CAMBRIDGE
UNIVERSITY PRESS

RESEARCH ARTICLE

On derangements in simple permutation groups

Timothy Burness[1] and Marco Fusari[2]

[1]School of Mathematics, University of Bristol, Bristol BS8 1UG, UK; E-mail: t.burness@bristol.ac.uk (corresponding author).
[2]Dipartimento di Matematica "Felice Casorati", University of Pavia, Via Ferrata 5, 27100 Pavia, Italy;
E-mail: lucamarcofusari@gmail.com.

Dedicated to Martin Liebeck on the occasion of his 70th birthday

Abstract

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite transitive permutation group and recall that an element in G is a derangement if it has no fixed points on Ω. Let $\Delta(G)$ be the set of derangements in G and define $\delta(G) = |\Delta(G)|/|G|$ and $\Delta(G)^2 = \{xy : x, y \in \Delta(G)\}$. In recent years, there has been a focus on studying derangements in simple groups, leading to several remarkable results. For example, by combining a theorem of Fulman and Guralnick with recent work by Larsen, Shalev and Tiep, it follows that $\delta(G) \geqslant 0.016$ and $G = \Delta(G)^2$ for all sufficiently large simple transitive groups G. In this paper, we extend these results in several directions. For example, we prove that $\delta(G) \geqslant 89/325$ and $G = \Delta(G)^2$ for all finite simple primitive groups with soluble point stabilisers, without any order assumptions, and we show that the given lower bound on $\delta(G)$ is best possible. We also prove that every finite simple transitive group can be generated by two conjugate derangements, and we present several new results on derangements in arbitrary primitive permutation groups.

Contents

1. Introduction

Let G be a finite transitive permutation group on a set Ω with $|\Omega| \geqslant 2$ and point stabiliser $H = G_\alpha$. Recall that an element of G is a *derangement* if it has no fixed points on Ω. We write $\Delta(G)$ for the set of derangements in G (sometimes we will use $\Delta(G, \Omega)$ or $\Delta(G, H)$ if we need to specify Ω or H). By a classical theorem of Jordan [56], published in 1872, we know that $\Delta(G)$ is nonempty. This elementary observation leads naturally to a wide range of problems and applications that have been intensively studied in recent years (for instance, see Serre's article [75] for interesting applications in number theory and topology).

In one direction, there is an extensive literature concerning the existence of derangements with specified properties. A well-known theorem of Fein, Kantor and Schacher [33], which relies on the Classification of Finite Simple Groups (CFSG), shows that every group G as above contains a derangement of prime power order, which in turn has important number-theoretic applications concerning the structure of Brauer groups of global field extensions (see [33]). However, transitive groups with no derangements of prime order do exist. For example, the smallest Mathieu group M_{11}, viewed as a primitive permutation group of degree 12, does not contain a prime order derangement. These so-called *elusive groups* have been the subject of numerous papers, and they are closely related to some interesting open problems, such as the *Polycirculant Conjecture* in algebraic graph theory (see the survey article [1] and [18, Section 1.3] for further details).

In a different direction, it is natural to consider the proportion of derangements in G,

$$\delta(G) = \delta(G, \Omega) = \delta(G, H) = \frac{|\Delta(G)|}{|G|},$$

which one can view as the probability that a uniformly random element in G has no fixed points. This has been widely studied since the 1990s, and there has been a special interest in determining lower bounds. For example, a theorem of Cameron and Cohen [22] shows that $\delta(G) \geqslant |\Omega|^{-1}$, with equality if and only if G is sharply 2-transitive. And by applying CFSG, the groups with $\delta(G) < 2|\Omega|^{-1}$ have been determined by Guralnick and Wan [51], motivated by applications to curves over finite fields in arithmetic geometry. The latter two results have been generalised in a recent preprint of Garzoni [42], where the main theorem states that if G is primitive and $|\Omega|$ is sufficiently large, then either G is a Frobenius group or

$$\delta(G) \geqslant \frac{|\Omega|^{\frac{1}{2}} + 1}{2|\Omega|}.$$

This lower bound is best possible, and it settles a conjecture of Guralnick and Tiep [50, p.272] on primitive affine groups.

Perhaps the most striking result on the proportion of derangements is the following deep theorem of Fulman and Guralnick, which establishes a conjecture of Boston and Shalev from the 1990s (see [9]). The proof is presented in the sequence of papers [36, 37, 38, 39].

Theorem 1.1 (Fulman & Guralnick). *There is an absolute constant $\epsilon > 0$ such that $\delta(G) \geqslant \epsilon$ for every finite simple transitive permutation group G.*

The constant ϵ is undetermined, although [39, Theorem 1.1] states that one can take $\epsilon = 0.016$ for all sufficiently large simple groups.

Since $\Delta(G)$ is a normal subset, it is also natural to consider the analogous problem for conjugacy classes. Here recent work of Eberhard and Garzoni [31] shows that the proportion of conjugacy classes consisting of derangements in simple transitive groups of Lie type is also bounded away from zero (it is easy to see that the conclusion is false for alternating groups). It is interesting to note that the latter result extends to almost simple groups of Lie type, whereas examples can be constructed to show that $\delta(G)$ can be arbitrarily small in the almost simple setting (we will return to this below).

In order to state our first result, it will be convenient to define

$$\alpha(G) = \min\{\delta(G, H) \; : \; H < G \text{ core-free}\},$$

where we recall that a subgroup H of G is *core-free* if $\bigcap_{g \in G} H^g = 1$ (equivalently, the natural transitive action of G on G/H is faithful). Then Theorem 1.1 implies that there is an absolute (and undetermined) constant $\epsilon > 0$ such that $\alpha(G) \geqslant \epsilon$ for every simple group G. In Theorem A below, we show that $\epsilon = 1/e$ is asymptotically the best possible constant for alternating groups, and we determine the optimal constant for every sporadic group. Note that Table 1 is presented in Section 2.2. Throughout

this paper, whenever we use the term 'simple group', we implicitly assume the group is non-abelian (and we adopt the notation for simple groups used in [57]).

Theorem A. *Let G be a simple alternating or sporadic group.*

(i) *If $G = A_n$, then $\alpha(G) \to 1/e$ as $n \to \infty$.*
(ii) *If G is a sporadic group, then $\alpha(G)$ is recorded in Table 1. In particular, we have*

$$\alpha(G) \geqslant \frac{2197}{7425},$$

with equality if and only if G is the McLaughlin group McL.

Remark 1.2. Let us record some comments on the statement of Theorem A.

(a) To prove part (i), we will show that

$$\alpha(A_n) = \sum_{j=2}^{n} \frac{(-1)^j}{j!} - \frac{(-1)^n (n-1)}{n!} = \frac{[n!/e]}{n!} - \frac{(-1)^n (n-1)}{n!}$$

for all sufficiently large n, where $[x]$ denotes the nearest integer to x. Here the key step is to show that if we take the natural action of $G = A_n$ on the set of k-element subsets of $\{1, \ldots, n\}$, then $\delta(G)$ is minimal when $k = 1$ or $n - 1$ (see Proposition 2.2).
(b) We conjecture that the formula for $\alpha(A_n)$ in (a) holds for all $n \geqslant 9$, which would imply that $\varepsilon = 13/45$ is the optimal constant in Theorem 1.1 as we range over all simple alternating groups (see Conjecture 2.6).
(c) The proof for sporadic groups relies on computational methods, working closely with the information on character tables and fusion maps available in the GAP Character Table Library [12].

Our next result gives an effective and best possible version of Theorem 1.1 for simple primitive groups with soluble point stabilisers. Here the possibilities for G and H have been determined by Li and Zhang [62] (see [62, Tables 14-20]). For example, if $G = A_n$ is an alternating group and $n \geqslant 17$, then $n = p$ is a prime and $H = \mathrm{AGL}_1(p) \cap G$ is the only possibility (up to conjugacy in G).

Theorem B. *Let G be a finite simple primitive permutation group with soluble point stabiliser H. Then*

$$\delta(G) \geqslant \frac{89}{325},$$

with equality if and only if $G = {}^2F_4(2)'$ and $H = 2^2.[2^8].S_3$.

Remark 1.3. Some comments on the statement of Theorem B are in order:

(a) For sporadic groups, the given lower bound is valid for all transitive actions with soluble point stabilisers. In fact, we prove that $\delta(G) \geqslant 21/55$, with equality if and only if $G = \mathrm{M}_{11}$ and $H = \mathrm{U}_3(2).2$ or $2.S_4$ (see Proposition 4.3).
(b) In order to establish Theorem C below, we require a slightly more general version of Theorem B. So we will actually prove that $\delta(G) \geqslant 89/325$ for every finite simple transitive group G with soluble point stabiliser H, where $H = G \cap M$ for some maximal subgroup M of an almost simple group with socle G.
(c) We conjecture that $\varepsilon = 89/325$ is the optimal constant for all transitive groups with soluble point stabilisers. In fact, we speculate that this is the best possible constant in Theorem 1.1, without any additional assumptions.

As noted above, Theorem 1.1 does not extend to almost simple groups. For example, as explained in [36, Section 6], if we take $G = \mathrm{Aut}(\mathrm{L}_2(p^r)) = \mathrm{PGL}_2(p^r){:}\langle\varphi\rangle$ and $\Omega = \varphi^G$, where p and r are primes

with $(r, p(p^2 - 1)) = 1$ and φ is a field automorphism of order r, then every element in $G \setminus \mathrm{PGL}_2(p^r)$ has a fixed point, and thus

$$\delta(G) \leqslant \frac{|\mathrm{PGL}_2(p^r)|}{|G|} = \frac{1}{r}$$

can be arbitrarily small.

In this example, notice that $\delta(G) < 3/\log n$ if $p = 2$ and $r \geqslant 5$, where $n = |\Omega|$ is the degree of G and log is the natural logarithm. This shows that [36, Theorem 1.5] is essentially best possible since it states that there exists an absolute constant $\gamma > 0$ such that $\delta(G) \geqslant \gamma/\log n$ for all almost simple primitive permutation groups G of degree n (moreover, this extends to all non-affine primitive groups). Here we use Theorem 1.1 to establish another natural extension to primitive permutation groups (recall that the *socle* of G is the product of its minimal normal subgroups).

Theorem C. *Let G be a finite primitive group with socle N and point stabiliser H. Then the following hold:*

(i) $\delta(N) \geqslant \varepsilon$, *where ε is the constant in Theorem 1.1.*
(ii) *If H is soluble, then $\delta(N) \geqslant 89/325$, with equality if and only if $N = {}^2F_4(2)'$ and $H \cap N = 2^2.[2^8].S_3$.*

Further motivation for studying derangements for simple groups stems from a theorem of Larsen, Shalev and Tiep [58]. In order to set the scene, let G be a finite transitive permutation group and recall that $\Delta(G)$ is a normal subset of G. We define the *derangement width* of G, denoted $w(G)$, to be the minimal positive integer k such that $G = \Delta(G)^k$, where

$$\Delta(G)^k = \{x_1 \cdots x_k \; : \; x_i \in \Delta(G) \text{ for all } i\},$$

setting $w(G) = \infty$ if $G \neq \Delta(G)^k$ for all k. Notice that if G is simple, then $G = \langle \Delta(G) \rangle$ and $w(G)$ is simply the diameter of the corresponding Cayley graph $\mathrm{Cay}(G, \Delta(G))$.

There is an extensive literature on so-called *width problems* for finite groups, and for finite simple groups and normal subsets in particular (we refer the reader to Liebeck's excellent survey article [63]). One of the main open problems in this area is a conjecture from the 1980s attributed to John Thompson, which asserts that every finite simple group G has a conjugacy class C such that $G = C^2$. This has turned out to be a very difficult problem, but there has been significant progress in recent years. For instance, through the work of several authors, the problem has been reduced to groups of Lie type defined over fields with at most 8 elements. It is also worth noting that Thompson's conjecture immediately implies a famous conjecture of Ore from 1951, which asserts that every element in a finite simple group is a commutator. The proof of the latter was completed by Liebeck et al. in [64] using character-theoretic methods.

It is therefore natural to study the derangement width of finite simple groups, and the main result here is the following theorem from [58].

Theorem 1.4 (Larsen, Shalev & Tiep). *Let G be a finite simple transitive group.*

(i) *If $|G|$ is sufficiently large, then $G = \Delta(G)^2$.*
(ii) *If $G = A_n$, then $G = \Delta(G)^2$ for all n.*

It is conjectured in [58] that the condition on $|G|$ in part (i) is not needed.

Conjecture 1.5 (Larsen, Shalev & Tiep). *We have $G = \Delta(G)^2$ for every finite simple transitive group G.*

It seems difficult to approach this conjecture for groups of Lie type with the character-theoretic methods adopted in [58], so we focus on some special cases of interest in Theorems D and E below. Note that $\Delta(G)$ is inverse-closed, so $\Delta(G)^2$ always contains the identity element. In part (i) of the next result, recall that the rank one groups of Lie type are the following:

$$L_2(q), \; q \geqslant 4; \quad U_3(q), \; q \geqslant 3; \quad {}^2B_2(q), \; q \geqslant 8; \quad {}^2G_2(q)', \; q \geqslant 3 \tag{1.1}$$

Theorem D. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite simple transitive group with point stabiliser H.*

(i) *If G is an alternating group, a sporadic group, or a rank one group of Lie type, then there exist conjugacy classes C, D of derangements such that*

$$G = \begin{cases} C^2 \cup CD & \text{if } G = \mathrm{L}_2(7) \text{ and } H = S_4 \\ \{1\} \cup CD & \text{otherwise.} \end{cases} \tag{1.2}$$

(ii) *If G is primitive and H is soluble, then $G = \Delta(G)^2$.*

Remark 1.6. Let us record some comments on Theorem D.

(a) It is easy to show that $G = \Delta(G)^2$ if $\delta(G) > 1/2$ (see Lemma 3.22), so there is a natural connection between Theorem B and part (ii) of Theorem D. This observation will be useful in several places (for example, see the proofs of Theorems E and F in Sections 3.4 and 3.5, respectively, and also the proof of Proposition 4.13(ii) in Section 4.4).

(b) For groups of Lie type, we rely heavily on earlier work of Guralnick and Malle [47, 48], where character-theoretic methods are used to show that $G = \{1\} \cup CD$ for certain conjugacy classes C and D. For example, in proving part (ii) for exceptional groups, we show that there exist classes C, D of derangements with $G = \{1\} \cup CD$.

(c) In part (i), if $G = A_n$ and $n \geqslant 9$, then we combine work of Bertram [6], Brenner [11] and Larsen and Tiep [59] to prove that either $G = C^2$ for some conjugacy class C of derangements, or $n \equiv 3$ (mod 4) and $\Omega = \{1, \ldots, n\}$ is the natural permutation domain. In the latter case, [59, Theorem 1] gives $G = \{1\} \cup D^2$ where D is a class of n-cycles, and we conjecture that $G = C^2$ for the class C of elements with cycle-type $(n - 4, 2^2)$. The latter assertion has been checked computationally for $n \leqslant 23$.

(d) If G is a sporadic group, then we use a computational approach to show that $G = CD$ for conjugacy classes C, D of derangements. Moreover, we can take $C = D$ unless (G, H) is one of the cases in Table 2 (see Section 3.1), and in the latter cases, it is easy to check that $G = \{1\} \cup C^2$, where C is the conjugacy class recorded in the third column of the table.

(e) Suppose $G = \mathrm{L}_2(7)$ and H is a maximal subgroup isomorphic to S_4 (there are two conjugacy classes of such subgroups). Then $\Delta(G) = C \cup D$, where C and D are the two conjugacy classes of elements of order 7, and one can check that

$$C^2 = D^2 = \{x \in G \; : \; |x| \neq 1, 4\}, \quad CD = \{x \in G \; : \; |x| \neq 2\},$$

which means that $G \neq \{1\} \cup C^2$, $G \neq \{1\} \cup CD$ and $G = C^2 \cup CD$. In addition, if we consider the action of G on G/K for any proper subgroup K of H, then it is easy to show that $G = E^2$ for some conjugacy class E of derangements.

(f) The property $G = \Delta(G)^2$ also extends to some almost simple groups. For instance, in Theorem 3.8, we generalise [58, Theorem B] by showing that $G = \Delta(G)^2$ for every faithful transitive action of $G = S_n$ with $n \geqslant 4$. However, it is worth noting that there exist almost simple primitive groups with infinite derangement width, even under the assumption that the point stabilisers are soluble. For example, if we take $G = \mathrm{Aut}(\mathrm{L}_2(3^r)) = \mathrm{PGL}_2(3^r){:}\langle \varphi \rangle$ and $\Omega = \varphi^G$, where $r \geqslant 5$ is a prime, then $H = \mathrm{PGL}_2(3) \times \langle \varphi \rangle$ is soluble and every derangement in G is contained in $\mathrm{PGL}_2(3^r)$. In particular, we have $\Delta(G)^k \subseteq \mathrm{PGL}_2(3^r) < G$ for every positive integer k.

It is easy to show that there are infinitely many simple transitive groups G such that $G \neq \{1\} \cup C^2$ for every conjugacy class C of derangements. For example, if $G = \mathrm{L}_2(q)$, q is even and H is a Borel subgroup, then

$$\Delta(G) = \{x \in G \; : \; x \neq 1, \; |x| \text{ divides } q + 1\} = \bigcup_{i=1}^{k} x_i^G,$$

and one can check that $(x_i^G)^2 = \{x \in G : |x| \neq 2\}$ for all i (see [41, Theorem 2(ii)]). However, in this case, we can show that $G = \{1\} \cup (x_1^G)(x_2^G)$. And as far as we are aware, the special case $(G, H) = (L_2(7), S_4)$ is the only one with $G \neq \{1\} \cup CD$ for all classes C, D of derangements. This leads us to propose the following stronger form of Conjecture 1.5.

Conjecture 1.7. *Let G be a finite simple transitive group with point stabiliser H. Then there exist conjugacy classes C and D of derangements such that (1.2) holds.*

In addition to the groups recorded in part (i) of Theorem D, our proof of Theorem D(ii) shows that Conjecture 1.7 also holds for every non-classical simple primitive group with soluble point stabilisers (see Remark 1.6).

By combining a result of Malle, Saxl and Weigel [71, Theorem 2.1] with the main theorems of Lev [61] and Guralnick et al. [49], we can prove a special case of Conjecture 1.5 for linear groups of arbitrary rank. In the statement, P_k denotes the stabiliser in G of a k-dimensional subspace of the natural module.

Theorem E. *Let $G = L_n(q)$ be a finite simple transitive group with point stabiliser H.*

 (i) *If $n = 3$ and $q \geqslant 3$, then $G = \{1\} \cup C^2$ for some conjugacy class C of derangements.*
(ii) *If $n \geqslant 4$ and $H \not\leqslant P_1, P_{n-1}$, then $G = \Delta(G)^2$.*

Remark 1.8. Some comments on the statement of Theorem E:

(a) As recorded in Theorem D(i), if $G = L_3(2) \cong L_2(7)$, then there exist classes C, D of derangements such that

$$G = \begin{cases} C^2 \cup CD & \text{if } H = P_1 \text{ or } P_2 \\ \{1\} \cup CD & \text{otherwise.} \end{cases}$$

(b) In part (ii), we work with a slightly stronger form of [58, Theorem 2.4(i)] to show that either $G = \{1\} \cup CD$ for classes C, D of derangements (in agreement with Conjecture 1.7), or $q = 2$, $H = Sp_n(2)$ and $n \leqslant 28$.
(c) We refer the reader to Remark 3.17 for comments on the special case excluded in (ii), where $n \geqslant 4$ and H is contained in a P_1 or P_{n-1} parabolic subgroup.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with socle N and, as before, let $\Delta(N)$ be the set of derangements contained in N. If G is almost simple, then N is simple and transitive, so Conjecture 1.5 asserts that $N = \Delta(N)^2$. If we assume the veracity of this conjecture, then we can use the O'Nan-Scott theorem to establish the following generalisation.

Theorem F. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with socle N and $|\Omega| \geqslant 3$. If Conjecture 1.5 holds, then $N = \Delta(N)^2$.*

Our final result concerns the generation properties of finite simple transitive groups. It is well known that every finite simple group is 2-generated (the proof requires CFSG), and there is a vast literature on the properties and distribution of generating pairs. For example, a theorem of Guralnick and Kantor [45] states that every finite simple group G has a conjugacy class C with the property that for all nontrivial $x \in G$, there exists an element $y \in C$ such that $G = \langle x, y \rangle$ (in this situation, we call C a *witness*). The proof of this theorem uses probabilistic methods, based on fixed point ratio estimates. Using similar methods, we prove that every finite simple transitive permutation group is generated by two derangements. Moreover, we can always find a generating pair of conjugate derangements.

Theorem G. *Let G be a finite simple transitive group. Then there exist conjugate derangements $x, y \in G$ such that $G = \langle x, y \rangle$.*

Let G be a finite simple group and suppose that $C = x^G$ and $D = y^G$ are witnesses, as defined above. It is easy to see that the conclusion in Theorem G follows if no maximal overgroup of x is conjugate to a maximal overgroup of y. Indeed, if this property holds, then either x or y is a derangement, and the

result follows since $G = \langle x, x^a \rangle = \langle y, y^b \rangle$ for some $a, b \in G$. So in the proof of Theorem G, we are often interested in identifying witnesses C and D with the property that the maximal overgroups of their respective representatives are severely restricted. Along the way, with this aim in mind, we prove that every conjugacy class of Singer cycles in a simple classical group is a witness (see Proposition 5.15), which may be of independent interest.

Notation. Our notation is standard. For a finite group G and positive integer n, we write C_n, or just n, for a cyclic group of order n and G^n for the direct product of n copies of G. An unspecified extension of G by a group H will be denoted by $G.H$; if the extension splits, then we may write $G{:}H$. We use $[n]$ for an unspecified soluble group of order n. Throughout the paper, we adopt the standard notation for simple groups of Lie type from [57] (so, for example, we write $L_n(q) = L_n^+(q)$ and $U_n(q) = L_n^-(q)$ for the groups $\mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$, respectively). In addition, for positive integers a and b, we use the familiar Kronecker delta symbol $\delta_{a,b}$ (so $\delta_{a,b} = 1$ if $a = b$, otherwise $\delta_{a,b} = 0$), and we write (a, b) for the highest common factor of a and b.

Organisation. Let us briefly outline the structure of the paper. We begin in Section 2 by studying the proportion of derangements in transitive actions of alternating and sporadic groups, culminating in a proof of Theorem A. We also establish part (i) of Theorem C, which gives a natural extension of Theorem 1.1 to primitive groups. In Section 3, we turn to the derangement width of simple transitive groups, proving part (i) of Theorem D. We also establish our main result on linear groups (Theorem E), and we present a short proof of Theorem F, which assumes the veracity of Conjecture 1.5. Next in Section 4, we focus on primitive simple groups with soluble point stabilisers, and our main goal is to prove Theorem B. Here we also complete the proofs of Theorems C and D. Finally, in Section 5, we study the 2-generation of simple groups, and we prove Theorem G.

2. Proportions

In this section, we prove Theorem A and part (i) of Theorem C. Recall that if $G \leqslant \mathrm{Sym}(\Omega)$ is a finite transitive permutation group with point stabiliser H, then $\Delta(G)$ denotes the set of derangements in G, and we write

$$\delta(G) = \delta(G, \Omega) = \delta(G, H) = \frac{|\Delta(G)|}{|G|}$$

for the proportion of derangements in G. For easy reference, we state the Fulman-Guralnick theorem, which is proved in the sequence of papers [36, 37, 38, 39].

Theorem 2.1. *There exists an absolute constant $\varepsilon > 0$ such that $\delta(G) \geqslant \varepsilon$ for every finite simple transitive group G.*

We begin by proving Theorem A, handling the alternating and sporadic groups in Sections 2.1 and 2.2, respectively. We will establish Theorem C(i) in Section 2.3.

2.1. Alternating groups

Let $G = A_n$ be an alternating group with $n \geqslant 5$ and recall that $\alpha(G)$ is defined to be the minimal value of $\delta(G, H)$ over all proper subgroups H of G. Here our goal is to prove that

$$\lim_{n \to \infty} \alpha(A_n) = \frac{1}{e}.$$

First observe that we only need to consider $\delta(G, H)$ when H is a maximal subgroup of G. In addition, by appealing to a well-known theorem of Łuczak and Pyber [70], we see that the proportion of elements in G that are contained in a proper transitive subgroup tends to 0 as n tends to infinity. As a consequence,

we may assume $H = (S_k \times S_{n-k}) \cap G$ for some $1 \leqslant k < n/2$, which allows us to identify $\Omega = G/H$ with the set of k-element subsets of $[n] = \{1, \ldots, n\}$. Let $f(n, k) = 1 - \delta(G)$ be the proportion of elements in G that fix a k-element subset of $[n]$.

An easy application of the inclusion-exclusion principle shows that the proportion of derangements in S_n with respect to the natural action on $[n]$ is given by the expression

$$\sum_{j=0}^{n} \frac{(-1)^j}{j!} = \frac{[n!/e]}{n!},$$

where $[x]$ denotes the nearest integer to x. As a consequence, we deduce that

$$f(n, 1) = 1 - \frac{[n!/e]}{n!} + \frac{(-1)^n (n-1)}{n!}$$

for all $n \geqslant 5$ (see [9, Corollary 2.6]). Clearly, $f(n, 1) \to 1 - 1/e$ as $n \to \infty$, so Theorem A(i) is a consequence of the following result.

Proposition 2.2. *We have $f(n, k) \leqslant f(n, 1)$ for all $1 \leqslant k < n/2$ and all $n \geqslant 5$.*

In order to prove Proposition 2.2, we need to introduce some additional notation. For integers $n \geqslant 5$ and $1 \leqslant k \leqslant n$, we define

$$a(n, k) = \frac{|A(n, k)|}{|A_n|}, \quad b(n, k) = \frac{|B(n, k)|}{|A_n|}, \quad c(n, k) = \max\{a(n, k), b(n, k)\},$$

where $A(n, k)$ (respectively, $B(n, k)$) is the set of even (respectively, odd) elements in S_n fixing a k-element subset of $[n]$. Note that $c(k, k) = 1$ and $c(n, k) = c(n, n-k)$. By arguing as in the proof of [29, Lemma 2(i)], it is straightforward to show that

$$c(n, k) \leqslant \frac{1}{n}\left(k + \sum_{j=k+1}^{n-k} c(n-j, k)\right). \tag{2.1}$$

Lemma 2.3. *We have $c(n, 1) \leqslant 2/3$ for all $n \geqslant 5$.*

Proof. First observe that

$$a(n, 1) = 1 - \delta(A_n), \quad b(n, 1) = 2(1 - \delta(S_n)) - a(n, 1)$$

with respect to the natural actions of A_n and S_n on $[n]$. By [9, Corollary 2.6], we have

$$\delta(A_n) = \delta(S_n) - \frac{(-1)^n (n-1)}{n!}, \quad \delta(S_n) = \frac{[n!/e]}{n!},$$

and it is easy to check that $c(n, 1) \leqslant 2/3$ for all $n \geqslant 5$. $\square$

Lemma 2.4. *We have $c(n, 2) \leqslant 0.63$ for all $n \geqslant 7$.*

Proof. First we compute $c(3, 2) = 1$, $c(4, 2) = 1/2$, $c(5, 2) = 3/5$, $c(6, 2) = 2/3$ and

$$c(7, 2) = \frac{38}{63}, \quad c(8, 2) = \frac{7}{12}, \quad c(9, 2) = \frac{3691}{6480}.$$

In addition, we check that $c(n, 2) \leqslant 0.63$ for $n = 10, 11, 12$. Now assume $n \geqslant 13$ and suppose we have $c(m, 2) \leqslant 0.63$ for all $7 \leqslant m \leqslant n-1$. Then (2.1) gives

$$c(n,2) \leqslant \frac{1}{n}\left(2 + \sum_{m=2}^{9} c(m,2) + \sum_{j=3}^{n-10} c(n-j,2)\right) \leqslant \frac{1}{n}\left(\frac{341233}{45360} + \frac{63}{100}(n-12)\right) < 0.63,$$

and the result follows. □

Lemma 2.5. *We have $c(n,k) \leqslant 0.63$ for all $3 \leqslant k < n/2$.*

Proof. First assume $k = 3$, so $n \geqslant 7$, and we compute

$$c(4,3) = \frac{3}{4}, \ c(5,3) = \frac{3}{5}, \ c(6,3) = \frac{3}{8}, \ c(7,3) = \frac{18}{35}, \ c(8,3) = \frac{25}{48}.$$

Suppose $n \geqslant 9$ and $c(m,3) \leqslant 0.63$ for all $5 \leqslant m \leqslant n-1$. Then by applying the upper bound in (2.1), we deduce that

$$c(n,3) \leqslant \frac{1}{n}\left(3 + 1 + \frac{3}{4} + \sum_{j=4}^{n-5} c(n-j,3)\right) \leqslant \frac{1}{n}\left(\frac{19}{4} + \frac{63}{100}(n-8)\right) < 0.63.$$

The case $k = 4$ is very similar.

Finally, let us assume $k \geqslant 5$. By Lemmas 2.3 and 2.4, we have $c(k+1,k) = c(k+1,1) \leqslant 2/3$ and $c(k+2,k) = c(k+2,2) \leqslant 0.63$. Let us assume $c(m,k) \leqslant 0.63$ for all $k+2 \leqslant m \leqslant n-1$. Then (2.1) gives

$$c(n,k) \leqslant \frac{1}{n}\left(k + 1 + \frac{2}{3} + \frac{63}{100}(n-2k-2)\right) = \frac{63}{100} - \frac{39k-61}{150n} < 0.63,$$

and the result follows. □

We are now in a position to prove Proposition 2.2. As explained above, this completes the proof of Theorem A(i).

Proof of Proposition 2.2. The cases $n \in \{5,6\}$ can be checked directly, so let us assume $n \geqslant 7$. Then Lemmas 2.4 and 2.5 imply that $f(n,k) \leqslant 0.63$ for all $2 \leqslant k < n/2$, while we have

$$f(n,1) = 1 - \frac{[n!/e]}{n!} + \frac{(-1)^n(n-1)}{n!} > 0.63.$$

The result follows. □

It seems difficult to prove a non-asymptotic version of Theorem A(i), but computations with the low degree alternating groups lead us to propose the following conjecture. In particular, this would imply that $13/45$ is the optimal constant for alternating groups in Theorem 2.1.

Conjecture 2.6. *Let $G = A_n$ be a finite simple transitive group with point stabiliser H.*

(i) *We have $\delta(G) \geqslant 13/45$, with equality if and only if $G = A_8$ and $H = \mathrm{AGL}_3(2)$.*
(ii) *If $n \geqslant 9$, then*

$$\delta(G) \geqslant \frac{[n!/e]}{n!} - \frac{(-1)^n(n-1)}{n!},$$

with equality if and only if $H = A_{n-1}$.

Table 1. *The values of $\alpha(G)$ for sporadic simple groups.*

G	H	$\alpha(G)$	
M_{11}	M_{10}	23/66	0.348
M_{12}	M_{11}	107/288	0.371
M_{22}	A_7	119/352	0.338
M_{23}	M_{22}	877/2415	0.363
M_{24}	M_{23}	1699/4608	0.368
J_1	$D_6 \times D_{10}$	573/1463	0.391
J_2	$3.A_6.2$	979/2100	0.466
J_3	$(3 \times A_6).2$	971/2907	0.334
McL	$2.A_8$	2197/7425	0.295
HS	$U_3(5).2$	13301/42240	0.314
He	$2^2.L_3(4).S_3$	23423/46648	0.502
Ru	$2^{1+4+6}.S_5$	26967/65975	0.408
Co_3	McL.2	47621/149040	0.319
Co_2	$2^{1+8}{:}Sp_6(2)$	350303/759000	0.461
Fi_{22}	$\Omega_7(3)$	934573/2365440	0.395
Fi_{23}	$P\Omega_8^+(3).S_3$	4624523/11561088	0.400
Suz	$G_2(4)$	6579421/13471920	0.488
O'N	$4.L_3(4).2$	5402647/14286195	0.378
HN	$2^{1+8}.(A_5 \times A_5).2$	13680272/24688125	0.554
Th	$2^{1+8}.A_9$	13838827/39073671	0.354
Ly	$2.A_{11}$	23715556/63400425	0.374
Co_1	$2^{1+8}.\Omega_8^+(2)$	7948916279/15664849200	0.507
J_4	$2^{3+12}.(S_5 \times L_3(2))$	20243299027/43786049417	0.462
Fi_{24}'	Fi_{23}	765137684779/1654006894848	0.462
$\mathbb{B}$	$2.{}^2E_6(2).2$	94738750847635861/167684218416000000	0.564
$\mathbb{M}$	$2^{1+24}.Co_1$	2670777082333978380 1504/49722462258718251877875	0.537

2.2. Sporadic groups

Next we use a computational approach to study the proportion of derangements for transitive actions of sporadic groups, working with GAP (version 4.13.0) and Magma (version V2.28-8).

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite simple transitive sporadic group with point stabiliser H and let $\chi = 1_H^G$ be the corresponding permutation character, so we have

$$\Delta(G) = \{x \in G : \chi(x) = 0\} = \{x \in G : x^G \cap H \text{ is empty}\}.$$

We can compute $\delta(G)$ if we know the sizes of the conjugacy classes in G, together with the *fusion map* from H-classes to G-classes. The latter map describes the embedding of each H-class in G, and so we can use it to read off the conjugacy classes of derangements in G. As explained in the proof of Proposition 2.7 below, in almost all cases, the relevant information we need concerning conjugacy classes can be accessed via the GAP Character Table Library [12], and this allows us to compute $\delta(G)$ (and subsequently $\alpha(G)$) in a few seconds.

The following result completes the proof of Theorem A (note that in the final column of Table 1, we give $\alpha(G)$ to 3 significant figures).

Proposition 2.7. *Let G be a finite simple transitive sporadic group with point stabiliser H.*

(i) *We have $\delta(G) \geqslant \alpha(G)$, where $\alpha(G)$ is recorded in Table 1. In addition, $\delta(G) = \alpha(G)$ if and only if H is conjugate to the maximal subgroup of G listed in the second column of the table.*

(ii) *We have $\delta(G) \geqslant 2197/7425$, with equality if and only if $G = \mathrm{McL}$ and $H = 2.A_8$.*

Proof. Part (ii) follows immediately from the information in Table 1, so we just need to consider part (i). As before, we may assume G is primitive, which means that H is a maximal subgroup of G.

To begin with, let us assume G is not the Monster group $\mathbb{M}$. Then in each case, the character tables of G and H are available in the GAP Character Table Library [12]. In addition, the corresponding fusion map from H-classes to G-classes is also available, with the single exception of the case where $G = \mathbb{B}$

is the Baby Monster and $H = (2^2 \times F_4(2)){:}2$. Putting the latter case to one side for now, we can use the fusion map to determine the G-classes comprising $\Delta(G)$, which in turn allows us to compute $\delta(G)$ precisely. We can then read off the minimum over all maximal subgroups, which gives the value of $\alpha(G)$ recorded in Table 1.

Now assume $G = \mathbb{B}$ and $H = (2^2 \times F_4(2)){:}2$. Here we use the function PossibleClassFusions to produce a list of 64 candidate fusion maps, and one checks that each candidate map produces the same permutation character $\chi = 1_H^G$. So once again, we can calculate $\delta(G)$ precisely, and the result follows.

Finally, let us assume $G = \mathbb{M}$ is the Monster. By the main theorem of [28], there are 46 conjugacy classes of maximal subgroups of G. For 31 of these classes, we can access the character tables of G and a representative H via the GAP function NamesOfFusionSources, as well as the corresponding fusion maps. So in each of these cases, we can compute $\delta(G)$ precisely, just as we did above. In particular, if $\mathcal{M}_1$ denotes this specific collection of maximal subgroups, then

$$\min\{\delta(G, H) \, : \, H \in \mathcal{M}_1\} = \frac{2670777082333978380150 4}{4972246225871825187787 5} = \gamma,$$

with equality if and only if $H = 2^{1+24}.\mathrm{Co}_1$. So in order to complete the proof, we need to show that $\delta(G, H) > \gamma$ for all of the remaining maximal subgroups H. To do this, let $\omega(H)$ be the *spectrum* of H, which is simply the set of element orders in H, and consider the crude lower bound

$$\delta(G) \geqslant \frac{|\{x \in G \, : \, |x| \notin \omega(H)\}|}{|G|}. \tag{2.2}$$

First assume H is one of the following maximal subgroups:

$$\mathrm{L}_2(13){:}2, \ \mathrm{L}_2(19){:}2, \ \mathrm{L}_2(29){:}2, \ \mathrm{U}_3(4){:}4, \ (\mathrm{L}_2(11) \times \mathrm{L}_2(11)).4, \ 11^2{:}(5 \times 2A_5),$$

$$7^2{:}\mathrm{SL}_2(7), \ 3^8.\mathrm{P\Omega}_8^-(3).2, \ 3^{3+2+6+6}.(\mathrm{L}_3(3) \times \mathrm{SD}_{16}), \ 3^{2+5+10}.(\mathrm{M}_{11} \times 2S_4),$$

$$(3^2{:}2 \times \mathrm{P\Omega}_8^+(3)).S_4, \ 2^{3+6+12+18}.(\mathrm{L}_3(2) \times 3S_6), \ 2^{2+11+22}.(\mathrm{M}_{24} \times S_3).$$

In each of these cases, a permutation representation of H is given in the Web Atlas [84], and with the aid of MAGMA [8], it is easy to determine $\omega(H)$. We can then verify the desired bound via (2.2). For example, if $H = 2^{3+6+12+18}.(\mathrm{L}_3(2) \times 3S_6)$, then the Web Atlas provides a representation of H on 1032192 points, and we can use MAGMA to compute

$$\omega(H) = \left\{ \begin{array}{l} 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 15, 16, 20, 21, 24, \\ 28, 30, 32, 35, 40, 42, 48, 56, 60, 70, 84, 105 \end{array} \right\}.$$

And then by inspecting the character table of G, the bound in (2.2) yields

$$\delta(G) \geqslant \frac{746174540081733025772653 07}{1057840310833592163982211 25} > \gamma,$$

and the result follows.

Finally, let us assume $H = 2^{5+10+20}.(S_3 \times \mathrm{L}_5(2))$ or $2^{10+16}.\Omega_{10}^+(2)$. In these two cases, the Web Atlas does not provide a permutation representation of H, and so we need to modify the argument. In the first case, one can check that the trivial bound

$$\delta(G) \geqslant \frac{|\{x \in G \, : \, |H| \text{ is indivisible by } |x|\}|}{|G|} \tag{2.3}$$

is sufficient, so we may assume $H = 2^{10+16}.\Omega_{10}^+(2)$. Here the same bound yields $\delta(G) > 1/2$, but we need to work a little bit harder to force $\delta(G) > \gamma$.

To do this, we first observe that

$$\{n \in \omega(G) \ : \ n \nmid |H|\} = \left\{ \begin{array}{l} 11, 13, 19, 22, 23, 26, 29, 33, 38, 39, 41, 44, 46, 47, 52, \\ 55, 57, 59, 66, 69, 71, 78, 87, 88, 92, 94, 95, 104, 110 \end{array} \right\} = A.$$

In addition, with the aid of MAGMA, we compute

$$\omega(\Omega_{10}^+(2)) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 17, 18, 20, 21, 24, 30, 31, 42, 45, 51, 60\}.$$

Since $H/N = \Omega_{10}^+(2)$ for some normal 2-subgroup N, it follows that every element in G of order 93, 105 and 119 is a derangement. So if we now set $B = A \cup \{93, 105, 119\}$, then

$$\delta(G) \geqslant \frac{|\{x \in G \ : \ |x| \in B\}|}{|G|} > \gamma,$$

and the proof is complete. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

Remark 2.8. It is easy to extend the above analysis to all almost simple sporadic groups. Indeed, let $G \leqslant \mathrm{Sym}(\Omega)$ be such a group with point stabiliser H and assume G is non-simple. Then we have $\delta(G) \geqslant 2516/7425$, with equality if and only if $G = \mathrm{McL}.2$ and $H = 2.S_8$.

2.3. Primitive groups

In this section, we extend our analysis of $\delta(G)$ to primitive permutation groups, and we prove Theorem C(i). The proof of Theorem C(ii) requires Theorem B, and the details will be presented in Section 4.5.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with socle N. Recall that N is the subgroup of G generated by the minimal normal subgroups of G, and recall that the primitivity of G implies that N is a direct product $N = T_1 \times \cdots \times T_k$, where each T_i is isomorphic to a fixed simple group T. The O'Nan-Scott theorem (see [65]) describes the primitive groups in terms of the structure and action of the socle, which leads to the following division into five families (recall that a transitive subgroup of G is *regular* if every nontrivial element is a derangement):

(a) Affine: $N = (C_p)^k$ is abelian and regular, p prime, $k \geqslant 1$, $G \leqslant \mathrm{AGL}_k(p)$
(b) Twisted wreath: N is non-abelian and regular
(c) Almost simple: $N = T$ is non-abelian simple, $G \leqslant \mathrm{Aut}(T)$
(d) Diagonal type: $N = T^k$ is non-abelian, $k \geqslant 2$, $G \leqslant N.(\mathrm{Out}(T) \times S_k)$
(e) Product type: $N = T^k$ is non-abelian, $k = ab$ with $a \geqslant 1$, $b \geqslant 2$, $G \leqslant L \wr S_b$ with L primitive of type (c) or (d).

Proof of Theorem C(i). Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with socle $N = T^k$, where T is simple. The possibilities for G and N are described by the O'Nan-Scott theorem, and we will refer to the five types briefly described above. Our goal is to prove that $\delta(N) \geqslant \varepsilon$, where $\varepsilon > 0$ is the constant in Theorem 2.1.

Of course, if G is an affine group or a twisted wreath product, then N is regular, and thus

$$\delta(N) = \frac{\Delta(N)}{|N|} = 1 - \frac{1}{|N|} \geqslant \frac{1}{2}.$$

And if G is almost simple, then N is a simple transitive permutation group on Ω, and thus Theorem 2.1 implies that $\delta(N) \geqslant \varepsilon$.

Next assume G is a diagonal type group, so $k \geqslant 2$. Let

$$D = \{(t, \ldots, t) \in N \ : \ t \in T\}$$

be the diagonal subgroup of N and note that we may identify Ω with the set N/D of right cosets of D in N. Given $x = (x_1, \ldots, x_k) \in N$ and $\omega = D(t_1, \ldots, t_k) \in \Omega$, we have $\omega^x = \omega$ if and only if $(t_1 x_1 t_1^{-1}, \ldots, t_k x_k t_k^{-1}) \in D$. Therefore, x is a derangement if and only if at least two of the components of x are not T-conjugate, and thus

$$\delta(N) = \frac{|N| - \left(\sum_{i=1}^m |t_i^T|^k\right)}{|N|} = 1 - \sum_{i=1}^m |C_T(t_i)|^{-k} \geqslant 1 - \sum_{i=1}^m |C_T(t_i)|^{-2},$$

where $\{t_1, \ldots, t_m\}$ is a complete set of representatives of the conjugacy classes in T. Since $|C_T(t_i)| \geqslant 3$ for all i (recall that a finite group with a self-centralising involution is soluble; see [7, Proposition 4.2], for example), we conclude that

$$\delta(N) \geqslant 1 - \frac{1}{3} \sum_{i=1}^m |C_T(t_i)|^{-1} = \frac{2}{3}.$$

Finally, let us assume G is a product type group. Here $G \leqslant L \wr S_b$, where $L \leqslant \mathrm{Sym}(\Gamma)$ is a primitive group with socle $S = T^a$, $b \geqslant 2$ and L is either almost simple or diagonal type. Then $N = S^b = T^{ab}$ and G acts on $\Omega = \Gamma^b$ with the product action. In particular, if $x = (x_1, \ldots, x_b) \in N$, where each x_i is contained in S, then

$$(\gamma_1, \ldots, \gamma_b)^x = (\gamma_1^{x_1}, \ldots, \gamma_b^{x_b})$$

for all $\omega = (\gamma_1, \ldots, \gamma_b) \in \Omega$. It follows that x is a derangement on Ω if and only if at least one x_i is a derangement on Γ, whence

$$\delta(N) > \frac{|\Delta(S, \Gamma)||S|^{b-1}}{|S|^b} = \delta(S, \Gamma). \tag{2.4}$$

If L is almost simple, then Theorem 2.1 implies that $\delta(N) \geqslant \varepsilon$. And if L is a diagonal type group, then our previous argument gives $\delta(N) \geqslant 2/3$. □

3. Derangement width

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite transitive permutation group, let k be a positive integer and recall that

$$\Delta(G)^k = \{x_1 \cdots x_k : x_i \in \Delta(G) \text{ for all } i\}.$$

In [58], Larsen, Shalev and Tiep prove that $G = \Delta(G)^2$ for all sufficiently large simple transitive groups, and they propose the following conjecture (this is stated as Conjecture 1.5 in Section 1).

Conjecture 3.1. *We have $G = \Delta(G)^2$ for every finite simple transitive group G.*

This conjecture is proved for alternating groups in [58, Theorem B]. In this section, we establish a strong form of Conjecture 3.1 for all sporadic groups and all rank one groups of Lie type, and we revisit the problem for alternating groups. In particular, we prove part (i) of Theorem D. We also establish an extension of [58, Theorem B] for symmetric groups (see Theorem 3.8), and we prove Theorem E, which settles Conjecture 3.1 for all the linear groups $\mathrm{L}_n(q)$ under a mild additional assumption on the point stabilisers (see Theorem 3.16). At the end of the section, we present a proof of Theorem F.

3.1. Sporadic groups

Here we establish a strong form of Conjecture 3.1 for sporadic groups. We will need the following result, which will also be useful later on.

Table 2. *The pairs (G, H) in Proposition 3.4(ii).*

G	H	C	D
M_{11}	S_5	11A	11B
M_{22}	$2^4{:}A_6$, $2^4{:}S_5$	11A	11B
M_{23}	M_{22}, $L_3(4).2$, $2^4{:}A_7$, M_{11}, $2^4{:}(3 \times A_5).2$	23A	23B
	$2^4{:}A_6$, $2^4{:}S_5$ (two classes), $2^4.(15{:}4)$		
M_{24}	$M_{12}.2$	23A	23B

Lemma 3.2. *Let G be a finite group with conjugacy classes $C_i = g_i^G$ for $i = 1, 2$. For an element $x \in G$, let $N(x)$ be the number of solutions to the equation $x = y_1 y_2$ with $y_i \in C_i$. Then*

$$N(x) = \frac{|C_1||C_2|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1)\chi(g_2)\overline{\chi(x)}}{\chi(1)},$$

where $\mathrm{Irr}(G)$ is the set of complex irreducible characters of G.

Proof. This is a special case of a well-known formula of Frobenius, which follows from the familiar orthogonality relations satisfied by the character table of G. See [54, Theorem 30.4], for example. □

Remark 3.3. Note that $G = C_1 C_2$ if and only if $N(x_i) > 0$ for all i, where $\{x_1, \dots, x_k\}$ is a complete set of representatives of the conjugacy classes in G.

The following result establishes a strong form of Theorem D for sporadic groups.

Proposition 3.4. *Let G be a transitive sporadic simple group with point stabiliser H.*

(i) *We have $G = CD$, where C and D are conjugacy classes of derangements.*
(ii) *Moreover, either $G = C^2$ for some class C of derangements, or (G, H) is one of the cases in Table 2 and*

$$G = CD = \{1\} \cup C^2 = \{1\} \cup D^2$$

for the classes C and D of derangements indicated in the table.

Proof. Let $\mathcal{C}(G)$ be the set of conjugacy classes C in G with $G = C^2$. Using the GAP Character Table Library [12] and Lemma 3.2, it is easy to determine all of the conjugacy classes in $\mathcal{C}(G)$. For example, if $G = \mathbb{M}$ is the Monster, then 146 of the 194 conjugacy classes in G are contained in $\mathcal{C}(G)$.

First assume $G \neq \mathbb{B}, \mathbb{M}$. In each of these cases, we can use the GAP function Maxes to access the character table of every maximal subgroup H of G, together with the fusion map from H-classes to G-classes. This allows us to determine all the conjugacy classes of derangements for the action of G on G/H, and it is a routine exercise to check whether or not one of these classes is contained in $\mathcal{C}(G)$. We find that there is always at least one such class, unless (G, H) is one of the following:

$$
\begin{aligned}
&M_{11}{:}\ H = S_5 \\
&M_{22}{:}\ H = 2^4{:}A_6 \text{ or } 2^4{:}S_5 \\
&M_{23}{:}\ H = M_{22},\ L_3(4).2,\ 2^4{:}A_7,\ M_{11} \text{ or } 2^4{:}(3 \times A_5).2 \\
&M_{24}{:}\ H = M_{12}.2
\end{aligned}
\tag{3.1}
$$

In each of these cases, we first check that we can always find two classes of derangements C and D with $G = CD$, which is easy to verify using GAP and Lemma 3.2. In addition, we check that $G = \{1\} \cup C^2 = \{1\} \cup D^2$.

So to complete the proof for $G \neq \mathbb{B}, \mathbb{M}$, we just need to inspect the special cases (G, H) in (3.1) in order to determine whether or not H has a proper subgroup K that meets every class in $\mathcal{C}(G)$. To do this, we use MAGMA to construct $G = M_n$ and H in the natural permutation representation on n points,

and we inspect the maximal subgroups of H. In this way, we deduce that if $G = \mathrm{M}_{11}$, M_{22} or M_{24}, then every proper subgroup of H fails to intersect at least one of the classes in $\mathcal{C}(G)$. Now assume $G = \mathrm{M}_{23}$. Here G has four maximal subgroups

$$H \in \{\mathrm{M}_{22}, \mathrm{L}_3(4).2, 2^4{:}A_7, 2^4{:}(3 \times A_5).2\}$$

with a maximal subgroup $K < H$ meeting every class in $\mathcal{C}(G)$. These second maximal subgroups of G are recorded in the second row for $G = \mathrm{M}_{23}$ in Table 2, up to conjugacy in G. In turn, one checks that if $J < K$ is maximal, then $J \cap C$ is empty for at least one class $C \in \mathcal{C}(G)$, so no further examples arise.

Next assume $G = \mathbb{B}$ is the Baby Monster. As above, we can use the GAP function Maxes to access the character table of each maximal subgroup H of G. And as explained in the proof of Proposition 2.7, we can also compute the corresponding permutation character 1_H^G, which allows us to check that there is always at least one class of derangements in $\mathcal{C}(G)$.

Finally, suppose $G = \mathbb{M}$ is the Monster. Recall that G has 46 conjugacy classes of maximal subgroups (see [28]). Now G has a unique class C of elements of order 41, and our earlier computation shows that $C \in \mathcal{C}(G)$. By inspecting [28, Table 1], we deduce that the only maximal subgroups intersecting C are $3^8.\mathrm{P}\Omega_8^-(3).2$ and $41{:}40$. In addition, G has a unique class D of elements of order 19, and we note that $D \in \mathcal{C}(G)$, so the result follows since neither $3^8.\mathrm{P}\Omega_8^-(3).2$ nor $41{:}40$ contains elements in D. □

3.2. *Alternating groups*

The main result of this section is the following proposition, which establishes a stronger version of [58, Theorem B]. In particular, this gives Theorem D for alternating groups.

Proposition 3.5. *Let $G = A_n$ be a simple transitive group with point stabiliser H.*

  (i) *There exists a conjugacy class C of derangements such that $G = \{1\} \cup C^2$.*
 (ii) *Moreover, either $G = C^2$, or one of the following holds:*
    (a) *$(G, H) = (A_5, A_4)$, (A_5, S_3) or $(A_8, 2^4{:}(S_3 \times S_3))$.*
    (b) *$n \geqslant 27$, $n \equiv 3 \pmod 4$ and $H = A_{n-1}$.*
(iii) *If $n \geqslant 6$, then $G = CD$ for classes C, D of derangements.*

Remark 3.6.

(a) The special cases in part (ii)(a) of Proposition 3.5 are genuine exceptions in the sense that $G \neq C^2$ for every class C of derangements. For the two cases with $G = A_5$, we have

$$G = \{1\} \cup CD = \{1\} \cup C^2 = \{1\} \cup D^2,$$

where C and D are the two classes of elements of order 5. And for $G = A_8$, we get

$$G = CD = \{1\} \cup C^2 = \{1\} \cup D^2 \tag{3.2}$$

if we take C and D to be the two classes of 7-cycles.
(b) We expect that the case recorded in (ii)(b) is not a genuine exception. Here [59, Theorem 1] gives $G = \{1\} \cup D^2$ where D is a class of n-cycles, and we conjecture that $G = C^2$ for the class C of elements with cycle-type $(n - 4, 2^2)$. We have used MAGMA [8] to check the latter claim computationally for $n \in \{7, 11, 15, 19, 23\}$, which explains why we include the condition $n \geqslant 27$.
(c) For $n \geqslant 11$, the proof of [58, Theorem B] combines a technical result [58, Proposition 7.1] with the main theorem of [6] to show that either $G = C^2$ for some S_n-class C of derangements in G, or n is even and $\Omega = \{1, \ldots, n\}$. In the latter case, the authors apply an inductive argument to show that $G = \Delta(G)^2$.

Our proof of Proposition 3.5 relies heavily on Proposition 3.7 below, which combines results from [6, 11, 59]. In order to state the proposition, let $\ell \leqslant n$ be a positive integer and let C_ℓ be the S_n-class of the ℓ-cycle $x = (1, \ldots, \ell)$. And if ℓ is odd, set $D_\ell = x^{A_n}$ and note that $D_\ell = C_\ell$ unless $\ell = n$ or $n - 1$.

Proposition 3.7. *Let $G = A_n$ with $n \geq 5$.*

(i) *If $\frac{3}{4}n \leq \ell \leq n$, then $G = C_\ell^2$.*

(ii) *If $n \geq 9$ and $n \equiv 1 \pmod 4$, then $G = D_n^2$.*

(iii) *Let $D = x^{S_n}$, where $x = (1, \dots, \ell_1)(\ell_1 + 1, \dots, \ell_1 + \ell_2)$ with $\ell_1, \ell_2 \geq 2$ and $\ell_1 + \ell_2 > \frac{3}{4}n + 3$. Then $G = D^2$.*

Proof. Part (i) is the main theorem of [6], while part (ii) is a recent result of Larsen and Tiep [59, Theorem 5(i)]. Finally, part (iii) is due to Brenner [11]. □

We are now ready to prove Proposition 3.5.

Proof of Proposition 3.5. The groups with $5 \leq n \leq 18$ can be checked using MAGMA [8]. To do this, we first construct the character table of G, and we use the Frobenius formula (see Lemma 3.2) to determine the set $\mathcal{C}(G)$ of conjugacy classes C with $G = C^2$. Next we construct a representative H of each conjugacy class of maximal subgroups of G, and it is straightforward to check that every class in $\mathcal{C}(G)$ meets H if and only if (G, H) is one of the cases recorded in part (ii)(a) of Proposition 3.5. And in each of these cases, it is routine to check that if $K < H$ is any maximal subgroup, then there exists a class $C \in \mathcal{C}(G)$ such that $C \cap K$ is empty. For the remainder, we will assume $n \geq 19$.

Suppose H acts intransitively on $[n] = \{1, \dots, n\}$, so $H \leq (S_k \times S_{n-k}) \cap G$ for some positive integer $k \leq n/2$. If n is even, then by applying parts (i) and (iii) of Proposition 3.7, we deduce that $G = D_{n-3}^2$ if $k \geq 4$ and $G = D^2$ if $k \leq 3$, where $D = x^G$ and $x = (1, \dots, 4)(5, \dots, n)$. If $n \equiv 1 \pmod 4$, then Proposition 3.7(ii) gives $G = D_n^2$, so we may assume $n \equiv 3 \pmod 4$. If $k \geq 3$, then every $(n-2)$-cycle in G is a derangement, and we have $G = D_{n-2}^2$ by Proposition 3.7(i). And if $k = 2$, then Proposition 3.7(iii) implies that $G = D^2$, where $D = x^G$ and $x = (1, \dots, 4)(5, \dots, n-1)$. Finally, suppose $k = 1$. As above, let $C = x^G$ with $x = (1, \dots, n)$ and set $D = (x^{-1})^G \neq C$. Then [59, Theorem 1] implies that (3.2) holds.

Next assume H is imprimitive, so $H \leq (S_a \wr S_b) \cap G$, where $n = ab$ and $a, b \geq 2$. If n is odd, then $a \geq 3$, and every $(n-2)$-cycle is a derangement because it does not preserve a partition of $[n]$ into b blocks of size a. The result follows since $G = D_{n-2}^2$ by Proposition 3.7(i). Now assume n is even and set $\ell = 5$ if $a = 3$, and $\ell = 3$ otherwise. Then every $(n - \ell)$-cycle is a derangement, and the desired conclusion holds since $G = D_{n-\ell}^2$ (note that if $a = 3$, then $n \geq 21$, and thus $n - 5 \geq 3n/4$).

Finally, let us assume H acts primitively on $[n]$. Fix an odd integer ℓ such that $3n/4 \leq \ell \leq n - 3$. Then Proposition 3.7(i) gives $G = D_\ell^2$, and the main theorem of [55] implies that every ℓ-cycle in G is a derangement (indeed, no proper primitive subgroup of G contains an ℓ-cycle). The result follows. □

3.3. Symmetric groups

Here we apply work of Brenner [11] to prove a strong form of [58, Theorem B] for symmetric groups.

Theorem 3.8. *Let $G = S_n$ be a transitive group on a set Ω with point stabiliser H, where $n \geq 4$.*

(i) *We have $G = \Delta(G)^2$.*

(ii) *Moreover, if $\Omega \neq \{1, \dots, n\}$, then there exist conjugacy classes C and D of derangements such that $G = C^2 \cup CD$.*

Set $L = A_n$ and observe that if C and D are conjugacy classes in $G = S_n$, then $C^2 \subseteq L$ and either $CD \subseteq L$ or $CD \subseteq G \setminus L$, according to whether or not the elements comprising C and D have the same parity. In particular, $G \neq \{1\} \cup C^2$ and $G \neq \{1\} \cup CD$, so the conclusion $G = C^2 \cup CD$ in part (ii) of Theorem 3.8 is essentially best possible. Clearly, in order to prove Theorem 3.8, we may assume that H is maximal in L or G. (Note that G may contain a non-maximal subgroup H that is not contained in a core-free maximal subgroup of G, such as $H = \mathrm{AGL}_3(2)$ in $G = S_8$. But in this situation, H is always maximal in L.)

Remark 3.9. We expect that the conclusion $G = C^2 \cup CD$ for classes C, D of derangements is still valid when $\Omega = \{1, \ldots, n\}$. Indeed, we conjecture that we can take $C = x^G$ and $D = y^G$, where $x = (1, \ldots, n)$ and $y = (1, 2)(3, \ldots, n)$. We have used MAGMA to check this for $4 \leqslant n \leqslant 20$.

It will be convenient to handle the low degree groups computationally.

Lemma 3.10. *The conclusion to Theorem 3.8 holds for* $n \leqslant 15$.

Proof. This is a straightforward computation. First we use MAGMA [8] to construct the character table of G, and we then apply Lemma 3.2 to determine the set $\mathcal{C}'(G)$ of pairs of classes (C, D) such that $G = C^2 \cup CD$. We then construct a representative H of each conjugacy class of core-free maximal subgroups in A_n and G, and in each case, it is easy to check that there is at least one pair $(C, D) \in \mathcal{C}'(G)$ such that $C \cap H$ and $D \cap H$ are both empty (including the special case $\Omega = \{1, \ldots, n\}$). □

For the remainder, we may assume $n \geqslant 16$. The main ingredient in the proof of Theorem 3.8 is the following. The statement is a combination of special cases of two results due to Brenner [11].

Proposition 3.11. *Let* $G = S_n$ *with* $n \geqslant 16$ *and set* $C = x^G$ *and* $D = y^G$, *where*

(i) $x = (1, \ldots, \ell)$ *and* $y = (1, \ldots, \ell + 1)$, *with* $n - 4 \leqslant \ell < n$; *or*
(ii) $x = (1, 2, 3)(4, 5, \ldots, n - 1)$ *and* $y = (1, 2, 3)(4, 5, \ldots, n)$.

Then $G = C^2 \cup CD$.

Proof. Suppose $x \in G$ has $n - t$ fixed points and c nontrivial orbits on $\{1, \ldots, n\}$. Then $t + c \leqslant 3n/2$, and the condition $n \geqslant 16$ allows us to appeal to Theorems 2.02 and 4.02 in [11], which immediately give $L = C^2$ and $G \setminus L = CD$ in both (i) and (ii). □

We will also need the following elementary lemma.

Lemma 3.12. *Let* $G = S_n$ *with* $n \geqslant 4$. *Then for all* $x \in G$, *there exists an* n-*cycle* $y \in G$ *such that* xy *has no fixed points on* $\{1, \ldots, n\}$.

Proof. We may assume x is nontrivial. Since the set of derangements on $\{1, \ldots, n\}$ is a normal subset of G, it suffices to show that some conjugate of x has the desired property. By considering the disjoint cycle decomposition of x, it is easy to see that there exists a conjugate z of x such that $n^z \neq 1$ and $i^z \neq i + 1$ for all $i \in \{1, \ldots, n - 1\}$. Then $z(n, \ldots, 1)$ has no fixed points on $\{1, \ldots, n\}$, and the result follows. □

We are now in a position to prove Theorem 3.8.

Proof of Theorem 3.8. In view of Lemma 3.10, we may assume $n \geqslant 16$. Also recall that we may assume H is maximal in $L = A_n$ or $G = S_n$. Set $[n] = \{1, \ldots, n\}$.

First assume H is intransitive on $[n]$, which means that we may assume $H = S_k \times S_{n-k}$ with $1 \leqslant k < n/2$, and we identify Ω with the set of k-element subsets of $[n]$. If $k = 1$, then Lemma 3.12 implies that $G = \Delta(G)C$, where C is the class of n-cycles, and the result follows since every n-cycle is a derangement. And for $k \geqslant 2$, we can define C and D as in part (i) of Proposition 3.11 with $\ell = n - 1$. Then the elements in C and D are derangements, and the proposition gives $G = C^2 \cup CD$, as required.

Next suppose H is transitive and imprimitive on $[n]$. Here we may assume $H = S_a \wr S_b$ for integers a and b with $n = ab$ and $a \geqslant 2$. If $a \geqslant 3$, then every $(n-2)$-cycle and every $(n-1)$-cycle is a derangement, and Proposition 3.11 yields $G = C^2 \cup CD$, where C and D are defined as in part (i) of the proposition, with $\ell = n - 2$. And if $a = 2$, then the same conclusion holds if we define C and D as in part (ii) of Proposition 3.11.

Finally, let us assume H acts primitively on $[n]$. By the main theorem of [55], every $(n - 4)$-cycle and every $(n - 3)$-cycle is a derangement. So the result follows by defining C and D as in part (i) of Proposition 3.11 with $\ell = n - 4$. □

Table 3. *The classes $C = x^G$ and $D = y^G$ in Proposition 3.14.*

G	Conditions	$|x|$	$|y|$
$^2B_2(q)$	$q \geqslant 8$	$q + \sqrt{2q} + 1$	$q - \sqrt{2q} + 1$
$^2G_2(q)$	$q \geqslant 27$	$q + \sqrt{3q} + 1$	$q - \sqrt{3q} + 1$
$U_3(q)$	$q \geqslant 3$	$(q^2 - q + 1)/(3, q + 1)$	$(q^2 - 1)/(3, q + 1)$
$L_2(q)$	$q \geqslant 5$ odd	$(q + 1)/2$	$(q - 1)/2$
	$q \geqslant 4$ even	$q - 1$	

3.4. Groups of Lie type

In this section, we consider the derangement width of simple groups of Lie type. We begin by stating our main result for rank one groups (see (1.1)), which completes the proof of Theorem D(i). Recall that $^2G_2(3)'$ is isomorphic to $L_2(8)$, so we assume $q \geqslant 27$ when considering $G = {}^2G_2(q)$ in Theorem 3.13, and also in Proposition 3.14 below.

Theorem 3.13. *Let G be a finite transitive simple rank one group of Lie type with point stabiliser H. Then there exist conjugacy classes C and D of derangements such that*

$$G = \begin{cases} C^2 & \text{if } G = {}^2B_2(q) \text{ or } {}^2G_2(q) \\ \{1\} \cup C^2 & \text{if } G = U_3(q) \\ \{1\} \cup CD & \text{if } G = L_2(q) \text{ and } (G, H) \neq (L_2(7), S_4) \\ C^2 \cup CD & \text{if } (G, H) = (L_2(7), S_4). \end{cases}$$

In particular, we have $G = \Delta(G)^2$.

The main ingredient in the proof of Theorem 3.13 is the following result. Note that $L_2(5) \cong L_2(4)$, so we assume $q \geqslant 7$ if $G = L_2(q)$ with q odd.

Proposition 3.14. *Let G be a rank one finite simple group of Lie type and set $C = x^G$ and $D = y^G$, where the order of x and y is given in Table 3.*

 (i) *If $G \in \{{}^2B_2(q), {}^2G_2(q), L_2(q)\ (q \geqslant 7 \text{ odd})\}$, then $G = C^2 = D^2$.*
 (ii) *If $G = U_3(q)$, then $G = \{1\} \cup C^2$.*
 (iii) *If $G = L_2(q)$ with q even, then $G = C^2 = \{1\} \cup AB$, where $A = z^G$, $B = (z^2)^G$ and $|z| = q + 1$.*
 (iv) *If $G = L_2(7)$, then $G = A^2 \cup AB = B^2 \cup AB$, where A and B are the two classes of elements of order 7.*

Proof. Parts (i) and (ii) follow immediately from [47, Theorem 7.1], noting that every semisimple conjugacy class in $^2B_2(q)$ and $^2G_2(q)$ is real (for example, this follows from Lemma 4.7 in Section 4.3 below). Now assume $G = L_2(q)$ with q even. Here [47, Theorem 7.1] gives $G = C^2$, so it just remains to show that $G = \{1\} \cup AB$, where A and B are the conjugacy classes of z and z^2, respectively, and we have $|z| = |z^2| = q + 1$.

Given a nontrivial element $g \in G$, let $N(g)$ be the number of solutions to the equation $g = ab$ with $a \in A$ and $b \in B$ and recall Lemma 3.2, which states that

$$N(g) = \frac{|A||B|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(z)\chi(z^2)\overline{\chi(g)}}{\chi(1)},$$

where $\mathrm{Irr}(G)$ is the set of complex irreducible characters of G. By inspecting the character table of G (see [30, Section 38], for example), it is a straightforward exercise to show that

$$N(g) = \begin{cases} q & \text{if } |g| = 2 \\ q - 1 & \text{if } |g| \text{ divides } q - 1 \\ q + 1 \text{ or } 1 & \text{if } |g| \text{ divides } q + 1, \end{cases}$$

and we conclude that $|N(g)| \geq 1$ for all $1 \neq g \in G$ (this can also be checked computationally, using the GAP package Chevie [43]). Therefore, $G = \{1\} \cup AB$, as claimed. □

Remark 3.15. For $G = L_2(q)$, Garion [41] gives a complete classification of the conjugacy classes C with $G = C^2$. In particular, [41, Theorem 2(ii)] shows that if q is even and $C = x^G$ with $|x|$ dividing $q + 1$, then $C^2 = \{y \in G : |y| \neq 2\}$.

Proof of Theorem 3.13. As usual, we may assume H is a maximal subgroup. For now, let us assume $G \neq L_2(q)$ if q is even (we will handle this special case at the end of the proof) and define the classes $C = x^G$ and $D = y^G$ as in Table 3. In view of Proposition 3.14, it suffices to show that either x or y is a derangement.

Suppose $G = {}^2B_2(q)$. Here $N_G(\langle x \rangle)$ is the unique maximal overgroup of x, so x is a derangement unless $H = (q + \sqrt{2q} + 1).4$. And in the latter case, y is a derangement since $|H|$ is indivisible by $|y|$, and the result follows. An entirely similar argument handles the groups $G = {}^2G_2(q)$ with $q \geq 27$.

Next assume $G = U_3(q)$ with $q \geq 3$, and note that $1 \notin C^2 \cup D^2$ since neither C nor D are real classes. Suppose $q \notin \{3, 5\}$. Since $|x| = (q^2 - q + 1)/(3, q + 1)$, it follows that x is a Singer cycle, and the main theorem of [5] implies that x is a derangement unless H is a field extension subgroup of type $GU_1(q^3)$. But in the latter case, y is a derangement, and once again, the result follows. Finally, if $q = 3$, then x is a derangement unless $H = L_2(7)$, in which case y is a derangement. Similarly, if $q = 5$, then x is a derangement unless H is isomorphic to A_7 (there are three conjugacy classes of such subgroups), and in the latter situation, it is clear that y is a derangement.

Now suppose $G = L_2(q)$ with $q \geq 7$ odd. If $q \geq 11$, then [5] implies that x is a derangement unless $H = D_{q+1}$ is a field extension subgroup of type $GL_1(q^2)$, in which case y is a derangement. If $q = 9$, then x is a derangement unless $H = A_5$ (there are two classes of such subgroups). But in the latter case, H does not contain any elements of order $|y| = 4$, so y is a derangement. Now assume $q = 7$, so $|x| = 4$, $|y| = 3$ and C, D are the unique conjugacy classes in G containing elements of order $4, 3$, respectively. If $H = 7{:}3$, then x is a derangement. However, if $H = S_4$ (there are two such classes), then x and y both have fixed points. Indeed, $\Delta(G) = A \cup B$ is the union of the two conjugacy classes of elements of order 7. It is easy to check that

$$A^2 = B^2 = \{z \in G : |z| \neq 1, 4\}, \quad AB = \{z \in G : |z| \neq 2\},$$

and thus G is not equal to $\{1\} \cup A^2$, $\{1\} \cup B^2$ nor $\{1\} \cup AB$, but we do get $G = A^2 \cup AB = B^2 \cup AB$ as required. Moreover, if we consider the action of G on G/K, where K is a proper subgroup of H, then we find that either x or y is a derangement, so we have $G = E^2$ for some conjugacy class E of derangements.

To complete the proof, we may assume $G = L_2(q)$ with $q \geq 4$ even. Set $C = x^G$ and $A = z^G$, $B = (z^2)^G$, where $|x| = q - 1$ and $|z| = q + 1$, so Proposition 3.14(iii) implies that $G = C^2 = \{1\} \cup AB$. By [5], z and z^2 are derangements unless $H = D_{2(q+1)}$ is a field extension subgroup of type $GL_1(q^2)$, and in the latter case, we see that x is a derangement. The result follows. □

To conclude this section, we briefly consider Conjecture 3.1 for groups of Lie type of rank two or more, focussing on the linear groups $L_n(q)$ with $n \geq 3$. Note that $L_3(2) \cong L_2(7)$, so we may assume $q \geq 3$ in part (i) of Theorem 3.16 below. In part (ii), we write P_k for the stabiliser of a k-dimensional subspace of the natural module for G.

The following result establishes Theorem E, as stated in Section 1.

Theorem 3.16. *Let $G = L_n(q)$ be a transitive simple group on a set Ω with point stabiliser H and assume $n \geq 3$.*

(i) *If $n = 3$ and $q \geq 3$, then $G = \{1\} \cup C^2$ for some conjugacy class C of derangements.*
(ii) *If $n \geq 4$ and $H \nleq P_1, P_{n-1}$, then $G = \Delta(G)^2$. Moreover, if $q \geq 3$ or $H \nleq Sp_n(2)$, then $G = \{1\} \cup CD$ for classes C, D of derangements.*

Remark 3.17. Suppose $n \geqslant 4$ and H is contained in a P_1 or P_{n-1} parabolic subgroup. If $n \geqslant 33$, then the two classes C, D in [58, Theorem 2.4(i)] are derangements, and we have $G = \{1\} \cup CD$. And the same conclusion holds if $n \geqslant 7$ and $q > 7^{481}$ by [58, Theorem 2.4(ii)]. So the open cases here are when $4 \leqslant n \leqslant 6$ (for all q at most some unspecified constant) and when $7 \leqslant n \leqslant 32$ with $q \leqslant 7^{481}$.

We will need the following lemma in the case where $G = L_n(2) = GL_n(2)$ and $n \geqslant 30$. For an integer $2 \leqslant k < n/2$, let $z_k \in G$ be a regular semisimple element of the form $z_k = \mathrm{diag}(A, B)$, where $A \in GL_k(2)$ and $B \in GL_{n-k}(2)$ are Singer cycles, so we have

$$|z_k| = \mathrm{lcm}(2^k - 1, 2^{n-k} - 1). \tag{3.3}$$

Lemma 3.18. *Let* $G = L_n(2)$ *with* $n \geqslant 30$ *and let* $x, y \in G$ *be regular semisimple elements of the form* $x = z_2$ *and* $y = z_3$. *Then* $G = \{1\} \cup CD$, *where* $C = x^G$ *and* $D = y^G$.

Proof. This follows from [58, Theorem 2.4(i)] if $n \geqslant 33$. By slightly tweaking some of the estimates in the proof of this result, we will show that the same argument also works for $n = 30, 31$ and 32.

In view of Lemma 3.2, we need

$$\left| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\overline{\chi(g)}}{\chi(1)} \right| > 0$$

for each non-identity element $g \in G$. As explained in the proof of [58, Theorem 2.4(i)], it suffices to show that

$$\sum_{i=2}^{8} \frac{|\chi_i(g)|}{\chi_i(1)} < 1,$$

where the χ_i are the non-principal unipotent characters of G listed in [58, (2.3)]. By repeating the argument in the proof of [58, Theorem 2.4(i)], setting $q = 2$ and applying [58, Lemma 2.3] and [46, Theorem 1.6(i)], we get

$$\sum_{i=2}^{4} \frac{|\chi_i(g)|}{\chi_i(1)} < \frac{2^{n-1} + 4}{2^n - 2} + 0.1254 + \frac{1.76}{2^{(4n-15)/n}} < 0.781$$

for all $n \geqslant 30$. As in [58, (2.8)], the combined contribution from the four remaining unipotent characters is at most

$$4 \cdot 2^{(21-n)/2} < 0.177,$$

so

$$\sum_{i=2}^{8} \frac{|\chi_i(g)|}{\chi_i(1)} < 0.781 + 0.177 < 1,$$

and the result follows. □

First we handle the case $n = 3$.

Lemma 3.19. *The conclusion to Theorem 3.16 holds for* $n = 3$.

Proof. Here $G = L_3(q)$ with $q \geqslant 3$, and we set $d = (3, q - 1)$. By [47, Theorem 7.3], we have $G = \{1\} \cup C^2 = \{1\} \cup D^2$, where $C = x^G$ and $D = y^G$ with $|x| = (q^2 + q + 1)/d$ and $|y| = (q^2 - 1)/d$. Note that x is a Singer cycle.

For $q \neq 4$, the main theorem of [5] implies that x is a derangement unless H is a field extension subgroup of type $GL_1(q^3)$. But in the latter case, y is clearly a derangement, and the result follows.

Finally, if $q = 4$, then $|x| = 7$, $|y| = 5$, and one checks that no maximal subgroup of G has order divisible by 35, so in each case, either x or y is a derangement. □

Now assume $n \geq 4$. The following result is part of [71, Theorem 2.1].

Proposition 3.20. *Let* $G = L_n(q)$ *with* $n \geq 4$ *and set* $d = (n, q - 1)$ *and* $e = (2, q - 1)$. *Then* $G = \{1\} \cup CD$, *where* $C = x^G$, $D = y^G$ *and*

$$|x| = \begin{cases} (q^{n/2} + 1)/e & \text{if } n \text{ is even} \\ (q^n - 1)/d(q - 1) & \text{if } n \text{ is odd,} \end{cases} \qquad |y| = \begin{cases} (q^{n-1} - 1)/d & \text{if } n \text{ is even} \\ q^{(n-1)/2} + 1 & \text{if } n \text{ is odd.} \end{cases}$$

Thompson's conjecture for the linear groups $L_n(q)$ was first proved by Lev in [61], where he established several additional results on conjugacy classes and their products. We will use Proposition 3.21 below, which is a special case of [61, Theorem 1]. In order to state this result, we need to introduce some notation.

Suppose $n \geq 3$ and $n_1, \ldots, n_k$ are positive integers such that $n = 2 + \sum_i n_i$. For a positive integer m and scalar $\lambda \in \mathbb{F}_q^\times$, let

$$J_m(\lambda) = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix} \in \mathrm{GL}_m(q)$$

be a standard $m \times m$ Jordan block with eigenvalue λ (for $\lambda = 1$, we will often write J_m, rather than $J_m(1)$). Then for an irreducible matrix $A \in \mathrm{GL}_2(q)$, let

$$x = (A, J_{n_1}(\lambda_1), \ldots, J_{n_k}(\lambda_k)) \in \mathrm{PGL}_n(q)$$

denote the image of the block-diagonal matrix $\mathrm{diag}(A, J_{n_1}(\lambda_1), \ldots, J_{n_k}(\lambda_k)) \in \mathrm{GL}_n(q)$. Note that $x \in L_n(q)$ if $\prod_i \lambda_i^{n_i} = \det(A)^{-1}$.

Proposition 3.21. *Let* $G = L_n(q)$ *with* $n \geq 3$ *and set* $C = x^G$, *where* $x \in G$ *is defined*

$$x = \begin{cases} (J_n) & \text{if } q = 2 \\ (A, J_{n_1}(\lambda_1), \ldots, J_{n_k}(\lambda_k)) & \text{if } q \geq 3, \end{cases}$$

and the λ_i *are distinct elements of* $\mathbb{F}_q^\times$. *Then* $G = C^2$.

Proof. If $q \geq 3$, then [61, Theorem 1] implies that $G = CC^{-1}$, and the result follows since $C = C^{-1}$ by [73, Theorem 1] (recall that $A \in \mathrm{GL}_2(q)$ is irreducible). Similarly, if $q = 2$, then C is the unique conjugacy class of cyclic matrices in G all of whose eigenvalues are contained in $\mathbb{F}_2$, and once again, the result follows from [61, Theorem 1] (also see [61, p.1243]). □

The following elementary observation will also be useful.

Lemma 3.22. *Let* G *be a finite permutation group with* $\delta(G) > 1/2$. *Then* $G = \Delta(G)^2$.

Proof. Suppose $x \notin \Delta(G)^2$. Then $x\Delta(G)^{-1} \cap \Delta(G)$ is empty, and thus $|\Delta(G)| \leq |G|/2$, which is a contradiction. □

We are now ready to complete the proof of Theorem 3.16 (recall that this is stated as Theorem E in Section 1).

Proof of Theorem 3.16. In view of Lemma 3.19, we may assume $n \geq 4$. In addition, we may assume $H \neq P_1, P_{n-1}$ is a maximal subgroup of G. The groups $L_6(2)$ and $L_7(2)$ can be handled using MAGMA, and in both cases, we check that $G = C^2$ for some conjugacy class C of derangements. So for the remainder, we may assume $(n, q) \neq (6, 2), (7, 2)$.

Write $q = p^f$, where p is a prime. Recall that if $e \geqslant 2$ is an integer, then a prime divisor r of $q^e - 1$ is a *primitive prime divisor* if $q^i - 1$ is indivisible by r for all $i < e$. By a theorem of Zsigmondy [85], such a divisor exists unless $(e, q) = (6, 2)$, or if $e = 2$ and q is a Mersenne prime. Define the conjugacy classes $C = x^G$ and $D = y^G$ as in Proposition 3.20 and set

$$m = \min\{|x|, |y|\}.$$

Since $(n, q) \neq (6, 2), (7, 2)$, it follows that $|x|$ and $|y|$ are divisible by primitive prime divisors of $p^{fn} - 1$ and $p^{f(n-1)} - 1$, respectively, so the maximal overgroups of x and y are described in [49], and we can work through the possibilities arising in [49, Examples 2.1-2.9]. In doing so, it will be convenient to adopt the standard notation $\mathcal{C}_1 \cup \cdots \cup \mathcal{C}_8 \cup \mathcal{S}$ for the nine collections of maximal subgroups of G arising in Aschbacher's subgroup structure theorem [2], appealing to [57] for a detailed description of the subgroups arising in each collection. We will often refer to the *type* of H, which gives a rough description of its structure (our usage is consistent with [57, p.58]). Let V be the natural module for G.

First assume $H \in \mathcal{C}_1$, so $H = P_k$ is a maximal parabolic subgroup with $2 \leqslant k \leqslant n - 2$, and we may identify Ω with the set of k-dimensional subspaces of V. Since x acts irreducibly on V, we have $x \in \Delta(G)$. Similarly, y fixes a decomposition $V = U \oplus W$, where U is 1-dimensional and y acts irreducibly on W. This means that U and W are the only proper nonzero subspaces of V fixed by y, so y is also a derangement on Ω, and we conclude by applying Proposition 3.20.

Next suppose $H \in \mathcal{C}_2$. By [49], either x and y are both derangements, or H is of type $\mathrm{GL}_1(q) \wr S_n$ with $q \geqslant 5$ and $(n, q) \neq (4, 5)$ (see [49, Example 2.3], [57, Table 3.5.A] and [10, Table 8.8]). Since x and y have at most 2 composition factors on V, containment in (a conjugate of) H implies that $m \leqslant n^2(q-1)/4$ (see [13, Remark 5.1(i)]), but it is easy to check that $m > n^2(q-1)/4$, so x and y are derangements as required.

Now assume $H \in \mathcal{C}_5$ is a subfield subgroup of type $\mathrm{GL}_n(q_0)$, where $q = q_0^k$ with k a prime divisor of f. We have $H \leqslant \mathrm{PGL}_n(q_0)$, and it is easy to see that $|\mathrm{PGL}_n(q_0)|$ is not divisible by a primitive prime divisor of $p^{f(n-\alpha)} - 1$ for $\alpha = 0$ or 1, whence x and y are derangements and the result follows.

Next assume $H \in \mathcal{C}_6$. Then by inspecting [49, Example 2.5] and [57, Proposition 4.6.6], we deduce that y is a derangement and that x has a fixed point only if $n = 2^k$ and $q = p \equiv 1 \pmod 4$ for some $k \geqslant 2$. Since $n/2$ is even, we note that $|x| = (q^{n/2} + 1)/(2, q - 1)$ is odd. But $H \leqslant 2^{2k}.\mathrm{Sp}_{2k}(2)$ and $|\mathrm{Sp}_{2k}(2)|$ is indivisible by $|x|$, so x must also be a derangement, and this completes the argument in this case.

By the main theorem of [49], both x and y are derangements if H is one of the tensor product subgroups in $\mathcal{C}_4 \cup \mathcal{C}_7$, so in order to complete the proof, we may assume

$$H \in \mathcal{C}_3 \cup \mathcal{C}_8 \cup \mathcal{S}.$$

Suppose $H \in \mathcal{C}_3$, in which case H is a field extension subgroup of type $\mathrm{GL}_{n/k}(q^k)$ for some prime divisor k of n. First assume $q \geqslant 3$ and set $E = z^G$, where $z = (A, J_{n-2})$ and $A \in \mathrm{SL}_2(q)$ has order $q + 1$. Then $G = E^2$ by Proposition 3.21, and we note that z^{q+1} has Jordan form (J_{n-2}, J_1^2). But there are no such elements in H, so z^{q+1}, and hence z itself, is a derangement and the result follows. Similarly, if $q = 2$, then $G = E^2$ for the class E of regular unipotent elements (see Proposition 3.21), and once again, the result follows since $E \cap H$ is empty.

Next assume $H \in \mathcal{C}_8$. There are several cases to work through:

(a) H is of type $\mathrm{U}_n(q_0)$ with $q = q_0^2$;
(b) H is of type $\mathrm{O}_n^\varepsilon(q)$ with q odd;
(c) H is of type $\mathrm{Sp}_n(q)$ with n even and $q \geqslant 2$.

First consider case (a), where we have $H \leqslant \mathrm{PGU}_n(q_0)$. We claim that x and y are derangements, where x and y are defined as in Proposition 3.20. To see this, first observe that every semisimple element in H has order at most $\alpha = q^{(n-1)/2} + (-1)^n$ by [44, Lemma 2.15]. If n is odd, then $m > \alpha$, and so the claim holds. Now assume n is even, in which case $|y| > \alpha$ and thus y is a derangement. And since $|x|$ is divisible by a primitive prime divisor of $p^{fn} - 1$, but $|H|$ is not, we conclude that x is also a derangement and the claim follows.

Finally, let us consider cases (b) and (c). Suppose $q = 2$ and $H = \mathrm{Sp}_n(2)$, so $n \geqslant 8$ is even. If $n \geqslant 30$, then Lemma 3.18 gives $G = \{1\} \cup CD$, where C and D are both conjugacy classes of elements of order at least $2^{n-3} - 1$ (see (3.3)). And since $|z| \leqslant 2^{n/2+1}$ for all $z \in H$ (see [44, Theorem 2.16]), we deduce that C and D comprise derangements and the result follows. For $8 \leqslant n \leqslant 28$, we can use MAGMA to determine all the conjugacy classes in G and H, which allows us to show that

$$\delta(G) \geqslant \frac{|\{x \in G \, : \, |x| \notin \omega(H)\}|}{|G|} > \frac{1}{2},$$

where $\omega(H) = \{|x| \, : \, x \in H\}$ is the spectrum of H. Therefore, $G = \Delta(G)^2$ by Lemma 3.22.

Now assume $q \geqslant 3$ and write $\mathbb{F}_q^\times = \langle \lambda \rangle$. Consider the conjugacy class $E = z^G$, where $z \in G$ is defined as follows:

$$z = \begin{cases} (A, J_1(\lambda^{-1}), J_{n-3}(1)) & \text{if } H \text{ is of type } \mathrm{O}_n(q) \text{ or } \mathrm{Sp}_n(q) \\ (B, J_{n-2}(1)) & \text{if } H \text{ is of type } \mathrm{O}_n^\pm(q). \end{cases}$$

Here $A, B \in \mathrm{GL}_2(q)$ are irreducible, with $\det(A) = \lambda$ and $\det(B) = 1$. By Proposition 3.21, we have $G = E^2$, and we claim that z is a derangement.

To see this, first assume H is of type $\mathrm{O}_n(q)$, so n is odd. Now z^{q^2-1} has Jordan form (J_{n-3}, J_1^3), but there are no such unipotent elements in H since all even size unipotent Jordan blocks must occur with an even multiplicity (see [68, Theorem 3.1(ii)], for example). Therefore, z is a derangement, and the result follows. Similarly, if H is of type $\mathrm{Sp}_n(q)$ with $q \geqslant 3$, then z is a derangement since odd size Jordan blocks have even multiplicity in the Jordan form of any unipotent element of H (see [68, Theorem 3.1(ii)] and [68, Lemma 6.2]). Finally, if n is even and H is of type $\mathrm{O}_n^\varepsilon(q)$, then z is a derangement because z^{q^2-1} has Jordan form (J_{n-2}, J_1^2), which is not compatible with the form of any unipotent element in H since the even-size Jordan block J_{n-2} has multiplicity 1.

To complete the proof, we may assume $H \in \mathcal{S}$, so H is almost simple with socle H_0. We claim that the elements x and y defined in Proposition 3.20 are derangements. Recall that $m = \min\{|x|, |y|\}$.

For the groups with $4 \leqslant n \leqslant 12$, we can read off the possibilities for H by inspecting the relevant tables in [10, Chapter 8], and it is straightforward to show that H does not contain any elements of order $|x|$ or $|y|$. For example, if $n = 6$, then $m = (q^3 + 1)/(2, q - 1)$, and by inspecting [10, Table 8.25], we see that either

$$H_0 \in \{\mathrm{M}_{12}, A_7, \mathrm{L}_2(11), \mathrm{L}_3(4), \mathrm{U}_4(3)\},$$

or $H_0 = \mathrm{L}_3(q)$ with q odd. In the latter case, [44, Theorem 2.16] gives $|z| \leqslant q^2 + q + 1 < m$ for all $z \in \mathrm{Aut}(H_0)$, so x and y are derangements. Similarly, in the remaining cases, one can check that $|z| \leqslant 28$ for all $z \in \mathrm{Aut}(H_0)$, which reduces the problem to $q \in \{2, 3\}$. Closer inspection of [10, Table 8.25] shows that $(q, H) = (3, \mathrm{M}_{12})$ is the only possibility, and the result follows since $|z| \leqslant 11 < 14 = m$ for all $z \in H$.

So for the remainder, we may assume $n \geqslant 13$. We now apply the main theorem of [49], using the fact that $|x|$ and $|y|$ are divisible by primitive prime divisors of $q^n - 1$ and $q^{n-1} - 1$, respectively. We consider [49, Examples 2.6-2.9] in turn.

First observe that Ex. 2.6(b,c) and Ex. 2.8 do not arise since $n \geqslant 13$. In Ex. 2.6(a), $H_0 = A_d$ is an alternating group and V is the fully deleted permutation module over $\mathbb{F}_p$. However, this representation embeds A_d in a symplectic or orthogonal group, so it does not arise. The relevant sporadic groups occurring in Ex. 2.7, as well as the cases in [49, Table 7], can all be eliminated by considering element orders, so it just remains to handle the cases recorded in [49, Table 8]. Here H_0 is a simple classical group over $\mathbb{F}_t$, where $(t, q) = 1$, and these possibilities can also be eliminated by considering element orders. For example, if $H_0 = \mathrm{PSp}_d(t)$ with t odd, then $n \geqslant (t^{d/2} - 1)/2$ and [44, Theorem 2.16] gives $|z| \leqslant (t^{d/2} + 1)/(t - 1)$ for all $z \in H$. But we have $m \geqslant 2^{(n-1)/2} + 1$ for all q, so $|z| < m$, and we conclude

that x and y are derangements. Similarly, if $H_0 = L_2(t)$ and $n = (t-1)/2$, then $t \geqslant 27$ since $n \geqslant 13$, and we have $|z| \leqslant t + 1$ for all $z \in H$. The result now follows since $m \geqslant 2^{(n-1)/2} + 1 > t + 1$.   □

3.5. Primitive groups

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with socle N and recall that the possibilities for G and N are described by the O'Nan-Scott theorem. Here our goal is to prove Theorem F, which states that $N = \Delta(N)^2$ if $|\Omega| \geqslant 3$, under the assumption that Conjecture 3.1 holds.

Proof of Theorem F. We consider the various possibilities for G in turn. If G is almost simple, then N is simple and transitive, so $N = \Delta(N)^2$ since we are assuming Conjecture 3.1 holds. If G is an affine group, or a twisted wreath product, then N is regular, and we deduce that $\delta(N) = 1 - |N|^{-1}$. So if $|N| > 2$, then $\delta(N) > 1/2$, and thus $N = \Delta(N)^2$ by Lemma 3.22. And if $|N| = 2$, then $G = N = S_2$, $\Omega = \{1, 2\}$, $\Delta(N) = \{(1, 2)\}$ and $\Delta(N)^2 = \{1\} \neq N$, which explains why we assume $|\Omega| \geqslant 3$ in Theorem F.

If G is a diagonal type group, then our proof of Theorem C(i) at the end of Section 2 shows that $\delta(N) \geqslant 2/3$, and thus $N = \Delta(N)^2$ by Lemma 3.22. Finally, let us assume $G \leqslant L \wr S_b$ is a product type group, where $b \geqslant 2$ and $L \leqslant \mathrm{Sym}(\Gamma)$ is a primitive almost simple or diagonal type group with socle $S = T^a$. Then $N = S^b = T^{ab}$ and G acts on $\Omega = \Gamma^b$ with the product action. Now

$$\Delta(N) = \{(x_1, \ldots, x_b) \in S^b \ : \text{ at least one } x_i \text{ is a derangement on } \Gamma\},$$

and thus $\Delta(N)$ contains $\Delta(S) \times S^{b-1}$. The result now follows since we have already shown that $\Delta(S)^2 = S$.   □

4. Soluble stabilisers

Let G be a (non-abelian) finite simple group and let $\mathcal{S}$ be the set of soluble maximal subgroups of G (note that $\mathcal{S}$ may be empty). In addition, let $\mathcal{S}^+$ be the set of soluble subgroups of G of the form $H = M \cap G$, where M is a maximal subgroup of an almost simple group with socle G. Note that if $H = M \cap G \in \mathcal{S}^+$, then the solubility of $\mathrm{Out}(G)$ implies that $GM/G \cong M/H$ is soluble, and thus M is also soluble. The subgroups in $\mathcal{S}$ and $\mathcal{S}^+$ were determined (up to conjugacy) by Li and Zhang in [62] (in particular, we refer the reader to Tables 14–20 in [62]).

The main result of this section is the following.

Theorem 4.1. *Let G be a finite simple transitive group with soluble point stabiliser H.*

 (i) *If $H \in \mathcal{S}^+$, then $\delta(G) \geqslant 89/325$, with equality if and only if $G = {}^2F_4(2)'$ and $H = 2^2.[2^8].S_3$.*
 (ii) *If $H \in \mathcal{S}$, then $G = \Delta(G)^2$.*

Note that part (i) establishes a slightly stronger version of Theorem B (see Remark 1.3(b)), while part (ii) is Theorem D(ii). In Section 4.5, we will use part (i) to prove Theorem C(ii) on primitive groups with soluble point stabilisers. In particular, in this section, we will complete the proofs of Theorems B, C and D.

Remark 4.2. Our proof of part (ii) of Theorem 4.1 shows that Conjecture 1.7 holds for every non-classical simple primitive group G with soluble point stabilisers. That is to say, in every case, we will exhibit classes C, D of derangements such that $G = \{1\} \cup CD$.

4.1. Sporadic groups

We begin the proof of Theorem 4.1 by assuming G is a sporadic group. Note that in the following result, H is an arbitrary soluble subgroup.

Proposition 4.3. *Let G be a transitive finite simple sporadic group with soluble point stabiliser H. Then* $G = \Delta(G)^2$ *and* $\delta(G) \geqslant 21/55$, *with equality if and only if* $G = \mathrm{M}_{11}$ *and* $H = \mathrm{U}_3(2).2$ *or* $2.S_4$.

Proof. The first claim $G = \Delta(G)^2$ follows from Proposition 3.4. More precisely, either $G = C^2$ for some conjugacy class C of derangements, or $(G, H) = (\mathrm{M}_{23}, 2^4.(15{:}4))$ and

$$G = \{1\} \cup C^2 = \{1\} \cup D^2 = CD,$$

where C and D are the two conjugacy classes in G of elements of order 23.

Now let us turn to the lower bound on $\delta(G)$. It will be convenient to define

$$\alpha_{\mathrm{s}}(G) = \min\{\delta(G, H) \ : \ H < G \text{ is soluble}\}. \tag{4.1}$$

Since $\alpha_{\mathrm{s}}(G) \geqslant \alpha(G)$, we only need to consider the groups with $\alpha(G) \leqslant 21/55$. By inspecting Table 1, it follows that $G \in \mathcal{A} \cup \mathcal{B}$, where

$$\mathcal{A} = \{\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{M}_{23}, \mathrm{M}_{24}, \mathrm{J}_3, \mathrm{McL}, \mathrm{HS}, \mathrm{Co}_3, \mathrm{O'N}\}$$
$$\mathcal{B} = \{\mathrm{Ly}, \mathrm{Th}\}.$$

For the groups in $\mathcal{A}$, we can use MAGMA to construct G as a primitive permutation group of minimal degree, together with a set of representatives of the conjugacy classes of elements and maximal subgroups of G. For each maximal subgroup H, it is then straightforward to determine the set of derangements on G/H, and we can read off $\delta(G, H)$. In particular, if H is soluble, then we find that $\delta(G, H) \geqslant 21/55$, with equality if and only if $G = \mathrm{M}_{11}$ and $H = \mathrm{U}_3(2).2$ or $2.S_4$. And if H is insoluble and $\delta(G, H) \leqslant 21/55$, then we construct a set of representatives of the conjugacy classes of maximal subgroups K of H, and in every case, one can check that $\delta(G, K) > 21/55$.

Finally, let us assume $G = \mathrm{Ly}$ or Th, and let H be a maximal subgroup of G. First we use GAP (as in the proof of Proposition 2.7) to show that $\delta(G, H) \leqslant 21/55$ if and only if $(G, H) = (\mathrm{Ly}, 2.A_{11})$ or $(\mathrm{Th}, 2^{1+8}.A_9)$.

Suppose $G = \mathrm{Ly}$. Here we use the MAGMA function MatrixGroup to obtain G as a subgroup of $\mathrm{GL}_{111}(5)$, and we construct $H = 2.A_{11}$ via the function MaximalSubgroups. We then construct a set of representatives of the conjugacy classes of maximal subgroups K of H, and in each case, we check that

$$\delta(G, K) \geqslant \frac{|\{x \in G \ : \ |x| \notin \omega(K)\}|}{|G|} > \frac{21}{55},$$

where $\omega(K) = \{|x| \ : \ x \in K\}$ is the spectrum of K. The case $G = \mathrm{Th}$ is entirely similar, working with a 248-dimensional matrix representation of G over $\mathbb{F}_2$. $\qquad\square$

Remark 4.4. We can compute $\alpha_s(G)$ precisely for all of the sporadic groups G recorded in Table 4. To explain how we do this, let d be a positive integer and let $\mathcal{M}_d$ be a set of representatives of the conjugacy classes in G of subgroups K such that

$$K = K_d < K_{d-1} < \cdots < K_1 < K_0 = G,$$

where K_i is maximal in K_{i-1} for all i. Setting $\beta_0(G) = 1$, we define

$$\beta_d(G) = \min\{\beta_{d-1}(G), \ \delta(G, H) \ : \ H \in \mathcal{M}_d \text{ is soluble}\}$$
$$\gamma_d(G) = \min\{1, \ \delta(G, H) \ : \ H \in \mathcal{M}_d \text{ is insoluble}\},$$

and we note that $\alpha_s(G) = \beta_d(G)$, where $d \geqslant 1$ is minimal such that $\beta_d(G) \leqslant \gamma_d(G)$. This observation allows us to compute $\alpha_s(G)$ for each of the groups in Table 4 by proceeding as in the proof of Proposition 4.3, working with a permutation representation of G and repeatedly applying the function MaximalSubgroups to descend deeper in to the subgroup lattice of G.

Table 4. *The values of $\alpha_s(G)$ for some alternating and sporadic groups.*

G	$\alpha_s(G)$	G	$\alpha_s(G)$
A_5	1/3	M_{11}	21/55
A_6	2/5	M_{12}	244/495
A_7	17/35	M_{22}	401/693
A_8	17/35	M_{23}	982/1771
A_9	227/560	M_{24}	87749/161920
A_{10}	7141/12600	J_1	573/1463
A_{11}	47063/69300	J_2	3251/6048
A_{12}	66541/103950	J_3	1398703/2511648
A_{13}	48632009/64864800	HS	108805/177408
A_{14}	1319450477/1816214400	McL	10673/18711
A_{15}	1728445871/2421619200	He	130507/217600
A_{16}	541166748751/697426329600	Suz	1030209/1601600
		Ru	1137154/1781325
		O'N	7129127/11111485
		Co_3	54763537/82627776
		Co_2	78264622699/112814456832
		Fi_{22}	18609741/25625600

4.2. Alternating groups

Proposition 4.5. *Let $G = A_n$ be a transitive finite simple alternating group with soluble point stabiliser H.*

(i) *We have $G = \Delta(G)^2$.*

(ii) *If $5 \leqslant n \leqslant 16$, then $\delta(G) \geqslant 1/3$, with equality if and only if $(G, H) = (A_5, D_{10})$.*

(iii) *If $n \geqslant 17$ and $H \in \mathcal{S}^+$, then $\delta(G) \geqslant 4531887936311/5230697472000$.*

Proof. Part (i) is a special case of Proposition 3.5. More precisely, either $G = C^2$ for some conjugacy class C of derangements, or

$$(G, H) \in \{(A_5, A_4),\ (A_5, S_3),\ (A_8, 2^4{:}(S_3 \times S_3))\}$$

and $G = \{1\} \cup CD$, where C and D are the two classes of elements order 5 (for $G = A_5$) or 7 (for $G = A_8$).

Part (ii) can be checked using MAGMA and the approach described in Remark 4.4. In particular, we can compute $\alpha_s(G)$ precisely for all $5 \leqslant n \leqslant 16$ (see (4.1) and Table 4).

For the remainder, we may assume $n \geqslant 17$ and $H \in \mathcal{S}^+$. Then the solubility of H implies that H acts primitively on $\{1, \ldots, n\}$, which in turn means that $n = p^d$ is a prime power and $H = \mathrm{AGL}_d(p) \cap G$. Moreover, since $n \geqslant 17$, it follows that $d = 1$ and $H = \mathrm{AGL}_1(p) \cap G = p{:}(p-1)/2$.

Suppose $x \in H$ has order r. Then either $r = p$ and x is a p-cycle, or r divides $(p-1)/2$ and x has cycle-type $(r^{(p-1)/r}, 1)$ as an element of G. (Note that H contains a Sylow p-subgroup of G, so every p-cycle in G has fixed points on Ω.) So if N denotes the number of elements in G with fixed points on Ω, then

$$N = 1 + (p-1)! + \sum_{r \in \Lambda} \frac{p!}{((p-1)/r)!\, r^{(p-1)/r}},$$

where Λ is the set of divisors $r \geqslant 2$ of $(p-1)/2$. For $17 \leqslant p < 100$, it is now entirely straightforward to check that the lower bound in part (iii) is satisfied (with equality if $p = 17$), so we may assume $p > 100$.

For $r \in \Lambda$, set

$$f(r) = \frac{p!}{((p-1)/r)!\, r^{(p-1)/r}}.$$

We claim that $f(r)$ is maximal when $r = (p-1)/2$. To see this, simply observe that $((p-1)/r)! \geqslant 2$ and $r^{(p-1)/r}$ is decreasing as a function of r, so we have $r^{(p-1)/r} \geqslant ((p-1)/2)^2$, and the claim follows.

Therefore,

$$f(r) \leqslant 2\left(\frac{p!}{(p-1)^2}\right),$$

and using the crude bound $|\Lambda| \leqslant 2\sqrt{(p-1)/2}$, we deduce that

$$N \leqslant 1 + (p-1)! + 2\sqrt{(p-1)/2} \cdot 2\left(\frac{p!}{(p-1)^2}\right).$$

In turn, this yields

$$\delta(G) \geqslant \frac{2\left(\frac{p!}{2} - 1 - (p-1)! - 2\sqrt{(p-1)/2} \cdot \frac{2(p!)}{(p-1)^2}\right)}{p!} = 1 - \frac{2}{p!} - \frac{2}{p} - \frac{8\sqrt{(p-1)/2}}{(p-1)^2},$$

and we conclude that $\delta(G) > 0.97$ for all $p > 100$. □

4.3. Exceptional groups

Next we assume G is a simple exceptional group of Lie type. Our main result is the following, which establishes strong forms of Theorems B and D(ii) for exceptional groups. Note that the possibilities for G and H are recorded in [62, Table 20].

Proposition 4.6. *Let G be a transitive finite simple exceptional group of Lie type with soluble point stabiliser H.*

 (i) *If $H \in \mathcal{S}^+$, then $\delta(G) \geqslant 89/325$, with equality if and only if $G = {}^2F_4(2)'$ and $H = 2^2.[2^8].S_3$.*
 (ii) *If $H \in \mathcal{S}$, then $G = \{1\} \cup CD$ for classes C, D of derangements.*

We begin by recording two preliminary lemmas. Recall that a conjugacy class x^G is *real* if $x^{-1} \in x^G$.

Lemma 4.7. *Let G be a finite simple exceptional group of Lie type over $\mathbb{F}_q$ and assume $G \neq E_6(q), {}^2E_6(q), G_2(2)'$. Then every semisimple conjugacy class in G is real.*

Proof. The groups ${}^2G_2(3)'$ and ${}^2F_4(2)'$ can be checked directly. In each of the remaining cases, the result follows from [80, Proposition 3.1] since the Weyl group of G contains a central involution. □

In the next lemma, G is a simple group of Lie type over $\mathbb{F}_q$, where $q = p^f$ and p is a prime, and h is the *Coxeter number* of G. The latter is defined by

$$h = \frac{\dim \bar{G}}{\operatorname{rank} \bar{G}} - 1,$$

where $\bar{G}$ is the ambient simple algebraic group defined over the algebraic closure of $\mathbb{F}_q$. So for example, the Coxeter number of $E_8(q)$ is $248/8 - 1 = 30$. Also recall that an element $x \in G$ is *regular semisimple* if the connected component of $C_{\bar{G}}(x)$ is a maximal torus of $\bar{G}$. This is equivalent to the condition that $|C_G(x)|$ is indivisible by p.

For the proof of the following lemma, we thank Martin Liebeck for drawing our attention to [53, Section 4], which plays a key role in the argument.

Lemma 4.8. *Let $G \neq \operatorname{Sp}_4(2)', G_2(2)', {}^2G_2(3)'$ be a finite simple group of Lie type with Coxeter number h and suppose $x \in G$ is semisimple. Then x is regular only if $|x| \geqslant h$.*

Proof. The claim is trivial if $h = 2$, and it can be checked directly for $G = {}^2F_4(2)'$, so we may assume $h \geqslant 3$ and $G \neq {}^2F_4(2)'$. Set $|x| = d$.

Let $\bar{G} = X_{\mathrm{sc}}$ and $\bar{L} = X_{\mathrm{ad}}$ be the corresponding simply connected and adjoint simple algebraic groups defined over the algebraic closure of $\mathbb{F}_q$ and write $G = O^{p'}(\bar{L}_\sigma)$ for a suitable Steinberg endomorphism σ of $\bar{L}$. We may assume that x is the image of $y \in \bar{G}$ under the natural map $\bar{G} \to X_{\mathrm{ad}}$. Embed y in a maximal torus $\bar{T}$ of $\bar{G}$ and let $\{\alpha_1, \ldots, \alpha_r\}$ be a set of simple roots for the corresponding root system of $\bar{G}$. Let $\alpha_0 = \sum_i m_i \alpha_i$ be the highest root and note that $\sum_i m_i = h - 1$.

The structure of $C_{\bar{G}}(y)$ is described in [53, Section 4]. In particular, from the discussion on [53, p.315], it follows that there exist integers $b_i \geqslant 0$ such that $\sum_i b_i m_i \leqslant d$ with the property that $C_{\bar{G}}(y)$ is a maximal torus only if each b_i is positive and $d > \sum_i b_i m_i$. Therefore, x is regular only if

$$d \geqslant 1 + \sum_i m_i = h,$$

and the result follows. □

It is convenient to use computational methods to prove Proposition 4.6 for some of the small exceptional groups.

Lemma 4.9. *The conclusion to Proposition 4.6 holds if G is one of the following:*

$$^2G_2(3)',\ G_2(2)',\ G_2(3),\ ^2F_4(2)',\ ^3D_4(2),\ ^3D_4(3).$$

Proof. We can use MAGMA [8] to handle these cases, working with a primitive permutation representation of G of minimal degree. First we construct the character table of G, and we use Lemma 3.2 to identify all the pairs of classes (C, D) with $G = \{1\} \cup CD$. Then for each $H \in \mathcal{S}^+$, we determine the set of derangements for the action of G on G/H, and we check that $\delta(G, H) \geqslant 89/325$, with equality if and only if $G = {}^2F_4(2)'$ and $H = 2^2.[2^8].S_3$. For example, if $G = {}^2G_2(3)' \cong L_2(8)$, then $\delta(G, H) \geqslant 3/7$, with equality if and only if $H = D_{18}$. Finally, in every case, we identify two classes C, D of derangements with $G = \{1\} \cup CD$. □

We now partition our analysis of the remaining exceptional groups according to the structure of the point stabiliser H.

Lemma 4.10. *The conclusion to Proposition 4.6 holds if H is a parabolic subgroup of G.*

Proof. Suppose $H \in \mathcal{S}^+$ is a parabolic subgroup of G, in which case the possibilities for G and H are recorded in parts (ii) and (iii) of [14, Lemma 5.4].

We begin by assuming (G, H) is one of the cases listed in [14, Lemma 5.4(ii)]. In view of Lemma 4.9, we can assume $G = F_4(2)$ and $H = [2^{22}]:S_3^2$. Here H is non-maximal in G, but $H.2$ is maximal in $L = \mathrm{Aut}(G) = G.2$, so $H \in \mathcal{S}^+ \setminus \mathcal{S}$ and we just need to bound $\delta(G, H)$. To do this, we first use MAGMA to construct G as a permutation group of degree 139776, and then we obtain H by constructing the maximal subgroups of $\mathrm{Aut}(G)$. In the usual manner, working with the conjugacy classes in G and H, we compute $\delta(G, H) = 5166407/7309575$.

To complete the proof of the lemma, it remains to consider the three infinite families recorded in [14, Table 2]:

(a) $G = {}^2B_2(q)$ and $H = [q^2]:(q - 1)$, where $q = 2^{2m+1} \geqslant 8$.
(b) $G = {}^2G_2(q)$ and $H = [q^3]:(q - 1)$, where $q = 3^{2m+1} \geqslant 27$.
(c) $G = G_2(q)$ and $H = [q^6]:(q - 1)^2$, where $q = 3^m \geqslant 9$.

In cases (a) and (b), Theorem 3.13 implies that $G = C^2$ for some conjugacy class C of derangements. Also note that $H \in \mathcal{S}^+ \setminus \mathcal{S}$ in (c), so in all three cases, it just remains to show that $\delta(G, H) > 89/325$.

First consider case (a). Let $\chi = 1_H^G$ be the corresponding permutation character and note that $\chi = 1 + \mathrm{St}$, where 1 and St denote the trivial and Steinberg characters of G, respectively (for example, see [60, p.416]). By inspecting the character table of G (see [79, Theorem 13]), we deduce that $x \in G$

is a derangement if and only if x is a regular semisimple element with $|C_G(x)| = q \pm \sqrt{2q} + 1$. As a consequence,

$$|\Delta(G,H)| = \frac{1}{4}(q + \sqrt{2q}) \cdot \frac{|G|}{q + \sqrt{2q} + 1} + \frac{1}{4}(q - \sqrt{2q}) \cdot \frac{|G|}{q - \sqrt{2q} + 1} = \frac{1}{2}q^3(q - 1)^2,$$

and thus

$$\delta(G,H) = \frac{q(q-1)}{2(q^2+1)} \geqslant \frac{28}{65}$$

for all $q \geqslant 8$.

Case (b) is very similar. Once again, we have $\chi = 1 + \mathrm{St}$, and we compute

$$|\Delta(G,H)| = \frac{1}{6}(q + \sqrt{3q}) \cdot \frac{|G|}{q + \sqrt{3q} + 1} + \frac{1}{6}(q - \sqrt{3q}) \cdot \frac{|G|}{q - \sqrt{3q} + 1} + \frac{1}{6}(q - 3) \cdot \frac{|G|}{q + 1},$$

which yields

$$\delta(G,H) = \frac{q^3 - 2q^2 - 1}{2(q^3 + 1)} \geqslant \frac{2278}{4921}.$$

Finally, we turn to case (c). If $x \in G$ is a regular semisimple element with $|C_G(x)| = q^2 \pm q + 1$ or $(q + 1)^2$, then $(|H|, |C_G(x)|) \leqslant 4$, and thus x is a derangement by Lemma 4.8 (note that $h = 6$). By inspecting [69], we deduce that

$$\delta(G,H) \geqslant \frac{1}{12}\left(\frac{2(q-1)(q+2)}{q^2 + q + 1} + \frac{2(q+1)(q-2)}{q^2 - q + 1} + \frac{q(q-4)}{(q+1)^2}\right) > \frac{89}{325}$$

for all $q \geqslant 9$. $\qquad\square$

Next we consider the groups where H is the normaliser of a maximal torus. These cases require a detailed analysis, and we divide the proof into two separate lemmas.

In the proof of the following result, we thank Gunter Malle for his assistance with a Chevie [43] computation arising when $G = {}^2F_4(q)$ in Case 4 of the proof.

Lemma 4.11. *The conclusion to Proposition 4.6 holds if $H = N_G(T)$ is the normaliser of a maximal torus and $G \neq F_4(q), E_6^\varepsilon(q), E_8(q)$.*

Proof. The possibilities for H can be read off from [67, Table 5.2], and we divide the proof into a number of separate cases. Note that for the rank one groups ${}^2B_2(q)$ and ${}^2G_2(q)$, we have already shown that $G = \{1\} \cup CD$ for classes C, D of derangements in Theorem 3.13.

Case 1. $G = {}^2B_2(q)$

Here $q \geqslant 8$, and H is either $D_{2(q-1)}$ or $(q \pm \sqrt{2q} + 1){:}4$. If $H = D_{2(q-1)}$, then every semisimple element $x \in G$ with $|C_G(x)| = q \pm \sqrt{2q} + 1$ is a derangement (since $(|H|, |C_G(x)|) = 1$), and thus

$$\delta(G,H) \geqslant \frac{1}{4}\left(\frac{q + \sqrt{2q}}{q + \sqrt{2q} + 1} + \frac{q - \sqrt{2q}}{q - \sqrt{2q} + 1}\right) \geqslant \frac{28}{65}.$$

Similarly, if $H = (q + \varepsilon\sqrt{2q} + 1){:}4$, then every semisimple element $x \in G$ with $|C_G(x)| = q - 1$ or $q - \varepsilon\sqrt{2q} + 1$ is a derangement (since $(|H|, |C_G(x)|) = 1$), whence

$$\delta(G, H) \geqslant \frac{1}{2}\left(\frac{q - 2}{q - 1} + \frac{q - \varepsilon\sqrt{2q}}{2(q - \varepsilon\sqrt{2q} + 1)}\right) \geqslant \frac{22}{35}.$$

Case 2. $G = {}^2G_2(q)$, $q \geqslant 27$

This is very similar to the previous case (note that the group ${}^2G_2(3)'$ was handled in Lemma 4.9). If $H = (q + 1){.}6$, then each element $x \in G$ with $|C_G(x)| = q \pm \sqrt{3q} + 1$ is a derangement (once again, we have $(|H|, |C_G(x)|) = 1$), and thus

$$\delta(G, H) \geqslant \frac{1}{6}\left(\frac{q + \sqrt{3q}}{q + \sqrt{3q} + 1} + \frac{q - \sqrt{3q}}{q - \sqrt{3q} + 1}\right) \geqslant \frac{225}{703}.$$

Similarly, if $H = (q + \varepsilon\sqrt{3q} + 1){.}6$ and $|C_G(x)| = q - 1$ or $q - \varepsilon\sqrt{3q} + 1$, then we have $|x| > 2$ and $(|H|, |C_G(x)|) \leqslant 2$, so x is a derangement and we deduce that

$$\delta(G, H) \geqslant \frac{1}{6}\left(\frac{3(q - 3)}{q - 1} + \frac{q - \varepsilon\sqrt{3q}}{q - \varepsilon\sqrt{3q} + 1}\right) \geqslant \frac{153}{247}.$$

Case 3. $G = G_2(q)$

Next assume $G = G_2(q)$. By inspecting [67, Table 5.2], we see that $p = 3$, $q \geqslant 9$ and $H \in \mathcal{S}^+ \setminus \mathcal{S}$, so we just need to verify the lower bound $\delta(G) > 89/325$.

For $H = (q - \varepsilon)^2{.}D_{12}$, it is clear that every regular semisimple element $x \in G$ with $|C_G(x)| = q^2 \pm q + 1$ is a derangement, and by inspecting [69], we deduce that

$$\delta(G, H) \geqslant \frac{1}{6}\left(\frac{q^2 + q}{q^2 + q + 1} + \frac{q^2 - q}{q^2 - q + 1}\right) \geqslant \frac{2187}{6643}$$

for all $q \geqslant 9$. Similarly, if $H = (q^2 + \varepsilon q + 1){.}6$, then each $x \in G$ with $|C_G(x)| = q^2 - 1$ or $q^2 - \varepsilon q + 1$ is a derangement and it is easy to check that this gives $\delta(G, H) > 89/325$.

Case 4. $G = {}^2F_4(q)$, $q \geqslant 8$

Next suppose $G = {}^2F_4(q)$ with $q \geqslant 8$ (see Lemma 4.9 for $G = {}^2F_4(2)'$). If C is a conjugacy class of elements of order $q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1$, then [47, Theorem 7.3] implies that $G = C^2$ (noting that C is real by Lemma 4.7). And by arguing as in the proof of [47, Theorem 7.3], using the GAP package Chevie [43], one can show that $G = D^2$ when D is a class of elements of order $q^2 - \sqrt{2q^3} + q - \sqrt{2q} + 1$.

First assume $H = (q + 1)^2{.}GL_2(3)$. If $x \in G$ is a regular semisimple element with

$$|C_G(x)| \in \{q^2 - q + 1,\ (q - 1)(q \pm \sqrt{2q} + 1),\ q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1\},$$

then x is a derangement (in each case, $(|H|, |C_G(x)|) = 1$ or 3), and by inspecting [76, Table IV], we deduce that

$$\delta(G,H) \geqslant \frac{(q-2)(q+1)}{6(q^2-q+1)} + \frac{(q-2)(q+\sqrt{2q})}{8(q-1)(q+\sqrt{2q}+1)} + \frac{(q-2)(q-\sqrt{2q})}{8(q-1)(q-\sqrt{2q}+1)}$$
$$+ \frac{q^2+\sqrt{2q^3}+q+\sqrt{2q}}{12(q^2+\sqrt{2q^3}+q+\sqrt{2q}+1)} > \frac{89}{325}$$

for all $q \geqslant 8$. In addition, $G = C^2$ for the class C of derangements defined above.

Similarly, if $H = (q + \varepsilon\sqrt{2q} + 1)^2.(4 \circ \mathrm{GL}_2(3))$, then every regular semisimple element $x \in G$ with $|C_G(x)| = q^2 - q + 1$, $q^2 - 1$ or $q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1$ is a derangement and the desired bound $\delta(G,H) > 89/325$ quickly follows. And finally, if $H = (q^2 + \varepsilon\sqrt{2q^3} + q + \varepsilon\sqrt{2q} + 1).12$, then each $x \in G$ with $|C_G(x)| = q^2 - q + 1$, $q^2 - 1$ or $q^2 - \varepsilon\sqrt{2q^3} + q - \varepsilon\sqrt{2q} + 1$ is a derangement, and we deduce that $\delta(G,H) > 89/325$. Note that in each of these cases, either C or D is a class of derangements, and we have $G = C^2 = D^2$.

By inspecting [67, Table 5.2], it just remains to consider the groups $G = {}^3D_4(q)$ in order to complete the proof of the lemma.

Case 5. $G = {}^3D_4(q)$

In view of Lemma 4.9, we may assume $q \geqslant 4$. We refer the reader to [27] for information on the semisimple conjugacy classes in G (for example, the number of semisimple classes with a given centraliser structure can be read off from [27, Table 4.4]). By [47, Theorem 7.3] and Lemma 4.7, we have $G = C^2$, where C is a class of elements of order $q^4 - q^2 + 1$.

Suppose $H = (q^4 - q^2 + 1).4$. If $x \in G$ is regular semisimple with $|C_G(x)| = (q^3 - \varepsilon)(q - \varepsilon)$, $(q^3 + \varepsilon)(q - \varepsilon)$ or $(q^2 + \varepsilon q + 1)^2$, then $(|H|, |C_G(x)|) \leqslant 4$, and thus x, is a derangement by Lemma 4.8. By adding up the contribution to $\delta(G)$ from these elements, we get

$$\delta(G,H) \geqslant \frac{1}{24}\left(\frac{q^4+2q^3-q^2-2q}{(q^2+q+1)^2} + \frac{q^4-2q^3-q^2+2q}{(q^2-q+1)^2} + \frac{2(q^4-4q^3+2q^2-2q+12)}{(q^3-1)(q-1)} \right.$$
$$\left. + \frac{2(q^4-2q^3+2q^2-4q)}{(q^3+1)(q+1)} + \frac{6(q^4-2q)}{(q^3-1)(q+1)} + \frac{6(q^4-2q^3)}{(q^3+1)(q-1)} \right) > \frac{89}{325}$$

for all $q \geqslant 4$. In addition, if we let $A = x^G$ and $B = y^G$, where $|C_G(x)| = (q^2 + q + 1)^2$ and $|C_G(y)| = (q^2 - q + 1)^2$, then we can use Chevie [43] to show that $G = \{1\} \cup AB$. In particular, $G = \Delta(G)^2$.

Finally, let us assume $H = (q^2 + \varepsilon q + 1)^2.\mathrm{SL}_2(3)$. First note that each element $x \in G$ with $|C_G(x)| = q^4 - q^2 + 1$ is a derangement (since $(|H|, |C_G(x)|) = 1$), and we have $G = C^2$ as noted above. In addition, elements with $|C_G(x)| = (q^2 - \varepsilon q + 1)^2$ are also derangements since $(|H|, |C_G(x)|) = 1$ or 3. It follows that

$$\delta(G,H) \geqslant \frac{1}{24}\left(\frac{6(q^4-q^2)}{q^4-q^2+1} + \frac{q^4+2\varepsilon q^3-q^2-2\varepsilon q}{(q^2+\varepsilon q+1)^2} \right) \geqslant \frac{11345}{40729} > \frac{89}{325}$$

for all $q \geqslant 4$. □

Lemma 4.12. *The conclusion to Proposition 4.6 holds if $H = N_G(T)$ is the normaliser of a maximal torus.*

Proof. In view of Lemma 4.11, we may assume $G = F_4(q)$, $E_6^\varepsilon(q)$ or $E_8(q)$. By inspecting [67, Table 5.2], one of the following holds:

(a) $G = F_4(q)$, q even and $H \in \mathcal{S}^+ \setminus \mathcal{S}$;
(b) $G = E_6^\varepsilon(q)$ and $T = \frac{1}{e}(q^2 + \varepsilon q + 1)^3$, where $e = (3, q - \varepsilon)$;
(c) $G = E_8(q)$ and $T = (q^4 - q^2 + 1)^2$ or $q^8 + \varepsilon q^7 - \varepsilon q^5 - q^4 - \varepsilon q^3 + \varepsilon q + 1$ with $\varepsilon = \pm$.

Recall Lemma 4.8, which states that $|x| \geq h$ for every regular semisimple element $x \in G$, where h is the Coxeter number of G (so $h = 12, 12, 30$ in cases (a),(b),(c) above). We refer the reader to [69] for a convenient source of detailed information on the semisimple conjugacy classes in G. We will write Φ_i for the i-th cyclotomic polynomial in $\mathbb{Z}[q]$.

Case 1. $G = F_4(q)$, q even

Here $H \in \mathcal{S}^+ \setminus \mathcal{S}$, so it suffices to verify the bound $\delta(G) > 89/325$. If $q = 2$, then we have $H = 7^2.(3 \times \mathrm{SL}_2(3)) = N_G(P)$, where P is a Sylow 7-subgroup of G, and with the aid of MAGMA, it is easy to check the result. For the remainder, we may assume $q \geq 4$.

Suppose $H = (q-1)^4.W$, where W is the Weyl group of G (this is a soluble group of order 1152). According to [67, Table 5.2], we may assume $q \geq 8$. Let $x \in G$ be a regular semisimple element with

$$|C_G(x)| \in \{\Phi_8, \ \Phi_{12}, \ \Phi_2^2\Phi_6, \ \Phi_2^2\Phi_4, \ \Phi_3^2, \ \Phi_6^2\}.$$

Since $(|H|, |C_G(x)|) \leq 9$, Lemma 4.8 implies that x is a derangement, and by inspecting [69], we deduce that

$$\delta(G, H) \geq \frac{q^4}{8\Phi_8} + \frac{q^2(q^2-1)}{12\Phi_{12}} + \frac{(q+1)(q^3 - 3q^2 + 4q - 4)}{18\Phi_2^2\Phi_6} + \frac{q^3(q-2)}{32\Phi_2^2\Phi_4}$$
$$+ \frac{(q-1)(q^3 + 3q^2 - 2q - 8)}{72\Phi_3^2} + \frac{q(q-1)(q^2 - q - 6)}{72\Phi_6^2} > \frac{89}{325}$$

for all $q \geq 8$.

Next assume $H = (q+1)^4.W$ with $q \geq 4$. Here each regular semisimple element $x \in G$ with $|C_G(x)| = \Phi_8$, Φ_{12}, $\Phi_1^2\Phi_3$, $\Phi_1^2\Phi_4$, Φ_3^2 or Φ_6^2 is a derangement (as above, $(|H|, |C_G(x)|) < h$ in each case), and by counting these elements, we get $\delta(G, H) > 89/325$ for all $q \geq 8$. For $q = 4$, we also claim that each $x \in G$ with $|C_G(x)| = \Phi_1\Phi_2\Phi_6 = 195$ is a derangement. To see this, first note that $C_G(x) = T$ is a cyclic maximal torus (see [26]) and we have $(|H|, |C_G(x)|) = 15 = q^2 - 1$. We can embed T in a subgroup $M = \mathrm{Sp}_2(4) \times \mathrm{Sp}_6(4)$ of G, and we observe that $C_M(S) = 3 \times \mathrm{GU}_3(4)$, where S is the unique subgroup of T of order 15. So if x has fixed points, then $T < C_M(x)$, which is absurd. This justifies the claim. By including the contribution from these elements, it is easy to check that $\delta(G, H) > 89/325$.

Next assume $H = (q^2 + q + 1)^2.(3 \times \mathrm{SL}_2(3))$ with $q \geq 4$. Here we find that every regular semisimple element $x \in G$ with $|C_G(x)| = \Phi_8$, Φ_{12}, $\Phi_2^2\Phi_6$, $\Phi_2^2\Phi_4$, Φ_6^2 or $\Phi_1\Phi_2\Phi_6$ is a derangement (since $(|H|, |C_G(x)|) < h$), and we get $\delta(G, H) > 89/325$ by adding up the contribution from these elements.

Similarly, if $H = (q^2 - q + 1)^2.(3 \times \mathrm{SL}_2(3))$ and $q \geq 4$, then each element with $|C_G(x)|$ one of Φ_8, Φ_{12}, $\Phi_1^2\Phi_3$, $\Phi_1^2\Phi_4$ or Φ_3^2 is a derangement, and this yields $\delta(G, H) > 89/325$ for $q \geq 16$. If $q \in \{4, 8\}$ and $|C_G(x)| = \Phi_1\Phi_2\Phi_3$, then we get $(|H|, |C_G(x)|) = 9$, so these regular semisimple elements are also derangements and this yields $\delta(G, H) > 89/325$, as required.

The remaining two cases with $G = F_4(q)$ can be handled in a very similar fashion. If we take $H = (q^2 + 1)^2.(4 \circ \mathrm{GL}_2(3))$, then each regular semisimple element $x \in G$ with $|C_G(x)| = \Phi_8$, Φ_{12}, $\Phi_1^2\Phi_3$, $\Phi_2^2\Phi_6$, Φ_3^2, Φ_6^2 or $\Phi_1\Phi_2\Phi_3$ is a derangement (indeed, in each case, $(|H|, |C_G(x)|) \leq 3$) and the desired bound follows. Similarly, if $H = (q^4 - q^2 + 1).12$, then the elements $x \in G$ with $|C_G(x)| = \Phi_8$, $\Phi_1^2\Phi_3$, $\Phi_2^2\Phi_6$, Φ_3^2, Φ_6^2 or $\Phi_1\Phi_2\Phi_3$ are derangements, and once again, we conclude that $\delta(G, H) > 89/325$.

Case 2. $G = E_6(q)$

Next assume $G = E_6(q)$ and $H = (q^2 + q + 1)^3/e.3^{1+2}.\mathrm{SL}_2(3)$, where $e = (3, q-1)$. First note that every element in G of order Φ_8 and Φ_9/e is a derangement (indeed, $|H|$ is indivisible by these two numbers), whence [47, Theorem 7.7] implies that there exist classes C, D of derangements with $G = \{1\} \cup CD$. Therefore, it remains to show that $\delta(G) > 89/325$.

If $q = 2$, then H is the normaliser of a Sylow 7-subgroup, and it is easy to verify the desired bound using MAGMA. For $q \geq 3$, it will be convenient to work in the quasisimple group $L = Z.G$,

where $Z = Z(L)$ has order e. Then $H = J/Z$ with $J = (q^2 + q + 1)^3.3^{1+2}.\mathrm{SL}_2(3)$, and we note that $\delta(G) = \delta(L, J)$.

Let $x \in L$ be a regular semisimple element. If $|C_L(x)| = \Phi_9$, then $(|J|, |C_L(x)|) = 1$, and by inspecting [69], we see that there are at least $\Phi_1\Phi_3(q^3 + 2)/9$ distinct L-classes of such elements. Next assume $|C_L(x)| = \Phi_1\Phi_2\Phi_8$, in which case $C_L(x) = T$ is a cyclic maximal torus (see [26]) and $(|J|, |C_L(x)|)$ divides $q^2 - 1$. So if x has fixed points on L/J, then $x \in S < T$, where S is the unique subgroup of T of order $q^2 - 1$. But T is contained in a subgroup $M < G$ of type $(q^2 - 1) \times \Omega_8^-(q)$, and we deduce that $T < C_M(x)$, which is absurd since $C_L(x) = T$. Therefore, x is a derangement on L/J, and by inspecting [69], we read off that L has at least $\Phi_1^2\Phi_2^2\Phi_4/8$ distinct classes of such elements.

A similar argument shows that each $y \in L$ with $|C_L(y)| = \Phi_1\Phi_2\Phi_4\Phi_6$ is a derangement. To see this, first note that $C_L(y) = T$ is a cyclic maximal torus and $(|J|, |C_L(y)|)$ divides $(q - 1)(q^3 + 1)$. Let S be the unique subgroup of T of order $(q - 1)(q^3 + 1)$ and note that $y \in S$ if y has fixed points. Now T is contained in a subgroup M of type $(q - 1) \times \Omega_{10}^+(q)$, and we observe that $T < C_M(S)$. So if y has fixed points, then $T < C_M(y)$, and we reach a contradiction as before. Therefore, y is a derangement, and [69] indicates that L has at least $q^3\Phi_1^2\Phi_2/12$ classes of regular semisimple elements of this form.

Putting this together, we deduce that

$$\delta(G) \geqslant \frac{\Phi_1\Phi_3(q^3 + 2)}{9\Phi_9} + \frac{\Phi_1^2\Phi_2^2\Phi_4}{8\Phi_1\Phi_2\Phi_8} + \frac{q^3\Phi_1^2\Phi_2}{12\Phi_1\Phi_2\Phi_4\Phi_6} > \frac{89}{325}$$

for all $q \geqslant 3$.

Case 3. $G = {}^2E_6(q)$

Next assume $G = {}^2E_6(q)$ and $H = (q^2 - q + 1)^3/e.3^{1+2}.\mathrm{SL}_2(3)$, where $e = (3, q + 1)$ and $q \geqslant 3$ (see [67, Table 5.2]). This is essentially identical to the previous case, and so we only give brief details.

First we note that $|H|$ is indivisible by Φ_8 and Φ_{18}/e, so by appealing to [47, Theorem 7.7], we deduce that $G = \{1\} \cup CD$, where C and D are conjugacy classes of derangements.

As in Case 2, it is convenient to work in the quasisimple group $L = Z.G$, and we set $H = J/Z$, where $Z = Z(L)$ has order e. By arguing as above, we can show that every regular semisimple element $x \in L$ with $|C_L(x)| = \Phi_{18}$, $\Phi_1\Phi_2\Phi_8$ or $\Phi_1\Phi_2\Phi_3\Phi_4$ is a derangement, and then by inspecting [69], we conclude that

$$\delta(G) \geqslant \frac{\Phi_2\Phi_6(q^3 - 2)}{9\Phi_{18}} + \frac{\Phi_1^2\Phi_2^2\Phi_4}{8\Phi_1\Phi_2\Phi_8} + \frac{q^3\Phi_1\Phi_2^2}{12\Phi_1\Phi_2\Phi_3\Phi_4} > \frac{89}{325}$$

for all $q \geqslant 3$.

Case 4. $G = E_8(q)$

Finally, let us assume $G = E_8(q)$, in which case H is one of the following:

$$(q^4 - q^2 + 1)^2.(12 \circ \mathrm{GL}_2(3)), \quad (q^8 \pm q^7 \mp q^5 - q^4 \mp q^3 \pm q + 1):30.$$

First observe that every element in G of order Φ_{20} or Φ_{24} is a derangement (since $|H|$ is indivisible by these numbers), so [47, Theorem 7.7] implies that $G = \{1\} \cup CD$ for classes C, D of derangements. Therefore, we just need to verify the bound $\delta(G) > 89/325$, and we will consider the three possibilities for H in turn.

Case 4(a). $H = (q^4 - q^2 + 1)^2.(12 \circ \mathrm{GL}_2(3))$

Let $x \in G$ be a regular semisimple element and recall that $|x| \geqslant 30$ by Lemma 4.8. First observe that $(|H|, |C_G(x)|) = 1$ if $|C_G(x)| = \Phi_i$ with $i \in \{20, 24, 15, 30\}$, so x is a derangement, and by inspecting

[69], we see that

$$\frac{(q^2+1)(q^6-2q^4+3q^2-4)}{20\Phi_{20}} + \frac{q^4(q^4-1)}{24\Phi_{24}} + \frac{q(q^4-1)}{30}\left(\frac{q^3-q^2+1}{\Phi_{15}} + \frac{q^3+q^2-1}{\Phi_{30}}\right)$$

is the contribution to $\delta(G,H)$ from these elements.

Next we claim that x is a derangement if

$$|C_G(x)| \in \{\Phi_1^2\Phi_7, \Phi_2^2\Phi_{14}, \Phi_1\Phi_2\Phi_7, \Phi_1\Phi_2\Phi_{14}\}.$$

To see this, first assume $|C_G(x)| = \Phi_1^2\Phi_7$ and set $T = C_G(x)$ and $d = (|H|, |T|)$. Then d divides $(q-1)^2$, and we note that $T = (q-1) \times (q^7-1)$ is contained in a subgroup M of type $\mathrm{SL}_2(q) \times E_7(q)$. If x has fixed points, then $|x|$ divides d. But $T < C_M(S)$ for every subgroup $S < T$ of order dividing d, so $T < C_M(x)$, and we reach a contradiction. The other three cases are very similar, and we omit the details (in every case, we can embed $T = C_G(x)$ in a subgroup of type $\mathrm{SL}_2(q) \times E_7(q)$). By inspecting [69], we see that the contribution to $\delta(G,H)$ from these elements is at least

$$\frac{q(q^6-1)}{28}\left(\frac{q-2}{\Phi_1^2\Phi_7} + \frac{q}{\Phi_2^2\Phi_{14}} + \frac{q}{\Phi_1\Phi_2\Phi_7} + \frac{q-2}{\Phi_1\Phi_2\Phi_{14}}\right).$$

Putting all of this together, we deduce that $\delta(G,H) > 89/325$ if $q \geqslant 7$, so we may assume $q \leqslant 5$.

We handle the remaining groups with $q \leqslant 5$ by identifying some additional derangements. If $|C_G(x)| = \Phi_1\Phi_2\Phi_9$, then $(|H|, |C_G(x)|) < 30$, and thus x is a derangement by Lemma 4.8. And the same conclusion holds if $|C_G(x)| = \Phi_1\Phi_2\Phi_{18}$ and $q \leqslant 4$. Therefore, we can add

$$\frac{q(q^3+2)(q^3-1)(q-1)}{36\Phi_1\Phi_2\Phi_9} + (1-\delta_{5,q})\frac{(q^3+2)(q^3+1)(q+1)(q-2)}{36\Phi_1\Phi_2\Phi_{18}}$$

to our previous lower bound, and this is good enough to force $\delta(G,H) > 89/325$ if $q \in \{3,4,5\}$. Finally, if $q = 2$ and $|C_G(x)| = q^8-1$, then $(|H|, |C_G(x)|) = 3$, and so we can include an additional contribution of $q^4(q^4-2)/16(q^8-1)$. One can now check that the desired bound holds for $q = 2$.

Case 4(b). $H = \Phi_{30}{:}30 = (q^8+q^7-q^5-q^4-q^3+q+1){:}30$

We claim that each regular semisimple element $x \in G$ with

$$|C_G(x)| \in \{\Phi_{20}, \Phi_{24}, \Phi_1\Phi_2\Phi_4\Phi_8, \Phi_1\Phi_2\Phi_4\Phi_{12}, \Phi_1^2\Phi_7, \Phi_2^2\Phi_{14}, \Phi_1\Phi_2\Phi_7, \Phi_1\Phi_2\Phi_{14}\} \qquad (4.2)$$

is a derangement. To see this, set $T = C_G(x)$ and observe that $d = (|H|, |T|)$ divides 30 in every case. Therefore, in view of Lemma 4.8, we immediately reduce to the case where $d = |x| = 30$. In particular, x is a derangement if $|C_G(x)| = \Phi_{20}$ or Φ_{24} since $d \leqslant 5$.

In each of the remaining cases, we can embed T in a maximal rank subgroup M of G with the property that $T < C_M(S)$ for every order d subgroup S of T. So if x has fixed points, then $T < C_M(x) \leqslant C_G(x) = T$, which is absurd.

For example, if $|T| = \Phi_1\Phi_2\Phi_4\Phi_8$ then d divides q^4-1, and we can embed the cyclic group T in a subgroup M of type $\mathrm{SL}_9(q)$ such that $T < C_M(S)$, where S is the unique order d subgroup of T. Similarly, if $|T| = \Phi_1\Phi_2\Phi_4\Phi_{12}$, then T is cyclic, d divides q^4-1 and we proceed by embedding T in $M = \mathrm{SU}_5(q^2)$. And in each of the four remaining cases, we can argue by embedding T in a subgroup M of type $\mathrm{SL}_2(q) \times E_7(q)$.

Using [69] to calculate the total number of regular semisimple elements $x \in G$ with $|C_G(x)|$ as in (4.2), we deduce that $\delta(G,H) > 89/325$ for all $q \geqslant 3$. Finally, for $q = 2$, it is easy to check that

$(|H|, |C_G(x)|) < 30$ for all

$$|C_G(x)| \in \{\Phi_{15}, \Phi_1\Phi_2\Phi_9, \Phi_1\Phi_2\Phi_{18}, \Phi_1\Phi_2\Phi_4\Phi_5, \Phi_1\Phi_2\Phi_4\Phi_{10}\},$$

and we get $\delta(G, H) > 89/325$ by including the additional contribution from these elements.

Case 4(c). $H = \Phi_{15}{:}30 = (q^8 - q^7 + q^5 - q^4 + q^3 - q + 1){:}30$

This is entirely similar to the previous case, the only difference being that the elements with $|C_G(x)| = \Phi_{30}$ are derangements, rather than those with $|C_G(x)| = \Phi_{15}$. We omit the details. □

We are now ready to complete the proof of Proposition 4.6. Recall that this completes the proofs of Theorems B and D(ii) for exceptional groups.

Proof of Proposition 4.6. In view of Lemmas 4.10 and 4.11, we may assume H is neither a parabolic subgroup, nor the normaliser of a maximal torus. The relevant cases are labelled (a)–(f) in the proof of [14, Proposition 7.1], and we have already handled (a)–(c) in Lemma 4.9.

First assume $(G, H) = (F_4(2), 3.\mathrm{U}_3(2)^2.3.2)$ or $(^2E_6(2), 3.\mathrm{U}_3(2)^3.3^2.S_3)$. In both cases, the character table of G is available in [12], and one can check that the crude bound in (2.3) implies that $\delta(G, H) > 1/2$. Using Lemma 3.2, it is also easy to check that $G = C^2$, where C is a conjugacy class of elements of order 17.

Finally, let us assume $G = E_8(2)$ and $H = 3^2.\mathrm{U}_3(2)^4.3^2.\mathrm{GL}_2(3)$ is of type $\mathrm{SU}_3(2)^4$. As before, let Φ_i be the i-th cyclotomic polynomial evaluated at $q = 2$. If $x \in G$ is any regular semisimple element with

$$|C_G(x)| \in \{\Phi_{20}, \Phi_{24}, \Phi_{15}, \Phi_{30}, \Phi_2^2\Phi_{14}, \Phi_1\Phi_2\Phi_7, \Phi_1\Phi_2\Phi_9, \Phi_1\Phi_2\Phi_{18}, \Phi_1\Phi_2\Phi_4\Phi_8\},$$

then $(|H|, |C_G(x)|) < 30$, and thus x is a derangement by Lemma 4.8. By inspecting [69], we can calculate the total number N of such elements, and we check that $\delta(G, H) \geqslant N/|G| > 89/325$. In addition, [47, Theorem 7.7] implies that $G = \{1\} \cup CD$, where C and D are classes of elements of order $\Phi_{20} = 205$ and $\Phi_{24} = 241$, respectively. □

4.4. Classical groups

In order to complete the proof of Theorem 4.1, we may assume G is a classical group, and so the possibilities for G and H are listed in Tables 16–19 of [62]. Our main result is the following, and we note that this completes the proofs of Theorems B and D.

Proposition 4.13. *Let G be a transitive finite simple classical group with soluble point stabiliser H.*

(i) *If $H \in \mathcal{S}^+$, then $\delta(G) > 89/325$.*
(ii) *If $H \in \mathcal{S}$, then $G = \Delta(G)^2$.*

Throughout this section, G will denote a finite simple classical group over $\mathbb{F}_q$, where $q = p^f$ and p is a prime. We will write V for the natural module, and we set $n = \dim V$. In view of isomorphisms between some of the low-dimensional groups, we may assume G is one of the following:

$$\mathrm{L}_n(q)\ (n \geqslant 2),\ \mathrm{U}_n(q)\ (n \geqslant 3),\ \mathrm{PSp}_n(q)\ (n \geqslant 4),\ \mathrm{P\Omega}_n^\varepsilon(q)\ (n \geqslant 7). \tag{4.3}$$

In addition, we may exclude the following groups

$$\mathrm{L}_2(q)\ (q \leqslant 9),\ \mathrm{L}_4(2),\ \mathrm{U}_3(3),\ \mathrm{Sp}_4(2)',\ \mathrm{PSp}_4(3) \tag{4.4}$$

due to the existence of the following isomorphisms (see [57, Proposition 2.9.1], for example):

$$L_2(4) \cong L_2(5) \cong A_5, \ L_2(7) \cong L_3(2), \ L_2(8) \cong {}^2G_2(3)', \ L_2(9) \cong Sp_4(2)' \cong A_6,$$

$$L_4(2) \cong A_8, \ U_3(3) \cong G_2(2)', \ PSp_4(3) \cong U_4(2).$$

4.4.1. Two-dimensional linear groups

Lemma 4.14. *The conclusion to Proposition 4.13 holds when* $G = L_2(q)$.

Proof. As explained above, we may assume $q \geqslant 11$. By Theorem 3.13, we have $G = \Delta(G)^2$, so we just need to show that $\delta(G, H) > 89/325$. The possibilities for H are recorded in [10, Table 8.1], and we refer the reader to [30, Section 38] for the character table of G. Set $d = (2, q - 1)$.

First assume $H = P_1$ is a Borel subgroup, which allows us to identify $\Omega = G/H$ with the set of 1-dimensional subspaces of V. Then $x \in G$ is a derangement if and only if it acts irreducibly on V, so either x is semisimple and $|C_G(x)| = (q + 1)/d$, or $q \equiv 3 \pmod 4$ and x is an involution. As a consequence, we deduce that

$$\delta(G, H) = \frac{q - 1 + \delta_{2,p}}{2(q + 1)} \geqslant \frac{5}{12} \tag{4.5}$$

for all $q \geqslant 11$, and the result follows.

Next assume H is of type $GL_1(q) \wr S_2$, so $H = D_{d(q-1)}$. Here $x \in G$ is a derangement if and only if x is semisimple with $|C_G(x)| = (q + 1)/d$, or if $|x| = p$ is odd. So for $p = 2$, we see that (4.5) holds, while we get

$$\delta(G, H) \geqslant \frac{q^2 - 1}{|G|} + \frac{q - 3}{2(q + 1)} = \frac{q^2 + q + 4}{2q(q + 1)} > \frac{1}{2}$$

if $p > 2$. Similarly, if H is of type $GL_1(q^2)$, then $H = D_{d(q+1)}$ and $x \in G$ is a derangement if and only if x is semisimple with $|C_G(x)| = (q - 1)/d$, or if $|x| = p$ is odd. So for $p = 2$, we get

$$\delta(G, H) = \frac{q - 2}{2(q - 1)} \geqslant \frac{7}{15}$$

for all $q \geqslant 16$, and for $p > 2$ and $q \geqslant 11$, we compute

$$\delta(G, H) \geqslant \frac{q^2 - 1}{|G|} + \frac{q - 5}{2(q - 1)} = \frac{q^2 - q - 4}{2q(q - 1)} \geqslant \frac{53}{110}.$$

Next assume $q = 3^k$ and H is a subfield subgroup of type $GL_2(3)$, where k is an odd prime. Here $H = L_2(3) \cong A_4$ and $x \in G$ is a derangement if and only if $|x| > 3$, so we get

$$\delta(G, H) = \frac{1}{|G|}\left(|G| - \frac{|G|}{q + 1} - q^2\right) = \frac{q(q - 3)}{q^2 - 1} \geqslant \frac{81}{91}.$$

Finally, suppose $q = p \geqslant 11$ and H is of type $2^{1+2}.O_2^-(2)$, so $H \in \{A_4, S_4\}$, with $H = S_4$ if and only if $q \equiv \pm 1 \pmod 8$ (see [10, Table 8.1] for the precise conditions on q required for maximality). Here the set of nontrivial elements with fixed points comprise the unique classes of elements of order 2 and 3, plus one class of elements of order 4 if $H = S_4$. This implies that

$$\delta(G, H) \geqslant \frac{1}{|G|}\left(|G| - 1 - \frac{5}{2}q(q + 1)\right) = \frac{q^3 - 5q^2 - 6q - 2}{q(q^2 - 1)} > \frac{1}{2}$$

Table 5. *The groups (G, H) in Lemma 4.15.*

G	Type of H	$\delta(G)$
$\mathrm{L}_3(2)$	P_1, P_2, $P_{1,2}$	0.285, 0.285, 0.619
$\mathrm{L}_3(3)$	P_1, P_2, $P_{1,2}$	0.307, 0.307, 0.682
$\mathrm{L}_4(3)$	P_2, $P_{1,3}$	0.507, 0.623
$\mathrm{L}_5(2)$	$P_{2,3}$	0.679
$\mathrm{L}_5(3)$	$P_{2,3}$	0.731
$\mathrm{L}_6(2)$	$P_{2,4}$	0.797
$\mathrm{L}_6(3)$	$P_{2,4}$	0.848
$\mathrm{U}_4(2)$	P_1	0.422
$\mathrm{U}_4(3)$	P_1	0.485
$\mathrm{U}_5(2)$	P_1	0.455
$\mathrm{Sp}_6(2)$	P_2	0.453
$\mathrm{PSp}_6(3)$	P_2	0.496
$\Omega_7(3)$	P_2	0.524
$\Omega_8^+(2)$	P_2, $P_{1,3,4}$	0.613, 0.804
$\mathrm{P}\Omega_8^+(3)$	P_2, $P_{1,3,4}$	0.656, 0.839

for all $q \geqslant 13$ (with equality if $q \equiv 1 \pmod{24}$, for example). If $q = 11$, then $H = A_4$, and we compute $\delta(G, H) = 32/55$. □

For the remainder, we may assume $G \neq \mathrm{L}_2(q)$. We now divide the possibilities for H according to whether or not H is a parabolic subgroup. The cases where H is parabolic will be handled in Section 4.4.2, and the possibilities that arise are recorded in [14, Lemma 5.4]; they comprise a handful of 'sporadic' cases, involving certain low-dimensional groups defined over small fields (see Table 5), together with three infinite families (G, H) where $G = \mathrm{L}_3^\varepsilon(q)$ or $\mathrm{Sp}_4(q)$ and H is a Borel subgroup. The remaining non-parabolic subgroups are listed in [14, Lemma 6.2], and they will be treated in Section 4.4.3.

4.4.2. Parabolic subgroups

In this section we handle the case where $G \neq \mathrm{L}_2(q)$ and H is a parabolic subgroup. We fix our notation for parabolic subgroups:

(a) We write P_k for the stabiliser in G of a k-dimensional totally singular subspace of V (if $G = \mathrm{L}_n(q)$, then all subspaces of V are totally singular).

(b) If $G = \mathrm{L}_n(q)$ and $1 \leqslant k < n/2$, then $P_{k,n-k}$ denotes the stabiliser of a flag $0 < U < W < V$, where $\dim U = k$ and $\dim W = n - k$.

(c) For $G = \mathrm{P}\Omega_8^+(q)$, we define $P_{1,3,4}$ to be the image of the parabolic subgroup

$$[q^{11}]:\left(\frac{q-1}{d}\right)^2 . \frac{1}{d}\mathrm{GL}_2(q).d^2 < \Omega_8^+(q),$$

where $d = (2, q-1)$ and $\frac{1}{d}\mathrm{GL}_2(q)$ is the unique subgroup of $\mathrm{GL}_2(q)$ with index d.

(d) If $G = \mathrm{Sp}_4(q)$ with $q \geqslant 4$ even, then $P_{1,2} = [q^4]:(q-1)^2$ is a Borel subgroup of G (that is to say, it is the normaliser of a Sylow 2-subgroup of G).

None of the subgroups H in (b), (c) or (d) are maximal in G, but they are of the form $H = M \cap G$ for some maximal subgroup M of an almost simple group with socle G.

The possibilities for G and H with $H \in \mathcal{S}^+$ are recorded in [14, Lemma 5.4], and we begin by handling the cases arising in part (i) of this lemma. These are the cases listed in Table 5, recalling that we may (and do) exclude the classical groups in (4.4).

Lemma 4.15. *The conclusion to Proposition 4.13 holds if (G, H) is one of the cases in Table 5.*

Proof. This is a straightforward MAGMA computation. In each case, we construct G and H in terms of a permutation representation of G of minimal degree, and by computing conjugacy classes, we determine the set $\Delta(G)$ of derangements with respect to the action of G on G/H. This allows us to compute

$\delta(G)$, which is recorded in the final column of Table 5 to 3 significant figures. If $\delta(G) > 1/2$, then $G = \Delta(G)^2$ by Lemma 3.22. Otherwise, we use MAGMA to construct the character table of G, and we apply Lemma 3.2 to check that either $G = L_3(2)$ and $H \in \{P_1, P_2\}$, or there exist classes C, D of derangements such that $G = \{1\} \cup CD$. Note that in the former case, we have $G \cong L_2(7)$, $H \cong S_4$, and thus $G = C^2 \cup CD$ for the two classes C, D of elements of order 7 (see Proposition 3.14(iv)). □

To complete the proof for parabolic subgroups, it just remains to consider the three infinite families recorded in [14, Lemma 5.4(ii)]:

(a) $G = L_3(q)$, $H = P_{1,2}$ and $q \geqslant 4$;
(b) $G = U_3(q)$, $H = P_1$ and $q \geqslant 4$;
(c) $G = Sp_4(q)$, $H = P_{1,2}$ and $q \geqslant 4$ even.

Notice that in each case, $H = N_G(P)$ is a Borel subgroup, where P is a Sylow p-subgroup of G. Also note that H is non-maximal in G in cases (a) and (c).

Lemma 4.16. *The conclusion to Proposition 4.13 holds if $G = L_3(q)$ and $H = P_{1,2}$.*

Proof. Set $d = (3, q-1)$, $e = (q^2 + q + 1)/d$ and note that $H \in \mathcal{S}^+ \setminus \mathcal{S}$, so it suffices to show that $\delta(G) > 89/325$.

Let χ be the corresponding permutation character and note that the character table of G is available in the literature (see [77, Table 2]). As observed in the proof of [14, Lemma 5.6], we have

$$\chi = 1 + St + 2\psi,$$

where $St = \chi_{q^3}$ is the Steinberg character and $\psi = \chi_{q(q+1)}$ in the notation of [77]. From the character table, we deduce that $x \in G$ is a derangement if and only if x is regular semisimple with $|C_G(x)| = (q^2 - 1)/d$ or e. Since there are $(e-1)/2 - (q-1)/d - (3-d)/2$ classes of the first type, and $(e-1)/3$ classes of the second, it follows that

$$\delta(G) = \left(\frac{1}{2}(e-1) - \frac{q-1}{d} - \frac{3-d}{2}\right)\frac{d}{q^2-1} + \frac{1}{3}(e-1)\frac{1}{e} \geqslant \frac{24}{35}$$

for all $q \geqslant 4$. □

Lemma 4.17. *The conclusion to Proposition 4.13 holds if $G = U_3(q)$ and $H = P_1$.*

Proof. Set $d = (3, q+1)$, $e = (q^2 - q + 1)/d$ and let χ be the permutation character. Then $\chi = 1 + St$, where St is the Steinberg character, and by inspecting the character table of G (see [77, Table 2]), we deduce that $x \in G$ is a derangement if and only if $|C_G(x)| = (q+1)^2/d$ or e, or if $|x| = d = 3$ and $|C_G(x)| = (q+1)^2$. Therefore,

$$\delta(G) = \frac{1}{6}(e-1)\frac{d}{(q+1)^2} + \frac{1}{3}(e-1)\frac{1}{e} + \delta_{3,d}\frac{1}{(q+1)^2} \geqslant \frac{126}{325}$$

for all $q \geqslant 4$. Finally, Theorem 3.13 implies that $G = \{1\} \cup C^2$ for a conjugacy class C of derangements, whence $G = \Delta(G)^2$. □

Lemma 4.18. *The conclusion to Proposition 4.13 holds if $G = Sp_4(q)$ and $H = P_{1,2}$.*

Proof. Here $q \geqslant 4$ is even and H is non-maximal in G, so we just need to establish the bound $\delta(G) > 89/325$. If $x \in G$ is a regular semisimple element with $|C_G(x)| = (q+1)^2$ or $q^2 + 1$, then $(|H|, |C_G(x)|) = 1$, and thus x is a derangement. The number of distinct conjugacy classes of such elements is recorded in [32, Table IV-1], and we deduce that

$$\delta(G) \geqslant \frac{q(q-2)}{8(q+1)^2} + \frac{q^2}{4(q^2+1)} \geqslant \frac{117}{425} > \frac{89}{325}$$

for all $q \geqslant 4$. □

Table 6. *The groups (G, H) in Lemma 4.19.*

G	Type of H	Maximal	$\delta(G)$
$L_3(2)$	$GL_2(2) \oplus GL_1(2)$	n	0.535
$L_3(3)$	$GL_2(3) \oplus GL_1(3)$, $O_3(3)$	n, y	0.418, 0.742
$L_3(4)$	$GU_3(2)$	y	0.685
$L_4(3)$	$GL_2(3) \wr S_2$, $O_4^+(3)$	n, y	0.649, 0.804
$L_6(3)$	$GL_2(3) \wr S_3$	y	0.907
$L_8(3)$	$GL_2(3) \wr S_4$	y	0.976
$U_4(2)$	$GU_3(2) \perp GU_1(2)$	y	0.418
$U_4(3)$	$GU_2(3) \wr S_2$	y	0.646
$U_5(2)$	$GU_3(2) \perp GU_2(2)$	y	0.538
$U_6(2)$	$GU_3(2) \wr S_2$	y	0.583
$U_6(3)$	$GU_2(3) \wr S_3$	y	0.883
$U_8(3)$	$GU_2(3) \wr S_4$	y	0.971
$U_9(2)$	$GU_3(2) \wr S_3$	y	0.897
$U_{12}(2)$	$GU_3(2) \wr S_4$	y	0.947
$PSp_6(3)$	$Sp_2(3) \wr S_3$	y	0.644
$PSp_8(3)$	$Sp_2(3) \wr S_4$	y	0.824
$\Omega_7(3)$	$O_4^+(3) \perp O_3(3)$	y	0.644
$\Omega_8^+(2)$	$O_2^-(2) \times GU_3(2)$	n	0.744
$P\Omega_8^+(3)$	$O_4^+(3) \wr S_2$	y	0.769
$P\Omega_{12}^+(3)$	$O_4^+(3) \wr S_3$	y	0.955
$P\Omega_{16}^+(3)$	$O_4^+(3) \wr S_4$	y	0.993

4.4.3. Non-parabolic subgroups

In order to complete the proof of Proposition 4.13, we may assume H is a non-parabolic subgroup. The possibilities for G and H are described in [14, Lemma 6.2], and we begin by handling the 'sporadic' cases recorded in Table 6, which involve certain low-dimensional groups with $n \leqslant 16$ and $q \leqslant 4$. Note that in the third column of the table, we indicate whether or not H is a maximal subgroup of G (this follows from the information in [10, 57]).

Lemma 4.19. *The conclusion to Proposition 4.13 holds if (G, H) is one of the cases in Table 6.*

Proof. All of these cases can be handled using MAGMA [8]. In the final column of Table 6, we calculate $\delta(G)$ to 3 significant figures.

First assume H is maximal in G and write $G = L/Z$ and $H = J/Z$, where L is one of the quasisimple matrix groups $SL_n^\varepsilon(q)$, $Sp_n(q)$, $\Omega_n^\varepsilon(q)$ and $Z = Z(L)$. In this situation, working with the standard matrix representation of L, we can use the function ClassicalMaximals to construct J, and we then compute $\delta(L, J) = \delta(G)$ by inspecting the conjugacy classes in L and J.

There are four remaining cases where H is non-maximal. Here $H = M \cap G$, where M is maximal in an almost simple group A with socle G. To handle these cases, we use the function AutomorphismGroup-SimpleGroup to construct a permutation representation of A, and we then construct M, and hence H, by using the function MaximalSubgroups. We then compute $\delta(G)$ by considering the conjugacy classes in G and H.

If $\delta(G) > 1/2$, then $G = \Delta(G)^2$ by Lemma 3.22. Otherwise, we have $(G, H) = (L_3(3), GL_2(3))$ or $(U_4(2), GU_3(2))$, and by working with the character table of G and Lemma 3.2, it is easy to show that $G = \{1\} \cup CD$ for certain conjugacy classes C, D of derangements. □

Finally, let us turn to the remaining infinite families (G, H) with H non-parabolic, which are recorded in Table 7 (see [14, Lemma 6.2(v)]). We consider each case in turn.

Lemma 4.20. *The conclusion to Proposition 4.13 holds if $G = L_n^\varepsilon(q)$ and H is of type $GL_1^\varepsilon(q^n)$, where $n \geqslant 3$ is prime.*

Proof. Here $H = N_G(T) = T.n$, where T is a cyclic maximal torus of order $(q^n - \varepsilon)/d(q - \varepsilon)$ with $d = (n, q - \varepsilon)$. If $G = L_3(2)$, then it is easy to check that $\delta(G) = 3/8$ and $G = \{1\} \cup CD$, where C and

Table 7. *The infinite families with H non-parabolic.*

G	Type of H	Conditions
$L_n^\varepsilon(q)$	$GL_1^\varepsilon(q^n)$	$n \geqslant 3$ prime
	$GL_1^\varepsilon(q) \wr S_n$	$n \in \{3, 4\}$
	$3^{1+2}.Sp_2(3)$	$n = 3, \; q = p \equiv \varepsilon \pmod 3$
	$GU_3(2)$	$(n, \varepsilon) = (3, -), \; q = 2^k, \; k \geqslant 3$ prime
$Sp_4(q)$	$O_2^\varepsilon(q) \wr S_2$	$q \geqslant 4$ even
	$O_2^-(q^2)$	$q \geqslant 4$ even
$P\Omega_8^+(q)$	$O_2^-(q^2) \times O_2^-(q^2)$	
	$O_2^\varepsilon(q) \wr S_4$	

D are the unique conjugacy classes of elements of order 2 and 4, respectively. In each of the remaining cases, we claim that $\delta(G) > 1/2$, so $G = \Delta(G)^2$ by Lemma 3.22.

First observe that every non-identity element $x \in H$ is regular as an element of G. More precisely, either $x \in T$ and $C_G(x) = T$, or x has order n and we calculate that G contains at most $d|G|/c$ regular elements of order n, where $c = (q-1)^{n-1}$ if $\varepsilon = +$ and $d = n$, otherwise $c = (q^2 - 1)^{(n-1)/2}$. For example, if n divides q, then every regular element in G of order n has Jordan form (J_n) on the natural module for G, and we deduce that there are

$$\frac{|SL_n^\varepsilon(q)|}{q^{n-1}} = \frac{d|G|}{q^{n-1}} < \frac{d|G|}{(q^2-1)^{(n-1)/2}}$$

such elements in G.

Since there are exactly $(|T|-1)/n$ distinct G-classes of regular semisimple elements $x \in G$ with $|C_G(x)| = |T|$ (see [34, Example (a), p.484], for example), it follows that

$$\delta(G) \geqslant \frac{1}{|G|} \left(|G| - 1 - \frac{d|G|}{c} - \frac{|T|-1}{n} \cdot \frac{|G|}{|T|} \right) = 1 - \frac{1}{|G|} - \frac{d}{c} - \frac{1}{n}\left(1 - \frac{1}{|T|}\right),$$

and thus $\delta(G) > 1/2$ unless $G = L_3(3)$. In the latter case, we compute $\delta(G) = 251/432$. □

Lemma 4.21. *The conclusion to Proposition 4.13 holds if we have $G = L_3^\varepsilon(q)$ and H is of type $GL_1^\varepsilon(q) \wr S_3$, $3^{1+2}.Sp_2(3)$ or $GU_3(2)$.*

Proof. Set $d = (3, q - \varepsilon)$ and $e = (q^2 + \varepsilon q + 1)/d$.

First assume H is of type $GL_1^\varepsilon(q) \wr S_3$ and note that $q \geqslant 5$ if $\varepsilon = +$ (see [10, Table 8.3]). If $x \in G$ is regular semisimple with $|C_G(x)| = e$, then $(|H|, |C_G(x)|) = 1$, and thus x is a derangement. As noted in [77], there are precisely $(e-1)/3$ conjugacy classes of such elements, and thus

$$\delta(G) \geqslant \frac{e-1}{3e} \geqslant \frac{2}{7}.$$

In addition, [47, Theorems 7.1 and 7.3] imply that $G = \{1\} \cup C^2$, where C is any class of elements of order e.

The case $H = 3^{1+2}.Sp_2(3)$ is entirely similar. Here $q = p \equiv \varepsilon \pmod 3$, $H \leqslant ASL_2(3)$ and every regular semisimple element with $|C_G(x)| = e$ is a derangement. Similarly, if H is of type $GU_3(2)$, then $\varepsilon = -$, $q = 2^k$ for some odd prime k, and the same argument applies since we have $H \leqslant PGU_3(2) \cong ASL_2(3)$. □

Lemma 4.22. *The conclusion to Proposition 4.13 holds if $G = L_4(q)$ and H is of type $GL_1(q) \wr S_4$.*

Proof. Set $d = (4, q - 1)$ and note that $q \geqslant 5$ (see [10, Table 8.8]).

First assume $x \in G$ is regular semisimple with $|C_G(x)| = (q^4 - 1)/d(q - 1)$. We claim that x is a derangement. Seeking a contradiction, suppose $x \in H$ and note that $(|H|, |C_G(x)|)$ divides $q + 1$,

which implies that $|x|$ divides $q + 1$. Since x is regular, it follows that x is conjugate to the image of a block-diagonal matrix of the form $\mathrm{diag}(A, B) \in \mathrm{SL}_4(q)$, where $A, B \in \mathrm{GL}_2(q)$ are irreducible, with distinct eigenvalues in $\mathbb{F}_{q^2}$. But this implies that $|C_G(x)| = (q + 1)(q^2 - 1)/d$, and we have reached a contradiction. This justifies the claim. From [34, Example (a), p.484], we see that G has exactly

$$\frac{1}{4d}(q + 1)(q^2 + 1 - e)$$

such conjugacy classes, where $e = (2, q - 1)$, whence

$$\frac{(q + 1)(q^2 + 1 - e)/4d}{(q^4 - 1)/d(q - 1)} = \frac{1}{4} - \frac{e}{4(q^2 + 1)}$$

is the contribution to $\delta(G)$ from these elements.

Next suppose $y \in G$ is regular semisimple with $|C_G(y)| = (q^3 - 1)/d$ and note that $(|H|, |C_G(x)|)$ divides $e'(q - 1)$, where $e' = (3, q - 1)$. If $e' = 1$, then by repeating the argument above, we deduce that y is a derangement (indeed, we have $|C_G(z)| = (q - 1)^3/d$ for every regular semisimple element $z \in G$ such that $|z|$ divides $q - 1$). Now assume $e' = 3$. As before, y is a derangement if $|y|$ divides $q - 1$, so we may assume that $|y| = 9m$ for some divisor m of $(q - 1)/3$. To analyse this situation, it will be convenient to switch to the matrix groups $L = \mathrm{SL}_4(q)$ and $J = (q - 1)^3{:}S_4$, where J is the stabiliser in L of a direct sum decomposition $V = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \langle v_3 \rangle \oplus \langle v_4 \rangle$ of the natural module.

Write $\mathbb{F}_q^\times = \langle \omega \rangle$. In terms of the basis $\{v_1, v_2, v_3, v_4\}$ for V, we observe that each $a \in J$ with $|C_L(a)| = q^3 - 1$ is J-conjugate to an element of the form

$$\begin{pmatrix} \omega^i & & & \\ & 1 & & \\ & & 1 & \\ & & & \omega^{-i} \end{pmatrix}(1, 2, 3) = \begin{pmatrix} & \omega^i & & \\ 1 & & & \\ & 1 & & \\ & & & \omega^{-i} \end{pmatrix} \in J,$$

where $1 \leqslant i < q$ is indivisible by 3. Since 3 divides $q - 1$, there are precisely $2(q - 1)/3$ such J-classes, none of which are fused in L.

By considering rational canonical forms, we see that each L-class a^L with $|C_L(a)| = q^3 - 1$ corresponds to a monic irreducible cubic polynomial over $\mathbb{F}_q$. So there are precisely

$$\frac{1}{3}\sum_{m|3}\mu(m)q^{\frac{3}{m}} = \frac{1}{3}q(q^2 - 1)$$

such classes, where μ is the Möbius function, and thus the contribution to $\delta(G)$ from the regular semisimple elements y with $|C_G(y)| = (q^3 - 1)/d$ is at least

$$\frac{q(q^2 - 1)/3 - 2(q - 1)/3}{q^3 - 1} = \frac{1}{3} - \frac{1}{q^2 + q + 1}.$$

Therefore,

$$\delta(G) \geqslant \frac{1}{4} - \frac{e}{4(q^2 + 1)} + \frac{1}{3} - \frac{1}{q^2 + q + 1} \geqslant \frac{643}{1209} > \frac{1}{2}$$

for all $q \geqslant 5$, and the result follows. $\qquad\square$

Lemma 4.23. *The conclusion to Proposition 4.13 holds if $G = \mathrm{U}_4(q)$ and H is of type $\mathrm{GU}_1(q) \wr S_4$.*

Proof. This is essentially identical to the previous case. Set $d = (4, q + 1)$ and first consider a regular semisimple element $x \in G$ with $|C_G(x)| = (q^4 - 1)/d(q + 1)$. Since $(|H|, |C_G(x)|)$ divides $q - 1$, we

deduce that x is a derangement (indeed, if $z \in G$ is regular semisimple and $|z|$ divides $q - 1$, then $|C_G(z)| = (q^2 - 1)(q - 1)/d)$, and we calculate that there are precisely

$$\frac{1}{4d}(q - 1)(q^2 + 1 - e)$$

such classes in G, where $e = (2, q - 1)$.

Next set $L = \mathrm{SU}_4(q)$ and $J = (q + 1)^3 {:} S_4$. Then L has exactly $q(q^2 - 1)/3$ regular semisimple classes y^L with $|C_L(y)| = q^3 + 1$, all of which contain derangements if $q + 1$ is indivisible by 3. However, if $q \equiv -1 \pmod 3$, then by arguing as in the proof of Lemma 4.22, we deduce that $2(q + 1)/3$ of these classes meet J. So it follows that the contribution to $\delta(G)$ from regular semisimple elements $y \in G$ with $|C_G(y)| = (q^3 + 1)/d$ is at least

$$\frac{q(q^2 - 1)/3 - 2(q + 1)/3}{q^3 + 1} = \frac{1}{3} - \frac{1}{q^2 - q + 1},$$

and this implies that

$$\delta(G) \geqslant \frac{1}{4} - \frac{e}{4(q^2 + 1)} + \frac{1}{3} - \frac{1}{q^2 - q + 1} \geqslant \frac{47}{91}$$

for all $q \geqslant 5$. If $q = 4$, we compute $\delta(G) = 3508723/4243200$, and similarly, we get $\delta(G) = 20128/25515$ for $q = 3$; hence, $\delta(G) > 1/2$ for all $q \geqslant 3$, and thus $G = \Delta(G)^2$ by Lemma 3.22. Finally, for $q = 2$, we compute $\delta(G) = 31/80$, and it is straightforward to check that $G = C^2$, where C is the unique conjugacy class of elements of order 5. $\qquad\square$

Lemma 4.24. *The conclusion to Proposition 4.13 holds if $G = \mathrm{Sp}_4(q)$ and H is of type $\mathrm{O}_2^\varepsilon(q) \wr S_2$ or $\mathrm{O}_2^-(q^2)$, where $q \geqslant 4$ is even.*

Proof. Here $H \in \mathcal{S}^+ \setminus \mathcal{S}$, and so we just need to verify the bound $\delta(G) > 89/325$.

First assume H is of type $\mathrm{O}_2^\varepsilon(q) \wr S_2$, so $H = D_{2(q-\varepsilon)} \wr S_2$. If $x \in G$ is a regular semisimple element with $|C_G(x)| = q^2 - 1$, then $(|H|, |C_G(x)|) = q - \varepsilon$, and we deduce that x is a derangement (indeed, $|C_G(z)| = (q-\varepsilon)^2$ for every regular semisimple element $z \in G$ such that $|z|$ divides $q-\varepsilon$). By inspecting [32, Table IV-1], we see that there are exactly $\frac{1}{2}q(q - 2)$ such classes, and thus

$$\delta(G) \geqslant \frac{q(q - 2)}{2(q^2 - 1)} \geqslant \frac{8}{21}$$

for all $q \geqslant 8$. And if $q = 4$, then $\varepsilon = -$ (see [10, Table 8.14]), and we compute $\delta(G) = 3481/4896$.

Now assume H is of type $\mathrm{O}_2^-(q^2)$, so $H = (q^2 + 1).4$. As above, each $x \in G$ with $|C_G(x)| = q^2 - 1$ is a derangement (indeed, we have $(|H|, |C_G(x)|) = 1$), and we deduce that $\delta(G) \geqslant 8/21$ for $q \geqslant 8$. Finally, for $q = 4$, we compute $\delta(G) = 21011/28800$. $\qquad\square$

Lemma 4.25. *The conclusion to Proposition 4.13 holds if $G = \mathrm{P}\Omega_8^+(q)$ and H is of type $\mathrm{O}_2^-(q^2) \times \mathrm{O}_2^-(q^2)$.*

Proof. Once again, we have $H \in \mathcal{S}^+ \setminus \mathcal{S}$, and so our goal is to show that $\delta(G) > 89/325$. Set $d = (2, q-1)$ and observe that

$$H = N_G(P) = (D_{2(q^2+1)/d} \times D_{2(q^2+1)/d}).2^2,$$

where P is a Sylow r-subgroup of G and r is an odd prime divisor of $q^2 + 1$. For $q = 2$, we compute $\delta(G) = 5740943/6967296$, so for the remainder, we may assume $q \geqslant 3$.

If q is even, then every semisimple element $x \in H$ is contained in the torus $(q^2 + 1)^2$, which means that $|C_G(x)| = (q^2 + 1)^2$ for every regular semisimple element $x \in H$. The conjugacy classes in G are

available in Chevie [43] (also see [69]), and it is a routine exercise to check that

$$\delta(G) \geqslant \frac{1}{|G|}|\{x \in G \ : \ x \text{ regular semisimple}, |C_G(x)| \neq (q^2+1)^2\}| > \frac{1}{2}$$

for all $q \geqslant 4$.

Now assume q is odd and let $x \in H$ be a regular semisimple element with $|C_G(x)| = (q^3 - \varepsilon)(q - \varepsilon)/2$ and $\varepsilon = \pm$. Since $(|H|, |C_G(x)|) \in \{1, 4, 16\}$, Lemma 4.8 implies that x is a derangement unless $|x| = 16$, which coincides with the order of a Sylow 2-subgroup of H. But the Sylow 2-subgroups of H are non-cyclic, so H does not contain any elements of order 16. It follows that each $x \in G$ with $|C_G(x)| = (q^3 - \varepsilon)(q - \varepsilon)/2$ is a derangement.

Set $K = \mathrm{Spin}_8^+(q)$, so $G = K/Z$ with $Z = Z(K) = C_2 \times C_2$. By inspecting [69], we observe that K has exactly

$$N = \frac{|K|}{(q^3 - \varepsilon)(q - \varepsilon)} \cdot \frac{1}{6}q(q - \varepsilon)(q^2 - 1)$$

elements y with $|C_K(y)| = (q^3 - \varepsilon)(q - \varepsilon)$. By considering the images of these elements, it follows that $G = K/Z$ has at least $N/4$ regular semisimple elements x with $|C_G(x)| = (q^3 - \varepsilon)(q - \varepsilon)/2$, and we deduce that

$$\delta(G) \geqslant \frac{1}{6}\left(\frac{q(q-1)(q^2-1)}{(q^3-1)(q-1)} + \frac{q(q+1)(q^2-1)}{(q^3+1)(q+1)}\right) > \frac{89}{325}$$

for all $q \geqslant 3$.   □

In order to complete the proof of Proposition 4.13, we may assume $G = \mathrm{P}\Omega_8^+(q)$ and H is of type $\mathrm{O}_2^\varepsilon(q) \wr S_4$.

Lemma 4.26. *The conclusion to Proposition 4.13 holds if $G = \mathrm{P}\Omega_8^+(q)$ and H is of type $\mathrm{O}_2^\varepsilon(q) \wr S_4$.*

Proof. First observe that $q \geqslant 5$ if $\varepsilon = +$ (see [10, Table 8.50]).

To begin with, we will assume q is even. For $q \in \{2, 4\}$, we have $e = -$, and with the aid of MAGMA, it is easy to check that $\delta(G) > 1/2$. Now assume $q \geqslant 8$.

If $x \in G$ is regular semisimple and $|C_G(x)| = (q + \varepsilon)(q^3 + \varepsilon)$, then Lemma 4.8 implies that x is a derangement since $(|H|, |C_G(x)|) \leqslant 3$. From [69], we read off that G has precisely $q(q^2 - 1)(q + \varepsilon)/6$ conjugacy classes of such elements.

Next let $y \in G$ be regular semisimple with $|C_G(y)| = q^4 - 1$, in which case $T = C_G(y)$ is cyclic and $(|H|, |T|) = (3, q + \varepsilon)(q - \varepsilon)$ divides $q^2 - 1$. Let S be the unique subgroup of T of order $q^2 - 1$ and note that we may embed T in a subgroup $M = \mathrm{GL}_4(q)$. Then $T < C_M(S)$, and we deduce that y is a derangement.

Since G has $3q^2(q^2 - 2)/8$ distinct classes y^G with $|C_G(y)| = q^4 - 1$ (see [69]), it follows that

$$\delta(G) \geqslant \frac{q(q^2-1)}{6(q^3+\varepsilon)} + \frac{3q^2(q^2-2)}{8(q^4-1)} > \frac{1}{2}$$

for all $q \geqslant 8$, and hence, $G = \Delta(G)^2$ by Lemma 3.22.

Now assume q is odd. If $q = 3$, then $\varepsilon = -$ and $H = N_G(P)$, where P is a normal subgroup of a Sylow 2-subgroup of G with $|P| = 2^7$. Using MAGMA, we compute $\delta(G) > 1/2$. In the same way, one can check that $\delta(G) > 1/2$ when $q = 5$, so for the remainder, we may assume $q \geqslant 7$. It will be convenient to work in the quasisimple group $L = \Omega_8^+(q)$, in which case H is the image of the subgroup $J = \Omega_2^\varepsilon(q)^4.[2^6].S_4$ of L. In addition, set $K = \mathrm{Spin}_8^+(q)$ and $Z = Z(K) = C_2 \times C_2$, so $G = K/Z$ and $L = K/Z_1$ for some central subgroup Z_1 of order 2.

Let $x \in L$ be a regular semisimple element with $|C_L(x)| = (q^4 - 1)/2$ or $q^4 - 1$. By arguing as above, we deduce that x is a derangement. In addition, by inspecting [69], we see that K has exactly

$$N = \frac{|K|}{q^4 - 1} \cdot \frac{3}{8}(q^4 - 4q^2 + 3)$$

elements y with $|C_K(y)| = q^4 - 1$. It follows that there are at least $N/2$ regular semisimple elements $x \in L$ with $|C_L(x)| = q^4 - 1$ or $(q^4 - 1)/2$.

Next consider a regular semisimple element $y \in L$ with $|C_L(y)| = (q + \varepsilon)(q^3 + \varepsilon)/2$ and note that $(|J|, |C_L(y)|)$ divides $(q + \varepsilon)^2/e$, where $e = (3, q + \varepsilon)$. Here $T = C_L(y) = \frac{1}{2}(q + \varepsilon) \times (q^3 + \varepsilon)$ is non-cyclic, and we may embed T in a subgroup M of type $\mathrm{GL}_4^{-\varepsilon}(q)$. Then $T < C_M(S)$ for every subgroup S of T such that $|S|$ divides $(q + \varepsilon)^2/e$, and it follows that y is a derangement. As noted in the proof of Lemma 4.25, there are at least

$$\frac{|L|}{(q^3 + \varepsilon)(q + \varepsilon)} \cdot \frac{1}{6}q(q + \varepsilon)(q^2 - 1)$$

such elements in L.

Putting this together, we deduce that

$$\delta(G) \geqslant \frac{3(q^4 - 4q^2 + 3)}{8(q^4 - 1)} + \frac{q(q^2 - 1)}{6(q^3 + \varepsilon)} > \frac{1}{2}$$

for all $q \geqslant 7$. The result follows.   □

This completes the proof of Proposition 4.13. By combining this result with Propositions 4.3, 4.5 and 4.6, we conclude that the proof of Theorem 4.1 is complete. In particular, we have now proved Theorems B and D in all cases.

4.5. Primitive groups

We now use Theorem 4.1(i) to prove part (ii) of Theorem C (recall that Theorem C(i) was established in Section 2.3, so this will complete the proof of Theorem C).

Proof of Theorem C(ii). Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with socle N and soluble point stabiliser H. Recall that our goal is to show that $\delta(N) \geqslant 89/325$, with equality if and only if $N = {}^2F_4(2)'$ and $H \cap N = 2^2.[2^8].S_3$.

As a consequence of the O'Nan-Scott theorem and our soluble point stabiliser hypothesis, G is either affine, almost simple or a product type group $G \leqslant L \wr S_b$, where G acts on $\Omega = \Gamma^b$ via the product action and $L \leqslant \mathrm{Sym}(\Gamma)$ is an almost simple primitive group with socle S and soluble point stabilisers.

If G is affine, then N is regular and $\delta(N) = 1 - |N|^{-1} \geqslant 1/2$. And if G is almost simple, then Theorem 4.1(i) implies that $\delta(N) \geqslant 89/325$, with equality if and only if $N = {}^2F_4(2)'$ and $H \cap N = 2^2.[2^8].S_3$. Finally, if $G \leqslant L \wr S_b$ is a product type group, then $N = S^b$ with S simple, and by combining (2.4) with Theorem 4.1(i), we deduce that

$$\delta(N) > \delta(S, \Gamma) \geqslant \frac{89}{325}.$$

The result follows.   □

5. Derangement generation

Recall that every alternating group can be generated by two elements. For example,

$$A_n = \langle (1, 2, 3), (\delta, \delta + 1, \ldots, n) \rangle,$$

for all $n \geqslant 4$, where $\delta = 1$ if n is odd, otherwise $\delta = 2$. By a celebrated theorem of Steinberg [78], every finite simple group of Lie type can also be generated by a pair of elements, and the same is true for all the sporadic simple groups (see [3]). So this allows us to conclude, via CFSG, that every finite simple group is generated by two elements. In recent years, this theorem has been extended in many different directions, and there is now a vast literature on a wide range of 2-generation properties of simple groups (for example, see the survey articles [15, 52] for a sample of some of the remarkable results that have been established).

Now suppose $G \leqslant \mathrm{Sym}(\Omega)$ is a finite transitive permutation group with $|\Omega| \geqslant 2$ and let $\Delta(G)$ be the set of derangements in G. The (normal) subgroup $D(G) = \langle \Delta(G) \rangle$ generated by $\Delta(G)$ has been studied by Bailey et al. in [4], where several interesting results concerning the order and structure of the quotient group $G/D(G)$ are established. Of course, if G is simple, then $G = D(G)$, and it is natural to ask whether or not G is generated by a pair of derangements. In this final section, our main theorem shows that this is indeed the case. Moreover, we will prove that such a group is generated by two *conjugate* derangements. The following result is stated as Theorem G in Section 1.

Theorem 5.1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite simple transitive permutation group. Then there exists a derangement $x \in G$ such that $G = \langle x, x^g \rangle$ for some $g \in G$.*

One of the key ingredients in our proof of Theorem 5.1 involves the concept of uniform spread. Following Breuer et al. [13], we say that a finite group G has *positive uniform spread* if there exists a conjugacy class $C = y^G$ with the property that for any non-identity $x \in G$, there exists an element $z \in C$ such that $G = \langle x, z \rangle$. In this situation, we call y, or the class C itself, a *witness*. The main theorem of [45] shows that every finite simple group has this remarkably strong 2-generation property, and we refer the reader to [13, 19, 20, 21] for more recent extensions and generalisations.

The next two lemmas will be applied repeatedly in the proof of Theorem 5.1. In the first one, and for the remainder of the paper, we write

$$\mathcal{M}(y) = \{H \ : \ H < G \text{ maximal and } y \in H\} \tag{5.1}$$

for the set of maximal subgroups of G containing the element $y \in G$. In addition,

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

is the *fixed point ratio* of $z \in G$ with respect to the natural transitive action of G on $\Omega = G/H$, which is simply the proportion of points in Ω fixed by z. The following elementary observation was a key tool in [45], and we include a short proof for completeness.

Lemma 5.2. *Let G be a finite group. An element $y \in G$ is a witness if*

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(z, G/H) < 1 \tag{5.2}$$

for all $z \in G$ of prime order.

Proof. Let $x \in G$ be a non-identity element and suppose $z = x^m$ has prime order. Let

$$\mathbb{P}(y, z) = \frac{|\{v \in y^G \ : \ G \neq \langle v, z \rangle\}|}{|y^G|}$$

be the probability that z and a uniformly random conjugate of y do not generate G. Now $G \neq \langle v, z \rangle$ if and only if $z^g \in H$ for some $g \in G$ and $H \in \mathcal{M}(y)$. And since $|z^G \cap H|/|z^G|$ is the probability that a random conjugate of z is contained in H, it follows that

$$\mathbb{P}(y, z) \leqslant \sum_{H \in \mathcal{M}(y)} \frac{|z^G \cap H|}{|z^G|} = \sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(z, G/H).$$

So if (5.2) holds, then $\mathbb{P}(y, z) < 1$, and thus $G = \langle z, y^g \rangle = \langle x, y^g \rangle$ for some $g \in G$. Since x is an arbitrary non-identity element, we conclude that y is a witness. $\square$

Remark 5.3. Suppose G is simple and $\{H_1, \ldots, H_t\}$ is a complete set of representatives of the conjugacy classes of maximal subgroups in G. Then each H_i is self-normalising and we have

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(z, G/H) = \frac{1}{|G|} \sum_{i=1}^{t} |H_i| \chi_i(y) \chi_i(z), \tag{5.3}$$

for all $z \in G$, where $\chi_i = 1_{H_i}^{G}$ is the permutation character for the action of G on G/H_i.

The connection between uniform spread and Theorem 5.1 is given by the following easy observation.

Lemma 5.4. *Let* $G \leqslant \mathrm{Sym}(\Omega)$ *be a finite transitive permutation group and suppose* $x, y \in G$ *are witnesses such that*

$$\{A^g \ : \ A \in \mathcal{M}(x), \ g \in G\} \cap \mathcal{M}(y) = \emptyset. \tag{5.4}$$

Then there exists a derangement $z \in G$ *such that* $G = \langle z, z^g \rangle$ *for some* $g \in G$.

Proof. Let H be a point stabiliser. Since the intersection in (5.4) is empty, it follows that some element $z \in \{x, y\}$ is a derangement on Ω. And since z is a witness, we conclude that $G = \langle z, z^g \rangle$ for some $g \in G$. $\square$

Remark 5.5. Notice that a weaker form of Lemma 5.4 will be sufficient for establishing the conclusion in Theorem 5.1. Indeed, it suffices to show that there exist elements $x, y \in G$ such that (5.4) holds, and we have

$$\sum_{H \in \mathcal{M}(z)} \mathrm{fpr}(z, G/H) < 1$$

for $z \in \{x, y\}$. In particular, it is not strictly necessary to show that x or y is a witness.

Remark 5.6. Let us also note that if $x, y \in G$ satisfy the condition in (5.4), then $\{x, y\}$ is an *invariable* generating set for G, in the sense that $G = \langle x^a, y^b \rangle$ for all $a, b \in G$.

In view of Lemma 5.4 and the connection with uniform spread, we will make extensive use of [13, 45], where explicit witnesses for simple groups are identified. In several cases, we will need to prove that some additional elements are also witnesses, and we will typically do this via Lemma 5.2, which involves determining the maximal overgroups and bounding the corresponding fixed point ratios. For example, if G is a classical group, then we will work closely with [5, 10, 49, 57] to study maximal overgroups and we will appeal to the fixed point ratio bounds in [16] and [45, Section 3]. We will also use computational methods to handle some of the small simple groups that are amenable to direct computation in GAP [40] or MAGMA [8] (see Propositions 5.10 and 5.16, for example).

5.1. Alternating groups

Here we prove Theorem 5.1 in the case where $G = A_n$ is an alternating group with $n \geqslant 5$. First we handle the groups of small degree.

Lemma 5.7. *The conclusion to Theorem 5.1 holds if $G = A_n$ and $n \leqslant 15$.*

Proof. This is a routine MAGMA [8] computation. First we construct a set of representatives of the conjugacy classes of maximal subgroups H of G. Then by inspecting the conjugacy classes of elements in H and G, it is straightforward to determine the set of derangements in G (with respect to the action of G on $\Omega = G/H$), and using random search, we can easily find two conjugate derangements that generate G. □

For the remainder of this section, we may assume $n \geqslant 16$. The following number-theoretic lemma will be useful (note that the conclusion is false if $n = 15$).

Lemma 5.8. *Let $n \geqslant 16$ be an integer. Then there exist primes p and q such that $n/2 < p < q \leqslant n - 3$ and $q \neq (n + p)/2$.*

Proof. The cases with $16 \leqslant n \leqslant 40$ can be checked directly, so let us assume $n \geqslant 41$. Then by a theorem of Ramanujan [74], there are at least 5 primes in the interval $(n/2, n]$, which immediately implies that there are primes p_i such that $n/2 < p_1 < p_2 < p_3 \leqslant n - 4$. The result now follows since we can set $p = p_1$ and $q = p_2$ or p_3, ensuring that $q \neq (n + p)/2$. □

Proposition 5.9. *The conclusion to Theorem 5.1 holds if G is an alternating group.*

Proof. Write $G = A_n$. In view of Lemma 5.7, we may assume $n \geqslant 16$, and we fix primes p and q as in Lemma 5.8. Let H be a point stabiliser and set $[n] = \{1, \ldots, n\}$.

First assume H acts transitively on $[n]$ and set $L = \langle x, y \rangle$, where x and y are the p-cycles

$$x = (1, 2, \ldots, p), \quad y = (n - p + 1, \ldots, n).$$

Since $p \geqslant n - p + 1$, it follows that L acts transitively on $[n]$. In addition, since $p > n/2$, we observe that no transitive imprimitive subgroup of G contains an element of order p, so L is primitive. Finally, a classical theorem of Jordan (see [82, Theorem 13.9]) implies that no proper primitive subgroup of G contains a p-cycle, whence $L = G$. In addition, this argument shows that neither x nor y is contained in a proper transitive subgroup of G, so x and y are conjugate derangements, and the result follows.

For the remainder, we may assume H is intransitive. Moreover, without loss of generality, we may assume that $H = (S_k \times S_{n-k}) \cap G$ for some $1 \leqslant k < n/2$, which allows us to identify Ω with the set of k-element subsets of $[n]$.

First assume $n \geqslant 16$ is even. Define the elements

$$x = (1, \ldots, p)(p + 1, \ldots, n)$$
$$y = (1, \ldots, p - 1, p + 1)(p + 2, p, p + 3, \ldots, n)$$

in G and set $L = \langle x, y \rangle$. Note that $y = x^z$, where $z = (p, p + 1, p + 2) \in G$, so x and y are G-conjugate. In addition, note that L is transitive on $[n]$ and x^{n-p} is a p-cycle, so by arguing as above, we deduce that $L = G$. Clearly, x and y are derangements unless $k = n - p$. And if $k = n - p$, then we can redefine x and y with p replaced by q and repeat the argument.

Finally, let us assume $n \geqslant 17$ is odd and set $L = \langle x, y \rangle$, where

$$x = (1, \ldots, p)(p + 1, \ldots, \ell)(\ell + 1, \ldots, n)$$
$$y = (1, \ldots, p - 1, p + 1)(p, p + 2, \ldots, \ell - 1, \ell + 1)(\ell, \ell + 2, \ldots, n)$$

and $\ell = (n + p)/2$. Note that x and y both have cycle-type $[p, (n - p)/2, (n - p)/2]$, so they are conjugate in G. Then L acts transitively on $[n]$ and it contains a p-cycle, so, as before, we deduce that $L = G$.

Table 8. *The elements* $x, y \in G$ *in the proof of Proposition 5.10.*

G	x	y	$\mathcal{M}(x)$	$\mathcal{M}(y)$
M_{11}	11A	8A	$L_2(11)$	M_{10}, $3^2{:}SD_{16}$, $2.S_4$
M_{12}	11A	10A	M_{11}, M_{11}, $L_2(11)$	$A_6.2^2$, $A_6.2^2$, $2 \times S_5$
M_{22}	11A	8A	$L_2(11)$	$2^4{:}A_6$, $2^4{:}S_5$, M_{10}
M_{23}	23A	15A	$23{:}11$	A_8, $2^4{:}(3 \times A_5).2$
M_{24}	23A	21A	M_{23}, $L_2(23)$	$L_3(4){:}S_3$, $2^6{:}(L_3(2) \times S_3)$
J_1	19A	15A	$19{:}6$	$D_6 \times D_{10}$
J_2	10C	7A	$2^{1+4}{:}A_5$, $A_5 \times D_{10}$, $5^2{:}D_{12}$	$U_3(3)$ (two), $L_3(2).2$
J_3	19A	17A	$L_2(19)$, $L_2(19)$	$L_2(16).2$, $L_2(17)$
J_4	43A	29A	$43{:}14$	$29{:}28$
HS	15A	11A	S_8, $5{:}4 \times A_5$	M_{22}, M_{11}, M_{11}
He	17A	14C	$Sp_4(4).2$	$2^{1+6}.L_3(2)$, $7^2{:}2.L_2(7)$, $7^{1+2}{:}(S_3 \times 3)$
McL	15A	11A	$3^{1+4}{:}2S_5$, $2.A_8$, $5^{1+2}{:}3{:}8$	M_{22}, M_{22}, M_{11}
Suz	14A	13A	$J_2.2$ (two), $(A_4 \times L_3(4)){:}2$	$G_2(4)$, $L_3(3).2$, $L_3(3).2$, $L_2(25)$ (three)
Ru	29A	26A	$L_2(29)$	$(2^2 \times {}^2B_2(8)){:}3$, $L_2(25).2^2$ (two)
O'N	31A	19A	$L_2(31)$, $L_2(31)$	$L_3(7).2$, $L_3(7).2$, J_1
Co_1	26A	23A	$(A_4 \times G_2(4)){:}2$	Co_2, Co_3, M_{24}
Co_2	30A	23A	$U_6(2).2$, $2^{1+8}{:}Sp_6(2)$, HS.2	M_{23}
Co_3	30A	23A	McL.2, $2.Sp_6(2)$, $U_3(5){:}S_3$, $3^{1+4}{:}4S_6$	M_{23}
HN	22A	19A	$2.HS.2$	$U_3(8).3$
Ly	67A	37A	$67{:}22$	$37{:}18$
Th	39A	36A	$(3 \times G_2(3)){:}2$	$2^{1+8}.A_9$, $3.[3^8].2S_4$
Fi_{22}	22A	13A	$2.U_6(2)$	$\Omega_7(3)$, $\Omega_7(3)$, ${}^2F_4(2)$
Fi_{23}	35A	23A	S_{12}	$2^{11}.M_{23}$, $L_2(23)$
Fi'_{24}	29A	23A	$29{:}14$	Fi_{23}, $2^{11}.M_{24}$
$\mathbb{B}$	55A	47A	$5{:}4 \times HS.2$, $S_5 \times M_{22}{:}2$	$47{:}23$
$\mathbb{M}$	71A	59A	$L_2(71)$	$L_2(59)$

Moreover, x and y are derangements unless $k \in \{(n - p)/2, n - p\}$, so let us assume we are in one of these two cases. Here we can repeat the argument, replacing p by q in the construction of x and y, noting that the condition $q \neq (n + p)/2$ in Lemma 5.8 implies that x and y are derangements on Ω when $k \in \{(n - p)/2, n - p\}$. □

5.2. Sporadic groups

Next let us turn to the sporadic groups. Here we adopt a computational approach, working extensively with Lemma 5.4. As before, we write $\mathbb{B}$ and $\mathbb{M}$ for the Baby Monster and Monster sporadic groups, respectively.

Proposition 5.10. *The conclusion to Theorem 5.1 holds if G is a sporadic group.*

Proof. First assume $G \neq \mathbb{B}, \mathbb{M}$. Using GAP [40] and the information available in the GAP Character Table Library [12], it is straightforward to evaluate the expression in (5.3) for all $y, z \in G$ (of course, to do this, we only need to work with a set of conjugacy class representatives). In every case, we can combine this with Lemma 5.2 to identify witnesses x and y satisfying all the conditions in Lemma 5.4, which gives the desired result. Two such elements are recorded in Table 8 (using the standard Atlas [24] labelling for conjugacy classes), together with the maximal overgroups $\mathcal{M}(x)$ and $\mathcal{M}(y)$ (see (5.1)), as well as Remark 5.11 below.

Next assume $G = \mathbb{B}$ and fix elements $x \in 55A$ and $y \in 47A$. The character table of every maximal subgroup of G is available in [12], and just by considering element orders, it is easy to check that every maximal overgroup of y is of the form $H = 47{:}23$. Moreover, we can compute the permutation character $\chi = 1_H^G$, and we find that $\chi(y) = 1$, which implies that y is contained in a unique maximal subgroup of G (namely, $N_G(\langle y \rangle) = 47{:}23$). Then by applying Lemma 5.2, we deduce that y is a witness. Similarly, one can check that $\mathcal{M}(x) = \{5{:}4 \times HS.2, S_5 \times M_{22}{:}2\}$, and once again, we see that x is a witness. The result now follows from Lemma 5.4.

Table 9. *The elements $x, y \in G$ in the proof of Lemma 5.12, $G \in \mathcal{A}$.*

G	x	y	$\mathcal{M}(x)$	$\mathcal{M}(y)$
$^2G_2(3)'$	7A	3A	$2^3{:}7$ (two), D_{14}	D_{18}
$G_2(2)'$	12A	7A	$3^{1+2}.D_8$, $4.S_4$	$L_3(2)$
$G_2(3)$	13A	9A	$L_3(3){:}2$, $L_3(3){:}2$, $L_2(13)$	$(3^2 \times 3^{1+2}){:}2S_4$, $(3^2 \times 3^{1+2}){:}2S_4$, $L_2(8){:}3$ (three)
$G_2(4)$	21A	13A	$3.L_3(4){:}2$	$U_3(4){:}2$, $L_2(13)$
$^2F_4(2)'$	16A	13A	$2.[2^8].5.4$, $2^2.[2^8].S_3$	$L_3(3).2$, $L_3(3).2$, $L_2(25)$ (three)
$^3D_4(2)$	13A	7D	$13{:}4$	$G_2(2)$ (seven), $(7 \times \mathrm{SL}_3(2)).2$ (four), $7^2.\mathrm{SL}_2(3)$
$F_4(2)$	28A	17A	$[2^{15}].\mathrm{Sp}_6(2)$, $^3D_4(2).3$, $[2^{20}].(S_3 \times L_3(2))$ (two), $L_3(2)^2.2$	$\mathrm{Sp}_8(2)$, $\mathrm{Sp}_8(2)$
$^2E_6(2)$	19A	13A	$U_3(8).3$	$F_4(2)$, $F_4(2)$, $F_4(2)$, Fi_{22} (two), Fi_{22} (two), Fi_{22} (two)

Finally, let us assume $G = \mathbb{M}$ is the Monster. Fix $x, y \in G$, where $x \in$ 71A and $y \in$ 59A. By inspecting the list of maximal subgroups of G (see [28, Table 1]), it is easy to see that $L_2(71)$ is the only maximal subgroup containing an element of order 71. And similarly, $L_2(59)$ is the only maximal subgroup with an element of order 59. In both cases, we can use [12] to compute the corresponding permutation characters, and we conclude that x and y both have unique maximal overgroups. As above, the result now follows from Lemma 5.4. □

Remark 5.11. In the final two columns of Table 8, we list the maximal subgroups in the sets $\mathcal{M}(x)$ and $\mathcal{M}(y)$. In order to clarify our notation, note that if $G = M_{12}$ and $x \in$ 11A, then $\mathcal{M}(x)$ contains two non-conjugate subgroups isomorphic to M_{11}. However, if $G = J_2$ and $y \in$ 7A, then $\mathcal{M}(y)$ contains two conjugate subgroups isomorphic to $U_3(3)$.

5.3. *Exceptional groups*

In this section, we assume G is a finite simple exceptional group of Lie type over $\mathbb{F}_q$, where $q = p^f$ and p is a prime. We begin by handling the groups in $\mathcal{A}$, which is defined as follows:

$$\mathcal{A} = \{{}^2G_2(3)', G_2(2)', G_2(3), G_2(4), {}^2F_4(2)', {}^3D_4(2), F_4(2), {}^2E_6(2)\}.$$

Lemma 5.12. *The conclusion to Theorem 5.1 holds if $G \in \mathcal{A}$.*

Proof. For $G \neq {}^2E_6(2)$, we can proceed as in the proof of Proposition 5.10, working the GAP Character Table Library [12] to evaluate the expression in (5.3) for all $y, z \in G$. In this way, using Lemma 5.2, we can find two elements $x, y \in G$ satisfying the conditions in Lemma 5.4, and the result follows (two such elements are presented in Table 9 with respect to the standard Atlas [24] notation for conjugacy classes, together with the respective maximal overgroups $\mathcal{M}(x)$ and $\mathcal{M}(y)$).

To complete the proof, we may assume $G = {}^2E_6(2)$. The maximal subgroups of G have been determined up to conjugacy by Wilson in [83] (also see Tables 3 and 10 in [25]). Fix elements $x \in$ 19A and $y \in$ 13A.

By inspecting the orders of the maximal subgroups of G, we find that $H = U_3(8).3$ is the only one containing an element of order 19. Moreover, we can use GAP to compute the character $\chi = 1_H^G$, and we deduce that $\chi(x) = 1$. Therefore, $\mathcal{M}(x) = \{H\}$, and thus x is a witness by Lemma 5.2.

Now let us consider y, which represents the unique conjugacy class of elements of order 13 in G. By inspection, we see that each $H \in \mathcal{M}(y)$ is isomorphic to $F_4(2)$ or Fi_{22}, noting that there are three conjugacy classes of each type. By working with the corresponding permutation characters, we deduce that $\mathcal{M}(y)$ comprises three subgroups isomorphic to $F_4(2)$, which represent the three classes of maximal subgroups of this type, together with six subgroups isomorphic to Fi_{22} (two subgroups from each of the

Table 10. The elements $x, y \in G$ in the proof of Proposition 5.14, $G \notin \mathcal{A}$, $G \neq {}^3D_4(q)$.

G		$|x|$	$|y|$	$\mathcal{M}(x)$	$\mathcal{M}(y)$
${}^2B_2(q)$		$q + \sqrt{2q} + 1$	$q - \sqrt{2q} + 1$	$T_x.4$	$T_y.4$
${}^2G_2(q)$		$q + \sqrt{3q} + 1$	$q - \sqrt{3q} + 1$	$T_x.6$	$T_y.6$
$G_2(q)$	$q \equiv \varepsilon \pmod 3$	$q^2 - \epsilon q + 1$	$q^2 + \epsilon q + 1$	$\mathrm{SL}_3^{-\epsilon}(q).2$	$\mathrm{SL}_3^{\epsilon}(q).2$
	$p = 3$	$q^2 + q + 1$	$q^2 - q + 1$	$\mathrm{SL}_3(q).2$ (two)	$\mathrm{SU}_3(q).2$ (two)
${}^2F_4(q)$		α^+	α^-	$T_x.12$	$T_y.12$
$F_4(q)$	$p \neq 2$	$q^4 - q^2 + 1$	$q^4 + 1$	${}^3D_4(q).3$	$2.\Omega_9(q)$
	$p = 2$	$q^4 - q^2 + 1$	$q^4 + 1$	${}^3D_4(q).3$ (two)	$\mathrm{Sp}_8(q)$ (two)
$E_6(q)$		Φ_9/e	$\Phi_{12}\Phi_3/e$	$\mathrm{L}_3(q^3).3$	$({}^3D_4(q) \times (q^2 + q + 1)/e).3$
${}^2E_6(q)$		Φ_{18}/e'	$\Phi_{12}\Phi_6/e'$	$\mathrm{U}_3(q^3).3$	$({}^3D_4(q) \times (q^2 - q + 1)/e').3$
$E_7(q)$	$q \geqslant 3$	$\Phi_{18}\Phi_2/d$	$\Phi_9\Phi_1/d$	H_1	H_2, H_3 (two)
	$q = 2$	129	73	$\mathrm{SU}_8(2)$	H_2, H_3 (two)
$E_8(q)$		Φ_{30}	Φ_{15}	$T_x.30$	$T_y.30$

three classes of this type). By [60, Theorem 1], we have $\mathrm{fpr}(z, G/H) \leqslant 1/57$ for all $z \in G$ of prime order and all maximal subgroups H of G, whence

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(z, G/H) \leqslant \frac{9}{57}$$

for all $z \in G$ of prime order. Therefore, y is a witness by Lemma 5.2, and we can now conclude by appealing to Lemma 5.4.   □

For the remainder of this section, we may assume $G \notin \mathcal{A}$. The following lemma will be a useful observation.

Lemma 5.13. *Suppose $G \notin \mathcal{A}$ and $x \in G$ satisfies $|\mathcal{M}(x)| \leqslant 12$. Then x is a witness.*

Proof. This follows by combining Lemma 5.2 with [60, Theorem 1], which implies that $\mathrm{fpr}(z, G/H) \leqslant 1/13$ for all $z \in G$ of prime order and all maximal subgroups H of G.   □

Proposition 5.14. *The conclusion to Theorem 5.1 holds if G is an exceptional group of Lie type.*

Proof. In view of Lemma 5.12, we may assume $G \notin \mathcal{A}$. In every case, we will show that there exist witnesses $x, y \in G$ satisfying the conditions in Lemma 5.4.

For now, let us assume $G \neq {}^3D_4(q)$ and choose $x, y \in G$ as in Table 10. In the table, we write Φ_i for the i-th cyclotomic polynomial evaluated at q and we use the notation $d = (2, q - 1)$, $e = (3, q - 1)$ and $e' = (3, q + 1)$. In addition, for $G = {}^2F_4(q)$, we define

$$\alpha^\varepsilon = q^2 + \varepsilon\sqrt{2q^3} + q + \varepsilon\sqrt{2q} + 1$$

for $\varepsilon = \pm$. For $G = E_7(q)$, we have

$$H_1 = e'.({}^2E_6(q) \times (q + 1)/de').e'.2, \quad H_2 = e.(E_6(q) \times (q - 1)/de).e.2$$

and H_3 is an E_6-parabolic subgroup of type P_7 (in terms of the standard labelling of maximal parabolic subgroups of G).

Observe that in every case, x and y generate distinct maximal tori of G, which we denote by T_x and T_y, respectively. The existence of cyclic tori of the given orders, and hence the existence of x and y, follows from the general theory of tori in finite reductive groups (see [23, Section 3.3], for example). So in view of Lemmas 5.4 and 5.13, it just remains to justify the given description of the sets $\mathcal{M}(x)$ and $\mathcal{M}(y)$ in Table 10.

For now, we will assume $G \neq G_2(q)$. If we exclude the groups

$$\{F_4(q), \, {}^2E_6(q), \, E_7(q) \, : \, q = 2, 3\}, \tag{5.5}$$

then the maximal overgroups of T_x are determined by Weigel [81] and we read off the subgroups in $\mathcal{M}(x)$ recorded in the fourth column of the table. And for the groups in (5.5), we can appeal to the proof of [45, Proposition 6.2]. Similarly, the description of $\mathcal{M}(y)$ in Table 10 follows from [48, Theorem 2.1].

Now suppose $G = G_2(q)$ and recall that $q \geqslant 5$ since we are assuming $G \notin \mathcal{A}$. As above, we can read off $\mathcal{M}(y)$ from [48, Theorem 2.1]. Similarly, our description of $\mathcal{M}(x)$ follows from [81] unless $q \equiv -1 \pmod 3$. Here $|x| = q^2 + q + 1$, and by inspecting the list of maximal subgroups of G (see [10, Tables 8.30, 8.41], for example), it is easy to see that each subgroup in $\mathcal{M}(x)$ is conjugate to $H = \mathrm{SL}_3(q).2$. Moreover, we note that $x^G \cap H$ is the union of two $\mathrm{SL}_3(q)$-classes, both of which have size $|\mathrm{SL}_3(q)|/(q^2 + q + 1)$. Therefore,

$$\mathrm{fpr}(x, G/H) \cdot |G : N_G(H)| = \frac{|x^G \cap H|}{|x^G|} \frac{|G|}{|H|} = 1,$$

and we conclude that x is contained in a unique conjugate of H, as recorded in Table 10.

To complete the proof, we may assume $G = {}^3D_4(q)$ with $q \geqslant 3$ (recall that ${}^3D_4(2) \in \mathcal{A}$). Let $x, y \in G$ be regular semisimple elements with respective orders $q^4 - q^2 + 1$ and $q^2 + q + 1$, and corresponding centralisers of order $q^4 - q^2 + 1$ and $(q^2 + q + 1)^2$. By [47, Proposition 2.11], we have $\mathcal{M}(x) = \{T.4\}$, where $T = \langle x \rangle$ is a maximal torus, and thus x is a witness. So to complete the proof, we may assume G has point stabiliser $H = T.4$.

Now let us consider y. As noted in the proof of [48, Proposition 2.3], each $H \in \mathcal{M}(y)$ is conjugate to one of the following:

$$H_1 = G_2(q), \; H_2 = ((q^2 + q + 1) \circ \mathrm{SL}_3(q)).(q^2 + q + 1, 3).2,$$

$$H_3 = (q^2 + q + 1)^2.\mathrm{SL}_2(3), \; H_4 = \mathrm{PGL}_3(q),$$

where H_4 only arises when $q \equiv 1 \pmod 3$. In particular, y is a derangement on $\Omega = G/H$, and so it just remains to show that $G = \langle y, y^g \rangle$ for some $g \in G$.

For $q = 3$, we can use MAGMA to show that $|\mathcal{M}(y)| = 18$, and the result follows via Lemmas 5.2 and 5.4 since [60, Theorem 1] gives $\mathrm{fpr}(z, G/H) \leqslant 1/73$ for all $z \in G$ of prime order and all maximal subgroups H of G. Now assume $q \geqslant 4$. As noted in Remark 5.5, we just need to show that

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(y, G/H) = \sum_{i=1}^4 n_i \cdot \mathrm{fpr}(y, G/H_i) = |G| \sum_{i=1}^4 |H_i|^{-1} \cdot \mathrm{fpr}(y, G/H_i)^2 < 1,$$

where n_i is the number of conjugates of H_i containing y. Since $|G| < q^{28}$ and $|y^G| > \frac{1}{2} q^{24}$, the crude bound

$$\mathrm{fpr}(y, G/H_i) < \frac{|H_i|}{|y^G|} < 2|H_i| q^{-24}$$

yields

$$|G| \sum_{i=1}^4 |H_i|^{-1} \cdot \mathrm{fpr}(y, G/H_i)^2 < 4q^{-20} \sum_{i=1}^4 |H_i| < 1,$$

and the result follows. □

Table 11. *Singer cycles.*

G	$|y|$	Conditions
$L_n(q)$	$(q^n-1)/e$	$n \geqslant 2$, $e = (n, q-1)(q-1)$
$U_n(q)$	$(q^n+1)/e'$	$n \geqslant 3$ odd, $e' = (n, q+1)(q+1)$
$PSp_n(q)$	$(q^{n/2}+1)/d$	$n \geqslant 4$, $d = (2, q-1)$
$P\Omega_n^-(q)$	$(q^{n/2}+1)/d$	$n \geqslant 8$, $d = (2, q-1)$

5.4. Classical groups

In order to complete the proof of Theorem 5.1, it remains to handle the classical groups. So let G be a finite simple classical group over $\mathbb{F}_q$, where $q = p^f$ and p is a prime. Let V be the natural module and set $n = \dim V$.

As explained at the start of Section 4.4, we may assume that G is one of the groups in (4.3). In addition, we may exclude the groups in (4.4) due to the existence of exceptional isomorphisms involving some of the low-dimensional classical groups.

Recall that the main theorem on the subgroup structure of finite classical groups is due to Aschbacher [2], and we will refer repeatedly to the detailed information on maximal subgroups in [10, 57]. Also recall that the *type* of a maximal subgroup gives an approximate description of its structure. For example, if $G = L_6(q)$ and H is the stabiliser of a direct sum decomposition $V = V_1 \oplus V_2 \oplus V_3$ of the natural module into 2-spaces, then we say that H is a subgroup of type $GL_2(q) \wr S_3$, noting that the precise structure can be read off from [57, Proposition 4.2.9] (also see [10, Table 8.24]). Detailed information on the maximal subgroups of classical groups is presented in [10, 57], including a complete classification (up to conjugacy) for the groups with $n \leqslant 12$.

Let us also recall that if $e, q \geqslant 2$ are integers, then a prime divisor r of $q^e - 1$ is a *primitive prime divisor* (ppd for short) if r does not divide $q^i - 1$ if $i < e$. By a theorem of Zsigmondy [85], a ppd exists unless $(e, q) = (6, 2)$, or if $e = 2$ and q is a Mersenne prime. If G is a classical group as above and $x \in G$ has prime order r, where r is a ppd of $q^e - 1$ with $e > n/2$, then the maximal overgroups of x (up to conjugacy) are described in [49], and we will use this important result in several proofs.

Let G be one of the groups listed in Table 11 and recall that an element $y \in G$ is a *Singer cycle* if the order of y is as given in the table. Note that every Singer cycle acts irreducibly on the natural module V. In the proof of the following result, we write $\pi(\ell)$ for the set of prime divisors of the integer $\ell \geqslant 2$.

Proposition 5.15. *Every Singer cycle is a witness.*

Proof. Let G be one of the groups in Table 11 and let $y \in G$ be a Singer cycle. We will consider each possibility for G in turn.

First assume $G = L_n(q)$ is a linear group, so $n \geqslant 2$ and $(n, q) \neq (2, 2), (2, 3)$. We begin by claiming that

$$\mathcal{M}(y) = \begin{cases} \{S_3, \, A_4(\text{two})\} & \text{if } (n, q) = (2, 5) \\ \{S_4, \, S_4\} & \text{if } (n, q) = (2, 7) \\ \{A_5, \, A_5\} & \text{if } (n, q) = (2, 9) \\ \{L_3(2), \, L_3(2), \, L_3(2)\} & \text{if } (n, q) = (3, 4) \\ \{H_k \, : \, k \in \pi(n)\} & \text{otherwise,} \end{cases} \tag{5.6}$$

where H_k is a field extension subgroup of type $GL_{n/k}(q^k)$. Here our notation indicates that $\mathcal{M}(y)$ contains two conjugate subgroups isomorphic to A_4 when $G = L_2(5)$, and it contains two non-conjugate subgroups isomorphic to S_4 when $G = L_2(7)$.

The groups with $(n, q) = (2, 5), (2, 7), (2, 9)$ and $(3, 4)$ can be handled using Magma, so we may assume that we are not in one of these cases. Then by the main theorem of [5], each $H \in \mathcal{M}(y)$ is a field extension subgroup of type $GL_{n/k}(q^k)$, where k is a prime divisor of n. Moreover, [13, Lemma 2.12]

implies that y is contained in a unique subgroup of type $GL_{n/k}(q^k)$ for each prime k, so this justifies (5.6), and it just remains to show that y is a witness. We will do this by establishing the inequality (5.2) in Lemma 5.2.

If $n \leqslant 5$, then $|\mathcal{M}(y)| = 1$, and thus (5.2) holds for all $z \in G$ of prime order. Now assume $n \geqslant 6$ and $H \in \mathcal{M}(y)$. Fix an element $z \in G$ of prime order and note that

$$\mathrm{fpr}(z, G/H) < |z^G|^{-\frac{1}{2}+\frac{1}{n}}$$

by the main theorem of [16]. Now $|\mathcal{M}(y)| = |\pi(n)| < \log_2 n$, and it is straightforward to show that $|z^G| > q^{2n-2}$ (see [17, Section 3], for example). Therefore,

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(z, G/H) < \log_2 n \left(q^{2n-2}\right)^{-\frac{1}{2}+\frac{1}{n}},$$

and it is easy to check that this upper bound is less than 1 for all $n \geqslant 6$ and $q \geqslant 2$.

Next assume $G = U_n(q)$, where $n \geqslant 3$ is odd and $(n, q) \neq (3, 2)$. Here we claim that

$$\mathcal{M}(y) = \begin{cases} \{L_2(7)\} & \text{if } (n, q) = (3, 3) \\ \{A_7, A_7, A_7\} & \text{if } (n, q) = (3, 5) \\ \{L_2(11)\} & \text{if } (n, q) = (5, 2) \\ \{H_k : k \in \pi(n)\} & \text{otherwise,} \end{cases} \tag{5.7}$$

where H_k is a field extension subgroup of type $GU_{n/k}(q^k)$. For $(n, q) = (3, 3), (3, 5)$ or $(5, 2)$, we can use MAGMA to verify the result (note that if $(n, q) = (3, 5)$, then G has three conjugacy classes of maximal subgroups isomorphic to A_7 and $\mathcal{M}(y)$ contains a representative from each class). And in each of the remaining cases, we apply [13, Proposition 5.21].

Now suppose $G = PSp_n(q)$ is a symplectic group, where $n = 2m \geqslant 4$ and $(n, q) \neq (4, 2)$. We claim that

$$\mathcal{M}(y) = \begin{cases} \{H_2, 2^4.A_5 \text{ (two)}\} & \text{if } (n, q) = (4, 3) \\ \{H_3\text{(three)}, O_6^-(2)\} & \text{if } (n, q) = (6, 2) \\ \{H_2, O_8^-(2), L_2(17)\} & \text{if } (n, q) = (8, 2) \\ \{H_k : k \in \pi(m)\} \cup \mathcal{J} & \text{otherwise,} \end{cases} \tag{5.8}$$

where H_k is a field extension subgroup of type $Sp_{n/k}(q^k)$ and

$$\mathcal{J} = \begin{cases} \{H\} & \text{if } q \text{ is even} \\ \{K\} & \text{if } qm \text{ is odd} \\ \emptyset & \text{otherwise} \end{cases}$$

with H, K of type $O_n^-(q)$ and $GU_m(q)$, respectively.

In order to justify the claim, first assume q is even. The cases $(n, q) = (6, 2), (8, 2)$ can be checked directly, and for each of the remaining groups, we can appeal to [13, Proposition 5.8] (and its proof). As indicated in (5.8), if $G = Sp_6(2)$, then y is contained in exactly 3 conjugate field extension subgroups of type $Sp_2(2^3)$ (this observation was not noted in the proof of [13, Proposition 5.8], and it was also incorrectly omitted in the statement of [21, Lemma 8.7]).

Now assume q is odd. The case $(n, q) = (4, 3)$ can be handled directly. For the remaining groups, the main theorem of [5] implies that each $H \in \mathcal{M}(y)$ is a field extension subgroup of type $Sp_{n/k}(q^k)$ or $GU_m(q)$, noting in the latter case that H contains a Singer cycle if and only if m is odd. The description of $\mathcal{M}(y)$ in (5.8) now follows from [13, Lemma 2.12].

To complete the argument for symplectic groups, we need to show that y is a witness when q is odd and $(n, q) \neq (4, 3)$. If $n = 4$, then $|\mathcal{M}(y)| = 1$, and the result follows from Lemma 5.2, so we

may assume $n \geqslant 6$. Fix a subgroup $H \in \mathcal{M}(y)$ and let $z \in G$ be an element of prime order. Now $|\mathcal{M}(y)| < \log_2 n$ and $|z^G| \geqslant (q^n - 1)/2$, so by applying the main theorem of [16], we deduce that

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(z, G/H) < \log_2 n \left(\frac{1}{2}(q^n - 1) \right)^{-\frac{1}{2} + \frac{1}{n} + \frac{1}{n+2}}.$$

It is routine to check that this upper bound is less than 1 for all $n \geqslant 6$, $q \geqslant 3$, and the result follows.

To complete the proof, let $G = \mathrm{P\Omega}_n^-(q)$ with $n = 2m \geqslant 8$. By combining the main theorem of [5] with [13, Lemma 2.12], we deduce that

$$\mathcal{M}(y) = \{ H_k \ : \ k \in \pi(m) \} \cup \mathcal{J}, \tag{5.9}$$

where H_k is a field extension subgroup of type $\mathrm{O}_{n/k}^-(q^k)$ and

$$\mathcal{J} = \begin{cases} \{H\} & \text{if } m \text{ is odd} \\ \emptyset & \text{otherwise} \end{cases}$$

with H of type $\mathrm{GU}_m(q)$. If $z \in G$ has prime order, then by combining the bounds $|\mathcal{M}(x)| < \log_2 n$ and $|z^G| > q^{2n-6}$ with the main theorem of [16], we get

$$\sum_{H \in \mathcal{M}(y)} \mathrm{fpr}(z, G/H) < \log_2 n \left(q^{2n-6} \right)^{-\frac{1}{2} + \frac{1}{n} + \frac{1}{n-2}} < 1$$

for all $n \geqslant 8$, $q \geqslant 2$, and the result follows via Lemma 5.2. $\qquad \square$

We are now ready to prove Theorem 5.1 for classical groups. It is convenient to use MAGMA to verify the result for some of the low-dimensional classical groups defined over small fields. With this aim in mind, let $\mathcal{B}$ denote the following collection of groups:

$L_2(11), L_3(2), L_3(3), L_3(4), L_4(3)$

$U_3(4), U_3(5), U_4(2), U_4(3), U_4(4), U_4(5), U_5(2), U_5(3), U_5(4), U_6(2), U_6(3), U_7(2)$

$\mathrm{PSp}_4(3), \mathrm{Sp}_4(4), \mathrm{PSp}_4(5), \mathrm{Sp}_6(2), \mathrm{PSp}_6(3), \mathrm{Sp}_6(4), \mathrm{Sp}_8(2), \mathrm{Sp}_{10}(2), \mathrm{Sp}_{12}(2)$

$\Omega_7(3), \Omega_8^\pm(2), \mathrm{P\Omega}_8^\pm(3), \Omega_8^+(4), \mathrm{P\Omega}_8^+(5), \Omega_{10}^\pm(2), \mathrm{P\Omega}_{10}^\pm(3), \Omega_{12}^\pm(2), \mathrm{P\Omega}_{12}^\pm(3)$

Proposition 5.16. *The conclusion to Theorem 5.1 holds if $G \in \mathcal{B}$.*

Proof. We can proceed as in the proof of Lemma 5.7, working with MAGMA [8]. Set $\Omega = G/H$, where H is a maximal subgroup of G. For the computation, it is convenient to work in the corresponding matrix group $L \in \{\mathrm{SL}_n^\varepsilon(q), \mathrm{Sp}_n(q), \Omega_n^\varepsilon(q)\}$, so we have $G = L/Z$ and $H = J/Z$, where $Z = Z(L)$. We can use the function ClassicalMaximals to construct a conjugate of J, and by taking conjugacy classes, we can determine the set $\Delta(L, J)$ of derangements in L with respect to the action on L/J. Finally, we use random search to find elements $x \in \Delta(L, J)$ and $y \in L$ such that $L = \langle x, x^y \rangle$, which in turn implies that G is generated by two conjugate derangements on Ω. $\qquad \square$

Remark 5.17. For the groups in $\mathcal{B}$ that are handled in Proposition 5.16, there is often no need to determine the complete set of derangements in order to reach the desired conclusion. For example, in many cases, we can simply construct L and J as in the proof of the proposition, and then randomly search for elements $x, y \in L$ such that $L = \langle x, x^y \rangle$ and $|J|$ is indivisible by $|x|$, which means that $x \in \Delta(L, J)$. Alternatively, we can construct a set representatives of the conjugacy classes in J and then seek random elements $x, y \in L$ such that $L = \langle x, x^y \rangle$ and J does not contain a conjugate of x (and in many cases, we can simply check that J has no element of order $|x|$).

We begin by considering the linear groups.

Proposition 5.18. *The conclusion to Theorem 5.1 holds if $G = L_n(q)$ is a linear group.*

Proof. As noted above (see (4.4)), we may assume $(n, q) \neq (4, 2)$ and $q \geqslant 11$ if $n = 2$. And in view of Proposition 5.16, we may assume $G \notin \mathcal{B}$. Set $d = (n, q - 1)$ and $e = d(q - 1)$. As usual, we write P_k for the stabiliser in G of a k-dimensional subspace of V.

Let $x \in G$ be a Singer cycle. By Proposition 5.15, x is a witness and each $H \in \mathcal{M}(x)$ is a field extension subgroup of type $\text{GL}_{n/k}(q^k)$, one for each prime divisor k of n (see (5.6)).

Let $y \in G$ be an element of order $(q^{n-1} - 1)/d$ and note that y fixes a decomposition $V = U \oplus W$ of the natural module, where W is an $(n - 1)$-dimensional subspace on which y acts irreducibly. We claim that y is a witness and

$$\mathcal{M}(y) = \begin{cases} \{D_{2(q-1)/d}, \, P_1(\text{two})\} & \text{if } n = 2 \text{ and } q \geqslant 13 \\ \{P_1, \, P_{n-1}\} & \text{if } n \geqslant 3 \text{ and } (n, q) \neq (3, 2), (3, 3), (3, 4), (4, 2), \end{cases}$$

so the desired result follows from Lemma 5.4.

To justify the claim, first assume $n = 2$ and $q \geqslant 13$. By inspecting [10, Tables 8.1, 8.2], we deduce that $\mathcal{M}(y)$ comprises $N_G(\langle y \rangle) = D_{2(q-1)/d}$, together with two P_1 parabolic subgroups (note that y is only contained in two such subgroups because it fixes exactly two 1-dimensional subspaces of V). By applying the main theorem of [66], we deduce that $\text{fpr}(z, G/H) < 1/3$ for all $z \in G$ of prime order and all $H \in \mathcal{M}(y)$, so Lemma 5.2 implies that y is a witness.

Now assume $n \geqslant 3$. Clearly, U and W are the only proper nonzero subspaces of V fixed by y, which implies that y is contained in unique P_1 and P_{n-1} parabolic subgroups. If we can show that $\mathcal{M}(y) = \{P_1, P_{n-1}\}$, then the result will follow via Lemmas 5.2 and 5.4 since

$$\text{fpr}(z, G/H) \leqslant \frac{2^{n-1} - 1}{2^n - 1} < \frac{1}{2}$$

for all $z \in G$ of prime order and $H \in \{P_1, P_{n-1}\}$ (maximal when $q = 2$ and z is a transvection). So it just remains to show that y is not contained in a proper irreducible subgroup.

For $n = 3$, this can be checked by inspecting the list of maximal subgroups of G presented in [10, Tables 8.3, 8.4], so let us assume $n \geqslant 4$. The case $(n, q) = (7, 2)$ can be verified directly, which means that we may assume $|y|$ is divisible by a primitive prime divisor r of $q^{n-1} - 1$. The maximal subgroups of G containing an element of order r are described in [49]. Using this, together with the fact that $|y| = (q^{n-1} - 1)/d$, it is a straightforward exercise to show that $\mathcal{M}(y) = \{P_1, P_{n-1}\}$ as required (see the proof of Theorem 3.16, where we used [49] to study the maximal overgroups of the element y defined in Proposition 3.20). This justifies the claim and the proof is complete. □

Next we prove Theorem 5.1 for the unitary groups.

Proposition 5.19. *The conclusion to Theorem 5.1 holds if $G = U_n(q)$ is a unitary group.*

Proof. We may assume $n \geqslant 3$. Recall that $U_3(2)$ is soluble and $U_3(3) \cong G_2(2)'$ was handled in Lemma 5.12, so we may assume $q \geqslant 4$ when $n = 3$. In addition, we may assume $G \notin \mathcal{B}$ (see Proposition 5.16). We will write P_k (respectively, N_k) for the stabiliser of a k-dimensional totally isotropic (respectively, non-degenerate) subspace of the natural module V. Set $d = (n, q + 1)$ and $e = d(q + 1)$.

Case 1. n is odd

First assume n is odd. Let $x \in G$ be a Singer cycle. Then Proposition 5.15 implies that x is a witness and (5.7) indicates that each $H \in \mathcal{M}(x)$ is a field extension subgroup of type $\text{GU}_{n/k}(q^k)$. In particular, each maximal overgroup of x acts irreducibly on V.

For $n = 2m + 1 \geqslant 9$, we define $y \in G$ as in [45, Table II]. Then y is a witness by [45, Proposition 4.1], and the final column of [45, Table II] indicates that each $H \in \mathcal{M}(y)$ acts reducibly on V. We now conclude by applying Lemma 5.4.

Now assume $n \in \{3, 5, 7\}$. Let $y \in G$ be a regular semisimple element of order $q^{n-2} + 1$ with $|C_G(y)| = (q^{n-2} + 1)(q + 1)/d$. More specifically, for $n = 3$, we take y to be the image of the diagonal matrix $\operatorname{diag}(\lambda, \lambda^2, \lambda^{q-2}) \in \operatorname{SU}_3(q)$ with respect to an orthonormal basis for V, where $\mathbb{F}_{q^2}^\times = \langle \mu \rangle$ and $\lambda = \mu^{q-1}$. Note that y fixes an orthogonal decomposition

$$V = U \perp W_1 \perp W_2$$

of the natural module, where each summand is non-degenerate and the W_i are 1-dimensional.

We claim that

$$\mathcal{M}(y) = \begin{cases} \{G_{W_1}, G_{W_2}, G_{U^\perp}\} = \{N_1 \text{ (two)}, N_2\} & \text{if } n \in \{5, 7\} \text{ and } (n, q) \neq (5, 2) \\ \{G_{W_1}, G_{W_2}, G_U, K\} = \{N_1 \text{ (three)}, K\} & \text{if } n = 3 \text{ and } q \geqslant 7, \end{cases}$$

where K is a subgroup of type $\operatorname{GU}_1(q) \wr S_3$.

Since y acts irreducibly on U, it is clear that the reducible subgroups in $\mathcal{M}(y)$ are as described. For $n \in \{5, 7\}$, we note that some power of y has order r, where r is a primitive prime divisor of $q^{2n-4} - 1$, and it is easy to verify the above claim by inspecting the maximal subgroups of G in [10]. Now assume $n = 3$, so $q \geqslant 7$ and representatives of the conjugacy classes of maximal subgroups of G are listed in [10, Tables 8.5, 8.6]. Visibly, y fixes a unique orthogonal decomposition of V into non-degenerate 1-spaces, so it is contained in a unique subgroup of type $\operatorname{GU}_1(q) \wr S_3$. In addition, if q is odd, then y is not contained in a subgroup of type $\operatorname{O}_3(q)$ (since by construction, y does not lift to an element in $\operatorname{SU}_3(q)$ with a nonzero 1-eigenspace). None of the remaining irreducible maximal subgroups of G contain an element of order $|y|$, and this establishes the claim.

We now complete the proof of the proposition for $n \in \{3, 5, 7\}$. Recall that we may assume $G \notin \mathcal{B}$, so $q \geqslant Q$ where $Q = 7, 5, 3$ for $n = 3, 5, 7$. In view of Lemma 5.4, it suffices to show that y is a witness. If $n = 3$, then $|\mathcal{M}(y)| = 4$, and the main theorem of [66] yields $\operatorname{fpr}(z, G/H) \leqslant 4/21$ for all $H \in \mathcal{M}(y)$ and all $z \in G$ of prime order. Now apply Lemma 5.2. Similarly, if $n \in \{5, 7\}$ and $q \geqslant 5$, then the bound $\operatorname{fpr}(z, G/H) \leqslant 4/15$ from [66] is good enough. So this just leaves $(n, q) = (7, 3), (7, 4)$. Here [45, Proposition 3.16] implies that $\operatorname{fpr}(z, G/H) < 1/3$ for all $H \in \mathcal{M}(y)$, and once again, the result follows from Lemma 5.2.

Case 2. n is even

For the remainder, we may assume $n = 2m \geqslant 4$ is even. In view of Proposition 5.16, we may assume $q \geqslant 7$ if $n = 4$, and $q \geqslant 4$ if $n = 6$. Let $x \in G$ be an element of order $(q^{n-1} + 1)/d$. Then [13, Proposition 5.22] gives $\mathcal{M}(x) = \{N_1\}$, and thus x is a witness.

Suppose $n \geqslant 8$ and let $y \in G$ be an element of order $(q^{m+\delta} + 1)(q^{m-\delta} + 1)/e$, where $\delta = 1$ if m is even, otherwise $\delta = 2$. By inspecting [45, Table II], we see that $\mathcal{M}(y) = \{N_{m-\delta}\}$, so y is a witness and we conclude via Lemma 5.4. So to complete the proof, we may assume $n = 4$ or 6.

Suppose $n = 6$ with $q \geqslant 4$ and let $y \in G$ be a regular semisimple element of order $(q^6 - 1)/e$. Now y fixes a decomposition $V = U \oplus W$ of the natural module, where U and W are totally isotropic 3-spaces on which y acts irreducibly. In particular, U and W are the only proper nonzero subspaces of V fixed by y, so $\mathcal{M}(y)$ contains two P_3 parabolic subgroups (namely, the stabilisers of U and W), together with a unique subgroup of type $\operatorname{GL}_3(q^2)$ corresponding to the stabiliser of the decomposition $V = U \oplus W$. By inspecting [10, Tables 8.26, 8.27], it is clear that any additional subgroup in $\mathcal{M}(y)$ must be a field extension subgroup of type $\operatorname{GU}_2(q^3)$. By arguing as in the proof of [21, Lemma 8.7], we deduce that y is contained in exactly one such subgroup, and thus $|\mathcal{M}(y)| = 4$. For $H = P_3$, [45, Proposition 3.15] implies that $\operatorname{fpr}(z, G/H) < 1/6$ for all $z \in G$ of prime order, while the main theorem of [66] yields $\operatorname{fpr}(z, G/H) \leqslant 1/3$ for H of type $\operatorname{GL}_3(q^2)$ or $\operatorname{GU}_2(q^3)$. Therefore, (5.2) holds, and thus y is a witness by Lemma 5.2. As before, we now complete the argument by appealing to Lemma 5.4.

Finally, suppose $n = 4$ with $q \geqslant 7$. Let $y \in G$ be a regular semisimple element of order $(q^4 - 1)/e$. By inspecting [10, Tables 8.10, 8.11], it is easy to see that $\mathcal{M}(y)$ comprises two P_2 parabolic subgroups

and a unique subgroup of type $GL_2(q^2)$. As above, it is straightforward to show that (5.2) holds for all $z \in G$ of prime order, and we now conclude via Lemmas 5.2 and 5.4. □

Proposition 5.20. *The conclusion to Theorem 5.1 holds if* $G = \mathrm{PSp}_n(q)$ *is a symplectic group.*

Proof. We may assume $n = 2m \geqslant 4$, with $(n, q) \neq (4, 2), (4, 3)$ and $G \notin \mathcal{B}$ (see (4.4) and Proposition 5.16). As before, we will write P_k (respectively, N_k) for the stabiliser of a k-dimensional totally isotropic (respectively, non-degenerate) subspace of the natural module V. Set $d = (2, q - 1)$.

First assume $m \geqslant 4$. Let $x \in G$ be a Singer cycle, so x is a witness by Proposition 5.15 and the maximal overgroups of x are listed in (5.8). If q is odd, then we can choose $y \in G$ as in [45, Table II]. Then y is a witness by [45, Proposition 4.1], and we note that every subgroup in $\mathcal{M}(y)$ acts reducibly on V. Since the maximal overgroups of x are irreducible, the desired result follows via Lemma 5.4.

Now assume q is even (with $m \geqslant 4$) and fix $y \in G$ with $|y| = \mathrm{lcm}(q^{m-1} + 1, q + 1)$. Then y fixes an orthogonal decomposition $V = U \perp W$ of the natural module, where $\dim U = 2$ and y acts irreducibly on both summands. We claim that y is a witness and $\mathcal{M}(y) = \{N_2, \mathrm{O}_n^+(q)\}$, which allows us to conclude via Lemma 5.4 once again.

In order to prove the claim, first observe that U and W are the only proper nonzero subspaces of V fixed by y, so the stabiliser N_2 of U is the only reducible subgroup in $\mathcal{M}(y)$. Let us also note that we may embed

$$y \in \mathrm{O}_2^-(q) \times \mathrm{O}_{n-2}^-(q) < \mathrm{O}_n^+(q) = H < G,$$

and we deduce that y is contained in a unique conjugate of H since $y^G \cap H = y^H$ and $C_H(y) = C_G(y)$. In addition, we observe that the action of y on V is not compatible with containment in an orthogonal subgroup $\mathrm{O}_n^-(q)$. At this point, we can now work with [49] to rule out the existence of any additional subgroups in $\mathcal{M}(y)$, noting that $|y|$ is divisible by a primitive prime divisor of $q^{n-2} - 1$ (recall that $\mathrm{Sp}_8(2)$ is in $\mathcal{B}$).

Here it is worth pausing to highlight the special case where $q = 2$, m is even and $H = S_{n+2}$ is irreducibly embedded in G via the fully deleted permutation module (see [49, Example 2.6(a)]). Now $|y| = 2^{m-1} + 1$ and [72, Theorem 2] gives

$$\log |z| \leqslant \sqrt{\ell \log \ell}\left(1 + \frac{\log \log \ell - \alpha}{2 \log \ell}\right)$$

for all $z \in H$, where $\ell = n + 2$ and $\alpha = 0.975$ (where log denotes the natural logarithm). It is straightforward to check that this upper bound implies that $|z| < |y|$ for all $m \geqslant 20$. And one can check directly that H does not contain an element of order $|y|$ if $8 \leqslant m \leqslant 18$, so there are no such subgroups in $\mathcal{M}(y)$. However, if $m = 6$, then $H = S_{14}$ has a unique conjugacy class of elements of order $2^5 + 1 = 33$, so for $(n, q) = (12, 2)$, one has to carefully choose y in order to avoid containment in a conjugate of H. This can always be done since G has three classes of such elements, only one of which meets H. But in any case, we should observe that the group $\mathrm{Sp}_{12}(2)$ was handled computationally in Proposition 5.16.

This leaves us with the cases $n = 4, 6$. For $n = 6$ with $q \geqslant 4$, we take x to be a Singer cycle, and we define y to be a regular semisimple element of order $(q^2 + 1)(q + 1)/d$. Here y fixes an orthogonal decomposition $V = U \perp W$, where U and W are non-degenerate spaces on which y acts irreducibly, with $\dim U = 2$. Then $\mathcal{M}(y) = \{N_2, \mathrm{O}_6^+(q)\}$ if q is even, and $\mathcal{M}(y) = \{N_2\}$ if q is odd (see [45, p.767]), so the result follows by combining (5.8) with Lemma 5.4.

Finally, let us assume $n = 4$ and $q \geqslant 7$. Let $x \in G$ be a Singer cycle and note that $\mathcal{M}(x) = \{\mathrm{Sp}_2(q^2).2, \mathrm{O}_4^-(q)\}$ if q is even and $\mathcal{M}(x) = \{H\}$ if q is odd, where H is a field extension subgroup of type $\mathrm{Sp}_2(q^2)$ (see (5.8)). We define $y \in G$ as follows. For q even, we take y to be a regular semisimple element of order $q + 1$ with $|C_G(y)| = (q + 1)^2$. More precisely, we take $y = \mathrm{diag}(A, A^2)$ with respect to a standard symplectic basis $\{e_1, f_1, e_2, f_2\}$ of the natural module, where $A \in \mathrm{Sp}_2(q)$ is a Singer cycle.

And for q odd, we choose y of order $p(q+1)$ with $|C_G(y)| = q(q+1)$. We claim that y is a witness and $\mathcal{M}(y) = \{H, K\}$, where H is of type $\mathrm{Sp}_2(q) \wr S_2$, and K is of type $\mathrm{O}_4^+(q)$ for q even and type P_1 for q odd. Given the claim, the main theorem of [66] implies that (5.2) holds for all $z \in G$ of prime order, and we conclude by applying Lemmas 5.2 and 5.4. So it just remains to determine the subgroups in $\mathcal{M}(y)$.

Suppose q is even and note that the maximal subgroups of G are listed in [10, Table 8.14]. Here y fixes an orthogonal decomposition $V = U \perp W$ of the natural module, where U and W are non-degenerate 2-spaces on which y acts irreducibly. Since U and W are the only proper nonzero subspaces of V fixed by y, it follows that y is contained in a unique subgroup of type $\mathrm{Sp}_2(q) \wr S_2$. In addition, y is not contained in a parabolic subgroup. Subgroups of type $\mathrm{Sp}_2(q^2)$ or $\mathrm{O}_4^-(q)$ do not contain regular semisimple elements of order $q+1$ with a trivial 1-eigenspace, and we note that $|{}^2B_2(q)|$ is indivisible by $q+1$. Next suppose $L = \mathrm{Sp}_4(q_0)$ is a subfield subgroup with $q = q_0^k$ and k is a prime. If k is odd, then L does not contain any elements of order $q+1$. And if $k = 2$, then each $z \in L$ of order $q+1 = q_0^2 + 1$ is a Singer cycle and the eigenvalues on $V \otimes \mathbb{F}_{q^2}$ of such an element are incompatible with those of y, so there are no subfield subgroups in $\mathcal{M}(y)$. Finally, we note that

$$y \in \mathrm{O}_2^-(q) \times \mathrm{O}_2^-(q) < \mathrm{O}_4^+(q) = H < G,$$

and we calculate that y is contained in a unique conjugate of H.

Now assume q is odd. Here y is the image (modulo scalars) of $\mathrm{diag}(A, B) \in \mathrm{Sp}_4(q)$ with respect to a symplectic basis $\{e_1, f_1, e_2, f_2\}$, where $A \in \mathrm{Sp}_2(q)$ is a Singer cycle and $B \in \mathrm{Sp}_2(q)$ is a transvection. Note that y fixes a unique 1-dimensional subspace of V, so it is contained in a unique P_1 parabolic subgroup. It also fixes a unique orthogonal decomposition $V = U \perp W$ with non-degenerate summands, so y is contained in a unique subgroup of type $\mathrm{Sp}_2(q) \wr S_2$. Finally, by inspecting [10, Tables 8.12, 8.13], we observe that no other maximal subgroup of G contains an element of order $p(q+1)$, and the proof is complete. □

In order to complete the proof of Theorem 5.1, we may assume $G = \mathrm{P\Omega}_n^\varepsilon(q)$ is an orthogonal group with $n \geqslant 7$. As before, P_k will denote the stabiliser in G of a k-dimensional totally singular subspace of V. In addition, if k is even, then we use N_k^δ to denote the stabiliser of a non-degenerate k-space of type $\delta \in \{+, -\}$. (Recall that if k is even then a non-degenerate k-space has *plus-type* if it contains a totally singular subspace of dimension $k/2$; otherwise, it has *minus-type*.)

Proposition 5.21. *The conclusion to Theorem 5.1 holds if $G = \Omega_n(q)$ is an orthogonal group with n odd.*

Proof. Here q is odd and $n = 2m + 1 \geqslant 7$. In view of Proposition 5.16, we may assume $(n, q) \neq (7, 3)$. Let $x \in G$ be a regular semisimple element of order $(q^m + 1)/2$ and note that x fixes an orthogonal decomposition $V = U \perp W$ of V, where U is a non-degenerate minus-type space of dimension $n - 1$. By [13, Proposition 5.20], we have $\mathcal{M}(x) = \{N_{n-1}^-\}$ (the proposition in [13] is stated for $q \geqslant 5$, but the given conclusion still holds when $q = 3$ and $n \geqslant 9$). In particular, x is a witness by Lemma 5.2.

We define $y = \mathrm{diag}(A, B)$, where $A \in \Omega_{n-3}^-(q)$ is a Singer cycle and $B \in \Omega_3(q)$ is a regular unipotent element (so B has Jordan form (J_3) on the natural 3-dimensional module). Note that $|y| = p(q^{m-1} + 1)/2$ and y fixes an orthogonal decomposition $V = U \perp W$, where U is a non-degenerate minus-type space of dimension $n - 3$. We claim that $\mathcal{M}(y) = \{P_1, N_{n-3}^-\}$, in which case the main theorem of [66] implies that (5.2) holds for all $z \in G$ of prime order and we conclude in the usual manner via Lemmas 5.2 and 5.4. So it remains to determine the subgroups in $\mathcal{M}(y)$.

To do this, first note that y fixes exactly three proper nonzero subspaces of V; namely, U and W, together with the totally singular 1-dimensional 1-eigenspace of B on W. Therefore, P_1 and N_{n-3}^- are the only reducible subgroups in $\mathcal{M}(y)$. The existence of an irreducible subgroup in $\mathcal{M}(y)$ can be ruled out by appealing to [49], noting that $|y|$ is divisible by a primitive prime divisor of $q^{n-3} - 1$. We leave the reader to check the details. □

Proposition 5.22. *The conclusion to Theorem 5.1 holds if* $G = P\Omega_n^-(q)$ *is an orthogonal group.*

Proof. We may assume $n = 2m \geqslant 8$. Let $x \in G$ be a Singer cycle, so x is a witness by Proposition 5.15 and the subgroups in $\mathcal{M}(x)$ are recorded in (5.9). For $n \geqslant 14$, we can define $y \in G$ as in [45, Table II]. Then y is a witness by [45, Proposition 4.1], while [45, Table II] indicates that every subgroup in $\mathcal{M}(y)$ acts reducibly on V. So for $n \geqslant 14$, we conclude by applying Lemma 5.4.

To complete the proof, we may assume $n \in \{8, 10, 12\}$. For $q \in \{2, 3\}$, we can use MAGMA to verify Theorem 5.1 directly (see Proposition 5.16), so we are free to assume $q \geqslant 4$. Let $y \in G$ be a regular semisimple element of type $(n-2)^- \perp (1 \oplus 1)$, so y fixes a decomposition $V = U \perp (W_1 \oplus W_2)$ of the natural module, where U is a non-degenerate minus-type space of dimension $n - 2$ on which y acts as a Singer cycle, and the W_i are totally singular 1-spaces. We claim that $\mathcal{M}(y) = \{H, K, L\}$, where H and K are P_1 parabolic subgroups and $L = N_{n-2}^-$.

By construction, y fixes exactly 4 proper nonzero subspaces of V, namely U, W_1, W_2 and $U^\perp = W_1 \oplus W_2$. Therefore, H, K and L are the only reducible subgroups in $\mathcal{M}(y)$. By inspecting the relevant tables in [10, Chapter 8], it is easy to see that there are no additional subgroups in $\mathcal{M}(y)$ and the claim follows.

Finally, let $z \in G$ be an element of prime order. Then by applying the upper bounds on $\mathrm{fpr}(z, G/H)$ in [45, Propositions 3.15, 3.16], we deduce that (5.2) holds, and the result follows via Lemma 5.4. □

Proposition 5.23. *The conclusion to Theorem 5.1 holds if* $G = P\Omega_n^+(q)$ *is an orthogonal group with* $n \geqslant 10$.

Proof. Write $n = 2m$. In view of Proposition 5.16, we may assume $q \geqslant 4$ if $n \in \{10, 12\}$. Define x as in [13, Proposition 5.13] for m odd, and as in [35, Theorem 2.14] for m even. Then as explained in [13, 35], we have

$$\mathcal{M}(x) = \begin{cases} \{N_{m-1}^-\} & \text{if } m \text{ is odd} \\ \{N_{m-2}^-, H, K\} & \text{if } m \text{ is even,} \end{cases}$$

where H and K are non-conjugate field extension subgroups of type $O_m^+(q^2)$ if $m \equiv 2 \pmod 4$ and type $GU_m(q)$ if $m \equiv 0 \pmod 4$. Clearly, if m is odd, then x is a witness. And the same conclusion holds for m even, in view of Lemma 5.2 and the fixed point ratio bounds in [16] and [45, Proposition 3.16].

Let $y \in G$ be a regular semisimple element fixing an orthogonal decomposition $V = U \perp W$ into minus-type non-degenerate spaces, where $\dim U = 2$ and y acts irreducibly on both summands. More precisely, we take y to be the image (modulo scalars) of an element in $\Omega_n^+(q)$ of order $\mathrm{lcm}(q^{m-1} + 1, q + 1)/d$, where $d = (2, q - 1)$. We claim that $\mathcal{M}(y)$ comprises N_2^- (namely, the stabiliser $G_U = G_W$), together with two non-conjugate field extension subgroups of type $GU_m(q)$ when m is even.

To see this, first note that U and W are the only proper nonzero subspaces of V fixed by y, so G_U is the only reducible subgroup in $\mathcal{M}(y)$. Since $|y|$ is divisible by a primitive prime divisor of $q^{n-2} - 1$, we can work with [49] to show that the only additional subgroups in $\mathcal{M}(y)$ are of type $GU_m(q)$ with m even. So let us assume m is even and note that G has two conjugacy classes of subgroups H of type $GU_m(q)$ (see [57, Proposition 4.3.18]). We calculate that $y^G \cap H = y^H$ and $C_G(y) = C_H(y)$, so y is contained in a unique conjugate of H, and the claim follows.

Finally, we can use Lemma 5.2 to show that y is a witness, and we conclude by applying Lemma 5.4. □

The following proposition completes the proof of Theorem 5.1.

Proposition 5.24. *The conclusion to Theorem 5.1 holds if* $G = P\Omega_8^+(q)$.

Proof. The groups with $q \leqslant 5$ can be handled using MAGMA (see Proposition 5.16), so we may assume $q \geqslant 7$. Define $x \in G$ as in [35, Theorem 2.14], which tells us that $\mathcal{M}(x) = \{H, K, L\}$, where H and K are field extension subgroups of type $O_4^+(q^2)$ and L is of type $O_4^-(q) \wr S_2$. In addition, define y as in the

proof of Proposition 5.23. Then $\mathcal{M}(y)$ contains a unique reducible subgroup of type N_2^-, together with two non-conjugate field extension subgroups of type $\mathrm{GU}_4(q)$ (see [45, p.767]), so y is a witness, and the result follows from Lemma 5.4. □

This completes the proof of Theorem G.

References

[1] M. Arezoomand, A. Abdollahi and P. Spiga, 'On problems concerning fixed-point-free permutations and on the polycirculant conjecture – a survey', *Trans. Comb.* **8** (2019), 15–40.

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

[3] M. Aschbacher and R. M. Guralnick, 'Some applications of the first cohomology group', *J. Algebra* **90** (1984), 446–460.

[4] R. A. Bailey, P. J. Cameron, M. Giudici and G. F. Royle, 'Groups generated by derangements', *J. Algebra* **572** (2021), 245–262.

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

[6] E. Bertram, 'Even permutations as a product of two conjugate cycles', *J. Combinatorial Theory Ser. A* **12** (1972), 368–380.

[7] S. R. Blackburn, J. R. Britnell and M. Wildon, 'The probability that a pair of elements of a finite group are conjugate', *J. Lond. Math. Soc.* **86** (2012), 755–778.

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

[9] N. Boston, W. Dabrowski, T. Foguel, P. J. Gies, J. Leavitt and D. T. Ose, 'The proportion of fixed-point-free elements of a transitive permutation group', *Comm. Algebra* **21** (1993), 3259–3275.

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

[11] J. L. Brenner, 'Covering theorems for finite nonabelian simple groups, IX: How the square of a class with two nontrivial orbits in S_n covers A_n', *Ars Combin.* **4** (1977), 151–176.

[12] T. Breuer, *The GAP Character Table Library, Version 1.3.3*, GAP package, http://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib, 2022.

[13] T. Breuer, R. M. Guralnick and W. M. Kantor, 'Probabilistic generation of finite simple groups, II', *J. Algebra* **320** (2008), 443–494.

[14] T. C. Burness, 'Base sizes for primitive groups with soluble stabilisers', *Algebra Number Theory* **15** (2021), 1755–1807.

[15] T. C. Burness, 'Simple groups, generation and probabilistic methods', in *Groups St Andrews 2017 in Birmingham* (London Math. Soc. Lecture Note Series) vol. 455 (Cambridge Univ. Press, Cambridge, 2019), 200–229.

[16] T. C. Burness, 'Fixed point ratios in actions of finite classical groups, I', *J. Algebra* **309** (2007), 69–79.

[17] T. C. Burness, 'Fixed point ratios in actions in finite classical groups, II', *J. Algebra* **309** (2007), 80–138.

[18] T. C. Burness and M. Giudici, *Classical Groups, Derangements and Primes* (Australian Mathematical Society Lecture Series) vol. 25 (Cambridge University Press, Cambridge, 2016).

[19] T. C. Burness, R. M. Guralnick and S. Harper, 'The spread of a finite group', *Ann. of Math.* **193** (2021), 619–687.

[20] T. C. Burness and S. Harper, 'On the uniform domination number of a finite simple group', *Trans. Amer. Math. Soc.* **372** (2019), 545–583.

[21] T. C. Burness and S. Harper, 'Finite groups, 2-generation and the uniform domination number', *Israel J. Math.* **239** (2020), 271–367.

[22] 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.

[23] R. W. Carter, *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters* (Wiley Classics Library) (John Wiley & Sons, Chichester, 1993).

[24] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *ATLAS of Finite Groups* (Oxford University Press, Eynsham, 1985).

[25] D. A. Craven, 'The maximal subgroups of the exceptional groups $F_4(q)$, $E_6(q)$ and $^2E_6(q)$ and related almost simple groups', *Invent. Math.* **234** (2023), 637–719.

[26] D. I. Deriziotis and A. P. Fakiolas, 'The maximal tori in the finite Chevalley groups of type E_6, E_7 and E_8', *Comm. Algebra* **19** (1991), 889–903.

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

[28] H. Dietrich, M. Lee and T. Popiel, 'The maximal subgroups of the Monster', *Adv. Math.* **469** (2025), Paper No. 110214.

[29] J. D. Dixon, 'Random sets which invariably generate the symmetric group', *Discrete Math.* **105** (1992), 25–39.

[30] L. Dornhoff, *Group Representation Theory, Part A: Ordinary Representation Theory* (Pure and Applied Mathematics) vol. 7 (Marcel Dekker, Inc., New York, 1971).

[31] S. Eberhard and D. Garzoni, 'Conjugacy classes of derangements in finite groups of Lie type', *Trans. Amer. Math. Soc. Ser. B* **12** (2025), 536–575.

[32] H. Enomoto, 'The characters of the finite symplectic group $\mathrm{Sp}(4,q)$, $q = 2^f$', *Osaka Math. J.* **9** (1972), 75–94.

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

[34] P. Fleischmann and I. Janiszczak, 'The number of regular semisimple elements for Chevalley groups of classical type', *J. Algebra* **155** (1993), 482–528.

[35] S. D. Freedman, A. Lucchini, D. Nemmi and C. M. Roney-Dougal, 'Finite groups satisfying the independence property', *Internat. J. Algebra Comput.* **33** (2023), 509–545.

[36] J. Fulman and R. M. Guralnick, 'Derangements in finite classical groups for actions related to extension field and imprimitive subgroups and the solution of the Boston-Shalev conjecture', *Trans. Amer. Math. Soc.* **370** (2018), 4601–4622.

[37] J. Fulman and R. M. Guralnick, 'Derangements in subspace actions of finite classical groups', *Trans. Amer. Math. Soc.* **369** (2017), 2521–2572.

[38] 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.

[39] J. Fulman and R. M. Guralnick, 'Derangements in simple and primitive groups', in Groups, Combinatorics & Geometry (Durham, 2001) (World Sci. Publ., River Edge, NJ, 2003), 99–121.

[40] The GAP Group , *GAP – Groups, Algorithms, and Programming*, Version 4.11.1, 2021 (http://www.gap-system.org).

[41] S. Garion, 'Expansion of conjugacy classes in $\mathrm{PSL}_2(q)$', *J. Group Theory* **18** (2015), 961–980.

[42] D. Garzoni, 'Derangements in non-Frobenius groups', Preprint, 2024, arXiv:2409.03305.

[43] M. Geck, G. Hiss, F. Lübeck, G. Malle and G. Pfeiffer, 'CHEVIE–a system for computing and processing generic character tables', in *Computational Methods in Lie theory (Essen, 1994)* (Appl. Algebra Engrg. Comm. Comput.) vol. 7 (1996), 175–210.

[44] S. Guest, J. Morris, C. E. Praeger and P. Spiga, 'On the maximum orders of elements of finite almost simple groups and primitive permutation groups', *Trans. Amer. Math. Soc.* **367** (2015), 7665–7694.

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

[46] R. M. Guralnick, M. Larsen and P. H. Tiep, 'Character levels and character bounds', *Forum Math. Pi* **8** (2020), e2, 81 pp.

[47] R. M. Guralnick and G. Malle, 'Products of conjugacy classes and fixed point spaces', *J. Amer. Math. Soc.* **25** (2012), 77–121.

[48] R. M. Guralnick and G. Malle, 'Simple groups admit Beauville structures', *J. Lond. Math. Soc.* **85** (2012), 694–721.

[49] R. M. Guralnick, T. Penttila, C. E. Praeger and J. Saxl, 'Linear groups with orders having certain large prime divisors', *Proc. London Math. Soc.* **78** (1999), 167–214.

[50] R. M. Guralnick and P. H. Tiep, 'Finite simple unisingular groups of Lie type', *J. Group Theory* **6** (2003), 271–310.

[51] 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.

[52] S. Harper, 'The spread of finite and infinite groups', in *Groups St Andrews 2022 in Newcastle* (London Math. Soc. Lecture Note Ser.) vol. 496 (Cambridge Univ. Press, Cambridge, 2025), 74–117.

[53] B. Hartley and M. Kuzucuoğlu, 'Centralizers of elements in locally finite simple groups', *Proc. Lond. Math. Soc.* **62** (1991), 301–324.

[54] G. James and M. W. Liebeck, *Representations and Characters of Groups* (Cambridge University Press, New York, 2001).

[55] G. A. Jones, 'Primitive permutation groups containing a cycle', *Bull. Aust. Math. Soc.* **89** (2014) 159–165.

[56] C. Jordan, 'Recherches sur les substitutions', *J. Math. Pures Appl. (Liouville)* **17** (1872), 351–367.

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

[58] M. Larsen, A. Shalev and P. H. Tiep, 'Products of derangements in simple permutation groups', *Forum Math. Sigma* **10** (2022), Paper No. e83, 30 pp.

[59] M. Larsen and P. H. Tiep, 'Squares of conjugacy classes in alternating groups', *Proc. Amer. Math. Soc.*, to appear.

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

[61] A. Lev, 'Covering the group $\mathrm{PSL}_n(F)$ by the square of a conjugacy class', *Comm. Algebra* **27** (1999), 1207–1253.

[62] C. H. Li and H. Zhang, 'The finite primitive groups with soluble stabilizers, and the edge-primitive s-arc transitive graphs', *Proc. Lond. Math. Soc.* **103** (2011), 441–472.

[63] M. W. Liebeck, 'Width questions for finite simple groups', in *Groups St Andrews 2013* (London Math. Soc. Lecture Note Ser.) vol. 422 (Cambridge Univ. Press, Cambridge, 2015), 51–72.

[64] M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep, 'The Ore conjecture', *J. Eur. Math. Soc. (JEMS)* **12** (2010), 939–1008.

[65] M. W. Liebeck, C. E. Praeger and J. Saxl, 'On the O'Nan-Scott theorem for finite primitive permutation groups', *J. Austral. Math. Soc. Ser. A* **44** (1988), 389–396.

[66] M. W. Liebeck and J. Saxl, 'Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces', *Proc. London Math. Soc.* **63** (1991), 266–314.

[67] M. W. Liebeck, J. Saxl and G. M. Seitz, 'Subgroups of maximal rank in finite exceptional groups of Lie type', *Proc. London Math. Soc.* **65** (1992), 297–325.

[68] M. W. Liebeck and G. M. Seitz, *Unipotent and Nilpotent Classes in Simple Algebraic Groups and Lie Algebras* (Mathematical Surveys and Monographs) vol. 180 (Amer. Math. Soc., Providence, RI, 2012).

[69] F. Lübeck, 'Centralisers and numbers of semisimple classes in finite groups of Lie type', http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/CentSSClasses

[70] T. Łuczak and L. Pyber, 'On random generation of the symmetric group', *Combin. Probab. Comput.* **2** (1993), 505–512.

[71] G. Malle, J. Saxl and T. Weigel, 'Generation of classical groups', *Geom. Dedicata* **49** (1994), 85–116.

[72] J.-P. Massias, J.-L. Nicolas and G. Robin, 'Effective bounds for the maximal order of an element in the symmetric group', *Math. Comp.* **53** (1989), 665–678.

[73] M. Newman, 'Similarity over $SL(n, F)$', *Linear and Multilinear Algebra* **12** (1982/83), 223–226.

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

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

[76] K. Shinoda, 'The conjugacy classes of the finite Ree groups of type (F_4)', *J. Fac. Sci. Univ. Tokyo* **22** (1975), 1–15.

[77] W. A. Simpson and J. S. Frame, 'The character tables for $SL(3, q)$, $SU(3, q^2)$, $PSL(3, q)$, $PSU(3, q^2)$', *Canadian J. Math.* **25** (1973), 486–494.

[78] R. Steinberg, 'Generators for simple groups', *Canadian J. Math.* **14** (1962), 277–283.

[79] M. Suzuki, 'On a class of doubly transitive groups', *Ann. of Math.* **75** (1962), 105–145.

[80] P. H. Tiep and A. E. Zalesski, 'Real conjugacy classes in algebraic groups and finite groups of Lie type', *J. Group Theory* **8** (2005), 291–315.

[81] T. Weigel, 'Generation of exceptional groups of Lie type', *Geom. Dedicata* **41** (1992), 63–87.

[82] H. Wielandt, *Finite Permutation Groups* (Academic Press, New York-London, 1964).

[83] R. A. Wilson, 'Maximal subgroups of $^2E_6(2)$ and its automorphism groups', Preprint, 2018, arXiv:1801.08374.

[84] R. A. Wilson et al., *A World-Wide-Web Atlas of Finite Group Representations*, http://brauer.maths.qmul.ac.uk/Atlas/v3/

[85] K. Zsigmondy, 'Zur Theorie der Potenzreste', *Monatsh. Math. Phys.* **3** (1892), 265–284.