# LOCALLY ELUSIVE CLASSICAL GROUPS

TIMOTHY C. BURNESS AND MICHAEL GIUDICI

ABSTRACT. Let $G$ be a transitive permutation group of degree $n$ with point stabiliser $H$ and let $r$ be a prime divisor of $n$. We say that $G$ is $r$-elusive if it does not contain a derangement of order $r$. The problem of determining the $r$-elusive primitive groups can be reduced to the almost simple case, and the purpose of this paper is to complete the study of $r$-elusivity for almost simple classical groups. Building on our earlier work for geometric actions of classical groups, in this paper we handle the remaining non-geometric actions where $H$ is almost simple and irreducible. This requires a completely different approach, using tools from the representation theory of quasisimple groups.

## 1. INTRODUCTION

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group on a finite set $\Omega$ of size at least 2. By the Orbit-Counting Lemma, $G$ contains elements that act fixed-point-freely on $\Omega$. Such elements are called *derangements*, and their existence turns out to have some interesting applications in many areas of mathematics, such as number theory and topology (see Serre's article [34]).

By a theorem of Fein, Kantor and Schacher [12], $G$ contains a derangement of prime power order (the proof requires the Classification of Finite Simple Groups). In fact, in most cases, $G$ contains a derangement of prime order, but there are some exceptions, such as the 3-transitive action of the smallest Mathieu group $\mathrm{M}_{11}$ on 12 points. The transitive permutation groups with this property are called *elusive* groups, and they have been extensively studied in recent years (see [11, 14, 15, 16, 37], for example).

A local notion of elusivity was introduced in [10]. For a prime divisor $r$ of $|\Omega|$, we say that $G$ is $r$-*elusive* if it does not contain a derangement of order $r$ (so $G$ is elusive if and only if it is $r$-elusive for all such primes $r$). In [10], the O'Nan-Scott theorem is used to essentially reduce the problem of determining the $r$-elusive primitive groups to the almost simple case, and the examples with an alternating or sporadic socle are identified in [10]. Therefore, it remains to determine the $r$-elusive primitive almost simple groups of Lie type and our goal in this paper is to complete the picture for classical groups (the locally elusive exceptional groups of Lie type will be the subject of a future paper).

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple classical group over $\mathbb{F}_q$ with socle $T$ and point stabiliser $H$. Let $V$ be the natural module for $T$ and write $n = \dim V$ and $q = p^f$, where $p$ is a prime. Note that $H$ is a maximal subgroup of $G$ with $G = HT$. Roughly speaking, Aschbacher's subgroup structure theorem [1] states that either $H$ belongs to one of eight natural, or *geometric*, subgroup collections (denoted by $\mathcal{C}_1, \ldots, \mathcal{C}_8$), or $H$ is almost simple and acts irreducibly on $V$. The geometric subgroups include the stabilisers of appropriate subspaces and direct sum and tensor product decompositions of $V$ (see [9, Table 1.4.2] for a brief description of the subgroups in each $\mathcal{C}_i$ collection). We write $\mathcal{S}$ for the collection of almost simple irreducible subgroups arising in Aschbacher's theorem (see Definition 2.10 for the precise definition of $\mathcal{S}$), and we say that the action of $G$ on $\Omega$ is an $\mathcal{S}$-*action* if $H \in \mathcal{S}$. We will write $S$ for the socle of a subgroup $H \in \mathcal{S}$.

A detailed analysis of the structure, maximality and conjugacy of the geometric sub-groups of $G$ is provided in [25]. This is used extensively in our study of the $r$-elusive geometric actions of almost simple classical groups in [9] (see [9, Section 1.5] for a summary of the main results), which is organised according to Aschbacher's theorem. This approach relies on the fact that there is a concrete description of the embedding of each geometric subgroup $H$ in $G$, which permits a detailed study of the fusion of the conjugacy classes of $H$ in $G$. This sort of information is not readily available when $H \in \mathcal{S}$ is a non-geometric subgroup of $G$, so a different approach is required. For example, it is not even possible to list all the subgroups in $\mathcal{S}$ of a given classical group, in general (of course, we do not even know the dimensions of all irreducible representations of simple groups). However, detailed information is available for the low-dimensional groups with $n \leqslant 12$ (see [4]), which we use in [9, Section 6.3] to determine the $r$-elusive $\mathcal{S}$-actions for $n \leqslant 5$. In this paper, our aim is to complete the study of $\mathcal{S}$-actions initiated in [9] by extending the analysis to all classical groups.

In order to state our main result (Theorem 1 below), we need to introduce two subcollections of $\mathcal{S}$, which we denote by the symbols $\mathcal{A}$ and $\mathcal{B}$. A subgroup $H \in \mathcal{S}$ with socle $S$ belongs to the collection $\mathcal{A}$ if and only if $S$ is an alternating group, $q = p$ is prime and $V$ is the fully deleted permutation module for $S$ over $\mathbb{F}_p$ (see Table 1). The collection $\mathcal{B}$ is recorded in Table 2. We need to highlight these specific cases in order to state an important theorem of Guralnick and Saxl [18, Theorem 7.1] on irreducible subgroups of classical groups (see Theorem 2.11), which plays a key role in our proof of Theorem 1.

**Remark 1.** Let us make a couple of comments on the cases in Tables 1 and 2.

(i) Consider Case ($\mathcal{A}$1) in Table 1. Here $S = A_d$ and $T = \mathrm{P}\Omega_n^\epsilon(p)$, where $d \geqslant 8$, $p$ is an odd prime and $n = d - \delta$, with $\delta = 2$ if $p$ divides $d$, otherwise $\delta = 1$. If $n$ is even then $\epsilon = +$ if and only if

$$\left(\frac{n+1}{p}\right) = (-1)^{\frac{1}{4}n(p-1)}$$

(see Section 3).

(ii) In Table 2 we write $L(\lambda)$ for the unique irreducible $\mathbb{F}_q\hat{S}$-module of highest weight $\lambda$ (up to quasiequivalence, where $\hat{S}$ denotes the full covering group of $S$), and we follow Bourbaki [3] in labelling the fundamental dominant weights $\lambda_i$. We also note that the conditions recorded in the final column of Table 2 are necessary, but not always sufficient, for the existence and maximality of $H$ in $G$; for the precise conditions, we refer the reader to the relevant tables in [4, Section 8.2].

Let $r \neq p$ be a prime and let $i \geqslant 1$ be minimal such that $r$ divides $q^i - 1$. As above, let $n$ be the dimension of the natural module for $T$ and set

$$c = \begin{cases} 2i & \text{if } i \text{ is odd and } T \neq \mathrm{PSL}_n(q) \\ i/2 & \text{if } i \equiv 2 \pmod 4 \text{ and } T = \mathrm{PSU}_n(q) \\ i & \text{otherwise} \end{cases} \tag{1}$$

as in [9]. We also introduce the following notation:

$$\kappa(T, r) \text{ is the number of conjugacy classes of subgroups of order } r \text{ in } T \tag{2}$$

and we highlight the following conditions

$$r \neq p, \ r > 2, \ r \text{ divides } |H \cap T| \text{ and either } c > n/2, \text{ or } c = n/2 \text{ and } T = \mathrm{P}\Omega_n^-(q). \tag{$\star$}$$

Note that if $r$ divides $|\Omega|$ and all the conditions in ($\star$) hold then $\kappa(T, r) = 1$ and thus $T$ is $r$-elusive (see Lemma 2.4 and Corollary 2.7).

| Case | $T$ | | Conditions |
|------|-----|--|-----------|
| ($\mathcal{A}$1) | $\begin{cases} \mathrm{P\Omega}^\epsilon_{d-1}(p) & \text{if } (d,p)=1 \\ \mathrm{P\Omega}^\epsilon_{d-2}(p) & \text{otherwise} \end{cases}$ | | $d \geqslant 8$, $p \neq 2$ |
| ($\mathcal{A}$2) | $\mathrm{Sp}_{d-2}(2)$ | | $d \geqslant 10$, $d \equiv 2 \pmod 4$, $p = 2$ |
| ($\mathcal{A}$3) | $\begin{cases} \Omega^+_{d-2}(2) & \text{if } d \equiv 0 \pmod 8 \\ \Omega^-_{d-2}(2) & \text{if } d \equiv 4 \pmod 8 \end{cases}$ | | $d \geqslant 12$, $d \equiv 0 \pmod 4$, $p = 2$ |
| ($\mathcal{A}$4) | $\begin{cases} \Omega^+_{d-1}(2) & \text{if } d \equiv \pm 1 \pmod 8 \\ \Omega^-_{d-1}(2) & \text{if } d \equiv \pm 3 \pmod 8 \end{cases}$ | | $d \geqslant 9$, $d$ odd, $p = 2$ |

TABLE 1. The collection $\mathcal{A}$, $S = A_d$

| Case | $T$ | $S$ | Conditions |
|------|-----|-----|-----------|
| ($\mathcal{B}$1) | $\mathrm{PSp}_{10}(p)$ | $\mathrm{PSU}_5(2)$ | $p \neq 2$ |
| ($\mathcal{B}$2) | $\mathrm{P\Omega}^+_8(q)$ | $\begin{cases} \Omega_7(q) & p > 2 \\ \mathrm{Sp}_6(q) & p = 2 \end{cases}$ | |
| ($\mathcal{B}$3) | $\mathrm{P\Omega}^+_8(q)$ | $^3D_4(q_0)$ | $q = q_0^3$ |
| ($\mathcal{B}$4) | $\mathrm{P\Omega}^+_8(p)$ | $\Omega^+_8(2)$ | $p \neq 2$ |
| ($\mathcal{B}$5) | $\mathrm{PSL}^\epsilon_7(p)$ | $\mathrm{PSU}_3(3)$ | $p \equiv \epsilon \pmod 3$, $p \geqslant 5$ |
| ($\mathcal{B}$6) | $\begin{cases} \Omega_7(q) & p > 2 \\ \mathrm{Sp}_6(q) & p = 2 \end{cases}$ | $G_2(q)$ | $q > 2$, $V = L(\lambda_1)$ |
| ($\mathcal{B}$7) | $\Omega_7(q)$ | $G_2(q)$ | $p = 3$, $V = L(\lambda_2)$ |
| ($\mathcal{B}$8) | $\Omega_7(p)$ | $\mathrm{Sp}_6(2)$ | $p \neq 2$ |
| ($\mathcal{B}$9) | $\mathrm{PSL}^\epsilon_6(q)$ | $\mathrm{PSL}^\epsilon_3(q)$ | $p \neq 2$, $V = L(2\lambda_1)$ |
| ($\mathcal{B}$10) | $\mathrm{PSL}^\epsilon_6(q)$ | $A_7$ | $q \leqslant p^2$, $p \equiv \epsilon \pmod 3$, $p \geqslant 5$ |
| ($\mathcal{B}$11) | $\mathrm{PSL}^\epsilon_6(q)$ | $A_6$ | $q \leqslant p^2$, $p \equiv \epsilon \pmod 3$, $p \geqslant 5$ |
| ($\mathcal{B}$12) | $\mathrm{PSL}^\epsilon_6(p)$ | $\mathrm{PSL}_3(4)$ | $p \equiv \epsilon \pmod 3$, $p \geqslant 5$ |
| ($\mathcal{B}$13) | $\mathrm{PSL}^\epsilon_6(p)$ | $\mathrm{PSU}_4(3)$ | $p \equiv \epsilon \pmod 3$, $p \geqslant 5$ |
| ($\mathcal{B}$14) | $\mathrm{PSL}_6(3)$ | $\mathrm{M}_{12}$ | |
| ($\mathcal{B}$15) | $\mathrm{PSU}_6(2)$ | $\mathrm{PSU}_4(3)$ | |
| ($\mathcal{B}$16) | $\mathrm{PSU}_6(2)$ | $\mathrm{M}_{22}$ | |
| ($\mathcal{B}$17) | $\mathrm{PSp}_6(q)$ | $\mathrm{J}_2$ | $q \leqslant p^2$, $p \geqslant 3$ |
| ($\mathcal{B}$18) | $\mathrm{PSp}_6(p)$ | $\mathrm{PSU}_3(3)$ | $p \neq 3$ |

TABLE 2. The collection $\mathcal{B}$

**Theorem 1.** *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple classical group with socle $T$ and point stabiliser $H \in \mathcal{S}$. Let $S$ denote the socle of $H$ and let $n$ be the dimension of the natural $T$-module. Let $r$ be a prime divisor of $|\Omega|$. Then $T$ is $r$-elusive if and only if one of the following holds:*

(i) *$n < 6$ and $(T, S, r)$ is one of the cases recorded in Table 3;*

(ii) *$n \geqslant 6$, $H \in \mathcal{A}$ and one of the following holds:*

    (a) *$r = 2$, $p \neq 2$, $T = \Omega_n(p)$ and $\left( \frac{(n+1)/2}{p} \right) = 1$;*

    (b) *$r = 2$, $p \neq 2$, $T = \mathrm{P\Omega}^\epsilon_n(p)$, $n \equiv 2 \pmod 4$ and $p \equiv 5\epsilon \pmod 8$;*

    (c) *$r \neq p$, $r > 2$, $r$ divides $|H \cap T|$ and $c = r - 1$;*

(iii) *$n \geqslant 6$, $H \in \mathcal{B}$ and $(T, S, r)$ is one of the cases recorded in Table 4;*

(iv) $n \geqslant 6$, $H \notin \mathcal{A} \cup \mathcal{B}$ and all the conditions in $(\star)$ hold.

**Remark 2.** As previously remarked, the $r$-elusive $\mathcal{S}$-actions with $n < 6$ are determined in [9, Proposition 6.3.1]. The relevant cases are listed in Table 3, where the final column records necessary and sufficient conditions for the $r$-elusivity of $T$ (in particular, the given conditions ensure that $r$ divides $|\Omega|$). These are additional to the conditions needed for the existence and maximality of $H$ in $G$, which can be read off from the relevant tables in [4, Section 8.2], or from [9, Table 6.3.1]. Similarly, we refer the reader to Remark 4.2 for further information on the conditions recorded in the final column of Table 4.

**Remark 3.** Note that $r^2$ must divide $q^c - 1$ if $(T, S, r)$ is an example arising in part (iv) of Theorem 1. It is easy to see that there are genuine examples. For example, take $T = \mathrm{P\Omega}_{12}^+(p)$, $S = \mathrm{PSL}_2(11)$ and $r = 11$, where $p$ is a prime such that $p \equiv -1 \pmod{605}$, so $c = 10$ and [4, Table 8.83] indicates that $S$ is a maximal subgroup of $T$. Note that there are infinitely many primes of this form by Dirichlet's theorem.

| $T$ | $S$ | $r$ | Conditions |
|---|---|---|---|
| $\mathrm{PSL}_5^\epsilon(q)$ | $\mathrm{PSU}_4(2)$ | 2 | |
| | | 5 | $q^2 \equiv -1 \pmod{25}$ |
| | $\mathrm{PSL}_2(11)$ | 5 | $q^2 \equiv -1 \pmod{25}$ |
| | | 11 | $q \not\equiv \epsilon \pmod{11}$, $q^5 \equiv \epsilon \pmod{121}$ |
| | $\mathrm{M}_{11}$ | 11 | $(\epsilon, q) = (+, 3)$ |
| $\mathrm{PSL}_4^\epsilon(q)$ | $\mathrm{PSU}_4(2)$ | 2 | $q \not\equiv \epsilon \pmod{8}$ |
| | | 3 | $q \equiv \epsilon \pmod{9}$ |
| | | 5 | $q^2 \equiv -1 \pmod{25}$ |
| | $A_7$ | 2 | $q \equiv 5\epsilon \pmod{8}$ |
| | | 3 | $q \equiv -\epsilon \pmod{9}$ |
| | | 5 | $q^2 \equiv -1 \pmod{25}$ |
| | | 7 | $q(q + \epsilon) \equiv -1 \pmod{49}$ |
| | $\mathrm{PSL}_2(7)$ | 2 | $q \equiv 5\epsilon \pmod{8}$ |
| | | 7 | $q(q + \epsilon) \equiv -1 \pmod{49}$ |
| | $\mathrm{PSL}_3(4)$ | 2 | $(\epsilon, q) = (-, 3)$ |
| $\mathrm{PSp}_4(q)'$ | $A_6$ | 2 | $q \equiv \pm 1 \pmod{12}$ |
| | | 3 | $q^2 \equiv 1 \pmod{9}$ |
| | | 5 | $q^2 \equiv -1 \pmod{25}$ |
| | $A_7$ | 5 | $q = 7$ |
| $\mathrm{PSL}_3^\epsilon(q)$ | $\mathrm{PSL}_2(7)$ | 2 | |
| | | 3 | $q \equiv 4\epsilon, 7\epsilon, 8\epsilon \pmod{9}$ |
| | | 7 | $q \equiv -\epsilon \pmod{49}$ or $q(q + \epsilon) \equiv -1 \pmod{49}$ |
| | $A_6$ | 2 | $(\epsilon, q) \neq (-, 5)$ |
| | | 5 | $q \equiv -\epsilon \pmod{25}$ |
| | $A_7$ | 2 | $(\epsilon, q) = (-, 5)$ |
| $\mathrm{PSL}_2(q)$ | $A_5$ | 2 | $q \equiv \pm 1 \pmod{8}$ |
| | | 3, 5 | $q \equiv \pm 1 \pmod{r^2}$ |

TABLE 3. The $r$-elusive $\mathcal{S}$-actions, $n < 6$

**Corollary 1.** *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple classical group with socle $T$ and point stabiliser $H \in \mathcal{S}$. Let $S$ denote the socle of $H$ and let $n$ be the dimension of the*

| Case | $T$ | $S$ | $r$ | Conditions |
|------|-----|-----|-----|-----------|
| ($\mathcal{B}1$) | $\mathrm{PSp}_{10}(p)$ | $\mathrm{PSU}_5(2)$ | 2 | $p \equiv \pm1 \;(\mathrm{mod}\ 8)$ |
| | | | 11 | $p^2 \not\equiv 1 \;(\mathrm{mod}\ 11)$, $p^5 \equiv \pm1 \;(\mathrm{mod}\ 121)$ |
| ($\mathcal{B}4$) | $\mathrm{P}\Omega_8^+(p)$ | $\Omega_8^+(2)$ | 2 | $p \geqslant 7$ |
| | | | 3 | $p^2 \equiv 1 \;(\mathrm{mod}\ 9)$ |
| | | | 5 | $p^2 \equiv -1 \;(\mathrm{mod}\ 25)$ |
| | | | 7 | $p^2 \not\equiv 1 \;(\mathrm{mod}\ 7)$, $p^3 \equiv \pm1 \;(\mathrm{mod}\ 49)$ |
| ($\mathcal{B}5$) | $\mathrm{PSL}_7^\epsilon(p)$ | $\mathrm{PSU}_3(3)$ | 7 | $p^2 \not\equiv 1 \;(\mathrm{mod}\ 7)$, $p^3 \equiv -\epsilon \;(\mathrm{mod}\ 49)$ |
| ($\mathcal{B}8$) | $\Omega_7(p)$ | $\mathrm{Sp}_6(2)$ | 2 | $p \geqslant 7$ |
| | | | 3 | $p^2 \equiv 1 \;(\mathrm{mod}\ 9)$ |
| | | | 5 | $p^2 \equiv -1 \;(\mathrm{mod}\ 25)$ |
| | | | 7 | $p^2 \not\equiv 1 \;(\mathrm{mod}\ 7)$, $p^3 \equiv \pm1 \;(\mathrm{mod}\ 49)$ |
| ($\mathcal{B}10$) | $\mathrm{PSL}_6^\epsilon(q)$ | $A_7$ | 5 | $q^2 \equiv -1 \;(\mathrm{mod}\ 25)$ |
| | | | 7 | $q^2 \not\equiv 1 \;(\mathrm{mod}\ 7)$, $q^3 \equiv -\epsilon \;(\mathrm{mod}\ 49)$ |
| ($\mathcal{B}11$) | $\mathrm{PSL}_6^\epsilon(q)$ | $A_6$ | 5 | $q^2 \equiv -1 \;(\mathrm{mod}\ 25)$ |
| ($\mathcal{B}12$) | $\mathrm{PSL}_6^\epsilon(p)$ | $\mathrm{PSL}_3(4)$ | 2 | $p \equiv -5\epsilon \;(\mathrm{mod}\ 24)$ |
| | | | 5 | $p^2 \equiv -1 \;(\mathrm{mod}\ 25)$ |
| | | | 7 | $p^2 \not\equiv 1 \;(\mathrm{mod}\ 7)$, $p^3 \equiv -\epsilon \;(\mathrm{mod}\ 49)$ |
| ($\mathcal{B}13$) | $\mathrm{PSL}_6^\epsilon(p)$ | $\mathrm{PSU}_4(3)$ | 2 | $p \equiv \epsilon \;(\mathrm{mod}\ 12)$ |
| | | | 5 | $p^2 \equiv -1 \;(\mathrm{mod}\ 25)$ |
| | | | 7 | $p^2 \not\equiv 1 \;(\mathrm{mod}\ 7)$, $p^3 \equiv -\epsilon \;(\mathrm{mod}\ 49)$ |
| ($\mathcal{B}14$) | $\mathrm{PSL}_6(3)$ | $\mathrm{M}_{12}$ | $2, 11$ | |
| ($\mathcal{B}15$) | $\mathrm{PSU}_6(2)$ | $\mathrm{PSU}_4(3)$ | 2 | |
| ($\mathcal{B}17$) | $\mathrm{PSp}_6(q)$ | $\mathrm{J}_2$ | 2 | $q^2 \equiv 1 \;(\mathrm{mod}\ 8)$ |
| | | | 5 | $q^2 \equiv -1 \;(\mathrm{mod}\ 125)$ |
| | | | 7 | $q^2 \not\equiv 1 \;(\mathrm{mod}\ 7)$, $q^3 \equiv \pm1 \;(\mathrm{mod}\ 49)$ |
| ($\mathcal{B}18$) | $\mathrm{PSp}_6(p)$ | $\mathrm{PSU}_3(3)$ | 2 | $p \equiv \pm1 \;(\mathrm{mod}\ 12)$ |
| | | | 7 | $p^2 \not\equiv 1 \;(\mathrm{mod}\ 7)$, $p^3 \equiv \pm1 \;(\mathrm{mod}\ 49)$ |

TABLE 4. The $r$-elusive $\mathcal{S}$-actions, $H \in \mathcal{B}$

*natural $T$-module. Let $r$ be a prime dividing $|\Omega|$ and $|H \cap T|$, and define $\kappa(T, r)$ as in (2). Then $T$ is $r$-elusive if and only if one of the following holds:*

(i) $\kappa(T, r) = 1$;

(ii) $r \geqslant 5$, $r \neq p$, $H \in \mathcal{A}$ and $c = r - 1$;

(iii) $r \in \{2, 3\}$ and $(T, S, r)$ is one of the cases recorded in Table 5.

*In particular, if $n > 10$ then $T$ is $r$-elusive only if $\kappa(T, r) = 1$ or $H \in \mathcal{A}$.*

This corollary is easily deduced from Theorem 1. To see this, first recall that $\kappa(T, r) = 1$ if the conditions in ($\star$) hold, and one checks that the same is true for all the cases in Tables 3 and 4 with $r \geqslant 5$. To determine the examples appearing in Table 5 we include the two cases with $H \in \mathcal{A}$ and $r = 2$ in Theorem 1(ii), and we exclude those in Tables 3 and 4 with $r \in \{2, 3\}$ and $\kappa(T, r) = 1$.

Notice that there are genuine examples arising in parts (i) and (ii) of Corollary 1. For (i), see Remark 3. For an example in (ii), take $T = \Omega_{15}(p)$, $S = A_{16}$ and $r = 7$, where $p$ is a prime such that $p(p - 1) \equiv -1 \;(\mathrm{mod}\ 49)$ (here $T$ is $r$-elusive and $\kappa(T, r) = 2$).

| $T$ | $S$ | $r$ | Conditions |
|---|---|---|---|
| $\Omega_{d-\delta}(p)$ | $A_d$ | 2 | $p \neq 2$, $d - \delta$ odd, $\left(\frac{(d-\delta+1)/2}{p}\right) = 1$ |
| $\mathrm{P}\Omega_{d-\delta}^\epsilon(p)$ | $A_d$ | 2 | $p \neq 2$, $(d - \delta) \equiv 2 \pmod 4$, $p \equiv 5\epsilon \pmod 8$ |
| $\mathrm{PSp}_{10}(p)$ | $\mathrm{PSU}_5(2)$ | 2 | $p \equiv \pm 1 \pmod 8$ |
| $\mathrm{P}\Omega_8^+(p)$ | $\Omega_8^+(2)$ | 2 | $p \geqslant 7$ |
| | | 3 | $p^2 \equiv 1 \pmod 9$ |
| $\Omega_7(p)$ | $\mathrm{Sp}_6(2)$ | 2 | $p \geqslant 7$ |
| | | 3 | $p^2 \equiv 1 \pmod 9$ |
| $\mathrm{PSL}_6^\epsilon(q)$ | $\mathrm{PSL}_3(4)$ | 2 | $p \equiv -5\epsilon \pmod{24}$ |
| | $\mathrm{PSU}_4(3)$ | 2 | $p \equiv \epsilon \pmod{12}$ |
| | $\mathrm{M}_{12}$ | 2 | $(\epsilon, q) = (+, 3)$ |
| $\mathrm{PSU}_6(2)$ | $\mathrm{PSU}_4(3)$ | 2 | |
| $\mathrm{PSp}_6(q)$ | $\mathrm{J}_2$ | 2 | $q^2 \equiv 1 \pmod 8$ |
| | $\mathrm{PSU}_3(3)$ | 2 | $q = p \equiv \pm 1 \pmod{12}$ |
| $\mathrm{PSL}_5^\epsilon(q)$ | $\mathrm{PSU}_4(2)$ | 2 | |
| $\mathrm{PSL}_4^\epsilon(q)$ | $\mathrm{PSU}_4(2)$ | 2 | $q \equiv -\epsilon \pmod 4$ |
| | | 3 | $q \equiv \epsilon \pmod 9$ |
| $\mathrm{PSL}_4^\epsilon(q)$ | $A_7$ | 3 | $q \equiv -\epsilon \pmod 9$ |
| $\mathrm{PSp}_4(q)'$ | $A_6$ | 2 | $q \equiv \pm 1 \pmod{12}$ |
| | | 3 | $q^2 \equiv 1 \pmod 9$ |

$\delta = 2$ if $p$ divides $d$, otherwise $\delta = 1$

TABLE 5. The $r$-elusive $\mathcal{S}$-actions with $r \in \{2, 3\}$ and $\kappa(T, r) \geqslant 2$

**Remark 4.** We can immediately determine the $r$-elusive $\mathcal{S}$-actions with $r = 2$ or 3 from Theorem 1 (there are no examples if $H \notin \mathcal{A}$ and $n > 10$). It is also worth noting that the only $p$-elusive $\mathcal{S}$-action, where $p$ is the defining characteristic, is the case labelled ($\mathcal{B}15$) in Table 2 with $T = \mathrm{PSU}_6(2)$ and $S = \mathrm{PSU}_4(3)$.

Let us briefly describe the proof of Theorem 1. First, recall that we may assume $n \geqslant 6$, where $n$ is the dimension of the natural module for $T$. We start by considering the collections $\mathcal{A}$ and $\mathcal{B}$, which are handled directly in Sections 3 and 4, respectively. In order to complete the proof, we may assume that $H \notin \mathcal{A} \cup \mathcal{B}$ and it remains to show that $T$ is $r$-elusive if and only if all the conditions in $(\star)$ hold.

To do this, we first apply a key theorem of Guralnick and Saxl (see Theorem 2.11), which provides an important reduction to the situation where

$$r \neq p, \ r > 2, \ r \text{ divides } |H \cap T| \text{ and } c > \max\{2, \sqrt{n}/2\}$$

with $c$ the integer defined in (1). This is the content of Proposition 5.1 and it essentially reduces the problem to showing that $T$ contains a derangement of order $r$ whenever $r \neq p$ is an odd prime such that

$$\max\{2, \sqrt{n}/2\} < c \leqslant n/2$$

(see Proposition 5.2 for the precise statement).

Not surprisingly, most of the work in this final part of the argument arises when $S$ is a simple group of Lie type. Here the analysis naturally splits into two cases, according to whether or not $S \in \mathrm{Lie}(p)$, where $\mathrm{Lie}(p)$ is the set of simple groups of Lie type in the defining characteristic $p$ (the case $S \notin \mathrm{Lie}(p)$ is studied in Section 5.3 and the proof is completed in Section 5.4). A similar approach applies in both cases; either we identify

a specific derangement of order $r$ (this is often an element $x \in T$ of order $r$ with the largest possible 1-eigenspace on the natural module), or we argue by estimating, and then comparing, the number of conjugacy classes of elements (or subgroups) of order $r$ in $T$ and $H \cap T$, respectively. For $S \notin \text{Lie}(p)$, the analysis relies heavily on the well known bounds of Landazuri and Seitz [27] on the dimensions of irreducible representations. In the defining characteristic, we use the highest weight theory of irreducible representations of quasisimple groups and the ambient simple algebraic groups. Work of Hiss and Malle [19] and Lübeck [31] also plays an important role.

We conclude by presenting several corollaries that are obtained by combining Theorem 1 with the main results of [9] on geometric actions of classical groups. We follow [25] in labelling the geometric subgroup collections $\mathcal{C}_1, \ldots, \mathcal{C}_8$ (see [9, Table 1.4.2]).

**Corollary 2.** *Let $G \leqslant \text{Sym}(\Omega)$ be a primitive almost simple classical group over $\mathbb{F}_q$, where $q = p^a$ with $p$ prime. Let $T$ and $H$ be the socle and point stabiliser of $G$, and let $r$ be a prime divisor of $|\Omega|$.*

   (i) *If $H \in \mathcal{C}_1 \cup \mathcal{C}_2$, $r = p > 2$ and $T$ is $r$-elusive, then $(G, H)$ belongs to a known list of cases.*

   (ii) *If $H \in \mathcal{S}$ then $T$ is $r$-elusive if and only if $(G, H, r)$ satisfies the conditions in Theorem 1.*

   (iii) *In all other cases, $T$ is $r$-elusive if and only if $(G, H, r)$ belongs to a known list of cases.*

**Remark 5.** In part (i) of Corollary 2, we refer the reader to [9, Theorems 4.1.4 and 5.1.2] for further details. Similarly in (iii), if $H \in \mathcal{C}_i$ then the relevant cases are recorded in [9, Theorem 5.i.1]. It is important to note that we are not claiming to have a complete classification of all the $r$-elusive classical groups. Indeed, in [9] we are unable to determine necessary and sufficient conditions for $p$-elusivity in all cases when $p$ is odd and $H \in \mathcal{C}_1 \cup \mathcal{C}_2$.

Next we extend [9, Theorem 1.5.3] to give a complete description of the 2-elusive almost simple primitive classical groups (note that $\kappa(T, 2) \geqslant 2$ if $n \geqslant 6$, where $n$ is the dimension of the natural module for $T$).

**Corollary 3.** *Let $G \leqslant \text{Sym}(\Omega)$ be a primitive almost simple classical group over $\mathbb{F}_q$ with socle $T$ and point stabiliser $H$. Then $T$ is 2-elusive if and only if $|\Omega|$ is even and one of the following holds:*

   (i) *$H \in \mathcal{C}_1$ and $(G, H)$ is one of the cases in [9, Table 4.1.3];*

   (ii) *$H \in \mathcal{S}$ and $(G, H)$ is one of the cases in Tables 3 or 5 (with $r = 2$);*

   (iii) *$H \notin \mathcal{C}_1 \cup \mathcal{S}$ and $(G, H)$ is one of the cases in [9, Table 5.1.2].*

Finally, by combining Corollary 1 with the main results in [9, Sections 5.3-5.9] we obtain Corollary 4 below. Notice that we omit the $\mathcal{C}_i$-actions with $i \in \{1, 2\}$ since it is not possible to state a definitive result in these cases when $r = p$ (and the required conditions when $r \neq p$ are rather complicated); we refer the reader to the relevant discussion in [9, Chapter 4 and Section 5.1]). In order to state the result, let us say that a partition $\lambda = (\lambda_1, \ldots, \lambda_t)$ of a positive integer is *p-bounded* (with $p$ prime) if $\lambda_i \leqslant p$ for all $i$. In addition, set $d(\lambda) = \gcd\{\lambda_1, \ldots, \lambda_t\}$.

**Corollary 4.** *Let $G \leqslant \text{Sym}(\Omega)$ be a primitive almost simple classical group over $\mathbb{F}_q$, where $q = p^a$ with $p$ prime. Let $T$ and $H$ be the socle and point stabiliser of $G$, respectively, and let $n$ denote the dimension of the natural $T$-module. Let $r > 5$ be a prime divisor of $|\Omega|$ and assume $n > 5$ and $H \notin \mathcal{C}_1 \cup \mathcal{C}_2$. Define $\kappa(T, r)$ as in (2). Then $T$ is $r$-elusive if and only if one of the following holds:*

(i) $\kappa(T, r) = 1$;

(ii) $r \neq p$, $H \in \mathcal{A}$ and $c = r - 1$;

(iii) $H \in \mathcal{C}_5$ is a subfield subgroup over $\mathbb{F}_{q_0}$ with $q = q_0^k$ for an odd prime $k$ and either $r = k$, or $r = p$ and the following conditions hold if $T = \mathrm{PSL}_n^\epsilon(q)$:

    (a) $(d(\lambda), q - \epsilon) = (d(\lambda), q_0 - \epsilon)$ for every $p$-bounded partition $\lambda$ of $n$;

    (b) If there is a partition $\lambda$ in (a) with $(d(\lambda), q - \epsilon) > 1$, then either $k \geqslant p$ or $(k, (n, q_0 - \epsilon)) = 1$.

(iv) $r = p$, $T = \mathrm{PSL}_n(q)$, $H \in \mathcal{C}_8$ is of type $\mathrm{GU}_n(q_0)$ with $q = q_0^2$, $n$ is odd and $(d(\lambda), q - 1) = (d(\lambda), q_0 + 1)$ for every $p$-bounded partition $\lambda$ of $n$.

See [9, Sections 5.5 and 5.8] for an explanation of the number-theoretic conditions appearing in parts (iii) and (iv) of Corollary 4. Notice that there are genuine $p$-elusive examples in these cases. For instance, in (iii) we see that $T = \mathrm{PSL}_6(q)$ is $p$-elusive when $p \geqslant 7$ and $k \geqslant 5$. Similarly in (iv), if we take $p \geqslant 7$ then $T = \mathrm{PSL}_7(q)$ is $p$-elusive.

**Notation.** We adopt the notation of [9, 25] for classical groups, so for example we write $\mathrm{PSL}_n^+(q) = \mathrm{PSL}_n(q)$ and $\mathrm{PSL}_n^-(q) = \mathrm{PSU}_n(q)$. We also use the standard notation for labelling involution class representatives presented in [17] and [2], in the odd and even characteristic settings, respectively. We use the notation in [9] for representatives of conjugacy classes of elements of odd prime order, which is recalled in Section 2.2. Finally, if $n$ is a positive integer then $Z_n$ (or just $n$) denotes a cyclic group of order $n$.

## 2. Preliminaries

In this section we record some preliminary results which will be needed in the proof of Theorem 1.

2.1. **Derangements.** We begin with a useful lemma on derangements in the socle of a primitive almost simple group.

**Lemma 2.1.** *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive group with socle $T$ and point stabiliser $H$. Set $H_0 = H \cap T$ and let $\Omega_0$ be the set of right cosets of $H_0$ in $T$. Then $\Delta(T) = \Delta_0(T)$, where $\Delta(T)$ and $\Delta_0(T)$ denote the set of derangements in $T$ on $\Omega$ and $\Omega_0$, respectively. In particular, if $r$ is a prime divisor of $|\Omega|$ then $T$ is $r$-elusive on $\Omega$ if and only if $T$ is $r$-elusive on $\Omega_0$.*

*Proof.* First observe that $|\Omega| = |\Omega_0|$. Suppose $x \in \Delta(T)$. If $x$ has a fixed point on $\Omega_0$ then $x \in H_0^t$ for some $t \in T$, so $x \in H^t$ and thus $x$ fixes a point of $\Omega$, which is a contradiction. Therefore, $\Delta(T) \subseteq \Delta_0(T)$. Now assume $y \in \Delta_0(T)$ and suppose $y$ fixes a point of $\Delta$, so $y \in H^g \cap T$ for some $g \in G$. Since $G = HT$, we can write $g = ht$ for some $h \in H$, $t \in T$, so $y \in H^t \cap T = H_0^t$, but this contradicts the fact that $y$ is a derangement on $\Omega_0$. The result follows. $\qquad\square$

**Corollary 2.2.** *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive group with socle $T$ and point stabiliser $H$. Let $r$ be a prime divisor of $|\Omega|$ and set $H_0 = H \cap T$. Suppose there are more $T$-classes of elements (or subgroups) of order $r$ in $T$ than there are $H_0$-classes of such elements (or subgroups) in $H_0$. Then $T$ is not $r$-elusive on $\Omega$.*

2.2. **Conjugacy classes.** The conjugacy classes of elements of prime order in the almost simple classical groups are studied in [9, Chapter 3], which brings together earlier work of Wall [36], Aschbacher and Seitz [2], Liebeck and Seitz [28], Gorenstein, Lyons and Solomon [17] and others. In order to highlight some of the results and the relevant notation, let us focus on conjugacy in the general linear group $G = \mathrm{GL}_n(q)$, where $q = p^f$ with $p$ a prime. Let $V$ be the natural module.

Let $x \in G$ be an element of prime order $r$. If $r \neq p$ then $x$ is diagonalisable over $\mathbb{F}_{q^i}$, but not over any proper subfield, where $i = \Phi(r, q)$ is the integer

$$\Phi(r, q) = \min\{i \in \mathbb{N} : r \text{ divides } q^i - 1\}. \tag{3}$$

In other words, $r$ is a primitive prime divisor of $q^i - 1$. By Maschke's Theorem, $x$ fixes a direct sum decomposition

$$V = U_1 \oplus \cdots \oplus U_m \oplus C_V(x),$$

where each $U_j$ is an $i$-dimensional subspace on which $x$ acts irreducibly, and $C_V(x)$ denotes the 1-eigenspace of $x$. The eigenvalues of $x$ on $U_j \otimes \mathbb{F}_{q^i}$ are of the form $\Lambda = \{\lambda, \lambda^q, \ldots, \lambda^{q^{i-1}}\}$ for some nontrivial $r$-th root of unity $\lambda \in \mathbb{F}_{q^i}$. In total, there are $t = (r-1)/i$ possibilities for $\Lambda$, say $\Lambda_1, \ldots, \Lambda_t$ (these are simply the orbits on the set of nontrivial $r$-th roots of unity in $\mathbb{F}_{q^i}$ under the permutation $\omega \mapsto \omega^q$). Following [9], if $a_j$ denotes the multiplicity of $\Lambda_j$ in the multiset of eigenvalues of $x$ on $V \otimes \mathbb{F}_{q^i}$, then we will write

$$x = [\Lambda_1^{a_1}, \ldots, \Lambda_t^{a_t}, I_e],$$

where $e = \dim C_V(x)$. This convenient notation is justified by [9, Lemma 3.1.7], which states that two elements of order $r$ in $G$ are conjugate if and only if they have the same multiset of eigenvalues (in $\mathbb{F}_{q^i}$).

There is a similar description of the semisimple conjugacy classes of elements of prime order in the other classical groups, with some suitable modifications. For instance, if $x \in \mathrm{Sp}_n(q)$ and $ir$ is odd, then $t = (r-1)/i = 2s$ is even and the $\Lambda_j$ can be labelled so that $\Lambda_j^{-1} = \Lambda_{s+j}$ for $1 \leqslant j \leqslant s$ (where $\Lambda_j^{-1} = \{\lambda^{-1} : \lambda \in \Lambda_j\}$). Then the fact that $x$ preserves a symplectic form on $V$ implies that $a_j = a_{s+j}$ for each $j$, so we can write

$$x = [(\Lambda_1, \Lambda_1^{-1})^{a_1}, \ldots, (\Lambda_s, \Lambda_s^{-1})^{a_s}, I_e].$$

Once again, two elements of order $r$ are conjugate if and only if they have the same eigenvalues. We refer the reader to [9, Chapter 3] for further details.

**Remark 2.3.** Let $T$ be a simple classical group over $\mathbb{F}_q$ with natural module $V$ and let $x \in T$ be an element of odd prime order $r \neq p$. Set $n = \dim V$, $i = \Phi(r, q)$ and assume $c \geqslant 2$, where $c$ is the integer in (1). By [9, Lemma 3.1.3] we may write $x = \hat{x}Z$, where $\hat{x} \in \mathrm{GL}(V)$, $Z = Z(\mathrm{GL}(V))$ and $\hat{x}$ has order $r$. Here $\hat{x}$ is conjugate to a block-diagonal matrix of the form $[X_1^{a_1}, \ldots, X_s^{a_s}, I_e]$, where $s = (r-1)/c$ and the $X_j$ are distinct $c \times c$ matrices with distinct eigenvalues in $\mathbb{F}_{q^i}$ (here $a_j$ denotes the multiplicity of $X_j$ as a diagonal block of $\hat{x}$). For example, if $T = \mathrm{PSL}_n(q)$ then $c = i$ and $X_j$ is irreducible with eigenvalues $\Lambda_j$ as above. In particular, there exists an element $x \in T$ of order $r$ such that $\dim C_V(\hat{x}) = n - c$ (and the nontrivial eigenvalues of such an element (in $\mathbb{F}_{q^i}$) are distinct).

Now suppose $x \in G$ has order $r = p$. Here we can write

$$x = [J_p^{a_p}, J_{p-1}^{a_{p-1}}, \ldots, J_1^{a_1}], \tag{4}$$

where $J_i$ is a standard unipotent Jordan block of size $i$, and $a_i$ denotes the multiplicity of $J_i$ in the Jordan form of $x$ on $V$. In $\mathrm{GL}_n(q)$, two elements of order $p$ are conjugate if and only if they have the same Jordan form. There is a similar description of the conjugacy classes of elements of order $p$ in the other classical groups (again, we refer the reader to [9, Chapter 3]).

In the proof of Theorem 1, we will often establish the existence of a derangement of order $r$ by comparing the number of $T$-classes of subgroups (or elements) in $T$ with the number of such $H_0$-classes in $H_0$ (recall that if the former is greater than the latter, then $T$ contains a derangement of order $r$ by Corollary 2.2). Therefore, it will be helpful to have some general bounds on the number of such classes. With this aim in mind, the following notation will be useful.

**Notation.** Let $G$ be a finite group and let $m$ be a positive integer. We write $\kappa(G, m)$ for the number of conjugacy classes of subgroups of order $m$ in $G$.

**Lemma 2.4.** *Let $T$ be a simple classical group over $\mathbb{F}_q$, let $n$ be the dimension of the natural module and let $r \neq p$ be an odd prime divisor of $|T|$. Set $m = \lfloor n/c \rfloor$, where $c$ is the integer in (1). Assume $c \geqslant 2$.*

   (i) $\kappa(T, r) = 1$ *if and only if $m = 1$, or $T = \mathrm{P\Omega}_n^-(q)$ and $c = n/2$.*
   (ii) *If $m = 2$, with $c \neq n/2$ if $T = \mathrm{P\Omega}_n^+(q)$, then $\kappa(T, r) \leqslant (r-1)/c + 1$.*
   (iii) $\kappa(T, r) \geqslant m - \delta$, *where $\delta = 1$ if $T$ is an orthogonal group and $n = mc$, otherwise $\delta = 0$. In particular, $\kappa(T, r) \geqslant \lfloor n/(r-1) \rfloor - 1$.*

*Proof.* First consider (i). If $m \geqslant 2$ (and $c \neq n/2$ if $T = \mathrm{P\Omega}_n^-(q)$) then $\langle [X_1, I_{n-c}]Z \rangle$ and $\langle [X_1^2, I_{n-2c}]Z \rangle$ represent two distinct $T$-classes of subgroups of order $r$, so $\kappa(T, r) \geqslant 2$. For the converse, let us assume $m = 1$, or $T = \mathrm{P\Omega}_n^-(q)$ and $c = n/2$. We claim that $\kappa(T, r) = 1$.

Let $x \in T$ be an element of order $r$. By replacing $x$ with a suitable conjugate, if necessary, we may assume that $x = \hat{x}Z$ with $\hat{x} = [X_1^{a_1}, \ldots, X_s^{a_s}, I_e]$ as in Remark 2.3 (so $s = (r-1)/c$). Suppose $T \neq \mathrm{P\Omega}_n^\pm(q)$. Since each $X_j$ has size $c$ we have $\hat{x} = [X_j, I_{n-c}]$ for some $j$, hence $T$ has $s$ conjugacy classes of elements of order $r$. Now the eigenvalues of $X_j$ coincide with the eigenvalues of a suitable power of $X_1$, so $\langle x \rangle$ is $T$-conjugate to $\langle y \rangle$, where $y = \hat{y}Z \in T$ and $\hat{y} = [X_1, I_{n-c}]$, so $\kappa(T, r) = 1$ as claimed.

Now assume $T = \mathrm{P\Omega}_n^\epsilon(q)$ with $\epsilon = \pm$. If $n/2 < c < n$ then the above argument goes through unchanged. If $c = n/2$ then $\epsilon = -$ and $C_V(\hat{x})$ has to be nontrivial (see [9, Remark 3.5.5(iii)]), so $\hat{x} = [X_j, I_{n/2}]$ and the same argument applies. Finally, suppose $c = n$. There are two cases to consider:

   (a) $T = \mathrm{P\Omega}_n^+(q)$, $n \equiv 2 \pmod 4$ and $r$ is a primitive prime divisor of $q^{n/2} - 1$.
   (b) $T = \mathrm{P\Omega}_n^-(q)$ and $r$ is a primitive prime divisor of $q^n - 1$.

Here $\hat{x} = [X_j]$ and for each choice of $j$ there are two $T$-classes of elements of this form, which are fused in $\mathrm{PO}_n^\epsilon(q)$ (see [9, Proposition 3.5.8]). In both cases, we observe that a Sylow $r$-subgroup of $\Omega_n^\epsilon(q)$ is contained in a cyclic maximal torus of $\mathrm{O}_n^\epsilon(q)$ of order $q^{n/2} - \epsilon$. In particular, the Sylow $r$-subgroups of $T$ are cyclic and we conclude that $\kappa(T, r) = 1$.

Now let us turn to (ii). As in (i), if $T = \mathrm{P\Omega}_n^-(q)$ and $c = n/2$ then $T$ has a unique class of subgroups of order $r$, so for the remainder we may assume that $c \neq n/2$ if $T$ is an orthogonal group. Let $\langle x \rangle$ be a subgroup of $T$ of order $r$. Since $m = 2$, it is easy to see that $\langle x \rangle$ is $T$-conjugate to one of $\langle [X_1, I_{n-c}]Z \rangle$ or $\langle [X_1, X_j, I_{n-2c}]Z \rangle$ for some $j \in \{1, \ldots, (r-1)/c\}$. The result follows.

Finally, consider (iii). Clearly, none of the subgroups $\langle [X_1^a, I_{n-ac}]Z \rangle$ are $T$-conjugate, where $1 \leqslant a < m$. In addition, if either $n > mc$, or $n = mc$ and $T$ is not an orthogonal group, then $\langle [X_1^m, I_{n-mc}]Z \rangle$ represents an additional class of subgroups of order $r$.   $\square$

**Remark 2.5.** The definition of $\delta$ in part (iii) of Lemma 2.4 can be explained as follows. Let $T = \mathrm{P\Omega}_n^\epsilon(q)$ and set $i = \Phi(r, q)$ as in (3), so $c = 2i$ if $i$ is odd, otherwise $c = i$. Suppose $i = r - 1$ and $n = mi = mc$. If $\epsilon = (-)^{m-1}$ then $C_V(\hat{x})$ is nontrivial for all $x \in T$ of

order $r$ (see [9, Remark 3.5.5]), so the subgroups $\langle [X_1^a, I_{n-ac}]Z \rangle$ with $1 \leqslant a < m$ form a complete set of representatives of the $T$-classes of subgroups of order $r$.

**Remark 2.6.** Observe that the inequality in Lemma 2.4(ii) need not be equality since $\langle [X_1, X_j, I_{n-2c}]Z \rangle$ and $\langle [X_1, X_k, I_{n-2c}]Z \rangle$ may be conjugate for $j \neq k$. For example, suppose $T = \mathrm{PSL}_4(16)$ and $r = 17$, so $c = m = 2$ and $X_i$ has eigenvalues $\{\omega^i, \omega^{r-i}\}$ for some $r$-th root of unity $\omega$. Then $[X_1, X_2]^8$ and $[X_1, X_8]$ are $T$-conjugate (they have the same set of eigenvalues), so $\langle [X_1, X_2]Z \rangle$ and $\langle [X_1, X_8]Z \rangle$ are conjugate subgroups.

The next result follows immediately from part (i) of Lemma 2.4; in the statement, we refer to the conditions recorded in $(\star)$ (see p.2).

**Corollary 2.7.** *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive classical group over $\mathbb{F}_q$ with socle $T$ and point stabiliser $H$. Let $n$ be the dimension of the natural $T$-module and let $r$ be a prime divisor of $|\Omega|$. If all of the conditions in $(\star)$ hold, then $T$ is $r$-elusive.*

**Lemma 2.8.** *Let $T_1$ and $T_2$ be finite simple classical groups over $\mathbb{F}_q$, where $q = p^f$ and $p$ is a prime. Let $n_1$ and $n_2$ be the dimensions of the respective natural modules and let $r \neq p$ be an odd prime divisor of $|T_1|$ and $|T_2|$. Set $i = \Phi(r, q)$ and*

$$c_j = \begin{cases} 2i & \text{if } i \text{ is odd and } T_j \neq \mathrm{PSL}_{n_j}(q) \\ i/2 & \text{if } i \equiv 2 \ (\mathrm{mod} \ 4) \text{ and } T_j = \mathrm{PSU}_{n_j}(q) \\ i & \text{otherwise} \end{cases}$$

*and assume that $c_1 \geqslant c_2 \geqslant 2$ and $n_2 > 2n_1$. Then $\kappa(T_2, r) > \kappa(T_1, r)$.*

*Proof.* First assume $c_1 = c_2 = c$ and set $s = (r-1)/c$. Let $\{\langle x_j \rangle : 1 \leqslant j \leqslant \kappa(T_1, r)\}$ be a set of representatives of the $T_1$-classes of subgroups of order $r$. Write $x_j = \hat{x}_j Z$ with

$$\hat{x}_j = [X_1^{a_{1,j}}, \ldots, X_s^{a_{s,j}}, I_{e_j}] \tag{5}$$

(up to conjugacy). By relabelling, if necessary, we may assume that there is an integer $\ell \geqslant 0$ such that $e_j > 0$ if and only if $j > \ell$.

Define elements $y_j, z_k \in T_2$ of order $r$ by setting

$$\hat{y}_j = [X_1^{a_{1,j}}, \ldots, X_s^{a_{s,j}}, I_{e_j+n_2-n_1}] \quad 1 \leqslant j \leqslant \kappa(T_1, r)$$
$$\hat{z}_k = [X_1^{2a_{1,k}}, \ldots, X_s^{2a_{s,k}}, I_{n_2-2n_1}] \quad 1 \leqslant k \leqslant \ell.$$

Note that the 1-eigenspaces of $\hat{y}_j$ and $\hat{z}_k$ are nontrivial, so $y_j$ and $z_k$ are indeed elements of $T_2$. Then none of the following subgroups

$$\{\langle y_j \rangle, \ \langle z_k \rangle : \ell < j \leqslant \kappa(T_1, r), 1 \leqslant k \leqslant \ell\} \tag{6}$$

are $T_2$-conjugate, so $\kappa(T_2, r) \geqslant \kappa(T_1, r)$. The desired result now follows because it is easy to see that $T_2$ has some additional classes of subgroups of order $r$. For example, if we take $x = \hat{x}Z \in T_2$ with

$$\hat{x} = \begin{cases} [X_1^{2\lfloor n_1/c \rfloor - 1}, I_{n_2 - c(\lfloor n_2/c \rfloor - 1)}] & \lfloor n_1/c \rfloor > 1 \\ [X_1^2, I_{n_2-2c}] & \lfloor n_1/c \rfloor = 1, n_1 > c \\ [X_1, I_{n_2-c}] & n_1 = c \end{cases}$$

then $\langle x \rangle$ is not $T_2$-conjugate to any of the subgroups in (6).

Now assume $c_1 > c_2$, in which case one of the following holds:

(a) $T_1 \neq \mathrm{PSL}_{n_1}(q)$, $T_2 = \mathrm{PSL}_{n_2}(q)$, $i \geqslant 3$ is odd, $c_1 = 2i$, $c_2 = i$;
(b) $T_1 \neq \mathrm{PSU}_{n_1}(q)$, $T_2 = \mathrm{PSU}_{n_2}(q)$, $i \equiv 2 \ (\mathrm{mod} \ 4)$, $i \geqslant 6$, $c_1 = i$, $c_2 = i/2$.

Set $s = (r-1)/c_1$ and $t = (r-1)/c_2$, so $t = 2s$. As before, let $\{\langle x_j \rangle : 1 \leqslant j \leqslant \kappa(T_1, r)\}$ be a set of representatives of the $T_1$-classes of subgroups of order $r$, where $x_j = \hat{x}_j Z$ and $\hat{x}_j$ is given in (5). Now every element $y \in T_2$ of order $r$ is of the form $y = \hat{y} Z$ with

$$\hat{y} = [Y_1^{a_1}, \dots, Y_s^{a_s}, Y_{s+1}^{a_{s+1}}, \dots, Y_t^{a_t}, I_{e'}].$$

Without loss of generality, we may assume that for each $j \in \{1, \dots, s\}$, the set of eigenvalues of $X_j$ (in $\mathbb{F}_{q^i}$) is the union of the eigenvalues of $Y_j$ and $Y_{s+j}$. We can now repeat the argument for the case $c_1 = c_2$, replacing each $X_m$ by $Y_m$. The result follows. $\qquad \square$

**Lemma 2.9.** *Let $T = \mathrm{PSL}_n^{\epsilon}(q)$ and let $r \geqslant 5$ be a prime divisor of $q^2 - 1$. Define $c$ as in* (1).

    (i) *If $(n, c) = (3, 1)$ then $\kappa(T, r) \leqslant r - 1$.*

    (ii) *If $(n, c) = (4, 1)$ then $\kappa(T, r) \leqslant (r^2 - 3r + 6)/2$.*

    (iii) *If $(n, c) = (6, 2)$ then $\kappa(T, r) \leqslant (r^2 + 15)/8$.*

*Proof.* Write $\mathrm{PGL}_n^{\epsilon}(q) = \mathrm{GL}_n^{\epsilon}(q)/Z$ and let $\omega \in \mathbb{F}_{q^2}$ and $x \in T$ be elements of order $r$. Since $r \geqslant 5$ and $n \in \{3, 4, 6\}$ we have $(r, n) = 1$ so we may write $x = \hat{x}Z$ with $\hat{x} \in \mathrm{GL}_n^{\epsilon}(q)$ of order $r$ (see [7, Lemma 3.11]).

First assume $(n, c) = (3, 1)$. By replacing $x$ by a suitable conjugate, we may assume $\hat{x} = [1, \lambda_1, \lambda_2] \in \mathrm{GL}_3^{\epsilon}(q)$, where $\lambda_1 \neq \lambda_2$ and $\lambda_2 \neq 1$. Clearly, if $\lambda_1 = 1$ then $\langle x \rangle$ is $T$-conjugate to $\langle [1, 1, \omega] Z \rangle$. On the other hand, if $\lambda_1 \neq 1$ then $\langle x \rangle$ is $T$-conjugate to $\langle [1, \omega, \omega^j] Z \rangle$ for some $1 < j < r$. The result follows. Similarly, if $(n, c) = (4, 1)$ then any subgroup of $T$ of order $r$ is conjugate to one of the following:

$$\langle [1, 1, 1, \omega] Z \rangle, \ \langle [1, 1, \omega, \omega^j] Z \rangle, \ \langle [1, \omega, \omega^k, \omega^{k'}] Z \rangle,$$

where $1 \leqslant j < r$ and $1 < k < k' < r$. Therefore, there are at most

$$1 + (r - 1) + \binom{r - 2}{2} = (r^2 - 3r + 6)/2$$

such classes. Finally, suppose $(n, c) = (6, 2)$. Set $s = (r - 1)/2$ and write

$$\hat{x} = [X_1^{a_1}, \dots, X_s^{a_s}, I_e]$$

as in Remark 2.3. Then the $T$-classes of subgroups of order $r$ are represented by

$$\langle [X_1, I_4] Z \rangle, \ \langle [X_1, X_j, I_2] Z \rangle, \ \langle [X_1^2, X_j] Z \rangle, \ \langle [X_1, X_k, X_{k'}] Z \rangle,$$

where $1 \leqslant j \leqslant (r - 1)/2$ and $1 < k < k' \leqslant (r - 1)/2$. Therefore, there are at most

$$r + \binom{(r-3)/2}{2} = (r^2 + 15)/8$$

such classes, as claimed. $\qquad \square$

### 2.3. Subgroup structure.

Let $G$ be an almost simple classical group over $\mathbb{F}_q$ with socle $T$ and natural module $V$. Set $n = \dim V$ and let $H$ be a maximal subgroup of $G$ with $G = HT$. Recall that Aschbacher's subgroup structure theorem states that either $H$ belongs to one of eight geometric subgroup collections, or $H$ is almost simple and acts irreducibly on $V$. The latter collection of non-geometric subgroups is denoted by $\mathcal{S}$, and the formal definition of this collection is as follows (see [25, p.3]). Note that the various conditions are designed to ensure that a subgroup in $\mathcal{S}$ is not contained in one of the geometric subgroup collections.

**Definition 2.10.** A subgroup $H$ of $G$ belongs to the collection $\mathcal{S}$ if and only if it satisfies the following conditions:

    (i) The socle $S$ of $H$ is a nonabelian simple group and $S \not\cong T$.

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

(iii) $\rho(\hat{S})$ cannot be realised over a proper subfield of $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_{q^2}$ if $T = \mathrm{PSU}_n(q)$, otherwise $\mathbb{F} = \mathbb{F}_q$.

(iv) If $\rho(\hat{S})$ fixes a nondegenerate quadratic form on $V$ then $T = \mathrm{P\Omega}_n^\epsilon(q)$.

(v) If $\rho(\hat{S})$ fixes a nondegenerate alternating form on $V$, but no nondegenerate quadratic form, then $T = \mathrm{PSp}_n(q)$.

(vi) If $\rho(\hat{S})$ fixes a nondegenerate hermitian form on $V$ then $T = \mathrm{PSU}_n(q)$.

(vii) If $\rho(\hat{S})$ does not fix a form as in (iv), (v) or (vi) then $T = \mathrm{PSL}_n(q)$.

Let $x \in G \cap \mathrm{PGL}(V)$ be a nontrivial element and write $x = \hat{x}Z$, where $V$ is the natural module for $T$, $\hat{x} \in \mathrm{GL}(V)$ and $Z = Z(\mathrm{GL}(V))$. Set $\bar{V} = V \otimes \bar{\mathbb{F}}_q$, where $\bar{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$, and define

$$\nu(x) = \min\{\dim[\bar{V}, \lambda\hat{x}] \,:\, \lambda \in \bar{\mathbb{F}}_q^\times\} \tag{7}$$

where $[\bar{V}, \lambda\hat{x}]$ is the subspace $\langle v - v^{\lambda\hat{x}} \mid v \in \bar{V}\rangle$. Note that $\nu(x)$ is the codimension of the largest eigenspace of $\hat{x}$ on $\bar{V}$.

The following theorem is a special case of [18, Theorem 7.1] (recall that the subgroups in the collections $\mathcal{A}$ and $\mathcal{B}$ are recorded in Tables 1 and 2, respectively).

**Theorem 2.11.** *Let $G$ be a finite almost simple classical group with socle $T$ and let $H \in \mathcal{S}$ be a subgroup of $G$. Let $n$ be the dimension of the natural module for $T$, and assume that $n \geqslant 6$ and $H \notin \mathcal{A} \cup \mathcal{B}$. Then*

$$\nu(x) > \max\{2, \sqrt{n}/2\}$$

*for all nontrivial $x \in H \cap \mathrm{PGL}(V)$.*

This result plays a central role in our proof of Theorem 1. First we handle the excluded cases; the relevant $r$-elusive groups with $n < 6$ were determined in [9] (see Table 3), and the groups with a point stabiliser in $\mathcal{A}$ or $\mathcal{B}$ will be handled in the next two sections. At this point we are in a position to apply Theorem 2.11, which immediately implies that any element $x \in T$ of order $r$ with $\nu(x) \leqslant \max\{2, \sqrt{n}/2\}$ is a derangement. In this way, we quickly reduce to the case $r \neq p$, $r \geqslant 5$ and $c > \max\{2, \sqrt{n}/2\}$, where $c$ is the integer in (1). Moreover, we may assume that $r$ divides $|H \cap T|$. If $c > n/2$ then $T$ is $r$-elusive by Corollary 2.7, so we can assume that

$$\max\{2, \sqrt{n}/2\} < c \leqslant n/2$$

and our goal will be to show that $T$ contains a derangement of order $r$. This final step will be carried out in Section 5.

## 3. The collection $\mathcal{A}$

Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive classical group over $\mathbb{F}_q$ with socle $T$ and point stabiliser $H \in \mathcal{S}$. Let $S$ denote the socle of $H$ and let $V$ be the natural $T$-module. Recall that $V$ is absolutely irreducible as an $\hat{S}$-module, where $\hat{S}$ is an appropriate covering group of $S$. In this section we investigate the special case where $H$ belongs to the collection $\mathcal{A}$. Here $S = A_d$ is the alternating group of degree $d$ and $V$ is the *fully deleted permutation module* for $S$ over $\mathbb{F}_p$. The relevant cases that arise are recorded in Table 1.

We begin by recalling the construction of $V$. Let $p$ be a prime, let $d \geqslant 5$ be an integer and consider the permutation module $\mathbb{F}_p^d$ for $S_d$. Define subspaces

$$U = \{(a_1, \ldots, a_d) \,:\, \sum_{i=1}^{d} a_i = 0\}, \quad W = \{(a, \ldots, a) \,:\, a \in \mathbb{F}_p\}$$

of $\mathbb{F}_p^d$, and observe that $U$ and $W$ are the only nonzero proper $A_d$-invariant submodules of $\mathbb{F}_p^d$. Then $V = U/(U \cap W)$ is the fully deleted permutation module for $A_d$, which is an absolutely irreducible $A_d$-module over $\mathbb{F}_p$. Set $n = \dim V$ and note that $n = d - 2$ if $p$ divides $d$, otherwise $n = d - 1$. Note that $A_d$ preserves the symmetric bilinear form $B' : U \times U \to \mathbb{F}_p$ defined by

$$B'((a_1, \ldots, a_d), (b_1, \ldots, b_d)) = \sum_{i=1}^{d} a_i b_i$$

and thus $B'$ induces a symmetric bilinear form $B$ on $V$. By [25, Proposition 5.3.5], if $d \geqslant 10$ then $V$ has the smallest dimension of all nontrivial irreducible $A_d$-modules over $\mathbb{F}_p$.

Suppose $p$ is odd. In this situation, the $A_d$-module $V$ affords an embedding of $A_d$ into an orthogonal group $\Omega_n^\epsilon(p)$. By choosing a suitable basis for $V$ it is straightforward to compute the determinant of the Gram matrix of $B$, and subsequently the discriminant $D(Q) \in \{\square, \boxtimes\}$ of the corresponding quadratic form $Q$ on $V$ (which is defined by $Q(v) = \frac{1}{2}B(v, v)$ for $v \in V$).

For example, suppose $d$ is even and $p$ divides $d$, so $n = d - 2$ and $U \cap W = W$. Let $\{v_1, \ldots, v_d\}$ be the standard basis for $\mathbb{F}_p^d$ and set $e_i = (v_i - v_{i+1}) + W$, $1 \leqslant i \leqslant n$. Then

$$\beta = \{e_1, \ldots, e_n\} \tag{8}$$

is a basis for $V$ and

$$J_\beta = \begin{pmatrix} 2 & -1 & & & & \\ -1 & 2 & -1 & & & \\ & & \ddots & & & \\ & & -1 & 2 & -1 \\ & & & -1 & 2 \end{pmatrix}$$

is the corresponding Gram matrix of $B$. Therefore $\det(J_\beta) = n + 1$, so $D(Q) = \square$ if $n + 1$ is a square in $\mathbb{F}_p$, otherwise $D(Q) = \boxtimes$.

In general, if $p$ is odd and $n$ is even then using [25, Proposition 2.5.10] we calculate that $\epsilon = +$ if and only if

$$\left( \frac{n+1}{p} \right) = (-1)^{\frac{1}{4}n(p-1)}$$

where the term on the left is the *Legendre symbol* (which takes the value 1 if $n + 1$ is a quadratic residue modulo $p$, 0 if $p$ divides $n + 1$, and $-1$ in the remaining cases; here $n + 1$ is indivisible by $p$, so it is always nonzero). Note that if $d$ is even and $p$ divides $d$ then

$$\left( \frac{n+1}{p} \right) = \left( \frac{-1}{p} \right) = (-1)^{\frac{1}{2}(p-1)} \tag{9}$$

and thus $\epsilon = -$ if and only if $d \equiv 2 \pmod 4$ and $p \equiv 3 \pmod 4$.

Now assume $p = 2$ so $n$ is even. Let $u = (a_1, \ldots, a_d) \in U$. We define a map $Q' : U \to \mathbb{F}_2$ by setting $Q'(u) = 1$ if the number of nonzero $a_i$ is congruent to 2 modulo 4, otherwise $Q'(u) = 0$. Then $Q'$ is an $A_d$-invariant quadratic form on $U$ with associated bilinear form $B'$. If $d \not\equiv 2 \pmod 4$ then $Q'$ induces a nondegenerate quadratic form $Q$ on $V$, so in this case we obtain an embedding $A_d \leqslant \Omega_n^\epsilon(2)$ where $\epsilon$ is given in Table 1 (see [25, p.187]). On the other hand, if $d \equiv 2 \pmod 4$ then $A_d$ does not fix a nondegenerate quadratic form on $V$, so we have an embedding $A_d \leqslant \mathrm{Sp}_{d-2}(2)$.

The specific irreducible embeddings that arise in this way are listed in Table 1. Note that the conditions on $d$ in the final column ensure that $S = A_d$ is simple and not isomorphic to $T$. For the remainder of this section we set $H_0 = H \cap T$.

**Lemma 3.1.** *We have $H_0 = S_d$ if and only if $T = \mathrm{Sp}_n(2)$, or $np$ is odd and $\left(\frac{(n+1)/2}{p}\right) = 1$.*

*Proof.* Let $x$ be the transposition $(1,2)$ in $S_d$. If $p = 2$ then $x$ has Jordan form $[J_2, J_1^{n-2}]$ on $V$, so $x \in T$ if and only if $T$ is a symplectic group. Now assume $p$ is odd, so $T$ is an orthogonal group. Up to conjugacy, $x$ acts on $V$ as a diagonal matrix $[-I_1, I_{n-1}]$ (modulo scalars), so $x \in T$ only if $n$ is odd. In terms of the above basis $\beta$ for $V$ (see (8)), $x$ maps $e_1$ to $-e_1$, $e_2$ to $e_1 + e_2$, and it fixes all the other basis vectors. Then $E = \langle e_1 + 2e_2, e_3, \ldots, e_n \rangle$ is the 1-eigenspace of $x$, which is a nondegenerate $(n-1)$-space of type $\epsilon'$. To determine whether or not $x \in T$ we need to calculate $\epsilon'$.

It is straightforward to check that the Gram matrix of the induced bilinear form on $E$ has determinant $(n+1)/2$, so [25, Proposition 2.5.10] implies that $\epsilon' = +$ if and only if

$$\left(\frac{(n+1)/2}{p}\right) = (-1)^{\frac{1}{4}(n-1)(p-1)}$$

If $\epsilon' = +$ (respectively, $\epsilon' = -$) then $x \in \mathrm{SO}_n(p)$ is an involution of type $t_{(n-1)/2}$ (respectively, $t'_{(n-1)/2}$) in the notation of [9, 17], and the desired result follows by inspecting [17, Table 4.5.1]. For example, if $\epsilon' = +$ then we find that an involution in $\mathrm{SO}_n(p)$ of type $t_{(n-1)/2}$ is in $T$ if and only if

$$p^{\frac{1}{2}(n-1)} \equiv 1 \pmod 4,$$

whence $H_0 = S_d$ if and only if $\left(\frac{(n+1)/2}{p}\right) = 1$. $\qquad\square$

In the statement of the next lemma, we use the notation in (4) for expressing the Jordan form of an element of order $p$.

**Lemma 3.2.** *Let $x \in S_d$ be an element of order $p$ with cycle-shape $(p^h, 1^s)$. Then the Jordan form of $x$ on $V$ is as follows:*

   (i) $[J_p^h, J_1^{s-1}]$ *if $s \geqslant 1$ and $(p, d) = 1$;*

   (ii) $[J_p^h, J_1^{s-2}]$ *if $s \geqslant 1$ and $p$ divides $d$;*

   (iii) $[J_p^{h-1}, J_{p-2}]$ *if $s = 0$ and $(p, h) = 1$;*

   (iv) $[J_p^{h-2}, J_{p-1}^2]$ *if $s = 0$, $p$ divides $h$, and $h \neq 2$;*

   (v) $[J_2]$ *if $s = 0$ and $p = h = 2$.*

*Proof.* Up to conjugacy, we may assume that

$$x = (1, \ldots, p) \cdots ((h-1)p + 1, \ldots, hp).$$

Suppose first that $s \geqslant 1$. Then for each $i \in \{0, \ldots, h-1\}$,

$$\mathcal{E}_i = \{e_{ip+1} - e_d + (U \cap W), \ldots, e_{(i+1)p} - e_d + (U \cap W)\}$$

is a set of $p$ linearly independent vectors in $V$, which are cyclically permuted by $x$, and $\mathcal{E}_0 \cup \ldots \cup \mathcal{E}_{h-1}$ is a linearly independent set of $hp$ vectors. Therefore, [9, Lemma 5.2.6] implies that $x$ has Jordan form $[J_p^h, J_1^{s-1}]$ if $(p, d) = 1$ and $[J_p^h, J_1^{s-2}]$ if $p$ divides $d$.

For the remainder, let us assume that $s = 0$, so $n = d - 2$, $U \cap W = W$ and $x$ cyclically permutes the $p$ vectors

$$\{e_1 - e_2 + W, \ldots, e_{p-1} - e_p + W, e_p - e_1 + W\}.$$

If $h = 1$ then $V$ is spanned by this set of vectors and the first $p-2$ form a basis for $V$. Thus $x$ has Jordan form $[J_{p-2}]$ on $V$. Suppose now that $h \geqslant 2$. Then for each $i \in \{1, \ldots, h-1\}$ the set

$$\mathcal{E}_i = \{e_1 - e_{ip+1} + W, e_2 - e_{ip+2} + W, \ldots, e_p - e_{(i+1)p} + W\}$$

is a set of $p$ linearly independent vectors cyclically permuted by $x$. If $(p,h) = 1$ then $\mathcal{E}_1 \cup \ldots \cup \mathcal{E}_{h-1}$ is an $x$-invariant set of linearly independent vectors and by Lemma [9, Lemma 5.2.6], the Jordan form of $x$ on the span of these vectors is $[J_p^{h-1}]$. By [33, Lemma 4.3], the 1-eigenspace of $x$ on $V$ has dimension $h$, so it follows that $x$ has Jordan form $[J_p^{h-1}, J_{p-2}]$ on $V$.

Now assume $p$ divides $h$. If $p = h = 2$ then $\dim V = 2$ and $x$ acts nontrivially on $V$, so $x$ has Jordan form $[J_2]$. Now assume $h \geqslant 3$. Note that $\mathcal{E}_1 \cup \ldots \cup \mathcal{E}_{h-1}$ is linearly dependent, whereas $\mathcal{E} = \mathcal{E}_1 \cup \ldots \cup \mathcal{E}_{h-2}$ is linearly independent. Let $Y$ be the span of $\mathcal{E}$. Now $x$ cyclically permutes the $p$ vectors

$$\{e_{(h-1)p+1} - e_{(h-1)p+2} + W, \ldots, e_{(h-1)p+p+1} - e_{hp} + W, e_{hp} - e_{(h-1)p+1} + W\}$$

which span a $(p-1)$-dimensional subspace $Z$ of $V$ such that $Y \cap Z = 0$. Moreover, the Jordan form of $x$ on $Z$ is $[J_{p-1}]$. By [33, Lemma 4.3], the 1-eigenspace of $x$ on $V$ is $h$-dimensional, and so $x$ has Jordan form $[J_{p-1}^{h-2}, J_{p-1}^2]$ on $V$. $\qquad\square$

**Lemma 3.3.** *Let $x \in S_d$ be an element of prime order $r \neq p$ with cycle-shape $(r^h, 1^s)$ and consider the action of $x$ on $\bar{V} = V \otimes \mathbb{F}$, where $\mathbb{F} = \bar{\mathbb{F}}_p$. Then every nontrivial $r$-th root of unity occurs as an eigenvalue of $x$ on $\bar{V}$ with multiplicity $h$.*

*Proof.* Let $\mathbb{F}^d$ be the permutation module for $S_d$ over $\mathbb{F}$ and set $\bar{U} = U \otimes \mathbb{F}$ and $\bar{W} = W \otimes \mathbb{F}$. Let $\omega \in \mathbb{F}$ be a nontrivial $r$-th root of unity. By [9, Lemma 5.2.6], $\omega$ occurs as an eigenvalue of $x$ on $\mathbb{F}^d$ with multiplicity $h$. If $p$ does not divide $d$ then $\mathbb{F}^d = \bar{U} \oplus \bar{W}$, $\bar{V} = \bar{U}$ and $\bar{W}$ is contained in the 1-eigenspace of $x$ on $\mathbb{F}^d$. Therefore, $\omega$ has multiplicity $h$ as an eigenvalue of $x$ on $\bar{V}$.

Now assume $p$ divides $d$, so $\bar{W} \leqslant \bar{U}$ and $\bar{V} = \bar{U}/\bar{W}$. Now $x$ has a fixed point and without loss of generality we may assume that $x$ fixes the standard basis element $v_d \in \mathbb{F}^d$. Since $\mathbb{F}^d = \bar{U} \oplus \langle v_d \rangle$ and $v_d$ is a 1-eigenvector for $x$, it follows that $\omega$ has multiplicity $h$ as an eigenvalue of $x$ on $\bar{U}$. Since $\bar{W}$ is also contained in the 1-eigenspace of $x$ we conclude that $\omega$ has multiplicity $h$ as an eigenvalue of $x$ on $\bar{V}$. $\qquad\square$

We are now ready to state the main result of this section. In the proof of the proposition, we freely use the notation for prime order elements introduced in Section 2.2, which is consistent with the notation adopted in [9]. In part (ii) of the statement, we define the integer $c$ as in (1).

**Proposition 3.4.** *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple classical group over $\mathbb{F}_q$ with socle $T$ and point stabiliser $H \in \mathcal{A}$. Let $r$ be a prime divisor of $|\Omega|$ and assume that $n \geqslant 6$. Set $H_0 = H \cap T$ and note that $q = p$ is a prime. Then $T$ is $r$-elusive if and only if one of the following holds:*

(i) *$r = 2$, $p \neq 2$ and either*
    (a) *$T = \Omega_n(p)$ and $\left(\frac{(n+1)/2}{p}\right) = 1$; or*
    (b) *$T = \mathrm{P}\Omega_n^\epsilon(p)$, $n \equiv 2 \pmod 4$ and $p \equiv 5\epsilon \pmod 8$.*
(ii) *$r \neq p$, $r > 2$, $r$ divides $|H_0|$ and $c = r - 1$.*

*Proof.* Here $H_0 \in \{A_d, S_d\}$ and $d \geqslant 5$. If $r = p > 2$ then $[J_2^2, J_1^{n-4}] \in T$ is a derangement by Lemma 3.2. Now assume $r = p = 2$ and note that by Lemma 3.2, $x = (1,2)(3,4) \in H_0$ has Jordan form $[J_2^2, J_1^{n-4}]$ on $V$. Moreover, in terms of the Aschbacher-Seitz [2] notation, we identify $x$ as a $c_2$-type involution since

$$B(e_3 + e_4, (e_3 + e_4)x) = B(v_3 + v_5, v_4 + v_5) = 1.$$

We conclude that the $a_2$-type involutions in $T$ are derangements.

Next suppose $r \neq p$ and $r > 2$. Let $i = \Phi(r, p)$ (see (3)), so $i$ is the smallest positive integer such that $r$ divides $p^i - 1$. Clearly, if $r$ fails to divide $|H_0|$ then every element in $T$ of order $r$ is a derangement, so let us assume $r$ divides $|H_0|$. Let $x \in H_0$ be an element of order $r$ and write $x = \hat{x}Z$, where $\hat{x} \in \mathrm{GL}_n(p)$ has order $r$. By Lemma 3.3, the multiset of eigenvalues of $\hat{x}$ on $\bar{V} = V \otimes \bar{\mathbb{F}}_q$ contains every nontrivial $r$-th root of unity with equal multiplicity. Therefore, if $i$ is even and $i < r - 1$ then $[\Lambda, I_{n-i}]$ is a derangement. Similarly, if $i$ is odd and $i < (r-1)/2$ then $[\Lambda, \Lambda^{-1}, I_{n-2i}]$ has the desired property. Now assume $i$ is even and $i = r - 1$, so $\hat{x}$ is conjugate to an element of the form $[\Lambda^h, I_{n-h(r-1)}]$ for some $h \geqslant 1$ with $hr \leqslant n$. There is a unique $T$-class of such elements for each value of $h$, and $x^T \cap H$ consists of the permutations in $H_0$ with cycle-shape $(r^h, 1^{d-hr})$. In particular, $T$ is $r$-elusive. An entirely similar argument applies if $i = (r-1)/2$ is odd.

To complete the proof of the proposition, we may assume that $r = 2$ and $p \neq 2$, so $T$ is an orthogonal group (see Table 1). By Lemma 3.3, if $x \in S_d$ has cycle-shape $(2^h, 1^s)$ then the $(-1)$-eigenspace of $x$ on $V$ has dimension $h \leqslant d/2$.

Suppose first that $T = \mathrm{P\Omega}_n^+(q)$. If $n \equiv 0 \pmod 4$ then $T$ contains involutions of type $t_{n/2}$ or $t'_{n/2}$, and these elements are derangements because they do not have $-1$ as an eigenvalue (see [9, Sections 3.5.2.10 and 3.5.2.11]). Now assume $n \equiv 2 \pmod 4$. If $p \equiv 1 \pmod 8$ then the same argument implies that involutions of type $t_{n/2}$ in $T$ are derangements. If $p \equiv 3 \pmod 4$ then $T$ contains two classes of involutions (namely, $t_1$ and $t'_1$) with a 2-dimensional $(-1)$-eigenspace and so one of these classes must consist of derangements. This leaves $p \equiv 5 \pmod 8$, in which case $H_0 = A_d$ by Lemma 3.1. Here every involution in $T$ has a $2\ell$-dimensional $(-1)$-eigenspace for some $1 \leqslant \ell < n/4$ (see [9, Table B.10]), and there is a unique class of such involutions for each $\ell$. We conclude that $T$ is 2-elusive. A very similar argument applies if $T = \mathrm{P\Omega}_n^-(q)$ and we omit the details.

Finally, suppose $T = \Omega_n(p)$ with $n$ odd. Here every involution in $T$ is of the form $[-I_{2\ell}, I_{n-2\ell}]$, and there is a unique such class for each $1 \leqslant \ell \leqslant (n-1)/2$ (see [9, Table B.8]). Now, if $H_0 = A_d$ then $H_0$ does not contain a transposition, so any involution in $T$ of the form $[-I_{n-1}, I_1]$ is a derangement. On the other hand, if $H_0 = S_d$ then it is easy to see that every involution in $T$ has fixed points, so $T$ is 2-elusive. Note that $H_0 = S_d$ if and only if $\left( \frac{(n+1)/2}{p} \right) = 1$ (see Lemma 3.1). $\qquad\square$

## 4. The collection $\mathcal{B}$

In this section we turn our attention to the case where $H \in \mathcal{S}$ is a subgroup in the collection $\mathcal{B}$ (see Table 2). Recall that these cases arise naturally as exceptions in the statement of Theorem 2.11, so $n \geqslant 6$ and

$$\nu(x) \leqslant \max\{2, \sqrt{n}/2\}$$

for some nontrivial element $x \in H \cap \mathrm{PGL}(V)$. Our main result is the following (note that Table 4 is located in the introduction).

**Proposition 4.1.** *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple classical group with socle $T$ and point stabiliser $H \in \mathcal{B}$. Let $r$ be a prime divisor of $|\Omega|$ and let $S$ denote the socle of $H$. Then $T$ is $r$-elusive if and only if $(T, S, r)$ is one of the cases listed in Table 4.*

**Remark 4.2.** The conditions recorded in the final column of Table 4 are needed to ensure that every element in $T$ of order $r$ has fixed points, and they also imply that $r$ divides the degree of $G$. Note that these conditions are additional to the ones given in Table 2, which are needed for the existence and maximality of $H$ in $G$. We refer the reader to the tables in [4, Section 8.2] for the precise conditions required for maximality, and for a detailed description of the structure of $H_0 = H \cap T$. Further information on these cases

can be found in [8, Section 2.3]. Also note that the relevant covering group $\hat{S}$ is given in the statement of [18, Theorem 7.1].

**Lemma 4.3.** *Proposition 4.1 holds in Case* ($\mathcal{B}1$) *of Table 2.*

*Proof.* Here $T = \mathrm{PSp}_{10}(p)$, $S = \mathrm{PSU}_5(2)$ and $p \neq 2$. According to [4, Table 8.65], we have $H_0 = S.2$ if and only if $p \equiv \pm 1 \pmod 8$. Let $r$ be a prime divisor of $|\Omega|$. If $r$ does not divide $|H_0|$ then any element in $T$ of order $r$ is a derangement, so we may as well assume that $r$ also divides $|H_0|$, hence $r \in \{2, 3, 5, 11\}$.

If $r = p$ then $H_0$ has at most six classes of elements of order $r$, but $T$ has at least seven by [9, Proposition 3.4.10] and thus $T$ is not $r$-elusive by Corollary 2.2. Now assume $r \neq p$. Set $i = \Phi(r, p)$ as in (3) and define $\nu(x)$ for $x \in T$ as in (7). Let $\chi$ be the corresponding Brauer character of $H_0$ (this is available in GAP [13], for example). One observes that $\{\chi(x) : x \in H_0, |x| = 3\} = \{-5, -2, 1, 4\}$, which implies that every $x \in T$ of order 3 with $\nu(x) = 2$ is a derangement (indeed, over $\overline{\mathbb{F}}_p$ such an element has eigenvalues $\omega$, $\omega^2$ and 1 (the latter with multiplicity 8), so $\chi(x) = 7$). In the same way, we deduce that the elements $x \in T$ of order 5 with $\nu(x) = 4$ are derangements. If $r = 11$ then $i \in \{1, 2, 5, 10\}$ and by considering $\chi$ we see that $T$ is 11-elusive if and only if $i > 2$ (in fact, we need the condition $p^5 \equiv \pm 1 \pmod{121}$ to ensure that $|\Omega|$ is divisible by 11).

Finally, let us assume $r = 2$. By inspecting the values of $\chi$ we deduce that the involutions $x \in T$ with $\nu(x) < 5$ have fixed points, whereas those with $\nu(x) = 5$ have fixed points if and only if $H_0 = S.2$ (in this situation, $H_0$ contains an involutory graph automorphism $\gamma$ of $S$ such that $\nu(\gamma) = 5$). We conclude that $T$ is 2-elusive if and only if $p \equiv \pm 1 \pmod 8$.  $\square$

**Lemma 4.4.** *Proposition 4.1 holds in Case* ($\mathcal{B}2$) *of Table 2.*

*Proof.* Here $T = \mathrm{P\Omega}_8^+(q)$ and $H_0 = \Omega_7(q)$ if $q$ is odd, otherwise $H_0 = \mathrm{Sp}_6(q)$. This embedding arises by restricting an irreducible spin representation of $\Omega_8^+(q)$ to the stabiliser of a 1-dimensional nonsingular subspace of the natural $\Omega_8^+(q)$-module. Let $r$ be a prime divisor of $|H_0|$ and $|\Omega|$.

First assume $q$ is even, so $H_0 = \mathrm{Sp}_6(q)$. By inspecting the proof of [8, Lemma 2.7], we deduce that every $c_2$-type involution in $T$ is a derangement (here we are using the standard Aschbacher-Seitz [2] notation for involutions). Now assume $r$ is odd. Let $i = \Phi(r, q)$, so $i \in \{1, 2, 4\}$. If $i \in \{1, 2\}$ then the proof of [8, Lemma 2.7] indicates that every element $x \in T$ of order $r$ with $\nu(x) = 2$ is a derangement. Similarly, if $i = 4$ then the elements with $\nu(x) = 4$ are derangements.

A very similar argument applies when $q$ is odd. For example, the proof of [8, Lemma 2.7] shows that $[J_3, J_1^5]$ and $[-I_2, I_6]$ are derangements in $T$ of order $p$ and 2, respectively. Finally, if $r \neq p$ and $r > 2$ then we can proceed as above in the $q$ even case.  $\square$

**Lemma 4.5.** *Proposition 4.1 holds in Case* ($\mathcal{B}3$) *of Table 2.*

*Proof.* Here $T = \mathrm{P\Omega}_8^+(q)$ and $H_0 = C_T(\psi) = {}^3D_4(q_0)$, where $q = q_0^3$ and $\psi$ is a triality graph-field automorphism of $T$. In view of the proof of [8, Lemma 2.12], this characterisation of $H_0$ implies that if $p \neq 2$ then unipotent elements with Jordan form $[J_3, J_1^5]$ are derangements of order $p$, and so are involutions of type $a_4$ when $p = 2$. Similarly, if $p \neq 2$ then the involutions of type $[-I_2, I_6]$ are also derangements.

Let $r \neq p$ be an odd prime divisor of $|\Omega|$ and $|H_0|$. Set $i = \Phi(r, q)$ and note that $i \in \{1, 2, 4\}$. Let $x \in T$ be an element of order $r$ with $\nu(x) = \alpha$, where $\alpha = 2$ if $i \in \{1, 2\}$, otherwise $\alpha = 4$. Then $x$ is not centralised by $\psi$ (see [7, Proposition 3.55(iv)]), so $x$ is a derangement. For example, if $i \in \{1, 2\}$ and $\nu(x) = 2$ then $\nu(x^\psi) = 4$.  $\square$

**Lemma 4.6.** *Proposition 4.1 holds in Case* ($\mathcal{B}4$) *of Table 2.*

*Proof.* Here $T = \mathrm{P}\Omega_8^+(p)$, $H_0 = \Omega_8^+(2)$ and $p \neq 2$ (see [4, Table 8.50]). Let $r$ be a prime divisor of $|\Omega|$ and $|H_0|$, so $r \in \{2, 3, 5, 7\}$. If $r = p$ then $H_0$ has at most five classes of subgroups of order $r$, whereas $T$ has at least six (see [9, Proposition 3.5.12]). Now assume $r \neq p$ and note that $p \geqslant 7$ (indeed, if $p \in \{3, 5\}$ then $p$ is the only prime dividing $|\Omega|$ and $|H_0|$). Set $i = \Phi(r, p)$.

Suppose $p = 7$, so $r \in \{2, 5\}$. If $r = 5$ then $i = 4$ and we deduce that $T$ is 5-elusive by considering the values of the corresponding Brauer character $\chi$ of $2.\Omega_8^+(2)$. Now assume $r = 2$. The involutions in $T$ are of type $t_1', t_2, t_3'$ and $t_4'$, in terms of the notation in [17, 9]. By inspecting $\chi$ we see that the $t_1'$ elements have fixed points, and so do the involutions in at least one of the other classes. Since $H_0$ is normalised by a triality graph automorphism $\tau$ of $T$, and $\tau$ permutes the $T$-classes represented by the elements $t_1', t_3', t_4'$, we conclude that every involution in $T$ has fixed points, so $T$ is 2-elusive.

Now assume $p > 7$. As above, $T$ is 2-elusive. By considering $\chi$ we see that every element of order 3 has fixed points, and we note that $|\Omega|$ is divisible by 3 if and only if $p^2 \equiv 1$ (mod 9). Similarly, if $r \in \{5, 7\}$ then $T$ is $r$-elusive if and only if $i > 2$.                                                                     $\square$

**Lemma 4.7.** *Proposition 4.1 holds in Cases $(\mathcal{B}6)$ and $(\mathcal{B}7)$ of Table 2.*

*Proof.* Here $H_0 = G_2(q)$ and $T = \Omega_7(q)$ or $\mathrm{Sp}_6(q)$, according to the parity of $p$. If $p = 3$ then $G_2(q)$ admits an involutory graph automorphism that interchanges the two irreducible 7-dimensional modules $L(\lambda_1)$ and $L(\lambda_2)$, so we only need to consider the standard embedding, labelled $(\mathcal{B}6)$. Let $r$ be a prime divisor of $|\Omega|$ and $|H_0|$.

If $r = p > 2$ then the proof of [8, Lemma 2.13] implies that $[J_3, J_1^4]$ is a derangement of order $r$. Similarly, every involution $x \in T$ with $\nu(x) = 1$ is a derangement.

Finally, suppose $r \neq p$ and $r > 2$. Set $i = \Phi(r, q)$ and note that $i \in \{1, 2\}$. Let $x \in T$ be an element of order $r$ with $\nu(x) = 2$. Let $\bar{H} = G_2$ and $\bar{G} = B_3$ (or $C_3$ if $p = 2$) be the ambient simple algebraic groups over the algebraic closure $\bar{\mathbb{F}}_q$, and note that $x$ is contained in a maximal rank subgroup $A_2$ of $\bar{H}$. If $\bar{V}$ denotes the natural module for $\bar{G}$, then

$$\bar{V} \downarrow A_2 = \begin{cases} V_3 \oplus V_3^* & p = 2 \\ V_3 \oplus V_3^* \oplus 0 & p \neq 2 \end{cases}$$

where $V_3$ and $0$ denote the natural and trivial $A_2$-modules, respectively. It follows that each $y \in A_2$ of order $r$ has a repeated nontrivial eigenvalue on $\bar{V}$. Since the two nontrivial eigenvalues of $x$ are distinct, we conclude that $x$ is a derangement.                    $\square$

**Lemma 4.8.** *Proposition 4.1 holds in each of the remaining cases in Table 2.*

*Proof.* The remaining cases are similar so we only give details in case $(\mathcal{B}13)$. Here $T = \mathrm{PSL}_6^\epsilon(p)$ and $S = \mathrm{PSU}_4(3)$, where $p \equiv \epsilon$ (mod 6) and $p \geqslant 5$. More precisely, $H_0 = S$ or $S.2$, with $H_0 = S.2$ if and only if $p \equiv \epsilon$ (mod 12) (see [4, Tables 8.25 and 8.27]). Let $r$ be a prime divisor of $|\Omega|$ and $|H_0|$, so $r \in \{2, 3, 5, 7\}$. Let $\chi$ be the corresponding Brauer character of $6.\mathrm{PSU}_4(3)$ or $6.\mathrm{PSU}_4(3).2$ (according to the value of $p$).

If $r = p$ then $r \in \{5, 7\}$ and $T$ is not $r$-elusive since $H_0$ has at most two classes of elements of order $r$. Next assume $r \neq p$ and $r > 2$. Set $i = \Phi(r, p)$. If $r = 3$ then $H_0$ has at most four classes of elements of order 3, but there are at least five in $T$ (see [9, Propositions 3.2.2 and 3.3.3], for example). Now assume $r = 5$. By inspecting $\chi$ we see that $\nu(y) = 4$ for all $y \in H_0$ of order 5, whence $T$ is 5-elusive if and only if $i = 4$ (in fact, we need $p^2 \equiv -1$ (mod 25) so that $|\Omega|$ is divisible by 5). Similarly, $T$ is 7-elusive if and only if $i = 3(3 + \epsilon)/2$ (here we need the condition $p^3 \equiv -\epsilon$ (mod 49)).

Finally, let us assume $r = 2$. If $H_0 = S$ then $H_0$ has a unique class of involutions, but $T$ has two such classes and thus $T$ is not 2-elusive. Now assume that $H_0 = S.2$, so $p \equiv \epsilon$ (mod 12) and $T$ has three classes of involutions, with representatives labelled $t_1, t_2$

and $t_3$ (see [17, Table 4.5.1]). Note that $H_0$ is an extension of $S$ by an involutory graph automorphism of type $\gamma_1$ (see [9, Sections 3.2.5 and 3.3.5]). By considering the Brauer character $\chi$ we deduce that the two classes of graph automorphisms in $H_0$ fuse to the $T$-classes represented by $t_1$ and $t_3$, while the involutions in $S$ are $T$-conjugate to $t_2$. We conclude that $T$ is 2-elusive. $\qquad\square$

This completes the proof of Proposition 4.1.

## 5. The proof of Theorem 1

As in the statement of Theorem 1, let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple classical group over $\mathbb{F}_q$ with socle $T$ and point stabiliser $H \in \mathcal{S}$. Set $H_0 = H \cap T$ and write $q = p^f$ with $p$ a prime. Let $S$ denote the socle of $H$ and let $n$ be the dimension of the natural $T$-module $V$. Let $r$ be a prime divisor of $|\Omega|$.

If $n < 6$ then [9, Proposition 6.3.1] states that $T$ is $r$-elusive if and only if $(T, S, r)$ is one of the cases in Table 3, so we may assume that $n \geqslant 6$. Similarly, if $H \in \mathcal{A} \cup \mathcal{B}$ then the conclusion to Theorem 1 follows from our work in Sections 3 and 4 (see Propositions 3.4 and 4.1). In addition, Corollary 2.7 implies that $T$ is $r$-elusive if all of the conditions in $(\star)$ hold.

Therefore, in order to complete the proof of Theorem 1 we may assume that $n \geqslant 6$ and $H \notin \mathcal{A} \cup \mathcal{B}$; our aim is to show that $T$ is $r$-elusive only if all the conditions in $(\star)$ hold. Proposition 5.1 below is a first step towards achieving this goal. In order to state this result, recall the definition of $i$ and $c$ in (1), and let $(\diamond)$ denote the following conditions:

$$r \neq p,\; r > 2,\; r \text{ divides } |H_0| \text{ and } c > \max\{2, \sqrt{n}/2\}. \tag{$\diamond$}$$

**Proposition 5.1.** *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple classical group with socle $T$ and point stabiliser $H \in \mathcal{S}$. Let $r$ be a prime divisor of $|\Omega|$ and let $S$ denote the socle of $H$. Assume that $n \geqslant 6$ and $H \notin \mathcal{A} \cup \mathcal{B}$. Then $T$ is $r$-elusive only if the conditions in $(\diamond)$ hold.*

*Proof.* We apply Theorem 2.11. For example, any element in $T$ with Jordan form $[J_2^2, J_1^{n-4}]$ is a derangement of order $p$. Similarly, if $p$ is odd then involutions in $T$ of type $[-I_2, I_{n-2}]$ are also derangements.

Now assume $r \neq p$ and $r > 2$. Clearly, $T$ contains derangements of order $r$ if $|H_0|$ is indivisible by $r$, so let us assume $r$ divides $|H_0|$. If $1 < c \leqslant \max\{2, \sqrt{n}/2\}$ then let $x \in T$ be an element of order $r$ with $\dim C_V(x) = n - c$ (see Remark 2.3). Here $\nu(x) = c$, so Theorem 2.11 implies that $x$ is a derangement. Similarly, if $c = 1$ then any element $x \in T$ of order $r$ with $\dim C_V(x) = n - 2$ is a derangement. We conclude that $T$ is $r$-elusive only if $c > \max\{2, \sqrt{n}/2\}$. $\qquad\square$

To complete the proof of Theorem 1, it remains to show that $T$ contains a derangement of order $r$ when the following conditions are satisfied:

$$n \geqslant 6,\; H \notin \mathcal{A} \cup \mathcal{B},\; r \neq p,\; r > 2,\; r \text{ divides } |H_0| \text{ and}$$

$$\max\{2, \sqrt{n}/2\} < c \leqslant n/2, \tag{$\boxtimes$}$$

with $c < n/2$ if $T = \mathrm{P\Omega}_n^-(q)$.

**Proposition 5.2.** *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive almost simple classical group with socle $T$ and point stabiliser $H \in \mathcal{S}$. Let $r$ be a prime divisor of $|\Omega|$ and assume that the conditions in $(\boxtimes)$ are satisfied. Then $T$ contains a derangement of order $r$.*

As in Sections 3.4 and 4.1, in order to prove Proposition 5.2 we will either identify a specific derangement of order $r$, or we will establish the existence of such an element by comparing the number of $T$-classes of subgroups (or elements) in $T$ of order $r$ with the number of such $H_0$-classes in $H_0$. As before, we will write $\kappa(T, r)$ to denote the number of $T$-classes of subgroups of order $r$ in $T$ (and similarly $\kappa(H_0, r)$). Note that the conditions in ($\boxtimes$) imply that $\kappa(T, r) \geqslant 2$ (this quickly follows from Lemma 2.4(iii)), so the desired conclusion follows immediately if $\kappa(H_0, r) = 1$.

Before we begin the proof of Proposition 5.2, let us record a couple of useful observations. Suppose the conditions in ($\boxtimes$) hold. First observe that $r \geqslant 5$ since $c \geqslant 3$. Also note that $r$ divides $q^{r-1} - 1$ by Fermat's Little Theorem, so $i$ divides $r - 1$. In particular, if $i$ is odd then $2i$ divides $r - 1$. It follows that $c$ divides $r - 1$ and thus

$$r \geqslant c + 1 \geqslant \lceil \sqrt{n}/2 \rceil + 1. \tag{10}$$

### 5.1. Sporadic groups.
We begin the proof of Proposition 5.2 by considering the special case where $S$ is a sporadic group.

**Proposition 5.3.** *Proposition 5.2 holds if $S$ is a sporadic group.*

*Proof.* This is a straightforward calculation, using the character table of $S$ and lower bounds on the dimensions of irreducible representations. To illustrate the general approach, we will consider the cases $S \in \{M_{11}, J_2, \mathbb{M}\}$. Set $i = \Phi(r, q)$ as in (3).

If $S = M_{11}$ then $r \in \{5, 11\}$ and the result follows since $\kappa(H_0, r) = 1$. Next suppose $S = \mathbb{M}$ is the Monster. Here $r \leqslant 71$ and by inspecting the character table of $H_0 = S$ (specifically, the associated power maps) we deduce that $\kappa(H_0, r) \leqslant 2$. But $n \geqslant 196882$ (see [23]) and thus $\kappa(T, r) \geqslant \lfloor 196882/70 \rfloor - 1 = 2811$ by Lemma 2.4(iii). Now apply Corollary 2.2.

Finally, let us assume that $S = J_2$, so $r \in \{5, 7\}$. From the character table we see that $\kappa(S, 5) = 2$ and $\kappa(S, 7) = 1$. Therefore we may assume that $r = 5$, so $i = 4$ since $c \geqslant 3$. If $n \geqslant 13$ then $\kappa(T, 5) \geqslant 3$ by Lemma 2.4(iii), so we can assume $n \leqslant 12$. By inspecting [20, Table 2] (or [4, Section 8.2]), it follows that $T = \mathrm{PSp}_6(q)$ is the only possibility, and either $q = p \equiv \pm 1 \pmod 5$ or $q = p^2 > 4$ and $p \equiv \pm 2 \pmod 5$. Clearly, neither of these conditions on $q$ are compatible with the fact that $i = 4$, so this case does not arise. (Alternatively, observe that this is the case labelled ($\mathcal{B}17$) in Table 2, so we can discard it since we are assuming that $H \notin \mathcal{B}$.)

The remaining cases are very similar and we leave the reader to check the details. $\square$

### 5.2. Alternating groups.
Next assume $S = A_d$ is an alternating group. Since we are assuming $H \notin \mathcal{A}$, it follows that $V$ is not the fully deleted permutation module for $S$. Note that $r \leqslant d$ since $r$ divides $|H_0|$. The following lemma gives a useful lower bound on $n$ in terms of $d$.

**Lemma 5.4.** *If $d \geqslant 15$ then $n \geqslant d(d-5)/4$.*

*Proof.* First observe that $\hat{S} = 2.S$ is the full covering group of $S$. If $Z(\hat{S})$ acts nontrivially on $V$ then $p \neq 2$ and the main theorem of [26] implies that $n \geqslant 2^{\lfloor (d-3)/2 \rfloor}$ and the result follows. Therefore, we may assume that $S$ acts linearly on $V$, in which case the desired bound follows from [22, Theorem 7]. $\square$

**Proposition 5.5.** *Proposition 5.2 holds if $S$ is an alternating group.*

*Proof.* First assume $d \geqslant 15$. Now $\kappa(S, r) = \lfloor d/r \rfloor$ and a combination of Lemmas 2.4(iii) and 5.4 implies that

$$\kappa(T, r) \geqslant \lfloor n/(r-1) \rfloor - 1 \geqslant \lfloor d(d-5)/4(r-1) \rfloor - 1 > \lfloor d/r \rfloor.$$

We conclude that $T$ contains derangements of order $r$.

Finally, let us assume that $5 \leqslant d \leqslant 14$. If $d \leqslant 9$ then $r \in \{5, 7\}$ and the result follows since $\kappa(S, r) = 1$. If $d \in \{10, 11, 12\}$ then we may assume that $r = 5$, in which case $\kappa(S, r) = 2$ (if $r > 5$, then $\kappa(S, r) = 1$). By inspecting [19, Table 3], we see that $n \geqslant 16$ and thus $\kappa(T, r) \geqslant 3$ by Lemma 2.4(iii). The result follows. A similar argument applies if $d \in \{13, 14\}$, using the fact that $n \geqslant 32$ (see [19]). $\qquad\square$

5.3. **Groups of Lie type: Cross-characteristic.** Let $S$ be a simple group of Lie type over $\mathbb{F}_t$, where $t = \ell^e$ and $\ell \neq p$ is a prime. Set $H_0 = H \cap T$. By (10) we have

$$r \geqslant \max\{5, \lceil \sqrt{n}/2 \rceil + 1\}. \tag{11}$$

We will make extensive use of the Landazuri-Seitz bounds in [27]. We consider each of the possibilities for $S$ in turn, starting with the classical groups.

5.3.1. *Linear groups.*

**Lemma 5.6.** *Proposition 5.2 holds if $S = \mathrm{PSL}_2(t)$ and $(t, p) = 1$.*

*Proof.* If $t \in \{4, 9\}$ then $r = 5$ and $\kappa(H_0, r) = 1$, so for the remainder we may assume that $t \geqslant 5$ and $t \neq 9$, hence $n \geqslant (t - 1)/(2, t - 1)$ by the main theorem of Landazuri and Seitz [27]. In particular, (11) implies that

$$r \geqslant \lceil \sqrt{n}/2 \rceil + 1 \geqslant \left\lceil \frac{1}{2} \sqrt{(t-1)/(2, t-1)} \right\rceil + 1. \tag{12}$$

Suppose $x \in H_0 \setminus S$ has order $r$. Then $x$ is a field automorphism and thus $r$ divides $e = \log_\ell t$. If $t > 2^7$ then (12) implies that $r > e$, so $t \in \{2^5, 2^7\}$ and one checks that $H_0 = \mathrm{P\Gamma L}_2(t)$ has a unique class of subgroups of order $r$.

For the remainder, we may assume that every element in $H_0$ of order $r$ is contained in $S$. If $r \neq \ell$ then $\kappa(S, r) = 1$, so we may assume that $r = \ell$. Note that $\kappa(S, r) \leqslant 2$ since $S$ has two classes of elements of order $r$. In fact, if $e = 1$ then $\kappa(S, r) = 1$ by Sylow's Theorem, so we may assume $e \geqslant 2$. By Lemma 2.4(iii) we have

$$\kappa(T, r) \geqslant \lfloor n/(\ell - 1) \rfloor - 1 \geqslant \lfloor (\ell^e - 1)/2(\ell - 1) \rfloor - 1.$$

This reduces us to the case $t = 5^2$. Here $n \geqslant 12$ and $r = 5$, so $\kappa(T, r) \geqslant 3$ (note that $T$ is symplectic if $n = 12$ – see [19, Table 2(b)]). $\qquad\square$

**Lemma 5.7.** *Proposition 5.2 holds if $S = \mathrm{PSL}_d(t)$ and $(t, p) = 1$.*

*Proof.* We may assume $d \geqslant 3$. If $(d, t) = (3, 2)$ or $(3, 4)$ then $r \in \{5, 7\}$ and $\kappa(H_0, r) = 1$. In each of the remaining cases we have $n \geqslant t^{d-1} - 1$ by [27] and thus

$$r \geqslant \lceil \sqrt{n}/2 \rceil + 1 \geqslant \left\lceil \frac{1}{2} \sqrt{t^{d-1} - 1} \right\rceil + 1 \tag{13}$$

In particular, $r > e$ so we only need to consider elements in $\mathrm{PGL}_d(t)$.

Suppose $r = \ell$, so $t \geqslant 5$. If $d \geqslant 4$ then (13) implies that $r > t$, so we must have $d = 3$. Then $S$ has at most four conjugacy classes of elements of order $r$ (see [9, Section 3.2.3], for example), but Lemma 2.4(iii) implies that $T$ has at least

$$\lfloor n/(r - 1) \rfloor - 1 \geqslant \lfloor (t^2 - 1)/(t - 1) \rfloor - 1 = t$$

such classes.

For the remainder, we may assume that $r \neq \ell$. Set $j = \Phi(r, t)$ (so $j$ is the smallest positive integer such that $r$ divides $t^j - 1$). If $j > d/2$ then $\kappa(S, r) = 1$ (see Lemma 2.4(i)), so we may assume that $j \leqslant d/2$. Now the lower bound in (13) implies that

$r > t^{(d-3)/2}$, so $j > (d-3)/2$. Therefore, either $d$ is odd and $j = (d-1)/2$, or $d$ is even and $j \in \{d/2-1, d/2\}$.

First assume $d = 3$, so $j = 1$ and $r$ divides $t - 1$. By Lemma 2.9(i) we have $\kappa(S, r) < r$, but Lemma 2.4(iii) implies that

$$\kappa(T, r) \geqslant \lfloor n/(r-1) \rfloor - 1 \geqslant \lfloor (t^2 - 1)/(t - 2) \rfloor - 1 \geqslant t > r,$$

so $T$ contains derangements of order $r$.

Next suppose $d \geqslant 5$ is odd. Here $j = (d-1)/2$, so $\lfloor d/j \rfloor = 2$ and Lemma 2.4(ii) implies that

$$\kappa(S, r) \leqslant (r-1)/j + 1 = 2(r-1)/(d-1) + 1 < r.$$

Since $r$ divides $t^{(d-1)/2} - 1$, by applying Lemma 2.4(iii) we deduce that

$$\kappa(T, r) \geqslant \lfloor n/(r-1) \rfloor - 1 \geqslant \lfloor (t^{d-1} - 1)/(t^{(d-1)/2} - 2) \rfloor - 1 \geqslant t^{(d-1)/2} > r$$

and the result follows.

Next assume $d \geqslant 8$ is even. Here $\lfloor d/j \rfloor = 2$ and thus

$$\kappa(S, r) \leqslant (r-1)/j + 1 \leqslant 2(r-1)/(d-2) + 1.$$

Now $r$ divides $(t^j - 1)/(t - 1)$, so $r - 1 \leqslant \alpha$ where $\alpha = (t^{d/2} - 1)/(t - 1) - 1$. Therefore, if $t > 2$ then

$$\kappa(T, r) \geqslant \lfloor n/(r-1) \rfloor - 1 \geqslant \lfloor (t^{d-1} - 1)/\alpha \rfloor - 1 \geqslant \alpha \geqslant r - 1 > 2(r-1)/(d-2) + 1.$$

Similarly, if $t = 2$ then

$$\kappa(T, r) \geqslant \lfloor (2^{d-1} - 1)/\alpha \rfloor - 1 = 2^{d/2-1} > \frac{1}{2}(2^{d/2} - 1) - \frac{1}{2} \geqslant \frac{1}{2}(r-1)$$

and once again the desired result follows.

Finally, let us assume that $d \in \{4, 6\}$. First assume $d = 4$ so $j \in \{1, 2\}$. If $j = 1$ then $r \leqslant t - 1$ and thus $t \geqslant 7$. Moreover, $\kappa(S, r) \leqslant (r^2 - 3r + 6)/2$ (see Lemma 2.9(ii)) and

$$\kappa(T, r) \geqslant \lfloor n/(r-1) \rfloor - 1 \geqslant \lfloor (t^3 - 1)/(t - 2) \rfloor - 1 > (t^2 - 5t + 10)/2 \geqslant (r^2 - 3r + 6)/2.$$

Similarly, if $j = 2$ then $t \geqslant 4$, $\kappa(S, r) \leqslant (r-1)/2 + 1 = (r+1)/2$ and

$$\kappa(T, r) \geqslant \lfloor n/(r-1) \rfloor - 1 \geqslant \lfloor (t^3 - 1)/t \rfloor - 1 > (t+2)/2 \geqslant (r+1)/2.$$

Now assume $d = 6$, so $j \in \{2, 3\}$. If $j = 2$ then $t \geqslant 4$ and $\kappa(S, r) \leqslant (r^2 + 15)/8$ by Lemma 2.9(iii), whereas Lemma 2.4(iii) implies that

$$\kappa(T, r) \geqslant \lfloor n/(r-1) \rfloor - 1 \geqslant \lfloor (t^5 - 1)/t \rfloor - 1 > (r^2 + 15)/8.$$

Finally, if $j = 3$ then $r \leqslant (t^3 - 1)/(t - 1) = t^2 + t + 1$ and $\kappa(S, r) \leqslant (r-1)/3 + 1 = (r+2)/3$. However,

$$\kappa(T, r) \geqslant \lfloor n/(r-1) \rfloor - 1 \geqslant \lfloor (t^5 - 1)/t(t+1) \rfloor - 1 > (r+2)/3$$

and the desired result follows. $\square$

### 5.3.2. *Unitary groups.*

**Lemma 5.8.** *Proposition 5.2 holds if $S = \mathrm{PSU}_d(t)$ and $(t, p) = 1$.*

*Proof.* In view of Lemma 5.6, we may assume that $d \geqslant 3$. If $d = 4$ and $t \leqslant 3$ then $r \in \{5, 7\}$ and $\kappa(H_0, r) = 1$, so we may assume that $t > 3$ if $d = 4$. Therefore, [27] implies that

$$n \geqslant \begin{cases} t(t^{d-1} - 1)/(t + 1) & d \text{ odd} \\ (t^d - 1)/(t + 1) & d \text{ even} \end{cases} \tag{14}$$

and thus

$$r \geqslant \lceil \sqrt{n}/2 \rceil + 1 \geqslant \left\lceil \frac{1}{2}\sqrt{t(t^{d-1} - 1)/(t + 1)} \right\rceil + 1 > \log_\ell t.$$

Therefore, every element of order $r$ in $H_0$ is contained in $\mathrm{PGU}_d(t)$. In fact, the same bound implies that $r > t$ if $d \geqslant 4$, so $r = \ell$ only if $d = 3$.

Suppose $r = \ell$, so $S = \mathrm{PSU}_3(t)$ and $t \geqslant 5$. Now $\kappa(S, r) \leqslant 4$ and by combining the lower bound on $n$ in (14) with Lemma 2.4(iii), we see that $\kappa(T, r) \geqslant t - 1$. Therefore, we may assume that $t = 5$ and thus $n \geqslant 20$. If $n = 20$ then $T$ is a symplectic group (see [20, Table 2]), so Lemma 2.4(iii) implies that $\kappa(T, r) \geqslant 5$ and the result follows.

For the remainder we may assume $r \neq \ell$. Set $j = \Phi(r, t)$ and

$$
c' = \left\{ \begin{array}{ll} j & j \equiv 0 \ (\mathrm{mod}\ 4) \\ j/2 & j \equiv 2 \ (\mathrm{mod}\ 4) \\ 2j & j \ \mathrm{odd}. \end{array} \right.
$$

Note that $\kappa(S, r) = 1$ if $c' > d/2$ (see Lemma 2.4(i)), so we may assume that $c' \leqslant d/2$.

First consider the special case $t = 2$, so $d \geqslant 4$ (since $\mathrm{PSU}_3(2)$ is not simple). The cases with $d \leqslant 9$ can be checked directly. For example, suppose $S = \mathrm{PSU}_9(2)$. If $r > 5$ then $c' \geqslant 5$ and thus $\kappa(S, r) = 1$. If $r = 5$ then $\kappa(S, r) = 2$ and (14) implies that $n \geqslant 170$, so $\kappa(T, r) \geqslant \lfloor 170/4 \rfloor - 1 = 41$. Now assume $d \geqslant 10$, so

$$
r \geqslant \left\lceil \frac{1}{2} \sqrt{2(2^{d-1} - 1)/3} \right\rceil + 1 > 2^{(d-4)/2} + 1
$$

and thus $j > (d - 4)/2$. If $j \equiv 0 \ (\mathrm{mod}\ 4)$ then $r$ divides $2^{j/2} + 1$ and $d - 3 \leqslant j = c' \leqslant d/2$, which is absurd since $d \geqslant 10$. Similarly, if $j$ is odd then $(d - 4)/2 < j \leqslant d/4$ and once again we reach a contradiction. Finally, suppose $j \equiv 2 \ (\mathrm{mod}\ 4)$. Here $d - 3 \leqslant j \leqslant d$ and $c' = j/2$, so $\lfloor d/c' \rfloor = 2$ since $d \geqslant 10$. Therefore, $\kappa(S, r) \leqslant (r - 1)/c' + 1$ by Lemma 2.4(ii), whereas $T$ has at least

$$
\lfloor n/(r-1) \rfloor - 1 \geqslant \left\lfloor \frac{2(2^{d-1} - 1)/3}{2^{d/2} + 1} \right\rfloor - 1 > \frac{1}{d} 2^{d/2+1} + 1 \geqslant \frac{1}{j} 2^{j/2+1} + 1 \geqslant \frac{r-1}{c'} + 1
$$

classes of subgroups of order $r$. The result follows.

Finally, let us assume $t \geqslant 3$. First observe that

$$
r \geqslant \left\lceil \frac{1}{2} \sqrt{t(t^{d-1} - 1)/(t+1)} \right\rceil + 1 > t^{(d-3)/2} + 1.
$$

If $j \equiv 0 \ (\mathrm{mod}\ 4)$ then $4 \leqslant j = c' \leqslant d/2$, so $d \geqslant 8$. Moreover, $r$ divides $t^{j/2} + 1$ and thus $d - 2 \leqslant j = c' \leqslant d/2$, but this is incompatible with the bound $d \geqslant 8$. Next assume $j$ is odd, so $2 \leqslant 2j = c' \leqslant d/2$ and $d \geqslant 4$. Since $(d - 3)/2 < j \leqslant d/4$, it follows that $d \in \{4, 5\}$ and $j = 1$, so $r \leqslant t - 1$. In particular, $\kappa(S, r) \leqslant (r + 1)/2$ (see Lemma 2.4(ii)) and

$$
\kappa(T, r) \geqslant \lfloor n/(r-1) \rfloor - 1 \geqslant \left\lfloor \frac{(t^4 - 1)/(t+1)}{t - 2} \right\rfloor - 1 > t/2 \geqslant (r+1)/2,
$$

so the result follows.

To complete the proof of the lemma, we may assume that $t \geqslant 3$ and $j \equiv 2 \ (\mathrm{mod}\ 4)$, in which case $t^{(d-3)/2} + 1 < r \leqslant t^{j/2} + 1$ and thus $d - 2 \leqslant j \leqslant d$. In particular, $d \not\equiv 1 \ (\mathrm{mod}\ 4)$. For now, we will assume that $d \geqslant 6$, so $\lfloor d/c' \rfloor = 2$ and Lemma 2.4(ii) implies that

$$
\kappa(S, r) \leqslant (r-1)/c' + 1 = 2(r-1)/j + 1.
$$

If $d \equiv 0 \ (\mathrm{mod}\ 4)$ and $d \geqslant 8$ then $j = d - 2$ and

$$
\kappa(T, r) \geqslant \lfloor n/(r-1) \rfloor - 1 \geqslant \left\lfloor \frac{(t^d - 1)/(t+1)}{t^{d/2-1}} \right\rfloor - 1 > \frac{2t^{d/2-1}}{d-2} + 1 \geqslant \frac{2(r-1)}{j} + 1.
$$

Similarly, if $d \equiv 3 \ (\mathrm{mod}\ 4)$ and $d \geqslant 7$, then $j = d-1$ and we see that $\kappa(T, r) > 2(r-1)/j+1$. Now assume $d \equiv 2 \ (\mathrm{mod}\ 4)$, so $d \geqslant 6$ and $j = d$. Here $r$ divides $(t^{d/2} + 1)/(t + 1)$, so

$r - 1 \leqslant (t^{d/2} + 1)/(t+1) - 1 = \alpha$ and thus

$$\kappa(T,r) \geqslant \lfloor n/(r-1) \rfloor - 1 \geqslant \left\lfloor \frac{(t^d - 1)/(t+1)}{\alpha} \right\rfloor - 1 > \frac{2}{d}\left( \frac{t^{d/2} + 1}{t+1} - 1 \right) + 1 \geqslant \frac{2(r-1)}{d} + 1.$$

Therefore, to complete the proof we may assume that $d \in \{3, 4\}$, in which case $j = 2$ and $r$ divides $t + 1$, so $t \geqslant 4$. If $d = 4$ then $\kappa(S, r) \leqslant (r^2 - 3r + 6)/2$ (see Lemma 2.9(ii)) and

$$\kappa(T,r) \geqslant \lfloor n/(r-1) \rfloor - 1 \geqslant \left\lfloor \frac{t^4 - 1}{(t+1)t} \right\rfloor - 1 > \frac{1}{2}(t^2 - t + 4) \geqslant \frac{1}{2}(r^2 - 3r + 6).$$

Finally suppose $d = 3$, so $\kappa(S, r) < r$ by Lemma 2.9(i). If $r < t + 1$ then $r \leqslant (t+1)/2$ and by applying Lemma 2.4(iii) we deduce that $\kappa(T, r) \geqslant 2t - 1 \geqslant r$. Therefore, we may assume that $r = t + 1$, so $t \geqslant 4$ is even. If $S = \mathrm{PSU}_3(4)$ then $r = 5$ and $\kappa(S, r) = 2$, whereas $\kappa(T, r) \geqslant 3$ since $n \geqslant 12$ (note that $T$ is a symplectic group if $n = 12$; see [20, Table 2]). Now assume $t \geqslant 16$ and let $\omega \in \mathbb{F}_{t^2}$ be a primitive $r$-th root of unity. As noted in the proof of Lemma 2.9(i), any subgroup of $\mathrm{PGU}_3(t)$ of order $r$ is conjugate to a subgroup of the form $\langle [1, 1, \omega]Z \rangle$ or $\langle [1, \omega, \omega^k]Z \rangle$ for some $1 < k < r$, where $Z$ denotes the centre of $\mathrm{GU}_3(t)$. In fact, we can exclude $k \in \{2, 4, 8\}$ since

$$[1, \omega, \omega^2]^{(t+2)/2} \sim [1, \omega, \omega^{(t+2)/2}], \quad [1, \omega, \omega^4]^{(3t+4)/4} \sim [1, \omega, \omega^{(3t+4)/4}]$$

and

$$[1, \omega, \omega^8]^{(7t+8)/8} \sim [1, \omega, \omega^{(7t+8)/8}],$$

where $\sim$ denotes $\mathrm{GU}_3(t)$-conjugacy. Therefore, $\kappa(S, r) \leqslant t - 3$ and Lemma 2.4(iii) implies that $\kappa(T, r) \geqslant t - 2$. This completes the proof of the lemma. $\square$

### 5.3.3. Symplectic groups.

**Lemma 5.9.** *Proposition 5.2 holds if $S = \mathrm{PSp}_4(t)'$ and $(t, p) = 1$.*

*Proof.* If $t \in \{2, 3\}$ then $r = 5$ and $\kappa(S, r) = 1$, so for the remainder we may assume that $t \geqslant 4$. By [27] we have

$$n \geqslant \begin{cases} \frac{1}{2}(t^2 - 1) & t \text{ odd} \\ \frac{1}{2}t(t-1)^2 & t \text{ even} \end{cases} \tag{15}$$

Suppose $t = 4$, so $r \in \{5, 17\}$ and $n \geqslant 18$. Now $\kappa(S, 5) = 3$ and $\kappa(S, 17) = 1$, so the result follows from the lower bound on $\kappa(T, r)$ in Lemma 2.4(iii). Next assume $t = 5$, so $r \in \{5, 13\}$ and $n \geqslant 12$. Since $\kappa(S, 5) = 4$ and $\kappa(S, 13) = 1$, we may assume $r = 5$. If $n > 13$ then by inspecting [20, Table 2] we deduce that $n \geqslant 40$ and thus $\kappa(T, 5) \geqslant 5$. Therefore, we may assume that $n \in \{12, 13\}$. By considering the corresponding Frobenius-Schur indicator in [20, Table 2] we see that $T = \mathrm{PSp}_{12}(q)$ or $\Omega_{13}(q)$. Set $i = \Phi(r, q)$ as before and note that $i \in \{1, 2, 4\}$. In fact, $i = 4$ is the only possibility since $c \geqslant 3$, so $q^2 \equiv -1 \pmod 5$. However, by inspecting the irrationalities of the corresponding Brauer character in [20, Table 2], we see that $q^2 \equiv 1 \pmod 5$, which is a contradiction.

For the remainder we may assume that $t \geqslant 7$, in which case (10) implies that

$$r \geqslant \left\lceil \frac{1}{2}\sqrt{(t^2 - 1)/2} \right\rceil + 1 > \log_\ell t$$

and thus every element in $H_0$ of order $r$ is contained in $S$.

First assume $r = \ell$, so $t$ is odd. According to [9, Proposition 3.4.10], $S$ has six classes of elements of order $r$, and Lemma 2.4(iii) implies that

$$\kappa(T,r) \geqslant \lfloor n/(t-1) \rfloor - 1 \geqslant \lfloor (t+1)/2 \rfloor - 1 = (t-1)/2.$$

Therefore, we may assume that $t \in \{7, 11, 13\}$. In each of these cases one checks that $\kappa(S, r) = 4$, so we can assume $r = t = 7$ and $c \in \{3, 6\}$. Note that $n \geqslant 24$. If $c = 3$ then $\kappa(T, r) \geqslant \lfloor 24/3 \rfloor - 1 = 7$, so we can assume $c = 6$. If $n > 25$ then $n \geqslant 126$ (see [20, Table 2]) and the desired result follows, so let us assume that $n \in \{24, 25\}$. Suppose $x \in S$ has order 7 and let $\chi$ be the corresponding Brauer character. Since $c = 6$, each nontrivial 7-th root of unity occurs as an eigenvalue of $x$ with equal multiplicity (in terms of the action of $x$ on $\bar{V} = V \otimes K$, where $K$ is the algebraic closure of $\mathbb{F}_q$), so $\chi(x)$ is an integer. However, [20, Table 2] indicates that $\chi$ has a $b7$ irrationality in the standard Atlas notation, which means that $\chi(x)$ is not an integer for some $x \in S$ of order 7. Therefore, $c \neq 6$ when $n \in \{24, 25\}$ and the result follows.

Now assume $r \neq \ell$. Set $j = \Phi(r, t)$ and note that $j \in \{1, 2, 4\}$. If $j = 4$ then $\kappa(S, r) = 1$, so we may assume that $j \in \{1, 2\}$, in which case $r \leqslant t + 1$ and $\kappa(S, r) \leqslant (r + 1)/2$ (see Lemma 2.4(ii)). If $t$ is even then a combination of (15) and Lemma 2.4(iii) implies that $\kappa(T, r) > t/2 + 1$. Similarly, if $t$ is odd then $r \leqslant (t + 1)/2$ and the same conclusion holds. $\qquad \square$

**Lemma 5.10.** *Proposition 5.2 holds if $S = \mathrm{PSp}_6(t)$ and $(t, p) = 1$.*

*Proof.* If $t = 2$ then $r \in \{5, 7\}$ and $\kappa(S, r) = 1$. For the remainder we may assume that $t \geqslant 3$, in which case [27] gives

$$n \geqslant \begin{cases} \frac{1}{2}(t^3 - 1) & t \text{ odd} \\ \frac{1}{2}t^2(t^2 - 1)(t - 1) & t \text{ even} \end{cases} \tag{16}$$

In particular, $r \geqslant \lceil \frac{1}{2}\sqrt{(t^3 - 1)/2} \rceil + 1 > \log_\ell t$. In fact, the same bound implies that $r > t$ if $t \geqslant 7$, so if $r = \ell$ then $t = 5$ is the only possibility. Now $S = \mathrm{PSp}_6(5)$ has 13 classes of elements of order 5, but $T$ has at least $\lfloor 62/(5 - 1) \rfloor = 15$ since $n \geqslant 62$.

Now assume $r \neq \ell$. Set $j = \Phi(r, t)$ and note that $j \in \{1, 2, 3, 4, 6\}$. If $j > 2$ then $\kappa(S, r) = 1$ and the result follows. Now assume that $j \in \{1, 2\}$, so $r \leqslant t + 1$. By arguing as in the proof of Lemma 2.9(iii) we see that $\kappa(S, r) \leqslant (r^2 + 15)/8$ and in the usual way, via (16) and Lemma 2.4, it is easy to check that $\kappa(T, r) > \kappa(S, r)$. $\qquad \square$

**Lemma 5.11.** *Proposition 5.2 holds if $S = \mathrm{PSp}_d(t)'$ and $(t, p) = 1$.*

*Proof.* We may assume $d \geqslant 8$. By [27] we have

$$n \geqslant \begin{cases} \frac{1}{2}(t^{d/2} - 1) & t \text{ odd} \\ \frac{1}{2}t^{d/2-1}(t^{d/2-1} - 1)(t - 1) & t \text{ even} \end{cases} \tag{17}$$

and (10) implies that $r > t^{(d-4)/4} + 1$. In particular, $r \neq \ell$ and every element in $H_0$ of order $r$ is contained in $S$. Let $j = \Phi(r, t)$ and set $c' = 2j$ if $j$ is odd, and $c' = j$ if $j$ is even.

If $j$ is odd and $j > d/4$ then $c' > d/2$ and thus $\kappa(S, r) = 1$. The same conclusion holds if $j$ is even and $j > d/2$. Note that if $j$ is even then $r$ divides $t^{j/2} + 1$, so the bound $r > t^{(d-4)/4} + 1$ implies that $j > (d - 4)/2$. Therefore, we may assume that one of the following holds:

    (a) $j$ odd: Either $d \equiv 4 \pmod 8$ and $j = d/4$, or $d \equiv 6 \pmod 8$ and $j = (d - 2)/4$.

    (b) $j$ even: Either $d \equiv 0 \pmod 4$ and $j = d/2$, or $d \equiv 2 \pmod 4$ and $j = (d - 2)/2$.

First assume that $j$ is odd and $d \equiv 4 \pmod 8$, so $d \geqslant 12$, $c' = d/2$ and $r$ divides $t^{d/4} - 1$. Since $\lfloor d/c' \rfloor = 2$, Lemma 2.4(ii) implies that $\kappa(S, r) \leqslant 2(r - 1)/d + 1$, whereas $T$ has at least

$$\lfloor n/(r - 1) \rfloor - 1 \geqslant \left\lfloor \frac{(t^{d/2} - 1)/2}{t^{d/4} - 2} \right\rfloor - 1 \geqslant \frac{1}{2}t^{d/4} - 1 \geqslant \frac{1}{2}(r - 1) > 2(r - 1)/d + 1$$

such classes. A similar argument applies if $j$ is odd and $d \equiv 6 \pmod 8$.

Next assume $j$ is even and $d \equiv 2 \pmod 4$, so $d \geqslant 10$, $c' = (d-2)/2$ and $r$ divides $t^{(d-2)/4} + 1$. In addition, since $\lfloor d/c' \rfloor = 2$ we have $\kappa(S, r) \leqslant 2(r-1)/(d-2) + 1$. By applying Lemma 2.4(iii) and the lower bound on $n$ given in (17), it is easy to check that $\kappa(T, r) \geqslant t^{(d-2)/4}$. The desired result follows since $t^{(d-2)/4} \geqslant r - 1 > 2(r-1)/(d-2) + 1$.

Finally, suppose that $j$ is even and $d \equiv 0 \pmod 4$, in which case $d \geqslant 8$, $c' = d/2$ and $r$ divides $t^{d/4} + 1$. In particular, $\kappa(S, r) \leqslant 2(r-1)/d + 1$. We claim that $\kappa(T, r) \geqslant t^{d/4}$, which is sufficient since $t^{d/4} \geqslant r - 1 > 2(r-1)/d + 1$. If $t$ is even, this follows in the usual way via Lemma 2.4(iii) and (17). If $t$ is odd then $t^{d/4} + 1$ is even and thus $r$ divides $(t^{d/4} + 1)/2$, whence Lemma 2.4(iii) implies that

$$\kappa(T, r) \geqslant \lfloor n/(r-1) \rfloor - 1 \geqslant \left\lfloor \frac{(t^{d/2} - 1)/2}{(t^{d/4} - 1)/2} \right\rfloor - 1 = t^{d/4}$$

as claimed. $\qquad\square$

### 5.3.4. *Orthogonal groups.*

**Lemma 5.12.** *Proposition 5.2 holds if $S = \mathrm{P\Omega}_d^\epsilon(t)$ and $(t, p) = 1$.*

*Proof.* We may assume that $d \geqslant 7$, with $t$ odd if $d$ is odd. If $S = \Omega_7(3)$ then $r \in \{5, 7, 13\}$ and $\kappa(S, r) = 1$. Next assume $S = \Omega_8^+(2)$. Here $r \in \{5, 7\}$ with $\kappa(S, 5) = 3$ and $\kappa(S, 7) = 1$. By [27] we have $n \geqslant 8$. If $n = 8$ then $T = \mathrm{P\Omega}_8^+(p)$ and this is the case labelled $(\mathcal{B}4)$ in Table 2. Therefore, we may assume that $n > 8$, in which case $n \geqslant 28$ (see [20, Table 2]) and thus Lemma 2.4(iii) implies that $\kappa(T, 5) \geqslant 6$.

In each of the remaining cases, the Landazuri-Seitz [27] bounds imply that

$$n \geqslant \begin{cases} (t^{(d-2)/2} + 1)(t^{(d-4)/2} - 1) & d \text{ even} \\ t^{(d-3)/2}(t^{(d-3)/2} - 1) & d \text{ odd.} \end{cases}$$

Suppose $d$ is odd. Then

$$r \geqslant \lceil \sqrt{n}/2 \rceil + 1 \geqslant \left\lceil \frac{1}{2}\sqrt{t^{(d-3)/2}(t^{(d-3)/2} - 1)} \right\rceil + 1 > t^{(d-1)/4} + 1$$

and thus $r \neq \ell$ and every element in $H_0$ of order $r$ is contained in $S$. Set $j = \Phi(r, t)$ and $c' = 2j$ if $j$ is odd, otherwise $c' = j$. Note that the above lower bound on $r$ implies that $j > (d-1)/4$. If $j$ is odd then $c' > (d-1)/2$ and thus $c' \geqslant (d+1)/2$ and $\kappa(S, r) = 1$. Similarly, if $j$ is even then $r$ divides $t^{j/2} + 1$, so $c' > (d-1)/2$ and the same conclusion holds.

Finally, let us assume $d$ is even. The cases with $d = 8$ and $t \in \{2, 3\}$ can be checked directly. For example, if $S = \mathrm{P\Omega}_8^+(3)$ then $r \in \{5, 7, 13\}$. If $r \in \{7, 13\}$ then $c' = 6$ and thus $\kappa(S, r) = 1$. If $r = 5$ then $c' = 4$ and $\kappa(S, r) = 2$, but $n \geqslant 224$ and thus $\kappa(T, r) > 2$. In all of the remaining cases we have

$$r \geqslant \lceil \sqrt{n}/2 \rceil + 1 \geqslant \left\lceil \frac{1}{2}\sqrt{(t^{(d-2)/2} + 1)(t^{(d-4)/2} - 1)} \right\rceil + 1 > t^{d/4} + 1$$

and by arguing as in the $d$ odd case we deduce that $\kappa(S, r) = 1$. $\qquad\square$

### 5.3.5. *Exceptional groups.*

**Lemma 5.13.** *Proposition 5.2 holds if $S \in \{E_7(t), E_8(t)\}$ and $(t, p) = 1$.*

*Proof.* First assume $S = E_8(t)$. Here $n \geqslant t^{27}(t^2 - 1)$ by [27], so (10) implies that

$$r \geqslant \lceil \sqrt{n}/2 \rceil + 1 \geqslant \left\lceil \frac{1}{2}\sqrt{t^{27}(t^2 - 1)} \right\rceil + 1 > t^{13}.$$

Therefore $r$ divides $|S|$, $r \neq \ell$ and by considering the order of $S$ we deduce that $j = \Phi(r, t) \in \{14, 18, 20, 24, 30\}$. Hence $r$ divides $t^{j/2} + 1$, so $j = 30$ is the only possibility. However, if $j = 30$ then $r$ divides $(t^{15}+1)/(t^5+1) = t^{10} - t^5 + 1$, which is incompatible with the bound $r > t^{13}$. The case $S = E_7(t)$ is entirely similar, using the bound $n \geqslant t^{15}(t^2 - 1)$ from [27]. $\qquad\square$

**Lemma 5.14.** *Proposition 5.2 holds if $S \in \{E_6(t), {}^2E_6(t)\}$ and $(t, p) = 1$.*

*Proof.* Here $n \geqslant t^9(t^2 - 1)$ (see [25, Table 5.3.A]) and we deduce that $r > t^4 + 1$. Set $j = \Phi(r, t)$ and first assume $S = E_6(t)$. Since $r > t^4 + 1$ and $r$ divides $|S|$, it follows that $j \in \{9, 12\}$. If $j = 12$ then $r$ divides $(t^6 + 1)/(t^2 + 1) = t^4 - t^2 + 1$, which contradicts the bound $r > t^4 + 1$. Now assume $j = 9$, in which case $r$ divides $(t^9 - 1)/(t^3 - 1) = t^6 + t^3 + 1$. By inspecting the structure of the maximal tori in $S$ (see [24, Section 2.7], for example), it follows that every subgroup of $S$ of order $r$ is contained in a cyclic maximal torus of order $t^6 + t^3 + 1$. Since $S$ has a unique class of such maximal tori, we deduce that $\kappa(S, r) = 1$ and the result follows.

A very similar argument applies if $S = {}^2E_6(t)$. Here $j \in \{10, 12, 18\}$ and we can rule out $j = 12$ as above. Similarly, if $j = 10$ then $r$ divides $(t^5 + 1)/(t + 1)$, but this is not possible since $r > t^4 + 1$. Finally, if $j = 18$ then $r$ divides $t^6 - t^3 + 1$, which implies that every subgroup of $S$ of order $r$ is contained in a cyclic maximal torus of order $t^6 - t^3 + 1$. Once again we deduce that $\kappa(S, r) = 1$ since $S$ has a unique class of such tori. $\qquad\square$

**Lemma 5.15.** *Proposition 5.2 holds if $S \in \{F_4(t), {}^2F_4(t)'\}$ and $(t, p) = 1$.*

*Proof.* First assume that $S = F_4(2)$, so $r \in \{5, 7, 13, 17\}$ and $n \geqslant 44$ (see [27]). If $r \in \{5, 13, 17\}$ then the character table of $S$ indicates that $\kappa(S, r) = 1$, so we may assume $r = 7$. Now $S$ has two classes of subgroups of order 7, but Lemma 2.4(iii) implies that $T$ has at least $\lfloor 44/6 \rfloor - 1 = 6$ such classes. The result follows.

Next suppose that $S = F_4(t)$ and $t \geqslant 3$. Here $n \geqslant t^6(t^2 - 1)$ (see [25, Table 5.3.A]) and thus

$$r \geqslant \left\lceil \frac{1}{2}\sqrt{t^6(t^2 - 1)} \right\rceil + 1 > t^3 + 1.$$

Set $j = \Phi(r, t)$. Since $r$ divides $|S|$ and $r > t^3 + 1$, it follows that $j \in \{8, 12\}$. If $j = 12$ then $r$ divides $(t^6 + 1)/(t^2 + 1) = t^4 - t^2 + 1$ and we deduce that every subgroup of $S$ of order $r$ is contained in a cyclic maximal torus of order $t^4 - t^2 + 1$. But there is a unique conjugacy class of such tori, whence $\kappa(S, r) = 1$. An entirely similar argument applies if $j = 8$, using the fact that $S$ has a unique class of cyclic maximal tori of order $t^4 + 1$.

Now assume $S = {}^2F_4(t)'$, so $t = 2^{2m+1}$ with $m \geqslant 0$. If $t = 2$ then $r \in \{5, 13\}$ and by inspecting the character table of $S$ we deduce that $\kappa(S, r) = 1$. Now assume $t \geqslant 8$. Here [27] gives $n \geqslant t^4(t - 1)\sqrt{t/2}$, which implies that $r > t^2 + 1$. Set $j = \Phi(r, t)$ and observe that $j \in \{6, 12\}$. If $j = 6$ then $r$ divides $(t^3 + 1)/(t + 1) = t^2 - t + 1$, which contradicts the bound $r > t^2 + 1$. Now assume $j = 12$, in which case $r$ divides

$$\frac{t^6 + 1}{t^2 + 1} = (t^2 - \sqrt{2t^3} + t - \sqrt{2t} + 1)(t^2 + \sqrt{2t^3} + t + \sqrt{2t} + 1).$$

Since $r > t^2 + 1$ it follows that $r$ divides $t^2 + \sqrt{2t^3} + t + \sqrt{2t} + 1$ and we deduce that every subgroup of $S$ of order $r$ is contained in a cyclic maximal torus in $S$ of order $t^2 + \sqrt{2t^3} + t + \sqrt{2t} + 1$. The result now follows since $S$ has a unique conjugacy class of such tori and thus $\kappa(S, r) = 1$. $\qquad\square$

**Lemma 5.16.** *Proposition 5.2 holds if $S \in \{{}^2B_2(t), G_2(t)', {}^2G_2(t)'\}$ and $(t, p) = 1$.*

*Proof.* First assume $S = {}^2B_2(t)$, so $t = 2^{2m+1}$ and $m \geqslant 1$. If $t = 8$ then $r \in \{5, 7, 13\}$ and $\kappa(S, r) = 1$. Now assume $t \geqslant 32$, so $n \geqslant (t-1)\sqrt{t/2}$ by [27]. Therefore $r > \log_2 t$ by (10), so every element in $H_0$ of order $r$ is contained in $S$. The maximal tori of $S$ are cyclic of order $t-1$, $t + \sqrt{2t} + 1$ and $t - \sqrt{2t} + 1$, and $S$ has a unique class of tori of each order. Since these orders are pairwise coprime, it follows that $\kappa(S, r) = 1$ and the result follows.

Next assume that $S = G_2(t)'$. If $t \in \{2, 3\}$ then $r \in \{7, 13\}$ and $\kappa(S, r) = 1$. If $t = 4$ then $n \geqslant 12$ (see [25, Table 5.3.A]) and $r \in \{5, 7, 13\}$. We have $\kappa(S, r) = 1$ if $r \in \{7, 13\}$, so we may assume $r = 5$ and thus $\kappa(S, r) = 2$. The result now follows from Lemma 2.4(iii) since $T$ is a symplectic group when $n = 12$ (see [20, Table 2]). Now assume $t \geqslant 5$. Here [27] gives $n \geqslant t(t^2 - 1)$ and thus

$$r \geqslant \left\lceil \frac{1}{2}\sqrt{t(t^2 - 1)} \right\rceil + 1 > t + 1.$$

Set $j = \Phi(r, t)$ and note that $j \in \{3, 6\}$ since $r$ divides $|S|$ and $r > t + 1$. If $j = 3$ then $r$ divides $t^2 + t + 1$ and we deduce that every subgroup of $S$ of order $r$ is contained in a cyclic maximal torus of order $t^2 + t + 1$. Since $S$ has a unique class of such tori, we see that $\kappa(S, r) = 1$. An entirely similar argument applies if $j = 6$.

Finally, let us assume $S = {}^2G_2(t)'$, where $t = 3^{2m+1}$ and $m \geqslant 0$. If $t = 3$ then $r = 7$ and $\kappa(S, r) = 1$. Now assume $t \geqslant 27$. By [27] we have $n \geqslant t(t - 1)$ and thus

$$r \geqslant \left\lceil \frac{1}{2}\sqrt{t(t - 1)} \right\rceil + 1 > \frac{1}{2}(t + 1)$$

so $r > \log_3 t$. Set $j = \Phi(r, t)$ and observe that $j \in \{1, 2, 6\}$. If $j = 1$ then $r$ divides $(t - 1)/2$, which is incompatible with the bound $r > (t + 1)/2$. Similarly, if $j = 2$ then $r$ divides $(t + 1)/2$ and once again we have reached a contradiction. Finally, suppose that $j = 6$, in which case $r$ divides

$$\frac{t^3 + 1}{t + 1} = t^2 - t + 1 = (t + \sqrt{3t} + 1)(t - \sqrt{3t} + 1).$$

If $r$ divides $t + \sqrt{3t} + 1$ then every subgroup of $S$ of order $r$ is contained in a cyclic maximal torus of order $t + \sqrt{3t} + 1$; there is a unique class of such tori, so $\kappa(S, r) = 1$. A very similar argument applies if $r$ divides $t - \sqrt{3t} + 1$. $\qquad \square$

**Lemma 5.17.** *Proposition 5.2 holds if $S = {}^3D_4(t)$ and $(t, p) = 1$.*

*Proof.* Here [27] gives $n \geqslant t^3(t^2 - 1)$. First assume $t = 2$, so $r \in \{7, 13\}$ and $n \geqslant 24$. Since $\kappa(S, 7) = 2$ and $\kappa(S, 13) = 1$, the result follows from Lemma 2.4(iii).

Next assume $t = 3$, so $r \in \{7, 13, 73\}$ and $n \geqslant 216$. If $r = 73$ then $\kappa(S, r) = 1$ by Sylow's Theorem. Similarly, if $r \in \{7, 13\}$ then the Sylow $r$-subgroups of $S$ are isomorphic to $Z_r \times Z_r$, which implies that $\kappa(S, r) \leqslant r + 1$. But Lemma 2.4(iii) implies that $T$ has at least $\lfloor 216/12 \rfloor - 1 = 17$ such classes, so the result follows. The case $t = 4$ is entirely similar (here $r \in \{5, 7, 13, 241\}$ and $n \geqslant 960$).

To complete the proof of the lemma, we may assume that $t \geqslant 5$. First observe that

$$r \geqslant \left\lceil \frac{1}{2}\sqrt{t^3(t^2 - 1)} \right\rceil + 1 > t^2 + 1.$$

In particular, $j = \Phi(r, t) \in \{3, 6, 12\}$. If $j = 6$ then $r$ divides $(t^3 + 1)/(t + 1) = t^2 - t + 1$, but this contradicts the bound $r > t^2 + 1$. Next suppose that $j = 12$, so $r$ divides $(t^6 + 1)/(t^2 + 1) = t^4 - t^2 + 1$. Every subgroup of $S$ of order $r$ is contained in a cyclic maximal torus of order $t^4 - t^2 + 1$; since $S$ has a unique class of such tori, it follows that $\kappa(S, r) = 1$.

Finally, let us assume that $j = 3$, so $r$ divides $(t^3 - 1)/(t - 1) = t^2 + t + 1$. If $t \geqslant 7$ then the bound $r \geqslant \left\lceil \sqrt{t^3(t^2 - 1)}/2 \right\rceil + 1$ implies that $r > t^2 + t + 1$, so we may assume that $t = 5$ and thus $r = 31$. The Sylow 31-subgroups of $S$ are isomorphic to $Z_{31} \times Z_{31}$, so $\kappa(S, 31) \leqslant 32$. But $n \geqslant 3000$ so Lemma 2.4(iii) implies that $\kappa(T, 31) \geqslant 99$. $\qquad \square$

This completes the proof of Proposition 5.2 in the case where $S$ is a simple group of Lie type in non-defining characteristic.

5.4. **Groups of Lie type: Defining characteristic.** In this final section we complete the proof of Proposition 5.2 by considering the case where $S$ is a simple group of Lie type over $\mathbb{F}_{p^e}$, for some positive integer $e$.

Let $K$ be the algebraic closure of $\mathbb{F}_p$, let $M$ be a $K\hat{S}$-module affording a representation $\rho$ and let $\gamma$ be an automorphism of $\hat{S}$. Following [25, p.192], we write $M^\gamma$ for the space $M$ with $\hat{S}$-action given by the representation $\gamma\rho$ (acting on the right) and we say that the $K\hat{S}$-modules $M$ and $M^\gamma$ are quasiequivalent. In particular, if $\gamma$ is a field automorphism of $\hat{S}$ induced by the map $\lambda \mapsto \lambda^p$ on $K$ then we will write $M^{\gamma^z} = M^{(z)}$ for all $z \in \mathbb{N}$.

By a theorem of Steinberg [35], the irreducible $K\hat{S}$-modules are parameterised by an appropriate set of weights for the ambient simple algebraic group $\bar{S}$ over $K$, with respect to a fixed set of fundamental dominant weights. We will write $\{\lambda_1, \ldots, \lambda_k\}$ for the latter weights, where we adopt the standard labelling given in Bourbaki [3]. In addition, $L(\lambda)$ will denote the irreducible $K\bar{S}$-module with highest weight $\lambda$. Note that if $M$ is an irreducible $K\hat{S}$-module and $\gamma$ is an automorphism of $\hat{S}$, then the highest weight of $M^\gamma$ can be read off from [25, Proposition 5.4.2]. Similarly, the highest weight of the dual module $M^*$ is described in [25, Proposition 5.4.3]. We refer the reader to [25, Section 5.4] and the references therein for further details.

5.4.1. *S is untwisted.* To begin with, we will assume $S$ is an untwisted simple group of Lie type over $\mathbb{F}_{p^e}$. Recall that $T$ is a finite simple classical group over $\mathbb{F}_q$ with natural module $V$, where $q = p^f$. Set $q' = p^{f'}$, where $f' = 2f$ if $T = \mathrm{PSU}_n(q)$, otherwise $f' = f$. Also recall that $V$ is an absolutely irreducible $\mathbb{F}_{q'}\hat{S}$-module which cannot be realised over a proper subfield of $\mathbb{F}_{q'}$ (see Definition 2.10). By applying [25, Proposition 5.4.6(i)] we deduce that $f'$ divides $e$ and there exists an irreducible $K\hat{S}$-module $M$ such that

$$\bar{V} = V \otimes K \cong M \otimes M^{(f')} \otimes M^{(2f')} \otimes \cdots \otimes M^{(e-f')} \tag{18}$$

(with $e/f'$ factors) as $K\hat{S}$-modules. Set $\ell = \dim M$ and note that $\ell \geqslant 2$ and $n = \ell^{e/f'}$.

We need a couple of preliminary lemmas.

**Lemma 5.18.** *Let $J$ be a finite group and let $V_1$ and $V_2$ be faithful finite dimensional $KJ$-modules, where $K$ is an algebraically closed field and $\dim V_i \geqslant 2$, $i = 1, 2$. Let $x \in J$ be a nontrivial element such that the action of $x$ on $V_1$ has a repeated eigenvalue. Then $x$ has a nontrivial repeated eigenvalue on $V_1 \otimes V_2$.*

*Proof.* This is an easy exercise. $\qquad \square$

**Lemma 5.19.** *Let $\bar{S} = \mathrm{SL}_d(K)$, where $d \geqslant 6$ and $K$ is an algebraically closed field of characteristic $p \geqslant 0$. Let $\bar{V} = L(\lambda)$ be an $n$-dimensional irreducible self-dual $K\bar{S}$-module with $n \leqslant 4d^2$. Then either $\bar{V}$ is the adjoint module, or*

$$(d, \lambda) \in \{(6, \lambda_3), (6, 2\lambda_3), (8, \lambda_4), (10, \lambda_5)\} \tag{19}$$

*up to quasiequivalence.*

*Proof.* We follow the proof of [5, Proposition 2.5]. Write $\lambda = \sum_{j=1}^{d-1} a_j \lambda_j$ where each $a_j$ is a non-negative integer. By self-duality, we have $a_j = a_{d-j}$ for all $j$. To begin with, let us assume that $\lambda$ is $p$-restricted (that is, $a_j < p$ for all $j$). If $d \leqslant 18$ then the result can be checked by inspecting the relevant tables in [31], so we may assume that $d \geqslant 19$. Let $\mathcal{W} \cong S_d$ be the Weyl group of $\bar{S}$, which acts naturally on the set of weights of $\bar{V}$.

Suppose $a_2 \neq 0$. By arguing as in the proof of [5, Proposition 2.5] we see that the $\mathcal{W}$-stabiliser of $\lambda$ is contained in a parabolic subgroup of type $A_1 \times A_{d-5} \times A_1$ and thus

$$n \geqslant |\mathcal{W} \cdot \lambda| = |\mathcal{W} : \mathcal{W}_\lambda| \geqslant \frac{|S_d|}{|S_2|^2 |S_{d-4}|} = \frac{1}{4}d(d-1)(d-2)(d-3) > 4d^2,$$

where $\mathcal{W} \cdot \lambda$ denotes the $\mathcal{W}$-orbit of $\lambda$. Therefore $a_2 = a_{d-2} = 0$. In this way, we quickly reduce the problem to the case where

$$\lambda = \begin{cases} a\lambda_1 + a\lambda_{d-1} & d \text{ odd} \\ a\lambda_1 + b\lambda_{d/2} + a\lambda_{d-1} & d \text{ even} \end{cases}$$

If $d$ is even and $b \neq 0$ then the $\mathcal{W}$-stabiliser of $\lambda$ is contained in a parabolic subgroup of type $A_{d/2-1} \times A_{d/2-1}$ and thus $n \geqslant d!/((d/2)!^2) > 4d^2$. Finally, we can repeat the argument in the proof of [5, Proposition 2.5] to see that $a = 1$ is the only option, so $\lambda = \lambda_1 + \lambda_{d-1}$ and thus $\bar{V}$ is the adjoint module.

Finally, let us relax the assumption that $\lambda$ is $p$-restricted. Write $\lambda = \mu_0 + p\mu_1 + \cdots + p^{e-1}\mu_{e-1}$, where each $\mu_i$ is $p$-restricted, so by Steinberg's tensor product theorem we have

$$\bar{V} = L(\lambda) \cong L(\mu_0) \otimes L(\mu_1)^{(1)} \otimes \cdots \otimes L(\mu_{e-1})^{(e-1)}.$$

If three or more of the $\mu_i$ are nonzero then $n \geqslant d^3 > 4d^2$, which is a contradiction. Next suppose two are nonzero, say $\lambda = p^i\mu_i + p^j\mu_j$ with $i \neq j$, so $n = \dim L(\mu_i) \cdot \dim L(\mu_j)$. The self-duality of $\bar{V}$ implies that $L(\mu_i)$ and $L(\mu_j)$ are also self-dual and thus the result in the $p$-restricted case rules out this situation for dimension reasons. Finally, if $\lambda = p^i\mu_i$ then $\mu_i$ is self-dual and $\bar{V}$ is quasiequivalent to $L(\mu_i)$. The result follows. $\qquad\square$

**Lemma 5.20.** *Proposition 5.2 holds if $S$ is untwisted and $e > f'$.*

*Proof.* First assume $\ell > 2$, where $\ell$ denotes the dimension of $M$ in (18). Fix an element $x \in T$ of order $r$ with $\nu(x) = c$, where $r \neq p$ and $r > 2$ (see Remark 2.3). We claim that $x$ is a derangement. In order to see this, we need to show that if $g \in H_0$ has order $r$, then $g$ is not $T$-conjugate to $x$. For instance, it suffices to show that $\nu(g) \neq c$, or that $g$ has a nontrivial repeated eigenvalue on $\bar{V}$.

Let $g \in H_0$ be an element of order $r$. If $g$ is a field automorphism then it must induce a fixed point free permutation on the $e/f'$ factors in the tensor product decomposition (18) (in particular, $r$ divides $e/f'$). This implies that $g$ has nontrivial repeated eigenvalues on $\bar{V}$, so it is not conjugate to $x$. To complete the argument, we may assume that $g$ is an inner-diagonal automorphism (recall that $r \geqslant 5$) and thus $g$ stabilises each of the tensor factors in (18). Let $\nu_1(g)$ and $\nu(g)$ denote the codimension of the largest eigenspace of $g$ on $M$ and $\bar{V}$, respectively. By applying [30, Lemma 3.7], we deduce that

$$\nu(g) \geqslant \nu_1(g)n/\ell. \tag{20}$$

If $\nu_1(g) < \ell - 1$ then Lemma 5.18 implies that $g$ has a nontrivial repeated eigenvalue on $\bar{V}$, so we may assume that $\nu_1(g) = \ell - 1$. Then (20) gives $\nu(g) > n/2$ and thus $g$ is not $T$-conjugate to $x$ (since $\nu(x) = c \leqslant n/2$).

Now assume $\ell = 2$, so $S = \mathrm{PSL}_2(p^e)$ is the only possibility. The previous argument shows that the element $x \in T$ above is a derangement if $c < n/2$, so we may assume that $c = n/2$. Here (10) implies that

$$r \geqslant c + 1 = n/2 + 1 = 2^{e/f'-1} + 1 > e/f',$$

so every element in $H_0$ of order $r$ is contained in $S$ (indeed, if $g \in H_0 \setminus S$ has order $r$, then $g$ is a field automorphism and $r$ divides $e/f'$, as noted above). Since $S$ has a unique conjugacy class of subgroups of order $r$, we conclude that $T$ contains derangements of order $r$. $\qquad\square$

**Lemma 5.21.** *Proposition 5.2 holds if $S$ is untwisted and $e = f'$.*

*Proof.* Set $q' = p^{f'}$ as before, so $f' = 2f$ if $T = \mathrm{PSU}_n(q)$, otherwise $f' = f$. Here $\bar{V} \cong M$ for some irreducible $K\hat{S}$-module $M$, which is not quasiequivalent to the natural module for $\hat{S}$ (see Definition 2.10). Note that every element of order $r$ in $H_0$ is inner-diagonal.

First assume $T = \mathrm{PSU}_n(q)$, in which case $M \cong (M^*)^{(f)}$, where $M^*$ denotes the dual of $M$ (see [25, Lemma 2.10.15(ii)], for example). By considering this isomorphism at the level of highest weights, and by applying Steinberg's tensor product theorem, we deduce that $M$ is isomorphic to a tensor product of two or more nontrivial irreducible $K\hat{S}$-modules. For example, if $S = \mathrm{PSL}_3(q^2)$ and $M$ has highest weight $\lambda_1 + q\lambda_2$, then $M \cong L(\lambda_1) \otimes L(\lambda_2)^{(f)}$ is 9-dimensional and $M \cong (M^*)^{(f)}$, so this yields an embedding of $S$ in $\mathrm{PSU}_9(q)$. By expressing $M$ as a tensor product in this way, we can repeat the argument in the proof of Lemma 5.20 to see that every element $x \in T$ of order $r$ with $\nu(x) = c$ is a derangement.

For the remainder of the proof we may assume that $T \neq \mathrm{PSU}_n(q)$, so $q = q'$. We will start by assuming $S$ is a classical group, with a $d$-dimensional natural module. Set $i = \Phi(r, q)$ and

$$c' = \begin{cases} 2i & \text{if } i \text{ is odd and } S \neq \mathrm{PSL}_d(q) \\ i/2 & \text{if } i \equiv 2 \ (\mathrm{mod}\ 4) \text{ and } S = \mathrm{PSU}_d(q) \\ i & \text{otherwise} \end{cases} \tag{21}$$

Note that if $c' > d/2$ then $\kappa(S, r) = 1$ by Lemma 2.4(i), so we may assume that $c' \leqslant d/2$. In addition, note that if $c' \geqslant c$ and $n > 2d$ then Lemma 2.8 implies that $\kappa(T, r) > \kappa(S, r)$ and thus $T$ contains derangements of order $r$.

*Case 1.* $S = \mathrm{PSp}_d(q)$, $d \geqslant 4$

First observe that $V$ is self-dual and thus $T$ is a symplectic or orthogonal group (see [25, Lemma 2.10.15(i) and Proposition 5.4.3]). In particular, $c' = c$ is even, so $c' \geqslant 4$ and thus $d \geqslant 8$ since we are assuming that $c' \leqslant d/2$. If $d \geqslant 12$ then [31, Theorems 4.4 and 5.1] imply that $n \geqslant (d^2 - d - 4)/2 > 2d$ and the result follows from Lemma 2.8. Similarly, if $d \in \{8, 10\}$ then $n \geqslant 2^{d/2}$ (see [31, Tables A.33 and A.34]) and we reduce to the case $d = 8$ with $n = 16$. Here $c' = c = 4$ and it is easy to see that $\kappa(S, r) < \kappa(T, r)$.

*Case 2.* $S \in \{\mathrm{P\Omega}_d^+(q), \Omega_d(q)\}$, $d \geqslant 7$

First assume that $V$ is self-dual, so $T$ is symplectic or orthogonal, and $c' = c$ is even. In particular, note that $d \geqslant 8$. Suppose $d$ is even. If $n \geqslant (d^2 - d - 4)/2$ then $n > 2d$ and the result follows as in Case 1. Therefore, by applying [31, Theorems 4.4 and 5.1], we may assume that $d \in \{8, 12\}$ and $n = 2^{d/2-1}$. If $d = 12$ then $n > 2d$ and the result follows as before. We can discard the case $d = 8$ since $S \not\cong T$. Now assume $d \geqslant 9$ is odd. By arguing as above we may assume that $n < (d^2 - d - 4)/2$, so $d \leqslant 23$ by [31, Theorem 5.1]. In each of the remaining cases it is easy to check that $n > 2d$ by inspecting the relevant tables in [31, Appendix A], unless $d = 9$ and $n = 16$. In the latter case, $c' = c = 4$ and $\kappa(S, r) < \kappa(T, r)$. Finally, if $V$ is not self-dual then $S = \mathrm{P\Omega}_d^+(q)$ with $d \equiv 2 \ (\mathrm{mod}\ 4)$ (see [25, Proposition 5.4.3]) and $T = \mathrm{PSL}_n(q)$. Here $c' \geqslant c$ and the above argument goes through.

*Case 3.* $S = \mathrm{PSL}_d(q)$, $d \geqslant 2$

If $d = 2$ then $\kappa(S, r) = 1$ so we may assume that $d \geqslant 3$. If $V$ is not self-dual, then $T = \mathrm{PSL}_n(q)$, $c' = c = i$ and $d \geqslant 6$. By applying [31, Theorems 4.4 and 5.1] we see that $n \geqslant d(d-1)/2 > 2d$. Similarly, if $V$ is self-dual and $i$ is even, then $c' = c = i \leqslant d/2$ and $n \geqslant d^2 - 2 > 2d$. In both cases, the desired result follows from Lemma 2.8.

Finally, let us assume $V$ is self-dual and $i$ is odd. Here $c' = i < 2i = c$ so we cannot appeal to Lemma 2.8. First observe that $i \geqslant 3$ and thus $d \geqslant 6$. Also recall that $c \geqslant \sqrt{n}/2$ and $c' \leqslant d/2$, hence $n \leqslant 4d^2$ and the possibilities for $V$ are recorded in Lemma 5.19.

First let us consider the exceptional cases in (19). Suppose $(d, \bar{V}) = (6, L(\lambda_3))$. Here $i = 3$ and $V = \Lambda^3(W)$ is 20-dimensional, where $W$ is the natural $S$-module. A straightforward calculation shows that $\nu(y) \geqslant 8$ for all $y \in S$ of order $r$ (see [6, Section 7], for example), so every element $x \in T$ of order $r$ with $\nu(x) = 6$ is a derangement. A very similar argument applies if $(d, \bar{V}) = (8, L(\lambda_4))$ or $(10, L(\lambda_5))$. Finally, suppose $(d, \bar{V}) = (6, L(2\lambda_3))$, so $p = 3$ and $n = 141$ (see [31, Table A.9]). Again, $i = 3$ and thus 6 divides $r - 1$. Set $a = (r-1)/6$ and observe that $S$ has $4a + \binom{2a}{2}$ conjugacy classes of elements of order $r$. If $r = 7$ then $T$ has $\lfloor 141/6 \rfloor = 23 > 5$ such classes, so we may assume that $r \geqslant 13$. It is easy to check that $T$ has at least $2a + 22\binom{a}{2}$ such classes, and the result follows by applying Corollary 2.2. (To obtain the latter lower bound, we simply count class representatives of the form $[X_1, I_{135}]$, $[X_1^2, I_{129}]$ and $[X_1^j, X_2, I_{141-6(j+1)}]$ with $1 \leqslant j \leqslant 22$.)

Now assume $V$ is the adjoint module, so $n = d^2 - 1$ or $d^2 - 2$ (according to whether or not $p$ divides $d$). Let $X$ be the Lie algebra of $\bar{S} = \mathrm{SL}_d(K)$, so $\bar{V}$ is the nontrivial irreducible constituent of $X$. Now $\dim C_X(y) = \dim C_{\bar{S}}(y)$ for every nontrivial semisimple element $y \in \bar{S}$ (see [21, Section 1.10]) and thus [6, Proposition 2.9] implies that

$$\dim C_X(y) = \dim C_{\bar{S}}(y) \leqslant d^2 - 2d + 1.$$

It follows that the dimension of the 1-eigenspace of any element in $S$ of order $r$ on $V$ is at most $d^2 - 2d + 1$. But if $x \in T$ is an element of order $r$ with $\nu(x) = c$, then

$$\dim C_V(x) = n - c \geqslant d^2 - d - 2 > d^2 - 2d + 1$$

and we conclude that $x$ is a derangement.

*Case 4. $S = E_8(q)$*

As before, $H_0$ does not contain any field automorphisms, so by considering the order of $S$ we deduce that $c \leqslant 30$ and thus $n \leqslant 3600$ since we have $c \geqslant \sqrt{n}/2$. By inspecting [31, Table A.53], we deduce that $n = 248$ is the only possibility, so $V$ is the adjoint module. In particular, since $\bar{V}$ is the Lie algebra of $\bar{S} = E_8(K)$ we have

$$\dim C_{\bar{V}}(y) = \dim C_{\bar{S}}(y) \leqslant 136$$

for all nontrivial semisimple elements $y \in \bar{S}$. Therefore, every $x \in T$ of order $r$ with $\nu(x) = c$ is a derangement.

*Case 5. $S = E_7(q)$*

Here $c \leqslant 18$ and thus $n \leqslant 1296$. Suppose $c \in \{14, 18\}$. By inspecting the structure of the maximal tori in $S$ (see [24, Section 2.9], for example), we deduce that every element in $S$ of order $r$ belongs to a unique conjugacy class of maximal tori, which are cyclic. Since such a torus has a unique subgroup of order $r$, it follows that $\kappa(S, r) = 1$ and thus $T$ contains derangements of order $r$.

By inspecting the order of $S$, we may assume that $c \leqslant 12$ and thus $n \leqslant 576$. By [31, Table A.52], it follows that $n \in \{56, 132, 133\}$, so $V$ is either the minimal or adjoint module

for $S$. Suppose $V$ is the adjoint module and let $X$ be the Lie algebra of $\bar{S} = E_7(K)$. Then

$$\dim C_X(y) = \dim C_{\bar{S}}(y) \leqslant 79$$

for all nontrivial semisimple elements $y \in \bar{S}$, so every $x \in T$ of order $r$ with $\nu(x) = c$ is a derangement. Finally, suppose $n = 56$ and consider the restriction of $\bar{V}$ to a maximal rank subgroup $A_7$ of $\bar{S}$. By [29, Proposition 2.3] we have

$$\bar{V} \downarrow A_7 = L(\lambda_2) \oplus L(\lambda_2)^* = \Lambda^2(W) \oplus \Lambda^2(W)^*,$$

where $W$ is the natural $A_7$-module. By calculating directly with the exterior square $\Lambda^2(W)$ we find that $\dim C_{L(\lambda_2)}(y) \leqslant 21$ for all nontrivial semisimple elements $y \in A_7$, so the 1-eigenspace of any element in $S$ of order $r$ on $V$ has dimension at most 42. Since $c \leqslant 12$, we conclude that each $x \in T$ of order $r$ with $\nu(x) = c$ is a derangement.

*Case 6.* $S = E_6(q)$

This is very similar to the previous case. First observe that $c \leqslant 12$ and thus $n \leqslant 576$. If $c \in \{9, 12\}$ then by considering the maximal tori of $S$ we deduce that $\kappa(S, r) = 1$ and the result follows. In view of $|S|$, we may assume that $c \leqslant 8$, so $n \leqslant 256$ and thus $n \in \{27, 77, 78\}$ by [31, Table A.51]. If $n \in \{77, 78\}$ then $V$ is the adjoint module and we see that every $x \in T$ of order $r$ with $\nu(x) = c$ is a derangement since $\dim C_X(y) = \dim C_{\bar{S}}(y) \leqslant 46$ for all nontrivial semisimple elements $y \in \bar{S}$ (where $X$ is the Lie algebra of $\bar{S} = E_6(K)$).

Finally, let us assume $c \leqslant 8$ and $n = 27$, so $V$ is the minimal module for $S$. Once again we claim that every element $x \in T$ of order $r$ with $\nu(x) = c$ is a derangement. To see this, first observe that

$$\bar{V} \downarrow A_1 A_5 = (L(\lambda_1) \otimes L(\lambda_1)) \oplus (0 \otimes L(\lambda_4)) = U_1 \oplus U_2,$$

where 0 denotes the trivial $A_1$-module (see [29, Proposition 2.3]). Let $y = y_1 y_2 \in A_1 A_5$ be a nontrivial semisimple element. If one $y_j$ is trivial then it is clear that $y$ has a repeated nontrivial eigenvalue on $\bar{V}$. On the other hand, if both $y_1$ and $y_2$ are nontrivial then we calculate that $\dim C_{U_1}(y) \leqslant 6$ and $\dim C_{U_2}(y) \leqslant 10$ (note that $U_2 \cong \Lambda^2(W)^*$, where $W$ is the natural $A_5$-module), so $\dim C_{\bar{V}}(y) \leqslant 16$. This justifies the claim.

*Case 7.* $S = F_4(q)$

Here $c \leqslant 12$ and thus $n \leqslant 576$. If $c \in \{8, 12\}$ then by considering the structure of the maximal tori of $S$ we see that $\kappa(S, r) = 1$, so we may assume that $c \leqslant 6$. In particular, $n \leqslant 144$ and thus $n \in \{25, 26, 52\}$ (see [31, Table A.50]). We claim that each $x \in T$ of order $r$ with $\nu(x) = c$ is a derangement.

If $n = 52$ then $\bar{V}$ is the Lie algebra of $\bar{S} = F_4(K)$, so $\dim C_{\bar{V}}(y) \leqslant 36$ and the claim follows. Finally, if $n \in \{25, 26\}$ then the proof of [6, Lemma 7.4] implies that $\nu(y) \geqslant 7$ for all nontrivial semisimple elements $y \in \bar{S}$, and once again the claim holds.

*Case 8.* $S = G_2(q)$

Since $c \geqslant 3$ and $|S| = q^6(q^2 - 1)(q^6 - 1)$, we see that $c = 6$ is the only possibility. By inspecting the maximal tori of $S$, we deduce that $\kappa(S, r) = 1$ and the result follows. $\quad\square$

5.4.2. *$S$ is twisted.* To complete the proof of Proposition 5.2 (and hence the proof of Theorem 1), we may assume that $S$ is a twisted group of Lie type over $\mathbb{F}_{p^e}$.

For now, let us assume that $S$ is of type $\mathrm{PSU}_d(p^e)$ (with $d \geqslant 3$), $\mathrm{P\Omega}_d^-(p^e)$ (with $d \geqslant 8$) or $^2E_6(p^e)$. In each of these cases, the ambient simple algebraic group admits a graph automorphism $\tau$ of order 2, which induces a symmetry of the corresponding Dynkin diagram.

We will also write $\tau$ to denote the restriction of this automorphism to the corresponding twisted group $\hat{S}$. Recall that if $M$ is a $K\hat{S}$-module affording the representation $\rho$, then $M^\tau$ denotes the space $M$ with $\hat{S}$ acting via $\tau\rho$.

As before, set $q = p^f$ and $q' = p^{f'}$, where $f' = 2f$ if $T = \mathrm{PSU}_n(q)$, otherwise $f' = f$. Since $V$ is an absolutely irreducible $\mathbb{F}_{q'}\hat{S}$-module which cannot be realised over a proper subfield of $\mathbb{F}_{q'}$, [25, Proposition 5.4.6(ii)] implies that one of the following occurs:

(a) $f'$ divides $e$ and there is an irreducible $K\hat{S}$-module $M$ such that $M^\tau \cong M$ and (18) holds.

(b) $f'$ divides $2e$, but $f'$ does not divide $e$. Moreover, if we write $\bar{V} = V \otimes K$ then there is an irreducible $K\hat{S}$-module $M$ such that $M^\tau \not\cong M$ and

$$\bar{V} \cong M \otimes (M^\tau)^{(f'/2)} \otimes M^{(f')} \otimes (M^\tau)^{(3f'/2)} \otimes \cdots \otimes (M^\tau)^{(e-f')} \otimes M^{(e-f'/2)} \qquad (22)$$

(with $2e/f'$ factors) as $K\hat{S}$-modules.

Set $\ell = \dim M$ and note that $\ell \geqslant 3$. Also note that $n = \ell^{e/f'}$ in (a), and $n = \ell^{2e/f'}$ in (b).

**Lemma 5.22.** *Proposition 5.2 holds if $S$ is of type $\mathrm{PSU}_d(p^e)$, $\mathrm{P\Omega}_d^-(p^e)$ or $^2E_6(p^e)$.*

*Proof.* First let us assume that we are in case (a) above, so $f'$ divides $e$ and (18) holds with respect to an irreducible $K\hat{S}$-module $M$ such that $M^\tau \cong M$. If $f' < e$ then the proof of Lemma 5.20 goes through unchanged (note that we always have $\ell > 2$) and we deduce that every element $x \in T$ of order $r$ with $\nu(x) = c$ is a derangement.

Now assume that (a) holds and $f' = e$. Here $\bar{V} \cong M \cong M^\tau$, so $V$ is self-dual (see [25, Proposition 5.4.3]). In particular, $T$ is either symplectic or orthogonal, and $q = q'$. Also note that every element in $H_0$ of order $r$ is inner-diagonal. Set $i = \Phi(r, q)$ as before and note that $c = 2i$ if $i$ is odd, otherwise $c = i$. Define the integer $c'$ as in (21). As noted in the proof of Lemma 5.21, we may assume that $c' \leqslant d/2$. In addition, Lemma 2.8 implies that if $c' \geqslant c$ then it suffices to show that $n > 2d$.

Suppose $S = \mathrm{PSU}_d(q)$ with $d \geqslant 3$. First assume that $i \not\equiv 2 \pmod 4$, so $3 \leqslant c = c' \leqslant d/2$ and [31] implies that $n \geqslant d(d-1)/2 > 2d$ as required. Now assume $i \equiv 2 \pmod 4$, so $c = i$ and $c' = i/2$. Since $c \geqslant 3$ and $c' \leqslant d/2$ we have $i, d \geqslant 6$. In addition, since $c \geqslant \sqrt{n}/2$ we deduce that $n \leqslant 4d^2$. The rest of the argument is now identical to the analysis in Case 3 in the proof of Lemma 5.21. The reader can check the details.

Next assume $S = \mathrm{P\Omega}_d^-(q)$ and $d \geqslant 8$. Here $c' = c$ and we can repeat the argument in Case 2 in the proof of Lemma 5.21. Finally, let us assume that $S = {}^2E_6(q)$. By inspecting the order of $S$ we see that $c \leqslant 18$. If $c > 8$ then by considering the structure of the maximal tori of $S$ we deduce that $\kappa(S, r) = 1$ and the result follows. Now assume $c \leqslant 8$ so $n \leqslant 256$. By inspecting [31, Table A.51] we see that $n \in \{27, 77, 78\}$ and we can now repeat the argument presented in Case 6 in the proof of Lemma 5.21.

To complete the proof of the lemma we may assume that (b) holds so $f'$ divides $2e$, but $f'$ does not divide $e$, and there is an irreducible $K\hat{S}$-module $M$ such that $M^\tau \not\cong M$ and (22) holds. Note that $n = \ell^{2e/f'}$, where $\ell = \dim M$. If $f' < 2e$ then the argument in the proof of Lemma 5.20 goes through, so we may assume that $f' = 2e$ and thus $\bar{V} \cong M$. Also note that $V^{(e)} \cong V^\tau$ (see [25, Proposition 5.4.6(ii)]).

First assume $S = \mathrm{PSU}_d(p^e)$ and $d \geqslant 3$. Here $V^{(e)} \cong V^\tau \cong V^*$ and thus $(V^*)^{(e)} \cong V$, so $T = \mathrm{PSU}_n(q)$, $f' = 2f$ and $S = \mathrm{PSU}_d(q)$. In particular, $c' = c$, $d \geqslant 6$ and $n \geqslant d(d-1)/2 > 2d$, so the result follows from Lemma 2.8.

Next assume $S = \mathrm{P\Omega}_d^-(p^e)$ with $d \geqslant 8$. Suppose $d \equiv 0 \pmod 4$. Then $V$ is self-dual (see [25, Proposition 5.4.3]), so $T$ is a symplectic or orthogonal group and thus $S = \mathrm{P\Omega}_d^-(q_0)$ with $q = q_0^2$. Note that $n > d$ (if $n = d$ then $V$ is the natural module for $\hat{S}$, which is

defined over a proper subfield of $\mathbb{F}_q$). Set $i = \Phi(r, q)$ and $i_0 = \Phi(r, q_0)$, so $i = i_0/2$ if $i_0$ is even, otherwise $i = i_0$. Also set $c' = 2i_0$ if $i_0$ is odd, otherwise $c' = i_0$. Then $c' = 2i \geqslant c$ and by arguing as in Case 2 in the proof of Lemma 5.21 we deduce that $n > 2d$.

Now suppose $S = \mathrm{P\Omega}_d^-(p^e)$, where $d \geqslant 10$ and $d \equiv 2 \,(\mathrm{mod}\ 4)$. In this situation, $V$ is not self-dual. In fact, $(V^*)^{(e)} \cong V$ and thus $T = \mathrm{PSU}_n(q)$ and $S = \mathrm{P\Omega}_d^-(q)$. Therefore $c' \geqslant c$ and once again it is easy to check that $n > 2d$.

Finally, let us assume that $S = {}^2E_6(p^e)$. As in the previous case, we have $T = \mathrm{PSU}_n(q)$ and $S = {}^2E_6(q)$. Note that every element of order $r$ in $H_0$ is contained in $S$. If $c > 8$ then $c \in \{9, 12\}$, $i \in \{12, 18\}$ and thus $\kappa(S, r) = 1$. On the other hand, if $c \leqslant 8$ then $n \leqslant 256$ and we can proceed as in Case 6 in the proof of Lemma 5.21.                    $\square$

We now complete the proof of Proposition 5.2 by dealing with the remaining twisted groups.

**Lemma 5.23.** *Proposition 5.2 holds if $S$ is of type ${}^3D_4(p^e)$, ${}^2B_2(2^e)$, ${}^2G_2(3^e)$ or ${}^2F_4(2^e)$.*

*Proof.* Set $q = p^f$ and note that $V$ is self-dual (see [25, p.192]), so $T = \mathrm{PSp}_n(q)$ or $\mathrm{P\Omega}_n^\epsilon(q)$. As usual, we set $H_0 = H \cap T$ and $i = \Phi(r, q)$. We partition the proof into several cases.

*Case 1.* $S = {}^3D_4(p^e)$

Set $t = p^e$ and note that $|S| = t^{12}(t^8 + t^4 + 1)(t^6 - 1)(t^2 - 1)$. Since $r \geqslant 5$, every element in $H$ of order $r$ is contained in $S.\langle \varphi \rangle$, where $\varphi$ is a field automorphism of order $r$. There are $r - 1$ distinct $S$-classes of field automorphisms of order $r$ in $\mathrm{Aut}(S)$, represented by the elements $\varphi^j$ with $1 \leqslant j < r$ (this follows from the fact that every element of order $r$ in the coset $S\varphi^j$ is $S$-conjugate to $\varphi^j$ – see [17, Proposition 4.9.1(d)]). Therefore, there is at most one $S$-class of subgroups of order $r$ with elements in $H_0 \setminus S$, so we may assume that $r$ divides $|S|$. As noted in [25, Remark 5.4.7(a)], either $f$ divides $e$, or $f$ divides $3e$ (and $f$ does not divide $e$).

First assume $f$ divides $e$, so $t = q^{e/f}$. According to [25, Remark 5.4.7(a)], there exists an irreducible $K\hat{S}$-module $M$ such that $M^\tau \cong M$ and
$$\bar{V} = V \otimes K \cong M \otimes M^{(f)} \otimes M^{(2f)} \otimes \cdots \otimes M^{(e-f)},$$
where $\tau$ denotes a triality graph automorphism of $\hat{S}$ of order 3. Note that the condition $M^\tau \cong M$ implies that $\dim M \geqslant 26$ (see [31, Table A.41], for example), so $n \geqslant 26^{e/f}$.

Suppose $r$ divides $t^8 + t^4 + 1$. Since $r$ divides $q^{12e/f} - 1$ it follows that $i$ divides $12e/f$. Therefore,
$$12e/f \geqslant c \geqslant \lceil \sqrt{n}/2 \rceil \geqslant \lceil \sqrt{26^{e/f}}/2 \rceil$$
and thus $e/f \leqslant 2$. In particular, $e/f$ is indivisible by $r$, so $H_0$ does not contain any field automorphisms of order $r$. By inspecting the structure of the maximal tori of $S$ (see [24, Section 2.4]) we deduce that $\kappa(S, r) = 1$ and the result follows.

Next assume $r$ divides $t^6 - 1$. Here $c \leqslant 6e/f$ and by arguing as above we deduce that $e/f \leqslant 2$. If $e/f = 2$ then $12 \geqslant c \geqslant \lceil 26/2 \rceil = 13$, which is absurd, so we may assume that $e/f = 1$, hence $i \in \{3, 6\}$ and $c = 6$. Moreover, the bound $6 \geqslant \lceil \sqrt{n}/2 \rceil$ implies that $n \leqslant 144$. By inspecting [31, Table A.41], using the fact that the highest weight of $M$ is fixed under the induced action of $\tau$ on weights, it follows that $n = 28 - 2\delta_{2,p}$ and $V$ is the adjoint module. Let $X$ be the Lie algebra of $\bar{S} = D_4$ and observe that
$$\dim C_X(y) = \dim C_{\bar{S}}(y) \leqslant 16$$
for all nontrivial semisimple elements $y \in \bar{S}$ (indeed, the proof of [6, Proposition 2.9] implies that $\dim y^{\bar{S}} \geqslant 12$). We immediately deduce that every element $x \in T$ of order $r$ with $\nu(x) = c$ is a derangement.

To complete the analysis of the case $S = {}^3D_4(p^e)$ we may assume that $f$ divides $3e$, but $f$ does not divide $e$. Here there is an irreducible $K\hat{S}$-module $M$ such that $M^\tau \not\cong M$ and

$$V \otimes K \cong M \otimes (M^\tau)^{(f/3)} \otimes (M^{\tau^2})^{(2f/3)} \otimes M^{(f)} \otimes \cdots$$

(with $3e/f$ factors in total). Note that $\dim M \geqslant 8$.

Suppose $r$ divides $t^8 + t^4 + 1$, in which case $r$ divides $q^{12e/f} - 1$ and thus

$$12e/f \geqslant c \geqslant \lceil \sqrt{n}/2 \rceil \geqslant \lceil \sqrt{8^{3e/f}}/2 \rceil$$

since $n \geqslant 8$. This implies that $3e/f = 1$ or $2$. In particular, $r$ does not divide $3e/f$, so $\kappa(H_0, r) = 1$ and the result follows. Finally, let us assume that $r$ divides $t^6 - 1$, so $c \leqslant 6e/f$ and we deduce that $3e/f \leqslant 2$ since $n \geqslant 8$. If $3e/f = 1$ then $c = 2$, which is a contradiction. If $3e/f = 2$ then $c = 4$ and $n = 8$ is the only possibility, but this can be ruled out by inspecting the relevant tables in [4, Section 8.2].

*Case 2.* $S = {}^2B_2(2^e)$

Set $t = 2^e$, where $e \geqslant 3$ is odd, and note that $|S| = t^2(t^2+1)(t-1)$ and $\mathrm{Aut}(S) = S.\langle \phi \rangle$, where $\phi$ is a field automorphism of order $e$. Now $S$ has exactly three conjugacy classes of maximal tori, all of which are cyclic. By considering the orders of the maximal tori, we deduce that $\kappa(S, r) = 1$ for every odd prime divisor $r$ of $|S|$. As in the previous case, there is at most one $S$-class of subgroups of order $r$ with elements in $H_0 \setminus S$, whence $\kappa(H_0, r) \leqslant 2$. The desired result follows immediately if $\kappa(H_0, r) = 1$, so we may assume that $r$ divides $|S|$.

Write $q = 2^f$ and note that $f$ divides $e$ and $n = \dim V \geqslant 4^{e/f}$ (see [25, Remark 5.4.7(b)]). Since $r$ divides $|S|$, it divides either $t - 1$ or $t^2 + 1$. Suppose $r$ divides $t - 1 = q^{e/f} - 1$, so $i$ divides $e/f$ and thus $i$ is odd, so

$$2e/f \geqslant 2i = c \geqslant \lceil \sqrt{n}/2 \rceil \geqslant 2^{e/f-1}$$

and it follows that $e/f = 1$ or $3$. But we are assuming that $c \geqslant 3$, so $e/f = 3$ and thus $i = 3$ and $c = 6$. Since $n \geqslant 4^{e/f} = 64$, we deduce that $\kappa(T, r) \geqslant 3$ and thus $T$ contains derangements of order $r$. A similar argument applies when $r$ divides $t^2 + 1$. Here $r$ divides $q^{2e/f} + 1$ and thus $i$ divides $4e/f$. If $i$ is odd then $i$ divides $e/f$, so $r$ divides $q^{e/f} - 1$, which is not possible. Therefore, $i$ is even and thus

$$4e/f \geqslant i = c \geqslant \lceil \sqrt{n}/2 \rceil \geqslant 2^{e/f-1},$$

so $e/f \in \{1, 3, 5\}$. If $e/f = 3$ or $5$ then the bound $n \geqslant 4^{e/f}$ quickly implies that $\kappa(T, r) \geqslant 3$. Finally, if $e/f = 1$ then $c = 4$ and $n \geqslant 16$ (indeed, every absolutely irreducible representation of $S$ over a field of characteristic 2 has dimension $4^m$ for some $m$; see [32, Lemma 1], for example) and once again we conclude that $\kappa(T, r) \geqslant 3$.

*Case 3.* $S = {}^2G_2(3^e)$

Write $t = 3^e$, where $e \geqslant 3$ is odd, and note that $|S| = t^3(t^3+1)(t-1)$. By inspecting the structure of the maximal tori of $S$, we deduce that $\kappa(S, r) = 1$ for every prime $r \geqslant 5$ dividing $|S|$. As in the previous case, we may assume that $r$ divides $|S|$ and it suffices to show that $\kappa(T, r) \geqslant 3$. By [25, Remark 5.4.7(b)], $f$ divides $e$ and $n \geqslant 7^{e/f}$.

First assume $r$ divides $t - 1$, so $i$ divides $e/f$ and thus $c = 2i \leqslant 2e/f$ and $e/f \geqslant 3$. Since

$$2e/f \geqslant c \geqslant \lceil \sqrt{n}/2 \rceil \geqslant \lceil \sqrt{7^{e/f}}/2 \rceil$$

we deduce that $e/f = 3$ is the only possibility, so $c = 6$, $n \geqslant 7^3$ and we clearly have $\kappa(T, r) \geqslant 3$. Now assume $r$ divides $t^3 + 1$, so $i$ divides $6e/f$. If $i$ is odd then $r$ divides $q^{3e/f} - 1$ and $q^{3e/f} + 1$, which is absurd, so $i = c$ is even. If $c \leqslant 2e/f$ then the previous

argument shows that $e/f = 3$, so $n \geqslant 7^3$ and the result follows as above. Finally, suppose that $c = 6e/f$. By the usual argument we deduce that $e/f \leqslant 3$. If $e/f = 3$ then $c = 18$, $n \geqslant 7^3$ and we see that $\kappa(T, r) \geqslant 3$. Now assume $e/f = 1$, so $c = 6$ and $n \geqslant 12$ (since $c \leqslant n/2$). By inspecting [31, Table A.49], noting that $p = 3$, we deduce that $n \geqslant 27$ and the desired result follows.

*Case 4.* $S = {}^2F_4(2^e)$

Set $t = 2^e$ and note that $|S| = t^{12}(t^6 + 1)(t^4 - 1)(t^3 + 1)(t - 1)$, where $e \geqslant 1$ is odd. As noted in [25, Remark 5.4.7(b)], $f$ divides $e$ and $n \geqslant 26^{e/f}$, where $q = 2^f$. As in the previous cases, there is at most one $S$-class of subgroups of order $r$ containing elements in $H_0 \setminus S$, so we may assume that $r$ divides $|S|$. Set $j = \Phi(r, t)$ and note that $j \in \{1, 2, 4, 6, 12\}$.

First assume that $j = 12$, so $r$ divides $t^4 - t^2 + 1$. By considering the structure of the maximal tori of $S$ we deduce that $\kappa(S, r) = 1$ so it suffices to show that $\kappa(T, r) \geqslant 3$. Since $c \leqslant 12e/f$ and $n \geqslant 26^{e/f}$, it follows that $12e/f \geqslant \lceil \sqrt{26^{e/f}}/2 \rceil$, so $e/f = 1$, $c = 12$ and $n \leqslant 576$. By inspecting [31, Table A.50], noting that $p = 2$, we deduce that $n = 26$ is the only possibility and thus $V$ is the minimal module for $S$. Since $V \not\cong V^{(z)}$ for any positive integer $z < f$, it follows that $H_0$ does not contain any field automorphisms, so $\kappa(H_0, r) = 1$ and the result follows.

Next assume $j = 6$, so $r$ divides $t^3 + 1$. Once again, we see that $\kappa(S, r) = 1$. Since $c \leqslant 6e/f$ and $n \geqslant 26^{e/f}$ we deduce that $e/f = 1$ is the only possibility, so $c = 6$, $n \geqslant 26$ and $\kappa(T, r) \geqslant 3$ as required. If $j \leqslant 2$ then $c \leqslant 2e/f < \lceil \sqrt{26^{e/f}}/2 \rceil$, so this case does not arise.

Finally, let us assume $j = 4$. Here $4e/f \geqslant c \geqslant \lceil \sqrt{26^{e/f}}/2 \rceil$ and thus $e/f = 1$, so $c = 4$ and $n \leqslant 64$. From [31, Table A.50], we deduce that $n = 26$ and thus $V$ is the minimal module for $S$. Set $\bar{S} = F_4(K)$ and $\bar{V} = L(\lambda_1)$ (or $L(\lambda_4)$), so $\bar{V}$ is a minimal module. From the proof of [6, Lemma 7.4], we see that $\nu(y) \geqslant 8$ for all nontrivial semisimple elements $y \in \bar{S}$ (with respect to the action of $\bar{S}$ on $\bar{V}$). We conclude that every element $x \in T$ of order $r$ with $\nu(x) = 4$ is a derangement. $\qquad\square$

This completes the proof of Proposition 5.2. By combining this result with Corollary 2.7 and Propositions 3.4, 4.1 and 5.1, we conclude that the proof of Theorem 1 is complete.

## 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] N. Bourbaki, *Lie Groups and Lie Algebras (Chapters 4-6)*, Springer, 2002.

[4] J.N. Bray, D.F. Holt and C.M. Roney-Dougal, *The Maximal Subgroups of the Low-dimensional Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 407, Cambridge University Press, 2013.

[5] T.C. Burness, *Fixed point spaces in primitive actions of simple algebraic groups*, J. Algebra **265** (2003), 744–771.

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

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

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

[9] T.C. Burness and M. Giudici, *Classical groups, derangements and primes*, Aust. Math. Soc. Lecture Series, vol. 25, Cambridge University Press, 2016.

[10] T.C. Burness, M. Giudici and R.A. Wilson, *Prime order derangements in primitive permutation groups*, J. Algebra **341** (2011), 158–178.

[11] P.J. Cameron, M. Giudici, G.A Jones, W.M. Kantor, M.H. Klin, D. Marušič, L.A. Nowitz, *Transitive permutation groups without semiregular subgroups*, J. London Math. Soc. **66** (2002), 325–333.

[12] B. Fein, W.M. Kantor and M. Schacher, *Relative Brauer groups II*, J. Reine Angew. Math. **328** (1981), 39–57.

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

[14] M. Giudici, *Quasiprimitive groups with no fixed point free elements of prime order*, J. London Math. Soc. **67** (2003), 73–84.

[15] M. Giudici and S. Kelly, *Characterizing a family of elusive permutation groups*, J. Group Theory **12** (2009), 95–105.

[16] M. Giudici, L. Morgan, P. Potočnik and G. Verret, *Elusive groups of automorphisms of digraphs of small valency*, European J. Combin. **46** (2015), 1–9.

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

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

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

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

[21] J.E. Humphreys, *Conjugacy Classes in Semisimple Algebraic Groups*, Amer. Math. Soc. Monographs and Surveys series, vol. 43, 1995.

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

[23] C. Jansen, *The minimal degrees of faithful representations of the sporadic simple groups and their covering groups*, LMS J. Comput. Math. **8** (2005), 122–144.

[24] W.M. Kantor and Á. Seress, *Prime power graphs for groups of Lie type*, J. Algebra **247** (2002), 370–434.

[25] 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.

[26] A.S. Kleshchev and P.H. Tiep, *Small-dimensional projective representations of symmetric and alternating groups*, Algebra Number Theory **6** (2012), 1773–1816.

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

[28] M.W. Liebeck and G.M. Seitz, *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, Math. Surveys Monogr., vol. 180, Amer. Math. Soc., 2012.

[29] M.W. Liebeck and G.M. Seitz, *Reductive subgroups of exceptional algebraic groups*, Mem. Amer. Math. Soc. **121** (1996), no. 580.

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

[31] F. Lübeck, *Small degree representations of finite Chevalley groups in defining characteristic*, LMS J. Comput. Math. **4** (2001), 135–169.

[32] R.P. Martineau, *On 2-modular representations of the Suzuki groups*, Amer. J. Math. **94** (1972), 55–72.

[33] C.E. Praeger, Á, Seress, and Ş. Yalçinkaya, *Generation of finite classical groups by pairs of elements with large fixed point spaces*, J. Algebra **421** (2015), 56–101.

[34] J.-P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. **40** (2003), 429–440.

[35] R. Steinberg, *Endomorphisms of linear algebraic groups*, Mem. Amer. Math. Soc. (1968), no. 80.

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

[37] J. Xu, *On elusive permutation groups of square-free degree*, Comm. Algebra **37** (2009), 3200–3206.

T.C. Burness, School of Mathematics, University of Bristol, Bristol BS8 1TW, UK

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

M. Giudici, The Centre for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics, The University of Western Australia, Crawley WA 6009, Australia

*E-mail address*: `michael.giudici@uwa.edu.au`