H| < q^{16} = a_3$ and $|x^G| > \frac{1}{8}q^{60} = b_3$ if $\lambda = (3, 2^4, 1^5)$, while $|x^G \cap H| < 2q^{12} = a_4$ and $|x^G| > \frac{1}{4}q^{44} = b_4$ if $\lambda = (2^4, 1^8)$. For $r = p = 2$, the proof of [12, Lemma

2.8] provides the following bounds $|x^G \cap H| < a_i$ and $|x^G| > b_i$:

i	$O_{16}^+(q)$-class of x	a_i	b_i
5	a_4	$2q^{12}$	$\frac{1}{2}q^{44}$
6	a_8	$2q^{14}+q^8$	$\frac{1}{2}q^{56}$
7	c_8	$2(q^{20}+q^{18}+q^{16})$	$\frac{1}{2}q^{64}$

Next suppose $r \neq p$. At the level of algebraic groups, we may assume $x \in D_4 < D_5$ and we note that $V \downarrow D_4 = V_8 \oplus V_8'$, where V_8 and V_8' are non-isomorphic 8-dimensional spin modules for D_4. In particular, if $r = 2$ then [11, Proposition 3.55(iii)] implies that $\nu(x) = 8$, whence $|x^G| > \frac{1}{4}Qq^{56} = b_8$ and we calculate that there are at most $2q^{20} = a_8$ involutions in $H \cap \mathrm{PGL}(V)$. Now assume $r > 2$. If $C_H(x)$ is not of type $O_7(q) \times \mathrm{GL}_1^\epsilon(q)$ then using [11, Proposition 3.55(iv)] we calculate that $|x^G| > \frac{1}{2}Qq^{76} = b_9$ (minimal if $C_{\bar{G}}(x)$ is of type $O_8 \times \mathrm{GL}_4$) and we note that $|H \cap \mathrm{PGL}(V)| < q^{36} = a_9$. Otherwise, if $C_H(x)$ is of type $O_7(q) \times \mathrm{GL}_1^\epsilon(q)$ then $C_{\bar{G}}(x)$ is of type GL_8, so $|x^{\tilde{G}} \cap H| < 2q^{14} = a_{10}$ and $|x^G| > \frac{1}{2}Qq^{56} = b_{10}$, where $\tilde{G} = \bar{G}_\sigma = \mathrm{Inndiag}(G_0)$ is the group of *inner-diagonal* automorphisms of G_0 (see [27, Section 2.5]). Further, since r divides q^2-1, there are fewer than $\log(q^2-1)$ possibilities for r and so there are less than $\frac{1}{2}q\log(q^2-1) = n_{10}$ distinct $\tilde{G}$-classes of this type.

Finally, suppose $x \in H \setminus \mathrm{PGL}(V)$ has prime order r. Then x is a field automorphism, so $|x^G \cap H| < 2q^{36(1-r^{-1})}$, $|x^G| > \frac{1}{4}q^{120(1-r^{-1})} = f(r)$ and thus $\mathrm{fpr}(x) < 8q^{-84(1-r^{-1})} = g(r)$. It follows that the contribution to $\widehat{Q}(G,2)$ from field automorphisms is less than

$$\sum_{r\in\pi}(r-1)\cdot h(r) < h(2)+2h(3)+2\log_2 q.q^{120}g(5)^2,$$

where $h(r) = f(r)g(r)^2$ and π is the set of prime divisors of $\log_p q$. Applying Proposition 2.2, we conclude that

$$\widehat{Q}(G,2) < \sum_{i=1}^{10} n_i b_i (a_i/b_i)^2 + h(2) + 2h(3) + 2\log_2 q.q^{120}g(5)^2 < q^{-1},$$

where $n_i = 1$ for $i \neq 10$. Therefore $b(G) = 2$, and we also observe that $\widehat{Q}(G,2) \to 0$ as $q \to \infty$, so the required asymptotic result also holds. □

Lemma 4.4. *Proposition 4.1 holds for the remaining cases in $\mathcal{B}$.*

Proof. First consider ($\mathcal{B}4$). Suppose $x \in H$ has prime order. If $x \in H \cap \mathrm{PGL}(V)$ then $\nu(x) \geq 4$ (see [10, Lemma 7.2]) and thus $|x^G| > \frac{1}{2}Qq^{96} = b$ by Proposition 2.6. According to Proposition 2.8, the same bound on $|x^G|$ also holds if $x \in H \setminus \mathrm{PGL}(V)$. Now $|H| < 2\log_2 q.q^{45} = a$ and thus $\widehat{Q}(G,2) < a^2/b < q^{-1}$. Cases ($\mathcal{B}5$) and ($\mathcal{B}6$) are very similar.

Next consider ($\mathcal{B}7$), where $G = \mathrm{L}_{11}(2)$ and $H = \mathrm{M}_{24}$. The 2-modular character table of H is available in the Modular Atlas (see [32, p.267]), and from the values of the relevant Brauer character we can compute precise fixed point ratios for semisimple elements. With the aid of Magma and the Web Atlas [48], we can explicitly construct H as a subgroup of the matrix group $G = \mathrm{SL}_{11}(2)$; we find that $2A$-elements in H have Jordan form $[J_2^4, I_3]$, while $2B$-elements have form $[J_2^5, I_1]$. Therefore we can compute $\widehat{Q}(G,2)$ precisely, and we deduce that $\widehat{Q}(G,2) < 1$. The cases ($\mathcal{B}8$) and ($\mathcal{B}9$) are similar. (Note that the 2-modular character tables of J_3 and Suz are available in the GAP Character Table Library [8]. Also note that $H \cap \mathrm{PGL}(V) = H_0$ in both cases.)

Next we turn to ($\mathcal{B}10$), so $G = \Omega_{24}^+(2)$, $H = \mathrm{Co}_1$ and $|H| < 2^{62} = a_1$. Suppose $x \in H$ has prime order r and note that $\nu(x) \geq 6$ (see [28, Table 1]). In particular, if $r \in \{5, 11, 13, 23\}$ then $|x^G| > 2^{146} = b_1$. Similarly, if $r = 3$ or 7 then $|x^G| > 2^{112} = b_2$ and

$b(G)$	G_0	H_0	Conditions
5	$\mathrm{U}_6(2)$	$\mathrm{U}_4(3)$	$G = G_0.2$
4	$\mathrm{P}\Omega_8^+(3)$	$\Omega_8^+(2)$	$G \neq G_0$
	$\mathrm{U}_6(2)$	$\mathrm{U}_4(3)$	$G = G_0$
	$\mathrm{Sp}_6(2)$	$\mathrm{U}_3(3)$	
3	$\Omega_7(3)$	$\mathrm{Sp}_6(2)$	
	$\mathrm{U}_6(2)$	M_{22}	

TABLE 7. $H \in \mathcal{C}$, $b(G) > 2$

$i_3(H)+i_7(H) < 2^{52} = a_2$, while $i_2(H) < 2^{34} = a_3$ and $|x^G| > 2^{101} = b_3$ if $r = 2$ (here $i_r(H)$ denotes the number of elements of order r in H). Therefore $\widehat{Q}(G,2) < \sum_{i=1}^{3} b_i(a_i/b_i)^2 < 1$ and thus $b(G) = 2$ as required.

In $(\mathcal{B}11)$ we have $(G,H) = (\mathrm{U}_{13}(2), \mathrm{PSp}_6(3))$ or $(\mathrm{U}_{13}(2).2, \mathrm{PGSp}_6(3))$. The 2-modular character table of $H_0 = \mathrm{PSp}_6(3)$ is available in the GAP Character Table Library [8] and we deduce that $\nu(x) \geq 4$ for all $x \in H_0$ of odd prime order. Using a combination of the Web Atlas and MAGMA, we see that the same bound also holds for involutions in H_0, so Proposition 2.6 implies that $|x^G| > 2^{70}$ for all $x \in H_0$ of prime order. Now if $x \in H \setminus H_0$ is an involution then x is a graph automorphism of G_0, so once again we have $|x^G| > 2^{70}$. Since $|H| < 2^{32}$ we deduce that $\widehat{Q}(G,2) < 2^{-6}$, so $b(G) = 2$. The case $(\mathcal{B}13)$ is very similar, while for $(\mathcal{B}12)$ we have $b(G) = 4 + \alpha$, where $\alpha = 1$ if $G = G_0.2$, otherwise $\alpha = 0$ (see [13, Lemma 3.4]). □

5. The $\mathcal{C}$ collection

Proposition 5.1. *Suppose $H \in \mathcal{C} \setminus \mathcal{C}2$ (see Table 5). Then either $b(G) = 2$, or one of the following holds:*

(i) $(G_0, H_0) = \begin{cases} (\Omega_7(q), G_2(q)) & q \text{ odd} \\ (\mathrm{Sp}_6(q), G_2(q)') & q \text{ even} \end{cases}$ *and $b(G) = 4$;*

(ii) $(G, H, b(G))$ *is one of the cases listed in Table 7.*

Moreover, if (G_i, H_i) is a sequence of primitive almost simple classical groups, with $H_i \in \mathcal{C} \setminus \mathcal{C}2$ and $|G_i|$ tending to infinity, then $P(G_i, 2)$ tends to 1 unless there exists an infinite subsequence with

$$(\mathrm{Soc}(G_i), \mathrm{Soc}(H_i)) = \begin{cases} (\Omega_7(q), G_2(q)) & q \text{ odd} \\ (\mathrm{Sp}_6(q), G_2(q)') & q \text{ even.} \end{cases}$$

For such a subsequence, $P(G_i, 4)$ tends to 1.

Note that in the statement of Proposition 5.1 we exclude the case labelled $(\mathcal{C}2)$; see Table 2. Also note that the cases labelled $(\mathcal{C}13)$ and $(\mathcal{C}18)$ have already been considered in the previous section (see $(\mathcal{B}12)$ and $(\mathcal{B}13)$, respectively).

Lemma 5.2. *Proposition 5.1 holds for $(\mathcal{C}1)$.*

Proof. Here $G_0 = \mathrm{L}_6^\epsilon(q)$ and $H_0 = \mathrm{L}_3^\epsilon(q)$, where q is odd and ρ is the representation afforded by the symmetric-square S^2V_3 of the natural module V_3 for $\mathrm{SL}_3^\epsilon(q)$. As before, we will find a function $F(q)$ such that $\widehat{Q}(G,2) \leq F(q) < 1$ for all $q \geq 3$, with the additional property that $F(q) \to 0$ as $q \to \infty$.

Let $x \in H \cap \mathrm{PGL}(V)$ be an element of prime order r. If $r > 2$ then an easy calculation with the symmetric-square yields $|x^G| > \frac{1}{2}Q^2q^{22} = b_1$ and we note that $|H \cap \mathrm{PGL}(V)| <$

$q^8 = a_1$. Similarly, if $r = 2$ then $|x^G \cap H| < 2q^4 = a_2$ and $|x^G| > \frac{1}{2}Qq^{16} = b_2$. Now, if $x \in H \setminus \mathrm{PGL}(V)$ is an involution then $|x^G| > \frac{1}{2}Qq^{13} = b_3$ and [36, Proposition 1.3] yields $i_2(\mathrm{Aut}(\mathrm{L}_3^\epsilon(q))) < 2(q+1)q^4 = a_3$. Finally, if x is a field automorphism of odd prime order r then $|x^G \cap H| < 2q^{8(1-r^{-1})}$ and $|x^G| > \frac{1}{12}q^{35(1-r^{-1})} = f(r)$, so $\mathrm{fpr}(x) < 24q^{-27(1-r^{-1})} = g(r)$ and the contribution to $\widehat{Q}(G,2)$ from odd order field automorphisms is less than $2h(3) + \log_3 q.q^{35}g(5)^2$, where $h(r) = f(r)g(r)^2$. Therefore

$$\widehat{Q}(G,2) < \sum_{i=1}^{3} b_i(a_i/b_i)^2 + 2h(3) + \log_3 q.q^{35}g(5)^2,$$

which is less than q^{-1} for all $q \geq 5$. The same bound also yields $\widehat{Q}(G,2) < 1$ when $q = 3$. □

Lemma 5.3. *Proposition 5.1 holds for* $(\mathcal{C}3)$.

Proof. Here $q = q_0^3$ and $H_0 = C_{G_0}(\psi)$, where ψ is a triality graph-field automorphism of G_0. Detailed information on the conjugacy classes in H_0 is given in [23] and [44].

Let $x \in H \cap \mathrm{PGL}(V)$ be an element of prime order r. First assume $r = p$. Let λ be the partition of 8 corresponding to the Jordan form of x on V. The unipotent classes in H_0 are listed in [44, p.677] and we adopt the notation therein. From this labelling we can read off λ, and consequently we derive the following bounds $|x^G \cap H| < a_i$ and $|x^G| > b_i$ when $p > 2$:

i	H_0-class of x	λ	a_i	b_i
1	A_1	$(2^2, 1^4)$	q_0^{10}	$\frac{1}{4}q_0^{30}$
2	$3A_1$	$(3, 2^2, 1)$	$2q_0^{16}$	$\frac{1}{8}q_0^{48}$
3	A_2', A_2''	$(3^2, 1^2)$	q_0^{18}	$\frac{1}{8}(q_0^3+1)^{-2}q_0^{60}$
4	$D_4(a_1)$	$(5, 3)$	q_0^{22}	$\frac{1}{8}q_0^{66}$
5	D_4	$(7, 1)$	q_0^{24}	$\frac{1}{8}q_0^{72}$

Similarly, if $r = p = 2$ then $|x^G \cap H| < a_i$ and $|x^G| > b_i$, where

i	H_0-class of x	G_0-class of x	a_i	b_i
6	A_1	a_2	q_0^{10}	$\frac{1}{2}q_0^{30}$
7	$3A_1$	c_4	$2q_0^{16}$	$\frac{1}{2}q_0^{48}$

(Note that a_2 and c_4 are the only ψ-stable G_0-classes of involutions - see [11, Proposition 3.55(ii)].) If $p > 2$ and $r = 2$ then [11, Proposition 3.55(iii)] implies that $C_G(x)$ is of type $O_4^+(q)^2$, so $|x^G \cap H| = i_2(H_0) < 2q_0^{16} = a_8$ and $|x^G| > \frac{1}{8}q_0^{48} = b_8$.

Next suppose $r \neq p$ and $r > 2$. As described in [23, Section 2], there are 13 possibilities for $C_{H_0}(x)$ (up to H_0-conjugacy), labelled s_j for $3 \leq j \leq 15$. The precise number of distinct H_0-classes of type s_j is given in [23, Table 4.4], and using [23, Tables 2.2a, 2.2b] it is easy to determine $C_{\bar{G}}(x)$, where $\bar{G} = D_4$ is the ambient algebraic group. In this way we compute the following bounds, where a_i is an upper bound for the total number of elements $x \in H_0$ with $C_{\bar{G}}(x)$ of type i, while b_i is a lower bound for $|x^G|$. (In the second column, T_i denotes an i-dimensional torus.)

i	$C_{\bar{G}}(x)$	Possibilities for $C_{H_0}(x)$	a_i	b_i
9	A_2T_2	s_4, s_9	$2q_0^{18}.(q_0^2+q_0)$	$\frac{1}{2}(q_0^3+1)^{-2}q_0^{60}$
10	$A_1^3T_1$	s_3, s_7	$2q_0^{18}.q_0$	$\frac{1}{2}(q_0^3+1)^{-1}q_0^{57}$
11	A_1T_3	s_5, s_{10}	$2q_0^{22}.(q_0^3-q_0^2)$	$\frac{1}{2}(q_0^3+1)^{-3}q_0^{75}$
12	T_4	$s_6, s_8, s_{11}, \ldots, s_{15}$	q_0^{28}	$\frac{1}{2}(q_0^3+1)^{-4}q_0^{84}$

r	H_0-class of x	$\nu(x)$	$\lvert x^G \cap H\rvert$	$\lvert x^G\rvert >$
2	$2A$	2	2835	5^{15}
	$2D$	1	252	5^9
	$2E$	3	11340	5^{17}
3	$3A$	3	560	5^{17}
	$3B$	2	3360	5^{17}
	$3C$, $3D$	4	43680	5^{22}
7	$7A$, $7B$	5	653184	5^{29}

TABLE 8. Case $(\mathcal{C}12)$, $p = 5$

Finally, suppose $x \in H \setminus \mathrm{PGL}(V)$ has prime order r. If x is a field automorphism and $r \neq 3$ then r divides $\log_p q_0$ and we have

$$|x^G \cap H| < 2q_0^{28\left(1-\frac{1}{r}\right)}, \ \ |x^G| > 4^{\delta_{2,p}-1} q_0^{84\left(1-\frac{1}{r}\right)} = f(r).$$

Therefore $\mathrm{fpr}(x) < 2.4^{1-\delta_{2,p}} q_0^{-56(1-r^{-1})} = g(r)$ and the contribution to $\widehat{Q}(G,2)$ from these elements is less than $h(2) + 3\log_2 q_0.q_0^{84}g(5)^2$, where $h(r) = f(r)g(r)^2$. Now, if x is a field automorphism of order 3 then x induces a triality automorphism on H_0, and using [36, Proposition 1.3] we obtain the bounds

$$|x^G \cap H| \leq i_3(\mathrm{Aut}(H_0)) < 2(q_0+1)q_0^{19} = a_{13}, \ \ |x^G| > \frac{1}{4}q_0^{56} = b_{13}.$$

The same bounds also apply if x is a triality graph-field automorphism.

Finally, suppose x is a triality graph automorphism. Then x induces a triality graph automorphism on H_0 and we claim that the centralizers $C_{H_0}(x)$ and $C_{G_0}(x)$ are of the same *type*. (There are two conjugacy classes of triality graph automorphisms in $\mathrm{Aut}(G_0)$, with representatives τ_1 and τ_2, where $C_{G_0}(\tau_1) \cong G_2(q)$ and $C_{G_0}(\tau_2) \cong \mathrm{PGL}_3^\epsilon(q)$ if $q \equiv \epsilon \pmod 3$, otherwise $C_{G_0}(\tau_2) \cong [q^5].\mathrm{SL}_2(q)$. We say that τ_1 is a *G_2-type triality*, while τ_2 is a *non-G_2 triality*. There is an analogous description of the conjugacy classes of triality automorphisms in $\mathrm{Aut}(H_0)$.)

To justify the claim, let $y \in \mathrm{Aut}(G_0)$ be a field automorphism of order 3. By conjugating appropriately, we may assume that x and y commute. By [27, Theorem 4.9.1(d)], xy is $\mathrm{Inndiag}(G_0)$-conjugate to any order 3 graph-field automorphism of G_0, so we may assume $H_0 = C_{G_0}(xy)$. Therefore $C_{H_0}(x) = C_{H_0}(y) = C_{C_{G_0}(x)}(y)$ and the result follows. For example, if $C_{G_0}(x)$ is of type $G_2(q)$ then we deduce that $C_{H_0}(x)$ is of type $G_2(q_0)$.

It follows that $|x^G \cap H| < a_i$ and $|x^G| > b_i$, where a_i and b_i are defined as follows:

i	Type of $C_{G_0}(x)$	a_i	b_i
14	G_2	$2q_0^{14}$	$2^{2\delta_{2,p}-3}q_0^{42}$
15	non-G_2	$2q_0^{20}$	$2^{2\delta_{2,p}-3}q_0^{60}$

Putting all this together, we conclude that

$$\widehat{Q}(G,2) < \sum_{i=1}^{15} n_i b_i (a_i/b_i)^2 + h(2) + 3\log_2 q_0.q_0^{84}g(5)^2,$$

where $n_{14} = n_{15} = 2$ and $n_i = 1$ for $i < 14$. This upper bound is less than q_0^{-1} for all $q_0 \neq 3$, and the same bound yields $\widehat{Q}(G,2) < 1$ when $q_0 = 3$. □

Lemma 5.4. *Proposition 5.1 holds for* $(\mathcal{C}12)$ *and* $(\mathcal{C}14)$.

r	H_0-class of x	$\lvert x^G \cap H\rvert$	$\lvert x^G\rvert >$
2	$2A$, $2E$	58275	$\frac{1}{8}7^{16}$
	$2B$, $2C$, $2D$	$3^{\zeta}.3780$	$3^{\zeta}.\frac{1}{4}\frac{7}{8}7^{12}$
	$2F$	120	$\frac{1}{4}7^{7}$
	$2G$	37800	$\frac{1}{4}7^{15}$
3	$3A$, $3B$, $3C$	$3^{\zeta}.2240$	$3^{\zeta}.\frac{1}{2}7^{12}$
	$3D$	89600	$\frac{1}{2}7^{18}$
	$3E$	268800	$\frac{1}{2}7^{18}$
5	$5A$, $5B$, $5C$	$3^{\zeta}.580608$	$3^{\zeta}.\frac{1}{2}7^{20}$
7	$7A$	24883200	$\frac{1}{8}7^{24}$

TABLE 9. Case ($\mathcal{C}16$), $p = 7$

Proof. Both cases are very similar, so we only give details for ($\mathcal{C}12$). Here $H_0 = \mathrm{U}_4(3)$ and $G_0 = \mathrm{L}_6^{\epsilon}(p)$, where $p \geq 5$ and $p \equiv \epsilon \pmod 3$. First assume $p = 5$ and let $x \in H \cap \mathrm{PGL}(V)$ be an element of prime order r. By inspecting the corresponding Brauer character (see [32, p.131]) we derive the results recorded in Table 8. If $r = 5$ then $|x^G \cap H| = i_5(H) = 653184$ and using MAGMA we deduce that x has Jordan form $[J_5, I_1]$ on V, whence $|x^G| > 5^{27}$. Now, if $x \in H \setminus \mathrm{PGL}(V)$ has prime order then x is an involutory graph automorphism, hence $|x^G \cap H| \leq i_2(\mathrm{Aut}(H_0)) - i_2(H \cap \mathrm{PGL}(V)) = 14148$ and $|x^G| > \frac{1}{12}5^{15}$. The desired bound $\widehat{Q}(G, 2) < 1$ quickly follows.

Similarly, the reader can check that $\widehat{Q}(G, 2) < p^{-1}$ if $p > 5$. Note that if $p = 7$ and $x \in H \cap \mathrm{PGL}(V)$ has order 7 then $|x^G \cap H| \leq i_7(H) = 933120$ and $|x^G| > 7^{29}$ since x has Jordan form $[J_6]$ on V. □

Lemma 5.5. *Proposition 5.1 holds for* ($\mathcal{C}16$).

Proof. For $p = 3$ a MAGMA calculation yields $b(G) = 3 + \alpha$, where $\alpha = 0$ if $G = G_0$, otherwise $\alpha = 1$ (see the proof of [13, Proposition 3.2]). For the remainder we may assume $p \geq 5$.

First assume $p = 7$. Suppose $x \in H \cap \mathrm{PGL}(V)$ has prime order r. By inspecting the 7-modular character table of $H_0 = \Omega_8^+(2)$ (see [32, p.238]), and by appealing to the proof of [12, Lemma 2.14], we derive the bounds presented in Table 9 (in the table, $\zeta = 1$ if G contains a triality graph automorphism, otherwise $\zeta = 0$). If $x \in H$ is a triality graph automorphism then the centralizers $C_{H_0}(x)$ and $C_{G_0}(x)$ are of the same type (see the proof of [12, Proposition 2.14]) and therefore the contribution to $\widehat{Q}(G, 2)$ from such elements is less than $2a_1^2/b_1 + 2a_2^2/b_2$, where $a_1 = 14400$, $a_2 = 806400$, $b_1 = \frac{1}{8}7^{14}$ and $b_2 = \frac{1}{8}7^{20}$. We conclude that $\widehat{Q}(G, 2) < 1$ when $p = 7$.

Similar reasoning applies when $p > 7$. Here every element in $H \cap \mathrm{PGL}(V)$ is semisimple and their contribution to $\widehat{Q}(G, 2)$ can be computed precisely by inspecting the character table of H in [22]. Now $i_3(\mathrm{Aut}(H_0)) - i_3(H_0) = 1641600 = a$ and so the contribution from triality automorphisms is less than $64a^2p^{-14}$ since $|x^G| > \frac{1}{8}p^{14}$ for any triality x. It is straightforward to check that $\widehat{Q}(G, 2) < p^{-1}$.

Finally, suppose $p = 5$. Let $x \in H \cap \mathrm{PGL}(V)$ be an element of prime order r. In the usual manner we derive the bounds recorded in Table 10, and we quickly deduce that $\widehat{Q}(G, 2) < 1$ if G does not contain triality automorphisms. According to the proof of [12, Proposition 2.14], the contribution to $\widehat{Q}(G, 2)$ from triality automorphisms is at most $2a_1^2/b_1 + 2a_2^2/b_2$, where $a_1 = 14400$, $a_2 = 806400$, $b_1 = 1521000000$ and $b_2 = 23575500000000$. This implies that $b(G) \in \{2, 3\}$ since $\widehat{Q}(G, 3) < 1$ and $\widehat{Q}(G, 2) > 1$. By using GAP [24] to construct G

r	H_0-class of x	$\lvert x^G \cap H\rvert$	$\lvert x^G\rvert \geq$
2	$2A$, $2E$	58275	42976171875
	$2B$, $2C$, $2D$	$3^{\zeta}.3780$	$3^{\zeta}.153562500$
	$2F$	120	39000
	$2G$	37800	15868125000
3	$3A$, $3B$, $3C$	$3^{\zeta}.2240$	$3^{\zeta}.201500000$
	$3D$	89600	2619500000000
	$3E$	268800	3438093750000
5	$5A$, $5B$, $5C$	$3^{\zeta}.580608$	$3^{\zeta}.47528208000000$
7	$7A$	24883200	47151000000000000

TABLE 10. Case ($\mathcal{C}16$), $p = 5$

and H as permutation groups of degree 58968, Dr. T. Breuer has proved that $b(G) = 2$ in this case (see [9] for the details of this calculation). □

Lemma 5.6. *Proposition 5.1 holds for the remaining cases in $\mathcal{C}$.*

Proof. For ($\mathcal{C}4$) and ($\mathcal{C}5$) we refer the reader to [13, Lemma 3.1 and Proposition 3.2], where the result $b(G) = 4$ is proved. At the algebraic group level, the action of $\bar{G} = \mathrm{SO}_7(\bar{\mathbb{F}}_q)$ on the cosets of $G_2(\bar{\mathbb{F}}_q)$ is considered in [15]. Here the *generic base size* of $\bar{G}$ is shown to be 4 (see [15, Proposition 4.4]), so the desired asymptotic result immediately follows from [15, Proposition 2.7].

For ($\mathcal{C}9$), the proof of [13, Proposition 3.1] gives $b(G) = 4$ if $p = 2$, and it is straightforward to check that $\widehat{Q}(G, 2) < p^{-1}$ for all $p > 2$. The other cases are similar and we leave the reader to fill in the details. □

6. The collections $\mathcal{D}$ and $\mathcal{E}$

We may now assume that (G, H) is not one of the cases in the collections $\mathcal{A}$, $\mathcal{B}$ or $\mathcal{C}$. We continue to assume that $n \geq 6$, and we set $N = 14$ if $G_0 = \mathrm{L}^{\epsilon}_n(q)$, otherwise $N = 64$.

Proposition 6.1. *If $n \geq N$ then $b(G) = 2$. Moreover, if (G_i, H_i) is a sequence of primitive almost simple classical groups, where $H_i \in \mathcal{S} \setminus (\mathcal{A} \cup \mathcal{B} \cup \mathcal{C})$, $|G_i|$ tends to infinity and the dimension of each natural G_i-module is at least N, then $P(G_i, 2)$ tends to 1.*

Proof. This follows quickly from Theorems 2.10 and 2.12. For example, suppose $G_0 = \mathrm{L}^{\epsilon}_n(q)$ and $n \geq 14$. Let $x \in H$ be an element of prime order. If $x \in H \cap \mathrm{PGL}(V)$ then Theorem 2.12 implies that $\nu(x) \geq 3$, whence Corollary 2.7 gives $|x^G| > \frac{1}{2}Qq^{6n-18} = b$ and the same bound also holds if $x \in H \setminus \mathrm{PGL}(V)$ (see Proposition 2.8). Now, Theorem 2.10 yields $|H| < q^{2n+4} = a$ and we conclude that $\widehat{Q}(G, 2) < a^2/b < q^{-n/40}$. □

For the remainder of this section we will assume $6 \leq n < N$. At this juncture it is natural to split the analysis, according to whether or not H_0 is a group of Lie type in characteristic p.

6.1. Defining characteristic.

First we assume H_0 is a simple group of Lie type over $\mathbb{F}_{q'}$ for some p-power q'.

Lemma 6.2. *If $H_0 = \mathrm{L}_2(q')$ then $b(G) = 2$ and $P(G, 2)$ tends to 1 as $|G|$ tends to infinity.*

Proof. Here $q' = q^i$ and $n = \ell^i$ for some positive integer i, where ℓ is the dimension of a nontrivial irreducible $K\widehat{H}_0$-module (see [34, Proposition 5.4.6]). The corresponding irreducible representation of $\widehat{H}_0$ is self-dual, so G_0 is either symplectic or orthogonal. Applying Theorem 2.12, together with Propositions 2.6 and 2.8, we deduce that

$$|H| \leq |\mathrm{Aut}(H_0)| = i \log_p q.q^i(q^{2i}-1), \quad |x^G| > \frac{1}{4}Qq^{\alpha(n-\alpha-1)}$$

for all $x \in H$ of prime order, where α is the smallest integer greater than $\max\{2, \frac{1}{2}\sqrt{n}\}$. Now, if $(n,i) \notin \{(9,2),(8,3),(6,1)\}$ then these bounds imply that $\widehat{Q}(G,2) < 1$, so $b(G) = 2$. Moreover, it is easy to check that $\widehat{Q}(G,2) \to 0$ as n or q tends to infinity, so we also have $P(G,2) \to 1$ as claimed. It remains to deal with the cases $(n,i) \in \{(9,2),(8,3),(6,1)\}$.

If $(n,i) = (9,2)$ then $|x^G| > \frac{1}{4}q^{16}$ for all $x \in H$ of prime order (since $\nu(x) \geq 3$ if $x \in H \cap \mathrm{PGL}(V)$, minimal if $r = p$ and x has Jordan form $[J_2^4, I_1]$), and the result follows as before. The case $(n,i) = (6,1)$ is similar. Here p is odd, $G_0 = \mathrm{PSp}_6(q)$ and $|x^G| > \frac{1}{4}q^{21/2}$ for all $x \in H$ of prime order (minimal if x is an involutory field automorphism). Again, the result follows in the usual manner.

Finally, suppose $(n,i) = (8,3)$. If $p = 2$ then $G_0 = \Omega_8^+(q)$ and we can discard this case since H is not maximal in G (see [33, Proposition 2.36]). Now assume p is odd, so $G_0 = \mathrm{PSp}_8(q)$ and $H \cap \mathrm{PGL}(V) \leqslant \mathrm{PGL}_2(q^3).3 = B.3 = \tilde{H}$. Let $x \in H \cap \mathrm{PGL}(V)$ be an element of prime order r.

If $r = p$ and $x \in B$ then x is conjugate to $[J_4, J_2^2]$ if $p \geq 5$, and to $[J_3^2, J_2]$ when $p = 3$, so $|x^G \cap H| < q^6 = a_1$ and $|x^G| > \frac{1}{4}q^{24} = b_1$. If $r = 2$ then Theorem 2.12 implies that $\nu(x) \geq 4$, so $|x^G \cap H| \leq q^6 = a_2$ and $|x^G| > \frac{1}{4}q^{16} = b_2$. Next assume $x \in B$ and $r \neq p$ is odd. Then x is conjugate to

$$[\omega, \omega^{-1}] \otimes [\omega^q, \omega^{-q}] \otimes [\omega^{q^2}, \omega^{-q^2}]$$

for some $\omega \in K$, and it is easy to see that $|x^G|$ is minimal when $\omega \in \mathbb{F}_q$. This gives $|x^G| > \frac{1}{2}Qq^{24} = b_3$ and we note that $|B| < q^9 = a_3$. Now, if $x \in \tilde{H} \setminus B$ has order 3 then an easy calculation reveals that x has Jordan form $[J_3^2, I_2]$ if $p = 3$, otherwise x is G-conjugate to $[I_4, \omega I_2, \omega^2 I_2]$, where $\omega \in K$ is a primitive cube root of unity. Therefore $|x^G \cap H| \leq 4q^6 = a_4$ and $|x^G| > \frac{1}{2}Qq^{22} = b_4$.

Finally, suppose $x \in H \setminus \mathrm{PGL}(V)$ is a field automorphism of prime order r. Then $|x^G \cap H| < 2q^{9(1-r^{-1})}$ and $|x^G| > \frac{1}{4}q^{36(1-r^{-1})} = f(r)$, so $\mathrm{fpr}(x) < 8q^{-27(1-r^{-1})} = g(r)$ and the contribution to $\widehat{Q}(G,2)$ from field automorphisms is less than

$$\sum_{r \in \pi} (r-1) \cdot h(r) < h(2) + 2h(3) + \log_3 q.q^{36} g(5)^2,$$

where $h(r) = f(r)g(r)^2$ and π is the set of prime divisors of $\log_p q$. We conclude that

$$\widehat{Q}(G,2) < \sum_{i=1}^{4} b_i(a_i/b_i)^2 + h(2) + 2h(3) + \log_3 q.q^{36} g(5)^2 < q^{-1}$$

for all $q \geq 3$. □

Now assume $H_0 \neq \mathrm{L}_2(q')$. We consider the various possibilities for H_0 in turn. To illustrate the general approach, suppose $H_0 = \mathrm{L}_m(q^i)$ and assume the underlying irreducible representation ρ is self-dual. Again, [34, Proposition 5.4.6] implies that $n = \ell^i \geq m^i$, where ℓ is the dimension of a nontrivial irreducible $K\widehat{H}_0$-module, and recall that we may assume $n < 64$. Suppose $x \in H$ has prime order. By applying Theorem 2.12 and Propositions 2.6

and 2.8 we deduce that

$$|H| \leq |\mathrm{Aut}(H_0)| < 2i \log_2 q . q^{i(m^2-1)}, \ \ |x^G| > \frac{1}{4} Q q^{\alpha(n-\alpha-1)},$$

where α is the smallest integer greater than $\max\{2, \frac{1}{2}\sqrt{n}\}$. The possibilities for n can be read off from the relevant tables in [40], and in the usual manner we deduce that $b(G) = 2$ and $P(G,2) \to 1$ (as n or q tends to infinity), with the exception of the following cases (each with $i = 1$):

$$(m,n) \in \{(3,7), (3,8), (4,14), (4,15), (6,20)\}.$$

These exceptional cases appear in Table 11 (see $(\mathcal{D}1)$, $(\mathcal{D}2)$ and $(\mathcal{D}3)$).

Next suppose $H_0 = \mathrm{PSp}_m(q^i)'$, where $m \geq 4$ is even. Once again we have $n = \ell^i \geq m^i$, where ℓ is the dimension of an irreducible $K\widehat{H}_0$-module. Furthermore, ρ is self-dual and we derive the bounds

$$|H| \leq |\mathrm{Aut}(H_0)| < \beta i \log_2 q . q^{\frac{1}{2} im(m+1)}, \ \ |x^G| > \frac{1}{4} Q q^{\alpha(n-\alpha-1)},$$

where α is defined as before and $\beta = 2$ if $(m,p) = (4,2)$, otherwise $\beta = 1$. Using [40], and applying Corollary 2.3, we quickly reduce to the cases

$$(m,n) \in \{(4,10), (4,12), (6,8), (6,13), (6,14), (8,16), (8,26), (8,27), (10,32)\},$$

each with $i = 1$. The cases $(m,n) \in \{(4,10), (6,13), (6,14), (8,26), (8,27)\}$ appear in Table 11, while $(6,8)$ and $(8,16)$ correspond to the embeddings $(\mathcal{B}2)$ and $(\mathcal{B}3)$ in the collection $\mathcal{B}$ (see Table 4). The two remaining cases can be handled in the usual way, using a more accurate lower bound for $|x^G|$. For example, if $(m,n) = (4,12)$ then the bound $\nu(x) \geq 3$ implies that $|x^G| > \frac{1}{4} q^{27}$ for all $x \in H$ of prime order, so $\widehat{Q}(G,2) < q^{-1}$ since $|H| < 2 \log_2 q . q^{10}$.

Proceeding in this way, excluding any examples which already belong to the $\mathcal{B}$ or $\mathcal{C}$ collections, we reduce to the specific cases listed in Table 11, which we refer to as the $\mathcal{D}$ collection. As before, $M(\lambda)$ denotes the unique irreducible $\mathbb{F}_q\widehat{H}_0$-module of highest weight λ (up to quasi-equivalence). In addition, we write V_{adj} for the nontrivial composition factor of the adjoint module for H_0.

Remark 6.3. Note that we exclude the case $\mathrm{P}\Omega_8^-(q_0) < \mathrm{P}\Omega_8^+(q_0^2)$ corresponding to the restriction of an irreducible spin representation; the action here is equivalent to the $\mathcal{C}_5$-action on the set of cosets of a subfield subgroup of type $O_8^-(q_0)$ (see Table 2).

Proposition 6.4. *If $H \in \mathcal{D}$ then $b(G) = 2$. Moreover, if (G_i, H_i) is a sequence of primitive almost simple classical groups, with $H_i \in \mathcal{D}$ and $|G_i|$ tending to infinity, then $P(G_i, 2)$ tends to 1.*

Lemma 6.5. *Proposition 6.4 holds for $(\mathcal{D}1)$.*

Proof. Here $H \cap \mathrm{PGL}(V) \leqslant \mathrm{PGL}_3^{\epsilon}(q).\langle\gamma\rangle$, where γ is an involutory graph automorphism. In addition, if $p \neq 3$ then $q \equiv \epsilon \pmod 3$. If $q = 3$ then H is non-maximal, so we may assume $q > 3$. Set $\bar{H} = \mathrm{PSL}_3(K)$.

For now we will assume $p = 3$, so $n = 7$ and $q \geq 9$. Let $x \in H \cap \mathrm{PGL}(V)$ be an element of prime order r. If $r = 3$ then a straightforward calculation with the adjoint module yields $|x^G \cap H| \leq a_i$ and $|x^G| \geq b_i$, where a_i and b_i are defined as follows. Here the partitions λ' and λ encode the Jordan form of x on the natural H_0- and G_0-modules, respectively (see Case i in the proof of [12, Lemma 2.20]).

i	λ'	λ	a_i	b_i
1	$(2,1)$	$(3,2^2)$	$(q+\epsilon)(q^3-\epsilon)$	$\frac{1}{2}q^2(q^4-1)(q^6-1)$
2	(3)	$(3^2,1)$	$q(q^2-1)(q^3-\epsilon)$	$\frac{1}{4}q^3(q-1)(q^4-1)(q^6-1)$

	H_0	G_0	Remarks
$(\mathcal{D}1)$	$\mathrm{L}_3^\epsilon(q)$	$\begin{cases} \mathrm{P}\Omega_8^+(q) & p\neq 3 \\ \Omega_7(q) & p=3 \end{cases}$	$V_{\mathrm{adj}},\ q>2$
$(\mathcal{D}2)$	$\mathrm{L}_4^\epsilon(q)$	$\begin{cases} \Omega_{15}(q) & p\neq 2 \\ \Omega_{14}^{\epsilon'}(q) & p=2 \end{cases}$	V_{adj}
$(\mathcal{D}3)$	$\mathrm{L}_6^\epsilon(q)$	$\begin{cases} \mathrm{PSp}_{20}(q) & p\neq 2 \\ \Omega_{20}^{\epsilon'}(q) & p=2 \end{cases}$	$\Lambda^3 V_6$
$(\mathcal{D}4)$	$\mathrm{L}_3(4)$	$\mathrm{L}_9^\epsilon(2)$	
$(\mathcal{D}5)$	$\mathrm{PSp}_4(q)'$	$\mathrm{P}\Omega_{10}^\epsilon(q)$	S^2V_4
$(\mathcal{D}6)$	$\mathrm{PSp}_6(q)$	$\mathrm{PSp}_{14}(q)$	$M(\lambda_3),\ p>2$
$(\mathcal{D}7)$	$\mathrm{PSp}_6(q)$	$\begin{cases} \mathrm{P}\Omega_{14}^\epsilon(q) & p\neq 3 \\ \Omega_{13}(q) & p=3 \end{cases}$	$M(\lambda_2)$
$(\mathcal{D}8)$	$\mathrm{PSp}_8(q)$	$\begin{cases} \Omega_{27}(q) & p\neq 2 \\ \Omega_{26}^\epsilon(q) & p=2 \end{cases}$	
$(\mathcal{D}9)$	$\begin{cases} \Omega_{11}(q) & p>2 \\ \mathrm{Sp}_{10}(q) & p=2 \end{cases}$	$\begin{cases} \mathrm{PSp}_{32}(q) & p>2 \\ \Omega_{32}^+(q) & p=2 \end{cases}$	spin module
$(\mathcal{D}10)$	$\mathrm{P}\Omega_{12}^+(q)$	$\begin{cases} \mathrm{PSp}_{32}(q) & p>2 \\ \Omega_{32}^+(q) & p=2 \end{cases}$	spin module
$(\mathcal{D}11)$	$F_4(q)$	$\begin{cases} \mathrm{P}\Omega_{26}^+(q) & p\neq 3 \\ \Omega_{25}(q) & p=3 \end{cases}$	$M(\lambda_1)$
$(\mathcal{D}12)$	$F_4(q)$	$\Omega_{26}^+(q)$	$M(\lambda_4),\ p=2$

TABLE 11. The collection $\mathcal{D}$: Defining characteristic subgroups

If $r=2$ a similar calculation reveals that x is conjugate to $[-I_4, I_3]$, so $|x^G|\geq \frac{1}{2}q^6(q^6-1)=b_3$ and we note that

$$i_2(H\cap \mathrm{PGL}(V))\leq \frac{|\mathrm{GL}_3^\epsilon(q)|}{|\mathrm{GL}_2^\epsilon(q)||\mathrm{GL}_1^\epsilon(q)|}+\frac{|\mathrm{PGL}_3^\epsilon(q)|}{|\mathrm{SO}_3(q)|}=q^2(q^2+\epsilon q+1)+q^2(q^3-\epsilon)=a_3.$$

Now suppose $r>3$. By Theorem 2.12 we have $\nu(x)\geq 4$ (there are no elements $y\in G$ of order r with $\nu(y)=3$). If $\nu(x)=4$ then a calculation with the adjoint module reveals that r divides $q-\epsilon$ and $C_{\bar{G}}(x)$ is of type $O_3\times \mathrm{GL}_2$, so

$$|x^G|\geq q^7(q+1)(q^2+1)(q^4+q^2+1)=b_4$$

and we note that there are at most

$$(q-\epsilon)\frac{|\mathrm{GL}_3^\epsilon(q)|}{|\mathrm{GL}_2^\epsilon(q)||\mathrm{GL}_1^\epsilon(q)|}=q^2(q^3-\epsilon)=a_4$$

elements of this type in H. Similarly, if $\nu(x)=5$ then r divides $q-\epsilon$ and $C_{\bar{G}}(x)$ is of type $\mathrm{GL}_2\times \mathrm{GL}_1$, so

$$|x^G|\geq q^8(q+\epsilon)^2(q^2+1)(q^4+q^2+1)=b_5$$

and H contains at most $q^3(q+\epsilon)(q^3-\epsilon)=a_5$ such elements. Finally, if $\nu(x)=6$ then

$$|x^G|\geq \frac{|\mathrm{SO}_7(q)|}{(q+1)^3}=q^9(q-1)^2(q^2+1)(q^3-1)(q^2-q+1)=b_6$$

and of course there are fewer than $|\mathrm{PGL}_3^\epsilon(q)|=a_6$ such elements in H.

If $x\in H$ is an involutory field automorphism then $|x^G|\geq q^{9/2}(q+1)(q^2+1)(q^3+1)=b_7$. Moreover, if $\epsilon=+$ then

$$|x^G\cap H|\leq \frac{|\mathrm{PGL}_3(q)|}{|\mathrm{PGL}_3(q^{1/2})|}+\frac{|\mathrm{PGL}_3(q)|}{|\mathrm{PGU}_3(q^{1/2})|}=2q^3(q+1),$$

while we get

$$|x^G \cap H| \leq \frac{|\mathrm{PGU}_3(q)|}{|\mathrm{SO}_3(q)|} = q^2(q^3+1) = a_7$$

when $\epsilon = -$. Finally, if x is a field automorphism of odd prime order r then $|x^G \cap H| < 2q^{8(1-r^{-1})}$ and $|x^G| > \frac{1}{4}q^{21(1-r^{-1})} = f(r)$, so $\mathrm{fpr}(x) < 8q^{-13(1-r^{-1})} = g(r)$ and it follows that the contribution to $\widehat{Q}(G,2)$ from these elements is less than

$$\sum_{r\in\pi}(r-1)\cdot h(r) < 2h(3) + 4h(5) + 6h(7) + \log_3 q.q^{21}g(11)^2,$$

where $h(r) = f(r)g(r)^2$ and π is the set of odd prime divisors of $\log_3 q$. We conclude that if $p = 3$ and $q \geq 9$ then

$$\widehat{Q}(G,2) < \sum_{i=1}^{7} b_i(a_i/b_i)^2 + 2h(3) + 4h(5) + 6h(7) + \log_3 q.q^{21}g(11)^2 < q^{-1/13},$$

so $b(G) = 2$, and $P(G,2)$ tends to 1 as q tends to infinity.

Now assume $p \neq 3$. The argument is similar and so for brevity we shall assume $p = 2$, in which case $q \geq 4$. Let $x \in H \cap \mathrm{PGL}(V)$ be an element of prime order r. If $r = 2$ then we obtain the following bounds $|x^G \cap H| \leq c_i$ and $|x^G| \geq d_i$:

i	x	G_0-class of x	c_i	d_i
1	$[J_2, I_1]$	c_4	$(q+\epsilon)(q^3-\epsilon)$	$q^2(q^4-1)^2(q^6-1)$
2	γ	b_3	$q^2(q^3-\epsilon)$	$q^3(q^2+1)(q^4-1)(q^6-1)$

Next assume $r > 2$, so Theorem 2.12 gives $\nu(x) \geq 4$. If $\nu(x) = 4$ then $|x^G| > \frac{1}{2}Qq^{18} = d_3$ and we have previously observed that there are at most $q^2(q^3-\epsilon) = c_3$ such elements in H. It is easy to see that there are no elements $x \in H$ with $\nu(x) = 5$, while $|x^G| > \frac{1}{2}Q^3q^{22} = d_4$ if $\nu(x) \geq 6$. Clearly, there are less than $|\mathrm{PGL}_3^\epsilon(q)| = c_4$ elements of odd prime order in $H \cap \mathrm{PGL}(V)$.

If x is an involutory field or graph-field automorphism then $q = q_0^2$, so $\epsilon = +$ (since $q \equiv 1 \pmod 3$), $|x^G| > q^{14} = d_5$ and

$$|x^G \cap H| \leq \frac{|\mathrm{PGL}_3(q)|}{|\mathrm{PGL}_3(q^{1/2})|} + \frac{|\mathrm{PGL}_3(q)|}{|\mathrm{PGU}_3(q^{1/2})|} = 2q^3(q+1) = c_5.$$

Next fix a triality graph automorphism τ of G_0 such that $C_{G_0}(\tau) = \mathrm{PGL}_3^\epsilon(q)$. If $x = \tau\phi$ is a triality graph-field automorphism, where ϕ is a field automorphism of order three and $[\tau,\phi] = 1$, then $x^G \cap H \subseteq \mathrm{PGL}_3^\epsilon(q)\phi \times \langle\tau\rangle$ and thus

$$|x^G \cap H| \leq 2\frac{|\mathrm{PGL}_3^\epsilon(q)|}{|\mathrm{PGL}_3^\epsilon(q^{1/3})|} < 4q^{16/3} = c_6$$

and $|x^G| > q^{56/3} = d_6$. Similarly, if x is a triality graph automorphism then $x^G \cap H \subseteq \mathrm{PGL}_3^\epsilon(q) \times \langle\tau\rangle$, so [36, Proposition 1.3] implies that

$$|x^G \cap H| \leq 2i_3(\mathrm{PGL}_3^\epsilon(q)) < 4(q+1)q^5 = c_7 = c_8.$$

Moreover, $|x^G| \geq q^6(q^4-1)^2 = d_7$ if x is a G_2-type triality, otherwise $|x^G| \geq q^9(q^4-1)^2(q^3-1) = d_8$.

Finally, if x is a field automorphism of odd prime order r then $|x^G \cap H| < 2q^{8(1-r^{-1})}$ and $|x^G| > q^{28(1-r^{-1})} = f'(r)$, so $\mathrm{fpr}(x) < 2q^{-20(1-r^{-1})} = g'(r)$ and it follows that the contribution to $\widehat{Q}(G,2)$ from these field automorphisms is less than

$$\sum_{r\in\pi'}(r-1)\cdot h'(r) < 2h'(3) + 4h'(5) + \log_2 q.q^{28}g'(7)^2,$$

where $h'(r) = f'(r)g'(r)^2$ and π' is the set of odd prime divisors of $\log_2 q$.

We conclude that if $p = 2$ then

$$\widehat{Q}(G,2) < \sum_{i=1}^{8} d_i(c_i/d_i)^2 + 2h'(3) + 4h'(5) + \log_2 q.q^{28}g'(7)^2,$$

which is less than $q^{-1/2}$ for all $q \geq 8$. Finally, if $q = 4$ then $\epsilon = +$ and a straightforward calculation yields $\widehat{Q}(G,2) < 1$ (note that $i_3(\mathrm{PGL}_3(4)) = 6368$). □

Lemma 6.6. *Proposition 6.4 holds for the remaining cases in $\mathcal{D}$.*

Proof. First consider ($\mathcal{D}2$). Suppose $x \in H \cap \mathrm{PGL}(V)$ has prime order r. If $r > 2$ then Theorem 2.12 implies that $\nu(x) \geq 4$ and a straightforward calculation with the adjoint module reveals that the same bound holds when $r = 2$, so Proposition 2.6 yields $|x^G| > \frac{1}{4}Qq^{36} = b$. By Proposition 2.8, this lower bound also applies if $x \in H \setminus \mathrm{PGL}(V)$, hence $\widehat{Q}(G,2) < a^2/b < q^{-1}$, where $a = 2\log_2 q.q^{15}$. The case ($\mathcal{D}3$) is very similar. Here an easy calculation with the relevant module yields $\nu(x) \geq 6$ for all $x \in H \cap \mathrm{PGL}(V)$ of prime order (see [10, p.337], for example), hence $|x^G| > \frac{1}{4}Qq^{78}$ and the result quickly follows.

Next consider ($\mathcal{D}4$). Suppose $\epsilon = -$ and let $x \in H_0$ be an element of odd prime order. By inspecting the 2-modular character table of H_0 (see [32, p.54]) we compute the following bounds:

H_0-class of x	$\lvert x^G \cap H\rvert \leq$	$\lvert x^G\rvert >$
$3A$	2240	2^{50}
$5A,\ 5B$	8064	2^{62}
$7A,\ 7B$	5760	2^{65}

Now, $i_3(\mathrm{Aut}(H_0)) - i_3(H_0) = 2592$ and Theorem 2.12 implies that $|x^G| > 2^{34}$ if $x \in H \setminus H_0$ has order 3 (see Proposition 2.6). The same bound on $|x^G|$ applies for any involution $x \in H$ and we calculate that $i_2(\mathrm{Aut}(H_0)) = 1963$. We quickly deduce that $\widehat{Q}(G,2) < 1$ as required. The case $\epsilon = +$ is entirely similar.

For ($\mathcal{D}5$), an easy calculation with the symmetric square S^2V_4 reveals that $|x^G| > \frac{1}{4}q^{30} = b_1$ for all $x \in H$ of odd prime order, while $|x^G| > \frac{1}{4}q^{45/2} = b_2$ for any involution $x \in H$. Now $|H| < 2\log_2 q.q^{10} = a_1$ and [36, Proposition 1.3] yields $i_2(\mathrm{Aut}(H_0)) < 2(q+1)q^5 = a_2$, whence $\widehat{Q}(G,2) < a_1^2/b_1 + a_2^2/b_2 < q^{-1}$.

The cases ($\mathcal{D}6$) and ($\mathcal{D}7$) are very similar. For instance, in ($\mathcal{D}6$), V is the wedge cube of the natural module for H_0, factored out by a copy of the natural module. It is easy to check that $|x^G| > \frac{1}{2}Qq^{46}$ for all $x \in H$ of odd prime order. For example, if $x \in H_0$ is a transvection then x has Jordan form $[J_2^5, I_4]$ and the bound on $|x^G|$ follows. Similarly, if $x \in H$ is an involution then $|x^G| > \frac{1}{2}q^{40}$ and we note that $i_2(\mathrm{Aut}(H_0)) < 2(q+1)q^{11}$ by [36, Proposition 1.3]. The desired result quickly follows.

For ($\mathcal{D}8$), V is the nontrivial composition factor of the H_0-module $\Lambda^2 V_8$. A straightforward calculation establishes $\nu(x) \geq 6$ for all $x \in H \cap \mathrm{PGL}(V)$ of prime order and it follows that $|x^G| > \frac{1}{2}q^{114}$ for any $x \in H$ of prime order. This is sufficient since $|H| < \log_2 q.q^{36}$.

The remaining cases are very easy. For ($\mathcal{D}9$) and ($\mathcal{D}10$) we note that [10, Lemma 7.2] gives $\nu(x) \geq 8$ for all $x \in H \cap \mathrm{PGL}(V)$, so $|x^G| > \frac{1}{2}q^{184}$ for all $x \in H$. Similarly, for ($\mathcal{D}11$) and ($\mathcal{D}12$) we deduce that $|x^G| > \frac{1}{4}q^{108}$ for all $x \in H$. In all four cases, the desired result follows in the usual manner, using a suitable upper bound for $|H|$. □

6.2. **Non-defining characteristic.** To complete the proof of Theorems 1 and 2 (for $n \geq 6$) we may assume that the simple group H_0 is not of Lie type in the defining characteristic.

Lemma 6.7. *Suppose $H_0 = \mathrm{L}_2(\ell)$, where $(\ell, p) = 1$. Then $b(G) = 2$, and $P(G,2)$ tends to 1 as $|G|$ tends to infinity.*

Proof. Here G is symplectic or orthogonal, and the various possibilities are listed in [29, Table 2]. Very similar arguments apply in each case, so we only provide details when $G_0 = \mathrm{PSp}_n(q)$ with $n = \frac{1}{2}(\ell - 1)$, $p > 2$, $\ell \equiv 1 \pmod 4$ and $\mathbb{F}_q = \mathbb{F}_p[\sqrt{\ell}]$. Let $x \in H$ be an element of prime order and note that $\ell \geq 13$ since we are assuming $n \geq 6$. By applying Theorem 2.12, together with Propositions 2.6 and 2.8, we deduce that

$$|H| \leq |\mathrm{Aut}(H_0)| \leq \log_3 \ell.\ell(\ell^2 - 1), \quad |x^G| > \frac{1}{4} Q q^{\alpha(n-\alpha)},$$

where α is the smallest integer greater than $\max\{2, \frac{1}{2}\sqrt{n}\}$. These bounds imply that $\widehat{Q}(G,2) \to 0$ as $|G| \to \infty$, so the desired asymptotic result holds. In addition, the bounds yield $\widehat{Q}(G,2) < 1$ (hence $b(G) = 2$), unless $(\ell, q) = (13, 3)$. Here $H = H_0$, $G = G_0$ and using Magma it is easy to check that $b(G) = 2$. □

Now suppose $H_0 \neq \mathrm{L}_2(\ell)$ and recall that we may assume $6 \leq n < N$, where $N = 14$ if $G_0 = \mathrm{L}^{\epsilon}_n(q)$, otherwise $N = 64$ (see Proposition 6.1). In [30], Hiss and Malle list all the absolutely irreducible representations of quasisimple groups with degree at most 250, excluding groups of Lie type in the defining characteristic. Frobenius-Schur indicators are also recorded and further information is given which allows one to calculate the smallest field over which each representation can be realized.

In order to illustrate how we apply these results, let us consider the case $G_0 = \mathrm{L}^{\epsilon}_n(q)$. As previously remarked, we may assume $n \leq 13$ and we note that Theorem 2.12 implies that $|x^G| > \frac{1}{2} Q q^{6n-18} = b$ for all $x \in H$ of prime order (see Corollary 2.7). Since $|H| \leq |\mathrm{Aut}(H_0)| = a$ we have $\widehat{Q}(G,2) < a^2/b$, and by examining [30] case-by-case, excluding any examples which have already appeared in one of the $\mathcal{A}$, $\mathcal{B}$ or $\mathcal{C}$ collections, we deduce that $b(G) = 2$ unless $G_0 = \mathrm{U}_6(2)$ and $H_0 = A_7$. (In the same way, we also deduce that $P(G,2)$ tends to 1 as $|G|$ tends to infinity.) The same approach applies if G is a symplectic or orthogonal group, and in this way we reduce to the specific list of cases in Table 12, which we refer to as the $\mathcal{E}$ collection. (If $G_0 = \mathrm{P}\Omega^+_8(q)$ we use [33] to exclude any non-maximal candidates for H.)

Proposition 6.8. *If $H \in \mathcal{E}$ then $b(G) = 2$.*

Proof. First consider ($\mathcal{E}6$), where $H = \mathrm{Co}_1$ and $G = \mathrm{P}\Omega^{\epsilon}_{24}(3)$. Suppose $x \in H$ has prime order r. Then [28, Table 1] implies that $\nu(x) \geq 5$, and thus $\nu(x) \geq 6$ since $x \in G_0$. Therefore $|x^G| > \frac{1}{16} 3^{103}$ (by Proposition 2.6) and the trivial bound $|x^G \cap H| \leq i_r(H)$ yields $\widehat{Q}(G,2) < 1$.

In each of the remaining cases the relevant modular character table is available in the GAP Character Table Library [8], and by inspecting the values of the corresponding Brauer character we quickly deduce that $\widehat{Q}(G,2) < 1$. For example, consider the embedding labelled ($\mathcal{E}12$) and let $x \in H$ be an element of prime order r. By inspecting the 2-modular character table of M_{12} (see [32, p.74]) we can compute $\mathrm{fpr}(x)$ precisely when $r > 2$. We can do the same for involutions by using the Web Atlas [48] and Magma to explicitly construct $\mathrm{M}_{12}.2$ as a subgroup of the matrix group $O^-_{10}(2)$. In this way we obtain the results listed in Table 13, where $\omega \in K$ is a primitive r-th root of unity. The desired bound $\widehat{Q}(G,2) < 1$ follows immediately. The other cases are very similar and we leave the details to the reader. □

	H_0	G_0
$(\mathcal{E}1)$	A_7	$\mathrm{U}_6(2)$
$(\mathcal{E}2)$	Co_3	$\mathrm{Sp}_{22}(2)$
$(\mathcal{E}3)$	Suz	$\mathrm{PSp}_{12}(3)$
$(\mathcal{E}4)$	$G_2(4)$	$\mathrm{PSp}_{12}(3)$
$(\mathcal{E}5)$	J_2	$\mathrm{Sp}_6(4)$
$(\mathcal{E}6)$	Co_1	$\mathrm{P}\Omega^{\epsilon}_{24}(3)$
$(\mathcal{E}7)$	Co_2	$\Omega^{+}_{22}(2)$
$(\mathcal{E}8)$	McL	$\Omega^{\epsilon}_{22}(2)$
$(\mathcal{E}9)$	A_{10}	$\Omega^{+}_{16}(2)$
$(\mathcal{E}10)$	$G_2(3)$	$\Omega^{\epsilon}_{14}(2)$
$(\mathcal{E}11)$	$\mathrm{L}_3(3)$	$\Omega^{-}_{12}(2)$
$(\mathcal{E}12)$	M_{12}	$\Omega^{-}_{10}(2)$
$(\mathcal{E}13)$	M_{12}	$\mathrm{P}\Omega^{+}_{10}(3)$
$(\mathcal{E}14)$	M_{11}	$\Omega^{-}_{10}(2)$
$(\mathcal{E}15)$	$\mathrm{Sz}(8)$	$\mathrm{P}\Omega^{+}_{8}(5)$
$(\mathcal{E}16)$	A_{10}	$\mathrm{P}\Omega^{+}_{8}(5)$

TABLE 12. The collection $\mathcal{E}$: Subgroups in non-defining characteristic

r	H_0-class of x	$O^{-}_{10}(2)$-class of x	$\lvert x^G \cap H\rvert$	$\lvert x^G\rvert$
2	$2A$	a_4	396	706860
	$2B$	c_4	495	21205800
	$2C$	b_5	792	33929280
3	$3A$	$[I_4, \omega I_3, \omega^2 I_3]$	1760	1072332800
	$3B$	$[I_2, \omega I_4, \omega^2 I_4]$	2640	107233280
5	$5A$	$[I_2, \omega I_2, \omega^2 I_2, \omega^3 I_2, \omega^4 I_2]$	9504	27794866176
	$11A$, $11B$	$[\omega, \ldots, \omega^{10}]$	17280	1516083609600

TABLE 13. Case $(\mathcal{E}12)$

7. The low dimensional classical groups

Here we complete the proof of Theorems 1 and 2 by dealing with the remaining classical groups with $n < 6$. The relevant subgroups are listed in Table 14, where as usual H_0 denotes the socle of H (see [7]). Our main result is the following:

Proposition 7.1. *Suppose $H \in \mathcal{S}$ and $n < 6$. Then either $b(G) = 2$, or $(G, H, b(G))$ is one of the cases listed in Table 15.*

Moreover, if (G_i, H_i) is a sequence of primitive almost simple classical groups, where $H_i \in \mathcal{S}$, $|G_i|$ tends to infinity and the dimension of each natural G_i-module is less than 6, then $P(G_i, 2)$ tends to 1 unless there exists an infinite subsequence with

$$(\mathrm{Soc}(G_i), \mathrm{Soc}(H_i)) = (\mathrm{PSp}_4(q)', \mathrm{Sz}(q))$$

(with q even). For such a subsequence, $P(G_i, 3)$ tends to 1.

Proof. First consider the case labelled $(\mathcal{S}13)$, so $G_0 = \mathrm{PSp}_4(q)$, $H_0 = \mathrm{Sz}(q)$ and $q \geq 8$ is even. Here [13, Lemma 4.2] states that $b(G) = 3$, and the proof of this lemma also implies

	G_0	H_0	Conditions
$(\mathcal{S}1)$	$\mathrm{L}_5(q)$	$\mathrm{U}_4(2)$	$q = p \equiv 1 \pmod 6$
$(\mathcal{S}2)$		$\mathrm{L}_2(11)$	$q = p \equiv 1, 3, 4, 5, 9 \pmod{11}$
$(\mathcal{S}3)$		M_{11}	$q = 3$
$(\mathcal{S}4)$	$\mathrm{U}_5(q)$	$\mathrm{U}_4(2)$	$q = p \equiv 5 \pmod 6$
$(\mathcal{S}5)$		$\mathrm{L}_2(11)$	$q = p \equiv 2, 6, 7, 8, 10 \pmod{11}$
$(\mathcal{S}6)$	$\mathrm{L}_4(q)$	$\mathrm{U}_4(2)$	$q = p \equiv 1 \pmod 6$
$(\mathcal{S}7)$		A_7	$q = p \equiv 1, 2, 4 \pmod 7$
$(\mathcal{S}8)$		$\mathrm{L}_2(7)$	$q = p \equiv 1, 2, 4 \pmod 7$, $q \neq 2$
$(\mathcal{S}9)$	$\mathrm{U}_4(q)$	$\mathrm{U}_4(2)$	$q = p \equiv 5 \pmod 6$
$(\mathcal{S}10)$		A_7	$q = p \equiv 3, 5, 6 \pmod 7$
$(\mathcal{S}11)$		$\mathrm{L}_2(7)$	$q = p \equiv 3, 5, 6 \pmod 7$, $q \neq 3$
$(\mathcal{S}12)$		$\mathrm{L}_3(4)$	$q = 3$
$(\mathcal{S}13)$	$\mathrm{PSp}_4(q)$	$\mathrm{Sz}(q)$	$q = 2^{2a+1} > 2$
$(\mathcal{S}14)$		$\mathrm{L}_2(q)$	$p \geq 5, q \neq 5$
$(\mathcal{S}15)$		A_6	$q = p \equiv 1, 5, 7, 11 \pmod{12}$, $q \neq 7$
$(\mathcal{S}16)$		A_7	$q = 7$
$(\mathcal{S}17)$	$\mathrm{L}_3(q)$	$\mathrm{L}_2(7)$	$q = p \equiv 1, 2, 4 \pmod 7$, $q \neq 2$
$(\mathcal{S}18)$		A_6	$q = p \equiv 1, 4 \pmod{15}$, or $q = p^2$, $p \equiv 2, 3 \pmod 5$, $p \neq 3$
$(\mathcal{S}19)$	$\mathrm{U}_3(q)$	$\mathrm{L}_2(7)$	$q = p \equiv 3, 5, 6 \pmod 7$
$(\mathcal{S}20)$		A_6	$q = 5$ or $q = p \equiv 11, 14 \pmod{15}$
$(\mathcal{S}21)$		A_7	$q = 5$
$(\mathcal{S}22)$	$\mathrm{L}_2(q)$	A_5	$q = p \equiv \pm 1 \pmod{10}$, or $q = p^2$, $p \equiv \pm 3 \pmod{10}$

TABLE 14. The collection $\mathcal{S}$: Low dimensional groups ($n < 6$)

$b(G)$	G_0	H_0	Conditions
4	$\mathrm{U}_4(3)$	$\mathrm{L}_3(4)$	
	$\mathrm{U}_3(5)$	A_7	
	$\mathrm{U}_3(3)$	$\mathrm{L}_2(7)$	$G = G_0.2$
3	$\mathrm{PSp}_4(q)$	$\mathrm{Sz}(q)$	$q = 2^{2a+1} > 2$
	$\mathrm{U}_4(3)$	A_7	
	$\mathrm{L}_3(4)$	A_6	
	$\mathrm{U}_3(5)$	A_6	
	$\mathrm{U}_3(5)$	$\mathrm{L}_2(7)$	$G = G_0.2$
	$\mathrm{U}_3(3)$	$\mathrm{L}_2(7)$	$G = G_0$
	$\mathrm{L}_2(19)$	A_5	
	$\mathrm{L}_2(11)$	A_5	

TABLE 15. $H \in \mathcal{S}$, $n < 6$, $b(G) > 2$

that $P(G, 3)$ tends to 1 as q tends to infinity. The cases $(\mathcal{S}3)$, $(\mathcal{S}12)$, $(\mathcal{S}16)$ and $(\mathcal{S}21)$ are all easily checked with the aid of MAGMA.

Next consider case $(\mathcal{S}14)$. Here $G_0 = \mathrm{PSp}_4(q)$, $H_0 = \mathrm{L}_2(q)$ and $p \geq 5$ (with $q \neq 5$). This embedding arises from the irreducible representation of $\mathrm{SL}_2(q)$ afforded by the module S^3V_2, where V_2 is the natural $\mathrm{SL}_2(q)$-module. For $q \leq 13$, an easy MAGMA calculation yields $b(G) = 2$, so let us assume $q \geq 17$. Set $\tilde{G} = \mathrm{PGSp}_4(q)$.

Let $x \in H \cap \mathrm{PGL}(V)$ be an element of prime order r. If $r = p$ then an easy calculation with the module S^3V_2 reveals that x has Jordan form $[J_4]$, so $|x^G| \geq \frac{1}{2}q^2(q^2-1)(q^4-1) = b_1$ and there are $q^2 - 1 = a_1$ such elements in H. Similarly, if $r = 2$ then $C_G(x)$ is of type $\mathrm{GL}_2^\epsilon(q)$, so $|x^G| \geq \frac{1}{2}q^3(q-1)(q^2+1) = b_2$ and we note that $H \cap \mathrm{PGL}(V)$ contains at most $q^2 = a_2$ involutions. Also, if $r = 3$ then x is $\bar{G}$-conjugate to $[I_2, \omega, \omega^2]$, whence $|x^G| \geq q^3(q-1)(q^2+1) = b_3$ and $|x^G \cap H| \leq q(q+1) = a_3$. Finally, suppose $r \geq 5$ and $r \neq p$. Let $i \geq 1$ be minimal such that r divides $q^i - 1$, so $i = 1$ or 2. If $i = 1$ then

$$|x^{\tilde{G}} \cap H| \leq \frac{|\mathrm{GL}_2(q)|}{(q-1)^2} = q(q+1) = a_4, \;\; |x^G| \geq \frac{|\mathrm{Sp}_4(q)|}{(q-1)^2} = q^4(q+1)^2(q^2+1) = b_4$$

and we note that there are fewer than $\frac{1}{2}q\log(q-1) = n_4$ distinct $\tilde{G}$-classes of such elements. On the other hand, if $i = 2$ then

$$|x^{\tilde{G}} \cap H| \leq \frac{|\mathrm{GL}_2(q)|}{(q^2-1)} = q(q-1) = a_5, \;\; |x^G| \geq \frac{|\mathrm{Sp}_4(q)|}{(q+1)^2} = q^4(q-1)^2(q^2+1) = b_5$$

and there are less than $\frac{1}{2}q\log(q+1) = n_5$ distinct $\tilde{G}$-classes in this case.

Finally, suppose $x \in H \setminus \mathrm{PGL}(V)$ has prime order r, so $q = q_0^r$ and x is a field automorphism. If $r = 2$ then

$$|x^G \cap H| \leq \frac{|\mathrm{SL}_2(q)|}{|\mathrm{SL}_2(q^{1/2})|} = q^{1/2}(q+1) = a_6, \;\; |x^G| \geq \frac{1}{2}q^2(q+1)(q^2+1) = b_6.$$

Similarly, if r is odd then $|x^G \cap H| < 2q^{3(1-1/r)}$ and $|x^G| > \frac{1}{4}q^{10(1-1/r)} = f(r)$, whence $\mathrm{fpr}(x) < 8q^{-7(1-1/r)} = g(r)$ and so the contribution to $\widehat{Q}(G,2)$ from field automorphisms is less than

$$\sum_{r \in \pi}(r-1)h(r) < b_6(a_6/b_6)^2 + 2h(3) + 4h(5) + 6h(7) + \log_5 q.q^{10}g(11)^2 = \Gamma,$$

where $h(r) = f(r)g(r)^2$ and π is the set of odd prime divisors of $\log_p q$. We conclude that

$$\widehat{Q}(G,2) < \sum_{i=1}^{5} n_i b_i (a_i/b_i)^2 + \alpha\Gamma < q^{-1/20}$$

for all $q \geq 7$, where $n_1 = n_2 = n_3 = 1$ and $\alpha = 1 - \delta_{p,q}$. Therefore $b(G) = 2$, and we also see that $\widehat{Q}(G,2)$ tends to 0 as q tends to infinity.

In each of the remaining cases we proceed in the usual manner, using the relevant character table to compute the precise fixed point ratios. As before, for small values of q it is convenient to use Magma to determine the base size via random search. We leave the reader to check the details. □

This completes the proof of Theorems 1 and 2.

References

[1] M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), 469–514.

[2] M. Aschbacher and G.M. Seitz, *Involutions in Chevalley groups over fields of even order*, Nagoya Math. J. **63** (1976), 1–91.

[3] J. Bamberg, M. Giudici, M.W. Liebeck, C.E. Praeger and J. Saxl, *The classification of almost simple $\frac{3}{2}$-transitive groups*, Trans. Amer. Math. Soc., to appear.

[4] A. Bochert, *Über die Zahl verschiedener Werte, die eine Funktion gegebener Buchstaben durch Vertauschung derselben erlangen kann*, Math. Ann. **33** (1889), 584–590.

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

[6] N. Bourbaki, *Groupes et Algebrès de Lie (Chapters 4,5 and 6)*, Hermann, Paris, 1968.

[7] J.N. Bray, D.F. Holt and C.M. Roney-Dougal, *The Maximal Subgroups of the Low-dimensional Finite Classical Groups*, to appear in the LMS Lecture Note Series, Cambridge University Press.

[8] T. Breuer, *Manual for the* GAP *Character Table Library, Version 1.1*, RWTH Aachen (2004).

[9] T. Breuer, GAP *Computations with* $O^+(8,5).S_3$ *and* $O^+(8,2).S_3$, RWTH Aachen (2006) (`http://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib/htm/o8p2s3_o8p5s3.htm`).

[10] T.C. Burness, *Fixed point spaces in actions of classical algebraic groups*, J. Group Theory **7** (2004), 311–346.

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

[12] T.C. Burness, *Fixed point ratios in actions of finite classical groups,* IV, J. Algebra **314** (2007), 749–788.

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

[14] T.C. Burness, R.M. Guralnick and J. Saxl, *On base sizes for symmetric groups*, Bull. London Math. Soc. **43** (2011), 386–391.

[15] T.C. Burness, R.M. Guralnick and J. Saxl, *On base sizes for algebraic groups*, preprint.

[16] T.C. Burness, R.M. Guralnick and J. Saxl, *Base sizes for geometric actions of finite classical groups*, in preparation.

[17] T.C. Burness, M.W. Liebeck, and A. Shalev, *Base sizes for simple groups and a conjecture of Cameron*, Proc. London Math. Soc. **98** (2009), 116–162.

[18] T.C. Burness, E.A. O'Brien, and R.A. Wilson, *Base sizes for sporadic simple groups*, Israel J. Math. **177** (2010), 307–334.

[19] T.C. Burness, C.E. Praeger and Á. Seress, *Extremely primitive classical groups*, J. Pure Appl. Algebra, in press.

[20] T.C. Burness, C.E. Praeger and Á. Seress, *Extremely primitive sporadic and alternating groups*, submitted.

[21] P.J. Cameron and W.M. Kantor, *Random permutations: some group-theoretic aspects*, Combin. Probab. Comput. **2** (1993), 257–262.

[22] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.

[23] D.I. Deriziotis and G. Michler, *Character table and blocks of the finite simple triality groups* ${}^3D_4(q)$, Trans. Amer. Math. Soc. **303** (1987), 39–70.

[24] The GAP Group, *GAP – Groups, Algorithms and Programming*, Version 4.4, 2004.

[25] D. Goldstein and R.M. Guralnick, *Alternating forms and self-adjoint operators*, J. Algebra **308** (2007), 330–349.

[26] D. Gorenstein and R. Lyons, *The local structure of finite groups of characteristic 2 type*, Mem. Amer. Math. Soc. **276** (1983).

[27] D. Gorenstein, R. Lyons, and R. Solomon, *The Classification of the Finite Simple Groups, Number 3*, Mathematical Surveys and Monographs, vol. 40, Amer. Math. Soc., 1998.

[28] R.M. Guralnick and J. Saxl, *Generation of finite almost simple groups by conjugates*, J. Algebra **268** (2003), 519–571.

[29] G. Hiss and G. Malle, *Low dimensional representations of quasi-simple groups*, LMS J. Comput. Math. **4** (2001), 22–63.

[30] G. Hiss and G. Malle, *Corrigenda: Low dimensional representations of quasi-simple groups*, LMS J. Comput. Math. **5** (2002), 95–126.

[31] G.D. James, *On the minimal dimensions of irreducible representations of symmetric groups*, Math. Proc. Camb. Phil. Soc. **94** (1983), 417–424.

[32] C. Jansen, K. Lux, R. Parker, and R. Wilson, *An Atlas of Brauer Characters*, LMS Monographs, no. 11, Oxford University Press, 1995.

[33] P.B. Kleidman, *The maximal subgroups of the finite 8-dimensional orthogonal groups* $\mathrm{P}\Omega_8^+(q)$ *and of their automorphism groups*, J. Algebra **110** (1987), 173–242.

[34] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 129, Cambridge University Press, 1990.

[35] V. Landazuri and G.M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443.

[36] R. Lawther, M.W. Liebeck, and G.M. Seitz, *Fixed point ratios in actions of finite exceptional groups of Lie type*, Pacific J. Math. **205** (2002), 393–464.

[37] M.W. Liebeck, *On the orders of maximal subgroups of the finite classical groups*, Proc. London Math. Soc. **50** (1985), 426–446.

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

[39] M.W. Liebeck and A. Shalev, *Character degrees and random walks in finite groups of Lie type*, Proc. London Math. Soc. **90** (2005), 61–86.
[40] F. Lübeck, *Small degree representations of finite Chevalley groups in defining characteristic*, LMS J. Comput. Math. **4** (2001), 135–169.
[41] A. Mann, C.E. Praeger, and Á. Seress, *Extremely primitive groups*, Groups Geom. Dyn. **1** (2007), 623–660.
[42] M. Neunhöffer, F. Noeske, E.A. O'Brien and R.A. Wilson, *Orbit invariants and an application to the Baby Monster*, J. Algebra **341** (2011), 297–305.
[43] Á. Seress, *Permutation Group Algorithms*, Cambridge Tracts in Mathematics, vol. 152, Cambridge University Press, Cambridge, 2003.
[44] N. Spaltenstein, *Caractères unipotents de* ${}^3D_4(\mathbb{F}_q)$, Comment. Math. Helv. **57** (1982), 676–691.
[45] A. Wagner, *The faithful linear representations of least degree of S_n and A_n over a field of characteristic* 2, Math. Z. **151** (1976), 127–137.
[46] A. Wagner, *The faithful linear representations of least degree of S_n and A_n over a field of odd characteristic*, Math. Z. **154** (1977), 103–114.
[47] A. Wagner, *An observation on the degrees of projective representations of the symmetric and alternating groups over an arbitrary field*, Arch. Math. **29** (1977), 583–589.
[48] R.A. Wilson et al., *A World-Wide-Web Atlas of finite group representations*, `http://brauer.maths.qmul.ac.uk/Atlas/v3/`.

School of Mathematics, University of Southampton, Southampton SO17 1BJ, UK

E-mail address: `t.burness@soton.ac.uk`

Department of Mathematics, University of Southern California, Los Angeles CA 90089, USA

E-mail address: `guralnic@usc.edu`

Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Cambridge CB3 0WB, UK

E-mail address: `j.saxl@dpmms.cam.ac.uk`