arXiv:1403.7666v1 [math.GR] 29 Mar 2014

DERANGEMENTS IN PRIMITIVE PERMUTATION GROUPS, WITH AN APPLICATION TO CHARACTER THEORY

TIMOTHY C. BURNESS AND HUNG P. TONG-VIET†

Abstract. Let G be a finite primitive permutation group and let $\kappa(G)$ be the number of conjugacy classes of derangements in G. By a classical theorem of Jordan, $\kappa(G) \geqslant 1$. In this paper we classify the groups G with $\kappa(G) = 1$, and we use this to obtain new results on the structure of finite groups with an irreducible complex character that vanishes on a unique conjugacy class. We also obtain detailed structural information on the groups with $\kappa(G) = 2$, including a complete classification for almost simple groups.

1. Introduction

Let G be a transitive permutation group on a finite set Ω of size $n \geqslant 2$, and let H be the stabiliser of a point. An element $x \in G$ is a *derangement* if it acts fixed-point-freely on Ω, or equivalently, if $x^G \cap H$ is empty, where x^G is the conjugacy class of x in G. The existence of derangements is guaranteed by a classical theorem of Jordan [37], and we will write

$$\Delta(G) = G \setminus \bigcup_{g \in G} H^g$$

for the set of derangements in G. As discussed by Serre [46], Jordan's theorem has many interesting applications in number theory and topology.

Various extensions and generalisations of Jordan's theorem have been studied in recent years. For example, let $\delta(G) = |\Delta(G)|/|G|$ be the proportion of derangements in G. By a theorem of Cameron and Cohen [10], $\delta(G) \geqslant 1/n$ and equality holds if and only if G is sharply 2-transitive (that is, either $(G, n) = (S_2, 2)$ or G is a Frobenius group of order $n(n-1)$ with n a prime power). Using the Classification of Finite Simple Groups (CFSG), Guralnick and Wan [30] have established the better bound $\delta(G) \geqslant 2/n$ (with prescribed exceptions), and a very recent theorem of Fulman and Guralnick (see [22, 23, 24, 25]) states that there is an absolute constant $\epsilon > 0$ such that $\delta(G) > \epsilon$ for any simple transitive group G. This latter result confirms a conjecture of Boston et al. [4] and Shalev.

In a different direction, one can consider the existence of derangements of a given order. By a theorem of Fein, Kantor and Schacher [17], G contains a derangement of prime-power order (their proof requires CFSG), and this result has important number-theoretic applications. However, G may not contain a derangement of prime order, and in this situation we say that G is *elusive*. The first construction of elusive groups was presented in [17]: let p be a Mersenne prime and take $G = \mathrm{AGL}_1(p^2)$ and $H = \mathrm{AGL}_1(p)$, so $n = p(p+1)$ and G is elusive since all elements of order 2 or p are conjugate in G. In [27], Giudici classifies the quasiprimitive elusive groups, and it follows that the 3-transitive action of the smallest Mathieu group M_{11} on 12 points is the only almost simple primitive elusive group. In [34], the transitive groups G in which all derangements are involutions are determined; G is either an elementary abelian 2-group, or a Frobenius group with kernel an elementary abelian 2-group.

Date: April 2, 2014.

2010 *Mathematics Subject Classification.* Primary 20B15; secondary 20C15.

† Supported by the project C13 'The geometry and combinatorics of groups' within the CRC 701.

$\kappa(G)$	(G,H)
1	(A_5, D_{10}), $(\mathrm{L}_2(8){:}3, D_{18}{:}3)$
2	(A_5, D_6), (A_5, A_4), (S_5, D_{12}), (S_5, S_4), $(A_6, 3^2{:}4)$, (A_6, A_5), $(S_6, 3^2{:}D_8)$
	$(\mathrm{M}_{10}, [16])$, $(\mathrm{L}_2(7), 7{:}3)$, $(\mathrm{L}_2(7), S_4)$, $(\mathrm{L}_3(4), 2^4{:}A_5)$, $({}^2B_2(8){:}3, 5{:}4 \times 3)$

TABLE 1. $\kappa(G) < 3$, G almost simple primitive

In this paper, we are interested in the number of conjugacy classes of derangements in G, which we denote by $\kappa(G)$ (note that $\Delta(G)$ is a normal subset of G). By Jordan's theorem, $\kappa(G) \geqslant 1$. Our first result determines the primitive groups with $\kappa(G) = 1$, and our second gives a stronger result for almost simple groups.

Theorem 1. *Let G be a finite primitive permutation group with point stabiliser H. Then $\kappa(G) = 1$ if and only if G is sharply 2-transitive, or $(G,H) = (A_5, D_{10})$ or $(\mathrm{L}_2(8){:}3, D_{18}{:}3)$.*

Theorem 2. *Let G be a finite almost simple primitive permutation group with point stabiliser H. Then either $\kappa(G) \geqslant 3$, or $(\kappa(G), G, H)$ is recorded in Table 1. Moreover, $\kappa(G)$ tends to infinity as $|G|$ tends to infinity.*

Note that in Table 1, we write $G = A_5$ rather than $\mathrm{L}_2(4)$ or $\mathrm{L}_2(5)$. Similarly, we write $G = A_6$ rather than $\mathrm{L}_2(9)$ or $\mathrm{PSp}_4(2)'$, etc. In addition, in the final row we write [16] to denote a Sylow 2-subgroup of $\mathrm{M}_{10} = A_6 \cdot 2$.

By considering the cases in Table 1, we easily deduce the following corollary.

Corollary 3. *Let G be a finite almost simple transitive permutation group with point stabiliser H. Assume G is imprimitive. Then either $\kappa(G) \geqslant 3$, or $\kappa(G) = 2$ and $(G,H) = (A_5, \mathbb{Z}_5)$.*

We also investigate the structure of a general primitive permutation group G with $\kappa(G) = 2$. A version of our main result is Theorem 4 below (see Section 4 for more details). Hering's classification [31, 32] of the 2-transitive affine permutation groups is a key tool in the proof.

Theorem 4. *Let G be a finite primitive permutation group of degree n with point stabiliser H. If $\kappa(G) = 2$, then one of the following holds:*

- (i) *$(G, n) = (\mathbb{Z}_3, 3)$;*
- (ii) *G is one of the almost simple groups recorded in Table 1;*
- (iii) *$G = HN$ is an affine group, where N is an elementary abelian p-group of order $n = p^k$, and one of the following holds:*
  - (a) *G is a Frobenius group with kernel N, p is odd and $|H| = (n-1)/2$;*
  - (b) *G is a non-Frobenius 2-transitive group, and either G is recorded in Table 2, or G is soluble, $H \leqslant \Gamma\mathrm{L}_1(p^k)$, k is even and $|H| = 2(n-1)$.*

Moreover, any group G as in (i), (ii), (iii)(a) *or Table 2 has the property $\kappa(G) = 2$.*

Remark 5. Let us make a couple of remarks on the statement of Theorem 4.

- (a) In Table 2 we use the notation $\mathcal{P}(n,i)$ to denote the i-th primitive permutation group of degree n in the library of primitive groups stored in MAGMA [3], which can be accessed via the command PrimitiveGroup(n,i).
- (b) Consider part (iii)(b) of Theorem 4, where $H \leqslant \Gamma\mathrm{L}_1(p^k)$, k is even and $|H| = 2(p^k - 1)$. Here it is difficult to give a complete description of the possibilities for G with the property $\kappa(G) = 2$, but we can show that $\kappa(G) = 2$ in the special case $H = \mathrm{GL}_1(p^k) \cdot 2$ (see Proposition 4.10).

n	G	
2^2	$2^2{:}S_3 \cong S_4$	$\mathcal{P}(4,2)$
5^2	$5^2{:}(2^{1+2}.6)$	$\mathcal{P}(5^2,17)$
11^2	$11^2{:}(2^{1+2}.[30])$	$\mathcal{P}(11^2,42)$
3^4	$3^4{:}((2\times Q_8){:}2){:}5$	$\mathcal{P}(3^4,70)$
29^2	$29^2{:}(7\times 2.\mathrm{SL}_2(5))$	$\mathcal{P}(29^2,104)$

TABLE 2. Some affine 2-transitive groups G with $\kappa(G)=2$

One of our main motivations stems from an application to the character theory of finite groups. Let G be a finite nonabelian group and let $\chi\in\mathrm{Irr}(G)$ be a nonlinear irreducible complex character of G. A classical theorem of Burnside [33, Theorem 3.15] states that $\chi(x)=0$ for some $x\in G$. In this situation, we say that χ *vanishes* at x, and x is called a *zero* of χ. Since χ is a class function, it vanishes on the conjugacy class x^G, and we write $n(\chi)$ for the number of conjugacy classes of G on which χ vanishes. Therefore, Burnside's theorem states that $n(\chi)\geqslant 1$ for all nonlinear $\chi\in\mathrm{Irr}(G)$. In fact, by a theorem of Malle, Navarro and Olsson [42], χ vanishes on some element of prime power order, and it is interesting to note that their proof uses the aforementioned theorem of Fein, Kantor and Schacher [17] on derangements in transitive permutation groups.

Several authors have investigated the structure of finite groups with a nonlinear irreducible character χ such that $n(\chi)$ is small, and there has been particular interest in the special case $n(\chi)=1$. For example, Zhmud' [51] obtained partial results on the structure of soluble groups with this property. In later work, Chillag [11, Corollary 2.4] proved that if $G\neq G'$ then either G is a Frobenius group with an abelian odd-order kernel of index two, or χ is irreducible upon restriction to G'. In fact, if G is any finite nonabelian group such that $n(\chi)\leqslant 1$ for all $\chi\in\mathrm{Irr}(G)$, then G is a Frobenius group with an abelian odd-order kernel of index two (see [11, Proposition 2.7]; the proof uses CFSG). See [16] and [44] for additional structural results on soluble groups with this extremal property.

Let us consider the general case: G is a finite nonabelian group with a nonlinear irreducible character χ such that $n(\chi)=1$. Recall that $\chi\in\mathrm{Irr}(G)$ is *imprimitive* if it can be induced from a character of a proper subgroup of G, i.e., $\chi=\phi^G$ for some $\phi\in\mathrm{Irr}(H)$ and proper subgroup H of G. Otherwise, χ is *primitive.*

Suppose $\chi\in\mathrm{Irr}(G)$ is a nonlinear imprimitive irreducible character such that $n(\chi)=1$, say $\chi=\phi^G$ where $\phi\in\mathrm{Irr}(H)$ and H is a proper subgroup of G. Set

$$\Delta_H(G):=G\setminus\bigcup_{g\in G}H^g.$$

Clearly, by definition of the induced character ϕ^G, if $x\in\Delta_H(G)$ then $\chi(x)=0$ and thus $\Delta_H(G)=x^G$. Note that the converse does not hold in general; the condition $\Delta_H(G)=x^G$ does not imply that there is a character $\phi\in\mathrm{Irr}(H)$ such that $\phi^G\in\mathrm{Irr}(G)$ and $n(\phi^G)=1$. For example, if $(G,H)=(A_5,D_{10})$ then $\Delta_H(G)=x^G$ by Theorem 1, but no character of H can be irreducibly induced to G since $|G:H|=6$ and $\chi(1)\leqslant 5$ for all $\chi\in\mathrm{Irr}(G)$.

If we assume further that H is core-free and maximal, then G is a primitive permutation group on $\Omega=G/H$ with $\kappa(G)=1$, so in this situation the possibilities for G and H are given by Theorem 1.

In general, the structure of G can be more complicated. In Theorem 6 below we describe the normal structure of finite groups G with the property that $n(\chi)=1$ for some nonlinear imprimitive irreducible character $\chi=\phi^G$, where $\phi\in\mathrm{Irr}(H)$ for some maximal subgroup H of G. In the statement of Theorem 6, recall that a finite group G is a *Camina group* if $|\mathrm{C}_G(x)|=|\mathrm{C}_{G/G'}(G'x)|$ for all $x\in G\setminus G'$.

Theorem 6. *Let H be a maximal subgroup of a finite group G such that $n(\chi) = 1$ for a nonlinear imprimitive irreducible character $\chi = \phi^G$ with $\phi \in \mathrm{Irr}(H)$. Write $\Delta_H(G) = x^G$ and let $N = H_G$ denote the normal core of H. Then one of the following holds:*

(i) *G is a Frobenius group with an abelian odd-order kernel $H = G'$ of index two.*

(ii) *G/N is a 2-transitive Frobenius group with an elementary abelian kernel M/N of order p^n for some prime p and integer $n \geqslant 1$, and a complement H/N of order $p^n - 1$. Moreover, $x^G = M \setminus N$, $|\mathrm{C}_G(x)| = p^n$, $|x^G| = |H|$, $M' = N$ and one of the following holds:*

  (a) *M is a Frobenius group with kernel M' and $p^n = p > 2$.*

  (b) *M is a Frobenius group with kernel $K \trianglelefteqslant G$ such that $G/K \cong \mathrm{SL}_2(3)$ and $M/K \cong Q_8$.*

  (c) *M is a Camina p-group.*

(iii) *$G/N \cong \mathrm{L}_2(8){:}3$, $H/N \cong D_{18}{:}3$, N is a nilpotent $7'$-group and $\mathrm{C}_G(x) = \langle x \rangle \cong \mathbb{Z}_7$.*

(iv) *$G/N \cong A_5$, $H/N \cong D_{10}$, N is a 2-group and $\mathrm{C}_G(x) = \langle x \rangle \cong \mathbb{Z}_3$.*

In particular, if $G = G'$ then either case (ii)(c) *holds with $p^n = 11^2$ and $G/N \cong 11^2{:}\mathrm{SL}_2(5)$, or case* (iv) *holds.*

Remark 7. Let us make some remarks on the statement of Theorem 6.

(a) Firstly, observe that there is no loss in assuming that H is a maximal subgroup of G. Indeed, if $n(\chi) = 1$ and $\chi = \lambda^G$ for some $\lambda \in \mathrm{Irr}(J)$ and proper subgroup $J < G$, then $\chi = (\lambda^H)^G = \phi^G$, whenever $J \leqslant H < G$ with $\phi = \lambda^H \in \mathrm{Irr}(H)$.

(b) For imprimitive characters, Theorem 6 extends several known results in the literature. For example, the conclusion in part (i) coincides with the first part of [11, Corollary 2.4], and parts (i) and (ii)(a,b) are exactly the conclusions (1)-(3) in [44, Theorem 1.1] (see also [16, Theorem 9]). It is worth noting that the relevant results in [16, 44] only apply in the case G is soluble, whereas Theorem 6 holds for any finite group G.

(c) In Section 5 we prove Theorem 6 under a weaker assumption, namely, we only require that G is a finite subgroup with a maximal subgroup H such that $\Delta_H(G) = x^G$ for some $x \in G$.

(d) In parts (iii) and (iv), we note that the core $N = H_G$ is nontrivial since the index $|G : H|$ is larger than any character degree of G/N.

(e) This structure theorem is an important step towards a complete classification of the finite groups with a nonlinear irreducible character that vanishes on a unique conjugacy class. Indeed, in a forthcoming paper, we study the structure of the groups arising in parts (ii)(c), (iii) and (iv) in more detail, and we will also consider the primitive case in future work.

Finally, let us make some comments on the notation and organisation of the paper. Our group-theoretic notation is fairly standard. In particular, we use the notation of Kleidman and Liebeck [39] for simple groups and their automorphism groups; for example, we write $\mathrm{L}_n(q)$ and $\mathrm{U}_n(q)$ for $\mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$, respectively. We use $\mathbb{Z}_n$, or just n, to denote a cyclic group of order n, and (a, b) denotes the highest common factor of the positive integers a and b.

In Section 2 we establish a useful result that immediately reduces the proof of Theorem 1 to almost simple groups. We focus on the almost simple groups in Section 3, where we complete the proofs of Theorem 1 and 2. The structure of the primitive groups G with $\kappa(G) = 2$ is investigated in Section 4, and we establish Theorem 4. Finally, in Section 5 we prove Theorem 6 on the finite groups G with a maximal subgroup H and a nonlinear imprimitive irreducible character $\chi = \phi^G$ such that $n(\chi) = 1$ and $\phi \in \mathrm{Irr}(H)$.

2. A reduction theorem

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group of degree n with point stabiliser $H = G_\alpha$. Recall that G is a *Frobenius group* if G is not regular and only the identity element has more than one fixed point (equivalently, $H \neq 1$ and $H \cap H^g = 1$ for all $g \in G \setminus H$). In this situation, $N := \{1\} \cup \Delta(G)$ is a regular normal subgroup of G (see [33, Theorem 7.2], for example) and we have $G = HN$ and $H \cap N = 1$ (we call N the *Frobenius kernel* of G). Since H acts semiregularly on $\Omega \setminus \{\alpha\}$ it follows that $|G| = n(n-1)/d$, where d divides $n-1$ (d is the number of H-orbits on $\Omega \setminus \{\alpha\}$). If G is 2-transitive, i.e., if H acts transitively on $\Omega \setminus \{\alpha\}$, then $d = 1$ and it follows that any two nontrivial elements of N are conjugate in G (so N is an elementary abelian p-group for some prime p, and n is a power of p). In particular, if G is a 2-transitive Frobenius group then $\kappa(G) = 1$.

Also recall that G is *sharply* 2*-transitive* if G acts regularly on the set of pairs of distinct elements of Ω (so G is 2-transitive and no nontrivial element of G fixes more than one point). In particular, G is sharply 2-transitive if and only if $(G, n) = (S_2, 2)$ or G is a 2-transitive Frobenius group. As noted above, the latter groups are precisely the Frobenius groups of order $n(n-1)$ with n a prime power.

Given a group X, we write $X^* = X \setminus \{1\}$ for the set of nontrivial elements in X.

Theorem 2.1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group and assume G is not almost simple. Then $\kappa(G) = 1$ if and only if G is sharply 2-transitive.*

Proof. Let $H = G_\alpha$ be a point stabiliser of G and let $n = |G : H|$ denote the degree of G. Suppose G is sharply 2-transitive. The case $(G, n) = (S_2, 2)$ is clear so let us assume G is a 2-transitive Frobenius group with kernel N. Here $\Delta(G) = N^*$ and H acts regularly on $\Omega \setminus \{\alpha\}$, so $|H| = n - 1$. Let $x \in N^*$. Then $\mathrm{C}_G(x) \leqslant N$ and thus $|x^G| \geqslant |G : N| = |H| = |N^*|$. Since N is normal we have $x^G \subseteq N^*$, so $\Delta(G) = N^* = x^G$ and $\kappa(G) = 1$.

Conversely, suppose $\kappa(G) = 1$. Let N be a minimal normal subgroup of G and note that N is transitive and $G = HN$. There are two cases to consider.

First assume N is regular, so $H \cap N = 1$ and $N^* \subseteq \Delta(G)$. In fact, since $\kappa(G) = 1$, we have $N^* = x^G = \Delta(G)$ for some $x \in N^*$. If N is nonabelian, then it is isomorphic to a direct product of isomorphic nonabelian simple groups and hence $|N|$ is divisible by at least three distinct primes, which is a contradiction since $N^* = x^G$. Therefore N is abelian and so $N \cong \mathbb{Z}_p^k$ for some prime p and integer $k \geqslant 1$. In particular, $N \leqslant \mathrm{C}_G(x)$. Now $|\Delta(G)| \geqslant |H|$ by [10], with equality if and only if G is sharply 2-transitive. Therefore, $|x^G| = |G : \mathrm{C}_G(x)| \geqslant |H|$ and thus $|N| \geqslant |\mathrm{C}_G(x)|$, so $\mathrm{C}_G(x) = N$ and G is sharply 2-transitive.

Now assume $H \cap N \neq 1$. It follows that $N \cong S^k$, where S is a nonabelian simple group and $k \geqslant 1$. By [15, Corollary 4.3B], N is the unique minimal normal subgroup of G. If $k = 1$ then G is almost simple as $\mathrm{C}_G(N) = 1$. So assume that $k \geqslant 2$. Let π_i denote the projection map from $H \cap N$ to the i-th simple factor of N. As noted in the proof of [8, Theorem 2.1], there exists a nontrivial subgroup R of S such that $\pi_i(H \cap N) \cong R$ for all $1 \leqslant i \leqslant k$.

If $R = S$, then there exists a partition $\mathcal{P}$ of $\{1, 2, \ldots, k\}$ such that $H \cap N = \prod_{P \in \mathcal{P}} D_P$, where $D_P \cong S$ and $\pi_i(D_P) = S$ if $i \in P$, otherwise $\pi_i(D_P) = 1$. For each $P \in \mathcal{P}$, let N_P be a subgroup given by the direct product of $|P| - 1$ of the simple direct factors of N corresponding to P. Then $N_0 := \prod_{P \in \mathcal{P}} N_P \leqslant N$ has trivial intersection with H and has order $|\Omega|$. In particular, N_0 is a regular subgroup whose order is divisible by $|S|$. Since $|S|$ is divisible by at least three distinct primes, it follows that N_0 has at least three elements of distinct prime orders and thus $\kappa(G) \geqslant 3$, a contradiction.

Finally, suppose $R \neq S$. By [15, Theorem 4.6A], $G \leqslant L \wr S_k$ acting with its product action on $\Omega = \Gamma^k$ for $k \geqslant 2$, where $L \leqslant \mathrm{Sym}(\Gamma)$ is a primitive almost simple group with socle S. If $u \in S$ is a derangement on Γ then $(u,1,1,\ldots,1),(u,u,1,\ldots,1) \in N$ are non-conjugate derangements on Ω, so $\kappa(G) \geqslant 2$. This final contradiction completes the proof of the theorem. □

3. Almost simple groups

In this section we will prove Theorem 2. Let G be a finite almost simple primitive permutation group with socle S. Let $A = \mathrm{Aut}(S)$, so $S \leqslant G \leqslant A$. In order to establish the bound $\kappa(G) \geqslant 3$ it suffices to show that if H is a maximal subgroup of S then there are at least three A-classes of elements $x \in S$ such that $x^A \cap H$ is empty. Similarly, to justify the asymptotic statement in Theorem 2, we will show that the number of such A-classes tends to infinity as $|S|$ tends to infinity.

In view of Theorem 2.1, we see that Theorem 1 follows immediately from Theorem 2. Similarly, Corollary 3 is easily deduced from Theorem 2.

3.1. **Preliminaries.** Here we record some preliminary results that will be useful in the proof of Theorem 2. Let $\phi : \mathbb{N} \to \mathbb{N}$ be Euler's totient function defined by

$$\phi(n) = |\{m \in \{1,\ldots,n-1\} \mid (m,n) = 1\}|.$$

We will need the following elementary lower bound.

Lemma 3.1. *If $n \in \mathbb{N}$ then $\phi(n) \geqslant \sqrt{n/a}$, where $a = 2$ if $n \equiv 2 \pmod 4$, otherwise $a = 1$.*

Proof. Write $n = \prod_i p_i^{a_i}$, where the p_i are distinct primes, so

$$\phi(n) = \prod_i \phi(p_i^{a_i}) = \prod_i p_i^{a_i-1}(p_i-1).$$

If $n \not\equiv 2 \pmod 4$ then $(p_i,a_i) \neq (2,1)$, so $p_i^{a_i-1}(p_i-1) \geqslant p_i^{a_i/2}$ and thus $\phi(n) \geqslant \sqrt{n}$. Similarly, if $n \equiv 2 \pmod 4$ then $n = 2m$ and m is odd, so $\phi(n) = \phi(m) \geqslant \sqrt{m} = \sqrt{n/2}$. □

Lemma 3.2. *Let $x \in S$ be a self-centralising element of order α with $|\mathrm{N}_S(\langle x\rangle) : \langle x\rangle| = n$. Then there are at least $\phi(\alpha)/n|\mathrm{Out}(S)|$ distinct A-classes of such elements in S.*

Proof. There are precisely $\phi(\alpha)$ elements in $\langle x\rangle$ of order α, and for any such element y we note that $|y^S \cap \langle x\rangle| = n$ since $\mathrm{C}_S(x) = \langle x\rangle$ and $|\mathrm{N}_S(\langle x\rangle) : \langle x\rangle| = n$. Therefore, $\langle x\rangle$ contains $\phi(\alpha)/n$ distinct S-class representatives of order α, so there are at least $\phi(\alpha)/n|\mathrm{Out}(S)|$ distinct A-classes. □

If S is a simple group of Lie type then $|\mathrm{Out}(S)|$ is conveniently recorded in [39, Tables 5.1.A, 5.1.B].

Finally, let us introduce some additional notation. Let G be an almost simple group with socle S and let $\mathcal{M}(G)$ be the set of maximal subgroups H of G such that $G = SH$. Given $H \in \mathcal{M}(G)$, let $\kappa(G,H)$ denote the number of conjugacy classes of derangements in G, with respect to the primitive action of G on G/H. We define

$$\Phi(G) = \min\{\kappa(G,H) \mid H \in \mathcal{M}(G)\}. \qquad (1)$$

In addition, if X is a finite group then $\pi(X)$ denotes the set of prime divisors of $|X|$.

3.2. **Sporadic groups.** Here we establish Theorem 2 for sporadic groups. Set

$$\mathcal{A} = \{\mathrm{HS}.2, \mathrm{He}.2, \mathrm{Fi}_{22}.2, \mathrm{HN}.2, \mathrm{O'N}.2, \mathrm{Fi}_{24}, \mathbb{B}, \mathbb{M}\}.$$

Proposition 3.3. *The conclusion to Theorem 2 holds if S is a sporadic simple group and $G \notin \mathcal{A}$.*

G	M_{11}	M_{22}	M_{12}	J_1	HS	$\mathrm{M}_{22}.2$	M_{23}	J_2	$\mathrm{M}_{12}.2$	M_{24}	J_3	McL	McL.2	$\mathrm{J}_2.2$	O′N
$\Phi(G)$	3	4	5	5	5	6	6	6	7	7	7	7	7	8	9

Co_3	$\mathrm{J}_3.2$	Th	Co_2	He	Ru	Ly	Fi_{22}	Fi_{23}	Suz	J_4	HN	Suz.2	Fi_{24}'	Co_1
10	11	11	12	13	13	14	14	15	15	17	19	21	26	27

TABLE 3. $\Phi(G)$ for some almost simple sporadic groups

Proof. In each case it is straightforward to calculate the exact value of $\kappa(G,H)$ using the information on the fusion of H-classes in G that is available in the GAPCTL Character Table Library [5]. For example, we obtain the following results when $G = \mathrm{M}_{11}$:

H	M_{10}	$\mathrm{L}_2(11)$	$\mathrm{M}_9.2$	S_5	$2.S_4$
$\kappa(G,H)$	3	3	3	4	3

In all cases, the exact value of $\Phi(G)$ (see (1)) is recorded in Table 3. □

Proposition 3.4. *The conclusion to Theorem 2 holds if S is a sporadic simple group.*

Proof. We may assume $G \in \mathcal{A}$. If $G \in \{\mathrm{HS}.2, \mathrm{He}.2, \mathrm{Fi}_{22}.2\}$ we can use MAGMA [3] to determine the fusion of H-classes in G, working with the respective permutation representations of degree 100, 2058 and 3510 provided in the Web-Atlas [50]. In this way, we calculate that $\Phi(\mathrm{HS}.2) = 11$, $\Phi(\mathrm{He}.2) = 16$ and $\Phi(\mathrm{Fi}_{22}.2) = 17$.

Of course, we can immediately discard any remaining cases (G,H) with the property that $|\pi(G) \setminus \pi(H)| \geqslant 3$, which eliminates the Baby Monster and the Monster. In fact, one can check that it only remains to deal with the following cases:

(1) $(\mathrm{HN}.2, S_{12})$ (2) $(\mathrm{HN}.2, 4.\mathrm{HS}.2)$ (3) $(\mathrm{HN}.2, \mathrm{U}_3(8){:}6)$
(4) $(\mathrm{HN}.2, (5{:}4 \times \mathrm{U}_3(5)).2)$ (5) $(\mathrm{O'N}.2, \mathrm{J}_1 \times 2)$ (6) $(\mathrm{Fi}_{24}, \mathrm{Fi}_{23} \times 2)$

In cases (1) – (3), the fusion of H-classes in G is stored in [5] and the result quickly follows as above (we get $\kappa(G,H) = 31, 23, 57$, respectively). In (4) and (6), [8, Proposition 4.3] implies that G contains at least three classes of derangements of prime order. For example, in (6) we find that G contains derangements of order $3, 7$ and 29. Similarly, in case (5), G contains derangements of order 7 and 31, and elements of order 14 are also derangements since $|H|$ is indivisible by 14. □

3.3. **Alternating groups.** In this section we establish Theorem 2 in the case where $S = A_n$ is an alternating group of degree $n \geqslant 5$.

Proposition 3.5. *The conclusion to Theorem 2 holds if $S = A_n$ and $n \leqslant 24$.*

Proof. We can use MAGMA [3] to determine the fusion of H-classes in G, and the result quickly follows. For instance, we obtain the results presented in Table 4 if $G \in \{A_5, S_5, A_6, S_6\}$. In addition, we calculate that $\Phi(G) = 4$ if $G = \mathrm{PGL}_2(9) = A_6.2$ or $\mathrm{Aut}(A_6) = A_6.2^2$, and if $G = \mathrm{M}_{10} = A_6.2$ we get $\kappa(G,[16]) = 2$ (where [16] is a Sylow 2-subgroup of G), $\kappa(G, 3^2{:}Q_8) = 3$ and $\kappa(G, 5{:}4) = 4$. For $7 \leqslant n \leqslant 24$ we record $\Phi(G)$ in Table 5. □

Proposition 3.6. *The conclusion to Theorem 2 holds if $S = A_n$.*

Proof. We may assume that $n > 24$. Let H be a maximal subgroup of G such that $G = SH$. We consider three cases according to the action of H on $\{1,\ldots,n\}$:

(a) H acts primitively on $\{1,\ldots,n\}$;

(b) H acts transitively and imprimitively on $\{1,\ldots,n\}$;

$\kappa(G,H)$	(G,H)
1	(A_5, D_{10})
2	(A_5, D_6), (A_5, A_4), (S_5, D_{12}), (S_5, S_4), $(A_6, 3^2{:}4)$, (A_6, A_5), $(S_6, 3^2{:}D_8)$
3	$(S_5, 5{:}4)$, (A_6, S_4), $(S_6, S_4 \times 2)$
4	(S_6, S_5)

TABLE 4. $\kappa(G,H)$ for $G \in \{A_5, S_5, A_6, S_6\}$

n	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
$\Phi(A_n)$	3	5	5	7	7	11	12	15	18	22	26	31	38	46	55	62	74	88
$\Phi(S_n)$	4	5	7	9	11	15	19	23	30	35	44	50	65	80	95	111	133	157

TABLE 5. $\Phi(G)$ for $G \in \{A_n, S_n\}$, $7 \leqslant n \leqslant 24$

(c) H acts intransitively on $\{1, \ldots, n\}$.

In case (a), let $x \in G$ be an r-cycle, where r is a prime such that $2 \leqslant r < n-2$. Then a theorem of Jordan [38] implies that x is a derangement, whence $\kappa(G,H) \geqslant 3$.

Next assume (b) holds, so H is of type $S_a \wr S_b$, where $n = ab$ and $a, b \geqslant 2$. Let r be a prime in the interval (a, n). As noted in the proof of [8, Proposition 3.6], any r-cycle in G is a derangement. Now, if $a \geqslant 9$ then there are at least three distinct primes in the interval $(a, 2a)$ (see [45], for example) and the result follows (we also note that the number of primes in $(a, 2a)$ tends to infinity as a tends to infinity). Similarly, if $a < 9$ then $b \geqslant 4$ (since $n > 24$) and there are at least three primes in $(a, 4a)$ for all $a \geqslant 2$.

Finally, let us consider (c), so H is of type $S_k \times S_{n-k}$ with $1 \leqslant k < n/2$. Clearly, if n is even then any $x \in G$ of cycle-shape $(\ell, n-\ell)$, where $1 \leqslant \ell \leqslant n/2$, $\ell \neq k$, is a derangement. Now assume n is odd. If $k \neq 3$ then any $x \in G$ of cycle-shape $(3, \ell, n-\ell-3)$, where $1 \leqslant \ell \leqslant (n-3)/2$, $\ell \notin \{k, k-3\}$, is a derangement. Similarly, if $k = 3$ then take $x \in G$ of cycle-shape $(5, \ell, n-\ell-5)$, where $1 \leqslant \ell \leqslant (n-5)/2$ and $\ell \neq 3$. The result follows.

In each case, note that we have also shown that $\kappa(G,H)$ tends to infinity as $|G|$ tends to infinity. $\square$

For the remainder, we may assume that S is a group of Lie type; we deal with the exceptional groups in Section 3.4 and the classical groups in Section 3.5. Our basic approach is similar in both cases. The aim is to identify a collection of elements in G that belong to very few maximal subgroups – if we can show that there are at least three A-classes of such elements (and the number of such classes tends to infinity as $|G|$ tends to infinity), then it just remains to deal with the specific possibilities for H that contain these elements. Given such a subgroup H, we choose an alternative collection of elements $x \in G$ such that $x^A \cap H$ is empty, and we then show that there are sufficiently many A-classes with this property. For some groups of low rank over small fields, we will use MAGMA [3] to obtain the desired result.

3.4. **Exceptional groups.** Let S be a finite simple group of exceptional Lie type over $\mathbb{F}_q$, where $q = p^f$ and p is a prime. Set

$$\mathcal{A} = \{G_2(3), G_2(4), G_2(5), {}^2B_2(8), {}^2B_2(32), {}^2G_2(27), {}^3D_4(2), {}^2F_4(2)'\}.$$

Proposition 3.7. *If $S \in \mathcal{A}$ then either $\kappa(G,H) \geqslant 4$, or $(G,H) = ({}^2B_2(8){:}3, 5{:}4 \times 3)$ and $\kappa(G,H) = 2$.*

Proof. This is a straightforward calculation, using MAGMA and a suitable permutation representation of G given in the Web-Atlas [50]. $\square$

S	$\lvert x_1\rvert$	n_1	$\lvert x_2\rvert$	n_2	$\mathcal{M}(x_1)$
${}^2B_2(q)$, $q \geqslant 2^7$	$q+\sqrt{2q}+1$	4	$q-\sqrt{2q}+1$	4	$\langle x_1\rangle{:}\mathbb{Z}_4$
${}^2G_2(q)$, $q \geqslant 3^5$	$q+\sqrt{3q}+1$	6	$q-\sqrt{3q}+1$	6	$\langle x_1\rangle{:}\mathbb{Z}_6$
${}^2F_4(q)$, $q \geqslant 2^3$	$q^2+\sqrt{2q^3}+q+\sqrt{2q}+1$	12	$q^2-\sqrt{2q^3}+q-\sqrt{2q}+1$	12	$\langle x_1\rangle{:}\mathbb{Z}_{12}$
${}^3D_4(q)$, $q \geqslant 3$	q^4-q^2+1	4	$(q^3-1)(q+1)$	4	$\langle x_1\rangle{:}\mathbb{Z}_4$
${}^2E_6(q)$, $q \geqslant 4$	$(q^6-q^3+1)/a$	9	$(q^5+1)(q-1)/a$	10	$\mathrm{SU}_3(q^3).3$
$G_2(q)$, $q \geqslant 9$	q^2-q+1	6	q^2+q+1	6	$\mathrm{SU}_3(q).2$
$F_4(q)$, $q \geqslant 4$	q^4-q^2+1	12	q^4+1	8	${}^3D_4(q).3$
$E_6(q)$	$(q^6+q^3+1)/b$	9	$(q+1)(q^5-1)/b$	10	$\mathrm{SL}_3(q^3).3$
$E_7(q)$, $q \geqslant 4$	$(q+1)(q^6-q^3+1)/c$	18	$(q-1)(q^6+q^3+1)/c$	18	$(\mathbb{Z}_{(q+1)/c}.{}^2E_6(q)).2$
$E_8(q)$	$q^8+q^7-q^5-q^4-q^3+q+1$	30	$q^8-q^7+q^5-q^4+q^3-q+1$	30	$\langle x_1\rangle{:}\mathbb{Z}_{30}$

$a=(3,q+1)$, $b=(3,q-1)$, $c=(2,q-1)$

TABLE 6.

For the remainder, we may assume that $S \notin \mathcal{A}$.

Proposition 3.8. *The conclusion to Theorem 2 holds if S is one of the simple groups listed in Table 6.*

Proof. Let S be one of the simple groups listed in Table 6. First we claim that there exist elements $x_1, x_2 \in S$ with the following properties:

(i) x_1 and x_2 are self-centralising;

(ii) $|x_i|$ (the order of x_i) and $|\mathrm{N}_S(\langle x_i\rangle):\langle x_i\rangle| = n_i$ are given in Table 6;

(iii) Let $\mathcal{M}(x_1)$ be the set of maximal subgroups of S containing x_1, up to isomorphism. Then $\mathcal{M}(x_1)$ is given in the final column of Table 6.

Detailed information on the conjugacy classes in S is readily available in the literature, and the existence and self-centralising nature of x_1 and x_2 can be quickly verified. In each case, $\langle x_i\rangle$ is a maximal torus of S and the indices n_i are easily computed. Indeed, if $S \neq E_7(q)$ then n_1 is given in [1, Table 1], and the same table also records n_2 in the cases $S \in \{{}^2B_2(q), {}^2G_2(q), {}^2F_4(q), E_8(q)\}$. If $S = {}^3D_4(q)$ then n_2 is given in [14, Table 1.1]. In the remaining cases we have $S = E_6^{\epsilon}(q)$ or $E_7(q)$, and the n_i can be read off from [18]. More precisely, if $S = E_6^{\epsilon}(q)$ then x_2 corresponds to the case labelled $w16$ on [18, p.103], where n_2 is denoted "cn". Similarly, if $S = E_7(q)$ then x_1 and x_2 are the cases labelled $w56$ and $w47$ on [18, p.134,135], respectively. Finally, the information on $\mathcal{M}(x_1)$ is taken from [49, Section 4] (see also [28, Table III]).

The argument in each case is very similar. For example, suppose $S = E_6(q)$. Define x_i, n_i, b as in Table 6 and note that $|\mathrm{Out}(S)| = 2b\log_p q$. Let H be a maximal subgroup of S and recall that it suffices to show that there are at least three A-classes in S that fail to meet H (and that the number of such classes tends to infinity as $|S|$ tends to infinity).

Set $\alpha_i = |x_i|$ and let a_i be the number of distinct A-classes of elements in S of order α_i. By Lemmas 3.1 and 3.2 we have

$$a_1 \geqslant \left\lceil \frac{\phi(\alpha_1)}{18b\log_p q} \right\rceil \geqslant \frac{\sqrt{\alpha_1}}{18b\log_p q},$$

so $a_1 \geqslant 3$, and we observe that a_1 tends to infinity as q tends to infinity. Now x_1 belongs to a unique maximal subgroup of S, which is isomorphic to $\mathrm{SL}_3(q^3).3$ (see [49, p.78–79]). Therefore, it remains to deal with the case $H = \mathrm{SL}_3(q^3).3$. Since $|H|$ is indivisible by α_2, it follows that any element of order α_2 is a derangement, and as before we deduce that

$$a_2 \geqslant \left\lceil \frac{\phi(\alpha_2)}{20b\log_p q} \right\rceil \geqslant \frac{\sqrt{\alpha_2/2}}{20b\log_p q}.$$

	S	Conditions
Linear	$\mathrm{L}_n(q)$	$n \geqslant 2$, $q \geqslant 7$ ($q \neq 9$) if $n=2$, $(n,q) \neq (3,2),(4,2)$
Unitary	$\mathrm{U}_n(q)$	$n \geqslant 3$, $(n,q) \neq (3,2)$
Symplectic	$\mathrm{PSp}_{2m}(q)$	$m \geqslant 2$, $(m,q) \neq (2,2),(2,3)$
Orthogonal	$\mathrm{P\Omega}_{2m}^{\pm}(q)$	$m \geqslant 4$
	$\Omega_{2m+1}(q)$	$m \geqslant 3$, q odd

Table 7. The simple classical groups

The result follows. The other cases are entirely similar, and we omit the details. □

Proposition 3.9. *The conclusion to Theorem 2 holds if S is an exceptional group of Lie type.*

Proof. We may assume that $S \in \mathcal{B}$, where $\mathcal{B}$ is defined as follows:

$$\mathcal{B} = \{G_2(7), G_2(8), {}^2E_6(2), {}^2E_6(3), F_4(2), F_4(3), E_7(2), E_7(3)\}.$$

If $S \in \{G_2(7), {}^2E_6(3), F_4(3), E_7(3)\}$ then the argument in the proof of Proposition 3.8 goes through unchanged (see [28, Table IV]). In each of the remaining cases, we define x_i, n_i, α_i, a_i as before. Let H be a maximal subgroup of S.

Suppose $S = G_2(8)$, so $\alpha_1 = 57$ and $\alpha_2 = 73$. Since $a_2 \geqslant \phi(\alpha_2)/18 = 4$ we may assume that $H = \mathrm{SL}_3(8).2$ since no other maximal subgroups of S contain elements of order 73 (the maximal subgroups of S are determined in [13]). Since $a_1 \geqslant 2$ and $|H|$ is indivisible by α_1 and 19, the result follows.

Next suppose $S = {}^2E_6(2)$. Note that the list of maximal subgroups H of S given in the Atlas [12] is complete (see [36, p.304]). If $|\pi(S) \setminus \pi(H)| \geqslant 3$ then we are done, so we may assume that $H \in \{F_4(2), \mathrm{Fi}_{22}, \Omega_{10}^-(2)\}$. In each of these cases, the fusion of H-classes in S is available in the GAPCTL Character Table Library [5], and the desired result quickly follows.

The case $S = F_4(2)$ is very similar. Here the maximal subgroups of S are determined in [43]. If $H = (2^{1+8} \times 2^6).\mathrm{Sp}_6(2)$ or $\mathrm{Sp}_8(2)$ then the fusion of H-classes in S is stored in [5] and we easily deduce that $\kappa = 12, 33$ in these cases. If $|\pi(S) \setminus \pi(H)| \geqslant 3$ then the result follows, so it remains to deal with the cases $H \in \{\mathrm{L}_4(3){:}2, {}^2F_4(2), {}^3D_4(2){:}3, \Omega_8^+(2){:}S_3\}$. In all four cases it is easy to check that H contains no elements of order 32, but there are four A-classes of such elements, so $\kappa \geqslant 4$ in each of these cases.

Finally, let us assume $S = E_7(2)$. Following [28, Table IV], let $x \in S$ be an element of order $\alpha = 2^7 + 1 = 129$. Then $\mathrm{C}_S(x) = \langle x \rangle$ and $|\mathrm{N}_S(\langle x \rangle) : \langle x \rangle| = 14$ (see the case labelled $w57$ in [18, p.120]), so Lemma 3.2 implies that there are at least $\phi(\alpha)/14 = 6$ distinct A-classes of such elements. Moreover, [28, Table IV] indicates that x is contained in a unique maximal subgroup $\mathrm{SU}_8(2)$ of S. Therefore, we may assume that $H = \mathrm{SU}_8(2)$. Now $|H|$ is indivisible by $\beta = 2^7 - 1 = 127$ and we calculate that there are at least $\phi(127)/14 = 9$ distinct A-classes of elements of order 127. The result follows. □

3.5. **Classical groups.** In order to complete the proof of Theorem 2, we may assume that S is one of the classical groups listed in Table 7. The conditions recorded in the final column ensure that S is simple, and that S is not isomorphic to one of the other groups in the table, or to one of the groups we have already considered (see [39, Proposition 2.9.1], for example). We will write $\mathrm{L}_n^+(q) = \mathrm{L}_n(q)$ and $\mathrm{L}_n^-(q) = \mathrm{U}_n(q)$ to denote $\mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$, respectively. Let V be the natural S-module and set $A = \mathrm{Aut}(S)$.

As before, it suffices to show that if H is a maximal subgroup of S then there are at least three A-classes of elements $x \in S$ such that $x^A \cap H$ is empty (and that the number of such A-classes tends to infinity as $|S|$ tends to infinity). As in the previous section, we will identify a sufficient number of A-classes of elements that belong to a very restricted collection of maximal subgroups (in almost all cases, these will be regular semisimple elements). In order to do this, we will use several results from [6, 28], which rely on the earlier analysis of primitive prime divisors in [29]. It then remains to deal with the primitive groups that correspond to this very specific list of maximal subgroups, and we will identify an alternative collection of A-classes of derangements. As before, it is convenient to use Magma for some low-dimensional groups over small fields.

3.5.1. *Linear and unitary groups.* Here we assume $S = \mathrm{L}_n^{\epsilon}(q)$. Set $d = (n, q-\epsilon)$ and $e = d(q-\epsilon)$.

Proposition 3.10. *The conclusion to Theorem 2 holds if S is one of the following:*

$$\mathrm{L}_2(q),\ q \leqslant 81;\ \mathrm{L}_3(q),\ q \leqslant 16;\ \mathrm{L}_4(q),\ q \leqslant 9;\ \mathrm{L}_5(2);\ \mathrm{L}_7(2);\ \mathrm{L}_{11}(2)$$
$$\mathrm{U}_3(q),\ q \leqslant 11;\ \mathrm{U}_4(q),\ q \leqslant 7;\ \mathrm{U}_5(2);\ \mathrm{U}_6(2);\ \mathrm{U}_8(2);\ \mathrm{U}_8(3);\ \mathrm{U}_9(2);\ \mathrm{U}_{12}(2).$$

Proof. This is a straightforward verification. For example, suppose $S = \mathrm{L}_2(q)$. If $16 < q \leqslant 81$ then an easy Magma calculation shows that if H is a maximal subgroup of S then there are at least three A-classes of elements in S that fail to meet H. If $7 \leqslant q \leqslant 16$ then we consider each possibility for G in turn, using Magma to compute $\kappa(G,H)$ for each maximal subgroup H of G (with $G = SH$). The other linear groups with $n \leqslant 5$ are handled in the same way. If $S = \mathrm{L}_7(2)$ then any element of order 2^7-1 is a derangement, unless H is a field extension subgroup of type $\mathrm{GL}_1(2^7)$, in which case elements of order 2^6-1 are derangements. The case $S = \mathrm{L}_{11}(2)$ is entirely similar.

The argument for the unitary groups $\mathrm{U}_n(q)$ with $n < 8$ is similar. If $S = \mathrm{U}_8(q)$ then [6, Proposition 5.22] implies that any element of order $(q^7+1)/d$ is a derangement unless H is a P_1 parabolic subgroup (the stabiliser of a totally singular 1-space), in which case we can take any element of order $(q^5+1)(q^3+1)/e$. Similarly, if $S = \mathrm{U}_{12}(2)$ then by considering elements of order $(2^{11}+1)/3$ we reduce to the case $H = P_1$, for which all elements of order $(2^7+1)(2^5+1)/9$ are derangements. Finally, if $S = \mathrm{U}_9(2)$ then any element of order $(2^9+1)/9$ is a derangement unless H is a field extension subgroup of type $\mathrm{GU}_3(8)$. In the latter case, elements of order $(2^8-1)/3$ are derangements. □

Proposition 3.11. *The conclusion to Theorem 2 holds if $S = \mathrm{L}_n^{\epsilon}(q)$ is one of the groups listed in Table 8.*

Proof. This is similar to the proof of Proposition 3.8. We may assume that S is not one of the groups in the statement of Proposition 3.10. There are several cases to consider.

First assume $\epsilon = +$ and $n = 2m$ is even, where $m \geqslant 3$ is odd. Let $T = \langle x_1 \rangle$ be a cyclic maximal torus of S of order $\alpha_1 = (q^{m+2}-1)(q^{m-2}-1)/e$ (see [7, Theorem 2.1], for example), so x_1 is self-centralising and $|\mathrm{N}_S(\langle x_1 \rangle) : \langle x_1 \rangle| = m^2-4$. Let a_1 be the number of distinct A-classes of elements in S of order α_1. By applying Lemmas 3.1 and 3.2, we deduce that

$$a_1 \geqslant \left\lceil \frac{\phi(\alpha_1)}{(m^2-4)\cdot 2d\log_p q} \right\rceil \geqslant \frac{\sqrt{\alpha_1/2}}{2d(m^2-4)\log_p q}.$$

It follows that $a_1 \geqslant 3$, and we also see that a_1 tends to infinity as $|S|$ tends to infinity.

Now x_1 belongs to exactly two maximal subgroups of S; parabolic subgroups of type P_{m-2} and P_{m+2} (see [28, Table II]). Therefore, in order to establish Theorem 2 in this case, we may assume that $H = P_{m-2}$. Let $x_2 \in S$ be an element of order $\alpha_2 = (q^n-1)/e$. Then x_2 is self-centralising, $|\mathrm{N}_S(\langle x_2 \rangle) : \langle x_2 \rangle| = n$ and x_2 is a derangement since it acts irreducibly on V. If a_2 is the number of A-classes of such elements then

$$a_2 \geqslant \left\lceil \frac{\phi(\alpha_2)}{2m\cdot 2d\log_p q} \right\rceil \geqslant \frac{\sqrt{\alpha_2/2}}{4md\log_p q}$$

and the result follows.

Conditions on $S = \mathrm{L}_n^{\epsilon}(q)$	$\lvert x_1\rvert$	n_1	$\lvert x_2\rvert$	n_2
$n=2m$, $m \geqslant 4-\epsilon$ odd	$(q^{m+2}-\epsilon)(q^{m-2}-\epsilon)/e$	m^2-4	$(q^n-1)/e$	n
$n=2m$, $m \geqslant 3-\epsilon$ even, $(\epsilon,m,q) \neq (+,2,2)$	$(q^{m+1}-\epsilon)(q^{m-1}-\epsilon)/e$	m^2-1	$(q^n-1)/e$	n
$n=2m+1$, $m \geqslant 2$, $\epsilon=+$, $(m,q) \neq (5,2)$	$(q^{m+1}-1)(q^m-1)/e$	$m(m+1)$	$(q^n-1)/e$	n
$n=2m+1$, $m \geqslant 5$ odd, $\epsilon=-$	$(q^{m+2}+1)(q^{m-1}-1)/e$	$(m+2)(m-1)$	$(q^n+1)/e$	n
$n=2m+1$, $m \geqslant 4$ even, $\epsilon=-$	$(q^{m+1}+1)(q^m-1)/e$	$m(m+1)$	$(q^n+1)/e$	n

$e=(q-\epsilon)(n,q-\epsilon)$

TABLE 8.

The other cases in Table 8 are very similar. In each case we take $x_1 \in S$ of the given order, noting that x_1 is self-centralising and $|\mathrm{N}_S(\langle x_1\rangle):\langle x_1\rangle| = n_1$. As above, we estimate the number of A-classes of such elements, and we appeal to [28, Table II] to see that the only maximal subgroups of S containing x_1 are reducible. To complete the proof, we now switch to the self-centralising elements x_2, as indicated in Table 8, and we repeat the above argument. □

Proposition 3.12. *The conclusion to Theorem 2 holds if S is a linear or unitary group.*

Proof. It remains to deal with the possibilities for S listed in Table 9, and we proceed as in the proof of the previous proposition. For example, suppose $S = \mathrm{L}_2(q)$. Let $x_1 \in S$ be an element of order $\alpha_1 = (q^2-1)/e$. Then x_1 is self-centralising and the number of distinct A-classes of such elements, denoted by a_1, satisfies the bound

$$a_1 \geqslant \left\lceil \frac{\phi(\alpha_1)}{2\cdot d\log_p q}\right\rceil \geqslant \frac{\sqrt{\alpha_1/2}}{2d\log_p q}.$$

In particular, a_1 tends to infinity as $|S|$ tends to infinity, and we calculate that $a_1 \geqslant 3$ since $q \geqslant 83$. Now x_1 belongs to a unique maximal subgroup of S, namely $H = \mathrm{N}_S(\langle x_1\rangle)$ (see [28, p.767]). Let $x_2 \in S$ be an element of order $\alpha_2 = (q-1)^2/e$ and let a_2 be the number of A-classes of such elements. Note that x_2 is a derangement since $|H|$ is indivisible by α_2. Then

$$a_2 \geqslant \left\lceil \frac{\phi(\alpha_2)}{2\cdot d\log_p q}\right\rceil \geqslant \frac{\sqrt{\alpha_2/2}}{2d\log_p q}$$

and thus $a_2 \geqslant 3$ if $q > 125$. In fact, if $81 < q \leqslant 125$ then an easy MAGMA calculation shows that $a_2 \geqslant 4$. The result follows.

The other cases in Table 9 are handled in the same way, using the information in [28, p.767] (in each case, note that $|x_1|$ and $|x_2|$ are coprime). We omit the details. □

3.6. **Symplectic groups.** Here we assume $S = \mathrm{PSp}_{2m}(q)$, where $m \geqslant 2$ and $(m,q) \neq (2,2),(2,3)$ (since $\mathrm{PSp}_4(2)' \cong A_6$ and $\mathrm{PSp}_4(3) \cong \mathrm{U}_4(2)$). Set $d = (2,q-1)$.

We will frequently refer to the regular semisimple elements $x_i \in S$ defined in Table 10. In the second column, we give an orthogonal decomposition of the natural S-module V that is fixed by x_i, with x_i acting irreducibly on each nondegenerate subspace in the decomposition (the same notation is used in [6, 28]). The order α_i of a lift $\hat{x}_i \in \mathrm{Sp}_{2m}(q)$ of x_i is given in the next column, and in the final column we record a lower bound $a_i \geqslant \beta_i$, where a_i denotes the number of A-classes of elements in S with the same shape and order as x_i (the lower bound follows from the fact that two semisimple elements in $\mathrm{Sp}_{2m}(q)$ are conjugate if and only if they have the same multiset of eigenvalues in $\bar{\mathbb{F}}_q$).

S	$\lvert x_1\rvert$	n_1	$\lvert x_2\rvert$	n_2
$\mathrm{L}_2(q), q \geqslant 83$	$(q^2-1)/e$	2	$(q-1)^2/e$	2
$\mathrm{L}_3(q), q \geqslant 17$	$(q^3-1)/e$	3	$(q^2-1)(q-1)/e$	2
$\mathrm{U}_3(q), q \geqslant 13$	$(q^3+1)/e$	3	$(q^2-1)(q+1)/e$	2
$\mathrm{U}_4(q), q \geqslant 8$	$(q^3+1)(q+1)/e$	3	$(q^4-1)/e$	4
$\mathrm{U}_5(q), q \geqslant 3$	$(q^5+1)/e$	5	$(q^4-1)(q+1)/e$	4
$\mathrm{U}_6(q), q \geqslant 3$	$(q^5+1)(q+1)/e$	5	$(q^6-1)/e$	6
$\mathrm{U}_7(q)$	$(q^7+1)/e$	7	$(q^6-1)(q+1)/e$	6

$e = (q-\epsilon)(n, q-\epsilon)$

TABLE 9.

	Decomposition	α_i	β_i
x_1	$2m$	q^m+1	$\phi(q^m+1)/2me$
x_2	$2 \perp (2m-2)$	$\mathrm{lcm}(q+1, q^{m-1}+1)$	$\phi(q+1)\phi(q^{m-1}+1)/2(2m-2)e$
x_3	$4 \perp (2m-4)$	$\mathrm{lcm}(q^2+1, q^{m-2}+1)$	$\phi(q^2+1)\phi(q^{m-2}+1)/4(2m-4)e$

$d = (2, q-1)$, $e = 2^{\delta} d \log_p q$, $\delta = 1$ if $m = p = 2$ and $\delta = 0$ otherwise

TABLE 10.

Proposition 3.13. *The conclusion to Theorem 2 holds if S is one of the following:*

$$\mathrm{PSp}_4(q),\ q \leqslant 8;\ \mathrm{PSp}_6(q),\ q \leqslant 3;\ \mathrm{Sp}_8(2);\ \mathrm{Sp}_{10}(2);\ \mathrm{Sp}_{12}(2);\ \mathrm{Sp}_{14}(2).$$

Proof. Set $S = \mathrm{PSp}_{2m}(q)$. In the cases with $m \leqslant 5$ we can use MAGMA to compute $\kappa(G, H)$ for every maximal subgroup H of G, and the result quickly follows. Now assume $(m, q) = (6, 2)$ or $(7, 2)$. Consider the irreducible elements of type x_1 defined in Table 10, and note that the bound $a_1 \geqslant \beta_1$ implies that $a_1 \geqslant 3$. By the proof of [6, Proposition 5.8], we may assume that H is of type $\mathrm{O}^-_{2m}(q)$ or $\mathrm{Sp}_{2m/k}(q^k)$, where k is a prime divisor of m (these are the only maximal subgroups of S that contain such elements). In both cases we observe that semisimple elements of type x_2, and regular unipotent elements (that is, unipotent elements with Jordan form $[J_{2m}]$) are derangements. The result now follows since the bound $a_2 \geqslant \beta_2$ in Table 10 implies that $a_2 \geqslant 2$. □

Proposition 3.14. *The conclusion to Theorem 2 holds if $S = \mathrm{PSp}_{2m}(q)$ and $m \geqslant 5$.*

Proof. Let H be a maximal subgroup of S. It suffices to show that there are at least three A-classes of elements $x \in S$ such that $x^A \cap H$ is empty (and that the number of such A-classes tends to infinity as $|S|$ tends to infinity). We will assume that S is not one of the groups in the statement of Proposition 3.13. We continue to adopt the notation introduced in Table 10. It is important to note that the bounds $a_i \geqslant \beta_i$ in Table 10, together with the conditions on m and q, imply that $a_i \geqslant 3$ in all cases (with the exception of a_3 if $(m, q) = (5, 3)$), and it is clear that a_i tends to infinity as $|S|$ tends to infinity.

First assume mq is odd. Consider elements of type x_2, as described in Table 10. According to [6, Proposition 5.10], the only maximal subgroup of S containing such an element is the stabiliser of a nondegenerate 2-space, denoted by N_2. Since $a_2 \geqslant 3$ (and a_2 tends to infinity as $|S|$ tends to infinity), we have reduced to the case $H = N_2$. In this situation, irreducible elements of type x_1 are derangements and the result follows.

Next suppose q is odd and $m \geqslant 6$ is even. Here we use elements of type x_3 to reduce to the case where H is either a subspace subgroup of type N_4 (the stabiliser of a nondegenerate 4-space), or a field extension subgroup of type $\mathrm{Sp}_m(q^2)$ (see [6, Proposition 5.10]). These subgroups can be handled as before, using elements of type x_1 and x_2, respectively (note that the order of the field extension subgroup is indivisible by $|x_2|$).

Finally, let us assume q is even. By considering elements of type x_1, and by inspecting the proof of [6, Proposition 5.8], we reduce to the case where H is of type $\mathrm{O}_{2m}^{-}(q)$ or $\mathrm{Sp}_{2m/k}(q^k)$ for a prime divisor k of m. Now x_2 fixes an orthogonal decomposition of the form $2 \perp (2m-2)$, which implies that $x_2 \in \mathrm{O}_2^-(q) \times \mathrm{O}_{2m-2}^-(q) < \mathrm{O}_{2m}^+(q)$ and thus x_2 is a derangement if H is of type $\mathrm{O}_{2m}^-(q)$. Since $|x_2|$ does not divide the order of a field extension subgroup, we also deduce that these elements are derangements if H is of type $\mathrm{Sp}_{2m/k}(q^k)$. The result follows. □

Proposition 3.15. *The conclusion to Theorem 2 holds if S is a symplectic group.*

Proof. We may assume that $2 \leqslant m \leqslant 4$. We may also assume that S is not one of the cases handled in Proposition 3.13. We continue to adopt the notation introduced in Table 10. In particular, we set $d = (2, q-1)$ and $e = 2^\delta d \log_p q$, where $\delta = 1$ if $m = p = 2$ and $\delta = 0$ otherwise. As usual, let H be a maximal subgroup of S.

First assume q is odd and note that the bound $a_1 \geqslant \beta_1$ in Table 10 implies that $a_1 \geqslant 3$. If $m = 2$ or 4 then by considering elements of type x_1 we reduce to the case where H is of type $\mathrm{Sp}_m(q^2)$ (see [6, Proposition 5.12]). In this situation, we define an element $x_4 \in S$ that fixes an orthogonal decomposition $2 \perp (2m-2)$ of V by centralising the 2-space and acting irreducibly on the $(2m-2)$-space. Then x_4 is a derangement and we note that

$$a_4 \geqslant \left\lceil \frac{\phi(q^{m-1}+1)}{(2m-2)e} \right\rceil \tag{2}$$

where a_4 denotes the number of A-classes of such elements. In particular, it follows that $a_4 \geqslant 3$ if $m = 2$ and $q > 29$, or if $m = 4$ and $q > 5$. (We also note that a_4 tends to infinity as $|S|$ tends to infinity.) Of course, unipotent elements with Jordan form $[J_2, J_1^{2m-2}]$ or $[J_4, J_1^{2m-4}]$ are also derangements (where J_i denotes a standard unipotent Jordan block of size i), so it is easy to see that there are always at least three distinct A-classes of derangements.

Similarly, if q is odd and $m = 3$ then we reduce to subgroups of type $\mathrm{GU}_3(q)$ and $\mathrm{Sp}_2(q^3)$ via elements of type x_1 (see [2, Main Theorem], for example). In these cases, elements of type x_2 are derangements, and the result follows since $a_2 \geqslant 3$ (if $q > 5$ then this follows from the bound $a_2 \geqslant \beta_2$, and for $q = 5$ it can be checked directly).

Finally, suppose q is even. In the usual manner, by considering elements of type x_1 and applying [6, Proposition 5.8], we reduce to the case where H is of type $\mathrm{O}_{2m}^-(q)$ or $\mathrm{Sp}_{2m/k}(q^k)$, with k a prime divisor of m. In the first case, elements of type x_2 are derangements and the result follows. Similarly, if H is of type $\mathrm{Sp}_{2m/k}(q^k)$ then elements of type x_4 (as defined above) are derangements, and the result follows via the lower bound in (2) (and the fact that unipotent elements with Jordan form $[J_2, J_1^{2m-2}]$ or $[J_4, J_1^{2m-4}]$ are also derangements). □

3.7. **Orthogonal groups.** Finally, let us assume $S = \mathrm{P\Omega}_n^\epsilon(q)$, where $n \geqslant 7$. Set $A = \mathrm{Aut}(S)$ and define $d = (2, q-1)$ if n is even, and $d = 1$ if n is odd. As in the previous section, we will denote an orthogonal decomposition $V = U \perp W$ with $\dim U = m$ by writing $m \perp (n-m)$. If m is even, in order to distinguish between nondegenerate m-spaces of plus and minus types, we will write m^+ and m^-, respectively. This is consistent with the notation used in [6, 28].

Proposition 3.16. *The conclusion to Theorem 2 holds if S is one of the following:*

$$\mathrm{P\Omega}_8^\epsilon(q),\ q \leqslant 4;\ \mathrm{P\Omega}_{10}^\epsilon(q),\ q \leqslant 3;\ \mathrm{P\Omega}_{12}^\epsilon(q),\ q \leqslant 3;\ \Omega_{14}^+(2);\ \Omega_{16}^+(2);\ \Omega_{18}^+(2).$$

Proof. Set $S = \mathrm{P\Omega}_{2m}^\epsilon(q)$. If $m \leqslant 4$ or $(m,q) \in \{(5,2),(6,2)\}$ then the result can be checked using MAGMA.

Next suppose $S = \Omega_{14}^+(2)$. Let $x \in S$ be an element of order 195 that fixes an orthogonal decomposition $2^- \perp 12^-$ of the natural S-module. Using MAGMA, we see that there are

	Decomposition	β_i
x_1	$2^- \perp (2m-2)^-$	$\phi(q+1)\phi(q^{m-1}+1)/2(2m-2)e$
x_2, m odd	$(m-1)^- \perp (m+1)^-$	$\phi(q^{(m-1)/2}+1)\phi(q^{(m+1)/2}+1)/(m^2-1)e$
x_3, m even	$(m-2)^- \perp (m+2)^-$	$\phi(q^{(m-2)/2}+1)\phi(q^{(m+2)/2}+1)/(m^2-4)e$

$e = 2d\log_p q$

TABLE 11.

at least three A-classes of such elements, and by the main theorem of [29] we deduce that the only maximal subgroup of S containing x is the stabiliser of a nondegenerate 2-space of minus-type, which we denote by N_2^-. Therefore, we have reduced to the case $H = N_2^-$. It is easy to identify three classes of derangements in this case. For instance, any unipotent element with Jordan form $[J_{13}, J_1]$, $[J_{11}, J_3]$ or $[J_9, J_5]$ is a derangement. The cases $S = \Omega_{16}^+(2)$ and $\Omega_{18}^+(2)$ are entirely similar.

It remains to deal with the cases $S = \mathrm{P}\Omega_{10}^{\epsilon}(3)$ and $\mathrm{P}\Omega_{12}^{\epsilon}(3)$. First assume $S = \mathrm{P}\Omega_{10}^+(3)$. Let $x \in S$ be an element of order 82 that fixes an orthogonal decomposition $2^- \perp 8^-$. There are at least three A-classes of such elements, and the main theorem of [29] implies that the only maximal subgroups of S that contain such elements are of type N_2^- or $\mathrm{O}_5(9)$. The result now follows because it is easy to see that there are at least three A-classes of derangements if H is of type N_2^- or $\mathrm{O}_5(9)$; for example, any unipotent element with Jordan form $[J_9, J_1]$, $[J_7, J_3]$ or $[J_5, J_2^2, J_1]$ is a derangement. The case $S = \mathrm{P}\Omega_{12}^+(3)$ is very similar (working with elements of order 122 that fix a decomposition $2^- \perp 10^-$).

The cases $S = \mathrm{P}\Omega_{10}^-(3)$ or $\mathrm{P}\Omega_{12}^-(3)$ are also similar. If $S = \mathrm{P}\Omega_{10}^-(3)$ then the only maximal subgroups of S that contain elements of order 61 are of type $\mathrm{GU}_5(3)$, and the result follows as before. Similarly, if $S = \mathrm{P}\Omega_{12}^-(3)$ then we work with elements of order 365, which only belong to maximal subgroups of type $\mathrm{O}_6^-(3^2)$ or $\mathrm{O}_4^-(3^3)$. Again, the result quickly follows. □

Proposition 3.17. *The conclusion to Theorem 2 holds if* $S = \mathrm{P}\Omega_{2m}^+(q)$ *and* $m \geqslant 5$.

Proof. We may assume that S is not one of the groups in the statement of Proposition 3.16. We define the regular semisimple elements $x_i \in S$ as in Table 11 (we use the same notation as in [6, 28]), where β_i is a lower bound on a_i, which is the number of distinct A-classes of elements in S with the same shape and order as x_i. Let H be a maximal subgroup of S.

First assume m is odd. Consider elements of type x_2. By [6, Proposition 5.13], the only maximal subgroups of S containing x_2 are of type N_{m-1}^-. The lower bound $a_2 \geqslant \beta_2$ implies that $a_2 \geqslant 3$ (and that a_2 tends to infinity as $|S|$ tends to infinity). Now, if $H = N_{m-1}^-$ then elements of type x_1 are derangements, and we observe that the lower bound $a_1 \geqslant \beta_1$ is sufficient.

Now assume m is even. By considering elements of type x_3, and by applying [6, Proposition 5.14], we reduce to the case where H is of type N_{m-2}^- or $\mathrm{O}_m^+(q^2)$. Here elements of type x_1 are derangements, and the result follows via the bound $a_1 \geqslant \beta_1$. □

Proposition 3.18. *The conclusion to Theorem 2 holds if* $S = \mathrm{P}\Omega_8^+(q)$.

Proof. In view of Proposition 3.16, we may assume that $q \geqslant 5$. Let $x_1 \in S$ be a regular semisimple element that fixes an orthogonal decomposition $2^- \perp 6^-$. Let a_1 denote the number of distinct A-classes of such elements. Then

$$a_1 \geqslant \left\lceil \frac{\phi(q+1)\phi(q^3+1)}{12 \cdot 6d\log_p q} \right\rceil$$

and we deduce that $a_1 \geqslant 3$ if $q \geqslant 7$ (and that a_1 tends to infinity as $|S|$ tends to infinity). If $q = 5$ then a direct calculation shows that there are at least three A-classes of such elements (in particular, none of the relevant $\mathrm{PGO}_8^+(5)$-classes are fused by a triality graph automorphism of S). By [28, p.767], the only maximal subgroups of S containing such elements are of type N_2^- or $\mathrm{GU}_4(q)$, so we may assume that H is one of these subgroups. Now let $x_2 \in S$ be a regular semisimple element that fixes an orthogonal decomposition $2^+ \perp 6^+$ and lifts to an element in $\Omega_8^+(q)$ of order q^3-1. Note that x_2 is a derangement, and let a_2 be the number of A-classes of such elements. Then

$$a_2 \geqslant \left\lceil \frac{\phi(q-1)\phi(q^3-1)}{12 \cdot 6d \log_p q} \right\rceil$$

and the result follows if $q > 7$. Finally, if $q = 5$ or 7 then one can check directly that there are at least three A-classes of such elements. □

Proposition 3.19. *The conclusion to Theorem 2 holds if* $S = \mathrm{P}\Omega_{2m}^-(q)$ *and* $m \geqslant 4$.

Proof. We may assume that S is not one of the groups in the statement of Proposition 3.16. Let $x_1 \in S$ be an irreducible element that lifts to an element of order $(q^m+1)/d$ in $\Omega_{2m}^-(q)$. Let a_1 be the number of A-classes of such elements. Then

$$a_1 \geqslant \left\lceil \frac{\phi(q^m+1)}{2m \cdot 2d \log_p q} \right\rceil \tag{3}$$

and thus $a_1 \geqslant 3$ (and a_1 tends to infinity as $|S|$ tends to infinity). By [2, Main Theorem], if H is a maximal subgroup of S that contains such an element then H is a field extension subgroup of type $\mathrm{O}_{2m/k}^-(q^k)$ or $\mathrm{GU}_m(q)$ (with m odd), where k is a prime divisor of m. In both of these cases, any element $x_2 \in S$ that fixes a decomposition $2^+ \perp (2m-2)^-$ of the natural S-module, centralising the 2-space and acting irreducibly on the $(2m-2)$-space, is a derangement. Now, if a_2 denotes the number of A-classes of such elements then

$$a_2 \geqslant \left\lceil \frac{\phi(q^{m-1}+1)}{(2m-2) \cdot 2d \log_p q} \right\rceil \tag{4}$$

and the result follows. □

Proposition 3.20. *The conclusion to Theorem 2 holds if* $S = \Omega_{2m+1}(q)$ *and* $m \geqslant 3$.

Proof. If $S = \Omega_7(3), \Omega_7(5)$ or $\Omega_9(3)$ then the result can be checked directly, using Magma [3], so we will assume that we are not in one of these cases.

Let $x_1 \in S$ be a regular semisimple element of order $(q^m+1)/2$ that fixes a decomposition $(2m)^- \perp 1$ of the natural S-module, and let a_1 be the number of distinct A-classes of such elements. Then (3) holds (setting $d = 1$), so $a_1 \geqslant 3$ (and a_1 tends to infinity as $|S|$ tends to infinity). By [6, Proposition 5.20], the only maximal subgroup of S containing such an element is the stabiliser of a nondegenerate $2m$-space of minus-type, denoted by $H = N_{2m}^-$. In this situation, let $x_2 \in S$ be an element of order $q(q^{m-1}+1)/2$ that fixes a decomposition $3 \perp (2m-2)^-$, where x_2 acts indecomposably on the 3-space and irreducibly on the $(2m-2)^-$-space. If a_2 denotes the number of A-classes of such elements then (4) holds (with $d = 1$), so $a_2 \geqslant 2$ and the result follows since every regular unipotent element is also a derangement. □

This completes the proof of Theorem 2.

4. Two classes of derangements

In this section we investigate the finite primitive permutation groups G with the property $\kappa(G) = 2$, with the aim of proving Theorem 4. We begin with a preliminary lemma. As before, if X is a group then $X^* = X \setminus \{1\}$ is the set of nontrivial elements in X.

Lemma 4.1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite transitive permutation group with point stabiliser $H \neq 1$. Let N be a regular normal subgroup of G. Then G is a Frobenius group with kernel N if and only if $\Delta(G) \subseteq N$.*

Proof. Since N is regular, we have $G = HN$ and $H \cap N = 1$. By definition, if G is a Frobenius group with kernel N then $\Delta(G) = N^*$.

Now assume $\Delta(G) \subseteq N$. First observe that if $x \in N^*$ then $x^G \cap H \subseteq N^* \cap H = \emptyset$, so $x \in \Delta(G)$ and thus $N^* \subseteq \Delta(G)$. Therefore $\Delta(G) = N^*$. Let $\{H_1, \ldots, H_k\}$ be the set of conjugates of H in G. Then $k = |G : \mathrm{N}_G(H)| \leqslant |G : H| = |N|$ and

$$|\bigcup_{i=1}^{k} H_i^*| \leqslant \sum_{i=1}^{k} |H_i^*| = \sum_{i=1}^{k}(|H| - 1) = k(|H| - 1).$$

Now

$$G = \{1\} \cup \Delta(G) \cup \left(\bigcup_{g \in G} (H^*)^g \right) = N \cup \left(\bigcup_{i=1}^{k} H_i^* \right)$$

and thus

$$|G| = |N| + |\bigcup_{i=1}^{k} H_i^*| \leqslant |N| + k(|H| - 1) \leqslant |N| + |N|(|H| - 1) = |N| \cdot |H| = |G|.$$

Since $|H| \neq 1$, it follows that $k = |N| = |G : H|$ and $|\bigcup_{i=1}^{k} H_i^*| = \sum_{i=1}^{k} |H_i^*|$. The latter equality forces $H_i \cap H_j = 1$ for every $1 \leqslant i \neq j \leqslant k$. Equivalently, $H \cap H^g = 1$ for all $g \in G \setminus H$ and thus G is a Frobenius group with kernel N. □

Recall that if J is a proper subgroup of G, then we set

$$\Delta_J(G) = G \setminus \bigcup_{g \in G} J^g.$$

We record the following easy result.

Lemma 4.2. *Let H be a maximal subgroup of a finite group G, M a normal subgroup of G such that $G = HM$, and let K be a proper subgroup of M containing $H \cap M$. Then $\Delta_K(M) \subseteq \Delta_H(G)$.*

Proof. Let $x \in \Delta_K(M)$ and assume that $x \notin \Delta_H(G)$. Then $x \in H^g$ for some $g \in G$. It follows that $x^{g^{-1}} \in H$ and since $x \in M \trianglelefteqslant G$, we also have $x^{g^{-1}} \in M$, so $x^{g^{-1}} \in H \cap M$ and thus $x \in (H \cap M)^g = H^g \cap M$. Since $g \in G = HM$, we can write $g = hm$ with $h \in H$ and $m \in M$. Then $x \in H^g \cap M = H^m \cap M = (H \cap M)^m \leqslant K^m$ with $m \in M$, contradicting our assumption that $x \in \Delta_K(M)$. The result follows. □

Proposition 4.3. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group of degree n with point stabiliser H. Assume G is not almost simple. If $\kappa(G) = 2$, then one of the following holds:*

(i) *$(G, n) = (\mathbb{Z}_3, 3)$;*

(ii) *$G = HN$ is a Frobenius affine group, where the kernel N is an elementary abelian p-group of order $n = p^k$ for some odd prime p, and $|H| = (n - 1)/2$;*

(iii) *G is a non-Frobenius 2-transitive affine group.*

Moreover, any primitive group G as in (i) *or* (ii) *has the property $\kappa(G) = 2$.*

Proof. Let $H = G_\alpha$ be a point stabiliser. First assume G is one of the groups in (i) or (ii). Clearly, $\kappa(G) = 2$ in case (i). In (ii), H acts semiregularly on $\Omega \setminus \{\alpha\}$ with exactly two orbits. In particular, $\Delta(G) = N^* = x^G \cup y^G$ and thus $\kappa(G) = 2$.

Now assume $\kappa(G) = 2$. We proceed as in the proof of Theorem 2.1. Let N be a minimal normal subgroup of G, so $G = HN$. If $H = 1$ then G is regular and clearly $(G, n) = (\mathbb{Z}_3, 3)$ is the only possibility. For the remainder, let us assume $H \neq 1$.

Suppose that $H \cap N \neq 1$. By the proof of Theorem 2.1, we may assume that $N \cong S^k$, where S is a nonabelian simple group, $k \geqslant 2$ and $G \leqslant L \wr S_k$ acting with its product action on $\Omega = \Gamma^k$, where $L \leqslant \mathrm{Sym}(\Gamma)$ is a primitive almost simple group with socle S. Let $u \in S$ be a derangement on Γ. Then $x = (u, 1, \ldots, 1) \in N$ and $y = (u, u, 1, \ldots, 1) \in N$ are non-conjugate derangements on Ω. If $k \geqslant 3$ then $z^G = (u, u, u, 1, \ldots, 1)^G$ would be another G-class of derangements, so $k = 2$ since $\kappa(G) = 2$. If S has two L-classes of derangements with representatives u and v, then $(u, 1), (u, u), (v, 1) \in N$ are non-conjugate derangements, which is a contradiction. Therefore S contains a unique L-class of derangements on Γ.

Write $N = S_1 \times S_2$, where $S_i \cong S$, $i = 1, 2$. Let K be a maximal subgroup of N such that $H \cap N \leqslant K$. By Lemma 4.2, every derangement of N on N/K is also a derangement of N on Ω. It is well known that either K is a diagonal subgroup of the form $\{(s, \phi(s)) \mid s \in S_1\}$ for some isomorphism $\phi : S_1 \to S_2$, or K is a standard maximal subgroup, that is $K = S_1 \times K_2$ or $K_1 \times S_2$, where $K_i < S_i$ is maximal (see, for example, [48, Lemma 1.3]). In the diagonal case, every element of the form $(s, 1)$ with $1 \neq s \in S_1$ is a derangement of N on N/K. Clearly, this case cannot happen. Now assume K is a standard maximal subgroup. Without loss of generality, we may assume that $K = K_1 \times S_2$, where K_1 is maximal in S_1. Let $s \in N$ be a derangement on N/K of prime power order, say p^e for some prime p and integer $e \geqslant 1$ (such an element exists by the main theorem of [17]). Since $|\pi(S)| \geqslant 3$, choose $a, b \in S_2$ of distinct prime orders that are both different from p. Then $(s, 1), (s, a)$ and (s, b) are derangements of N on N/K with distinct orders, so N has at least three distinct N-classes of derangements on N/K and thus N has at least three distinct G-classes of derangements on Ω. We have now eliminated the case $H \cap N \neq 1$.

Finally, suppose that $H \cap N = 1$, so N is regular and we may identify Ω with N. By arguing as in the proof of Theorem 2.1, we deduce that N is an elementary abelian p-group for some prime p, say $|N| = n = p^k$. In particular, G is an affine group. If $\Delta(G) \subseteq N$ then G is Frobenius by Lemma 4.1, and we deduce that (ii) holds (here H acts semiregularly on $\Omega \setminus \{\alpha\}$, with exactly two orbits). On the other hand, if $\Delta(G) \not\subseteq N$ then $N^* = x^G \subset \Delta(G)$ for some $x \in N^*$, and thus H acts transitively on N^*, so G is a 2-transitive affine group. □

To complete the proof of Theorem 4, we may assume that G is a non-Frobenius 2-transitive affine group. Write $G = HN$, where $H = G_\alpha$ and N is a regular normal elementary abelian subgroup of order p^k (p prime). Assume that $\kappa(G) = 2$, so $N^* = x^G$ and $\Delta(G) = x^G \cup y^G$ for some $x \in N^*$ and $y \in G \setminus N$. Note that $N \leqslant \mathrm{C}_G(x) \leqslant G = HN$ and $|x^G| = |G : \mathrm{C}_G(x)| = |N^*| = p^k - 1$, so $\mathrm{C}_G(x) = N\mathrm{C}_H(x)$ and

$$|H| = |G : N| = |G : \mathrm{C}_G(x)| \cdot |\mathrm{C}_G(x) : N| = (p^k - 1)|\mathrm{C}_H(x)|. \tag{5}$$

We need a couple of preliminary results.

Lemma 4.4. *Let $C = \mathrm{C}_H(x)$. Then $|C| = p^b r^c$, where $r \neq p$ is a prime and $b, c \geqslant 0$.*

Proof. If $\mathrm{C}_H(x)$ is a p-group, then we are done. Assume that $|\mathrm{C}_H(x)|$ is divisible by a prime $r \neq p$. Then $\mathrm{C}_H(x)$ contains an element of u order r. Let $z := xu \in G$. Then $|z| = pr$ and z is a derangement. Indeed, if $z \in H^g$ for some $g \in G$, then $z^r = x^r \in H^g$, which implies that $\langle x^r \rangle = \langle x \rangle \leqslant H^g$ as $(r, p) = 1$, so $x \in H^g$ and this is a contradiction since $x \in \Delta(G)$. Since $\kappa(G) = 2$ and $|z| \neq |x|$, we must have $z^G = y^G$. Therefore r is uniquely determined and the result follows. □

In the next lemma, note that part (i) holds for *any* non-Frobenius 2-transitive group $G = HN$ such that $|N| = p^k$ and p divides $|H|$.

Lemma 4.5. *Let H_p be a Sylow p-subgroup of H, and assume that $H_p \neq 1$.*

(i) *$[N, H_p]$ is a proper subgroup of N, and $tz \in \Delta(G)$ for all $t \in H_p$ and all $z \in N \setminus [N, H_p]$.*

(ii) *H_p has exponent p and $H_p^* \subseteq t^H$ for some $t \in H_p^*$. Furthermore, $|\mathrm{C}_H(x)| = p^b$ and thus $|H| = (p^k - 1)p^b$, for some $b \geqslant 1$.*

Proof. Let $P = NH_p$ and observe that P is a Sylow p-subgroup of G.

First consider (i). Let c be the nilpotency class of P, so if we define $\gamma_0(P) = P$ and $\gamma_{i+1}(P) = [\gamma_i(P), P]$ for all $i \geqslant 0$, then $\gamma_c(P) = 1$ and $\gamma_{c-1}(P) \neq 1$. Seeking a contradiction, suppose that $N = [N, H_p]$. Then $N \subseteq [P, P] = \gamma_1(P)$, so

$$N = [N, H_p] \subseteq [\gamma_1(P), P] = \gamma_2(P)$$

and so on. In this way, we deduce that $N \subseteq \gamma_c(P) = 1$, which is a contradiction. Hence $[N, H_p] \neq N$ and we fix an element $z \in N \setminus [N, H_p]$.

We claim that $tz \in \Delta(G)$ for all $t \in H_p$. Assume otherwise. Then $tz \in H^g$ for some $g \in G$. Since $G = HN$, we can write $g = hn$ with $h \in H, n \in N$. Then $tz \in H^n$ and thus $ntzn^{-1} \in H$. Since $z, n \in N$ we have $zn = nz$ and

$$ntzn^{-1} = t(t^{-1}ntn^{-1})z = t[t, n^{-1}]z \in H.$$

Hence $[t, n^{-1}]z \in H \cap N = 1$, which implies that $z = [n^{-1}, t] \in [N, H_p]$, contradicting our choice of z. This completes the proof of part (i).

Now let us turn to (ii). By (i), $tz \in \Delta(G)$ for all $t \in H_p$. If $t \in H_p^*$ then $tz \notin N^* = x^G$, so $tz \in y^G$ and thus $(H_p^*)z \subseteq y^G$.

Let $s, t \in H_p^*$. Then $sz, tz \in y^G$, so $(tz)^g = sz$ for some $g = hn \in HN = G$ with $h \in H, n \in N$. It follows that $n^{-1}h^{-1}tzhn = sz$ so

$$s^{-1}t^h = n^s zn^{-1}(z^h)^{-1} \in H \cap N = 1,$$

and thus $t^h = s$. Therefore $H_p^* \subseteq t^H$, so all elements in H_p^* have the same order, which must be p.

Now $tz \in y^G$ and $tz \in P = NH_p$, so y is a p-element and thus every element in $\Delta(G)$ has p-power order. Let $C = \mathrm{C}_H(x)$. Suppose $|C|$ is divisible by a prime $r \neq p$ and let $u \in C$ be an element of order r. Then $ux \in \Delta(G)$ has order rp, which is a contradiction. Therefore $|C| = p^b$ for some $b \geqslant 1$, and the result follows (see (5)). □

Let $G = HN \leqslant \mathrm{Sym}(\Omega)$ be a primitive affine permutation group, where $|N| = p^k$ for a prime p. We may identify Ω with $N \cong (\mathbb{F}_p)^k$ and take H to be the stabiliser of the zero vector in N, so $H \leqslant \mathrm{GL}_k(p)$ is irreducible. The 2-transitive affine permutation groups were classified by Hering [31, 32] (also see [9, Section 7.3] and [41, Appendix 1]). Four infinite families arise, together with finitely many sporadic cases of degree at most 59^2. By inspecting these cases, we can severely restrict the possibilities for a non-Frobenius 2-transitive affine group G with $\kappa(G) = 2$.

For the remainder of this section, we will write $\mathcal{P}(n, i)$ for the i-th primitive permutation group of degree n in the library of primitive groups stored in Magma [3], which can be accessed via the command $\mathsf{PrimitiveGroup}(n, i)$.

Proposition 4.6. *Let $G = HN$ be a non-Frobenius 2-transitive affine group of degree p^k, where $H \leqslant \mathrm{GL}_k(p)$ as above. If $\kappa(G) = 2$ then one of the following holds:*

(i) *$H \leqslant \Gamma\mathrm{L}_1(p^k)$;*

(ii) *$\mathrm{SL}_2(q) \trianglelefteq H$, where $q^2 = p^k$;*

	n	H	Conditions
(i)	p^k	$H \leqslant \Gamma\mathrm{L}_1(p^k)$	
(ii)	q^a	$\mathrm{SL}_a(q) \trianglelefteqslant H \leqslant \Gamma\mathrm{L}_a(q)$	$a \geqslant 2$
(iii)	q^a	$\mathrm{Sp}_a(q) \trianglelefteqslant H$	$a \geqslant 4$
(iv)	q^6	$G_2(q)' \trianglelefteqslant H$	$p = 2$
(v)	$5^2, 7^2, 11^2, 23^2$	$\mathrm{SL}_2(3) \trianglelefteqslant H$	
(vi)	3^4	$2^{1+4} \trianglelefteqslant H$	
(vii)	$9^2, 11^2, 19^2, 29^2, 59^2$	$\mathrm{SL}_2(5) \trianglelefteqslant H$	
(viii)	2^4	A_6	
(ix)	2^4	A_7	
(x)	3^6	$\mathrm{SL}_2(13)$	

TABLE 12. 2-transitive affine groups

(iii) $G = \mathcal{P}(5^2, 17) = 5^2{:}(2^{1+2}.6)$, $\mathcal{P}(11^2, 42) = 11^2{:}(2^{1+2}.[30])$, $\mathcal{P}(3^4, 70) = 3^4{:}((2 \times Q_8){:}2){:}5$ *or* $\mathcal{P}(29^2, 104) = 29^2{:}(7 \times 2.\mathrm{SL}_2(5))$.

Moreover, each group G in (iii) *has the property $\kappa(G) = 2$.*

Proof. By Hering's Theorem, the possibilities for H are given in Table 12, where $n = p^k$ denotes the degree of G. In order to prove the proposition, we need to eliminate cases (iii) – (x), and also case (ii) with $a \geqslant 3$.

As before, write $N^* = x^G$ and $\Delta(G) = x^G \cup y^G$, where $y \in G \setminus N$. Set $C = \mathrm{C}_H(x)$ and recall that $|H| = (p^k - 1)|C|$. By Lemma 4.4, it follows that

$$\frac{|H|_{p'}}{p^k-1} \text{ is a prime power.} \tag{6}$$

We start by considering the cases (ii), (iii) and (iv). Write $q = p^m$, so $ma = k$ and $q^a = p^k$ (where $a = 6$ in case (iv)).

Suppose (ii) holds. If $a \geqslant 4$ then $(q^2 - 1)(q^3 - 1)$ divides $|H|_{p'}/(p^k - 1)$, but this is incompatible with (6). Now assume $a = 3$. Here (6) implies that $q^2 - 1 = r^t$ for some prime $r \neq p$ and integer $t \geqslant 0$, so $p^{2m} = 1 + r^t$ and we deduce that $m = 1$ and $p \in \{2, 3\}$. If $p = 2$ then $\Gamma\mathrm{L}_3(2) \cong \mathrm{SL}_3(2)$, so $H = \mathrm{SL}_3(2)$, $G = 2^3{:}\mathrm{SL}_3(2)$ and using MAGMA we calculate that $\kappa(G) = 5$. Similarly, if $p = 3$ then $\Gamma\mathrm{L}_3(3) = \mathrm{GL}_3(3)$ and thus $G = 3^3{:}\mathrm{SL}_3(3)$ or $3^3{:}\mathrm{GL}_3(3)$. Here we calculate that $\kappa(G) = 10$ or 11, respectively.

Now assume (iii) holds, so $a \geqslant 4$ is even. If $a \geqslant 6$ then $(q^2 - 1)(q^4 - 1)$ divides $|H|_{p'}/(p^k - 1)$, which contradicts (6), so we may assume that $a = 4$. Here $q^2 - 1 = r^t$, where r is a prime and $t \geqslant 0$, so as in the previous case we deduce that $m = 1$ and $p \in \{2, 3\}$. In particular, $\mathrm{Sp}_4(p) \trianglelefteqslant H \leqslant \mathrm{GL}_4(p)$ with $p = 2, 3$. If $p = 2$ then $H = \mathrm{Sp}_4(2)$ since $\mathrm{Sp}_4(2)$ is a maximal subgroup of $\mathrm{GL}_4(2)$, so $G = 2^4{:}\mathrm{Sp}_4(2)$ and we calculate that $\kappa(G) = 10$. If $p = 3$ then $H \cong \mathrm{Sp}_4(3)$ or $\mathrm{N}_{\mathrm{GL}_4(3)}(\mathrm{Sp}_4(3)) = \mathrm{Sp}_4(3).2$, and we find that $\kappa(G) = 24$ or 18, respectively.

Next consider (iv). Here $p = 2$, $a = 6$ and $q^2 - 1$ divides $|H|_{p'}/(p^k - 1)$, so $q^2 - 1 = r^t$ for some prime $r \neq p$ and integer $t \geqslant 0$. The only possibility is $m = 1$, so $G = 2^6{:}G_2(2)'$ or $2^6{:}G_2(2)$, and we calculate that $\kappa(G) = 10$ or 14, respectively.

To complete the proof of the proposition, we need to deal with the remaining cases labelled (v) to (x) in Table 12. In each of these cases we use the library of primitive groups in MAGMA to determine the possiblities for G, and in each case we compute $\kappa(G)$.

Consider (v). Here $k = 2$ and $\mathrm{SL}_2(3) \trianglelefteqslant H \leqslant \mathrm{GL}_2(p)$, where $p \in \{5, 7, 11, 23\}$. We use the library of primitive groups of degree p^2 to determine the possibilities for G with

$\kappa(G) = 2$; we find that either $p = 5$ and $G = \mathcal{P}(5^2, 17) = 5^2{:}(2^{1+2}.6)$, or $p = 11$ and $G = \mathcal{P}(11^2, 42) = 11^2{:}(2^{1+2}.[30])$. Similarly, in (vi) we find that the only example is $G = \mathcal{P}(3^4, 70) = 3^4{:}((2 \times Q_8){:}2){:}5$, and in (vii) the only example is $G = \mathcal{P}(29^2, 104) = 29^2{:}(7 \times 2.\mathrm{SL}_2(5))$. Finally, in cases (viii), (ix) and (x) we calculate that $\kappa(G) = 5, 6$ and 3, respectively. $\square$

We now focus on the possibilities that can arise in cases (i) and (ii) of Proposition 4.6. We begin with a preliminary lemma.

Lemma 4.7. *Let G be the primitive affine group $q^2{:}\mathrm{SL}_2(q)$, where $q = 2^m$ and $m \geqslant 2$. Then $\kappa(G) \geqslant 3$.*

Proof. Write $G = HN$, where $H = \mathrm{SL}_2(q)$ and N is elementary abelian of order $q^2 = 2^{2m}$. We can embed G into $\mathrm{SL}_3(q)$ as follows:

$$G = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ \alpha & a & b \\ \beta & c & d \end{pmatrix} \mid \alpha, \beta, a, b, c, d \in \mathbb{F}_q,\ ad - bc = 1 \right\}$$

$$N = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \beta & 0 & 1 \end{pmatrix} \mid \alpha, \beta \in \mathbb{F}_q \right\} \cong q^2$$

$$H = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{F}_q,\ ad - bc = 1 \right\} \cong \mathrm{SL}_2(q).$$

Note that

$$H_2 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & c & 1 \end{pmatrix} \mid c \in \mathbb{F}_q \right\}$$

is a Sylow 2-subgroup of H. Direct computation shows that

$$[N, H_2] = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \beta & 0 & 1 \end{pmatrix} \mid \beta \in \mathbb{F}_q \right\}.$$

By Lemma 4.5(i), we deduce that

$$z_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

and

$$z_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ \gamma & 1 & 0 \\ \gamma & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ \gamma & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

are derangements, where $\gamma \in \mathbb{F}_q$ is a generator for $\mathbb{F}_q^*$. Since $z_1, z_2 \notin N$, it suffices to show that z_1 and z_2 are not G-conjugate.

Seeking a contradiction, assume that $z_1^g = z_2$ for some $g \in G$, say

$$g = \begin{pmatrix} 1 & 0 & 0 \\ \alpha & a & b \\ \beta & c & d \end{pmatrix}$$

where $a, b, c, d, \alpha, \beta \in \mathbb{F}_q$ and $ad - bc = 1$. Now it follows from the equation $z_1^g = z_2$ that $z_1 g = g z_2$ and hence

$$\begin{pmatrix} 1 & 0 & 0 \\ \alpha + 1 & a & b \\ \alpha + \beta & a + c & b + d \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ \alpha + \gamma a & a + b & b \\ \beta + \gamma c & c + d & d \end{pmatrix}$$

which implies that

$$\left\{\begin{array}{ccc} \alpha+1 & = & \alpha+\gamma a \\ a & = & a+b \\ \alpha+\beta & = & \beta+\gamma c \\ a+c & = & c+d \\ b+d & = & d \end{array}\right.$$

and thus

$$\left\{\begin{array}{ccc} \gamma a & = & 1 \\ b & = & 0 \\ d & = & a \\ \alpha & = & \gamma c. \end{array}\right.$$

Since $ad-bc=1$ we deduce that

$$1 = ad = a^2 = \gamma^{-2}$$

and thus $\gamma^2=1$. This implies that $\gamma=1$, which is a contradiction since $m \geqslant 2$. □

Proposition 4.8. *Let $G=HN$ be a non-Frobenius 2-transitive affine group of degree p^k, where $\mathrm{SL}_2(q) \trianglelefteqslant H$ and $q^2=p^k$. Then $\kappa(G)=2$ if and only if $G \cong S_4$.*

Proof. Let us assume that $\kappa(G)=2$ and write $\Delta(G)=x^G \cup y^G$ as before, where $N^*=x^G$. Set $C=\mathrm{C}_H(x)$ and let H_p be a Sylow p-subgroup of H. Recall that $|H|=(p^k-1)|C|$ (see (5)). Write $k=2m$, where $m\geqslant 1$ is an integer.

Here $|\mathrm{SL}_2(q)| = p^m(p^k-1)$ divides $|H|$ and thus p^m divides $|C|$, so Lemma 4.5(ii) implies that $|C|=p^b$ where $b\geqslant m$. Therefore, $|H:\mathrm{SL}_2(p^m)|=p^{b-m}$. Since $|\Gamma\mathrm{L}_2(p^m):\mathrm{SL}_2(p^m)| = m(p^m-1)$, it follows that $H\leqslant \Gamma\mathrm{SL}_2(p^m)$ and thus $H/\mathrm{SL}_2(p^m)$ is cyclic. More precisely, either $H=\mathrm{SL}_2(p^m)$ or $H=\mathrm{SL}_2(p^m)\langle\tau\rangle$ where τ is a p-element and $\tau^{p^{b-m}} \in \mathrm{SL}_2(p^m)$. By Lemma 4.5(ii), H_p has exponent p and thus $|\tau|=p$.

First assume that $H=\mathrm{SL}_2(p^m)\langle\tau\rangle$ with $|\tau|=p$. Let $1\neq\sigma\in H_p\cap\mathrm{SL}_2(p^m)$. By Lemma 4.5(ii), $\tau=\sigma^h\in\mathrm{SL}_2(p^m)$ for some $h\in H$, which is a contradiction. Therefore, this case does not occur.

Finally, suppose that $H=\mathrm{SL}_2(p^m)$. Here H_p is an elementary abelian p-group of order p^m. By Lemma 4.5(ii), all nontrivial elements in H_p are H-conjugate and we quickly deduce that $p=2$. If $m=1$ then $G\cong 2^2{:}S_3\cong S_4$ and $\kappa(G)=2$, and Lemma 4.7 implies that $\kappa(G)\geqslant 3$ if $m\geqslant 2$. □

The next proposition completes the proof of Theorem 4.

Proposition 4.9. *Let $G=HN$ be a non-Frobenius 2-transitive affine group of degree p^k, where $H\leqslant \Gamma\mathrm{L}_1(p^k)$. Then $\kappa(G)=2$ only if k is even and $|H|=2(p^k-1)$.*

Proof. Suppose $\kappa(G)=2$ and write $\Delta(G)=x^G\cup y^G$ as before, where $N^*=x^G$. Set $C=\mathrm{C}_H(x)$ and let H_p be a Sylow p-subgroup of H. Note that H is soluble and recall that $|H|=(p^k-1)|C|$.

Set $H_0=H\cap \mathrm{GL}_1(p^k)$ and note that $\mathrm{GL}_1(p^k)$ is cyclic of order p^k-1. Then H/H_0 is also cyclic and $|H/H_0|$ divides k. Moreover, NH_0 is a Frobenius group, so $H_0\cap C=1$ and $C\cong H_0C/H_0$ is cyclic. Write $|H_0|=(p^k-1)/d$ for some integer $d\geqslant 1$. Since $|H|$ is divisible by p^k-1, it follows that d divides $|H:H_0|$. Therefore H/H_0 has a normal subgroup of order d, and the inverse image of this subgroup in H, say L, is a normal subgroup of H containing H_0, and $|L|=p^k-1$. There are two cases to consider.

First assume that $|C|$ is divisible by p. Then $H_p\neq 1$, so Lemma 4.5(ii) implies that H_p has exponent p and C is a p-group, say $|C|=p^b$. Since C is cyclic we have $p^b=p$ and thus $|H|=p(p^k-1)$, which implies that $H=LC$, $L\cap C=1$ and C is a Sylow p-subgroup of H. Write $C=\langle t\rangle$ with $|t|=p$. By Lemma 4.5(ii), $t^h=t^{-1}$ for some $h\in H$, say $h=t^sl$

where $l \in L$ and $s \in \mathbb{Z}$. Then $t^h = t^l = t^{-1}$ which implies that $t^{-2} = [t, l] \in L \cap \langle t \rangle = 1$. Therefore $|t| = 2 = p$ and $|H| = 2(2^k - 1)$. In particular, k is even.

Now assume that $|C|$ is indivisible by p. Then $|C| = r^c$ for some prime $r \neq p$ and $c \geqslant 1$ (see Lemma 4.4). Write $C = \langle t \rangle$. As in the proof of Lemma 4.4, $sx \in \Delta(G) \setminus x^G = y^G$ for all $1 \neq s \in C$. It follows that $|C| = r$, so $|H| = r(p^k - 1)$ and our aim is to show that $r = 2$. Since $\{tx, t^{-1}x\} \subseteq y^G$, we deduce that $t^h = t^{-1}$ for some $h \in H$. There are now two cases to consider.

If $t \notin L$, then $H = LC$ with $L \cap C = 1$, and by arguing as above we deduce that $|t| = |C| = r = 2$, k is even and $G = (NL).2$, where NL is a 2-transitive Frobenius group.

Now assume that $t \in L$ for every subgroup L of index r in H with $H_0 \leqslant L$. Since t fixes $x \in N^*$ it follows that $t \notin H_0$, so tH_0 is a nontrivial real element of order r in the cyclic group H/H_0, which implies that tH_0 is an involution and thus $r = 2$. Since $t \in L$ and $|L| = p^k - 1$ is even, it follows that p is odd. Moreover, since $H_0 \trianglelefteqslant H_0C \trianglelefteqslant L \trianglelefteqslant H$ with $|H : L| = 2$, $|H_0C : H_0| = 2$ and $|H : H_0|$ dividing k, we deduce that k is divisible by 4. □

In [21, Section 15], Foulser gives detailed information on the precise structure of the 2-transitive affine groups $G = HN$ with $H \leqslant \Gamma\mathrm{L}_1(p^k)$. To close this section, we show that $\kappa(G) = 2$ in the special case $H = \mathrm{GL}_1(p^k).2$ (with k even). We thank Bob Guralnick for helpful comments on the proof.

Proposition 4.10. *Let $G = HN$ be a non-Frobenius 2-transitive affine group of degree p^k, where k is even and $H = \mathrm{GL}_1(p^k).2 \leqslant \Gamma\mathrm{L}_1(p^k)$. Then $\kappa(G) = 2$.*

Proof. Write $q^2 = p^k$ and set $L = \mathrm{GL}_1(q^2)$ and $H = L\langle\phi\rangle$, where ϕ is a field automorphism of order 2. By Theorem 1, $\kappa(G) \geqslant 2$. Moreover, since $NL = \mathrm{AGL}_1(q^2)$ is sharply 2-transitive, it suffices to show that there is a unique G-class of derangements in the coset $NL\phi$. Let $y \in NL\phi$ be a derangement. To prove the proposition, we will show that y^G meets $N\phi$, and then we prove that any two derangements in $N\phi$ are G-conjugate.

Consider $y^2 \in NL$. If $y^2 \in NL \setminus N$ then y^2 has a unique fixed point (since NL is Frobenius), which contradicts the fact that y is a derangement. Therefore, $y^2 \in N$. Now $y \in N\ell\phi$ for some $\ell \in L$, so $(\ell\phi)^2 \in N \cap L = 1$ and thus $\ell\phi$ is an involution. We claim that $\ell\phi$ is L-conjugate to ϕ. To see this, note that there are precisely $q + 1$ involutions in the coset $L\phi$ (involutions correspond to elements in L that are inverted under the action of ϕ), and we calculate that $|\phi^L| = q + 1$. This justifies the claim, and we deduce that $y^g \in N\phi$ for some $g \in G$. Set $z = y^g$.

It is easy to check that there are precisely $q-1$ involutions in the coset $N\phi$, each having q fixed points. Therefore, z is one of $q(q-1)$ elements in $N\phi$ of order at least 3, and to complete the proof it suffices to show that any two of these elements are G-conjugate. Let $C = C_{NL}(\phi)$ and note that $z^{NC} \subset N\phi$, so it suffices to show that $|z^{NC}| = q(q-1)$. Now $|C| = |C_N(\phi)||C_L(\phi)| = q(q-1)$ and $|NC| = |N||C|/|N \cap C| = q^3(q-1)/q = q^2(q-1)$, so we need $|C_{NC}(z)| = q$. Since $z^2 \in N^*$ and NL is a Frobenius group, we have $C_{NL}(z^2) \leqslant N$, so $C_{NL}(z^2) = C_N(z^2)$ and thus $C_{NL}(z) = C_N(z) = C_{NC}(z)$. Since z acts on N as a field automorphism of order 2, we deduce that $|C_N(z)| = q$ and the result follows. □

5. Zeros of characters

Let G be a finite group, let H be a proper subgroup of G and let $H_G = \bigcap_{g \in G} H^g$ denote the core of H in G. Set

$$\Delta_H(G) = G \setminus \bigcup_{g \in G} H^g$$

and let $\kappa_H(G)$ be the number of conjugacy classes in $\Delta_H(G)$. Note that if $H_G = 1$ then G is a permutation group on G/H, $\Delta_H(G)$ is the set of derangements in G, and $\kappa_H(G) = \kappa(G)$ as before. The aim of this section is to prove Theorem 6.

Following [20], a triple (G, H, L) with $L \trianglelefteqslant H \leqslant G$ is called a *W-triple* if $H \cap H^g \leqslant L$ for every $g \in G \setminus H$. By a theorem of Wielandt, if (G, H, L) is a W-triple then

$$M = G \setminus \bigcup_{g \in G} (H \setminus L)^g$$

is a normal subgroup of G and we have $G = HM$ and $H \cap M = L$ (see [47, Exercise 1, p.347] for a proof using character theory). The normal subgroup M is called the *kernel* of the W-triple (G, H, L). This is a natural generalisation of Frobenius' theorem.

Let χ be a complex character of G. Recall that $x \in G$ is a *zero* of χ if $\chi(x) = 0$. Let $n(\chi)$ be the number of G-classes on which χ vanishes. Note that the conditions $\kappa_H(G) = 1$ and $n(1_H^G) = 1$ are equivalent, where 1_H^G is the permutation character of G.

In the next lemma, we consider the structure of finite groups G that contain a maximal subgroup H such that $\kappa_H(G) = 1$.

Lemma 5.1. *Let H be a maximal subgroup of a finite group G and assume that $\Delta_H(G) = x^G$ for some $x \in G$. Let $N = H_G$ and $M = \langle x^G \rangle$.*

(i) *If $H \trianglelefteqslant G$, then G is a Frobenius group with an abelian odd-order kernel $H = G'$ of index two;*

(ii) *If $H \ntrianglelefteq G$, then $N \trianglelefteqslant M \trianglelefteqslant G'$ and either $M = G = G'$, or $M \neq G$ and $(G, H, H \cap M)$ is a W-triple with kernel M.*

Proof. First assume that $H \trianglelefteqslant G$. Then $G/H \cong \mathbb{Z}_p$ for some prime p as H is normal and maximal in G. Since $\Delta_H(G) = G \setminus H = x^G$, G/H has exactly two conjugacy classes and thus $|G : H| = p = 2$. Hence, $G = H \cup Hx$ and $Hx = G \setminus H = x^G$, where $H \cap Hx = \emptyset$. Thus

$$|x^G| = |G : \mathrm{C}_G(x)| = |H| = \frac{1}{2}|G|.$$

Therefore, $|\mathrm{C}_G(x)| = 2$ and so $\mathrm{C}_G(x) = \langle x \rangle$ is cyclic of order 2. Clearly, $G' \leqslant H$. Now, if $h \in H$ then $hx \in Hx = x^G$, so $hx = x^g$ for some $g \in G$ and thus $h = x^g x^{-1} \in G'$. Therefore $H \leqslant G'$ and thus $H = G'$. As $\mathrm{N}_G(\langle x \rangle) = \mathrm{C}_G(x) = \langle x \rangle$, we deduce that G is a Frobenius group with Frobenius complement $\langle x \rangle$ of order 2 and a Frobenius kernel G' of odd order. Moreover, since each element $h \in H = G'$ can be written in the form $h = x^g x^{-1}$ for some $g \in G$, we have

$$h^x = x^{-1} x^g x^{-1} x = x^{-1} x^g = x(x^g)^{-1} = h^{-1}.$$

Therefore x inverts every element of G', so G' is abelian.

Now assume H is not normal in G. Then $G' \nleqslant H$ and thus $G = HG'$ and $H \cap G' < G'$, so $x^G \cap G'$ is nonempty. Let $y \in x^G \cap G'$. Clearly, $\Delta_H(G) = y^G = x^G$, hence $M = \langle x^G \rangle = \langle y^G \rangle \trianglelefteqslant G'$ as $y \in G' \trianglelefteqslant G$. Next, we claim that $N \leqslant M$. Let $n \in N$. If $nx \in \bigcup_{g \in G} H^g$ then $nx \in H^z$ for some $z \in G$, but $n \in N = N^z \leqslant H^z$ and thus $x \in n^{-1}(H^z) = H^z$, which is a contradiction. Therefore, $nx \in \Delta_H(G) = x^G$, which implies that $nx \in M$ and so $n \in M$ as $x \in M$. We conclude that $N \trianglelefteqslant M \trianglelefteqslant G'$, as claimed.

If $M = G$, then $M = G = G'$ and we are done. Now assume that $M \neq G$. Let $k = |G : \mathrm{N}_G(H)| = |G : H|$ and let $\{H^{g_1}, \ldots, H^{g_k}\}$ be the set of distinct conjugates of H in G. Since $x \in M \setminus H$, we deduce that $G = HM$ and thus $k = |G : H| = |M : L|$, where $L = H \cap M \trianglelefteqslant H$. Observe that

$$G \setminus M = \left(\bigcup_{i=1}^{k} H^{g_i} \right) \setminus \bigcup_{i=1}^{k} (H^{g_i} \cap M) = \left(\bigcup_{i=1}^{k} H^{g_i} \right) - \bigcup_{i=1}^{k} (H \cap M)^{g_i} = \bigcup_{i=1}^{k} (H \setminus L)^{g_i}.$$

It follows that

$$|G| - |M| = |G \setminus M| = |\bigcup_{i=1}^{k} (H \setminus L)^{g_i}| \leqslant k|H \setminus L| = k(|H| - |L|).$$

Since $|G| = k|H|$ and $|M| = k|L|$, we deduce that $|G| - |M| = k(|H| - |L|)$ and thus

$$|\bigcup_{i=1}^{k}(H \setminus L)^{g_i}| = \sum_{i=1}^{k} |(H \setminus L)^{g_i}|.$$

Therefore, $(H \setminus L) \cap (H \setminus L)^g = \emptyset$ for all $g \in G \setminus H$, and thus (G, H, L) is a W-triple with kernel M. □

Recall that if $G \leqslant \mathrm{Sym}(\Omega)$ is a transitive permutation group of degree $n \geqslant 2$ with point stabiliser H then $\Delta(G) \geqslant |H|$, with equality if and only if G is sharply 2-transitive (see [10]). The next lemma gives a similar lower bound on $|\Delta_H(G)|$ for any finite group G and proper subgroup H.

Lemma 5.2. *Let G be a finite group, let H be a proper subgroup of G, and set $N = H_G$. Then $|\Delta_H(G)| = |\Delta_{H/N}(G/N)| \cdot |N| \geqslant |H|$.*

Proof. Let Ω be the set of right cosets of H/N in G/N and note that G/N is a transitive permutation group on Ω with point stabiliser H/N. Write

$$\Delta_{H/N}(G/N) = \{Na_1, Na_2, \dots, Na_k\}$$

and note that $k \geqslant |H : N|$ (see [10]), so to complete the proof it suffices to show that $\Delta_H(G) = \bigcup_{i=1}^{k} Na_i$.

Let $n \in N$ and $i \in \{1, 2, \dots, k\}$. If $na_i \in H^g$ for some $g \in G$ then since $n \in N \trianglelefteqslant G$ and $N \leqslant H$, we have $Na_i = Nna_i \in (H/N)^{Ng}$, which is a contradiction. Conversely, if $a \in \Delta_H(G)$, then $Na \in \Delta_{H/N}(G/N)$ so $Na = Na_j$ for some $j \in \{1, 2, \dots, k\}$. We conclude that $\Delta_H(G) = \bigcup_{i=1}^{k} Na_i$ and the result follows. □

Lemma 5.3. *Let H be a maximal subgroup of a finite group G and assume that $\Delta_H(G) = x^G$ for some $x \in G$. Then x is a p-element and $\mathrm{C}_G(x)$ is a p-group for some prime p.*

Proof. Let $N = H_G$. As in the proof of the previous lemma, first note that G/N is a transitive permutation group on the set of right cosets of H/N in G/N. By [17, Theorem 1], $Nx \in G/N$ is a derangement of order p^b for some prime p and integer $b \geqslant 1$. Write $|x| = p^a m$ with $(p, m) = 1$ and $a \geqslant 1$. Then $a \geqslant b$ and there exist $u, v \in \mathbb{Z}$ with $1 = up^a + vm$. We have that $x^{p^a} = (x^{p^b})^{p^{a-b}} \in N$ and thus $n^{-1} := x^{up^a} \in N$. Clearly, $nx = x^{mv} \in \Delta_H(G) = x^G$, so x^{mv} and x have the same order. It follows that $m = 1$ and hence x is a p-element (with $|x| = p^a$).

Finally, seeking a contradiction, suppose that $\mathrm{C}_G(x)$ is not a p-group. Let $r \neq p$ be a prime divisor of $|\mathrm{C}_G(x)|$ and fix $y \in \mathrm{C}_G(x)$ with $|y| = r$. Then $|xy| = p^a r$. Since $(p^a, r) = 1$, we can write $1 = up^a + vr$ for some $u, v \in \mathbb{Z}$. Assume that $xy \notin \Delta_H(G)$. Then $xy \in H^g$ for some $g \in G$. We have that $x^r = (xy)^r \in H^g$, so $x^{vr} \in H^g$ and thus $x = x^{up^a}x^{vr} = x^{vr} \in H^g$, which is a contradiction. Therefore $xy \in \Delta_H(G) = x^G$, but this is not possible since $|xy| = r|x| \neq |x|$. We conclude that $\mathrm{C}_G(x)$ is a p-group, as required. □

Remark 5.4. Let G be a finite group and let χ be a nonlinear irreducible character of G such that $\chi = \phi^G$ and $n(\chi) = 1$ for some $\phi \in \mathrm{Irr}(H)$ and proper subgroup $H < G$. Then $\Delta_H(G) = x^G$ for some $x \in G$ with $\chi(x) = 0$, and thus $\kappa_H(G) = 1$. However, the condition $\kappa_H(G) = 1$ for some subgroup H of G does *not* imply that G admits an irreducible character $\chi = \phi^G$ for some $\phi \in \mathrm{Irr}(H)$ with the property $n(\chi) = 1$. For example, Theorem 1 implies that $\kappa_H(G) = 1$ if $(G, H) = (A_5, D_{10})$, but no irreducible character of H can induce irreducibly to G.

We are now in a position to comlete the proof of Theorem 6, on the normal structure of finite groups G with an induced irreducible character χ such that $n(\chi) = 1$. In order to state the result, let us recall that if N is a proper nontrivial normal subgroup of G

then (G,N) is a *Camina pair* if and only if $|\mathrm{C}_G(g)| = |\mathrm{C}_{G/N}(Ng)|$ for all $g \in G \setminus N$. In addition, G is a *Camina group* if (G,G') is a Camina pair.

Remark 5.5. As noted in Remark 7(b), Theorem 5.6 below can be viewed as a generalisation of [16, Theorem 9] and [44, Theorem 1.1], which give partial structural information in the case where G is soluble. More precisely, [16, Theorem 9(e)] states that if G is a finite soluble group with an imprimitive irreducible character χ such that $n(\chi) = 1$, then G has a normal subgroup L such that G/L is a 2-transitive Frobenius group of prime power degree. Similarly, assuming G is soluble, parts (2) and (3) in [44, Theorem 1.1] correspond to parts (i)(a,b) in Theorem 5.6 (note that the conclusion in part (1) of [44, Theorem 1.1] coincides with part (i) in Lemma 5.1).

Theorem 5.6. *Let H be a maximal subgroup of a finite group G and assume that $\Delta_H(G) = x^G$ for some $x \in G$. Let $N = H_G$, $M = \langle x^G \rangle$ and assume that H is not normal in G. Then one of the following holds:*

(i) *G/N is a 2-transitive Frobenius group with an elementary abelian kernel M/N of order p^n for some prime p, and a complement H/N of order $p^n - 1$. Moreover, $x^G = M \setminus N$, $|\mathrm{C}_G(x)| = p^n$, $|x^G| = |H|$, $M' = N$ and one of the following holds:*
   - (a) *M is a Frobenius group with kernel M' and $p^n = p > 2$.*
   - (b) *M is a Frobenius group with kernel $K \trianglelefteqslant G$ such that $G/K \cong \mathrm{SL}_2(3)$ and $M/K \cong Q_8$.*
   - (c) *M is a Camina p-group.*

(ii) *$G/N \cong \mathrm{L}_2(8){:}3$, $H/N \cong D_{18}{:}3$, N is a nilpotent $7'$-group and $\mathrm{C}_G(x) = \langle x \rangle \cong \mathbb{Z}_7$.*

(iii) *$G/N \cong A_5$, $H/N \cong D_{10}$, N is a 2-group and $\mathrm{C}_G(x) = \langle x \rangle \cong \mathbb{Z}_3$.*

In particular, if $G = G'$ then either case (i)(c) *holds with $p^n = 11^2$ and $G/N \cong 11^2{:}\mathrm{SL}_2(5)$, or case* (iii) *holds.*

Proof. As previously noted, G/N is a primitive permutation group on the set Ω of right cosets of H/N in G/N, with point stabiliser H/N. Clearly, G/N has only one class of derangements on Ω. By Theorem 1, we deduce that one of the following holds:

- G/N is a Frobenius group with an elementary abelian kernel M/N of order p^n for some prime p, and a complement H/N of order $p^n - 1$;
- $G/N \cong \mathrm{L}_2(8){:}3$ and $H/N \cong D_{18}{:}3$;
- $G/N \cong A_5$ and $H/N \cong D_{10}$.

Moreover, $x^r \in N$ with $r = p, 7$ or 3, respectively.

By Lemma 5.2, $|\Delta_H(G)| = |x^G| = |G : \mathrm{C}_G(x)| \geqslant |H|$ and thus $|\mathrm{C}_G(x)| \leqslant |G : H|$.

Suppose that $G/N \cong \mathrm{L}_2(8){:}3$. Then $|\mathrm{C}_G(x)| \leqslant |G : H| = 28$. By Lemma 5.3, we know that x is a 7-element and so $\mathrm{C}_G(x)$ is a 7-group. Since $\langle x \rangle \leqslant \mathrm{C}_G(x)$, we deduce that $\mathrm{C}_G(x) = \langle x \rangle$ with $|x| = 7$ and hence x acts fixed point freely on N. Thompson's Theorem [47, Theorem 4.22] now implies that N is a nilpotent $7'$-group.

Similarly, if $G/N \cong A_5$ then $|G : H| = 6$ and $\mathrm{C}_G(x) = \langle x \rangle \cong \mathbb{Z}_3$, so x acts fixed point freely on N. In this case, N must be a 2-group by the main theorem of [19].

Finally, let us assume that G/N is a Frobenius group with elementary abelian kernel M/N of order p^n. Then $G = HM$ with $H \cap M = N$ and $|H/N| = |M/N| - 1 = p^n - 1$. In terms of permutation characters, it follows that $(1_H^G)_M = 1_N^M$. As $N \trianglelefteqslant M$, 1_N^M vanishes on $M \setminus N$ and thus 1_H^G also vanishes on this set, which implies that $M \setminus N \subseteq x^G$. Furthermore, since $x^G \subseteq M$ and $x^G \cap N \subseteq x^G \cap H = \emptyset$, we have $x^G \subseteq M \setminus N$ and thus $x^G = M \setminus N$. Now

$$|x^G| = |G : \mathrm{C}_G(x)| = |M \setminus N| = |M| - |N| = |N|(|M : N| - 1) = |N| \cdot |H : N| = |H|$$

and

$$|\mathrm{C}_G(x)| = |G : H| = |M : N| = p^n.$$

Let $y \in M \setminus N = x^G$. Then $y = x^g$ for some $g \in G$ and so $|\mathrm{C}_G(y)| = |M : N| = |\mathrm{C}_{G/N}(Ny)|$ (the last equality holds as G/N is a Frobenius group with an elementary abelian kernel M/N of order p^n). Hence

$$|M : N| \leqslant |M : M'| \leqslant |\mathrm{C}_M(y)| \leqslant |\mathrm{C}_G(y)| = |M : N|.$$

So

$$|\mathrm{C}_{M/M'}(yM')| = |M : M'| = |M : N| = |\mathrm{C}_G(y)| = |\mathrm{C}_M(y)|.$$

Thus M is a Camina group. Using the classification of Camina groups (see, for example, [40]), one of the following cases holds:

(a) M is a Frobenius group with kernel $M' = N$. Since M/M' is elementary abelian, we deduce that M/M' is cyclic and thus $p^n = p$, which implies that $|H/N| = p-1$ and so G/N is a Frobenius group of order $p(p-1)$.

(b) M is a Frobenius group with complement Q_8, and $p = 2$. In this case, $|M : N| = |M : M'| = 4$ so $M/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and thus $H/N \cong \mathbb{Z}_3$. Let K be the kernel of M. Then $K \trianglelefteqslant G$ and $G/K \cong Q_8{:}3 \cong \mathrm{SL}_2(3)$.

(c) M is a p-group.

Finally, to complete the proof of the theorem, assume that $G = G'$. Then either case (i)(c) or (iii) holds. Suppose that case (i)(c) holds. Then G/N is a Frobenius group with a perfect Frobenius complement H/N. By [35, Theorem A], we have $H/N \cong \mathrm{SL}_2(5)$. In particular, since $|H/N| = 120 = p^n - 1$, we deduce that $p^n = 121 = 11^2$. □

In view of Remark 5.4, by combining Lemma 5.1 and Theorem 5.6, the proof of Theorem 6 is now complete.

References

[1] L. Babai, P.P. Pálfy and J. Saxl, *On the number of p-regular elements in finite simple groups*, LMS J. Comput. Math. **12** (2009), 82–119.

[2] Á. Bereczky, *Maximal overgroups of Singer elements in classical groups*, J. Algebra **234** (2000), 187–206.

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

[4] N. Boston, W. Dabrowski, T. Foguel, P.J. Gies, D.A. Jackson, J. Leavitt and D.T. Ose, *The proportion of fixed-point-free elements of a transitive permutation group*, Comm. Algebra **21** (1993), 3259–3275.

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

[6] T. Breuer, R.M. Guralnick and W.M. Kantor, *Probabilistic generation of finite simple groups,* II, J. Algebra **320** (2008), 443–494.

[7] A.A. Buturlakin and M.A. Grechkoseeva, *The cyclic structure of maximal tori in finite classical groups*, Algebra Logika **46** (2007), 129–156.

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

[9] P. J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts, vol. 45 (Cambridge University Press, 1999).

[10] P.J. Cameron and A.M. Cohen, *On the number of fixed point free elements in a permutation group*, Discrete Math. **106/107** (1992), 135–138.

[11] D. Chillag, *On zeroes of characters of finite groups*, Proc. Amer. Math. Soc. **127** (1999), 977–983.

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

[13] B. N. Cooperstein, *Maximal subgroups of* $G_2(2^n)$, J. Algebra **70** (1981), 23–36.

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

[15] J.D. Dixon and B. Mortimer, *Permutation Groups*, Springer-Verlag, New York, 1996.

[16] J.D. Dixon and A. Rahnamai Barghi, *Irreducible characters which are zero on only one conjugacy class,* Proc. Amer. Math. Soc. **135** (2007), 41–45.

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

[18] P. Fleischmann and I. Janiszczak, *The semisimple conjugacy classes of finite groups of Lie type E_6 and E_7*, Comm. Alg. **21** (1993), 93–161.

[19] W. Feit and J.G. Thompson, *Finite groups which contain a self-centralizing subgroup of order* 3, Nagoya Math. J. **21** (1962), 185–197.

[20] P. Flavell, *Generating finite groups with maximal subgroups of maximal subgroups*, J. Algebra **177** (1995), 372–384.

[21] D.A. Foulser, *The flag-transitive collineation groups of the finite Desarguesian affine planes*, Canad. J. Math. **16** (1964), 443–472.

[22] J. Fulman and R.M. Guralnick, *Derangements in simple and primitive groups*, in Groups, Combinatorics and Geometry (Durham, 2001), 99–121, World Sci. Publ., 2003.

[23] J. Fulman and R.M. Guralnick, *Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements*, Trans. Amer. Math. Soc. **364** (2012), 3023–3070.

[24] J. Fulman and R.M. Guralnick, *Derangements in subspace actions of finite classical groups*, preprint (arXiv:1303.5480)

[25] J. Fulman and R.M. Guralnick, *Derangements in finite classical groups for actions related to extension field and imprimitive subgroups*, in preparation

[26] P.X. Gallagher, *Zeros of characters of finite groups,* J. Algebra **4** (1966), 42–45.

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

[28] R.M. Guralnick and W.M. Kantor, *Probabilistic generation of finite simple groups*, J. Algebra **234** (2000), 743–792.

[29] R. Guralnick, T. Pentilla, C.E. Praeger, and J. Saxl, *Linear groups with orders having certain large prime divisors*, Proc. London Math. Soc. **78** (1999), 167–214.

[30] R.M. Guralnick and D. Wan, *Bounds for fixed point free elements in a transitive group and applications to curves over finite fields*, Israel J. Math. **101** (1997), 255–287.

[31] C. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order*, Geom. Dedicata **2** (1974), 425–460.

[32] C. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order,* II, J. Algebra **93** (1985), 151–164.

[33] I.M. Isaacs, *Character Theory of Finite Groups*, AMS Chelsea Publishing, 2006.

[34] I.M. Isaacs, T.M. Keller, M.L. Lewis, A. Moretó, *Transitive permutation groups in which all derangements are involutions*, J. Pure Appl. Algebra **207** (2006), 717–724.

[35] U. Meierfrankenfeld, *Perfect Frobenius complements,* Arch. Math. (Basel) **79** (2002), 19–26.

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

[37] C. Jordan, *Recherches sur les substitutions*, J. Math. Pures Appl. (Liouville) **17**, 351–387.

[38] C. Jordan, *Sur la limite de transitivité des groupes non alternés*, Bull. Soc. Math. France **1** (1872/73), 40–71.

[39] 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.

[40] M.L. Lewis, *Classifying Camina groups: a theorem of Dark and Scoppola*, Rocky Mountain J. Math., to appear.

[41] M.W. Liebeck, *The affine permutation groups of rank* 3, Proc. London Math. Soc. **54** (1987), 477–516.

[42] G. Malle, G. Navarro, J.B. Olsson, *Zeros of characters of finite groups*, J. Group Theory **3** (2000), 353–368.

[43] S.P. Norton and R.A. Wilson, *The maximal subgroups of $F_4(2)$ and its automorphism group*, Comm. Algebra **17** (1989), 2809–2824.

[44] G. Qian, *Finite solvable groups with an irreducible character vanishing on just one class of elements,* Comm. Algebra **35** (2007), 2235–2240.

[45] S. Ramanujan, *A proof of Bertrand's Postulate*, J. Indian Math. Soc. **11** (1919), 181–182.

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

[47] M. Suzuki, *Group theory.* II. Translated from the Japanese. Grundlehren der Mathematischen Wissenschaften **248**, Springer-Verlag, New York, 1986.

[48] J. Thévenaz, *Maximal subgroups of direct products*, J. Algebra **198** (1997), 352–361.

[49] T.S. Weigel, *Generation of exceptional groups of Lie-type*, Geom. Dedicata **41** (1992), 63–87.

[50] R.A. Wilson et al., *A World-Wide-Web Atlas of finite group representations*, `http://brauer.maths.qmul.ac.uk/Atlas/v3/`.

[51] E.M. Zhmud', *Finite groups having an irreducible complex character with a class of zeros*, Soviet Math. Dokl. **20** (1979), 795–797.

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

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

E-mail address: ptongviet@math.uni-bielefeld.de

H.P. Tong-Viet, Fakultät für Mathematik, Universität Bielefeld, D-33501 Bielefeld, Germany