Fixed point ratios in actions of finite classical groups, II

Timothy C. Burness
St John's College
Oxford OX1 3JP
England

July 8, 2006

Abstract

This is the second in a series of four papers on fixed point ratios in non-subspace actions of finite classical groups. Our main result states that if G is a finite almost simple classical group and Ω is a non-subspace G-set then either $\mathrm{fpr}(x) \lesssim |x^G|^{-\frac{1}{2}}$ for all elements $x \in G$ of prime order, or (G, Ω) is one of a small number of known exceptions. In this paper we record a number of preliminary results and prove the main theorem in the case where the stabilizer G_ω is contained in a maximal non-subspace subgroup which lies in one of the Aschbacher families $\mathscr{C}_i$, where $4 \leqslant i \leqslant 8$.

1 Introduction

Let G be a finite almost simple classical group over $\mathbb{F}_q$, with socle G_0 and natural module V, where $q = p^f$ for a prime p. Recall that if G acts on a set Ω then the *fixed point ratio of* $x \in G$, which we denote by $\mathrm{fpr}(x)$, is defined to be the proportion of points in Ω which are fixed by x. If G acts transitively then it is easy to see that

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

where $H = G_\omega$ is the point stabilizer of an element $\omega \in \Omega$. In studying actions of classical groups, it is natural to make a distinction between those actions which permute subspaces of the natural module and those which do not.

Recall from [3] that $H \leqslant G$ is a *subspace subgroup* if every maximal subgroup M of G_0 containing $H \cap G_0$ is either reducible on V or $(G_0, M, p) = (\mathrm{Sp}_{2m}(q)', \mathrm{O}^{\pm}_{2m}(q), 2)$. All other subgroups are *non-subspace* and a transitive action of G on a set Ω is a *non-subspace action* if the point stabilizer G_ω of an element $\omega \in \Omega$ is a non-subspace subgroup of G. Our main result, which we refer to as Theorem 1, states that if Ω is a faithful, transitive, non-subspace G-set then

$$\mathrm{fpr}(x) < |x^G|^{-\frac{1}{2}+\frac{1}{n}+\iota}$$

for all elements $x \in G$ of prime order, where either $\iota = 0$ or (G_0, Ω, ι) belongs to a short list of known exceptions (see [3, Table 1]). In almost all cases $n = \dim V$ (see Remark 1.2).

In order to prove Theorem 1, it is clear from (1) that we may assume G acts primitively. In particular, we can base our proof on Aschbacher's main theorem on the subgroup structure of finite classical groups. In [1], eight collections of subgroups of G are defined, labelled $\mathscr{C}_i$ for $1 \leqslant i \leqslant 8$, and it is shown that if H is a maximal subgroup of G not containing G_0 then either H is contained in one of the $\mathscr{C}_i$ collections, or it belongs to a family $\mathscr{S}$ of almost simple groups

E-mail address: burness@maths.ox.ac.uk

	description
$\mathscr{C}_4$	stabilizers of tensor product decompositions $V = V_1 \otimes V_2$
$\mathscr{C}_5$	stabilizers of subfields of $\mathbb{F}_q$ of prime index
$\mathscr{C}_6$	normalizers of symplectic-type k-groups (k prime) in absolutely irreducible representations
$\mathscr{C}_7$	stabilizers of decompositions $V = \bigotimes_{i=1}^{t} V_i$, where $\dim V_i = a$
$\mathscr{C}_8$	stabilizers of non-degenerate unitary, symplectic or quadratic forms on V

Table 1.1: The subgroup collections $\mathscr{C}_i$, $4 \leqslant i \leqslant 8$

G_0	type of H	ι
$\mathrm{PSL}_n^{\epsilon}(q)$	$\mathrm{Sp}_n(q)$	$1/n$
$\mathrm{PSp}_4(3)$	$2^4.\mathrm{O}_4^-(2)$	.086

Table 1.2: The exceptional cases with $\iota > 0$

which act irreducibly on V (see [18] for a detailed description of these subgroup collections). A small additional collection of subgroups, which we denote by $\mathscr{N}$, arises when G_0 is $\mathrm{Sp}_4(q)'$ (q even) or $\mathrm{P\Omega}_8^+(q)$ (see Table 3.1 and [5, §3]). We follow [18] in labelling the $\mathscr{C}_i$ collections and we note that a maximal subgroup of G is non-subspace unless it is a member of the collection $\mathscr{C}_1$, or is a particular example of a subgroup in $\mathscr{C}_8$.

In [3] we provided some background to Theorem 1 and established a number of corollaries. In addition, we described how Theorem 1 can be applied to the study of bases for primitive actions of finite classical groups and we explained how it may be useful in efforts to classify primitive monodromy groups of covers of Riemann surfaces. In this paper we prove Theorem 1 in the case where G_ω is contained in a maximal non-subspace subgroup which lies in one of the collections $\mathscr{C}_i$, where $4 \leqslant i \leqslant 8$. This is the content of Theorem 1.1 below. A rough description of the relevant $\mathscr{C}_i$ collections is given in Table 1.1.

Theorem 1.1. *Let G be a finite almost simple classical group acting transitively and faithfully on a set Ω with point stabilizer $G_\omega \leqslant H$, where $H \leqslant G$ is a maximal non-subspace subgroup in one of the Aschbacher collections $\mathscr{C}_i$, where $4 \leqslant i \leqslant 8$. Then*

$$\mathrm{fpr}(x) < |x^G|^{-\frac{1}{2}+\frac{1}{n}+\iota}$$

for all elements $x \in G$ of prime order, where either $\iota = 0$ or (G_0, H, ι) is listed in Table 1.2, where G_0 denotes the socle of G.

Remark 1.2. In general, the integer $n = n(G)$ in the statement of Theorem 1.1 is simply the dimension of the natural G_0-module. More precisely, if $G_0 \in \{\mathrm{Sp}_4(2)', \mathrm{SL}_3(2)\}$ then $n = n(G) = 2$, otherwise $n = n(G)$ is defined to be the minimal degree of a non-trivial irreducible $K\widehat{G}_0$-module, where $\widehat{G}_0$ is a covering group of G_0 and K is the algebraic closure of $\mathbb{F}_q$ (see [3, Definition 2]). Following [18, §4], the *type of H* referred to in Table 1.2 provides an approximate group-theoretic structure for $H \cap \mathrm{PGL}(V)$.

This paper is organised as follows. In Section 2 we begin with some general remarks on the proof of Theorem 1 and in Section 3 we present a number of preliminary results which will be needed for the proof; some of these are new and may be of independent interest. The proof proper begins in Section 4 when we consider the tensor product subgroups which comprise Aschbacher's collection $\mathscr{C}_4$. Moreover, for $4 \leqslant i \leqslant 8$, Section i is devoted to a proof of Theorem 1.1 in the case where the stabilizer G_ω is a non-subspace subgroup contained in a member of $\mathscr{C}_i$; the specific cases we need to consider are listed in Table i.1. We adopt the notation of [18] for the possible subgroup types which appear in Table i.1. (For convenience, the $\mathscr{C}_5$-subgroups of type $\mathrm{Sp}_n(q)$ and $\mathrm{O}_n^{\epsilon}(q)$ in unitary groups are considered in §8 and not §5 as might be expected.)

The proof of Theorem 1 is completed in [4] and [5]. In [4] we deal with the imprimitive subgroup collection $\mathscr{C}_2$ and also the field extension subgroups which comprise $\mathscr{C}_3$. Finally, in [5] we consider the irreducible almost simple subgroups in Aschbacher's collection $\mathscr{S}$, together with the small additional set $\mathscr{N}$ of subgroups which arise when G is either an 8-dimensional orthogonal group or a 4-dimensional symplectic group in even characteristic. In both [4] and [5] we will refer repeatedly to the preliminary results collected in §3 of this note.

Notation. Our notation and terminology for classical groups are standard (see [18] for example). In particular, a finite classical group G is said to be *over* $\mathbb{F}_q$ if the natural G-module is defined over $\mathbb{F}_{q^u}$, where $u = 2$ if G is unitary, otherwise $u = 1$. We write $\mathrm{PSL}_n^{\epsilon}(q)$ for $\mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$ if $\epsilon = +$ and $-$ respectively. In addition, for $x \in \mathbb{R}$ it is convenient to write $x - \epsilon$ for $x - \epsilon 1$, where $\epsilon = \pm$. We use the notation $a|b$ to signify that the integer b is divisible by the integer a. Further, $Z(G)$ denotes the centre of a group G; G' is its derived subgroup; G^m is the direct product of m copies of G and $H.G$ denotes an (arbitrary) extension of a group H by G. We write $\mathbb{Z}_n$ or just n to denote a cyclic group of order n, while $\mathbb{Z}_p^m$ or p^m denotes an elementary abelian p-group of order p^m for a prime p. We also use $(a_1, \ldots, a_m)$ to denote the highest common factor of the integers $a_1, \ldots, a_m$.

2 Remarks on the proof of Theorem 1

According to Aschbacher's theorem, a maximal non-subspace subgroup of a finite almost simple classical group belongs to one of nine subgroup collections. In turn, we consider the primitive actions for which the stabilizer of a point belongs to each collection, hence the proof of Theorem 1 is naturally partitioned into nine parts. Inevitably, our methods differ somewhat between the collections; for instance, in some cases we require a greater degree of accuracy than in others. However, there are some common features to our approach which apply quite generally.

Let G be an almost simple classical group over $\mathbb{F}_q$ with socle G_0, where $q = p^f$ for a prime p. Let $H \leqslant G$ be a maximal non-subspace subgroup. In view of (1), it suffices to show that

$$f(x, H) := \frac{\log |x^G \cap H|}{\log |x^G|} < \frac{1}{2} + \frac{1}{n} + \iota \qquad (2)$$

for all elements $x \in G$ of prime order, where $n = n(G_0)$ is defined as in Remark 1.2 and $\iota \geqslant 0$ is given in the statement of [3, Theorem 1]. Of course, we can always assume $x \in H$ and $n \geqslant 3$; in addition, we may also assume $n \geqslant 7$ if G_0 is an orthogonal group. We start by identifying the structure of $H \cap \mathrm{PGL}(V)$, where V is the natural G_0-module, and we then consider the cases $x \in H \cap \mathrm{PGL}(V)$ and $x \in H - \mathrm{PGL}(V)$ in turn.

Case 1. $x \in H \cap \mathrm{PGL}(V)$
Our initial aim is to partition the elements of (fixed) prime order r in $H \cap \mathrm{PGL}(V)$ according to a set of parameters $\underline{z} = (z_1, \ldots, z_m)$ associated to the action of these elements on V. For example, we may choose to partition the elements of order p according to the parameters $\underline{z} = (z_1, z_2, z_3)$, where $z_1 = a_1$, z_2 is the number of non-zero a_j in λ with $j \geqslant 2$ and z_3 is the sum of the terms a_j with j odd, with respect to a general partition $\lambda = (n^{a_n}, \ldots, 1^{a_1}) \vdash n = \dim V$ which corresponds to the possible Jordan normal forms on V of the elements of order p in H. Similar parameters can be defined in the semisimple case (see Definition 3.32 for example). The number of parameters we choose will depend on the degree of accuracy required.

Given $\underline{z}$, we derive bounds on $|x^G \cap H|$ and $|x^G|$ of the form

$$|x^G \cap H| < f_1(\underline{z}')q^{f_2(\underline{z}')\dim x^{\bar{G}}}, \;\; |x^G| > f_3(\underline{z}')q^{\dim x^{\bar{G}}},$$

where $\underline{z}' = (\underline{z}, n, q, \iota)$ and $\bar{G}$ is a simple classical algebraic group over the algebraic closure of $\mathbb{F}_q$ such that $G_0 = O^{p'}(\bar{G}_\sigma)$ for a suitable Frobenius morphism σ of $\bar{G}$. Then (2) holds if

$$\Gamma = (n + 2 + 2n\iota - 2nf_2(\underline{z}'))\dim x^{\bar{G}}\log q + (n + 2 + 2n\iota)\log f_3(\underline{z}') - 2n\log f_1(\underline{z}') \geqslant 0.$$

A lower bound on $\dim x^{\bar{G}}$ can be given in terms of $\underline{z}'$ (see Propositions 3.25 and 3.33 for example) and this yields $\Gamma \geqslant \Gamma'(\underline{z}')$. It then remains to show that Γ' is non-negative for all possible values of $\underline{z}'$, with perhaps the exception of a small number of cases for which we can derive more accurate bounds through direct calculation. It is often the case that the function Γ' is increasing in each of its variables and thus it is quite straightforward to check that Γ' is non-negative. In more complicated cases, we have used a computer to identify the precise values of $\underline{z}'$ for which $\Gamma'(\underline{z}') < 0$. When a direct calculation is required, we present bounds to three decimal places; often a worked example is presented and the reader is encouraged to check the other cases. We do not claim that the bounds we obtain through direct calculation are the best possible.

Of course, there are cases where this approach is not applicable, or perhaps not appropriate. For instance, it is not always clear how arbitrary elements of H act on V. This comment is particularly pertinent to the almost simple irreducible subgroups in Aschbacher's $\mathscr{S}$ collection. In these cases we can often bound $|x^G|$ by applying Corollary 3.38, together with various lower bounds on the codimension of the largest eigenspace of x on V (see Definition 3.16, Lemmas 6.3, 7.1 and [5, 2.2] for example). Fortunately, in these cases we often find that $|H|$ is small compared with $|G|$ (see [5, 2.4] for instance) and the trivial bound $|x^G \cap H| \leqslant |H \cap \mathrm{PGL}(V)|$ is often sufficient.

Case 2. $x \in H - \mathrm{PGL}(V)$
Here x is a field, graph or graph-field automorphism of G_0 and in most cases we consider each type in turn. Lower bounds for $|x^G|$ are given in Lemma 3.48 and we often find that the trivial bound $|x^G \cap H| < |H|$ is sufficient. Alternatively, if x has order r then $|x^G \cap H| \leqslant i_r(H)$, where $i_r(H)$ is the number of elements of order r in H, and thus Proposition 3.14 is particularly useful when $r = 2$ or 3. In other cases, a more accurate upper bound on $|x^G \cap H|$ can be derived by applying Proposition 3.43 and Lemma 3.50 for example.

3 Preliminary results

In this section we present a number of results which are needed for the proof of Theorem 1. We begin with a brief description of Aschbacher's main theorem on the subgroup structure of the finite classical groups; this provides the organising principle on which the proof of Theorem 1 is based. Much of this section concerns the prime order automorphisms of finite simple classical groups; we consider unipotent and semisimple elements in §3.3 and §3.4 respectively, and outer automorphisms are studied in §3.5. Finally, in §3.6 we make some further remarks on orthogonal groups, concentrating in particular on the dimension eight case.

3.1 Subgroup structure

A general theorem on the subgroup structure of the finite classical groups was established by M. Aschbacher in 1984. Let G_0 be a finite simple classical group over $\mathbb{F}_q$, with natural (projective) module V of dimension n. Write $q = p^f$, where p is prime. Let $\Gamma \leqslant \mathrm{Aut}(G_0)$ denote the projective semilinear group corresponding to G_0, i.e. $\Gamma = \langle \widetilde{G}, \phi \rangle$ where $\widetilde{G} = \mathrm{Aut}(G_0) \cap \mathrm{PGL}(V)$ and ϕ is naturally induced from the field automorphism of $\mathbb{F}_{q^u}$ which sends μ to μ^p, where $u = 2$ if G_0 is unitary, otherwise $u = 1$. Let G be a group such that

$$G_0 \trianglelefteqslant G \leqslant \Gamma. \tag{3}$$

In [1], eight collections of subgroups of G are defined, labelled $\mathscr{C}_i = \mathscr{C}_i(G)$ for $1 \leqslant i \leqslant 8$, and Aschbacher proves that any maximal subgroup H of G not containing G_0 is either in $\mathscr{C}(G) := \bigcup_{i=1}^{8} \mathscr{C}_i$, or is almost simple and satisfies numerous irreducibility conditions (see [18, §1.2]). We write $\mathscr{S} = \mathscr{S}(G)$ for this collection of almost simple irreducible subgroups. We refer the reader to [18] for detailed information on each of these subgroup collections.

Of course, this fundamental theorem relies on the hypothesis that (3) holds. It is well-known that $\mathrm{Aut}(G_0) \neq \Gamma$ only if $G_0 = \mathrm{PSL}_n(q)$ $(n \geqslant 3)$, $G_0 = \mathrm{Sp}_4(q)'$ (q even) or $G_0 = \mathrm{P\Omega}_8^+(q)$. In

G_0	type of H	conditions
$\mathrm{P\Omega}_8^+(q)$	$\mathrm{GL}_3^\epsilon(q) \times \mathrm{GL}_1^\epsilon(q)$	$q \geqslant 3$ if $\epsilon = +$
	$\mathrm{O}_2^-(q^2) \times \mathrm{O}_2^-(q^2)$	
	$\mathrm{O}_1(q) \wr S_8$	$q = p > 2$
	$G_2(q)$	
$\mathrm{Sp}_4(q)'$	$\mathrm{O}_2^\epsilon(q) \wr S_2$	$\epsilon = -$ if $q = 2$
(q even)	$\mathrm{O}_2^-(q^2).2$	

Table 3.1: The collection $\mathscr{N}$

G_0	collection	type of H	conditions
$\mathrm{P\Omega}_8^+(q)$	$\mathscr{C}_2$	$\mathrm{O}_4^+(q) \wr S_2$	$q \geqslant 3$
		$\mathrm{O}_2^\epsilon(q) \wr S_4$	$q \geqslant 5$ if $\epsilon = +$
	$\mathscr{C}_5$	$\mathrm{O}_8^+(q_0)$	$q = q_0^k$, k prime
	$\mathscr{S}$	$\mathrm{PSL}_3^\epsilon(q)$	$q \equiv \epsilon\,(3)$
		${}^3D_4(q_1)$	$q = q_1^3$
		$\Omega_8^+(2)$	$q = p \geqslant 3$
		$Sz(8)$	$q = 5$
$\mathrm{Sp}_4(q)'$	$\mathscr{C}_5$	$\mathrm{Sp}_4(q_0)$	$q = q_0^k$, k prime
(q even)	$\mathscr{S}$	$Sz(q)$	$\log_2 q \geqslant 3$ odd

Table 3.2: Some maximal non-subspace subgroups

[1], Aschbacher proves a similar theorem in the case where $G \not\leqslant \Gamma$ and $G_0 \neq \mathrm{P\Omega}_8^+(q)$. In later work [17], Kleidman gives a complete description of the maximal subgroups of the almost simple groups with socle $G_0 = \mathrm{P\Omega}_8^+(q)$.

Proposition 3.1. *Let G be a finite almost simple classical group with socle G_0 and suppose $G \not\leqslant \Gamma$. Let H be a maximal non-subspace subgroup of G not containing G_0. Then $H = N_G(K)$ where $K \leqslant \Gamma \cap G$ and either $K \in \mathscr{C}(\Gamma \cap G) \cup \mathscr{S}(\Gamma \cap G)$ or (G_0, H) is listed in Table 3.1.*

Proof. There are three cases to consider. If $G_0 = \mathrm{Sp}_4(q)'$ and q is even then the result follows from [1, 14.2] (note that the normalizer in G of a Sylow 2-subgroup of $\mathrm{Sp}_4(q)$ is a subspace subgroup). The case $G_0 = \mathrm{P\Omega}_8^+(q)$ is similar, using [17, Tables I, III] (again, we exclude the subspace subgroups labelled P_2 and R_{s2} in [17, Table III]). Finally, if $G_0 = \mathrm{PSL}_n(q)$ and $n \geqslant 3$ then an additional collection $\mathscr{C}_1'$ of subspace subgroups of G can be defined and a version of Aschbacher's result is proved using $\mathscr{C}_1'$ (see [1, §13]). □

Definition 3.2. Suppose $G \not\leqslant \Gamma$ and $H = N_G(K)$ is a maximal non-subspace subgroup of G, where $K \leqslant \Gamma \cap G$. We say that H belongs to the collection $\mathscr{C}_i$ (resp. $\mathscr{S}(G)$) if $K \in \mathscr{C}_i(\Gamma \cap G)$ (resp. $K \in \mathscr{S}(\Gamma \cap G)$), otherwise (G_0, H) is listed in Table 3.1 and we say that $H \in \mathscr{N}$. As before, we write $\mathscr{C}(G) = \bigcup_i \mathscr{C}_i$.

Proposition 3.3. *Suppose $G \not\leqslant \Gamma$ and $H \in \mathscr{C}(G) \cup \mathscr{S}(G)$ is a maximal non-subspace subgroup of G. Then the possibilities for H are given in Table 3.2.*

Proof. This follows from [1, 14.2] and [17, Tables I, III]. □

Remark 3.4. In Tables 3.1 and 3.2 we refer to the *type of H* (see Remark 1.2). If $H \in \mathscr{S}$ then the type of H is just the socle of the almost simple group $H \cap G_0$. The conditions listed in the final column are necessary (but not always sufficient) for H to be maximal in G (see [17, 18]).

3.2 Preliminaries

Let $\bar{G}$ be an algebraic group and fix an element $x \in \bar{G}_\sigma = \{g \in \bar{G} : g^\sigma = g\}$, where σ is a Frobenius morphism of $\bar{G}$. Then σ restricts to an endomorphism of the centralizer $E = C_{\bar{G}}(x)$ and induces a homomorphism $\sigma : E/E^0 \to E/E^0$, where E^0 denotes the connected component of E containing the identity.

Definition 3.5. Let $\sigma : X \to X$ be a homomorphism of a group X and let $H^1(\sigma, X)$ denote the set of equivalence classes of X under the equivalence relation

$$x \sim y \Leftrightarrow y = z^{-1}xz^\sigma \text{ for some } z \in X.$$

The equivalence class containing x is called the *σ-class of x*.

Let $H^1(\sigma, E/E^0)$ denote the set of equivalence classes corresponding to the induced homomorphism $\sigma : E/E^0 \to E/E^0$ described above. Then the following proposition is an application of the well-known Lang-Steinberg Theorem (see [23, 10.1]) and the corollary follows at once.

Proposition 3.6 ([22, I, 2.7]). *Let $\bar{G}$ be a connected linear algebraic group, and let σ be a Frobenius morphism of $\bar{G}$. If $x \in \bar{G}_\sigma$ then $x^{\bar{G}} \cap \bar{G}_\sigma$ is a union of precisely $|H^1(\sigma, E/E^0)|$ distinct $\bar{G}_\sigma$-conjugacy classes, where $E = C_{\bar{G}}(x)$.*

Corollary 3.7. *If $x \in \bar{G}_\sigma$ and $C_{\bar{G}}(x)$ is connected then $(x^{\bar{G}})_\sigma = x^{\bar{G}_\sigma}$.*

Consequently, much of this preliminary section is dedicated to studying the conjugacy classes of elements of prime order in finite classical groups of the form $\bar{G}_\sigma$, where $\bar{G}$ is a simple classical algebraic group of adjoint type over the algebraic closure of $\mathbb{F}_q$. Then $\bar{G}_\sigma$ is almost simple, with socle G_0. In the terminology of [11], $\bar{G}_\sigma$ is the group $\mathrm{Inndiag}(G_0)$ of *inner-diagonal* automorphisms of the finite simple classical group G_0. We start with a number of basic results on the order of certain finite classical groups which will be used repeatedly in the proof of Theorem 1.

Notation. Unless otherwise stated, for the remainder of §3 we shall adopt the following notation: $\bar{G}$ is a simple classical algebraic group of adjoint type over the algebraic closure K of $\mathbb{F}_q$, where $q = p^f$ for a prime p; σ is a Frobenius morphism of $\bar{G}$ such that $\bar{G}_\sigma$ is a finite almost simple classical group over $\mathbb{F}_q$ with socle G_0 and natural module V of dimension n.

Lemma 3.8 ([19, 1.2(i)]). *If $\{a_1, \ldots, a_l\}$ and $\{b_1, \ldots, b_m\}$ are two sets of distinct integers, all at least 2, then*

$$\frac{\prod_1^l (q^{a_i} - 1)}{\prod_1^m (q^{b_i} - 1)} < 2q^{\sum a_i - \sum b_i}.$$

Proposition 3.9. *The following bounds hold:*

(i) $\frac{1}{2}q^{\dim \bar{G}} < |\bar{G}_\sigma| < q^{\dim \bar{G}}$;

(ii) *If* $q \geqslant 3$ *then* $\frac{1}{2}q^{n^2} < |\mathrm{GL}_n(q)| < q^{n^2}$;

(iii) $q^{n^2} < |\mathrm{GU}_n(q)| \leqslant (q+1)q^{n^2-1}$;

(iv) *If* $a = \{a_1, \ldots, a_s\}$ *and* $b = \{b_1, \ldots, b_s\}$ *are two sets of natural numbers and* $n \geqslant \sum_j a_j b_j$ *then*

$$\frac{|\mathrm{GU}_n(q)|}{\prod_j |\mathrm{GU}_{a_j}(q^{b_j})|} \leqslant \left(\frac{q+1}{q}\right)^\alpha q^{n^2 - \sum_j a_j^2 b_j},$$

where $\alpha = 0$ *if* $s \geqslant 2$ *and each* $b_j = 1$*, otherwise* $\alpha = 1$*;*

(v) *If* l*,* m *and* n *are natural numbers such that* l *is even and* $lm \leqslant n$ *then*

$$|\mathrm{GU}_n(q)| < 2|\mathrm{GL}_m(q^l)|q^{n^2 - lm^2}.$$

Proof. First consider (i) and suppose $G_0 = \mathrm{P}\Omega_n^\epsilon(q)$, where n is even. Then

$$|\bar{G}_\sigma| = q^{\frac{1}{4}n(n-2)}(q^{\frac{n}{2}} - \epsilon)\prod_{i=1}^{n/2-1}(q^{2i}-1)$$

and the upper bound is immediate since $(q^2-1)(q^{n/2}+1) < q^{n/2+2}$ for all $n \geqslant 4$. If $n \equiv 2\,(4)$ then the lower bound follows at once from Lemma 3.8; if $n \equiv 0\,(4)$ then

$$|\bar{G}_\sigma| > q^{\frac{1}{4}n(n-2)+1}(q^2-1)(q^4-1)\ldots(q^{n-2}-1)(q^{\frac{n}{2}-1}-1)$$

and again Lemma 3.8 gives the lower bound. The other cases in (i) are very similar. In (ii), the upper bound is trivial and the lower bound holds since

$$\frac{|\mathrm{GL}_n(q)|}{q^{n^2}} = \prod_{i=1}^{n}\frac{q^i-1}{q^i} > \prod_{i=1}^{\infty}\frac{q^i-1}{q^i} \geqslant 1 - \frac{1}{q} - \frac{1}{q^2}$$

for all $q \geqslant 2$ (see [21, 3.5]). Part (iii) is an easy exercise. If $\alpha = 1$ then (iv) is immediate from (iii), otherwise we may as well assume $s = 2$. If a_i is odd then $|\mathrm{GU}_n(q) : \mathrm{GU}_{a_i}(q)| \leqslant q^{n^2-a_i^2}$ since

$$(q^{2j}-1)(q^{2j+1}+1) < q^{4j+1} \tag{4}$$

for all $j \geqslant 1$ and the result follows from (iii). On the other hand, if both a_1 and a_2 are even, say $a_1 = 2k$ and $a_2 = 2l$ with $k \geqslant l \geqslant 1$, then (iv) holds if and only if

$$\prod_{j=1}^{2l}\left(\frac{q^{2k+j}-(-1)^j}{q^j-(-1)^j}\right)\cdot\prod_{j=1}^{n-2(k+l)}(q^{2(k+l)+j}-(-1)^j) < q^{\frac{1}{2}(n-2(k+l))(n+2(k+l)+1)+4kl}.$$

Now (4) implies that

$$\prod_{j=1}^{n-2(k+l)}(q^{2(k+l)+j}-(-1)^j) \leqslant (q^{2(k+l)+1}+1)q^{\frac{1}{2}(n-2(k+l))(n+2(k+l)+1)-2(k+l)-1}$$

and so we may as well assume $n = 2(k+l)+1$. It is easy to check that

$$(q^{2k+2m}-1)(q^{2k+2m+1}+1) < q^{4k+2}(q^{2m-1}+1)(q^{2m}-1)$$

for all $k, m \geqslant 1$ and we quickly reduce to the case $l = 1$. The desired result follows since

$$(q^{2k+1}+1)(q^{2k+2}-1)(q^{2k+3}+1) < q^{6k+3}(q+1)(q^2-1)$$

for all $k \geqslant 1$. Finally, let us consider (v). Summing over the odd positive integers we get

$$\sum_{i\text{ odd}}\log(1+q^{-i}) < \sum_{i\text{ odd}}q^{-i} = \frac{q}{q^2-1} < \log 2$$

and thus $\prod_{i=1}^{k}(q^{2i-1}+1) < 2q^{k^2}$ for all $k \geqslant 1$ and (v) follows. □

Remark 3.10. The lower bound in (ii) does not hold if $q = 2$. In this case (i) implies that $|\mathrm{GL}_n(2)| = |\mathrm{PGL}_n(2)| > 2^{n^2-2}$. In (iv) we note that $|\mathrm{GU}_n(q) : \mathrm{GU}_a(q)| \leqslant q^{n^2-a^2}$ if and only if a is odd.

Next we record a useful result on the lifting of elements of odd prime order.

Lemma 3.11. *Let $x \in \bar{G}_\sigma$ be an element of odd prime order r. Define $(G, \widehat{G})$ as follows:*

G_0	$\mathrm{PSL}_n^\epsilon(q)$	$\mathrm{PSp}_n(q)$	$\mathrm{P}\Omega_n^\epsilon(q)$
$(G, \widehat{G})$	$(\bar{G}_\sigma, \mathrm{GL}_n^\epsilon(q))$	$(G_0, \mathrm{Sp}_n(q))$	$(G_0, \Omega_n^\epsilon(q))$

Then one of the following holds:

(i) x lifts to an element $\hat{x} \in \widehat{G}$ of order r such that $|x^G| = |\hat{x}^{\widehat{G}}|$;

(ii) $G_0 = \mathrm{PSL}_n^{\epsilon}(q)$, $r|(q-\epsilon)$ and x is $\bar{G}$-conjugate to $[I_{\frac{n}{r}}, \omega I_{\frac{n}{r}}, \ldots, \omega^{r-1} I_{\frac{n}{r}}]$, where $\omega \in K$ is a primitive r^{th} root of unity.

Proof. First suppose $G_0 = \mathrm{PSL}_n^{\epsilon}(q)$ and (ii) does not hold. Let $Z = \langle \lambda \rangle$ denote the centre of $\widehat{G}$, so $\bar{G}_{\sigma} = \widehat{G}/Z$ and $x = \tilde{x}Z$ for some $\tilde{x} \in \widehat{G}$. Since x has order r we have $\tilde{x}^r = \lambda^l$ for an integer l such that $0 \leqslant l \leqslant q-\epsilon-1$. Now, if $(r, q-\epsilon) = 1$ then there exists an integer y such that $yr \equiv l \mod (q-\epsilon)$ and we define $\hat{x} = \lambda^{-y}\tilde{x}$. On the other hand, if $r|(q-\epsilon)$ then we claim that $\tilde{x}$ is diagonalisable. Seeking a contradiction, suppose $\tilde{x}$ is not diagonalisable. Then $f(z) = z^r - \lambda^l$ is the minimal polynomial of $\tilde{x}$ and thus $\tilde{x}$ has rational canonical form $\mathrm{diag}[A_1, \ldots, A_m]$, where $mr = n$ and

$$A_i = \begin{pmatrix} & \lambda^l \\ I_{r-1} & \end{pmatrix}$$

for each i. Therefore $\tilde{x}$ is $\mathrm{GL}_n(K)$-conjugate to the block-diagonal matrix

$$[\lambda^{l/r} I_{\frac{n}{r}}, \omega\lambda^{l/r} I_{\frac{n}{r}}, \ldots, \omega^{r-1}\lambda^{l/r} I_{\frac{n}{r}}]$$

and thus x is $\bar{G}$-conjugate to $[I_{n/r}, \omega I_{n/r}, \ldots, \omega^{r-1} I_{n/r}]$, where $\omega \in K$ is a primitive r^{th} root of unity, a contradiction. Therefore $\tilde{x}$ is diagonalisable, say $\tilde{x} = [\lambda_1, \ldots, \lambda_n]$, and $\hat{x} = \lambda_1^{-1}\tilde{x}$ is a lift of x of order r. To see that $|x^G| = |\hat{x}^{\widehat{G}}|$, consider the natural embedding $\rho : C_{\widehat{G}}(\hat{x})/Z \to C_{\widehat{G}/Z}(x)$. If $\hat{y}Z \in C_{\widehat{G}/Z}(x)$ then $\hat{y}^{-1}\hat{x}\hat{y} = \mu\hat{x}$ for an element $\mu \in Z$ with $\mu^r = 1$. If $\mu \neq 1$ then r must divide $|Z| = q-\epsilon$ and we deduce that $\hat{x}$ is $\widehat{G}$-conjugate to $[I_{n/r}, \omega I_{n/r}, \ldots, \omega^{r-1} I_{n/r}]$, a contradiction. Therefore $\mu = 1$, so ρ is an isomorphism and the result follows.

Finally, let us assume G_0 is a symplectic or orthogonal group. If $p = 2$ or n is odd then $G = \widehat{G}$ so assume otherwise. Then $G_0 = G/Z$, where $Z \cong \mathbb{Z}_2$ is the centre of G, and $x \in G_0$ since r is odd. The result now follows as before. □

Remark 3.12. If $x \in \bar{G}_{\sigma}$ is a semisimple element of odd prime order then Lemma 3.11(i) holds if and only if $|H^1(\sigma, E/E^0)| = 1$, where $E = C_{\bar{G}}(x)$ (see Lemmas 3.34 and 3.35).

Remark 3.13. If $r \neq p$ then $x^{G_0} = x^{\bar{G}_{\sigma}}$ (see [11, 4.2.2(j)]). In general, this is not true for unipotent elements; we refer the reader to Lemma 3.20 for further details.

Let X be a subset of a finite group and let r be a positive integer. Then we define $i_r(X)$ to be the number of elements of order r in X. The next result gives an upper bound for the number of elements of order two and three in a finite almost simple classical group.

Proposition 3.14 ([19, 1.3]). *Let $N = |\Phi^+(\bar{G})|$ be the number of positive roots in the root system of $\bar{G}$ and define $N_2 = \dim \bar{G} - N$, $N_3 = \dim \bar{G} - 2N/3$. If $r = 2$ or 3 then*

$$i_r(\mathrm{Aut}(G_0)) < 2(1+q^{-1})q^{N_r}.$$

The next lemma is a useful observation.

Lemma 3.15 ([15, 2.24]). *Let N be a normal subgroup of a finite group G and let $\bar{x} \in G/N$ denote the image of $x \in G$ under the natural homomorphism $G \to G/N$. Then*

$$|x^G| \leqslant |N| \cdot |\bar{x}^{G/N}|.$$

Definition 3.16. Let $\bar{V} = V \otimes K$ and for $x \in \mathrm{PGL}(V)$ let $\hat{x}$ be a pre-image of x in $\mathrm{GL}(V)$. Define

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

and observe that $\nu(x)$ is equal to the codimension of the largest eigenspace of $\hat{x}$ on $\bar{V}$. In particular, we note that $\nu(x) > 0$ if $x \neq 1$.

Bounds on $|x^{\bar{G}_\sigma}|$ in terms of $\nu(x)$, $\dim V$ and q for elements of prime order will serve as a useful tool in the proof of Theorem 1. Such bounds are obtained in [20, 3.4] and we slightly refine these results in Propositions 3.22 and 3.36 below. In particular, our bounds do not involve undetermined constants.

Definition 3.17. Let $G \leqslant \mathrm{PGL}(V)$ be a finite classical group over $\mathbb{F}_q$. We define $k_{s,r,u}(G)$ (resp. $k_{s,r,s}(G)$) to be the number of conjugacy classes in G of unipotent (resp. semisimple) elements x of prime order r such that $\nu(x) = s$ with respect to the natural action on V. Upper bounds for $k_{s,r,\cdot}(\bar{G}_\sigma)$ are established in Propositions 3.24 and 3.40.

3.3 Unipotent elements

Let $\bar{G}$ be a simple classical algebraic group of adjoint type over an algebraically closed field of characteristic $p \geqslant 0$ with natural module $\bar{V}$. If $\bar{G}$ is symplectic or orthogonal then we say that p is *good* for $\bar{G}$ if $p \neq 2$, whereas any p is good if $\bar{G} = \mathrm{PSL}(\bar{V})$. From the natural correspondence arising from the Jordan normal form we can associate a unique partition of $\dim \bar{V} = n$ to each unipotent conjugacy class as follows

$$(n^{a_n}, \ldots, 1^{a_1}) \vdash n \longleftrightarrow [J_n^{a_n}, \ldots, J_1^{a_1}]^{\bar{G}}, \tag{5}$$

where J_i denotes a standard Jordan block of size i. The partition $\lambda \vdash n$ corresponding to the $\bar{G}$-class of a unipotent element x is called the *associated partition of* x. In good characteristic, a partition $\lambda \vdash n$ corresponds to a unipotent class in a symplectic (resp. orthogonal) group if and only if odd (resp. even) parts in λ occur with an even multiplicity. It is well-known that if p is good for $\bar{G}$ then this map from unipotent $\bar{G}$-classes to partitions of n is almost always injective. Indeed, the single exception is the case $\bar{G} = \mathrm{PSO}_n$, where n is even and the associated partition has no odd parts. Here such a partition corresponds to precisely two distinct unipotent $\bar{G}$-classes which fuse in PO_n.

Detailed information on conjugacy classes in the finite classical groups $\mathrm{GL}_n^\epsilon(q)$, $\mathrm{Sp}_n(q)$ and $\mathrm{O}_n^\epsilon(q)$ is given by Wall in [25]. In the next lemma we use some of these results to compute $|x^{\bar{G}_\sigma}|$ for unipotent elements $x \in \bar{G}_\sigma$ of prime order.

Lemma 3.18. *Suppose $x \in \bar{G}_\sigma$ has order p and associated partition $\lambda = (n^{a_n}, \ldots, 1^{a_1}) \vdash n$. If p is good for $\bar{G}$ then the order of the centralizer $C_{\bar{G}_\sigma}(x)$ is recorded in Table 3.3, where*

G_0	$\lvert C_{\bar{G}_\sigma}(x)\rvert$
$\mathrm{PSL}_n^\epsilon(q)$	$(q-\epsilon)^{-1} q^{\alpha_1} \prod_i \lvert \mathrm{GL}_{a_i}^\epsilon(q)\rvert$
$\mathrm{PSp}_n(q)$	$2^{-\beta} q^{\alpha_2} \prod_{i \text{ even}} \lvert \mathrm{O}_{a_i}^{\epsilon_i}(q)\rvert \prod_{i \text{ odd}} \lvert \mathrm{Sp}_{a_i}(q)\rvert$
$\mathrm{P\Omega}_n^\epsilon(q)$	$2^{-\gamma} q^{\alpha_3} \prod_{i \text{ odd}} \lvert \mathrm{O}_{a_i}^{\epsilon_i}(q)\rvert \prod_{i \text{ even}} \lvert \mathrm{Sp}_{a_i}(q)\rvert$

Table 3.3: Unipotent centralizers, p good

$$\alpha_1 = 2\sum_{i<j} i a_i a_j + \sum_i (i-1)a_i^2 = 2\alpha_2 - \sum_{i \text{ even}} a_i = 2\alpha_3 + \sum_{i \text{ even}} a_i$$

and where

$$\beta = \begin{cases} 0 & \text{if each non-zero } a_j \text{ is even} \\ 1 & \text{otherwise,} \end{cases}$$

$$\gamma = \begin{cases} 0 & \text{if } a_j = 0 \text{ for all odd } j \\ 1 & \text{if } n \text{ is odd or if each non-zero } a_j \text{ is even} \\ 2 & \text{otherwise} \end{cases}$$

and $\{\epsilon_i\}$ is a choice of signs so that $\prod_i \epsilon_i = \epsilon$ if $G_0 = \mathrm{P\Omega}_n^\epsilon(q)$ and n is even.

Proof. First observe that x lies in G_0 since $|\bar{G}_\sigma : G_0|$ is not divisible by p. Now if $G_0 = \mathrm{PSL}_n^\epsilon(q)$ and p is odd then Lemma 3.11 implies that x lifts to an element $\hat{x} \in \mathrm{GL}_n^\epsilon(q)$ such that $\hat{x}^p = 1$ and $|x^{\bar{G}_\sigma}| = |\hat{x}^{\mathrm{GL}_n^\epsilon(q)}|$; it is clear from the proof of Lemma 3.11 that the same conclusion also holds if $p = 2$. The centralizer order $|C_{\bar{G}_\sigma}(x)|$ now follows from [25, p.34]. The other cases are similar. For example, suppose $G_0 = \mathrm{P}\Omega_n^\epsilon(q)$ and n is even. Then p is odd and Lemma 3.11 implies that there exists $\hat{x} \in \Omega_n^\epsilon(q)$ such that $\hat{x}^p = 1$ and $|x^{G_0}| = |\hat{x}^{\Omega_n^\epsilon(q)}|$. If l denotes the number of non-zero terms a_j with j odd in λ then [25, p.39] gives $|\hat{x}^{\mathrm{O}_n^\epsilon(q)}| = 2^{1-l}f(q)$, where $f(q)$ is a monic polynomial in q of degree $\dim x^{\bar{G}}$. Now, if $E = C_{\bar{G}}(x)$ then Proposition 3.6 implies that $|x^{\bar{G}_\sigma}| = |H^1(\sigma, E/E^0)|^{-1}f(q)$, where $|H^1(\sigma, E/E^0)| = |E : E^0|$ since E/E^0 is either trivial or is an elementary abelian 2-group. More precisely, [8, p.399] gives

$$|H^1(\sigma, E/E^0)| = \begin{cases} 2^{l-1-\delta} & \text{if } l > 0 \\ 1 & \text{otherwise,} \end{cases}$$

where $\delta = 1$ if there is an odd a_j, otherwise $\delta = 0$. The polynomial $f(q)$ can be read off from [25, p.39] and the desired result follows. The other cases are very similar. □

Remark 3.19. According to [25, p.38], if $x \in \mathrm{P}\Omega_n^-(q)$ is unipotent and q is odd then the associated partition of x has at least one odd part.

Lemma 3.20. *Suppose $x \in \bar{G}_\sigma$ has order p and associated partition $\lambda = (n^{a_n}, \ldots, 1^{a_1}) \vdash n$. If p is good for $\bar{G}$ then the following hold:*

(i) If $\bar{G}_\sigma = \mathrm{PGL}_n^\epsilon(q)$ then $|x^{\bar{G}_\sigma}| = (v, q-\epsilon)|x^{G_0}|$, where $v = \mathrm{hcf}\{j : a_j > 0\}$;

(ii) If $\bar{G}_\sigma$ is symplectic then $|x^{\bar{G}_\sigma}| = 2^\alpha|x^{G_0}|$, where $\alpha = 1$ if a_j is odd for some even j, otherwise $\alpha = 0$;

(iii) If $\bar{G}_\sigma$ is orthogonal and n is even then $|x^{\bar{G}_\sigma}| = 4|x^{G_0}|$ only if a_j is odd for some odd j.

Proof. In (i), x lifts to a unique element $\hat{x} \in \mathrm{SL}_n^\epsilon(q)$ of order p such that $|x^{G_0}| = |\hat{x}^{\mathrm{SL}_n^\epsilon(q)}|$ and Lemma 3.18 gives $|x^{\bar{G}_\sigma}| = f(q)$, where f is a monic polynomial in q. Now [22, 1.10] states that E/E^0 is cyclic of order v, where $E = C_{\mathrm{SL}_n(K)}(\hat{x})$, hence $|H^1(\sigma, E/E^0)| = (v, q-\epsilon)$ and therefore $|x^{G_0}| = (v, q-\epsilon)^{-1}f(q)$ as claimed. For (ii), let $\hat{x} \in \mathrm{Sp}_n(q)$ be the unique lift of x to an element of order p (see Lemma 3.11). Then $|x^{G_0}| = |\hat{x}^{\mathrm{Sp}_n(q)}| = 2^{-l'}f(q)$, where l' denotes the number of even j with $a_j > 0$ and f is a monic polynomial in q (see [25, p.36]). Now [8, p.399] gives $|C_{\bar{G}}(x) : C_{\bar{G}}(x)^0| = 2^{l'-\delta'}$, where $\delta' = 1$ if there exists an even j with a_j odd, otherwise $\delta' = 0$. The result now follows since $|x^{\bar{G}_\sigma}| = 2^{-l'+\delta'}f(q)$.

Now consider (iii). Let $\hat{x} \in \Omega_n^\epsilon(q)$ be the unique lift of x to an element of order p such that $|x^{G_0}| = |\hat{x}^{\Omega_n^\epsilon(q)}|$ and define the integers l and δ as in the proof of Lemma 3.18. Since $|\mathrm{O}_n^\epsilon(q) : \Omega_n^\epsilon(q)| = 4$ we have $4|x^{G_0}| \geqslant |\hat{x}^{\mathrm{O}_n^\epsilon(q)}|$. Now, if $l = 0$ then $|\hat{x}^{\mathrm{O}_n^\epsilon(q)}| = 2|x^{\bar{G}_\sigma}|$ and therefore $2|x^{G_0}| \geqslant |x^{\bar{G}_\sigma}|$ as claimed. If $l > 0$ then $|\hat{x}^{\mathrm{O}_n^\epsilon(q)}| = 2^{1-l}f(q)$ for some monic polynomial f in q and $|x^{\bar{G}_\sigma}| = 2^{1+\delta-l}f(q)$. Moreover, x and x^γ are $\bar{G}$-conjugate, where γ is an involutory graph automorphism of $\bar{G}$, and thus $|\hat{x}^{\mathrm{SO}_n^\epsilon(q)}| = |\hat{x}^{\mathrm{O}_n^\epsilon(q)}|$. In turn, this implies that $2|x^{G_0}| \geqslant |\hat{x}^{\mathrm{O}_n^\epsilon(q)}|$ and the result follows since $|x^{\bar{G}_\sigma}| = |\hat{x}^{\mathrm{O}_n^\epsilon(q)}|$ if $\delta = 0$. □

Corollary 3.21. *Suppose $\bar{G}$ is symplectic or orthogonal, p is odd and $x \in \bar{G}_\sigma$ has order p and associated partition $\lambda = (n^{a_n}, \ldots, 1^{a_1}) \vdash n$. If l is the number of odd j with $a_j > 0$ then*

$$|x^{G_0}| > \left(\frac{1}{2}\right)^{l+1+\delta_{l,0}} \left(\frac{q}{q+1}\right)^{l} q^{\dim x^{\bar{G}}}.$$

In [2] one can find detailed information on involutions in symplectic and orthogonal groups over fields of even characteristic and we adopt the notation therein for labelling representatives of involution classes.

Proposition 3.22. *Let $x \in \bar{G}_\sigma$ be an element of order p such that $\nu(x) = s$. Then*

$$f_i(n,s,q) < |x^{\bar{G}_\sigma}| < g_i(n,s,q),$$

where $i = 1 + \delta_{2,p}$ and the functions f_i and g_i are defined in Tables 3.4 and 3.5 below.

Proof. We begin by assuming p is odd. Let $\lambda = (n^{a_n}, \ldots, 1^{a_1}) \vdash n$ denote the associated partition of x, let $t \geqslant 1$ be the number of non-zero a_j and observe that the hypothesis $\nu(x) = s$ implies that $\sum_j a_j = n - s$. If $G_0 = \mathrm{PSL}_n(q)$ then Lemmas 3.8, 3.18 and Proposition 3.9(ii) imply that

G_0	$f_1(n,s,q)$	$g_1(n,s,q)$
$\mathrm{PSL}_n^\epsilon(q)$	$\frac{1}{2}\left(\frac{q}{q+1}\right)\max(q^{2s(n-s)}, q^{ns})$	$2q^{s(2n-s-1)}$
$\mathrm{PSp}_n(q)$	$\frac{1}{2}\left(\frac{q}{q+1}\right)\max(q^{s(n-s)}, q^{\frac{1}{2}ns})$	$q^{\frac{1}{2}(2ns-s^2+1)}$
$\mathrm{P\Omega}_n^\pm(q)$	$\frac{1}{2}\left(\frac{q}{q+1}\right)\max(q^{s(n-s-1)}, q^{\frac{1}{2}n(s-1)})$	$2q^{\frac{1}{2}s(2n-s-2)}$
$\Omega_n(q)$	$\frac{1}{2}\max(q^{s(n-s-1)}, q^{\frac{1}{2}n(s-1)})$	$q^{\frac{1}{2}s(2n-s-2)}$

Table 3.4: Bounds on unipotent conjugacy classes, $p > 2$

$$\frac{1}{2}q^{\dim x^{\bar{G}}} < |x^{\bar{G}_\sigma}| < 2^{t-1}q^{\dim x^{\bar{G}}} \tag{6}$$

and thus $|x^{\bar{G}_\sigma}| > f_1(n,s,q)$ by [6, 2.9]. For the upper bound, first observe that [6, 2.4] implies that $\dim x^{\bar{G}} \leqslant \dim y^{\bar{G}}$, where $y \in \bar{G}$ is unipotent with associated partition

$$\lambda' = (s + 3t/2 - t^2/2, t-1, t-2, \ldots, 2, 1^{n-s-t+1}) \vdash n.$$

Using [6, 2.3] we calculate that $\dim y^{\bar{G}} = 2ns - s^2 - s - t^3/3 - t^2 + 2t/3$ and (6) yields

$$|x^{\bar{G}_\sigma}| < 2^{t-1}q^{\dim x^{\bar{G}}} < 2q^{\dim y^{\bar{G}}+t-2} \leqslant g_1(n,s,q)$$

as claimed. Next suppose $G_0 = \mathrm{PSU}_n(q)$. Here

$$\frac{1}{2}\left(\frac{q}{q+1}\right)^{t-1} q^{\dim x^{\bar{G}}} < |x^{\bar{G}_\sigma}| < 2q^{\dim x^{\bar{G}}}$$

and [6, 2.9] gives $|x^{\bar{G}_s}| < g_1(n,s,q)$. For the lower bound, [6, 2.4] implies that $\dim x^{\bar{G}} \geqslant \dim y^{\bar{G}}$, where $y \in \bar{G}$ is unipotent with associated partition $((m+1)^r, m^{n-s-r}) \vdash n$ and $m = \lfloor n/(n-s) \rfloor$. In particular, if $|x^{\bar{G}_\sigma}|$ is minimal then $t = 2$ and again the result follows via [6, 2.9]. The other

G_0	conditions	x	$f_2(n,s,q)$	$g_2(n,s,q)$
$\mathrm{PSL}_n^\epsilon(q)$		$[J_2^s, I_{n-2s}]$	$\frac{1}{2}\left(\frac{q}{q+1}\right)q^{2s(n-s)}$	$2^{1+\delta_{2,q}}q^{2s(n-s)}$
$\mathrm{Sp}_n(q)$		a_s	$\frac{1}{2}q^{s(n-s)}$	$2q^{s(n-s)}$
		$b_s,\ c_s$	$\frac{1}{2}q^{s(n-s+1)}$	$2q^{s(n-s+1)}$
$\Omega_n^\epsilon(q)$	$(s,\epsilon) \neq (\frac{n}{2}, +)$	a_s	$\frac{1}{2}q^{s(n-s-1)}$	$2q^{s(n-s-1)}$
		c_s	$\frac{1}{2}q^{s(n-s)}$	$2q^{s(n-s)}$
$\Omega_n^+(q)$	$s = \frac{n}{2}$	$a_{\frac{n}{2}},\ a'_{\frac{n}{2}}$	$\frac{1}{2}q^{\frac{1}{4}n(n-2)}$	$q^{\frac{1}{4}n(n-2)}$
		$c_{\frac{n}{2}}$	$\frac{1}{2}q^{\frac{1}{4}n^2}$	$2q^{\frac{1}{4}n^2}$

Table 3.5: Bounds on unipotent conjugacy classes, $p = 2$

cases with p odd are similar. For example, if $G_0 = \mathrm{PSp}_n(q)$ and $\nu(x) = s$ is odd then the largest possible partition is $(s+1, 1^{n-s-1}) \vdash n$ (with respect to the familiar dominance ordering on partitions) and using Lemma 3.18 we deduce that

$$|x^{\bar{G}_\sigma}| \leqslant \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_{n-s-1}(q)|q^{n-s/2-1/2}} < q^{\frac{1}{2}(2ns-s^2+1)} = g_1(n,s,q).$$

Now assume $p=2$. If $\bar{G} = \mathrm{PSL}_n(K)$ then [2, 4.3] gives

$$|x^{\bar{G}_\sigma}| = \frac{|\mathrm{GL}_n^\epsilon(q)|}{|\mathrm{GL}_s^\epsilon(q)||\mathrm{GL}_{n-2s}^\epsilon(q)|q^{2ns-3s^2}}$$

and the desired bounds follow at once from Proposition 3.9. Next suppose $\bar{G} = \mathrm{Sp}_n(K)$. If s is even then there are precisely two distinct classes of involutions in $\bar{G}_\sigma$ whose elements satisfy $\nu(x) = s$ (see [2, §7]). These classes are represented by a_s and c_s, where

$$\frac{1}{2}q^{s(n-s)} < |a_s^{\bar{G}_\sigma}| = \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_s(q)||\mathrm{Sp}_{n-2s}(q)|q^{ns-3s^2/2+s/2}} < 2q^{s(n-s)}$$

and

$$\frac{1}{2}q^{s(n-s+1)} < |c_s^{\bar{G}_\sigma}| = \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_{s-2}(q)||\mathrm{Sp}_{n-2s}(q)|q^{ns-3s^2/2+3s/2-1}} < 2q^{s(n-s+1)}.$$

If s is odd then x is $\bar{G}_\sigma$-conjugate to b_s and

$$\frac{1}{2}q^{s(n-s+1)} < |b_s^{\bar{G}_\sigma}| = \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{Sp}_{s-1}(q)||\mathrm{Sp}_{n-2s}(q)|q^{ns-3s^2/2+s/2}} < 2q^{s(n-s+1)}.$$

Finally suppose that $G_0 = \Omega_n^\epsilon(q)$, where n is even. Here $\bar{G}_\sigma = G_0$ since q is even. We first consider involution classes in $\widetilde{G} = \mathrm{O}_n^\epsilon(q) = \bar{G}_\sigma.2$. As described in [2, §8], there are precisely two distinct $\widetilde{G}$-classes of involutions in $\widetilde{G}$ whose elements satisfy $\nu(x) = s$, where $s < n/2$ is even. These classes are represented by the elements a_s and c_s. The same is true if $s = n/2$ is even and $\epsilon = +$, whereas every involution with $s = n/2$ even is $\widetilde{G}$-conjugate to $c_{n/2}$ if $\epsilon = -$. In all cases, applying [2, 8.6, 8.8] (or [25, p.60]) we deduce that

$$\frac{1}{2}q^{s(n-s-1)} < |a_s^{\widetilde{G}}| = \frac{|\mathrm{O}_n^\epsilon(q)|}{|\mathrm{Sp}_s(q)||\mathrm{O}_{n-2s}^\epsilon(q)|q^{ns-3s^2/2-s/2}} < 2q^{s(n-s-1)}$$

and

$$\frac{1}{2}q^{s(n-s)} < |c_s^{\widetilde{G}}| = \frac{|\mathrm{O}_n^\epsilon(q)|}{2|\mathrm{Sp}_{s-2}(q)||\mathrm{Sp}_{n-2s}(q)|q^{n(s-1)-3s^2/2+5s/2-1}} < 2q^{s(n-s)}.$$

If s is odd then there is a unique $\widetilde{G}$-class of such involutions, with class representative b_s such that

$$\frac{1}{2}q^{s(n-s)} < |b_s^{\widetilde{G}}| = \frac{|\mathrm{O}_n^\epsilon(q)|}{2|\mathrm{Sp}_{s-1}(q)||\mathrm{Sp}_{n-2s}(q)|q^{n(s-1)-3s^2/2+3s/2}} < 2q^{s(n-s)}.$$

The elements a_s and c_s lie in $\bar{G}_\sigma$ whereas $b_s \in \widetilde{G} - \bar{G}_\sigma$. According to [2, 8.12] we have $x^{\bar{G}_\sigma} = x^{\widetilde{G}}$, unless $\epsilon = +$ and x is $\widetilde{G}$-conjugate to $a_{n/2}$ in which case $a_{n/2}^{\widetilde{G}} = a_{n/2}^{\bar{G}_\sigma} \cup a_{n/2}'^{\bar{G}_\sigma}$, and $|a_{n/2}^{\bar{G}_\sigma}| = |a_{n/2}'^{\bar{G}_\sigma}|$. The bounds listed in Table 3.5 follow at once. □

Remark 3.23. Suppose $G_0 = \mathrm{Sp}_n(q)$ and H is a $\mathscr{C}_8$-subgroup of type $\mathrm{O}_n^\epsilon(q)$, where q is even, so H is a subspace subgroup of G (see §1). If $x \in H$ is an involution which is $\mathrm{Sp}_n(q)$-conjugate to a_l then $x^G \cap H = x^H$ and the bounds in Table 3.5 imply that $\mathrm{fpr}(x) > |x^G|^{-\alpha}$, where

$$\alpha = \frac{\log 4q^l}{\log 2q^{l(n-l)}} \to 0 \text{ as } n, q \to \infty.$$

The maximal subgroups in $\mathscr{C}_1$ exhibit a similar behaviour and therefore it is necessary to exclude subspace subgroups from the statement of Theorem 1.

As previously remarked, in good characteristic p the natural map from unipotent classes in $\bar{G}$ to partitions of n (see (5)) is almost always injective. According to Proposition 3.6, if the $\bar{G}$-class of x is uniquely determined by its associated partition $\lambda \vdash n$ then there are precisely $|H^1(\sigma, E/E^0)|$ distinct $\bar{G}_\sigma$-classes which correspond to λ, where $E = C_{\bar{G}}(x)$. As we now describe, this observation provides an effective means of computing $k_{s,p,u}(\bar{G}_\sigma)$.

Let $x \in \bar{G}$ be an element of order p such that $\nu(x) = s$, where p is a good prime for $\bar{G}$. Then the associated partition of x has the form

$$\lambda = (p^{a_p}, (p-1)^{a_{p-1}}, \ldots, 1^{a_1}) \vdash n, \tag{7}$$

where $\sum_i a_i = n - s$ and a_i is even if i is odd (resp. even) if $\bar{G}$ is symplectic (resp. orthogonal). Subtracting 1 from each part gives a partition of s and we let $P(s)$ denote the number of (unordered) partitions of s. If $\bar{G} = \mathrm{PSL}_n(K)$ then $C_{\bar{G}}(x)$ is connected and thus Corollary 3.7 implies that

$$k_{s,p,u}(\bar{G}_\sigma) \leqslant P(s) < 2^s. \tag{8}$$

If $\bar{G} = \mathrm{PSp}_n(K)$ with $p \neq 2$ then [8, p.399] implies that $|E : E^0| \leqslant 2^l$, where l is the number of even integers i such that $a_i > 0$. Given n and l it is clear that $\sum_i a_i$ is maximal if

$$\lambda = (2l, 2(l-1), \ldots, 2, 1^{n-l(l+1)}) \vdash n$$

and we deduce that $l \leqslant \sqrt{s}$. In turn, this implies that

$$k_{s,p,u}(\bar{G}_\sigma) \leqslant P(s)2^{\sqrt{s}} < 2^{s+\sqrt{s}}. \tag{9}$$

If $\bar{G}$ is orthogonal then $k_{s,p,u}(\bar{G}_\sigma) = 0$ if s is odd and it is easy to check that (9) holds if s is even and p is odd. If $p = 2$ then [2, §§7,8] gives

$$k_{s,2,u}(\mathrm{Sp}_n(q)) = \begin{cases} 2 & \text{if } s \text{ is even} \\ 1 & \text{if } s \text{ is odd.} \end{cases}$$

Similarly, if n is even then $k_{s,2,u}(\Omega_n^\epsilon(q)) = 0$ if s is odd; for even s we have

$$k_{s,2,u}(\Omega_n^\epsilon(q)) = \begin{cases} 3 & \text{if } (s,\epsilon) = (\frac{n}{2}, +) \\ 1 & \text{if } (s,\epsilon) = (\frac{n}{2}, -) \\ 2 & \text{otherwise.} \end{cases}$$

Proposition 3.24. *$k_{s,p,u}(\bar{G}_\sigma) \leqslant p^{\frac{s}{2}}$.*

Proof. Let $P(s,m)$ be the number of partitions of s with no part of size greater than m. Then $P(s,2) \leqslant \frac{s}{2} + 1$ and working recursively we compute

$$P(s,3) \leqslant \sum_{i=0}^{\lfloor s/3 \rfloor} \left[\frac{1}{2}(s-3i) + 1\right] \leqslant \frac{1}{12}s^2 + \frac{7}{12}s + 1 \tag{10}$$

and

$$P(s,4) \leqslant \sum_{i=0}^{\lfloor s/4 \rfloor} \left[\frac{1}{12}(s-4i)^2 + \frac{7}{12}(s-4i) + 1\right] \leqslant \frac{1}{144}s^3 + \frac{11}{96}s^2 + \frac{43}{72}s + 1. \tag{11}$$

If $\bar{G} = \mathrm{PSL}_n(K)$ then $k_{s,p,u}(\bar{G}_\sigma) = P(s, p-1)$ and the above bounds are sufficient for $p \leqslant 5$; if $p > 5$ then the result follows via (8). Now assume $\bar{G}$ is symplectic or orthogonal. In view of our earlier comments, we may assume p is odd. For $s \leqslant 3$, the upper bounds for $k_{s,p,u}(\bar{G}_\sigma)$ recorded in the following table are readily verified:

$\bar{G}$	$s = 1$	2	3
$\mathrm{PSp}_n(K)$	1	2	2
$\mathrm{PSO}_n(K)$	0	3	0

Therefore we may assume $s \geqslant 4$ and applying (9) we reduce to the case $p \leqslant 7$. If $p \in \{3, 5\}$ then the desired result follows via (11) since

$$k_{s,3,u}(\bar{G}_\sigma) \leqslant 2.P(s,2), \quad k_{s,5,u}(\bar{G}_\sigma) \leqslant 2^2.P(s,4)$$

and $P(s,2) \leqslant \frac{s}{2}+1$. Finally, if $p = 7$ then we may as well assume $s \leqslant 6$ as the result is immediate from (9) if $s > 6$. Now, if $\bar{G} = \mathrm{PSp}_n(K)$ and $x \in \bar{G}$ has associated partition λ, with parts labelled as in (7), then the hypothesis $s \leqslant 6$ implies that $a_7 = a_5 = 0$ and $a_6 \leqslant 1$. In fact, it is clear that $\lambda = (6, 2^{s-5}, 1^{n-2s+4})$ is the only possibility with $a_6 = 1$ and applying (10) we deduce that

$$k_{s,7,u}(\bar{G}_\sigma) \leqslant 2 + 2.P(s,3) \leqslant 7^{\frac{s}{2}}$$

for all $4 \leqslant s \leqslant 6$. Similarly, if $\bar{G} = \mathrm{PSO}_n(K)$ then $k_{s,7,u}(\bar{G}_\sigma) \leqslant 5 + 2.P(s,2)$. □

Lemma 3.25. *Suppose p is good for $\bar{G}$ and $x \in \bar{G}$ is unipotent with precisely $t > 1$ distinct Jordan block sizes in its action on $\bar{V}$. Then $\dim x^{\bar{G}} \geqslant g(n,t)$, where g is defined as follows:*

$\bar{G}$	$g(n,t)$
$\mathrm{PSL}_n(K)$	$(t^2-t)n - \frac{1}{4}t^4 + \frac{1}{6}t^3 + \frac{1}{4}t^2 - \frac{1}{6}t$
$\mathrm{PSp}_n(K)$	$\frac{1}{2}(t^2-t)n - \frac{1}{8}t^4 + \frac{1}{12}t^3 + \frac{3}{8}t^2 - \frac{1}{12}t - \frac{1}{4}$
$\mathrm{PSO}_n(K)$	$\frac{1}{2}(t^2-t)n - \frac{1}{8}t^4 + \frac{1}{12}t^3 - \frac{1}{8}t^2 - \frac{1}{12}t$

Proof. If $\bar{G} = \mathrm{PSL}_n(K)$ then the result follows immediately from [6, 2.3, 2.4]: simply compute $\dim y^{\bar{G}}$, where $y \in \bar{G}$ is a unipotent element with associated partition

$$\lambda = (t, t-1, \ldots, 2, 1^{n-t^2/2-t/2+1}) \vdash n, \tag{12}$$

and apply [6, 2.4]. Next assume $\bar{G} = \mathrm{PSp}_n(K)$. For an arbitrary partition $\rho = (n^{a_n}, \ldots, 1^{a_1}) \vdash n$ define

$$f(\rho) = \frac{1}{2}n(n+1) - \sum_{i<j} i a_i a_j - \frac{1}{2}\sum_i i a_i^2 - \frac{1}{2}\sum_{i \text{ odd}} a_i$$

and observe that $f(\rho) = \dim x^{\bar{G}}$ if $x \in \mathrm{PSp}_n(K)$ has associated partition ρ (see [6, 2.3]). Now $g(n,t) = f(\lambda)$, where λ is the partition in (12), and so we need to show that $f(\rho) \geqslant f(\lambda)$ for all partitions $\rho \vdash n$ which correspond to unipotent classes in $\mathrm{PSp}_n(K)$. Let $m = \max\{j : a_j > 0\}$, write $\rho = (m^{a_m}, \ldots, 1^{a_1})$ and define

$$\rho' = (m^{a_m - 1}, (m-1)^{a_{m-1}}, \ldots, 2^{a_2}, 1^{a_1+m}) \vdash n.$$

Then

$$f(\rho') = f(\rho) - \left(\frac{1}{2}m^2 - m - \alpha + \sum_{i=1}^{m}(m-i)a_i\right), \tag{13}$$

where $\alpha = 1/2$ if m is odd, otherwise $\alpha = 0$. Therefore we may assume $m = t$. If there exists some $k > 1$ such that $a_k > 1$ then define

$$\rho' = (t^{a_t}, \ldots, (k+1)^{a_{k+1}}, k^{a_k - 1}, (k-1)^{a_{k-1}}, \ldots, 2^{a_2}, 1^{a_1+k}) \vdash n$$

and observe that (13) holds, with m replaced by k. We conclude that $f(\rho) \geqslant f(\lambda)$ as required. The argument for $\bar{G} = \mathrm{PSO}_n(K)$ is very similar. □

3.4 Semisimple elements

Let $r \neq p$ be an odd prime and write $\mathscr{S}_r$ for the complete set of r^{th} roots of unity in K. With respect to $\bar{G}_\sigma$ we define a bijection $\mathscr{S}_r \to \mathscr{S}_r$ as follows:

$$\lambda \mapsto \begin{cases} \lambda^{-q} & \text{if } \bar{G}_\sigma = \mathrm{PGU}_n(q) \\ \lambda^q & \text{otherwise.} \end{cases}$$

We write $\sigma(\lambda)$ to denote the image of $\lambda \in \mathscr{S}_r$ under this mapping and we call $\{\sigma^j(\lambda) : j \geqslant 0\}$ the *σ-orbit of* λ; the σ-orbit $\{1\}$ is the *trivial orbit.* If Λ is a σ-orbit then we define $\Lambda^{-1} = \{\lambda^{-1} : \lambda \in \Lambda\}$. Evidently, the σ-orbits partition $\mathscr{S}_r$.

Lemma 3.26. *Let $r \neq p$ be an odd prime and let $\{1\}, \Omega_j$ $(1 \leqslant j \leqslant t)$ denote the distinct σ-orbits on $\mathscr{S}_r$. Let $i \geqslant 1$ be minimal such that r divides $q^i - 1$.*

(i) If $\bar{G}_\sigma$ is not unitary then $|\Omega_j| = i$ for each j, and $\Omega_j = \Omega_j^{-1}$ if and only if i is even.

(ii) If $\bar{G}_\sigma$ is unitary then $|\Omega_j| = ci$, where

$i \bmod 4$	0	1	2	3
c	1	2	1/2	2

and $\Omega_j = \Omega_j^{-1}$ if and only if $i \not\equiv 2\,(4)$.

Proof. Fix $1 \neq \lambda \in \mathscr{S}_r$ and let Ω_j denote the σ-orbit of λ. In (i) we have $\sigma^m(\lambda) = \lambda^{q^m} = \lambda$ if and only if $r|(q^m - 1)$, whence $|\Omega_j| = \min\{m : \sigma^m(\lambda) = \lambda\} = i$. Furthermore, if $i = 2l$ then r divides $q^l + 1$, so $\sigma^l(\lambda) = \lambda^{-1}$, $\Omega_j = \Omega_j^{-1}$ and (i) follows. In (ii) we have $\sigma^m(\lambda) = \lambda^{(-q)^m}$ and $|\Omega_j| = m$, where $m \geqslant 1$ is the smallest integer such that r divides $q^m - (-1)^m$. If $i = 4l$ then the minimality of i implies that $m = i$ and thus $\Omega_j = \Omega_j^{-1}$ since $\sigma^{2l}(\lambda) = \lambda^{-1}$. The other cases are just as straightforward. $\square$

Let us assume for now that $x \in \bar{G}_\sigma$ is a semisimple element of odd prime order r and $C_{\bar{G}}(x)$ is connected. If $\bar{G}_\sigma = \mathrm{PGL}_n^\epsilon(q)$ then Lemma 3.11 (in view of Lemma 3.34 below) implies that x lifts to an element $\hat{x} \in \mathrm{GL}_n^\epsilon(q)$ of order r such that $|x^{\bar{G}_\sigma}| = |\hat{x}^{\mathrm{GL}_n^\epsilon(q)}|$ and we define $\mathcal{E}_{\hat{x}}$ to be the multiset of eigenvalues of $\hat{x}$ in K, so each $\mu \in \mathcal{E}_{\hat{x}}$ is an r^{th} root of unity. If $(r, q-\epsilon) = 1$ then $\hat{x}$ is uniquely determined and we define $\mathcal{E}_x$ by setting $\mathcal{E}_x = \mathcal{E}_{\hat{x}}$. Of course, if r divides $|Z(\mathrm{GL}_n^\epsilon(q))| = q - \epsilon$ then $\mathcal{E}_{\hat{x}}$ is determined only up to scalar multiplication by an r^{th} root of unity and we shall treat this as a special case in our subsequent analysis. If $\bar{G} = \mathrm{PSp}_n(K)$ then Lemma 3.11 applies and we define $\mathcal{E}_x$ to be the multiset of eigenvalues of the unique lift $\hat{x} \in \mathrm{Sp}_n(q)$ of order r. We make an analogous definition when $\bar{G}$ is orthogonal.

The simple observation that $\mathcal{E}_x$ is a union of σ-orbits suggests the following definition.

Definition 3.27. Let $x \in \bar{G}_\sigma$ be a semisimple element of prime order $r > 2$, let $\{1\}, \Omega_j$ $(1 \leqslant j \leqslant t)$ denote the distinct σ-orbits on $\mathscr{S}_r$ and assume $(r, q-\epsilon) = 1$ if $\bar{G}_\sigma = \mathrm{PGL}_n^\epsilon(q)$. The *associated σ-tuple of x* is the $(t+1)$-tuple $\mu = (l, a_1, \ldots, a_t)$, where $l \geqslant 0$ is equal to the multiplicity of 1 in $\mathcal{E}_x$ and $a_j \geqslant 0$ denotes the multiplicity of Ω_j in $\mathcal{E}_x$.

Remark 3.28. Let $i \geqslant 1$ be minimal such that $r|(q^i - 1)$. If i is odd and $\bar{G}_\sigma$ is not a unitary group then we may assume that the non-trivial σ-orbits are labelled so that $\Omega_j^{-1} = \Omega_{j+s}$ for all $1 \leqslant j \leqslant s = t/2$. In particular, if $\bar{G}$ is symplectic or orthogonal then $a_j = a_{j+s}$ for all $1 \leqslant j \leqslant s$ if i is odd since $1 \neq \lambda \in \mathcal{E}_x$ must occur with the same multiplicity as λ^{-1}.

Remark 3.29. Suppose $G_0 = \mathrm{P}\Omega_n^\epsilon(q)$, where n is even. Let $x \in \bar{G}_\sigma$ be a semisimple element of odd prime order r with associated σ-tuple $\mu = (l, a_1, \ldots, a_t)$ and let $i \geqslant 1$ be minimal such that r divides $q^i - 1$. Then according to [25, p.38] we have the following conditions on μ.

(i) If i is odd and $\epsilon = -$ then $l > 0$.

(ii) If i is even, $l = 0$ and $\epsilon = +$ (resp. $\epsilon = -$) then $\sum_j a_j$ is even (resp. odd).

The next lemma describes how the centralizer order $|C_{\bar{G}_\sigma}(x)|$ of a semisimple element of odd prime order can be read off from the associated σ-tuple μ.

Lemma 3.30. *Let $x \in \bar{G}_\sigma$ be a semisimple element of odd prime order r such that $C_{\bar{G}}(x)$ is connected. Assume $(r, q-\epsilon) = 1$ if $\bar{G}_\sigma = \mathrm{PGL}_n^\epsilon(q)$. Let $i \geqslant 1$ be minimal such that $r|(q^i - 1)$ and let $\mu = (l, a_1, \ldots, a_t)$ be the associated σ-tuple of x. Let $d \geqslant 1$ be the number of non-zero terms a_j in μ. Then $|C_{\bar{G}_\sigma}(x)|$ and subsequent bounds $f < |x^{\bar{G}_\sigma}| < g$ are given in Table 3.6, where $\alpha = 1 - \delta_{l,0}$.*

G_0	i	$\lvert C_{\bar{G}_\sigma}(x)\rvert$	f	g
$\mathrm{PSL}_n(q)$	arbitrary	$(q-1)^{-1}\lvert\mathrm{GL}_l(q)\rvert\prod_j\lvert\mathrm{GL}_{a_j}(q^i)\rvert$	$\frac{1}{2}q^{\dim x^{\bar{G}}}$	$2^d q^{\dim x^{\bar{G}}}$
$\mathrm{PSU}_n(q)$	$i\equiv 0\,(4)$	$(q+1)^{-1}\lvert\mathrm{GU}_l(q)\rvert\prod_j\lvert\mathrm{GL}_{a_j}(q^i)\rvert$	$\frac{1}{2}q^{\dim x^{\bar{G}}}$	$2^d\left(\frac{q+1}{q}\right)^\alpha q^{\dim x^{\bar{G}}}$
	$i\equiv 2\,(4)$	$(q+1)^{-1}\lvert\mathrm{GU}_l(q)\rvert\prod_j\lvert\mathrm{GU}_{a_j}(q^{\frac{i}{2}})\rvert$	$\frac{1}{2}\left(\frac{q}{q+1}\right)^d q^{\dim x^{\bar{G}}}$	$\left(\frac{q+1}{q}\right) q^{\dim x^{\bar{G}}}$
	odd	$(q+1)^{-1}\lvert\mathrm{GU}_l(q)\rvert\prod_j\lvert\mathrm{GL}_{a_j}(q^{2i})\rvert$	$\frac{1}{2}q^{\dim x^{\bar{G}}}$	$2^d\left(\frac{q+1}{q}\right)^\alpha q^{\dim x^{\bar{G}}}$
$\mathrm{PSp}_n(q)$	even	$\lvert\mathrm{Sp}_l(q)\rvert\prod_j\lvert\mathrm{GU}_{a_j}(q^{\frac{i}{2}})\rvert$	$\frac{1}{2}\left(\frac{q}{q+1}\right)^d q^{\dim x^{\bar{G}}}$	$q^{\dim x^{\bar{G}}}$
	odd	$\lvert\mathrm{Sp}_l(q)\rvert\prod_{j=1}^s\lvert\mathrm{GL}_{a_j}(q^i)\rvert$	$\frac{1}{2}q^{\dim x^{\bar{G}}}$	$2^d q^{\dim x^{\bar{G}}}$
$\mathrm{P}\Omega_n^\epsilon(q)$	even	$2^{-\alpha}\lvert\mathrm{O}_l^{\epsilon'}(q)\rvert\prod_j\lvert\mathrm{GU}_{a_j}(q^{\frac{i}{2}})\rvert^\dagger$	$\frac{1}{2}\left(\frac{q}{q+1}\right)^{d+\alpha} q^{\dim x^{\bar{G}}}$	$2^\alpha q^{\dim x^{\bar{G}}}$
(n even)	odd	$2^{-\alpha}\lvert\mathrm{O}_l^\epsilon(q)\rvert\prod_{j=1}^s\lvert\mathrm{GL}_{a_j}(q^i)\rvert$	$\frac{1}{2}\left(\frac{q}{q+1}\right)^\alpha q^{\dim x^{\bar{G}}}$	$2^{d+\alpha}q^{\dim x^{\bar{G}}}$
$\Omega_n(q)$	even	$\lvert\mathrm{SO}_l(q)\rvert\prod_j\lvert\mathrm{GU}_{a_j}(q^{\frac{i}{2}})\rvert$	$\frac{1}{2}\left(\frac{q}{q+1}\right)^d q^{\dim x^{\bar{G}}}$	$q^{\dim x^{\bar{G}}}$
(n odd)	odd	$\lvert\mathrm{SO}_l(q)\rvert\prod_{j=1}^s\lvert\mathrm{GL}_{a_j}(q^i)\rvert$	$\frac{1}{2}q^{\dim x^{\bar{G}}}$	$2^d q^{\dim x^{\bar{G}}}$

† $\epsilon'=\epsilon$ if and only if there are an even (or zero) number of odd parts a_j.

Table 3.6: Semisimple centralizers, $C_{\bar{G}}(x)$ connected

Proof. First observe that $x^{G_0}=x^{\bar{G}_\sigma}$ (see [11, 4.2.2(j)]) and $|x^{\bar{G}_\sigma}|$, and thus $|C_{\bar{G}_\sigma}(x)|$, is a monic polynomial in q (see Corollary 3.7). If $\bar{G}_\sigma=\mathrm{PGL}_n^\epsilon(q)$ then Lemma 3.11 implies that x lifts to an element $\hat{x}\in\mathrm{GL}_n^\epsilon(q)$ which has order r and satisfies $|x^{\bar{G}_\sigma}|=|\hat{x}^{\mathrm{GL}_n^\epsilon(q)}|$. In this case the result follows from [25, p.34]; the other cases are similar. For instance, if $G_0=\mathrm{P}\Omega_n^\epsilon(q)$, where n is even, then $x\in G_0$ (since r is odd) and x lifts to an element $\hat{x}\in\Omega_n^\epsilon(q)$ of order r such that $|x^{G_0}|=|\hat{x}^{\Omega_n^\epsilon(q)}|$ (see Lemma 3.11). Now [25, p.39] gives $|\hat{x}^{\mathrm{O}_n^\epsilon(q)}|=2^\alpha f(q)$, where $f(q)$ is a monic polynomial and $\alpha=1-\delta_{l,0}$. We conclude that $|x^{\bar{G}_\sigma}|=f(q)$ and the result follows. The bounds $f<|x^{\bar{G}_\sigma}|<g$ quickly follow via Proposition 3.9. □

Remark 3.31. As previously remarked, if $x\in\bar{G}_\sigma=\mathrm{PGL}_n^\epsilon(q)$ has prime order r and $C_{\bar{G}}(x)$ is connected, where $r|(q-\epsilon)$, then $\mathcal{E}_{\hat{x}}$ depends on the choice of preimage $\hat{x}\in\mathrm{GL}_n^\epsilon(q)$ and the associated σ-tuple of x is not well-defined. However, the centralizer order $|C_{\bar{G}_\sigma}(x)|$ is easily computed: choose any lift $\hat{x}$ of order r and suppose ω^j occurs with a multiplicity a_j in $\mathcal{E}_{\hat{x}}$, where $\omega\in K$ is a primitive r^{th} root of unity. Then $|C_{\bar{G}_\sigma}(x)|=(q-\epsilon)^{-1}\prod_j|\mathrm{GL}_{a_j}^\epsilon(q)|$.

Definition 3.32. Let $x\in\bar{G}_\sigma$ be a semisimple element of odd prime order r such that $C_{\bar{G}}(x)$ is connected. We associate unique integers l and d to x as follows.

(i) If $\bar{G}_\sigma=\mathrm{PGL}_n^\epsilon(q)$ and $r|(q-\epsilon)$ then let $\hat{x}\in\mathrm{GL}_n^\epsilon(q)$ be a lift of x of order r such that $\nu(\hat{x})=n-l'$, where l' is the dimension of the 1-eigenspace of $\hat{x}$. We set $l=l'$ and define d to be the number of distinct primitive r^{th} roots of unity which occur as eigenvalues of $\hat{x}$. Note that $l>0$ and $d+l\leqslant n\leqslant l(d+1)$.

(ii) Otherwise, let $\mu=(l,a_1,\ldots,a_t)$ be the associated σ-tuple of x and define d to be the number of non-zero terms a_j.

Lemma 3.33. *Let $x\in\bar{G}_\sigma$ be a semisimple element of odd prime order r such that $C_{\bar{G}}(x)$ is connected. Define the integers l and d as above and let $i\geqslant 1$ be minimal such that $r|(q^i-1)$. Then $\dim x^{\bar{G}}\geqslant L$, where L is defined as follows:*

G_0	L
$\mathrm{PSL}_n^\epsilon(q)$	$n^2-l^2-\frac{1}{c}(n-l-c(d-1))^2-c(d-1)$
$\mathrm{PSp}_n(q)$	$\frac{1}{2}(n^2+n-l^2-l-\frac{1}{ei}(n-l-i(d-e))^2-i(d-e))$
$\mathrm{P}\Omega_n^\epsilon(q)$	$\frac{1}{2}(n^2-n-l^2+l-\frac{1}{ei}(n-l-i(d-e))^2-i(d-e))$

Here
$$c = c(i,\epsilon) = \begin{cases} 2i & \text{if } \epsilon = - \text{ and } i \text{ is odd} \\ i/2 & \text{if } \epsilon = - \text{ and } i \equiv 2\,(4) \\ i & \text{otherwise} \end{cases}$$
and $e = 2$ if i is odd, otherwise $e = 1$.

Proof. This is immediate since $\dim \mathrm{GL}_{a+b} \geqslant \dim \mathrm{GL}_a + \dim \mathrm{GL}_b$ for all integers a and b. □

A well-known theorem of Steinberg states that centralizers of semisimple elements in a *simply connected* algebraic group are always connected (see [8, 3.5.6] for example) but this is not always the case for the *adjoint* algebraic groups we are working with. However, the next lemma reveals that very few semisimple elements of odd prime order have a non-connected centralizer.

Lemma 3.34. *Let $x \in \bar{G}$ be a semisimple element of odd prime order r. Then either $C_{\bar{G}}(x)$ is connected or $\bar{G} = \mathrm{PSL}_n(K)$, r divides n and x is $\bar{G}$-conjugate to $[I_{\frac{n}{r}}, \omega I_{\frac{n}{r}}, \ldots, \omega^{r-1} I_{\frac{n}{r}}]$ (modulo scalars) where $\omega \in K$ is a primitive r^{th} root of unity.*

Proof. The argument for $\bar{G} = \mathrm{PSL}_n(K)$ is entirely straightforward. The fact that $C_{\bar{G}}(x)$ is connected when $\bar{G}$ is symplectic or orthogonal follows from [22, Corol. 4.6, p.204]. □

Lemma 3.35. *Suppose $\bar{G} = \mathrm{PSL}_n(K)$ and $x \in \bar{G}_\sigma$ is a semisimple element of odd prime order r such that $E = C_{\bar{G}}(x)$ is non-connected. Then the following hold.*

(i) $|H^1(\sigma, E/E^0)| = (r, q-\epsilon)$.

(ii) If r divides $q - \epsilon$ then
$$(x^{\bar{G}})_\sigma = \bigsqcup_{j=0}^{r-1} x_j^{\bar{G}_\sigma} \tag{14}$$
where
$$|C_{\bar{G}_\sigma}(x_j)| = \begin{cases} |\mathrm{SL}^{\epsilon}_{\frac{n}{r}}(q)||\mathrm{GL}^{\epsilon}_{\frac{n}{r}}(q)|^{r-1} r & \text{if } j = 0 \\ (q-\epsilon)^{-1}|\mathrm{GL}^{\epsilon}_{\frac{n}{r}}(q^r)| r & \text{if } 1 \leqslant j \leqslant r-1. \end{cases}$$

(iii) If $(r, q-\epsilon) = 1$ then $(x^{\bar{G}})_\sigma = x^{\bar{G}_\sigma}$ and $|C_{\bar{G}_\sigma}(x)|$ is as follows

ϵ	i	$\lvert C_{\bar{G}_\sigma}(x)\rvert$
$+$	arbitrary	$\lvert \mathrm{SL}_{\frac{n}{r}}(q)\rvert \lvert \mathrm{GL}_{\frac{n}{r}}(q^i)\rvert^{\frac{1}{i}(r-1)}$
$-$	$i \equiv 0\,(4)$	$\lvert \mathrm{SU}_{\frac{n}{r}}(q)\rvert \lvert \mathrm{GL}_{\frac{n}{r}}(q^i)\rvert^{\frac{1}{i}(r-1)}$
	$i \equiv 2\,(4)$	$\lvert \mathrm{SU}_{\frac{n}{r}}(q)\rvert \lvert \mathrm{GU}_{\frac{n}{r}}(q^{\frac{i}{2}})\rvert^{\frac{2}{i}(r-1)}$
	odd	$\lvert \mathrm{SU}_{\frac{n}{r}}(q)\rvert \lvert \mathrm{GL}_{\frac{n}{r}}(q^{2i})\rvert^{\frac{1}{2i}(r-1)}$

where $i \geqslant 1$ is minimal such that $r|(q^i - 1)$.

Proof. First observe that $E/E^0 \cong \mathbb{Z}_r$ and therefore $|H^1(\sigma, E/E^0)| = 1$ or r since the number of elements in each equivalence class divides r. In particular, $|H^1(\sigma, E/E^0)| = r$ if and only if $z^{-1}z^\sigma = 1$ for all $z \in E/E^0$. Without loss we may assume $z^\sigma = z^{\epsilon q}$ and (i) follows immediately. If $|H^1(\sigma, E/E^0)| = 1$ then Lemma 3.11 implies that x lifts to an element $\hat{x} \in \mathrm{GL}^\epsilon_n(q)$ of order r such that $|x^{\bar{G}_\sigma}| = |\hat{x}^{\mathrm{GL}^\epsilon_n(q)}|$ and so (iii) follows from Lemma 3.30. Finally, let us consider (ii). Here (14) follows from Proposition 3.6 and so it remains to justify the orders of the $\bar{G}_\sigma$-centralizers. Relabelling if necessary, we may assume that $x_j \in \mathrm{PGL}^\epsilon_n(q)$ lifts to an element $\hat{x}_j \in \mathrm{GL}^\epsilon_n(q)$ which is $\mathrm{GL}^\epsilon_n(q)$-conjugate to the monomial matrix
$$\begin{pmatrix} & \lambda^j I_{n/r} \\ I_{n-n/r} & \end{pmatrix},$$

where $Z(\mathrm{GL}_n^\epsilon(q)) = \langle \lambda I_n \rangle$. Since r divides $|Z(\mathrm{GL}_n^\epsilon(q))|$ we have $r|x_j^{\bar{G}_\sigma}| = |\hat{x}_j^{\mathrm{GL}_n^\epsilon(q)}|$. If $j = 0$ then $\hat{x}_j$ has order r and we can argue as we did in the proof of Lemma 3.30. Now assume $j > 0$. Then $\hat{x}_j$ has order $r_j = (r/j)[j, q-\epsilon]$, where $[j, q-\epsilon]$ denotes the lowest common multiple of j and $q-\epsilon$, and thus $i_j = \frac{1}{2}(3-\epsilon)r$, where $i_j \geqslant 1$ is the least integer such that r_j divides $q^{i_j} - 1$. The desired result now follows from [25, p.34]. □

Next we establish a semisimple analogue of Proposition 3.22.

Proposition 3.36. *Let $x \in \bar{G}_\sigma$ be an element of odd prime order $r \neq p$ such that $\nu(x) = s$ and $C_{\bar{G}}(x)$ is connected. Then $f_3(n,s,q) < |x^{\bar{G}_\sigma}| < g_3(n,s,q)$, where the functions f_3 and g_3 are defined in Table 3.7 and $a = \frac{1}{2}(1-\epsilon)$.*

G_0	$f_3(n,s,q)$	$g_3(n,s,q)$
$\mathrm{PSL}_n^\epsilon(q)$	$\begin{cases} \frac{1}{2}\left(\frac{q}{q+1}\right)^a q^{2s(n-s)} & s < n/2 \\ \frac{1}{2}\left(\frac{q}{q+1}\right)^{\frac{as}{n-s}} q^{ns} & s \geqslant n/2 \end{cases}$	$2\left(\frac{q}{q-1}\right)^s q^{s(2n-s-1)}$
$\mathrm{PSp}_n(q)$	$\frac{1}{2}\max(q^{s(n-s)}, q^{\frac{1}{2}ns})$	$2\left(\frac{q}{q-1}\right)^{\frac{s}{2}} q^{\frac{1}{2}(2ns-s^2+1)}$
$\mathrm{P\Omega}_n^\epsilon(q)$	$\begin{cases} \frac{1}{4}\left(\frac{q}{q+1}\right) q^{s(n-s)} & s < n/2 \\ \frac{1}{2}\left(\frac{q}{q+1}\right)^{\frac{n}{2(n-s)}} q^{\frac{1}{2}n(s-1)} & s \geqslant n/2 \end{cases}$	$2\left(\frac{q}{q-1}\right)^{\frac{s}{2}} q^{\frac{1}{2}s(2n-s-2)}$

Table 3.7: Bounds on semisimple conjugacy classes

Proof. We begin with the case $G_0 = \mathrm{PSL}_n^\epsilon(q)$. Since $C_{\bar{G}}(x)$ is connected, Lemmas 3.11 and 3.34 imply that there exists a lift $\hat{x} \in \mathrm{GL}_n^\epsilon(q)$ of x such that $\hat{x}$ has order r and $|x^{\bar{G}_\sigma}| = |\hat{x}^{\mathrm{GL}_n^\epsilon(q)}|$. If $\epsilon = +$ then the hypothesis $\nu(x) = s$ implies that $\mathrm{GL}_{n-s}(q^l) \leqslant C_{\mathrm{GL}_n(q)}(\hat{x})$ for some $l \geqslant 1$ and thus

$$|x^{\bar{G}_\sigma}| \leqslant \frac{|\mathrm{GL}_n(q)|}{|\mathrm{GL}_{n-s}(q)||\mathrm{GL}_1(q)|^s} < g_3(n,s,q).$$

Further, Lemma 3.30 implies that $|x^{\bar{G}_\sigma}| > \frac{1}{2}q^{\dim x^{\bar{G}}}$ and the lower bound follows since [6, 2.9] gives $\dim x^{\bar{G}} \geqslant \max(2s(n-s), ns)$. Now assume $\epsilon = -$. Then

$$|x^{\bar{G}_\sigma}| \leqslant \frac{|\mathrm{GU}_n(q)|}{|\mathrm{GU}_{n-s}(q)||\mathrm{GL}_1(q^2)|^{\frac{s}{2}}} < 2\left(\frac{q^2}{q^2-1}\right)^{\frac{s}{2}} q^{2ns-s^2-s} < g_3(n,s,q)$$

and the lower bound holds if $s < n/2$ since $|x^{\bar{G}_\sigma}| \geqslant |\mathrm{GU}_n(q) : \mathrm{GU}_{n-s}(q)\mathrm{GU}_s(q)|$. If $s \geqslant n/2$ then

$$|x^{\bar{G}_\sigma}| \geqslant \frac{|\mathrm{GU}_n(q)|}{|\mathrm{GU}_{n-s}(q)|^{n/(n-s)}} > f_3(n,s,q)$$

as claimed. The symplectic and orthogonal cases are very similar. For example, if $G_0 = \mathrm{PSp}_n(q)$ and s is odd then $s \geqslant n/2$ and the result follows via Proposition 3.9 since

$$\frac{|\mathrm{Sp}_n(q)|}{|\mathrm{GU}_{n-s}(q)|^{n/2(n-s)}} \leqslant |x^{\bar{G}_\sigma}| \leqslant \frac{|\mathrm{Sp}_n(q)|}{|\mathrm{GL}_{n-s}(q)||\mathrm{GL}_1(q)|^{s-\frac{n}{2}}}.$$

The remaining cases are left to the reader. □

Detailed information on the semisimple involution classes in $\bar{G}$ and $\bar{G}_\sigma$ is given in [11]. We summarise some of this data in the next proposition.

Proposition 3.37. *Suppose p is odd and $x \in \bar{G}_\sigma$ is an involution. Then $|C_{\bar{G}_\sigma}(x)|$ and bounds $f_4(n,s,q) < |x^{\bar{G}_\sigma}| < g_4(n,s,q)$ are recorded in Table 3.8.*

G_0	s	$k_{s,2,s}(\bar{G}_\sigma)$	$\lvert C_{\bar{G}_\sigma}(x)\rvert$	$f_4(n,s,q)$	$g_4(n,s,q)$
$\mathrm{PSL}^\epsilon_n(q)$	$< \frac{n}{2}$	1	$\lvert\mathrm{SL}^\epsilon_s(q)\rvert\lvert\mathrm{GL}^\epsilon_{n-s}(q)\rvert$	$\frac{1}{2}\left(\frac{q}{q+1}\right)^{\frac{1}{2}(1-\epsilon)} q^{2s(n-s)}$	$2^{\frac{1}{2}(1+\epsilon)}q^{2s(n-s)}$
	$\frac{n}{2}$	2	$\lvert\mathrm{SL}^\epsilon_{\frac{n}{2}}(q)\rvert\lvert\mathrm{GL}^\epsilon_{\frac{n}{2}}(q)\rvert 2$	$\frac{1}{4}\left(\frac{q}{q+1}\right)^{\frac{1}{2}(1-\epsilon)} q^{\frac{1}{2}n^2}$	$2^{-\frac{1}{2}(1-\epsilon)}q^{\frac{1}{2}n^2}$
			$(q-\epsilon)^{-1}\lvert\mathrm{GL}_{\frac{n}{2}}(q^2)\rvert 2$	$\frac{1}{4}q^{\frac{1}{2}n^2}$	$2^{\frac{1}{2}(1-\epsilon)}q^{\frac{1}{2}n^2}$
$\mathrm{PSp}_n(q)$	$< \frac{n}{2}$, even	1	$\lvert\mathrm{Sp}_s(q)\rvert\lvert\mathrm{Sp}_{n-s}(q)\rvert$	$\frac{1}{2}q^{s(n-s)}$	$2q^{s(n-s)}$
	$\frac{n}{2}$ odd	2	$\lvert\mathrm{GL}^\epsilon_{\frac{n}{2}}(q)\rvert 2$	$\frac{1}{4}\left(\frac{q}{q+1}\right) q^{\frac{1}{4}n(n+2)}$	$q^{\frac{1}{4}n(n+2)}$
	$\frac{n}{2}$ even	4	$\lvert\mathrm{GL}^\epsilon_{\frac{n}{2}}(q)\rvert 2$	$\frac{1}{4}\left(\frac{q}{q+1}\right) q^{\frac{1}{4}n(n+2)}$	$q^{\frac{1}{4}n(n+2)}$
			$\lvert\mathrm{Sp}_{\frac{n}{2}}(q)\rvert^2 2$	$\frac{1}{4}q^{\frac{1}{4}n^2}$	$q^{\frac{1}{4}n^2}$
			$\lvert\mathrm{Sp}_{\frac{n}{2}}(q^2)\rvert 2$	$\frac{1}{4}q^{\frac{1}{4}n^2}$	$\frac{1}{2}q^{\frac{1}{4}n^2}$
$\mathrm{P\Omega}^+_n(q)$	$< \frac{n}{2}$, even	2	$\lvert\mathrm{SO}^\epsilon_s(q)\rvert\lvert\mathrm{SO}^\epsilon_{n-s}(q)\rvert 2$	$\frac{1}{4}\left(\frac{q}{q+1}\right) q^{s(n-s)}$	$2q^{s(n-s)}$
	$\frac{n}{2}$ odd	1	$\lvert\mathrm{GL}_{\frac{n}{2}}(q)\rvert$	$\frac{1}{2}q^{\frac{1}{4}n(n-2)}$	$2q^{\frac{1}{4}n(n-2)}$
	$\frac{n}{2}$ even	8	$\lvert\mathrm{GL}^\epsilon_{\frac{n}{2}}(q)\rvert 2^\dagger$	$\frac{1}{4}\left(\frac{q}{q+1}\right) q^{\frac{1}{4}n(n-2)}$	$q^{\frac{1}{4}n(n-2)}$
			$\lvert\mathrm{SO}^+_{\frac{n}{2}}(q^2)\rvert 4^\dagger$	$\frac{1}{8}q^{\frac{1}{4}n^2}$	$\frac{1}{2}q^{\frac{1}{4}n^2}$
			$\lvert\mathrm{SO}^\epsilon_{\frac{n}{2}}(q)\rvert^2 4$	$\frac{1}{8}q^{\frac{1}{4}n^2}$	$q^{\frac{1}{4}n^2}$
$\mathrm{P\Omega}^-_n(q)$	$< \frac{n}{2}$, even	2	$\lvert\mathrm{SO}^\epsilon_s(q)\rvert\lvert\mathrm{SO}^{-\epsilon}_{n-s}(q)\rvert 2$	$\frac{1}{4}\left(\frac{q}{q+1}\right) q^{s(n-s)}$	$2q^{s(n-s)}$
	$\frac{n}{2}$ odd	1	$\lvert\mathrm{GU}_{\frac{n}{2}}(q)\rvert$	$\frac{1}{2}\left(\frac{q}{q+1}\right) q^{\frac{1}{4}n(n-2)}$	$q^{\frac{1}{4}n(n-2)}$
	$\frac{n}{2}$ even	2	$\lvert\mathrm{SO}^+_{\frac{n}{2}}(q)\rvert\lvert\mathrm{SO}^-_{\frac{n}{2}}(q)\rvert 2$	$\frac{1}{4}q^{\frac{1}{4}n^2}$	$2q^{\frac{1}{4}n^2}$
			$\lvert\mathrm{SO}^-_{\frac{n}{2}}(q^2)\rvert 2$	$\frac{1}{4}q^{\frac{1}{4}n^2}$	$q^{\frac{1}{4}n^2}$
$\Omega_n(q)$	1	2	$\lvert\mathrm{SO}^\epsilon_{n-1}(q)\rvert 2$	$\frac{1}{4}\left(\frac{q}{q+1}\right) q^{n-1}$	q^{n-1}
	even	2	$\lvert\mathrm{SO}^\epsilon_s(q)\rvert\lvert\mathrm{SO}_{n-s}(q)\rvert 2$	$\frac{1}{4}\left(\frac{q}{q+1}\right) q^{s(n-s)}$	$q^{s(n-s)}$
	> 1, odd	2	$\lvert\mathrm{SO}_s(q)\rvert\lvert\mathrm{SO}^\epsilon_{n-s}(q)\rvert 2$	$\frac{1}{4}\left(\frac{q}{q+1}\right) q^{s(n-s)}$	$q^{s(n-s)}$

† There are precisely two distinct $\bar{G}_\sigma$-classes with centralizer of this type

Table 3.8: Semisimple involutions

Proof. The entries in the third and fourth columns of Table 3.8 follow from [11, Table 4.5.1], while the bounds on $|x^{\bar{G}_\sigma}|$ are obtained via Proposition 3.9. $\square$

As an immediate corollary to Propositions 3.22, 3.36 and 3.37 we obtain the next result.

Corollary 3.38. *Let $x \in \bar{G}_\sigma$ be an element of prime order r such that $\nu(x) = s$. Then*

$$F(n,s,q) < |x^{\bar{G}_\sigma}| < G(n,s,q),$$

where the functions F and G are defined in Table 3.9 and $a = \frac{1}{2}(1-\epsilon)$. Here $b = 1$ if n is odd and $(r,s) = (2,1)$, otherwise $b = 0$.

G_0	$F(n,s,q)$	$G(n,s,q)$
$\mathrm{PSL}_n^\epsilon(q)$	$\begin{cases} \frac{1}{2}\left(\frac{q}{q+1}\right)^{a} q^{2s(n-s)} & s < n/2 \\ \frac{1}{2r}\left(\frac{q}{q+1}\right)^{\frac{as}{n-s}} q^{ns} & s \geqslant n/2 \end{cases}$	$2\left(\frac{q}{q-1}\right)^{s} q^{s(2n-s-1)}$
$\mathrm{PSp}_n(q)$	$\frac{1}{4}\left(\frac{q}{q+1}\right)\max(q^{s(n-s)}, q^{\frac{1}{2}ns})$	$2\left(\frac{q}{q-1}\right)^{\frac{s}{2}} q^{\frac{1}{2}(2ns-s^2+1)}$
$\mathrm{P\Omega}_n^\epsilon(q)$	$\begin{cases} \frac{1}{4}\left(\frac{q}{q+1}\right) q^{s(n-s-1)} & s \leqslant n/2 \\ \frac{1}{2}\left(\frac{q}{q+1}\right)^{\frac{n}{2(n-s)}} q^{\frac{1}{2}n(s-1)} & s > n/2 \end{cases}$	$2\left(\frac{q}{q-1}\right)^{\frac{s}{2}} q^{\frac{1}{2}s(2n-s-2)+\frac{b}{2}}$

Table 3.9: Bounds on conjugacy classes of elements of prime order

To close this section on semisimple elements we establish a semisimple analogue of Proposition 3.24. Let $x \in \bar{G}_\sigma$ be a semisimple element of odd prime order r, with associated σ-tuple μ. In order to compute $k_{s,r,s}(\bar{G}_\sigma)$, it is important to know when μ uniquely determines the $\bar{G}_\sigma$-class of x. According to Corollary 3.7, this happens if and only if the $\bar{G}$-class of x is uniquely determined by $\mathcal{E}_x$.

Lemma 3.39. *Let $x \in \bar{G}_\sigma$ be a semisimple element of odd prime order r such that $C_{\bar{G}}(x)$ is connected and $(r, q-\epsilon) = 1$ if $\bar{G}_\sigma = \mathrm{PGL}_n^\epsilon(q)$. Then one of the following holds:*

(i) The $\bar{G}$-class of x is uniquely determined by $\mathcal{E}_x$;

(ii) $\bar{G} = \mathrm{PSO}_n(K)$, n is even, $1 \notin \mathcal{E}_x$ and there are precisely two distinct $\bar{G}$-classes corresponding to $\mathcal{E}_x$ which fuse in $\mathrm{PO}_n(K)$.

Proof. Let $y \in \bar{G}_\sigma$ be a semisimple element of prime order r such that $C_{\bar{G}}(y)$ is connected and $\mathcal{E}_y = \mathcal{E}_x = \{\lambda_1, \ldots, \lambda_n\}$. We begin by assuming $\bar{G}_\sigma = \mathrm{PGL}_n^\epsilon(q)$. Let $\hat{x}$ and $\hat{y}$ denote the unique lifts of x and y to elements of order r in $\mathrm{GL}_n^\epsilon(q)$ and observe that $\hat{x}, \hat{y} \in \mathrm{SL}_n^\epsilon(q) \leqslant \mathrm{SL}_n(K)$. Replacing y by a suitable $\bar{G}$-conjugate, we may assume that there is a K-basis $\{v_1, \ldots, v_n\}$ of $\bar{V} = V \otimes K$ and a permutation $\rho \in S_n$ such that $v_k\hat{x} = \lambda_k v_k$ and $v_k\hat{y} = \lambda_{\rho(k)}v_k$ for each $1 \leqslant k \leqslant n$. Write $\rho = \rho_1 \cdots \rho_l$ as a product of transpositions. If a transposition $\pi \in S_n$ swaps i and j ($i \neq j$) then define T_π to be the unique element in $\mathrm{SL}_n(K)$ which maps $v_i \mapsto v_j$, $v_j \mapsto -v_i$ and fixes every other basis vector. Then $\hat{x} = z^{-1}\hat{y}z$, where $z = \prod_1^l T_{\rho_i}$, and thus x and y are $\bar{G}$-conjugate as claimed.

If $\bar{G} = \mathrm{PSp}_n(K)$ then we may lift x and y to elements $\hat{x}$ and $\hat{y}$ of order r in $\mathrm{Sp}_n(K)$. The previous argument implies that $\hat{x}$ and $\hat{y}$ are $\mathrm{SL}_n(K)$-conjugate and thus $\mathrm{Sp}_n(K)$-conjugate (see [25, p.36] for example). Similarly, if $\bar{G} = \mathrm{PSO}_n(K)$ then $\hat{x}$ and $\hat{y}$ are $\mathrm{O}_n(K)$-conjugate. If $1 \in \mathcal{E}_x$ (which must be the case if n is odd) then $\mathrm{O}_n(K)$-conjugacy implies $\mathrm{SO}_n(K)$-conjugacy as we can always ensure that our conjugating element comprises an even number of reflections. On the other hand, if $1 \notin \mathcal{E}_x$ then the $\mathrm{O}_n(K)$-class of x splits into two $\mathrm{SO}_n(K)$-classes, with representatives x and x^γ where $\gamma \in \mathrm{O}_n(K)$ is a reflection. $\square$

Proposition 3.40. *If r is prime then*

$$k_{s,r,s}(\bar{G}_\sigma) \leqslant \begin{cases} q^{\zeta s} & \text{if } s < n/2 \\ q^{\zeta(s+1)} & \text{otherwise,} \end{cases}$$

where $\zeta = 1$ if $\bar{G} = \mathrm{PSL}_n(K)$, otherwise $\zeta = 1/2$.

Proof. In view of Proposition 3.37 we may assume r is odd. Let $i \geqslant 1$ be minimal such that $r|(q^i - 1)$ and assume for now that $\bar{G}_\sigma = \mathrm{PGL}_n^\epsilon(q)$. Define $c = c(i, \epsilon)$ as in the statement of Lemma 3.33 and let $x \in \bar{G}_\sigma$ be a semisimple element of prime order r with $\nu(x) = s$. If $c = 1$ and $C_{\bar{G}}(x)$ is connected then x lifts to an element $\hat{x} \in \mathrm{GL}_n^\epsilon(q)$ such that $\hat{x} = [I_{n-s}, \lambda_1, \ldots, \lambda_s]$, where each λ_j is a primitive r^{th} root of unity. Applying Lemma 3.35 we deduce that

$$k_{s,r,s}(\bar{G}_\sigma) \leqslant (r-1)^s + \alpha(r-1),$$

where $\alpha = 1$ if $s = n(1 - 1/r)$, otherwise $\alpha = 0$. The result now follows since the hypothesis $c = 1$ implies that $r - 1 \leqslant q$. Now assume $c > 1$. Here we apply Lemma 3.39 and count the number of possible associated σ-tuples. Let N_1 (resp. N_2) denote the set of associated σ-tuples $(l, a_1, \ldots, a_t)$ with $l = n - s$ (resp. $l < n - s$) which correspond to semisimple $\bar{G}_\sigma$-classes $x^{\bar{G}_\sigma}$, where x has order r and $\nu(x) = s$. Then Lemma 3.39 implies that $k_{s,r,s}(\bar{G}_\sigma) \leqslant |N_1| + |N_2|$ and we note that N_2 is empty if $s < n/2$. A tuple $\mu = (l, a_1, \ldots, a_t)$ in N_1 satisfies $\sum_j a_j = s/c$ and since there are precisely $(r-1)/c$ distinct non-trivial σ-orbits on $\mathscr{S}_r$ it follows that

$$|N_1| \leqslant \left(\frac{r-1}{c}\right)^{\frac{s}{c}} \leqslant \left(\frac{q^c}{c}\right)^{\frac{s}{c}} \leqslant \frac{1}{2}q^s.$$

If $s = n - 1$ and N_2 is non-empty then $n = mc$ for some $m \leqslant (r-1)/c$ and

$$|N_2| = \binom{(r-1)/c}{m} \leqslant \left(\frac{r-1}{c}\right)^{\frac{1}{c}(s+1)} \leqslant \frac{1}{2}q^{s+1}$$

since $m = (s+1)/c$ and $\binom{a}{b} \leqslant a^b$ for all integers $a \geqslant b \geqslant 0$. If $n - s > 1$ then define N_2^j to be the set of tuples in N_2 with $a_j = n - s$, where $1 \leqslant j \leqslant (r-1)/c$. If $\mu \in N_2^j$ then $0 \leqslant \sum_{m \neq j} a_m \leqslant \lfloor n/c - n + s \rfloor = k$ and thus

$$|N_2| = \sum_{j=1}^{(r-1)/c} |N_2^j| \leqslant \left(\frac{r-1}{c}\right) \sum_{m=0}^{k} \left(\frac{r-1}{c} - 1\right)^m < \sum_{m=0}^{k} \left(\frac{q^c}{c}\right)^{m+1} \leqslant \frac{1}{2}q^{c(k+1)}.$$

The result now follows since the hypothesis $n - s > 1$ implies that $c(k+1) \leqslant s$.

Now assume $\bar{G}$ is symplectic or orthogonal. Define i, N_1 and N_2 as before and note that we may assume $n \geqslant 4$. Also observe that Lemma 3.39 implies that $k_{s,r,s}(\bar{G}_\sigma) \leqslant |N_1| + 2^a|N_2|$, where $a = 1$ if $\bar{G} = \mathrm{PSO}_n(K)$ and n is even, otherwise $a = 0$. Assume for now that i is even, so $r - 1 \leqslant q^{i/2}$,

$$|N_1| \leqslant \left(\frac{r-1}{i}\right)^{\frac{s}{i}} \leqslant \frac{1}{2}q^{\frac{s}{2}} \tag{15}$$

and $|N_2| = 0$ if $s < n/2$. If $r - 1 = i$ then $|N_2| \leqslant 1$ and the result follows. Now assume $r - 1 > i$, whence $q \geqslant 4$ if $i = 2$. If $s = n - 1$ then

$$|N_2| \leqslant \binom{(r-1)/i}{(s+1)/i} \leqslant \left(\frac{1}{i}\right)^{\frac{1}{i}(s+1)} q^{\frac{1}{2}(s+1)} < \frac{1}{4}q^{\frac{1}{2}(s+1)}$$

and the result follows via (15). Now assume $s < n - 1$. Then

$$|N_2| < \sum_{m=0}^{k} \left(\frac{q^{i/2}}{i}\right)^{m+1} < \left(\frac{2}{i^{k+1}}\right) q^{\frac{i}{2}(k+1)} \leqslant \left(\frac{2}{i^{k+1}}\right) q^{\frac{1}{2}(n-ni+si+i)},$$

G_0	r	type of $C_{G_0}(\alpha)$
$\mathrm{PSL}_n^{\epsilon}(q)$	2	$\mathrm{PSO}_n(q)$ n odd
$(n \geqslant 3)$		$\mathrm{PSO}_n^{\epsilon}(q)$, $\mathrm{PSp}_n(q)$ n even, q odd
		$\mathrm{Sp}_n(q)$, $C_{\mathrm{Sp}_n(q)}(t)$ n even, q even
$\mathrm{P\Omega}_8^+(q)$	3	$G_2(q)$, $\mathrm{PGL}_3^{\epsilon}(q)$ if $q \equiv \epsilon\,(3)$
		$G_2(q)$, $C_{G_2(q)}(t)$ if $q \equiv 0\,(3)$

Table 3.10: Graph automorphisms of prime order r

where $k = \lfloor n/i - n + s \rfloor$. Since i is even we have $n - ni + si + i \leqslant s$ and thus

$$|N_2| < \left(\frac{2}{q^{1/2} i^{k+1}}\right) q^{\frac{1}{2}(s+1)} = b.q^{\frac{1}{2}(s+1)}.$$

If $k \geqslant 1$ then $b \leqslant 1/4$ and the result follows; if $k = 0$ then

$$|N_2| \leqslant \frac{1}{i}(r-1) \leqslant \frac{1}{i} q^{\frac{i}{2}} \leqslant \frac{1}{i} q^{\frac{1}{2}(s+1)}$$

and we are left to deal with the case $(i, a) = (2, 1)$. Here $s \geqslant 2$, $q \geqslant 4$ and thus $|N_2| \leqslant \frac{1}{2}q \leqslant \frac{1}{4}q^{(s+1)/2}$ as required. The argument when i is odd is very similar. $\square$

3.5 Outer automorphisms

We now consider the other automorphisms of a finite simple classical group. The following fundamental theorem is due to Steinberg.

Theorem 3.41 ([24, Theorem 30]). *If G_0 is a finite simple group of Lie type then* $\mathrm{Aut}(G_0)$ *is generated by inner, diagonal, field and graph automorphisms.*

Remark 3.42. We adopt the terminology of [11, 2.5.13] for the various automorphisms of G_0. In particular, if $G_0 \in \{\mathrm{PSU}_n(q), \mathrm{P\Omega}_n^-(q)\}$ then there are no field automorphisms of even order and no graph-field automorphisms.

In the next proposition it is convenient to write $L(q)$ for a simple group of Lie type, where L ranges over the familiar Lie symbols A_{n-1}, ${}^3D_4$, E_6 and so on. We write $\Delta_{L(q)}$ for the group of inner-diagonal automorphisms of $L(q)$.

Proposition 3.43 ([11, 4.9.1]). *Let $L = L(q)$ be a simple group of Lie type over $\mathbb{F}_q$ and let x be a field or graph-field automorphism of prime order r. Then the following hold.*

(i) If $y \in \Delta_L x$ has order r then x and y are Δ_L-conjugate;

(ii) If x is a field automorphism then $q = q_0^r$ and $C_{\Delta_L}(x) \cong \Delta_{L(q_0)}$, while if x is a graph-field automorphism and $(L, p) \neq (\mathrm{Sp}_4(q)', 2)$ then $r = 2$ or 3, $q = q_0^r$ and $C_{\Delta_L}(x) \cong \Delta_{{}^rL(q_0)}$.

Remark 3.44. If $p = 2$ then $G_0 = \mathrm{Sp}_4(q)'$ admits an outer automorphism $\varphi \in \mathrm{Aut}(G_0) - \mathrm{PGL}(V)$. Following [11, 2.5.13], we say that φ is a graph-field automorphism. If $\log_2 q$ is odd then G_0 admits a field automorphism θ such that $\tau = \varphi\theta$ is an involution and $C_{\Delta_{G_0}}(\tau) = Sz(q)$. We refer the reader to Proposition 3.52 (and its proof) for further details.

Proposition 3.45. *If $\alpha \in G - \mathrm{PGL}(V)$ is a graph automorphism of prime order r then the possibilities for G_0, $C_G(\alpha)$ and r are listed in Table 3.10, where t is a long root element.*

Proof. If $G_0 = \mathrm{PSL}_n^{\epsilon}(q)$ then this follows from [11, Table 4.5.1] when p is odd and [2, §19] when $p = 2$. See [17, 1.4.1] for the case $G_0 = \mathrm{P\Omega}_8^+(q)$. $\square$

Remark 3.46. In Table 3.10, $C_{G_0}(\alpha)$ could contain the listed group with small index, hence the term 'type'. More precisely, if $C_{G_0}(\alpha)$ is of type T then $C_{G_0}(\alpha) = N_{G_0}(T)$ and we note that $N_{G_0}(T) = T$ if $G_0 = \mathrm{P\Omega}_8^+(q)$ (see [17, 1.4.1]). The element t appearing in the fourth row of the table is a long root element of $\mathrm{Sp}_n(q)$, i.e. t is a b_1-involution in the terminology of Proposition 3.22 and thus $|t^{\mathrm{Sp}_n(q)}| = q^n - 1$. Similarly, in the last row we have $|t^{G_2(q)}| = q^6 - 1$. If $G_0 = \mathrm{PSL}_n^\epsilon(q)$ (resp. $\mathrm{P\Omega}_8^+(q)$) then each possible type for $C_{G_0}(\alpha)$ corresponds to precisely one (resp. two) Δ_{G_0}-class(es) of graph automorphisms.

Definition 3.47. Suppose $\alpha \in G - \mathrm{PGL}(V)$ is a graph automorphism of prime order. If $G_0 = \mathrm{PSL}_n^\epsilon(q)$ then we say that α is of *symplectic-type* if $C_{G_0}(\alpha)$ has socle $\mathrm{PSp}_n(q)$, otherwise α is *non-symplectic* (or *orthogonal* if q is odd). If $G_0 = \mathrm{P\Omega}_8^+(q)$ then α is said to be a *triality graph automorphism*; it is of *G_2-type* if $C_{G_0}(\alpha) = G_2(q)$, otherwise α is a *non-G_2 triality*. In general, a *triality automorphism* is any order three graph or graph-field automorphism of $\mathrm{P\Omega}_8^+(q)$.

Lower bounds on the size of G_0-classes of certain outer automorphisms are recorded in the next lemma. Here we denote the *type* of each outer automorphism by writing f, g and gf for $f$ield, $g$raph and $g$raph-$f$ield automorphisms respectively.

Lemma 3.48. *Let $x \in \mathrm{Aut}(G_0) - \mathrm{PGL}(V)$ be an element of prime order r. Then $|x^{G_0}| > h(n,r,q)$, where h is given in Table 3.11.*

Proof. For field and graph-field automorphisms we apply Proposition 3.43(ii). For example, if $G_0 = \mathrm{P\Omega}_n^\epsilon(q)$, where n is even and $q = q_0^r$, then the relevant bounds hold since

$$|\mathrm{O}_n^\epsilon(q_0^r) : \mathrm{O}_n^\epsilon(q_0)| > q^{\frac{1}{2}n(n-1)\left(1-\frac{1}{r}\right)}, \quad |\mathrm{O}_n^+(q_0^2) : \mathrm{O}_n^-(q_0)| > q^{\frac{1}{4}n(n-1)}.$$

Similarly, if $G_0 = \mathrm{PSL}_n^\epsilon(q)$ and x is a field automorphism then

$$|x^{G_0}| \geqslant (n, q-\epsilon)^{-1}|x^{\bar{G}_\sigma}| = \frac{|\mathrm{PSL}_n^\epsilon(q)|}{|\mathrm{PGL}_n^\epsilon(q^{1/r})|} > \frac{1}{2}\left(\frac{q}{q+1}\right)^{\frac{1}{2}(1-\epsilon)} q^{(n^2-1)\left(1-\frac{1}{r}\right)-1}$$

as claimed. If $G_0 = \mathrm{P\Omega}_8^+(q)$, $q = q_0^3$ and x is a triality graph-field automorphism then $C_{G_0}(x) \cong {}^3D_4(q_0)$ and the result follows since

$$|x^{G_0}| = |\mathrm{P\Omega}_8^+(q_0^3) : {}^3D_4(q_0)| \geqslant \frac{1}{4}q_0^{24}(q_0^2+1)(q_0^{12}-1)(q_0^{18}-1) > \frac{1}{4}q_0^{56}.$$

The possibilities for $C_{G_0}(x)$ when x is a triality graph automorphism are listed in Table 3.10 and the bound $|x^{G_0}| > \frac{1}{8}q^{14}$ quickly follows. If $G_0 = \mathrm{Sp}_4(q)'$ and x is an involutory graph-field automorphism then $|x^{G_0}| \geqslant |\mathrm{Sp}_4(q) : Sz(q)| = q^2(q+1)(q^2-1) > q^5$ as claimed. Finally, let us assume x is an involutory graph automorphism of $G_0 = \mathrm{PSL}_n^\epsilon(q)$. If n is odd then $C_{G_0}(x)$ is orthogonal and the desired bound follows since $|C_{G_0}(x)| = 2^{-\alpha}|\mathrm{O}_n(q)|$, where $\alpha = 2 - \delta_{2,p}$ (see [18, 4.5.5, 4.8.4] and [2, 19.9(i)]). If n is even then the bound follows from [18, 4.5, 4.8] if q is odd and from [2, 19.9(ii)] if q is even. □

Corollary 3.49. *If $x \in \mathrm{Aut}(G_0) - \mathrm{PGL}(V)$ has prime order then $|x^{G_0}| > H(n,q)$, where H is defined as follows:*

G_0	$H(n,q)$
$\mathrm{PSL}_n^\epsilon(q)$	$\frac{1}{2}\left(\frac{q}{q+1}\right)^{\frac{1}{2}(1-\epsilon)} q^{\frac{1}{2}(n^2-n-4)}$
$\mathrm{PSp}_n(q)$	$\frac{1}{4}q^{\frac{1}{4}n(n+1)}$
$\mathrm{P\Omega}_n^\epsilon(q)$	$\frac{1}{8}q^{\frac{1}{4}n(n-1)}$

Lemma 3.50. *Let $H \leqslant G$ be a subgroup and suppose $x \in H - \mathrm{PGL}(V)$ has prime order. Then either $x^G \cap H \subseteq \widetilde{H}x$, where $\widetilde{H} = H \cap \bar{G}_\sigma$, or x is a triality automorphism of $G_0 = \mathrm{P\Omega}_8^+(q)$, G contains an involutory graph automorphism of G_0 and $x^G \cap H \subseteq \widetilde{H}x \cup \widetilde{H}x^2$.*

G_0	type	conditions	$h(n,r,q)$
$\mathrm{PSL}^{\epsilon}_n(q)$	f	$q=q_0^r$, $r>2$ if $\epsilon=-$	$\frac{1}{2}\left(\frac{q}{q+1}\right)^{\frac{1}{2}(1-\epsilon)}q^{(n^2-1)\left(1-\frac{1}{r}\right)-1}$
	g	$r=2$, n odd	$\frac{1}{2}\left(\frac{q}{q+1}\right)^{\frac{1}{2}(1-\epsilon)}q^{\frac{1}{2}(n^2+n-4)}$
	g	$r=2$, n even	$\frac{1}{2}\left(\frac{q}{q+1}\right)^{\frac{1}{2}(1-\epsilon)}q^{\frac{1}{2}(n^2-n-4)}$
	gf	$(r,q,\epsilon)=(2,q_0^2,+)$	$\frac{1}{2}q^{\frac{1}{2}(n^2-3)}$
$\mathrm{PSp}_n(q)$	f	$q=q_0^r$	$\frac{1}{4}q^{\frac{1}{2}n(n+1)\left(1-\frac{1}{r}\right)}$
	gf	$(n,r,p)=(4,2,2)$, $\log_2 q$ odd	q^5
$\mathrm{P\Omega}^{\epsilon}_n(q)$, n even	f	$q=q_0^r$	$\frac{1}{4}q^{\frac{1}{2}n(n-1)\left(1-\frac{1}{r}\right)}$
	gf	$(r,q,\epsilon)=(2,q_0^2,+)$	$\frac{1}{4}q^{\frac{1}{4}n(n-1)}$
	gf	$(n,r,q,\epsilon)=(8,3,q_0^3,+)$	$\frac{1}{4}q^{\frac{56}{3}}$
	g	$(n,r,\epsilon)=(8,3,+)$	$\frac{1}{8}q^{14}$
$\Omega_n(q)$, nq odd	f	$q=q_0^r$	$\frac{1}{4}q^{\frac{1}{2}n(n-1)\left(1-\frac{1}{r}\right)}$

Table 3.11: Conjugacy classes of graph, field and graph-field automorphisms

Proof. Define $\widetilde{G}=G\cap\bar{G}_\sigma$. According to [11, 2.5.12], field and graph automorphisms of G_0 commute modulo $\bar{G}_\sigma$ and it follows that either $x^G=x^{\widetilde{G}}$ or x is a triality automorphism of $G_0=\mathrm{P\Omega}^+_8(q)$, G contains an involutory graph automorphism and $x^G=x^{\widetilde{G}}\cup(x^2)^{\widetilde{G}}$. Since $\widetilde{G}$ is normal in G we have $(x^i)^{\widetilde{G}}\cap H\subseteq\widetilde{H}x^i$ and the desired result follows. □

In the next proposition we describe how the elements of $\mathrm{Aut}(G_0)$ permute the $\bar{G}_\sigma$-classes of elements of prime order. Two cases merit special attention:

(a) $G_0=\mathrm{Sp}_4(q)'$, q even: action of graph-field automorphisms;
(b) $G_0=\mathrm{P\Omega}^+_8(q)$: action of triality graph automorphisms.

We deal with cases (a) and (b) in Propositions 3.52 and 3.55 respectively; the remaining cases are considered in Proposition 3.51 below. Here we adopt the $c(i,\epsilon)$ notation from Lemma 3.33 and also the x_j notation from Lemma 3.35.

Proposition 3.51. *Let $x\in\bar{G}_\sigma$ be an element of prime order r and define*

$$G=\begin{cases}\mathrm{Sp}_4(q).\langle\phi\rangle & \text{if } G_0=\mathrm{Sp}_4(q)',\ q \text{ even}\\ \mathrm{PGO}^+_8(q).\langle\phi\rangle & \text{if } G_0=\mathrm{P\Omega}^+_8(q)\\ \mathrm{Aut}(G_0) & \text{otherwise,}\end{cases}$$

where ϕ is a field automorphism of order $f=\log_p q$.

(i) *Suppose $r\neq p$ is odd. Let $i\geqslant 1$ be minimal such that $r|(q^i-1)$ and set $c=c(i,\epsilon)$ if $G_0=\mathrm{PSL}^{\epsilon}_n(q)$.*

(a) *If x has associated σ-tuple $\mu=(l,a_1,\ldots,a_t)$ and $\tau\in G$ then x^τ has corresponding σ-tuple $\mu'=(l,a_{\rho(1)},\ldots,a_{\rho(t)})$ for one of M possible permutations $\rho\in S_t$, where M divides $N=2^\alpha f$ and $\alpha=1$ if $G_0=\mathrm{PSL}^{\epsilon}_n(q)$ and c is odd, otherwise $\alpha=0$.*

(b) *Suppose $G_0=\mathrm{PSL}^{\epsilon}_n(q)$. If $C_{\bar{G}}(x)$ is connected and $c=1$ then x^G is a union of d distinct $\bar{G}_\sigma$-classes, for some divisor d of $2f$. If $C_{\bar{G}}(x)$ is non-connected and $c=1$ then either $x=x_0$ and $x^G=x^{\bar{G}_\sigma}$ or $x=x_j$ for some $1\leqslant j\leqslant r-1$ and $x^G=\bigcup_{\lambda\in\Lambda}x_\lambda^{\bar{G}_\sigma}$ for a subset $\Lambda\subseteq\{1,\ldots,r-1\}$ where $|\Lambda|$ divides $2f$. If $C_{\bar{G}}(x)$ is non-connected and $c>1$ then $x^G=x^{\bar{G}_\sigma}$.*

(ii) *Now assume $r = 2$ if $r \neq p$. Then either $x^G = x^{\bar{G}_\sigma}$ or $G_0 = \mathrm{P\Omega}_n^+(q)$ and $x^G = x^{\bar{G}_\sigma} \cup (x^\tau)^{\bar{G}_\sigma}$ where τ is an involutory graph automorphism, $n \equiv 0\,(4)$ and one of the following holds:*

(a) *$r = p > 2$ and the associated partition of x has no odd parts;*

(b) *$r = p = 2$ and x is $\mathrm{O}_n^+(q)$-conjugate to $a_{n/2}$;*

(c) *$r = 2 < p$ and $|C_{\bar{G}_\sigma}(x)| = |\mathrm{GL}_{n/2}^\epsilon(q)|2$ or $|\mathrm{O}_{n/2}^+(q^2)|2$.*

Proof. We begin with (i)(a). If τ is a field automorphism then without loss we may assume τ is standard, say $\tau = \sigma_p^j$ where σ_p is the Frobenius morphism corresponding to the automorphism $\lambda \mapsto \lambda^p$ of the underlying finite field. Then μ' has the given form since σ_p^j permutes the non-trivial σ-orbits. Furthermore, μ' is determined by $\mathcal{E}_{x^\tau}$ and so the number of distinct possibilities for μ' divides $\log_p q = f$. If $G_0 = \mathrm{PSL}_n^\epsilon(q)$ and $\tau \in G$ is an involutory graph automorphism then $\mathcal{E}_{x^\tau} = \{\lambda^{-1} : \lambda \in \mathcal{E}_x\}$. Therefore $\mathcal{E}_x \neq \mathcal{E}_{x^\tau}$ if and only if c is odd and the multiplicity of a non-trivial σ-orbit Ω_j in $\mathcal{E}_x$ differs from that of Ω_j^{-1} for some j. Now consider (i)(b). If $C_{\bar{G}}(x)$ is non-connected then Lemma 3.34 implies that x is $\bar{G}$-conjugate to $[I_{n/r}, \omega I_{n/r}, \ldots, \omega^{r-1} I_{n/r}]$, where $\omega \in K$ is a primitive r^{th} root of unity. If $c > 1$ then $\mathcal{E}_x$ is well-defined and $x^G = x^{\bar{G}_\sigma}$ since $\mathcal{E}_x = \mathcal{E}_{x^\tau}$ for all $\tau \in G$. The same argument applies if $c = 1$ and x is $\bar{G}_\sigma$-conjugate to x_0. The remaining claims are trivial since $|G : \bar{G}_\sigma| = 2f$.

For (ii), let us begin by assuming $G_0 = \mathrm{PSL}_n^\epsilon(q)$. If $r = p$ then the $\bar{G}_\sigma$-class of x is uniquely determined by its associated partition λ. Of course, if $\tau \in G$ is a field automorphism then x and x^τ have the same Jordan decomposition on $\bar{V} = V \otimes K$ and therefore x and x^τ are $\bar{G}_\sigma$-conjugate since $C_{\bar{G}}(x)$ is connected. The same conclusion holds if τ is a graph automorphism since A and A^{-t} are conjugate whenever $A \in \mathrm{GL}_n(K)$ is unipotent. If x is a semisimple involution then inspection of Table 3.8 reveals that $|x^{\bar{G}_\sigma}|$ uniquely determines the $\bar{G}_\sigma$-class of x and thus $x^G = x^{\bar{G}_\sigma}$ as claimed. Now assume G_0 is symplectic and let $\tau \in G$ be a field automorphism of order l. Without loss we may assume $\sigma = \sigma_p^f$ and $\tau = \sigma_p^{f/l}$, so $\bar{G}_\tau \leqslant \bar{G}_\sigma$. If x is a semisimple involution then the previous argument applies so let us assume $r = p$. As before, x and x^τ have the same Jordan decomposition on $\bar{V} = V \otimes K$ and the result follows from Proposition 3.22 in the case $p = 2$. Now assume $p > 2$. We claim that the map $y^{\bar{G}_\tau} \mapsto y^{\bar{G}_\sigma}$ induces a bijection between the set of $\bar{G}_\tau$-classes of elements of order p in $\bar{G}_\tau$ and the set of $\bar{G}_\sigma$-classes of order p elements in $\bar{G}_\sigma$ (so in particular, every unipotent class in $\bar{G}_\sigma$ is defined over the prime field). To see this, fix an element $y \in \bar{G}_\tau$ of order p, set $E = C_{\bar{G}}(y)$ and define bijections

$$\psi_1 : \{\bar{G}_\tau\text{-classes in } y^{\bar{G}} \cap \bar{G}_\tau\} \to H^1(\tau, E/E^0), \quad \psi_2 : \{\bar{G}_\sigma\text{-classes in } y^{\bar{G}} \cap \bar{G}_\sigma\} \to H^1(\sigma, E/E^0)$$

(see Proposition 3.6). Since $|H^1(\tau, E/E^0)| = |H^1(\sigma, E/E^0)| = |E : E^0|$, the map

$$\varphi : \ H^1(\tau, E/E^0) \to H^1(\sigma, E/E^0), \quad \psi_1((y^z)^{\bar{G}_\tau}) \mapsto \psi_2((y^z)^{\bar{G}_\sigma})$$

is a bijection and hence the composition $\psi_2^{-1}\varphi\psi_1$ is also a bijection and the claim follows. Therefore $(x^\tau)^{\bar{G}_\sigma} \cap \bar{G}_\tau$ is non-empty and so there exists an element $z \in \bar{G}_\sigma$ such that $z^{-1}x^\tau z \in \bar{G}_\tau$. Since $\bar{G}_\tau \leqslant \bar{G}_{\tau^{l-1}}$ and $\tau^l = \sigma$ we have

$$z^{-1}x^\tau z = (z^{-1}x^\tau z)^{\tau^{l-1}} = (z^{-1})^{\tau^{l-1}} x^\sigma z^{\tau^{l-1}} = (z^{\tau^{l-1}})^{-1} x z^{\tau^{l-1}}$$

and we conclude that x and x^τ are $\bar{G}_\sigma$-conjugate.

Finally, suppose $G_0 = \mathrm{P\Omega}_n^\epsilon(q)$. Let us start by assuming x has order $r = p > 2$. Now, if the associated partition λ of x has no odd parts then $\epsilon = +$ (see Remark 3.19) and there are precisely two distinct $\bar{G}$-classes corresponding to λ, with representatives $x_1 = x$ and x_2 say, which fuse in $\mathrm{PO}_n(K)$. Since $C_{\bar{G}}(x_i)$ is connected (see [8, p.399]) we have $(x_i^{\bar{G}})_\sigma = x_i^{\bar{G}_\sigma}$ and thus $x^G = x_1^{\bar{G}_\sigma} \cup x_2^{\bar{G}_\sigma}$ since x and x^g have the same Jordan form on $\bar{V}$ for all $g \in G$. Because x_1 and x_2 are conjugate in $\mathrm{PO}_n(K)$, there exists a reflection $\tau \in G$ such that $x_2 = x_1^\tau$. We claim that this is the only case for which $x^G \neq x^{\bar{G}_\sigma}$. To see this, recall that a unipotent $\bar{G}$-class is uniquely determined by its associated partition λ if and only if λ has one or more odd parts.

Consequently, if λ has odd parts and $\epsilon \neq -$ then x and x^τ are $\bar{G}_\sigma$-conjugate for all $\tau \in \mathrm{PGL}(V)$. Further, if τ is a field automorphism then our earlier argument applies and the same conclusion holds. Now assume $\bar{G}_\sigma$ has socle $G_0 = \mathrm{P}\Omega_n^-(q)$, so $\bar{G}_\sigma \leqslant \bar{G}_{\sigma^2}$ and $\bar{G}_{\sigma^2}$ has socle $\mathrm{P}\Omega_n^+(q^2)$. Let $y \in \bar{G}_\sigma$ be an element of order p. Repeating our earlier argument, we find that the natural map $y^{\bar{G}_\sigma} \mapsto y^{\bar{G}_{\sigma^2}}$ of conjugacy classes extends to an injection ι from the set of $\bar{G}_\sigma$-classes of elements of order p in $\bar{G}_\sigma$ to the corresponding set of $\bar{G}_{\sigma^2}$-classes in $\bar{G}_{\sigma^2}$. Any $\tau \in \mathrm{Aut}(G_0)$ is the restriction of an automorphism of $\mathrm{P}\Omega_n^+(q^2)$ and therefore our earlier work implies that x and x^τ are $\bar{G}_{\sigma^2}$-conjugate and thus $\bar{G}_\sigma$-conjugate since ι is injective. Finally, let us assume x is an involution. If $p = 2$ then the result follows from [2, 8.12]; the case $p \neq 2$ is entirely straightforward and is left to the reader. $\square$

Proposition 3.52. *Let $\bar{G} = \mathrm{Sp}_4(K)$, where K is the algebraic closure of $\mathbb{F}_q$ and $q = 2^f$ with $f = 2m+1$. Let σ be a Frobenius morphism of $\bar{G}$ such that $\bar{G}_\sigma = \mathrm{Sp}_4(q)$, let $x \in \bar{G}_\sigma$ be an element of prime order r and let $\tau \in \mathrm{Aut}(G_0)$ be an involutory graph-field automorphism. If x and x^τ are $\bar{G}_\sigma$-conjugate then one of the following holds:*

(i) $r = 2$ and x is $\bar{G}_\sigma$-conjugate to c_2;

(ii) $r \geqslant 5$ and $\mathcal{E}_x = \{\omega, \omega^{-1}, \omega^{2\theta+\epsilon}, \omega^{-2\theta-\epsilon}\}$ for $\epsilon = \pm 1$, where $\omega \in K$ is a primitive r^{th} root of unity and $\theta : \mathbb{F}_q \to \mathbb{F}_q$ is the field automorphism $\mu \mapsto \mu^{2^m}$.

Proof. Let $\Pi = \{a, b\}$ be a set of simple roots which generate a root system Φ of type B_2, where a is short and b is long. Then $\Phi = \{\pm a, \pm b, \pm(a+b), \pm(2a+b)\}$ is the full root system, where $\pm\, b$ and $\pm\,(2a+b)$ are long roots, and $\bar{G}_\sigma$ is generated by the corresponding root elements $\{x_\alpha(t) : \ \alpha \in \Phi, \ t \in \mathbb{F}_q\}$. As described in [7, §12.3], there is a bijection ρ of Φ which interchanges long and short roots; we may assume that $a^\rho = b$ and $(a+b)^\rho = 2a+b$. It is also well-known that the bijection $\varphi : \bar{G}_\sigma \to \bar{G}_\sigma$ defined by

$$\varphi : x_\alpha(t) \mapsto x_{\alpha^\rho}(t^{\lambda(\alpha^\rho)}) \tag{16}$$

extends to a graph-field automorphism φ of $\bar{G}_\sigma$, where $\lambda(\beta) = 2$ if β is a long root, otherwise $\lambda(\beta) = 1$. We note that $\varphi^2 = \phi$ is the field automorphism induced from the map $\mathbb{F}_q \to \mathbb{F}_q$ which sends μ to μ^2. In particular, $\phi^m\varphi$ is an involutory graph-field automorphism and in view of Proposition 3.43(i) we may assume that $\tau = \phi^m\varphi$.

Next we identify the root subgroups $X_\alpha = \{x_\alpha(t) : \ t \in \mathbb{F}_q\}$ for each positive root $\alpha \in \Phi^+$. Fix a standard symplectic basis $\{e_1, e_2, f_2, f_1\}$ of V, where $(e_i, e_j) = (f_i, f_j) = 0$ and $(e_i, f_j) = \delta_{i,j}$ with respect to the non-degenerate $\bar{G}_\sigma$-invariant symmetric bilinear form $(\ ,\ )$ on V. For $t \in \mathbb{F}_q$ define

$$x_a(t) = I_4 + E_{21}(t) + E_{43}(t), \ \ x_b(t) = I_4 + E_{32}(t),$$
$$x_{a+b}(t) = I_4 + E_{31}(t) + E_{42}(t), \ \ x_{2a+b}(t) = I_4 + E_{41}(t)$$

where $(E_{ij}(t))_{kl} = t\delta_{i,k}\delta_{j,l}$ with respect to this specific ordered basis. Evidently, representatives for the three classes of involutions in $\bar{G}_\sigma$ can be chosen by setting

$$a_2 = x_a(1), \ \ b_1 = x_b(1), \ \ c_2 = x_a(1)x_b(1)$$

and (i) follows since (16) implies that τ maps a_2 to b_1 and fixes the $\bar{G}_\sigma$-class of c_2.

Now consider (ii). For each $\alpha \in \Phi$ and $t \in K^*$ define

$$h_\alpha(t) = x_\alpha(t)x_{-\alpha}(t^{-1})x_\alpha(t)x_\alpha(1)x_{-\alpha}(1)x_\alpha(1) \in \bar{G},$$

where $x_\alpha(t)$ for $t \in K^*$ is represented in the obvious way. Then

$$\{h_a(t), h_b(t), h_{a+b}(t), h_{2a+b}(t)\} = \{[t^{-1}, t, t^{-1}, t], \ [1, t^{-1}, t, 1], \ [t^{-1}, t^{-1}, t, t], \ [t^{-1}, 1, 1, t]\},$$

where the diagonal matrices are written with respect to the basis ordering $\{e_1, e_2, f_2, f_1\}$, and any $x \in \bar{G}$ of odd order is $\bar{G}$-conjugate to an element in $\langle h_a(s), h_b(t) : \ s, t \in K\rangle$. Furthermore, the proof of [7, 12.3.3] gives

$$\tau : h_\alpha(t) \mapsto h_{\alpha^\rho}(t^{\theta\lambda(\alpha^\rho)}), \tag{17}$$

where ρ and λ are defined as before and $\theta = \phi^m$. Now if $\nu(x) = 2$ then x is $\bar{G}$-conjugate to $h_a(t)$ or $h_b(t)$ for some $t \in K^* - 1$ and therefore (17) implies that x and x^τ belong to distinct $\bar{G}$-classes, and hence distinct $\bar{G}_\sigma$-classes. Now assume $\nu(x) = 3$, say

$$x = \mathrm{diag}[\lambda^{-1}, \mu^{-1}, \mu, \lambda] = h_a(\lambda)h_b(\lambda)h_b(\mu)$$

(up to $\bar{G}$-conjugacy) where λ and μ are primitive r^{th} roots of unity. Then $r \geqslant 5$ and (17) implies that x^τ is $\bar{G}$-conjugate to $\mathrm{diag}[\lambda^{-\theta}\mu^{-\theta}, \lambda^{-\theta}\mu^{\theta}, \lambda^{\theta}\mu^{-\theta}, \lambda^{\theta}\mu^{\theta}]$ and we easily deduce that x and x^τ are $\bar{G}$-conjugate (and hence $\bar{G}_\sigma$-conjugate) if and only if $\mu^{2\theta+\epsilon} \in \{\lambda, \lambda^{-1}\}$ for some $\epsilon = \pm 1$. $\square$

3.6 Some further remarks on orthogonal groups

Let us assume $\bar{G} = \mathrm{PSO}_n(K)$ and $\bar{G}_\sigma$ has socle $G_0 = \mathrm{P}\Omega_n^\epsilon(q)$, where n is even. For the proof of Theorem 1 we require results analogous to Propositions 3.22, 3.24, 3.36 and 3.40 for the group $\widetilde{G} = \mathrm{PGO}_n^\epsilon(q) = \bar{G}_\sigma.\langle\gamma\rangle$, where γ is an involutory graph automorphism of G_0. In the statement of the next proposition, the functions F and G are defined as in Corollary 3.38.

Proposition 3.53. *If $x \in \widetilde{G}$ has prime order and $\nu(x) = s$ then $F(n,s,q) < |x^{\widetilde{G}}| < 2.G(n,s,q)$. Also, if r is prime then*

$$k_{s,p,u}(\widetilde{G}) \leqslant p^{\frac{s}{2}}, \quad k_{s,r,s}(\widetilde{G}) \leqslant \begin{cases} q^{\frac{1}{2}s} & \text{if } s < n/2 \\ q^{\frac{1}{2}(s+1)} & \text{otherwise.} \end{cases}$$

Proof. If $x \in \bar{G}_\sigma$ then Corollary 3.38 gives

$$F(n,s,q) < |x^{\bar{G}_\sigma}| \leqslant |x^{\widetilde{G}}| \leqslant 2|x^{\bar{G}_\sigma}| < 2.G(n,s,q)$$

so we may as well assume $x \in \widetilde{G} - \bar{G}_\sigma$ is an involution and thus $s \leqslant n/2$ is odd. If q is even then x is $\widetilde{G}$-conjugate to b_s and the proof of Proposition 3.22 gives $\frac{1}{2}q^{s(n-s)} < |x^{\widetilde{G}}| < 2q^{s(n-s)}$. On the other hand, if q is odd and $s < n/2$ then

$$\frac{1}{2}q^{s(n-s)} < |x^{\widetilde{G}}| = \frac{|\mathrm{SO}_n^\epsilon(q)|}{|\mathrm{SO}_s(q)||\mathrm{SO}_{n-s}(q)|} < 2q^{s(n-s)}$$

and there is a unique $\widetilde{G}$-class for each such s. If $s = n/2$ is odd then there are precisely two distinct $\widetilde{G}$-classes, with representatives y and z where

$$\frac{1}{4}q^{\frac{1}{4}n^2} < |y^{\widetilde{G}}| = \frac{|\mathrm{SO}_n^\epsilon(q)|}{|\mathrm{SO}_{n/2}(q)|^2 2} < 2q^{\frac{1}{4}n^2}, \quad \frac{1}{4}q^{\frac{1}{4}n^2} < |z^{\widetilde{G}}| = \frac{|\mathrm{SO}_n^\epsilon(q)|}{|\mathrm{SO}_{n/2}(q^2)|2} < q^{\frac{1}{4}n^2}.$$

Finally, let r be a prime. If s is even or r is odd then $k_{s,r,\alpha}(\widetilde{G}) \leqslant k_{s,r,\alpha}(\bar{G}_\sigma)$ for $\alpha \in \{s,u\}$ and the result follows from Propositions 3.24 and 3.40. On the other hand, if $s \leqslant n/2$ is odd and $r = 2$ then as above we have $k_{s,2,n/2}(\widetilde{G}) = 2$ if $s = n/2$, otherwise $k_{s,2,\alpha}(\widetilde{G}) = 1$. $\square$

Remark 3.54. We also require similar results for the (non-almost simple) group $\widetilde{G} = \mathrm{PGO}_4^+(q)$. Here $s = 2$ or 3 and the reader can check that the conclusion to Proposition 3.53 holds for $\widetilde{G}$.

For the remainder we shall assume $G_0 = \mathrm{P}\Omega_8^+(q)$. Here the corresponding Dynkin diagram D_4 admits a rotational symmetry of order three, giving rise to the triality automorphisms we introduced in Definition 3.47. As remarked in §3.1, Aschbacher's main theorem excluded the case $G_0 = \mathrm{P}\Omega_8^+(q)$ with G containing triality automorphisms; an extension to these groups was obtained later by Kleidman [17].

If $G_0 = \mathrm{P}\Omega_8^+(q)$ and G contains a triality automorphism then Proposition 3.51 fails to hold. This underlines the fact that this special case needs to be treated separately in our subsequent analysis. In Proposition 3.55 below we describe how a triality graph automorphism acts on the conjugacy classes of elements of prime order in $\mathrm{Inndiag}(G_0)$.

As before, let K denote the algebraic closure of $\mathbb{F}_q$, where $q = p^f$ for some prime p. Let $\bar{G} = \mathrm{PSO}_8(K)$ and let σ be a Frobenius morphism of $\bar{G}$ such that $\bar{G}_\sigma$ has socle $G_0 = \mathrm{P\Omega}_8^+(q)$. As previously described, we can uniquely associate a partition λ to each unipotent $\bar{G}_\sigma$-class; if p is odd then this correspondence is 1-1 unless $\lambda \in \{(4^2), (3^2, 1^2), (2^4)\}$ in which case λ corresponds to precisely two distinct $\bar{G}_\sigma$-classes, with representatives λ and λ' say. For semisimple involutions we label $\bar{G}_\sigma$-class representatives as follows (see Table 3.8):

type of $\bar{G}_\sigma$-centralizer	$\bar{G}_\sigma$-class representatives
$\mathrm{O}_4^-(q)^2$	y_1
$\mathrm{O}_4^+(q^2)$	$y_2,\ y_3$
$\mathrm{GL}_4^\epsilon(q)$	$z_1^\epsilon,\ z_2^\epsilon$
$\mathrm{O}_6^\epsilon(q) \times \mathrm{O}_2^\epsilon(q)$	z_3^ϵ

Proposition 3.55. *With the notation established, let $x \in \bar{G}_\sigma$ be an element of prime order r and fix a triality graph automorphism $\tau \in \mathrm{Aut}(G_0)$. Then the following hold.*

(i) If $r = p > 2$ then τ permutes the class representatives in the sets $\{(2^4), (2^4)', (3, 1^5)\}$ and $\{(4^2), (4^2)', (5, 1^3)\}$ and fixes all others.

(ii) If $r = p = 2$ then τ permutes the $\bar{G}_\sigma$-class representatives $\{c_2, a_4, a_4'\}$ and fixes all others.

(iii) If $r = 2$ and p is odd then τ permutes the $\bar{G}_\sigma$-class representatives $\{y_1, y_2, y_3\}$, $\{z_1^\epsilon, z_2^\epsilon, z_3^\epsilon\}$ and fixes the remaining class.

(iv) If $r \neq p$ is odd and $\mathcal{E}_x = \{\mu_i^\pm : 1 \leqslant i \leqslant 4\}$ then

$$\mathcal{E}_{x^\tau} = \frac{1}{\alpha_\zeta}\{\mu_1^\zeta\mu_2, \mu_1^\zeta\mu_3, \mu_1^\zeta\mu_4, \mu_2\mu_3, \mu_2\mu_4, \mu_3\mu_4, 1, \alpha_\zeta^2\},$$

where $\alpha_\zeta^2 = \mu_1^\zeta\mu_2\mu_3\mu_4$ and $\zeta = \pm$ is a choice of sign.

Proof. Part (iv) follows from [18, p.196]. (There is a choice of sign since $\mathcal{E}_{x^{\tau^{-1}}} = \mathcal{E}_{x^{\gamma\tau}}$, where $\gamma \in \mathrm{Aut}(G_0)$ is an involutory graph automorphism.) Now consider parts (i), (ii) and (iii). Inspecting $\bar{G}_\sigma$-class sizes, it is clear that the only classes which could possibly be cyclically permuted by τ are precisely the classes which we claim are indeed permuted. To justify this claim we appeal to [17, Table I]. For example, suppose $r = p > 2$ and x has associated partition $\lambda = (2^4)$. According to [17, Table I] we may assume without loss that x lies in a $\mathscr{C}_4$-subgroup H_1 of type $\mathrm{Sp}_4(q) \otimes \mathrm{Sp}_2(q)$ with the property that H_1^τ is a $\mathscr{C}_1$-subgroup of type $\mathrm{O}_5(q) \times \mathrm{O}_3(q)$. Clearly there are no unipotent elements in H_1^τ with associated partition (2^4) and we conclude that τ does indeed cyclically permute the $\bar{G}_\sigma$-class representatives in the set $\{(2^4), (2^4)', (3, 1^5)\}$. Similarly, if $r = p = 2$ and x is a c_2-involution then x lies in a $\mathscr{C}_1$-subgroup K_1 of type $\mathrm{O}_6^+(q) \times \mathrm{O}_2^+(q)$ and K_1^τ is a $\mathscr{C}_2$-subgroup of type $\mathrm{GL}_4(q)$. The result follows since there are no c_2-type involutions in K_1^τ. We leave the remaining cases to the reader. □

Remark 3.56. Let $x \in \bar{G}_\sigma$ be a semisimple element of odd prime order. Then part (iv) of Proposition 3.55 implies that $\mathcal{E}_{x^\tau} = \mathcal{E}_{x^{\tau^{-1}}}$ if and only if $1 \in \mathcal{E}_x$. Further, if $1 \in \mathcal{E}_x$ then either x and x^τ are $\bar{G}_\sigma$-conjugate or $1 \notin \mathcal{E}_{x^\tau}$.

Remark 3.57. There are exactly six distinct $\bar{G}_\sigma$-classes of involutory graph automorphisms in $\mathrm{Aut}(G_0)$ and a triality graph automorphism permutes these classes with cycle-shape (3^2).

4 Proof of Theorem 1.1: $H \in \mathscr{C}_4$

We begin the proof of Theorem 1.1 by considering the collection $\mathscr{C}_4$. The subgroups here arise from a tensor product decomposition $V = V_1 \otimes V_2$ of the natural module V; the specific cases to be considered are listed in Table 4.1, where $\dim V = n = ab$ (see [18, Tables 3.5.H, 4.4.A]).

	G_0	type of H	conditions
(i)	$\mathrm{PSL}^{\epsilon}_n(q)$	$\mathrm{GL}^{\epsilon}_a(q) \otimes \mathrm{GL}^{\epsilon}_b(q)$	$a > b \geqslant 2$, $(b,q) \neq (2,2)$
(ii)	$\mathrm{PSp}_n(q)$	$\mathrm{Sp}_a(q) \otimes \mathrm{O}^{\epsilon}_b(q)$	a even, q odd, $b \geqslant 3$, $(b,q) \neq (3,3)$
(iii)	$\mathrm{P\Omega}^{+}_n(q)$	$\mathrm{Sp}_a(q) \otimes \mathrm{Sp}_b(q)$	$a > b \geqslant 4$, a,b even
(iv)	$\mathrm{P\Omega}^{+}_n(q)$	$\mathrm{Sp}_a(q) \otimes \mathrm{Sp}_2(q)$	$a \geqslant 4$ even, $q \neq 2$, $(a,p) \neq (4,2)$
(v)	$\Omega_n(q)$	$\mathrm{O}_a(q) \otimes \mathrm{O}_b(q)$	$a > b \geqslant 3$, abq odd
(vi)	$\mathrm{P\Omega}^{+}_n(q)$	$\mathrm{O}^{\epsilon_1}_a(q) \otimes \mathrm{O}^{\epsilon_2}_b(q)$	$a > b \geqslant 4$, a,b even, q odd
(vii)	$\mathrm{P\Omega}^{\epsilon}_n(q)$	$\mathrm{O}^{\epsilon}_a(q) \otimes \mathrm{O}_b(q)$	bq odd, $a \geqslant 4$ even, $b \geqslant 3$

Table 4.1: The collection $\mathscr{C}_4$

Proposition 4.1. *The conclusion to Theorem 1.1 holds in case (i) of Table 4.1.*

Proof. Let σ be a Frobenius morphism of $\bar{G} = \mathrm{PSL}_n(K)$ such that $\bar{G}_\sigma = \mathrm{PGL}^{\epsilon}_n(q)$. Observe that $H \cap \mathrm{PGL}(V) \leqslant \mathrm{PGL}^{\epsilon}_a(q) \times \mathrm{PGL}^{\epsilon}_b(q) = \widetilde{H}$.

Case 1. $x \in H \cap \mathrm{PGL}(V)$
Let $x \in H \cap \mathrm{PGL}(V)$ be an element of prime order r such that $\nu(x) = s$ (with respect to V) and note that

$$|x^G \cap H| \leqslant |H \cap \mathrm{PGL}(V)| < q^{a^2+b^2-2}. \tag{18}$$

If $s > n/2$ and $C_{\bar{G}}(x)$ is connected then Corollary 3.38 implies that

$$|x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^n q^{\frac{1}{2}(n^2+2n-2)}$$

and thus (18) gives $f(x,H) < 1/2 + 1/n$ as required (see (2)). Similarly, if $s > n/2$ and $C_{\bar{G}}(x)$ is non-connected then r is odd and again (18) is sufficient since

$$|x^G| > \frac{1}{2r}\left(\frac{q}{q+1}\right)^r q^{n^2(1-\frac{1}{r})}.$$

Now assume $s = n/2$. Here $C_{\bar{G}}(x)$ is non-connected if and only if $r = 2$ and $p > 2$, whence Corollary 3.38 gives $|x^G| > \frac{1}{4}(q+1)^{-1}q^{\frac{1}{2}n^2+1}$ and (18) is sufficient unless $(n,a,q) = (6,3,3)$. (Note that Lemma 3.20(i) implies that $|x^{G_0}| \geqslant \frac{1}{2}|x^{\bar{G}_\sigma}|$ if $r = p$.) In this case the desired result quickly follows through direct calculation. For example, if $\epsilon = +$ then Lagrange's Theorem implies that $r \in \{2,3,13\}$ and the hypothesis $s = 3$ rules out $r = 13$. If $(r,\epsilon) = (2,+)$ then we calculate that $f(x,H) < .374$ since

$$|x^G \cap H| \leqslant \left(\frac{|\mathrm{GL}_3(3)|}{|\mathrm{GL}_2(3)||\mathrm{GL}_1(3)|}+1\right)\left(\frac{|\mathrm{GL}_2(3)|}{|\mathrm{GL}_1(3)|^2 2}+\frac{|\mathrm{GL}_2(3)|}{|\mathrm{GL}_1(3^2)|2}\right),\ \ |x^G| \geqslant \frac{|\mathrm{GL}_6(3)|}{|\mathrm{GL}_3(3^2)|2}.$$

The other cases are similar.

Now assume $s < n/2$. Following the proof of [20, 4.3], write $x = (x_1, x_2)$ and define $s_i = \nu(x_i)$ with respect to the obvious natural modules. Then [20, 3.7] states that

$$s \geqslant \max(as_2, bs_1) \tag{19}$$

and thus $s_1 < a/2$ and $s_2 < b/2$. Furthermore, Lemma 3.40 yields

$$k_{s,r,s}(\widetilde{H}) \leqslant \sum_{s_1=0}^{\lfloor s/b \rfloor} q^{s_1}. \sum_{s_2=0}^{\lfloor s/a \rfloor} q^{s_2} < \left(\frac{q}{q-1}\right)^2 q^{\frac{s}{a}+\frac{s}{b}}$$

and if we assume x is semisimple then Corollary 3.38 implies that

$$|x^G \cap H| < k_{s,r,s}(\widetilde{H}).4\left(\frac{q}{q-1}\right)^{\frac{s}{a}+\frac{s}{b}} \max_{s_1 \leqslant \lfloor s/b \rfloor,\, s_2 \leqslant \lfloor s/a \rfloor}\{q^{2as_1-s_1^2-s_1+2bs_2-s_2^2-s_2}\}.$$

The maximum is realized when s_1 and s_2 are as large as possible, whence

$$|x^G \cap H| < 4\left(\frac{q}{q-1}\right)^{2+\frac{s}{a}+\frac{s}{b}} q^{\frac{2as}{b}-\frac{s^2}{b^2}+\frac{2bs}{a}-\frac{s^2}{a^2}}$$

and it is clear that this upper bound also holds if x is unipotent (see Lemma 3.24 and Corollary 3.38). The hypothesis $s < n/2$ implies that $|x^{\bar{G}_\sigma}| = |x^{G_0}|$, so Corollary 3.38 gives $|x^G| > \frac{1}{2}(q+1)^{-1}q^{2s(n-s)+1}$ and the result follows since $2 \leqslant s \leqslant \frac{1}{2}(n-1)$.

Case 2. $x \in H - \mathrm{PGL}(V)$
First assume x is a field automorphism of prime order r. Then $q = q_0^r$, $(\epsilon, r) \neq (-, 2)$ (see Remark 3.42) and Lemma 3.48 gives

$$|x^G| > \frac{1}{2}(q+1)^{-1}q^{(n^2-1)(1-\frac{1}{r})}. \tag{20}$$

Now Lemma 3.50 states that $x^G \cap H \subseteq \widetilde{H}x$, where x induces field automorphisms on both direct factors of $\widetilde{H}$, whence Proposition 3.43 implies that

$$|x^G \cap H| \leqslant |x^{\mathrm{PGL}_a^\epsilon(q)}||x^{\mathrm{PGL}_b^\epsilon(q)}| < 4q^{(a^2+b^2-2)\left(1-\frac{1}{r}\right)}$$

and the desired result follows. The argument for an involutory graph-field automorphism is very similar. Finally, if x is an involutory graph automorphism then $|x^G| > \frac{1}{2}(q+1)^{-1}q^{\frac{1}{2}(n^2-n-2)}$ and applying Lemma 3.14 we deduce that

$$|x^G \cap H| \leqslant i_2(\mathrm{Aut}(\mathrm{PSL}_a^\epsilon(q))).i_2(\mathrm{Aut}(\mathrm{PSL}_b^\epsilon(q))) < 4(1+q^{-1})^2 q^{\frac{1}{2}(a^2+a+b^2+b-4)}.$$

These bounds are sufficient unless $(n, a) = (6, 3)$ and $q \in \{3, 4\}$. Here $f(x, H) < .591$ since $|x^G| \geqslant |\mathrm{PSL}_6^\epsilon(q)|/|\mathrm{Sp}_6(q)|$ and $i_2(\mathrm{Aut}(\mathrm{PSL}_m^\epsilon(q)))$ takes the following values:

m	$(q,\epsilon) = (3,+)$	$(3,-)$	$(4,+)$	$(4,-)$
3	351	315	1963	1235
2	9	9	25	25

□

Proposition 4.2. *The conclusion to Theorem 1.1 holds in case (iv) of Table 4.1.*

Proof. Set $\bar{G} = \mathrm{PSO}_{2a}(K)$, $\bar{H} = \mathrm{PSp}_a(K) \times \mathrm{PSp}_2(K)$ and let σ be a Frobenius morphism of $\bar{G}$ such that $\bar{G}_\sigma$ has socle $G_0 = \mathrm{P}\Omega_n^+(q)$, where $n = 2a$. If $a = 4$ then we may assume p is odd (see Table 4.1) and G does not contain any triality automorphisms (see Proposition 3.3). Observe that

$$H \cap \mathrm{PGL}(V) \leqslant \mathrm{PGSp}_a(q) \times \mathrm{PGSp}_2(q) = \widetilde{H}.$$

Now, if $x \in H - \mathrm{PGL}(V)$ has prime order r then $q = q_0^r$ and the bounds

$$|x^G \cap H| \leqslant |x^{\mathrm{PGSp}_a(q)}||x^{\mathrm{PGSp}_2(q)}| < 4q^{\left(\frac{1}{2}(a^2+a)+3\right)\left(1-\frac{1}{r}\right)}, \quad |x^G| > \frac{1}{4}q^{(2a^2-a)\left(1-\frac{1}{r}\right)}$$

are always sufficient. For the remainder, let us assume $x \in H \cap \mathrm{PGL}(V)$ has prime order r. Write $x = (x_1, x_2)$ and define s, s_1 and s_2 as before, so (19) reads $s \geqslant \max(2s_1, as_2)$.

Case 1. $s < a$
Since $s \geqslant \max(2s_1, as_2)$, the hypothesis $s < a$ implies that $x_2 = I_2$, whence $s = 2s_1$ and $x \in \bar{G}_\sigma$. Let us start by assuming x is semisimple. Then $2 \leqslant s_1 < a/2$ and thus $s \geqslant 4$ and $a \geqslant 6$. Applying Corollary 3.38 and Proposition 3.51 we deduce that

$$|x^G \cap H| \leqslant \log_2 q.|x_1^{\mathrm{PGSp}_a(q)}| < \log_2 q.2\left(\frac{q}{q-1}\right)^{\frac{s}{4}} q^{\frac{as}{2}-\frac{s^2}{8}+\frac{1}{2}}, \quad |x^G| > \frac{1}{4}\left(\frac{q}{q+1}\right)q^{s(2a-s-1)}$$

and the desired result follows.

Next assume $r = p > 2$. Let $\lambda' = (a^{m_a}, \ldots, 1^{m_1}) \vdash a$ denote the associated partition of $x_1 \in \mathrm{PSp}_a(K)$ and observe that the Jordan form of $x = x_1 \otimes I_2$ on V is described by the partition $\lambda = (a^{2m_a}, \ldots, 1^{2m_1}) \vdash 2a$. Therefore $x^{\bar{G}} \cap \bar{H} = x^{\bar{H}}$ and [6, 2.3] implies that

$$\dim x^{\bar{H}} = \frac{1}{4}\dim x^{\bar{G}} + \frac{3}{4}(a - \sum_{j \text{ odd}} m_j)$$

since p is odd. If t denotes the number of non-zero terms m_j in λ then the hypothesis $s < a$ implies that $t \geqslant 2$ and applying Lemma 3.18 and Corollary 3.21 we deduce that

$$|x^G \cap H| < 2^t q^{\frac{1}{4}(\dim x^{\bar{G}}+3a)}, \;\; |x^G| > \left(\frac{1}{2}\right)^{t+1}\left(\frac{q}{q+1}\right)^t q^{\dim x^{\bar{G}}}, \tag{21}$$

where $a \geqslant \max(4, \frac{1}{2}t(t+1))$. Now [6, 2.3, 2.4] imply that

$$\dim x^{\bar{G}} \geqslant 2at(t-1) - \frac{1}{2}t^4 + \frac{1}{3}t^3 - \frac{1}{3}t$$

and thus (21) is sufficient if $t \geqslant 3$. Now assume $t = 2$. If $\lambda' = (2, 1^{a-2})$ (which must be the case if $a = 4$) then $|x^G \cap H| \leqslant q^a - 1$, $|x^G| > \frac{1}{8}q^{4a-6}$ and the result follows. If not, then $\dim x^{\bar{G}} \geqslant 8a - 20$ (minimal if $\lambda' = (2^2, 1^{a-4})$) and the bounds in (21) are sufficient for all $a \geqslant 6$ and $q \geqslant 3$.

Finally, let us assume $r = p = 2$. Here it is easy to see that the $\mathrm{Sp}_a(q)$-class of x_1 and the $\mathrm{Sp}_2(q)$-class of x_2 determine the $\mathrm{O}_n^+(q)$-class of x as follows:

	$x_2 = I_2$	b_1
$x_1 = I_a$	I_{2a}	a_a
a_l	a_{2l}	a_a
b_l, c_l	a_{2l}	c_a

(22)

For instance, if $x_2 = b_1$ then x is $\mathrm{O}_n^+(q)$-conjugate to either a_a or c_a since $J_2 \otimes J_2 = I_2 \otimes J_2 = [J_2^2]$ (up to conjugacy). If $v = v_1 \otimes v_2 \in V$ then

$$(vx, v) = (v_1x_1, v_1)_1(v_2x_2, v_2)_2,$$

where $(\,,\,)$, $(\,,\,)_1$ and $(\,,\,)_2$ denote the relevant non-degenerate symmetric bilinear forms on V, V_1 and V_2 respectively. By definition, if x_1 is an a-type involution then $(v_1x_1, v_1)_1 = 0$ for all $v_1 \in V_1$ and thus $(vx, v) = 0$ for all $v \in V$ and x is also an a-involution. If not, then there exists some $v = v_1 \otimes v_2 \in V$ such that $(v_1x_1, v_1)_1 \neq 0$ and $(v_2x_2, v_2)_2 \neq 0$, so $(vx, v) \neq 0$ and x is a c-type involution. In particular, the hypothesis $s < a$ implies that x is $\bar{G}$-conjugate to a_s and Proposition 3.22 yields

$$|x^G \cap H| < 2bq^{\frac{1}{4}s(2a-s)} + 2q^{\frac{1}{4}s(2a-s+2)}, \;\; |x^G| > \frac{1}{2}q^{s(2a-s-1)}$$

where $b = 1$ if $s \equiv 0\,(4)$, otherwise $b = 0$. These bounds are always sufficient.

Case 2. $s \geqslant a$, $r = 2$

Here $s = a$ and we start by assuming $p = 2$, so $a \geqslant 6$ (see Table 4.1). If x is an a-type involution then (22) implies that

$$|x^G \cap H| \leqslant \sum_{j=0}^{\lfloor a/4 \rfloor} |(a_{2j} \otimes b_1)^{\widetilde{H}}| + \begin{cases} |(a_{\frac{a}{2}} \otimes I_2)^{\widetilde{H}}| + |(c_{\frac{a}{2}} \otimes I_2)^{\widetilde{H}}| & \text{if } a \equiv 0\,(4) \\ |(b_{\frac{a}{2}} \otimes I_2)^{\widetilde{H}}| & \text{if } a \equiv 2\,(4), \end{cases}$$

where we set $a_0 = I_a$. Using Proposition 3.22 we deduce that

$$|x^G \cap H| < 2(q^2-1)^{-1}q^{\frac{1}{4}a^2+4} + 2q^{\frac{1}{4}a^2+\frac{1}{2}a}(1 + q^{-\frac{1}{2}a}) < 4q^{\frac{1}{4}a^2+\frac{1}{2}a}$$

and the result follows since $|x^G| > \frac{1}{2}q^{a(a-1)}$. Similarly, if x is $\bar{G}$-conjugate to c_a then $|x^G| > \frac{1}{2}q^{a^2}$ and Proposition 3.22 gives

$$|x^G \cap H| \leqslant \sum_{j=1}^{\lfloor a/4 \rfloor} |(c_{2j} \otimes b_1)^{\widetilde{H}}| + \sum_{j=0}^{\lfloor a/4-1/2 \rfloor} |(b_{2j+1} \otimes b_1)^{\widetilde{H}}| < 2(q^2-1)^{-1}q^{\frac{1}{4}(a^2+2a+16)}.$$

Again, one can check that these bounds are always sufficient.

Now assume p is odd. If x is conjugate to $[-I_a, I_a]$ then $|x^G| > \frac{1}{8}q^{a^2}$ and $x^{\bar{G}} \cap \bar{H}$ is a union of at most two distinct $\bar{H}$-classes. The result follows since Proposition 3.37 implies that $|x^G \cap H| < 2q^{a^2/4+a/2+2} + 2bq^{a^2/4}$ where $b=1$ if $a \equiv 0\,(4)$, otherwise $b=0$. On the other hand, if $C_{\bar{G}}(x)$ is of type GL_a then $x^{\bar{G}} \cap \bar{H}$ is a union of precisely $\lfloor a/4 \rfloor + 2$ distinct $\bar{H}$-classes, with representatives

$$z_0 = [-iI_{a/2}, iI_{a/2}] \otimes I_2, \;\; z_j = [-I_{2j}, I_{a-2j}] \otimes [-i, i], \;\; 0 \leqslant j \leqslant a/4,$$

where $i \in K$ satisfies $i^2 = -1$. Using Proposition 3.37 we deduce that

$$|x^G \cap H| < 2q^{\frac{1}{4}(a^2+2a)} + \sum_{j=0}^{\lfloor a/4 \rfloor} 4q^{2aj-4j^2+2} < 2q^{\frac{1}{4}a^2}(q^{\frac{1}{2}a} + 2(q^2-1)^{-1}q^4)$$

and $|x^G| > \frac{1}{4}(q+1)^{-1}q^{a^2-a+1}$. It remains to deal with the case $a=4$ for $q \leqslant 5$. Here we can calculate directly. For example, if $q=3$ then $|x^G \cap H| \leqslant A + AB + C = 1548$, where

$$A = \frac{|\mathrm{Sp}_2(3)|}{|\mathrm{GL}_1(3)|2} + \frac{|\mathrm{Sp}_2(3)|}{|\mathrm{GU}_1(3)|2}, \; B = \frac{|\mathrm{Sp}_4(3)|}{|\mathrm{Sp}_2(3^2)|2} + \frac{|\mathrm{Sp}_4(3)|}{|\mathrm{Sp}_2(3)|^2 2}, \; C = \frac{|\mathrm{Sp}_4(3)|}{|\mathrm{GL}_2(3)|2} + \frac{|\mathrm{Sp}_4(3)|}{|\mathrm{GU}_2(3)|2}$$

and we conclude that $f(x,H) < .605$ since $|x^G| \geqslant \frac{1}{2}|\mathrm{SO}_8^+(3) : \mathrm{GU}_4(3)| = 189540$.

Case 3. $s \geqslant a$**,** $r = p > 2$
Here $x \in \bar{G}_\sigma$ and s is even. We claim that $x^{\bar{G}} \cap \bar{H}$ is a union of at most two distinct $\bar{H}$-classes. To see this, first observe that up to conjugacy we have $J_i \otimes I_2 = [J_i^2]$ and

$$J_i \otimes J_2 = \begin{cases} [J_{i+1}, J_{i-1}] & \text{if } i < p \\ [J_p^2] & \text{if } i = p. \end{cases} \tag{23}$$

Since p is odd, a unipotent class in $\mathrm{PSp}_a(K)$ is uniquely determined by its associated partition and therefore it is sufficient to show that elements (x_1, x_2), (x_1', x_2) in $\widetilde{H}$ are $\bar{G}$-conjugate only if x_1 and x_1' are $\mathrm{PSp}_a(K)$-conjugate. This is trivial if $x_2 = I_2$ so assume $x_2 = J_2$ and suppose x_1 and x_1' have associated partitions $(p^{a_p}, \ldots, 1^{a_1}) \vdash a$ and $(p^{b_p}, \ldots, 1^{b_1}) \vdash a$ respectively. Then applying (23) we deduce that $x_1 \otimes x_2$ has associated partition λ, where

$$\lambda = (p^{2a_p+a_{p-1}}, (p-1)^{a_{p-2}}, (p-2)^{a_{p-1}+a_{p-3}}, \ldots, 2^{a_3+a_1}, 1^{a_2}) \vdash 2a \tag{24}$$

if $p \geqslant 5$ and $\lambda = (3^{2a_3+a_2}, 2^{a_1}, 1^{a_2}) \vdash 2a$ if $p=3$. Therefore $x_1 \otimes x_2$ and $x_1' \otimes x_2$ are $\bar{G}$-conjugate only if

$$2a_p + a_{p-1} = 2b_p + b_{p-1}, \; a_{p-2} = b_{p-2}, \; a_2 = b_2$$

and

$$a_{p-i+2} + a_{p-i} = b_{p-i+2} + b_{p-i}, \; 3 \leqslant i \leqslant p-1.$$

The claim follows since these equations hold if and only if $a_j = b_j$ for each $1 \leqslant j \leqslant p$.

Suppose $x \in \bar{G}$ has associated partition $\lambda = (p^{m_p}, \ldots, 1^{m_1}) \vdash 2a$, with precisely t non-zero terms m_j. If $y = x_1 \otimes J_2$ is conjugate to x, where x_1 has associated partition $(p^{a_p}, \ldots, 1^{a_1}) \vdash a$, then (24) and [6, 2.3] imply that $|y^G \cap H| < 2^t q^{\dim y^{\bar{H}}}$, where

$$\begin{aligned} \dim y^{\bar{H}} &= \frac{1}{4}\dim x^{\bar{G}} + \frac{3}{4}a + 2 - \frac{1}{4}\left(a_p + \sum_{j=1}^{p-1} a_j^2 + \sum_{j=1}^{p-2} a_j a_{j+1} + \sum_j a_j + \sum_{j \text{ odd}} a_j\right) \\ &\leqslant \frac{1}{4}\dim x^{\bar{G}} + \frac{3}{4}a + \frac{3}{2}. \end{aligned}$$

Applying our earlier work (see (21)) we deduce that

$$|x^G \cap H| < 2^t(1+q^{\frac{3}{2}})q^{\frac{1}{4}(\dim x^{\bar{G}}+3a)}, \quad |x^G| > \left(\frac{1}{2}\right)^{t+1}\left(\frac{q}{q+1}\right)^t q^{\dim x^{\bar{G}}}$$

where $\dim x^{\bar{G}} \geqslant a(a-1)$ (minimal if $t=1$ and $\lambda = (2^a)$). The reader can check that these bounds are sufficient unless $a=4$. Here the possibilities are listed in the following table (the symbol † denotes the additional condition $p \geqslant 5$ which ensures x has prime order).

x	$[J_5, J_3]^\dagger$	$[J_4^2]^\dagger$	$[J_3^2, I_2]$	$[J_3, J_2^2, I_1]$	$[J_2^4]$
$x_1 \otimes x_2$	$[J_4] \otimes [J_2]$	$[J_4] \otimes [I_2]$	$[J_2^2] \otimes [J_2]$	$[J_2, I_2] \otimes [J_2]$	$[J_2^2] \otimes [I_2],\ [I_4] \otimes [J_2]$
$f(x,H) <$	.472	.408	.488	.400	.552

For example, if $x = [J_3^2, I_2]$ and $q=3$ then $f(x,H) < .488$ since

$$|x^G \cap H| \leqslant \frac{|\mathrm{Sp}_4(3)|}{|\mathrm{SO}_2^+(3)|3^3}.\frac{|\mathrm{Sp}_2(3)|}{3} = 7680, \quad |x^G| \geqslant \frac{|\mathrm{O}_8^+(3)|}{|\mathrm{O}_2^-(3)|^2 3^8} = 94348800.$$

The same bound holds for all $q \geqslant 5$ and the other bounds are derived in a similar fashion.

Case 4. $s \geqslant a$**,** $r \neq p$**,** $r > 2$
Let $i \geqslant 1$ be minimal such that $r|(q^i-1)$ and let $\mu = (l, a_1, \ldots, a_t)$ denote the associated σ-tuple of $x \in \bar{G}_\sigma$. Let d be the number of non-zero terms a_j in μ and set $e=2$ if i is odd, otherwise $e=1$. We note that d is even if i is odd and we also observe that

$$|x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^{d(2-e)+1} q^{\dim x^{\bar{G}}}. \tag{25}$$

Let $y = (y_1, y_2)$ be an arbitrary element of $x^G \cap H$. Now, if $i \geqslant 3$ then $y_2 = I_2$ and y_1 has associated σ-tuple $\mu' = (l/2, a_{\rho(1)}/2, \ldots, a_{\rho(t)}/2)$ for some $\rho \in S_t$. Therefore

$$\dim x^{\bar{H}} = \frac{1}{2}a^2 + \frac{1}{2}a - \frac{1}{8}l^2 - \frac{1}{4}l - \frac{i}{4e}\sum_j a_j^2 = \frac{1}{4}\dim x^{\bar{G}} + \frac{3}{4}(a-l) \tag{26}$$

and

$$|x^G \cap H| < \log_2 q.2^{\frac{d}{2}(e-1)}q^{\frac{1}{4}(\dim x^{\bar{G}}+3a)},$$

where $\dim x^{\bar{G}} \geqslant a(a-1)$ (see [6, 2.9]). This bound with (25) is always sufficient.

Now assume $i \leqslant 2$. We claim that if the elements $y_1 \otimes y_2$ and $z_1 \otimes z_2$ in $\widetilde{H}$ are $\mathrm{PO}_{2a}(K)$-conjugate and y_2 is $\mathrm{PSp}_2(K)$-conjugate to z_2 then y_1 and z_1 are $\mathrm{PSp}_a(K)$-conjugate. This is trivial if $y_2 = I_2$ so assume $\mathcal{E}_{y_2} = \{\omega, \omega^{-1}\}$, where $\omega \in K$ is a primitive r^{th} root of unity. Set $\Gamma_0 = \{1,1\}$ and $\Gamma_j = \{\omega^j, \omega^{-j}\}$ for $1 \leqslant j \leqslant t$, where $t = \frac{1}{2}(r-1)$. For any two subsets $A = \{a_1, a_2\}$ and $B = \{b_1, b_2\}$ of K define $A \otimes B = \{a_1b_1, a_1b_2, a_2b_1, a_2b_2\}$ and observe that

$$\Gamma_0 \otimes \Gamma_1 = \Gamma_1 \cup \Gamma_1, \quad \Gamma_t \otimes \Gamma_1 = \Gamma_t \cup \Gamma_{t-1}, \quad \Gamma_j \otimes \Gamma_1 = \Gamma_{j+1} \cup \Gamma_{j-1} \quad 1 \leqslant j \leqslant t-1.$$

If c_j (resp. d_j) denotes the multiplicity of Γ_j in $\mathcal{E}_{y_1}$ (resp. $\mathcal{E}_{z_1}$) then these relations imply that

$$c_1 = d_1, \quad 2c_0 + c_2 = 2d_0 + d_2, \quad c_{t-1} + c_t = d_{t-1} + d_t, \quad c_j + c_{j+2} = d_j + d_{j+2} \quad 1 \leqslant j \leqslant t-2$$

and therefore $c_j = d_j$ for all j. In particular, $\mathcal{E}_{y_1} = \mathcal{E}_{z_1}$ and Lemma 3.39 implies that y_1 and z_1 are $\mathrm{PSp}_a(K)$-conjugate as claimed.

Now, if $y = y_1 \otimes y_2$ is conjugate to x, where $\mathcal{E}_{y_2} = \Gamma_1$ and c_j denotes the multiplicity of Γ_j in $\mathcal{E}_{y_1}$, then the above relations imply that $\dim y^{\bar{H}} \leqslant \frac{1}{4}(\dim x^{\bar{G}} + 3a + 8)$ since

$$\dim y^{\bar{H}} = \frac{1}{4}(\dim x^{\bar{G}} + 3a + 8 - 4c_0 - c_1 - (2c_0 - c_2)^2 - (c_{t-1} - c_t)^2) - \frac{1}{4}\sum_{j=1}^{t-2}(c_j - c_{j+2})^2.$$

Our above work implies that the $\widetilde{H}$-classes in $x^G \cap H$ are parameterized by the number N of choices for $y_2 \in \mathrm{PSp}_2(K)$ (up to conjugacy). Evidently, $N \leqslant t+1 = \frac{1}{2}(r+1)$ and therefore $N \leqslant \frac{1}{2}(q+4-2e)$ since $i \leqslant 2$. In view of (26) we conclude that

$$|x^G \cap H| < \log_2 q.2^{\frac{d}{2}(e-1)}(1+\frac{1}{2}(q+4-2e)q^2)q^{\frac{1}{4}(\dim x^{\bar{G}}+3a)}, \tag{27}$$

where $\dim x^{\bar{G}} \geqslant a(a-1)$. The reader can check that this bound with (25) is sufficient unless $a=4$. Here q is odd (see Table 4.1). If $C_{\bar{G}}(x) = \mathrm{GL}_4$ then $x^G \cap H$ is a union of at most two distinct $\widetilde{H}$-classes, with representatives $[I_4] \otimes [\lambda, \lambda^{-1}]$ and $[\lambda I_2, \lambda^{-1} I_2] \otimes [I_2]$ for some $\lambda \in K^*$. In this case the bounds

$$|x^G \cap H| \leqslant \log_3 q.(q(q+\epsilon)+q^3(q+\epsilon)(q^4-1)), \ \ |x^G| \geqslant q^6(q+\epsilon)(q^2+1)(q^3+\epsilon)(q^4-1)$$

are always sufficient, where $\epsilon = (-1)^{i+1}$. If $C_{\bar{G}}(x) \neq \mathrm{GL}_4$ then $\dim x^{\bar{G}} \geqslant f(d)$, where $f(e) = f(2e) = 18$, $f(3e) = 22$ and $f(4e) = 24$. The result follows via (25) and (27). $\square$

The remaining cases in Table 4.1 are entirely straightforward and are left to the reader.

5 Proof of Theorem 1.1: $H \in \mathscr{C}_5$

Here $q = q_0^k$, where k is a prime, and the specific cases are recorded in Table 5.1 (see [18, Table 4.5.A]). For convenience we postpone the analysis of the $\mathscr{C}_5$-subgroups of type $\mathrm{Sp}_n(q)$ and $\mathrm{O}_n^{\epsilon}(q)$ in unitary groups to §8 and our work with the collection $\mathscr{C}_8$.

	G_0	type of H	conditions
(i)	$\mathrm{PSL}_n^{\epsilon}(q)$	$\mathrm{GL}_n^{\epsilon}(q_0)$	k odd if $\epsilon = -$
(ii)	$\mathrm{PSp}_n(q)$	$\mathrm{Sp}_n(q_0)$	
(iii)	$\mathrm{P}\Omega_n^{\epsilon}(q)$	$\mathrm{O}_n^{\epsilon}(q_0)$	k odd if $\epsilon = -$
(iv)	$\mathrm{P}\Omega_n^{+}(q)$	$\mathrm{O}_n^{-}(q_0)$	$k = 2$

Table 5.1: The collection $\mathscr{C}_5$

Proposition 5.1. *The conclusion to Theorem 1.1 holds in case (i) of Table 5.1.*

Proof. We may assume $n \geqslant 3$. Let σ_0 be a Frobenius morphism of $\bar{G} = \mathrm{PSL}_n(K)$ such that $\bar{G}_\sigma$ has socle $G_0 = \mathrm{PSL}_n^{\epsilon}(q_0^k)$, where $\sigma = \sigma_0^k$. We begin by considering elements $x \in H \cap \mathrm{PGL}(V)$ of prime order r, where $H \cap \mathrm{PGL}(V) \leqslant \mathrm{PGL}_n^{\epsilon}(q_0) = \bar{G}_{\sigma_0}$ (see [18, (4.5.5)]).

Case 1. $x \in H \cap \mathrm{PGL}(V)$**,** $r = p$
Let $\lambda = (n^{a_n}, \ldots, 1^{a_1}) \vdash n$ be the associated partition of x and observe that $|x^G \cap H| \leqslant |x^{\bar{G}_{\sigma_0}}|$. Applying Lemma 3.18 we deduce that

$$|x^G \cap H| < 2^{(t-1)(\delta_{2,q_0}+\frac{1}{2}(1+\epsilon))}\left(\frac{q_0+1}{q_0}\right)^{\frac{1}{2}(1-\epsilon)} q_0^{\dim x^{\bar{G}}} \tag{28}$$

and

$$|x^G| > \frac{1}{2}\left(\frac{q_0^k}{q_0^k+1}\right)^{\frac{t}{2}(1-\epsilon)} q_0^{k(\dim x^{\bar{G}}-1)} \tag{29}$$

where t denotes the number of non-zero terms a_j in λ.

First assume $\lambda = (2^j, 1^{n-2j})$ for some $j \geqslant 1$ (note that λ must have this form if $p=2$). Then $\dim x^{\bar{G}} = 2j(n-j)$, $t \leqslant 2$ and the bounds (28) and (29) are always sufficient if $k \geqslant 3$. Now assume $k=2$, so $\epsilon = +$ (see Table 5.1). If $j > 1$ then $n \geqslant 4$, $\dim x^{\bar{G}} \geqslant 4n-8$ and (28) and (29) are sufficient unless $(n, q_0) = (4, 2)$, where direct calculation yields $f(x, H) < .483$. If $j = 1$ and $q_0 \geqslant 3$ then we are left to deal with the case $(n, q_0) = (3, 3)$ where a similar calculation gives $f(x, H) < .523$. Finally, if $(j, q_0) = (1, 2)$ then the bounds $|x^G \cap H| < 2^{2n-1}$ and $|x^G| > 2^{4n-5}$ are sufficient for all $n \geqslant 3$.

Now assume $\lambda \neq (2^j, 1^{n-2j})$ and p is odd. If $t = 1$ then [6, 2.4] implies that $\dim x^{\bar{G}} \geqslant \frac{1}{2}n^2$ (minimal if $\lambda = (2^{n/2})$) and the result follows via (28) and (29). If $t \geqslant 2$ then $n \geqslant \frac{1}{2}t(t+1)$ and if we assume $(t, k) \neq (2, 2)$ then the above bounds are sufficient since $\dim x^{\bar{G}} \geqslant g(n, t)$, where g is defined in the statement of Lemma 3.25. If $(t, k) = (2, 2)$ then $\epsilon = +$ and the bounds (28) and (29) are sufficient since $n \geqslant 4$ and $\dim x^{\bar{G}} \geqslant 4n - 6$ (minimal if $\lambda = (3, 1^{n-3})$).

Case 2. $x \in H \cap \mathrm{PGL}(V)$**,** $r \neq p$
Let us begin by assuming $r = 2$. If $C_{\bar{G}}(x)$ is connected then $\dim x^{\bar{G}} \geqslant 2n - 2$ and the bounds

$$|x^G \cap H| \leqslant |x^{\bar{G}_{\sigma_0}}| < 2q_0^{\dim x^{\bar{G}}}, \ \ |x^G| > \frac{1}{2}\left(\frac{q_0^k}{q_0^k + 1}\right) q_0^{k \dim x^{\bar{G}}}$$

are always sufficient. On the other hand, if $C_{\bar{G}}(x)$ is non-connected then n is even,

$$|x^G \cap H| \leqslant \frac{|\mathrm{GL}_n^\epsilon(q_0)|}{|\mathrm{GL}_{n/2}^\epsilon(q_0)|^2 2} + \frac{|\mathrm{GL}_n^\epsilon(q_0)|}{|\mathrm{GL}_{n/2}(q_0^2)|2} < 2q_0^{\frac{1}{2}n^2}, \ \ |x^G| > \frac{1}{4}\left(\frac{q_0^k}{q_0^k + 1}\right) q_0^{\frac{1}{2}kn^2}$$

and the result follows.

Assume for the remainder that r is odd. If $C_{\bar{G}}(x)$ is non-connected then Lemma 3.35 implies that r divides n and we deduce that

$$|x^G \cap H| < 2^{r-1} q_0^{n^2(1-\frac{1}{r})}, \ \ |x^G| > \frac{1}{2r}\left(\frac{q_0^k}{q_0^k + 1}\right)^{r-1} q_0^{kn^2(1-\frac{1}{r})}.$$

These bounds are sufficient unless $(n, k, r, q_0) = (3, 2, 3, 2)$, where a more accurate calculation yields $f(x, H) < .587$. Now assume $C_{\bar{G}}(x)$ is connected and let $i \geqslant 1$ (resp. $i_0 \geqslant 1$) be minimal such that $r|(q^i - 1)$ (resp. $r|(q_0^{i_0} - 1)$), so

$$i = \begin{cases} i_0/k & \text{if } k \text{ divides } i_0 \\ i_0 & \text{otherwise.} \end{cases} \tag{30}$$

Define the integers l and d as in Definition 3.32 (with respect to σ-orbits). Now, if k does not divide i_0 then σ_0- and σ-orbits coincide, otherwise each non-trivial σ_0-orbit is a union of k distinct σ-orbits and thus k divides d. Applying Lemma 3.30 we deduce that

$$|x^G \cap H| < 2\log_2 q_0 . 2^{\frac{di}{i_0}(1-\alpha)} \left(\frac{q_0 + 1}{q_0}\right)^{\frac{1}{2}(1-\epsilon)} q_0^{\dim x^{\bar{G}}}, \ \ |x^G| > \frac{1}{2}\left(\frac{q_0^k}{q_0^k + 1}\right)^{\alpha d} q_0^{k \dim x^{\bar{G}}},$$

where $\alpha = 1$ if $\epsilon = -$ and $i \equiv 2\,(4)$, otherwise $\alpha = 0$. The result now follows by applying the lower bound for $\dim x^{\bar{G}}$ given in Lemma 3.33.

Case 3. $x \in H - \mathrm{PGL}(V)$
First assume $x \in G$ is a field automorphism of prime order r. Then Lemma 3.50 implies that $x^G \cap H \subseteq \bar{G}_{\sigma_0} x$ and Lemma 3.49 gives

$$|x^G| > \frac{1}{2}(q_0^k + 1)^{-1} q_0^{k(n^2-1)(1-\frac{1}{r})}. \tag{31}$$

If $r \neq k$ then $q_0 = q_1^r$ and x induces a field automorphism on $\bar{G}_{\sigma_0}$. In this case, Proposition 3.43 implies that $|x^G \cap H| \leqslant |x^{\bar{G}_{\sigma_0}}| < 2q_0^{(n^2-1)(1-1/r)}$ and the result follows. If $r = k$ then we may assume that x centralizes $\bar{G}_{\sigma_0}$ and thus $|x^G \cap H| \leqslant i_r(\bar{G}_{\sigma_0}) + 1$. In fact, if $r = k \geqslant 3$ then it is easy to see that the bounds $|x^G \cap H| \leqslant |\bar{G}_{\sigma_0}| < q_0^{n^2-1}$ and (31) are always sufficient. If $r = k = 2$ then $\epsilon = +$ and Lemma 3.14 implies that

$$|x^G \cap H| \leqslant i_2(\bar{G}_{\sigma_0}) + 1 \leqslant 2(1+q_0^{-1})q_0^{\frac{1}{2}(n^2+n-2)}.$$

Now $|x^G| > \frac{1}{2}(n, q_0^2-1)^{-1}q_0^{n^2-1}$ and we find that we are left to deal with the following cases:

(n, q_0)	$(4,3)$	$(4,2)$	$(3,4)$	$(3,2)$
$i_2(\bar{G}_{\sigma_0})$	8451	315	315	21
$f(x,H) <$	.594	.534	.572	.646

Here the listed upper bounds are derived using the upper bound $|x^G \cap H| \leqslant i_2(\bar{G}_{\sigma_0}) + 1$ and an accurate lower bound for $|x^G|$. For example, if $(n, q_0) = (3, 2)$ then $f(x,H) < .646$ since $i_2(\mathrm{PGL}_3(2)) = \frac{1}{8}|\mathrm{GL}_3(2)| = 21$ and $|x^G| \geqslant \frac{1}{3}|\mathrm{SL}_3(4) : \mathrm{SL}_3(2)| = 120$.

The argument for an involutory graph-field automorphism is similar and is left to the reader. Finally, let us assume $x \in G$ is an involutory graph automorphism. Then $x^G \cap H \subseteq \bar{G}_{\sigma_0}x$ and each $y \in x^G \cap H$ induces an involutory graph automorphism on $\bar{G}_{\sigma_0}$ such that $C_{\bar{G}_{\sigma_0}}(y)$ and $C_{G_0}(x)$ are of the same type, i.e. they are either both symplectic or non-symplectic (see Definition 3.47). Therefore

$$|x^G \cap H| < 2q_0^{\frac{1}{2}(n^2+\alpha n-2)}, \quad |x^G| > \frac{1}{2}\left(\frac{q_0^k}{q_0^k+1}\right)q_0^{\frac{k}{2}(n^2+\alpha n-4)},$$

where $\alpha = 1$ if x is non-symplectic, otherwise $\alpha = -1$. If x is non-symplectic then these bounds are sufficient unless $(k, n, q_0) = (2, 3, 2)$, where direct calculation yields $f(x,H) < .573$. On the other hand, if x is symplectic then n is even and we are left to deal with the case $(n, k) = (4, 2)$ for $q_0 < 4$. Here $\epsilon = +$, $|x^G \cap H| \leqslant q_0^2(q_0^3-1)$, $|x^G| \geqslant \frac{1}{4}q_0^4(q_0^6-1)$ and thus $f(x,H) < .603$ for all $q_0 \geqslant 2$. □

Proposition 5.2. *The conclusion to Theorem 1.1 holds in case (ii) of Table 5.1.*

Proof. This is very similar to the previous case and to avoid unnecessary repetition we shall assume $(n, p) = (4, 2)$ and G contains a graph-field automorphism (see Remark 3.44).

We start by assuming $x \in H \cap \mathrm{PGL}(V)$ has prime order r, where $H \cap \mathrm{PGL}(V) \leqslant \mathrm{Sp}_4(q_0) = \widetilde{H}$. If $r = 2$ and x is G-conjugate to c_2 then Lemma 3.22 gives $|x^G \cap H| < 2q_0^6$, $|x^G| > \frac{1}{2}q_0^{6k}$ and the result follows. On the other hand, if x is G-conjugate to b_1 then the subsequent bounds $|x^G \cap H| = 2|b_1^{\mathrm{Sp}_4(q_0)}| < 2q_0^4$ and $|x^G| > q_0^{4k}$ are always sufficient (note that the involutions b_1 and a_2 are G-conjugate - see Proposition 3.52). The case $r > 2$ is just as easy. Define the integers i, i_0, l and d as in the proof of the previous proposition and set $e = 2$ if i is odd, otherwise $e = 1$. Note that (30) holds. Now, if i and i_0 have the same parity then replacing x by a suitable G-conjugate we deduce that

$$|x^G \cap H| < 2\log_2 q_0 . 2^{\frac{di}{2i_0}(e-1)}q_0^{\dim x^{\bar{G}}}, \quad |x^G| > \frac{1}{2}\left(\frac{q_0^k}{q_0^k+1}\right)^{(2-e)d} q_0^{k\dim x^{\bar{G}}}$$

and the result follows via Lemma 3.33. The argument when i and i_0 are of different parity is just as easy.

Finally, let us assume $x \in H - \mathrm{PGL}(V)$. If x is a field automorphism of prime order $r \neq k$ then $q_0 = q_1^r$ and the bounds

$$|x^G \cap H| \leqslant |x^{\widetilde{H}}| < 2q_0^{10\left(1-\frac{1}{r}\right)}, \quad |x^G| > \frac{1}{4}q_0^{10k\left(1-\frac{1}{r}\right)}$$

are always sufficient. If $r = k$ then we may assume x centralizes $\widetilde{H}$, thus $|x^G \cap H| \leqslant i_r(\widetilde{H}) + 1$. In fact if k is odd then the trivial bound $|x^G \cap H| \leqslant |\widetilde{H}|$ is always sufficient; if $k = 2$ then

Lemma 3.14 implies that $|x^G \cap H| \leqslant 2(1+q_0^{-1})q_0^6$ and it remains to deal with the case $q_0 = 2$. Here $f(x,H) < .601$ since $i_2(\widetilde{H}) = 75$. Finally, let us assume x is an involutory graph-field automorphism. Then $x^G \cap H \subseteq \widetilde{H}x$ and l and k are both odd, where $q_0 = 2^l$. If $l > 1$ then applying Proposition 3.43 we deduce that

$$|x^G \cap H| \leqslant |\mathrm{Sp}_4(q_0) : Sz(q_0)| < 2q_0^5, \;\; |x^G| \geqslant |\mathrm{Sp}_4(q_0^k) : Sz(q_0^k)| > q_0^{5k}$$

and the result follows. Alternatively, if $l = 1$ then the bounds $|x^G \cap H| \leqslant |\widetilde{H}x| = 720$ and $|x^G| \geqslant |\mathrm{Sp}_4(8) : Sz(8)| = 36228$ imply that $f(x,H) < .627$. □

Proposition 5.3. *The conclusion to Theorem 1.1 holds in cases (iii) and (iv) of Table 5.1.*

Proof. We consider both cases simultaneously. Fix a Frobenius morphism σ_0 of $\bar{G} = \mathrm{PSO}_n(K)$ such that $\bar{G}_\sigma$ has socle $G_0 = \mathrm{P}\Omega_n^\epsilon(q_0^k)$, where $\sigma = \sigma_0^k$ and $n \geqslant 7$. Observe that $H \cap \mathrm{PGL}(V) \leqslant \mathrm{PGO}_n^{\epsilon'}(q_0) = \widetilde{H}$. Let ($\triangle$) denote the hypothesis "$(n,\epsilon) = (8,+)$ *and G contains triality automorphisms*". According to Proposition 3.3, if ($\triangle$) holds then we may assume $\epsilon' = +$. The argument when $x \in H \cap \mathrm{PGL}(V)$ is straightforward and is left to the reader. Note that if ($\triangle$) holds then a triality graph automorphism τ of G_0 induces a triality on $\mathrm{P}\Omega_8^+(q_0)$ and Proposition 3.55 describes the action of τ on $\widetilde{H}$-classes.

For the remainder let us assume $x \in H - \mathrm{PGL}(V)$ has prime order r, beginning with the case where $x \in G$ is a field automorphism. Here Lemma 3.50 implies that $x^G \cap H \subseteq \widehat{H}x$, where $\widehat{H} = \bar{G}_{\sigma_0} \leqslant \widetilde{H}$, and Lemma 3.49 gives

$$|x^G| > \frac{1}{4}q_0^{\frac{k}{2}(n^2-n)\left(1-\frac{1}{r}\right)}. \tag{32}$$

If $r \neq k$ then $q_0 = q_1^r$ for some q_1 and the result follows via (32) since Proposition 3.43 gives

$$|x^G \cap H| < 2q_0^{\frac{1}{2}(n^2-n)\left(1-\frac{1}{r}\right)}.$$

If $r = k$ is odd then the bounds (32) and $|x^G \cap H| \leqslant |\widehat{H}x| < q_0^{n(n-1)/2}$ are sufficient. If $r = k = 2$ then $\epsilon = +$ if n is even (see Remark 3.42) and we may assume that x centralizes $\widehat{H}$ if n is odd or $\epsilon' = +$; if $\epsilon' = -$ then x induces an involutory graph automorphism on $\widehat{H}$. In all cases we have $|x^G \cap H| \leqslant i_2(\widetilde{H}) + 1$ and applying Lemma 3.14 we deduce that

$$|x^G \cap H| \leqslant i_2(\widetilde{H}) + 1 \leqslant 2(1+q_0^{-1})q_0^{\frac{1}{4}(n^2-\gamma)}, \tag{33}$$

where $n \equiv \gamma\,(2)$. If q_0 is even then $|x^G| > \frac{1}{2}q_0^{n(n-1)/2}$ and we may assume that n is even. Here we find that (33) is sufficient unless $(n,q_0) \in \{(10,2),(8,2)\}$. Similarly, if q_0 is odd then (32) holds and we are left to deal with the cases $(n,q_0) \in \{(8,3),(7,3)\}$. In these exceptional cases we derive the following upper bounds through direct calculation:

(n,q_0)	$(10,2)$	$(8,2)$	$(8,3)$	$(7,3)$
$f(x,H) <$	.585	.617	.608	.630

For instance, if $(n,q_0) = (8,2)$ then $f(x,H) < .617$ since $|x^G| \geqslant |\mathrm{O}_8^+(4) : \mathrm{O}_8^+(2)|$ and (33) gives $|x^G \cap H| \leqslant 3.2^{16}$. Similarly, if $(n,q_0) = (8,3)$ then $|x^G| \geqslant \frac{1}{4}|\mathrm{O}_8^+(9) : \mathrm{O}_8^+(3)|$ and we deduce that $f(x,H) < .608$ since Propositions 3.37 and 3.53 imply that $i_2(\mathrm{PGO}_8^{\epsilon'}(3)) \leqslant 61301583$.

The argument when x is an involutory graph-field automorphism is very similar and is left to the reader. Finally, let us assume ($\triangle$) holds and recall that we may assume H is of type $\mathrm{O}_8^+(q_0)$. Now if $x \in G$ is a triality graph automorphism then Lemma 3.50 implies that $x^G \cap H \subseteq \widehat{H}x \cup \widehat{H}x^2$, where x^i induces a triality graph automorphism on $\widehat{H}$ such that the centralizers $C_{\mathrm{P}\Omega_8^+(q_0)}(x^i)$ and $C_{G_0}(x^i)$ are of the same type. The possibilities for $C_{G_0}(x)$ are listed in Table 3.10 and the result quickly follows. For instance, if x is a G_2-type triality (see Definition 3.47) then

$$|x^G \cap H| \leqslant \frac{|\mathrm{PGO}_8^+(q_0)|}{|G_2(q_0)|} < 4q_0^{14}, \;\; |x^G| \geqslant \frac{|\mathrm{P}\Omega_8^+(q_0^k)|}{|G_2(q_0^k)|} > 2^{2\delta_{2,p}-3}q_0^{14k}$$

and we conclude that $f(x,H) < 5/8$ for all $k, q_0 \geqslant 2$. Finally, if $x \in G$ is a triality graph-field automorphism then Lemma 3.48 gives $|x^G| > \frac{1}{4}q_0^{56k/3}$ and we find that the trivial bound $|x^G \cap H| < |H| < 6k\log_2 q_0.q_0^{28}$ is sufficient for all $k \geqslant 3$ and $q_0 \geqslant 2$. If $k=2$ then $q_0 = q_1^3$ for some q_1 and again Lemma 3.50 implies that $x^G \cap H \subseteq \widehat{H}x \cup \widehat{H}x^2$, where x^i acts on $\widehat{H}$ as a triality graph-field automorphism. Therefore Proposition 3.43 implies that $|x^G \cap H| \leqslant 2|\widehat{H} : {}^3D_4(q_0^{1/3})| < 4q_0^{56/3}$ and the bound $|x^G| > \frac{1}{4}q_0^{112/3}$ is always sufficient. $\square$

6 Proof of Theorem 1.1: $H \in \mathscr{C}_6$

Let k be a prime. Then a k-group R is said to be of *symplectic type* if every characteristic abelian subgroup of R is cyclic. Let R be a symplectic type k-group of minimal exponent, i.e. $\exp(R) = k(k,2)$, and fix a prime $p \neq k$. Then R has precisely $|Z(R)|-1$ inequivalent faithful absolutely irreducible representations over an algebraically closed field of characteristic p. Furthermore, each of these representations has degree k^m for some fixed $m \geqslant 1$ and the smallest field over which they are realized is $\mathbb{F}_{p^e}$, where

$$e = \min\{z \in \mathbb{N} : p^z \equiv 1 \bmod |Z(R)|\} \tag{34}$$

(see [18, 4.6.3] for example). In this way we obtain embeddings $R \leqslant Cl_n(q)$, where $n = k^m$, $Cl_n(q)$ is a finite almost simple classical group over $\mathbb{F}_q$ with socle G_0 and

$$q = \begin{cases} p^{\frac{e}{2}} & \text{if } G_0 \text{ is unitary} \\ p^e & \text{otherwise.} \end{cases} \tag{35}$$

The members of the collection $\mathscr{C}_6$ are the subgroups $N_G(R)$, where $R \leqslant G$ is a symplectic type k-group of minimal exponent irreducibly embedded in G. Here $n = k^m$ and q is defined by (35), with e given in (34) (this restriction on the underlying field ensures that a subgroup in $\mathscr{C}_6$ is not contained in a member of the subfield subgroup collection $\mathscr{C}_5$). The cases we need to consider are listed in Table 6.1 (see [18, Table 4.6.B]).

	G_0	type of H	$\lvert Z(R)\rvert$	conditions
(i)	$\mathrm{PSL}_n^{\epsilon}(q)$	$k^{2m}.\mathrm{Sp}_{2m}(k)$	k	k odd, $\epsilon = (-1)^{e+1}$
(ii)	$\mathrm{PSL}_n^{\epsilon}(q)$	$2^{2m}.\mathrm{Sp}_{2m}(2)$	4	$k=2$, $\epsilon = (-1)^{e+1}$
(iii)	$\mathrm{PSp}_n(q)$	$2^{2m}.\mathrm{O}_{2m}^{-}(2)$	2	$k=2$, $e=1$
(iv)	$\mathrm{P\Omega}_n^{+}(q)$	$2^{2m}.\mathrm{O}_{2m}^{+}(2)$	2	$k=2$, $e=1$

Table 6.1: The collection $\mathscr{C}_6$

Lemma 6.1. *Let G be a finite group, V an m-dimensional faithful irreducible $\mathbb{F}_qG$-module, where $q=p^f$, and let $X = V.G$ be an extension of V by G. Fix a prime r dividing $|X|$ and let $\{g_1,\ldots,g_N\}$ be a complete set of representatives for the G-classes of elements of order r in G.*

(i) If $r \neq p$ then $i_r(X) \leqslant \sum_{i=1}^N q^{m-m_i}|g_i^G|$, where $m_i = \dim C_V(g_i)$.

(ii) If $r = p$ then $i_r(X) \leqslant q^m - 1 + \sum_{i=1}^N q^{m-m_i'}|g_i^G|$, where m_i' is the number of Jordan r-blocks in the Jordan normal form of g_i on V.

Proof. Let $x \in X - V$ be an element of prime order r and let $\bar{x} = Vx$ denote the image of x under the quotient map $X \to X/V \cong G$. Now an element $vx \in Vx$ has order r if and only if

$$v + v^x + v^{x^2} + \cdots + v^{x^{r-1}} = 0$$

which is equivalent to the condition $v(1+\bar{x}+\bar{x}^2+\cdots+\bar{x}^{r-1}) = 0$ as a linear map. If $r \neq p$ then $v(1+\bar{x}+\cdots+\bar{x}^{r-1}) = 0$ if and only if $v \in \mathrm{im}\,(1-\bar{x})$ and thus $i_r(Vx) \leqslant |\mathrm{im}\,(1-\bar{x})| = q^{m-l}$, where $l = \dim C_V(\bar{x})$. Then (i) follows since $i_r(V) = 0$ and $\dim C_V(\bar{x}_1) = \dim C_V(\bar{x}_2)$ if $\bar{x}_1$ and $\bar{x}_2$ are G-conjugate. On the other hand, if $r = p$ then $i_r(V) = q^m - 1$ and (ii) holds since

$$i_r(Vx) \leqslant |\ker(1 + \bar{x} + \cdots + \bar{x}^{r-1})| = q^{m-a_r},$$

where a_r denotes the number of Jordan r-blocks in the Jordan normal form of $\bar{x}$ on V. $\square$

Remark 6.2. If $V.G$ is a split extension then equality holds in both parts of Lemma 6.1.

Let H be a $\mathscr{C}_6$-subgroup of G and let V be the natural G_0-module. Then $H \cap \mathrm{PGL}(V)$ is primitive, irreducible and tensor-indecomposable on V. In particular, each non-trivial $x \in H \cap \mathrm{PGL}(V)$ lifts to an element $\hat{x} \in \mathrm{GL}(\bar{V})$, where $\bar{V} = V \otimes \bar{\mathbb{F}}_q$, with the property that there exist four $\mathrm{GL}(\bar{V})$-conjugates of $\hat{x}$ whose product is a non-trivial scalar (see [13, p.452]). This implies that $\nu(x) \geqslant n/4$, where $n = \dim V$, and lower bounds on $|x^G|$ follow via Corollary 3.38. For easy reference, we record this fact in the next lemma.

Lemma 6.3. *If $x \in H \cap \mathrm{PGL}(V)$ is non-trivial then $\nu(x) \geqslant n/4$, where $n = \dim V$.*

Proposition 6.4. *The conclusion to Theorem 1.1 holds in case (i) of Table 6.1.*

Proof. Let $x \in H$ be an element of prime order r and observe that [18, Table 4.6.A, (4.6.1)] implies that $H \cap \mathrm{PGL}(V) \leqslant k^{2m}.\mathrm{Sp}_{2m}(k) = \widetilde{H}$. First assume $x \in H \cap \mathrm{PGL}(V)$. Then applying Lemma 6.3 and Corollary 3.38 we deduce that

$$|x^G \cap H| \leqslant |\widetilde{H}| < k^{2m^2+3m}, \;\; |x^G| > \frac{1}{2}(q+1)^{-2}q^{\frac{3}{8}n^2+1}$$

and we are left to deal with the cases $(k,m) \in \{(5,1),(3,1)\}$ and $(k,m,q) = (3,2,2)$. If $(k,m,q) = (3,2,2)$ then $G_0 = \mathrm{PSU}_9(2)$, $\widetilde{H} = 3^4.\mathrm{Sp}_4(3)$ and Lagrange's Theorem implies that $r \in \{2,3,5\}$. Applying Lemma 6.1 we get $i_r(\widetilde{H}) \leqslant n_r$, where

$$n_5 = 3^4.5184, \;\; n_3 = 3^4 - 1 + 3^4.(480+240+40+40), \;\; n_2 = 3^4.1 + 3^2.90.$$

Since $n = 9$, Lemma 6.3 implies that $\nu(x) \geqslant 3$. In particular, if $r = 2$ then $|x^G|$ is minimal when x has associated partition $\lambda = (2^3, 1^3)$ and thus $f(x,H) < .276$ since $|x^G \cap H| \leqslant n_2$. The case $r \in \{3,5\}$ is similar. If $(k,m) = (3,1)$ then $\widetilde{H} = 3^2.\mathrm{Sp}_2(3)$, $r \in \{2,3\}$ and we may assume $p \geqslant 5$ since $p \neq k$ and $\mathrm{PSU}_3(2) \cong 3^2.Q_8$. Therefore x is semisimple, hence $|x^G| > \frac{1}{2}(q+1)^{-1}q^5$ and the result follows since Lemma 6.1 implies that $|x^G \cap H| \leqslant 9$ if $r = 2$ and $|x^G \cap H| \leqslant 80$ if $r = 3$. The case $(k,m) = (5,1)$ is just as easy.

Now assume $x \in H - \mathrm{PGL}(V)$. If x is a field automorphism of prime order r then $q = q_0^r$, $k \geqslant 5$ (since $q = p$ if $k = 3$) and the result follows via Lemma 3.48 since

$$|x^G \cap H| < |H| < 2\log_2 q.k^{2m^2+3m}. \tag{36}$$

The argument for an involutory graph-field automorphism is entirely similar. Now assume x is an involutory graph automorphism. Since $n = k^m$ is odd we have $|x^G| > \frac{1}{2}(q+1)^{-1}q^{(n^2+n-2)/2}$ (see Lemma 3.48) and (36) is sufficient unless $(k,m) = (3,1)$. Here $q = p \geqslant 5$, $|x^G \cap H| \leqslant |\widetilde{H}x| = 216$ and the previous bound for $|x^G|$ is sufficient unless $p = 5$. In this exceptional case we have $G_0 = \mathrm{PSU}_3(5)$ and therefore $f(x,H) < .773$ since $|x^G| \geqslant 1050$. $\square$

Proposition 6.5. *The conclusion to Theorem 1.1 holds in case (ii) of Table 6.1.*

Proof. Here $n = 2^m$, $m \geqslant 2$ and $G_0 = \mathrm{PSL}_n^{\epsilon}(q)$, where $q = p$ and $\epsilon = (-1)^{e+1}$. Observe that $H \cap \mathrm{PGL}(V) \leqslant 2^{2m}.\mathrm{Sp}_{2m}(2) = \widetilde{H}$ and first assume $x \in H \cap \mathrm{PGL}(V)$ has prime order r. Then arguing as in the proof of the previous proposition we quickly reduce to the case $m = 2$. Here $r \in \{2,3,5\}$ and Lemma 6.1 implies that $i_r(\widetilde{H}) \leqslant n_r$, where

$$n_5 = 2^4.144, \;\; n_3 = 2^4.40 + 2^2.40, \;\; n_2 = 2^4 - 1 + 2^3.15 + 2^2.(45+15).$$

If $\nu(x)=1$ then we claim that x is semisimple and r divides $q-\epsilon$. Of course, if x is semisimple and $\nu(x)=1$ then r must divide $q-\epsilon$ since each σ-orbit must be a singleton set. To rule out unipotent elements, we appeal to [16, Theorem II]. Here Kantor lists all subgroups of $\mathrm{SL}(V)$ which are generated by transvections and it is easy to see that no subgroup of $\widetilde{H}$ belongs to this list. This justifies the claim. In particular, if $\nu(x)=1$ then

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

and one can check that the bounds $|x^G\cap H| \leqslant n_r$ are sufficient unless $(\epsilon,r,q)=(-,2,3)$. In this exceptional case the associated permutation character χ is given in [9, p.53] and we derive the following results, where $\mathrm{PGU}_4(3)$-classes are labelled as in [9].

$\mathrm{PGU}_4(3)$-class of x	$\nu(x)$	$\lvert x^G\cap H\rvert$	$\lvert x^G\rvert$	$f(x,H)<$
$2A$	2	195	2835	.664
$2B$	1	60	540	.651
$2C$	2	120	4536	.569

Similarly, if $\nu(x)\geqslant 2$ then $|x^G| > \frac{1}{4}(q+1)^{-1}q^9$ and we are left to deal with the case $q=3$. Here we can work with the associated permutation character and the desired result quickly follows.

Now assume $x\in H-\mathrm{PGL}(V)$ has prime order. Then x is an involutory graph automorphism since $q=p$. According to Lemma 3.50 we have $|x^G\cap H|\leqslant|\widetilde{H}x|<2^{2m^2+3m}$ and if we assume $C_{G_0}(x)$ is orthogonal then $|x^G|>\frac{1}{2}(q+1)^{-1}q^{(n^2+n-2)/2}$ and the desired result follows for all $m\geqslant 3$. Similarly, if $C_{G_0}(x)$ is symplectic then $|x^G|>\frac{1}{2}(q+1)^{-1}q^{(n^2-n-2)/2}$ and if we assume $m\geqslant 3$ then we are left to deal with the case $(m,q)=(3,3)$. Here $H\leqslant 2^7.\mathrm{Sp}_6(2)$ and we deduce that $f(x,H)<.471$ since

$$|x^G\cap H|\leqslant i_2(H)\leqslant 2^7 i_2(\mathrm{Sp}_6(2)) = 2^7.4823, \quad |x^G|\geqslant|\mathrm{PSU}_8(3):\mathrm{PSp}_8(3).2|.$$

Finally, if $m=2$ then using GAP [10, 14] we obtain the following bounds:

$\mathrm{Aut}(G_0)$-class of x	$\lvert x^G\cap H\rvert\leqslant$	$\lvert x^G\rvert\geqslant$	$f(x,H)<$
$2D$	36	126	.741
$2E$	340	5670	.675

(Note that the class labelled $2F$ does not meet H.) □

Proposition 6.6. *The conclusion to Theorem 1.1 holds in case (iii) of Table 6.1.*

Proof. Here $G_0=\mathrm{PSp}_n(q)$, where $n=2^m$ and $m\geqslant 2$. Since $q=p$ is odd we have $H\leqslant\mathrm{PGL}(V)$ and [18, (4.6.1)] implies that $H\leqslant 2^{2m}.\mathrm{O}_{2m}^{-}(2)=\widetilde{H}$. Applying Lemma 6.3 and Corollary 3.38 we deduce that

$$|x^G\cap H|\leqslant|\widetilde{H}|<2^{2m^2+m+1}, \quad |x^G|>\frac{1}{8}(q+1)^{-1}q^{\frac{3}{16}n^2+1}$$

and if we assume $m\geqslant 3$ then these bounds are sufficient unless $m=3$ and $q<11$. Here $\widetilde{H}=2^6.\mathrm{O}_6^{-}(2)$, so $r\in\{2,3,5\}$ and Lemma 6.1 implies that $i_r(\widetilde{H})\leqslant n_r$, where

$$n_5=2^4.5184, \quad n_3=2^6.80+2^4.480+2^2.240, \quad n_2=2^6-1+2^5.36+2^4.(270+45)+2^3.540.$$

Now $|x^G\cap H|\leqslant n_r$ and we find that the previous bound for $|x^G|$ is sufficient unless $q=3$ or $(q,r)=(5,5)$. If $(q,r)=(5,5)$ then $|x^G|$ is minimal when x has associated partition $\lambda=(2^2,1^4)$ and we find that an accurate bound for $|x^G|$ is sufficient. If $(q,r)=(3,3)$ then using GAP [10] we calculate that $\nu(x)\geqslant 4$ and $f(x,H)<.369$. The other cases with $q=3$ are dealt with in a similar fashion.

It remains to deal with the case $m = 2$. Here $\widetilde{H} = 2^4.\mathrm{O}_4^-(2)$ so Lagrange's Theorem implies that $r \in \{2, 3, 5\}$ and Lemma 6.1 gives $i_r(\widetilde{H}) \leqslant n_r$, where

$$n_5 = 2^4.24, \;\; n_3 = 2^2.20, \;\; n_2 = 2^4 - 1 + 2^3.10 + 2^2.15.$$

Clearly, there are no semisimple elements $x \in H$ with $\nu(x) = 1$ (indeed, there are no such elements in G) and [16, Theorem II] implies that the same is true for unipotent elements. Therefore Corollary 3.38 implies that $|x^G| > \frac{1}{8}(q+1)^{-1}q^5$ and the bounds $|x^G \cap H| \leqslant n_r$ are sufficient unless $(q, r) = (11, 5)$ or $q \leqslant 7$. If $(q, r) = (11, 5)$ then $f(x, H) < .411$ since $|x^G \cap H| \leqslant n_5$ and $|x^G| \geqslant |\mathrm{Sp}_4(11) : \mathrm{Sp}_2(11)\mathrm{GL}_1(11)|$. We claim that the following upper bounds for $f(x, H)$ hold when $q \leqslant 7$.

	$r = 2$	3	5
$q = 3$	.836*	.800*	.696
5	.526	.629	.681
7	.392	.371	.384

Here the asterisk indicates that we have an exception to the main statement of Theorem 1.1 and therefore the case $(m, q) = (2, 3)$ is listed in Table 1.2. We now explain how we derive these results. In the case $r = 2$, GAP [10] gives the following results, where $q \equiv \epsilon\,(4)$ and G-classes are labelled as in [9]. The relevant entries in the above table follow at once.

$\mathrm{PGSp}_4(q)$-class of x	$\lvert x^G \cap H\rvert$	$\lvert x^G\rvert$
$2A$	5	$\frac{1}{2}q^2(q^2+1)$
$2B$	70	$\frac{1}{2}q^3(q+\epsilon)(q^2+1)$
$2C$	20	$\frac{1}{2}q^2(q^2-1)$
$2D$	60	$\frac{1}{2}q^3(q-\epsilon)(q^2+1)$

Now assume $r \in \{3, 5\}$. If $q \in \{5, 7\}$ then we compute more accurate lower bounds for $|x^G|$ and apply the bound $|x^G \cap H| \leqslant n_r$. For instance, if $(q, r) = (7, 5)$ then $|x^G| = |\mathrm{Sp}_4(7) : \mathrm{GU}_1(7^2)|$ and thus $f(x, H) < .384$ since $n_5 = 2^4.24$. Finally, if $q = 3$ then the associated permutation character χ is given in [9] and we can compute accurate values for both $|x^G \cap H|$ and $|x^G|$. For instance, if $r = 3$ then $\chi(x) > 0$ if and only if x resides in the G_0-class labelled $3C$, whence $|x^G \cap H| = 80$, $|x^G| = 240$ and thus $f(x, H) < .800^*$. $\square$

Proposition 6.7. *The conclusion to Theorem 1.1 holds in case (iv) of Table 6.1.*

Proof. Here $G_0 = \mathrm{P}\Omega_n^+(q)$, where $n = 2^m$, $m \geqslant 3$ and $q = p$ is odd. According to Proposition 3.3 we may assume G does not contain any triality automorphisms if $m = 3$ and thus [18, (4.6.1)] implies that $H \leqslant 2^{2m}.\mathrm{O}_{2m}^+(2) = \widetilde{H} \leqslant \mathrm{PGL}(V)$.

Since $|x^G \cap H| \leqslant |\widetilde{H}| < 2^{2m^2+m+1}$, we quickly reduce to the case $m = 3$ by applying Lemma 6.3 and Corollary 3.38. Then $r \in \{2, 3, 5, 7\}$ and using Lemma 6.1 we deduce that $i_r(\widetilde{H}) \leqslant n_r$, where $n_7 = 2^6.5760$, $n_5 = 2^4.1344$ and

$$n_3 = 2^4.1120 + 2^2.112, \;\; n_2 = 2^6 - 1 + 2^5.28 + 2^4.(210 + 105) + 2^3.420.$$

Applying Lemma 6.3 and Corollary 3.38 we deduce that $|x^G| > \frac{1}{8}(q+1)^{-1}q^{11}$ and the bound $|x^G \cap H| \leqslant n_r$ is sufficient unless $(q, r) = (7, 7)$ or $q \leqslant 5$. If $(q, r) = (7, 7)$ then [16, Theorem I] implies that

$$|x^G| \geqslant \frac{|\mathrm{O}_8^+(7)|}{|\mathrm{O}_5(7)||\mathrm{O}_1(7)|7^6}$$

(minimal if x has associated partition $\lambda = (3, 1^5)$) and we conclude that $f(x, H) < .566$. In the remaining cases we derive the following upper bounds for $f(x, H)$:

	$r = 2$	3	5	7
$q = 3$	.590	.534	.459	.495
5	.497	.514	.536	.334

The entries in the case $q=5$ are obtained by applying the bound $|x^G \cap H| \leqslant n_r$, together with a more accurate bound for $|x^G|$. For instance, if $(q,r)=(5,3)$ then $|x^G| \geqslant |\mathrm{O}_8^+(5) : \mathrm{O}_6^-(5)\mathrm{GU}_1(5)|$ and therefore $f(x,H) < .514$ since $|x^G \cap H| \leqslant n_3$. If $q=3$ then the listed bounds are easily checked using GAP [10]. □

7 Proof of Theorem 1.1: $H \in \mathscr{C}_7$

Here V admits a tensor decomposition $V = V_1 \otimes \cdots \otimes V_t$, where $\dim V_i = a$ and $t \geqslant 2$. The subgroups in $\mathscr{C}_7$ preserve this tensor product structure; the particular cases which we must consider are listed in Table 7.1, where $n = a^t$ (see [18, Tables 3.5.B-E, 4.7.A] and [17, p.194]).

	G_0	type of H	conditions
(i)	$\mathrm{PSL}_n^\epsilon(q)$	$\mathrm{GL}_a^\epsilon(q) \wr S_t$	$a \geqslant 3$, $(a,q) \neq (3,2)$ if $\epsilon = -$
(ii)	$\mathrm{PSp}_n(q)$	$\mathrm{Sp}_a(q) \wr S_t$	a even, qt odd, $(a,q) \neq (2,3)$
(iii)	$\Omega_n(q)$	$\mathrm{O}_a(q) \wr S_t$	aq odd, $(a,q) \neq (3,3)$
(iv)	$\mathrm{P\Omega}_n^+(q)$	$\mathrm{Sp}_a(q) \wr S_t$	a, qt even, $(a,q) \notin \{(2,2),(2,3)\}$, $(a,t) \neq (2,3)$
(v)	$\mathrm{P\Omega}_n^+(q)$	$\mathrm{O}_a^\epsilon(q) \wr S_t$	q odd, $a \geqslant 4$ if $\epsilon = -$, $a \geqslant 6$ if $\epsilon = +$

Table 7.1: The collection $\mathscr{C}_7$

We begin with a preliminary lemma which is taken from the proof of [12, 7.1].

Lemma 7.1. *Let $X \leqslant \mathrm{GL}(V)$ be a group preserving a tensor product structure $V = V_1 \otimes \cdots \otimes V_t$, where $t \geqslant 2$ and $\dim V_i = a$ for each i. If $x \in X$ is a non-scalar element of prime order r and $(a,t,r) \notin \{(2,2,2),(2,3,2)\}$ then $\nu(x) \geqslant a^{t/2}$.*

Proof. Let $(r^h, 1^{t-hr})$ be the cycle-shape of the permutation induced by x on the subspaces $\{V_1, \ldots, V_t\}$. If $t = hr$ then without loss of generality we may assume $x = x_1 \otimes x_2$, where $x_1 \in \mathrm{GL}(V_1 \otimes \cdots \otimes V_r) = \mathrm{GL}(U)$, $x_2 \in \mathrm{GL}(V_{r+1} \otimes \cdots \otimes V_t) = \mathrm{GL}(W)$ and $\langle x_1 \rangle$ acts transitively on $\{V_1, \ldots, V_r\}$. It follows that $\nu_U(x_1) = (a^r - a)(1 - r^{-1})$, where $\nu_U(x_1)$ denotes the codimension of the largest eigenspace of x_1 in its action on U, and thus (19) implies that

$$\nu(x) \geqslant a^{t-r}(a^r - a)(1 - r^{-1}). \tag{37}$$

We conclude that $\nu(x) \geqslant a^{t/2}$ for all $(a,t,r) \notin \{(2,2,2),(2,3,2)\}$. Now assume $k = t - hr > 0$, say x fixes the subspaces $\{V_1, \ldots, V_k\}$. If $k = t$ then (19) gives $\nu(x) \geqslant a^{t-1} \geqslant a^{t/2}$ so let us assume otherwise. Write $x = x_1' \otimes x_2'$, where $x_1' \in \mathrm{GL}(V_1 \otimes \cdots \otimes V_k) = \mathrm{GL}(U')$ and $x_2' \in \mathrm{GL}(V_{k+1} \otimes \cdots \otimes V_t) = \mathrm{GL}(W')$. Then as before we have $\nu_{W'}(x_2') \geqslant a^{t-k-r}(a^r - a)(1 - r^{-1})$ and a further application of (19) implies that (37) holds. □

Proposition 7.2. *The conclusion to Theorem 1.1 holds when $H \in \mathscr{C}_7$.*

Proof. Consider case (ii) of Table 7.1. The other cases are very similar and are left to the reader. Let σ be a Frobenius morphism of $\bar{G} = \mathrm{PSp}_n(K)$ such that $\bar{G}_\sigma$ has socle $G_0 = \mathrm{PSp}_n(q)$, with q odd. Observe that $H \cap \mathrm{PGL}(V) \leqslant \mathrm{PGSp}_a(q)^t.S_t$. Let $x \in H \cap \mathrm{PGL}(V)$ be an element of prime order r and assume $(a,t) \neq (2,3)$. Then applying Lemma 7.1 and Corollary 3.38 we deduce that $|x^G| > \frac{1}{8}(q+1)^{-1}q^{a^t(a^{t/2}-1)+1}$ and the result follows since $|x^G \cap H| \leqslant |H \cap \mathrm{PGL}(V)| < t!q^{t(a^2+a)/2}$.

If $(a,t) = (2,3)$ then we may assume $q \geqslant 5$ (see Table 7.1). Now if $x^G \cap H \subseteq B$, where $B = \mathrm{PGSp}_2(q)^3$, then $|x^G \cap H| < q^9$ and the result follows via Corollary 3.38 since (19) implies that $\nu(x) \geqslant 4$. Now assume $x^G \cap H \not\subseteq B$, so $r \in \{2,3\}$. If $r=3$ then the proof of [6, 5.3] gives

$$x = \begin{cases} [I_4, \omega I_2, \omega^2 I_2] & \text{if } p \neq 3 \\ [J_3^2, I_2] & \text{if } p = 3 \end{cases}$$

(up to $\bar{G}$-conjugacy) where $\omega \in K$ is a primitive cube root of unity. Therefore $|x^G| > \frac{1}{4}q^{22}$ and the trivial bound $|x^G \cap H| \leqslant |H \cap \mathrm{PGL}(V)| < 6q^9$ is always sufficient. If $r = 2$ then without loss we may assume that $x \in B\pi$, where $\pi = (12) \in S_3$ fixes V_3. Evidently there are precisely three distinct B-classes of involutions in the coset $B\pi$, with representatives π, $(1,1,z)\pi$ and $(1,1,z')\pi$, where z and z' represent the two classes of involutions in $\mathrm{PGSp}_2(q)$. If x is B-conjugate to either $(1,1,z)\pi$ or $(1,1,z')\pi$ then x is $\bar{G}$-conjugate to $[-iI_4, iI_4]$, where $i \in K$ satisfies $i^2 = -1$. Therefore $|x^G| > \frac{1}{4}q^{20}$ and the bound $|x^G \cap H| < 6q^9$ is always sufficient. On the other hand, if x is B-conjugate to π then $|x^G| > \frac{1}{2}q^{12}$ since x is $\bar{G}$-conjugate to $[-I_2, I_6]$. In particular, $\pi = \pi_1$ is $\bar{G}$-conjugate to both $\pi_2 = (13)$ and $\pi_3 = (23)$ and therefore $|x^G \cap H| < 3q^3$ since $C_B(\pi_i) \cong \mathrm{PGSp}_2(q)^2$. The result now follows.

Finally, if $x \in H - \mathrm{PGL}(V)$ has prime order r then $q = q_0^r$,

$$|x^G \cap H| < |H| < \log_3 q.t!q^{\frac{t}{2}(a^2+a)}$$

and Corollary 3.49 gives $|x^G| > \frac{1}{4}q^{(a^{2t}+a^t)/4}$. These bounds are always sufficient. □

8 Proof of Theorem 1.1: $H \in \mathscr{C}_8$

In this final section we assume H is a maximal non-subspace subgroup in the classical collection $\mathscr{C}_8$. As advertised in §5, we also include the $\mathscr{C}_5$-subgroups of type $\mathrm{Sp}_n(q)$ and $\mathrm{O}_n^{\epsilon'}(q)$ in almost simple groups with socle $G_0 = \mathrm{PSU}_n(q)$. Therefore $G_0 = \mathrm{PSL}_n^{\epsilon}(q)$ and the cases to be considered are listed in Table 8.1 (see [18, Tables 4.5.A, 4.8.A]).

	type of H	conditions
(i)	$\mathrm{Sp}_n(q)$	n even
(ii)	$\mathrm{O}_n^{\epsilon'}(q)$	q odd
(iii)	$\mathrm{U}_n(q_0)$	$\epsilon = +$, $q = q_0^2$

Table 8.1: The collection $\mathscr{C}_8$

Proposition 8.1. *The conclusion to Theorem 1.1 holds in case (i) of Table 8.1.*

Proof. Here $\iota = 1/n$ (see Table 1.2) and so we may assume $n \geqslant 6$. Let σ be a Frobenius morphism of $\bar{G} = \mathrm{PSL}_n(K)$ such that $\bar{G}_\sigma$ has socle $G_0 = \mathrm{PSL}_n^{\epsilon}(q)$. Let $\bar{H} = \mathrm{PSp}_n(K)$ and observe that $H \cap \mathrm{PGL}(V) \leqslant \mathrm{PGSp}_n(q) = \widetilde{H}$.

Case 1. $x \in H \cap \mathrm{PGL}(V)$
Let $x \in H \cap \mathrm{PGL}(V)$ be an element of prime order r, so [6, Theorem 1] implies that

$$\dim x^{\bar{H}} \leqslant \left(\frac{1}{2} + \frac{1}{n}\right) \dim x^{\bar{G}}. \tag{38}$$

First suppose $r = p > 2$. Let $\lambda = (n^{a_n}, \ldots, 1^{a_1}) \vdash n$ denote the associated partition of x and let t be the number of non-zero terms a_j in λ (note that odd parts in λ must occur with an even multiplicity). Since p is odd, the $\bar{H}$-class of x is uniquely determined by λ and applying (38) we deduce that

$$|x^G \cap H| < 2^t q^{\left(\frac{1}{2}+\frac{1}{n}\right)\dim x^{\bar{G}}}, \quad |x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^t q^{\dim x^{\bar{G}}-1}. \tag{39}$$

If $t = 1$ then [6, 2.4] implies that $\dim x^{\bar{G}} \geqslant \frac{1}{2}n^2$ and these bounds are always sufficient. Now assume $t \geqslant 3$. Here the parity condition on the parts of λ implies that

$$n \geqslant 2\sum_{i=0}^{\alpha}(2i+1) + \sum_{i=1}^{t-1-\alpha} 2i \geqslant \frac{2}{3}t^2 + \frac{2}{3}t - \frac{1}{12},$$

where $\alpha = \lfloor (t-1)/3 \rfloor$, and if we assume $t \geqslant 3$ then the result follows via (39) since $\dim x^{\bar{G}} \geqslant g(n,t)$, where g is given in the statement of Lemma 3.25. If $t = 2$ and $\lambda \neq (2, 1^{n-2})$ then $\dim x^{\bar{G}} \geqslant 4n-8$ (minimal if $\lambda = (2^2, 1^{n-4})$) and (39) is sufficient unless $(n,q) = (6,3)$. Here we may assume $\lambda = (2^2, 1^2)$ (if not, then $\dim x^{\bar{G}} \geqslant 24$ and (39) is sufficient) and direct calculation yields $f(x,H) < .637$. Finally, if $\lambda = (2, 1^{n-2})$ then the bounds $|x^G \cap H| < q^n$ and $|x^G| > \frac{1}{2}(q+1)^{-1}q^{2n-3}$ are always sufficient.

Next assume $r = p = 2$. Then x is $\bar{G}$-conjugate to $[J_2^l, I_{n-2l}]$ for some integer $1 \leqslant l \leqslant n/2$ and applying Lemma 3.20 and Proposition 3.22 we deduce that

$$|x^G| > \frac{1}{2}(q+1)^{-1}q^{2l(n-l)+1}. \tag{40}$$

If l is odd then x is $\widetilde{H}$-conjugate to b_l, so $|x^G \cap H| < 2q^{l(n-l+1)}$ and (40) is always sufficient. Similarly, if l is even then Proposition 3.22 implies that $|x^G \cap H| < 2q^{l(n-l)} + 2q^{l(n-l+1)}$ and again the desired result follows via (40). The case $r = 2 < p$ is just as easy so assume $r \neq p$ and r is odd. If $C_{\bar{G}}(x)$ is non-connected then Lemma 3.34 implies that r divides n and the bounds

$$|x^G \cap H| < 2^{\frac{1}{2}(r-1)}q^{\frac{1}{2}(n^2+n)\left(1-\frac{1}{r}\right)}, \quad |x^G| > \frac{1}{2r}\left(\frac{q}{q+1}\right)^{r-1}q^{n^2\left(1-\frac{1}{r}\right)}$$

are always sufficient. Now suppose $C_{\bar{G}}(x)$ is connected. Let $i \geqslant 1$ be minimal such that $r|(q^i-1)$ and define the integers l and d as in Definition 3.32, and $c = c(i,\epsilon)$ as in the statement of Lemma 3.33. Observe that l is even (or zero) and d is even if c is odd. Then

$$|x^G| > \frac{1}{2}\left(\frac{q}{q+1}\right)^{\alpha d}q^{\dim x^{\bar{G}}},$$

where $\alpha = 1$ if $\epsilon = -$ and $i \equiv 2\,(4)$, otherwise $\alpha = 0$. Applying (38) we deduce that

$$|x^G \cap H| < \log_2 q . 2^{\frac{d}{2}\beta}q^{\left(\frac{1}{2}+\frac{1}{n}\right)\dim x^{\bar{G}}},$$

where $\beta = 0$ if i is even, otherwise $\beta = \frac{1}{2}(3-\epsilon)$. Now $n \geqslant l + dc$ and the reader can check that these bounds are always sufficient by applying the lower bound on $\dim x^{\bar{G}}$ from Lemma 3.33.

Case 2. $x \in H - \mathrm{PGL}(V)$

If x is a field automorphism of prime order r then $q = q_0^r$ and (20) holds. The result now follows since $x^G \cap H \subseteq \widetilde{H}x$ (see Lemma 3.50) and Proposition 3.43 implies that

$$|x^G \cap H| \leqslant |\mathrm{Sp}_n(q) : \mathrm{Sp}_n(q^{1/r})| < 2q^{\frac{1}{2}n(n+1)\left(1-\frac{1}{r}\right)}.$$

The same bounds hold (with $r = 2$) if x is an involutory graph-field automorphism. To complete the proof, let us assume x is an involutory graph automorphism of G_0, so

$$|x^G| > \frac{1}{2}(q+1)^{-1}q^{\frac{1}{2}(n^2+\alpha n-2)}, \tag{41}$$

where $\alpha = 1$ if x is non-symplectic, otherwise $\alpha = -1$. Let γ be a symplectic-type graph automorphism of G_0 which centralizes $\widetilde{H}$. If we identify $\mathrm{GL}_n \leqslant \mathrm{Sp}_{2n}$ as the stabilizer of a maximal totally singular subspace then we may assume that

$$\gamma = \begin{pmatrix} & J \\ -J & \end{pmatrix} \in \mathrm{Sp}_{2n}, \quad \text{where } J = \begin{pmatrix} & I_{n/2} \\ -I_{n/2} & \end{pmatrix} \in \mathrm{Sp}_n$$

and J is written with respect to the specific ordering $\{e_1, \ldots, e_{n/2}, f_1, \ldots, f_{n/2}\}$ of a standard symplectic basis for V. First assume $C_{G_0}(x)$ is symplectic. Then $x^G \cap H \subseteq \{h \in I_2(\widetilde{H}) : h\gamma \sim \gamma\}$, where the relation $\sim$ signifies $\bar{G}_\sigma$-conjugacy and $I_2(\widetilde{H})$ denotes the set of elements $h \in \widetilde{H}$

such that $h^2 = 1$. Now if q is odd and $h \in I_2(\widetilde{H})$ satisfies $C_{\bar{H}}(h)^0 = \mathrm{GL}_{n/2}$ then we may view h as the block diagonal matrix $[J, J] \in \mathrm{Sp}_{2n}$ and we deduce that $C_{G_0}(h\gamma)$ is orthogonal since

$$h\gamma = \begin{pmatrix} & -I_n \\ I_n & \end{pmatrix} \in \mathrm{Sp}_{2n}.$$

In fact, we see that $h\gamma$ is an orthogonal-type graph automorphism if and only if $C_{\bar{H}}(h)^0 = \mathrm{GL}_{n/2}$. Therefore

$$|x^G \cap H| < \sum_{j=0}^{\lfloor n/4 \rfloor} 2q^{2j(n-2j)} < 2\left(\frac{q^2}{q^2-1}\right) q^{\frac{1}{4}n^2} \tag{42}$$

and (41) is always sufficient. Now assume $p = 2$. Here $h\gamma \sim \gamma$ if and only if $h\gamma \in \mathrm{Sp}_{2n}$ is conjugate to a_n and this is true if and only if h is an a-type involution. Therefore (42) holds and (41) is sufficient unless $(n, q) = (6, 2)$, where direct calculation yields $f(x, H) < .658$. Finally, if x is non-symplectic then the desired result follows via (41) since

$$|x^G \cap H| < \sum_{j=0}^{n/2} 2q^{j(n-j+1)} < 2\left(\frac{q^2}{q^2-1}\right) q^{\frac{1}{4}n(n+2)}.$$

□

Proposition 8.2. *The conclusion to Theorem 1.1 holds in case (ii) of Table 8.1.*

Proof. Here q is odd (see Table 8.1) and we may assume $n \geqslant 3$. Define $\bar{G} = \mathrm{PSL}_n(K)$, $\bar{H} = \mathrm{PSO}_n(K)$ and let σ be a Frobenius morphism of $\bar{G}$ such that $\bar{G}_\sigma$ has socle $G_0 = \mathrm{PSL}_n^\epsilon(q)$. Observe that $H \cap \mathrm{PGL}(V) \leqslant \mathrm{PGO}_n^{\epsilon'}(q) = \widetilde{H}$. If $x \in H \cap \mathrm{PGL}(V)$ then we proceed as in the proof of Proposition 8.1 and the reader is left to make the necessary minor adjustments. For the remainder we will assume $x \in H - \mathrm{PGL}(V)$ has prime order r.

If x is a field automorphism of prime order r then $q = q_0^r$, (20) holds and Lemma 3.50 implies that $x^G \cap H \subseteq \widetilde{H}x$. Moreover, if either n or r is odd then $x^G \cap H \subseteq \widehat{H}x$, where $\widehat{H} = \mathrm{Inndiag}(\mathrm{P}\Omega_n^{\epsilon'}(q))$, and the desired result follows since Proposition 3.43 implies that

$$|x^G \cap H| \leqslant |\mathrm{O}_n^{\epsilon'}(q) : \mathrm{O}_n^{\epsilon'}(q^{1/r})| < 2q^{\frac{1}{2}n(n-1)(1-\frac{1}{r})}.$$

Now assume both n and r are even, in which case $\epsilon = +$ (see Remark 3.42). If $\epsilon' = +$ then Proposition 3.43 gives

$$|x^G \cap H| \leqslant |\mathrm{O}_n^+(q) : \mathrm{O}_n^+(q^{1/2})| + |\mathrm{O}_n^+(q) : \mathrm{O}_n^-(q^{1/2})| < 4q^{\frac{1}{4}n(n-1)}$$

and the result follows via (20). On the other hand, if $\epsilon' = -$ then x induces an inner automorphism on $\widetilde{H}$ and again (20) is sufficient since Lemma 3.14 implies that

$$|x^G \cap H| \leqslant i_2(\widetilde{H}) + 1 \leqslant 2(1 + q^{-1})q^{\frac{1}{4}n^2}.$$

Similar reasoning applies when x is an involutory graph-field automorphism.

To complete the proof, let us assume x is an involutory graph automorphism. Let γ be an orthogonal graph automorphism of G_0 which centralizes $\widetilde{H}$. Now, if $C_{G_0}(x)$ is orthogonal (which must be the case if n is odd) then Lemma 3.14 implies that

$$|x^G \cap H| \leqslant i_2(\widetilde{H}) + 1 \leqslant 2(1 + q^{-1})q^{\frac{1}{4}(n^2-\zeta)},$$

where $n \equiv \zeta\,(2)$. This bound with (41) is sufficient unless $(n, q) = (3, 3)$, where $f(x, H) < .423$ since $i_2(\widetilde{H}) = 9$ and $|x^G| \geqslant |\mathrm{SL}_3(3) : \mathrm{SO}_3(3)| = 234$. Finally, if n is even and $C_{G_0}(x)$ is symplectic then $|x^G \cap H|$ is at most the number of involutions $h \in \widetilde{H}$ such that $h\gamma \in G$ is a symplectic graph automorphism. Identifying $\mathrm{GL}_n \leqslant \mathrm{Sp}_{2n}$ we may assume

$$\gamma = \begin{pmatrix} & I_n \\ -I_n & \end{pmatrix} \in \mathrm{Sp}_{2n}$$

and arguing as in the proof of the previous proposition we deduce that $h\gamma$ is a symplectic-type graph automorphism if and only if $C_{\bar{H}}(h)^0 = \mathrm{GL}_{n/2}$. Therefore $|x^G \cap H| < 3q^{n(n-2)/4}$ and (41) is sufficient for all $n \geqslant 6$. If $n = 4$ then we may assume $\epsilon' = +$ (see Proposition 3.37) and we calculate that $f(x, H) < .711$ for all $q \geqslant 3$ since

$$|x^G \cap H| \leqslant \frac{|\mathrm{SO}_4^+(q)|}{|\mathrm{GL}_2(q)|} + \frac{|\mathrm{SO}_4^+(q)|}{|\mathrm{GU}_2(q)|} = 2q^2, \;\; |x^G| \geqslant \frac{|\mathrm{PSL}_4(q)|}{|\mathrm{Sp}_4(q)|} \geqslant \frac{1}{4}q^2(q^3 - 1).$$

□

Proposition 8.3. *The conclusion to Theorem 1.1 holds in case (iii) of Table 8.1.*

Proof. We may assume $n \geqslant 3$. Let σ_0 be a Frobenius morphism of $\bar{G} = \mathrm{PSL}_n(K)$ such that $\bar{G}_{\sigma_0} = \mathrm{PGL}_n(q_0)$ and let γ denote the inverse-transpose graph automorphism of $\bar{G}$. Then

$$H \cap \mathrm{PGL}(V) \leqslant \bar{G}_{\sigma_0\gamma} = \mathrm{PGU}_n(q_0) < \mathrm{PGL}_n(q) = \bar{G}_\sigma,$$

where $\sigma = \sigma_0^2$ and $q = q_0^2$. The argument for elements $x \in H \cap \mathrm{PGL}(V)$ is straightforward. For example, suppose x has odd prime order $r \neq p$ and $C_{\bar{G}}(x)$ is connected. Let $i \geqslant 1$ (resp. $i_0 \geqslant 1$) be minimal such that $r|(q^i - 1)$ (resp. $r|(q_0^{i_0} - 1)$) and observe that $i = i_0/2$ if i_0 is even, otherwise $i = i_0$. Define the integers l and d as in Definition 3.32 (with respect to σ-orbits) and note that each non-trivial $\sigma_0\gamma$-orbit is a union of two distinct σ-orbits if $i_0 \not\equiv 2\,(4)$, whereas $\sigma_0\gamma$- and σ-orbits coincide if $i_0 \equiv 2\,(4)$. In particular, d is even if $i_0 \not\equiv 2\,(4)$ and we deduce that

$$|x^G \cap H| < 2^{1-\alpha}\log_2 q_0.2^{\frac{\alpha d}{2}+1}q_0^{\dim x^{\bar{G}}},$$

where $\alpha = 0$ if $i_0 \equiv 2\,(4)$, otherwise $\alpha = 1$. Now $|x^G| > \frac{1}{2}q_0^{2\dim x^{\bar{G}}}$ and the result follows by applying the lower bound on $\dim x^{\bar{G}}$ given in Lemma 3.33 (with $c = i$).

Now suppose $x \in H - \mathrm{PGL}(V)$. If $x \in G$ is a field automorphism of odd prime order r then $q_0 = q_1^r$ and the bounds

$$|x^G \cap H| < 2q_0^{(n^2-1)\left(1-\frac{1}{r}\right)}, \;\; |x^G| > \frac{1}{2}q_0^{2(n^2-1)\left(1-\frac{1}{r}\right)-2}$$

obtained via Proposition 3.43 are always sufficient. If $\phi \in G$ is an involutory field automorphism then $\phi^G \cap H \subseteq \widetilde{H}\phi$ (see Lemma 3.50) and ϕ induces an involutory graph automorphism on $\widetilde{H} = \mathrm{PGU}_n(q_0)$. Applying Lemma 3.14 we deduce that

$$|\phi^G \cap H| \leqslant i_2(\mathrm{Aut}(\mathrm{PSU}_n(q_0))) < 2(1 + q_0^{-1})q_0^{\frac{1}{2}(n^2+n-2)}. \tag{43}$$

Similarly, if $\psi \in G$ is an involutory graph-field automorphism then we may assume ψ centralizes $\widetilde{H}$, whence $|\psi^G \cap H| \leqslant i_2(\widetilde{H}) + 1$ and again (43) holds (with ϕ replaced by ψ). Now if $x = \phi$ or ψ then $|x^G| > \frac{1}{2}(n, q_0^2 - 1)^{-1}q_0^{n^2-1}$ and one can check that (43) is sufficient unless $(n, q_0) \in \{(4, 3), (4, 2), (3, 4), (3, 2)\}$. Let us assume (n, q_0) is one of these exceptional cases. Now

$$|x^G| \geqslant (n, q_0^2 - 1)^{-1}q_0^{\frac{1}{2}n(n-1)}\prod_{j=2}^{n}(q_0^j + \beta^j),$$

where $\beta = 1$ if $x = \phi$, $\beta = -1$ if $x = \psi$, and we calculate that (43) is sufficient unless $(n, q_0) = (3, 2)$. Here $f(\phi, H) < .609$ since

$$|x^G \cap H| = 3^\zeta|\mathrm{PSU}_3(2) : \Omega_3(2)| = 3^\zeta.12, \;\; |x^G| = 3^{\zeta-1}|\mathrm{PGL}_3(4) : \mathrm{PGL}_3(2)| = 3^\zeta.120,$$

where $\zeta = 1$ if $\mathrm{PGL}_3(4) \leqslant G$, otherwise $\zeta = 0$. Similarly, for ψ we have $f(\psi, H) < .409$ since $|\psi^G \cap H| \leqslant i_2(\mathrm{PGU}_3(2)) + 1 = 10$ and $|\psi^G| \geqslant 280$.

Finally, let us assume $x \in G$ is an involutory graph automorphism of G_0, so

$$|x^G| > \frac{1}{2n} q_0^{n^2+\alpha n-2}, \tag{44}$$

where $\alpha = 1$ if x is non-symplectic, otherwise $\alpha = -1$. Then $x^G \cap H \subseteq \widetilde{H}x$ and each $y \in x^G \cap H$ induces a graph automorphism on $\mathrm{PSU}_n(q_0)$ such that the centralizers $C_{\mathrm{PSU}_n(q_0)}(y)$ and $C_{G_0}(x)$ are of the same type. If x is non-symplectic (which must be the case if n is odd) then the bounds $|x^G \cap H| < 2q_0^{(n^2+n-2)/2}$ and (44) are always sufficient; otherwise $|x^G \cap H| < 2q_0^{(n^2-n-2)/2}$ and we are left to deal with the case $(n, q_0) = (4, 2)$. Here we calculate that $f(x, H) < .519$ since $|x^G \cap H| = |\mathrm{SU}_4(2) : \mathrm{Sp}_4(2)| = 36$ and $|x^G| = |\mathrm{SL}_4(4) : \mathrm{Sp}_4(4)| = 1008$. □

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] T.C. Burness, *Fixed point ratios in actions of finite classical groups,* I, to appear.

[4] ———, *Fixed point ratios in actions of finite classical groups,* III, to appear.

[5] ———, *Fixed point ratios in actions of finite classical groups,* IV, to appear.

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

[7] R.W. Carter, *Simple Groups of Lie Type*, Wiley, 1972.

[8] ———, *Finite Groups of Lie Type: Conjugacy Classes and Characters*, Wiley Interscience, 1985.

[9] J. Conway, R. Curtis, S. Norton, R. Parker, and R. Wilson, *Atlas of Finite Groups*, Oxford University Press, 1985.

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

[11] 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.

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

[13] J. Hall, M.W. Liebeck, and G.M. Seitz, *Generators for finite simple groups with applications to linear groups*, Quart. J. Math. Oxford **43** (1992), 441–458.

[14] A. Hulpke, private communication, 2005.

[15] I.M. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976.

[16] W. Kantor, *Subgroups of classical groups generated by long root elements*, Trans. Amer. Math. Soc. **248** (1979), 347–379.

[17] 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.

[18] 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.

[19] 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.

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

[21] P. Neumann and C. Praeger, *Cyclic matrices over finite fields*, J. London Math. Soc. **52** (1995), 263–284.

[22] T.A. Springer and R. Steinberg, *Conjugacy Classes*, Seminar on Algebraic Groups and Related Topics (A. Borel et al., ed.), Lecture Notes in Math., vol. 131, Springer, Berlin, 1970, pp. 168–266.

[23] R. Steinberg, *Endomorphisms of linear algebraic groups*, Mem. Amer. Math. Soc. **80** (1968).

[24] ———, *Lectures on Chevalley groups*, Yale University Mathematics Department, 1968.

[25] G.E. Wall, *On the conjugacy classes in the unitary, symplectic and orthogonal groups*, J. Austral. Math. Soc. **3** (1963), 1–62.