
Publisher's PDF, also known as Version of record

License (if available):
CC BY

Link to published version (if available):
10.1007/s00229-015-0795-x

Link to publication record in Explore Bristol Research
PDF-document

This is the final published version of the article (version of record). It first appeared online via Springer at http://link.springer.com/article/10.1007%2Fs00229-015-0795-x. Please refer to any applicable terms of use of the publisher.

University of Bristol - Explore Bristol Research

General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available: http://www.bristol.ac.uk/red/research-policy/pure/user-guides/ebr-terms/
Primitive permutation groups and derangements of prime power order

Received: 19 May 2015 / Accepted 16 October 2015

Abstract. Let $G$ be a transitive permutation group on a finite set of size at least 2. By a well known theorem of Fein, Kantor and Schacher, $G$ contains a derangement of prime power order. In this paper, we study the finite primitive permutation groups with the extremal property that the order of every derangement is an $r$-power, for some fixed prime $r$. First we show that these groups are either almost simple or affine, and we determine all the almost simple groups with this property. We also prove that an affine group $G$ has this property if and only if every two-point stabilizer is an $r$-group. Here the structure of $G$ has been extensively studied in work of Guralnick and Wiegand on the multiplicative structure of Galois field extensions, and in later work of Fleischmann, Lempken and Tiep on $r'$-semiregular pairs.

1. Introduction

Let $G$ be a transitive permutation group on a finite set $\Omega$ of size at least 2. An element $x \in G$ is a derangement if it acts fixed-point-freely on $\Omega$. An easy application of the orbit-counting lemma shows that $G$ contains derangements (this is originally a classical theorem of Jordan [36]), and we will write $\Delta(G)$ for the set of derangements in $G$. Note that if $H$ is a point stabilizer, then $x$ is a derangement if and only if $x^G \cap H$ is empty, where $x^G$ denotes the conjugacy class of $x$ in $G$, so we have

$$\Delta(G) = G \setminus \bigcup_{g \in G} H^g. \quad (1)$$

The existence of derangements in transitive permutation groups has interesting applications in number theory and topology (see Serre’s article [48], for example).

Various extensions of Jordan’s theorem on the existence of derangements have been studied in recent years. For example, if $\delta(G) = |\Delta(G)|/|G|$ denotes the proportion of derangements in $G$, then a theorem of Cameron and Cohen [13] states that $\delta(G) \geq |\Omega|^{-1}$, with equality if and only if $G$ is sharply 2-transitive. More recently, Fulman and Guralnick have established the existence of an absolute
constant $\epsilon > 0$ such that $\delta(G) > \epsilon$ for any simple transitive group $G$ (see [21–24]). This latter result confirms a conjecture of Boston et al. [4] and Shalev.

The study of derangements with special properties has been another major theme in recent years. By a theorem of Fein et al. [18], $\Delta(G)$ contains an element of prime power order (their proof requires the classification of finite simple groups), and this result has important number-theoretic applications. For instance, it implies that the relative Brauer group of any finite extension of global fields is infinite. In most cases, $\Delta(G)$ contains an element of prime order, but there are some exceptions, such as the 3-transitive action of the smallest Mathieu group $M_{11}$ on 12 points. The transitive permutation groups with this property are called elusive groups, and they have been investigated by many authors; see [14,26,27], for example.

In this paper, we are interested in the permutation groups with the special property that every derangement is an $r$-element (that is, has order a power of $r$) for some fixed prime $r$. One of our main motivations stems from a theorem of Isaacs et al. [35], which describes the finite transitive groups in which every derangement is an involution; by [35, Theorem A], such a group is either an elementary abelian 2-group, or a Frobenius group with kernel an elementary abelian 2-group. In [9], this result is used to classify the finite groups whose irreducible characters vanish only on involutions. It is natural to consider the analogous problem for odd primes, and more generally for prime powers. As noted in [35], it is easy to see that such a generalization will involve a wider range of examples. For instance, if $p$ is an odd prime then every derangement in the affine group $\text{ASL}_2(p) = \text{SL}_2(p); p^2$ (of degree $p^2$) has order $p$ (if $p = 2$, the derangements have order 2 or 4).

Our first result is a reduction theorem.

**Theorem 1.** Let $G$ be a finite primitive permutation group such that every derangement in $G$ is an $r$-element for some fixed prime $r$. Then $G$ is either almost simple or affine.

Our next result, Theorem 2 below, describes all the almost simple primitive groups that arise in Theorem 1. Notice that in Table 1, we write $P_1$ for a maximal parabolic subgroup of $L_2(q)$ or $L_3(q)$, which can be defined as the stabilizer of a 1-dimensional subspace of the natural module (similarly, $P_2$ is the stabilizer of a 2-dimensional subspace). In addition, we define

$$\mathcal{E}(G) = \{ |x| : x \in \Delta(G) \}.$$

**Theorem 2.** Let $G$ be a finite almost simple primitive permutation group with point stabilizer $H$. Then every derangement in $G$ is an $r$-element for some fixed prime $r$ if and only if $(G, H, r)$ is one of the cases in Table 1. In particular, every derangement has order $r$ if and only if $|\mathcal{E}(G)| = 1$.

**Remark 3.** Let us make a couple of comments on the cases arising in Table 1.

(i) Firstly, notice that the group $G$ is recorded up to isomorphism. For example, the case $(G, H) = (A_6, (S_3 \wr S_2) \cap A_6)$ is listed as $(L_2(9), P_1)$, $(G, H) = (A_5, A_4)$ appears as $(L_2(4), P_1)$, and we record $(G, H) = (L_2(7), S_4)$ as $(L_3(2), P_1)$, etc.
Table 1. The cases \((G, H, r)\) in Theorem 2

<table>
<thead>
<tr>
<th>(G)</th>
<th>(H)</th>
<th>(r)</th>
<th>(E(G))</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>(L_3(q))</td>
<td>(P_1, P_2)</td>
<td>(r)</td>
<td>(r)</td>
<td>(q^2 + q + 1 = (3, q - 1)r)</td>
</tr>
<tr>
<td>(M_11)</td>
<td>(L_2(11))</td>
<td>2</td>
<td>4</td>
<td>(q^2 + q + 1 = 3r^2)</td>
</tr>
<tr>
<td>( \Gamma L_2(q) )</td>
<td>(N_G(D_2(q+1)))</td>
<td>(r)</td>
<td>(r, r^2)</td>
<td>(r = q - 1) Mersenne prime</td>
</tr>
<tr>
<td>( \Gamma L_2(8) )</td>
<td>(N_G(P_1), N_G(D_{14}))</td>
<td>3</td>
<td>3, 9</td>
<td></td>
</tr>
<tr>
<td>(PGL_2(q))</td>
<td>(N_G(P_1))</td>
<td>2</td>
<td>(2^i, 1 \leq i \leq 1 + 1)</td>
<td>(q = 2^{e+1} - 1) Mersenne prime</td>
</tr>
<tr>
<td>(L_2(q))</td>
<td>(P_1)</td>
<td>(r)</td>
<td>(r^i, 1 \leq i \leq e)</td>
<td>(q = 2^{r^e - 1})</td>
</tr>
<tr>
<td></td>
<td>(P_1, D_{2(q-1)})</td>
<td>(r)</td>
<td>(r)</td>
<td>(r = q + 1) Fermat prime</td>
</tr>
<tr>
<td></td>
<td>(D_{2(q+1)})</td>
<td>(r)</td>
<td>(r)</td>
<td>(r = q - 1) Mersenne prime</td>
</tr>
</tbody>
</table>

(ii) In the first two rows of the table we have \(G = L_3(q)\) and \(H = P_1\) or \(P_2\). Here \(q^2 + q + 1 \in \{r, 3r, 3r^2\}\), which implies that either \(q = 4\), or \(q = p^f\) for a prime \(p\) and \(f\) is a 3-power (see Lemma 2.9).

Now let us turn our attention to the affine groups that arise in Theorem 1. In order to state Theorem 4 below, we need to introduce some additional terminology. Let \(F\) be a field and let \(V\) be a finite dimensional vector space over \(F\). Let \(H \leq \text{GL}(V)\) be a finite group and let \(r\) be a prime. Recall that \(x \in H\) is an \(r\)'-element if the order of \(x\) is indivisible by \(r\). Following Fleischmann et al. [19], the pair \((H, V)\) is said to be \(r\)'-semiregular if every nontrivial \(r\)'-element of \(H\) has no fixed points on \(V \setminus \{0\}\) (equivalently, no nontrivial \(r\)'-element of \(H\) has eigenvalue 1 on \(V\)).

**Theorem 4.** Let \(G = HV \leq AGL(V)\) be a finite affine primitive permutation group with point stabilizer \(H = G_0\) and socle \(V = (\mathbb{Z}_p)^k\), where \(p\) is a prime and \(k \geq 1\). Then every derangement in \(G\) is an \(r\)-element for some fixed prime \(r\) if and only if \(r = p\) and the pair \((H, V)\) is \(r\)'-semiregular.

Let \(G = HV\) be an affine group as in Theorem 4 and notice that \((H, V)\) is \(r\)'-semiregular if and only if every two-point stabilizer in \(G\) is an \(r\)-group. As a special case, observe that if \(G\) is a Frobenius group then every two-point stabilizer is trivial and it is clear that every derangement in \(G\) has order \(r\). Therefore, it is natural to focus our attention on the non-Frobenius affine groups arising in Theorem 4, which correspond to \(r\)'-semiregular pairs \((H, V)\) such that \(r\) divides \(|H|\). In this situation, Guralnick and Wiegand [33, Section 4] obtain detailed information on the structure of \(H\), which they use to investigate the multiplicative structure of finite Galois field extensions. Similar results were established in later work of Fleischmann et al. [19]. We refer the reader to the end of Sect. 5 for further details (see Propositions 5.4 and 5.5).

Transitive groups with the property in Theorem 1 arise naturally in several different contexts. For instance, let us recall that the existence of a derangement of prime power order in any finite transitive permutation group implies that the relative Brauer group \(B(L/K)\) of any finite extension \(L/K\) of global fields is infinite. More precisely, let \(L = K(\alpha)\) be a separable extension of \(K\), let \(E\) be a Galois closure of
Let $L$ over $K$, and let $\Omega$ be the set of roots in $E$ of the minimal polynomial of $\alpha$ over $K$. Then the $r$-primary component $B(L/K)_r$ is infinite if and only if the Galois group $\text{Gal}(E/K)$ contains a derangement of $r$-power order on $\Omega$ (see [18, Corollary 3]). In this situation, it follows that the relative Brauer group $B(L/K)_r$ has a unique infinite primary component if and only if every derangement in $\text{Gal}(E/K)$ is an $r$-element for some fixed prime $r$.

In a different direction, our property arises in the study of permutation groups with *bounded movement*.

**Remark 5.** Let $G = HV \leq AGL(V)$ be a finite affine primitive permutation group as above, and assume that every derangement in $G$ is an $r$-element for some fixed prime $r$. Let $P$ be a Sylow $r$-subgroup of $G$ and set $K = H \cap P$. As explained in Proposition 5.6, $P$ is a transitive permutation group on $P/K$ with $E(G) = E(P)$, so $E(G) = \{r\}$ if and only if $E(P) = \{r\}$, and we will show that $E(P) = \{r\}$ if and only if $P$ has exponent $r$ (see Theorem 5.7).

There is also a connection between our property and 2-coverings of abstract groups. First notice that Jordan’s theorem on the existence of derangements is equivalent to the well known fact that no finite group $G$ can be expressed as the union of $G$-conjugates of a proper subgroup (see (1)). However, it may be possible to express $G$ as the union of the $G$-conjugates of two proper subgroups; if $H$ and $K$ are proper subgroups such that

$$G = \bigcup_{g \in G} H^g \cup \bigcup_{g \in G} K^g,$$

then $G$ is said to be 2-coverable and the pair $(H, K)$ is a 2-covering for $G$. This notion has been widely studied in the context of finite simple groups. For instance, Bubboloni [8] proves that $A_n$ is 2-coverable if and only if $5 \leq n \leq 8$, and similarly $L_n(q)$ is 2-coverable if and only if $2 \leq n \leq 4$ (see [10]). We refer the reader to [11] and [46] for further results in this direction. The connection between 2-coverable groups and the property in Theorem 1 is transparent. Indeed, if $G$ is a transitive
Derangements of prime power order

permutation group with point stabilizer $H$, then every derangement in $G$ is an $r$-element (for some fixed prime $r$) if and only if $(H,K)$ is a 2-covering for $G$, where $K$ is a Sylow $r$-subgroup of $G$.

Finally, some words on the organisation of this paper. In Sect. 2 we record several preliminary results that we will need in the proofs of our main theorems. The proof of Theorem 1 is given in Sect. 3, and the almost simple groups are handled in Sect. 4, where we prove Theorem 2. Finally, in Sect. 5 we turn to affine groups and we establish Theorem 4.

Notation Our group-theoretic notation is standard, and we adopt the notation of Kleidman and Liebeck [38] for simple groups. For instance,

$$PSL_n(q) = L^+_n(q) = L_n(q), \quad PSU_n(q) = L^-_n(q) = U_n(q).$$

If $G$ is a simple orthogonal group, then we write $G = P\Omega_\epsilon^n(q)$, where $\epsilon = +$ (respectively $-$) if $n$ is even and $G$ has Witt defect 0 (respectively 1), and $\epsilon = o$ if $n$ is odd (in the latter case, we also write $G = \Omega_n(q)$). Following [38], we will sometimes refer to the type of a subgroup $H$, which provides an approximate description of the group-theoretic structure of $H$.

For integers $a$ and $b$, we use $(a,b)$ to denote the greatest common divisor of $a$ and $b$. If $p$ is a prime number, then we write $a = a_p \cdot a_p'$, where $a_p$ is the largest power of $p$ dividing $a$. Finally, if $X$ is a finite set, then $\pi(X)$ denotes the set of prime divisors of $|X|$.

2. Preliminaries

In this section we record several preliminary results that will be useful in the proofs of our main theorems. Let $H$ be a proper subgroup of a finite group $G$ and set

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

Notice that if $G$ is a transitive permutation group with point stabilizer $H$, then $\Delta(G) = \Delta_H(G)$ is the set of derangements in $G$ (see (1)).

It will be convenient to define the following property:

Every element in $\Delta_H(G)$ is an $r$-element for some fixed prime $r$. \hfill (⋆)

Lemma 2.1. Let $H$ be a proper subgroup of a finite group $G$. If (⋆) holds, then

(i) $\pi(G) = \pi(H) \cup \{r\}$; and

(ii) $C_G(x)$ is an $r$-group for every $x \in \Delta_H(G)$.

Proof. If $s \in \pi(G) \setminus \pi(H)$, then $\Delta_H(G)$ contains an $s$-element, so (i) follows. Now consider (ii). Let $x \in \Delta_H(G)$ and assume $s \neq r$ is a prime divisor of $|C_G(x)|$. Let $y \in C_G(x)$ with $|y| = s$ and let $z = xy = yx$, so $z^s = x^s$ and $\langle x \rangle \leq \langle z \rangle$. Then $z \in \Delta_H(G)$, but this is incompatible with property (⋆). \hfill □
Lemma 2.2. Let $H$ be a proper subgroup of a finite group $G$, let $N$ be a normal subgroup of $G$ such that $G = NH$, and let $K$ be a proper subgroup of $N$ containing $H \cap N$. Then $\Delta_K(N) \subseteq \Delta_H(G)$.

Proof. Let $x \in \Delta_K(N)$ and assume that $x \notin \Delta_H(G)$. Then $x^g \in H$ for some $g \in G$. Since $g \in G = NH$, we may write $g = nh$ for some $n \in N$ and $h \in H$. Then $x^g = (x^n)^h \in H$ which implies that $x^n \in H h^{-1} = H$. Since both $x$ and $n$ are in $N$, we deduce that $x^n \in H \cap N \subseteq K$, contradicting the fact that $x \in \Delta_K(N)$. \hfill \Box

Remark 2.3. Recall that the prime graph (or Gruenberg–Kegel graph) of a finite group $G$ is the graph $\Gamma(G)$ with vertex set $\pi(G)$ and the property that two distinct vertices $p$ and $q$ are adjacent if and only if $G$ contains an element of order $pq$. Now, a transitive permutation group $G$ with point stabilizer $H$ has property $(\ast)$ only if one of the following holds:

(a) $r$ is an isolated vertex in $\Gamma(G)$;
(b) $\pi(G) = \pi(H)$.

The finite simple groups with a disconnected prime graph are recorded in [39, Tables 1–3], and a similar analysis for almost simple groups is given in [41,42]. In particular, one could use these results to study the almost simple permutation groups for which (a) holds. Similarly, if $G$ is almost simple and (b) holds, then the possibilities for $G$ and $H$ can be read off from [40, Corollary 5]. However, this is not the approach that we will pursue in this paper.

The next result is a special case of [31, Lemma 3.3].

Lemma 2.4. Let $G$ be a finite permutation group and let $N$ be a transitive normal subgroup of $G$ such that $G/N = \langle Ng \rangle$ is cyclic. Then $Ng \cap \Delta(G)$ is empty if and only if every element of $Ng$ has a unique fixed point.

We will also need several number-theoretic lemmas. Given a positive integer $n$ we write $n_2$ for the largest power of 2 dividing $n$. In addition, recall that $(a,b)$ denotes the greatest common divisor of the positive integers $a$ and $b$. The following result is well known.

Lemma 2.5. Let $q \geq 2$ be an integer. For all integers $n, m \geq 1$ we have

\[
(q^n - 1, q^m - 1) = q^{(n,m)} - 1
\]

\[
(q^n - 1, q^m + 1) = \begin{cases} 
q^{(n,m)} + 1 & \text{if } 2m_2 \leq n_2 \\
(2, q - 1) & \text{otherwise}
\end{cases}
\]

\[
(q^n + 1, q^m + 1) = \begin{cases} 
q^{(n,m)} + 1 & \text{if } m_2 = n_2 \\
(2, q - 1) & \text{otherwise}
\end{cases}
\]

Let $q = p^f$ be a prime power, let $e \geq 2$ be an integer and let $r$ be a prime dividing $q^e - 1$. We say that $r$ is a primitive prime divisor (ppd for short) of $q^e - 1$ if $r$ does not divide $q^i - 1$ for all $1 \leq i < e$. A classical theorem of Zsigmondy [53] states that if $e \geq 3$ then $q^e - 1$ has a primitive prime divisor unless $(q, e) = (2, 6)$. 

Primitive prime divisors also exist when \( e = 2 \), provided \( q \) is not a Mersenne prime. Note that if \( r \) is a ppd of \( q^e - 1 \) then \( r \equiv 1 \pmod{e} \). Also note that if \( n \) is a positive integer, then \( r \) divides \( q^n - 1 \) if and only if \( e \) divides \( n \). If a ppd of \( q^e - 1 \) exists, then we will write \( \ell_e(q) \) to denote the largest ppd of \( q^e - 1 \). Note that \( \ell_e(q) > e \).

**Lemma 2.6.** Let \( r, s \) be primes, and let \( m, n \) be positive integers. If \( r^m + 1 = s^n \), then one of the following holds:

(i) \((r, s, m, n) = (2, 3, 3, 2)\);
(ii) \((r, n) = (2, 1), m \) is a 2-power and \( s = 2^m + 1 \) is a Fermat prime;
(iii) \((s, m) = (2, 1), n \) is a prime and \( r = 2^n - 1 \) is a Mersenne prime.

**Proof.** This is a straightforward application of Zsigmondy’s theorem [53]. For completeness, we will give the details.

First assume that \( m = 1 \), so \( r = s^n - 1 \) is a prime. If \( s \) is odd, then \( r \) is even, so \( r = 2 \) and \( s^n = 3 \), which implies that \( n = 1 \) and \( s = 3 \). This case appears in (i). Now assume \( s = 2 \), so \( r = 2^n - 1 \) is prime. It follows that \( n \) must also be a prime and thus \( r \) is a Mersenne prime. This is (iii).

For the remainder, we may assume that \( m \geq 2 \). Notice that \( r^{2m} - 1 = s^n(r^m - 1) \). If \((m, r) = (3, 2)\), then \( s^n = 2^3 + 1 = 3^2 \) and thus \((s, n) = (3, 2)\) as in (i). Now assume that \((m, r) \neq (3, 2)\). By Zsigmondy’s theorem [53], the ppd \( \ell_{2m}(r) \) exists and divides \( r^{2m} - 1 = s^n(r^m - 1) \), but not \( r^m - 1 \), hence \( s = \ell_{2m}(r) > 2m \geq 4 \).

Therefore \( s \geq 5 \) is an odd prime and \( r^m = s^n - 1 \) is even, so \( r = 2 \). We now consider three cases.

If \( n = 1 \), then \( s = r^m + 1 = 2^m + 1 \) is an odd prime, which implies that \( m \) is a 2-power as in case (ii). Next assume that \( n = 2 \). Here \( 2^m = s^2 - 1 = (s - 1)(s + 1) \) and thus \( s - 1 = 2^a \) and \( s + 1 = 2^b \) for some positive integers \( a \) and \( b \). Then \( 2^b - 2^a = (s + 1) - (s - 1) = 2 \) and thus \( 2^b - 2^a = 2^{a - 1} + 1 \), which implies that \( (a, b) = (1, 2) \), so \( s = 3 \) and thus \( m = 3 \). Therefore, \((r, s, m, n) = (2, 3, 3, 2)\) as in case (i). Finally, let us assume that \( n \geq 3 \). Now \( 2^m = s^n - 1 \) and Zsigmondy’s theorem implies that the ppd \( \ell_n(s) > n \geq 3 \) exists and divides \( 2^m \), which is absurd. \[\Box\]

**Lemma 2.7.** Let \( q \) be a prime power and let \((a, \epsilon), (b, \delta) \in \mathbb{N} \times \{\pm 1\}, \) where \( b > a \geq 2 \) and \((a, \epsilon) \neq (2, -1)\). Let \( N = (q^a + \epsilon)(q^b + \delta) \). Then one of the following holds:

(i) \( N \) has two distinct prime divisors that do not divide \( q^2 - 1 \);
(ii) \((a, \epsilon) = (2, 1), (b, \delta) = (4, -1) \) and \( q^2 + 1 = (2, q - 1)r^e \) for some prime \( r \) and positive integer \( e \);
(iii) \( q = 3, (a, \epsilon) = (2, 1) \) and \((b, \delta) = (3, 1)\);
(iv) \( q = 2, (a, \epsilon) = (3, 1) \) and \( 2^b + \delta \) is divisible by at most two distinct primes, one of which is 3;
(v) \( q = 2, a = 3 \) and \((b, \delta) = (6, -1)\).

**Proof.** There are four cases to consider, according to the possibilities for the pair \((\epsilon, \delta)\).

First assume that \((\epsilon, \delta) = (1, 1)\). Suppose that neither \((a, q)\) nor \((b, q)\) is equal to \((3, 2)\). Then the primitive prime divisors \( \ell_{2a}(q) \) and \( \ell_{2b}(q) \) exist, and they both
and positive integer \( a \geq q \).

\[
\text{Lemma 2.8. Let } q \text{ be a prime power and let } N \text{ be one of the integers in Table 2, and divide } N. \text{ Moreover, these primes are distinct since } 2a < 2b, \text{ and neither of them divides } q^2 - 1 \text{ since } 2b > 2a \geq 4. \text{ If } (a, q) = (3, 2) \text{ then } b \geq 4, N = 3^2(2^b + 1) \text{ and either (i) or (iv) holds. If } (b, q) = (3, 2), \text{ then } a = 2, N = 3^2 \cdot 5 \text{ and (iii) holds.}

Next suppose that \((\epsilon, \delta) = (-1, -1), \text{ so } a \geq 3. \text{ If neither } (a, q) \text{ nor } (b, q) \text{ is equal to } (6, 2), \text{ then } N \text{ is divisible by the distinct primes } \ell_a(q) \text{ and } \ell_b(q), \text{ neither of which divide } q^2 - 1. \text{ If } (a, q) = (6, 2), \text{ then } N = 3^2 \cdot 7(2^b - 1) \text{ is divisible by 7 and } \ell_b(2) > b \geq 7. \text{ Finally, suppose that } (b, q) = (6, 2), \text{ so } N = 3^2 \cdot 7(2^a - 1) \text{ and } 3 \leq a \leq 5. \text{ It is easy to check that (i) holds if } a = 4 \text{ or 5, and that (v) holds if } a = 3.

Now assume that \((\epsilon, \delta) = (1, -1). \text{ If } (a, q) = (3, 2) \text{ then (i) or (iv) holds, so we may assume that } (a, q) \neq (3, 2). \text{ If } (b, q) = (6, 2) \text{ then } N = 3^2 \cdot 7(2^a + 1), a \in \{2, 4, 5\} \text{ and (i) holds. In each of the remaining cases, the primitive prime divisors } \ell_{2a}(q) \text{ and } \ell_b(q) \text{ exist, and they divide } N, \text{ but not } q^2 - 1. \text{ Clearly, if } b \neq 2a \text{ then these two primes are distinct and (i) holds, so let us assume that } b = 2a, \text{ so } N = (q^a + 1)^2(q^a - 1). \text{ If } (a, q) = (6, 2) \text{ then (i) holds. If } (a, q) \neq (6, 2) \text{ and } a \geq 3 \text{ then we can take the primitive prime divisors } \ell_a(q) \text{ and } \ell_{2a}(q), \text{ so once again (i) holds. Finally, if } a = 2 \text{ and } b = 4 \text{ then } N = (q^2 - 1)(q^2 + 1)^2 \text{ and either (i) or (ii) holds.}

Finally, let us assume that \((\epsilon, \delta) = (-1, 1). \text{ Here we may assume that } a \geq 3. \text{ If } (a, q) \neq (6, 2) \text{ then take } \ell_a(q) \text{ and } \ell_{2b}(q), \text{ otherwise } N = 3^2 \cdot 7(2^b + 1) \text{ is divisible by 7 and } \ell_{2b}(2). \text{ In both cases, (i) holds.} \quad \square

\textbf{Lemma 2.8. Let } q \text{ be a prime power and let } N \text{ be one of the integers in Table 2, where } \epsilon = \pm 1. \text{ Then } N \text{ is a prime power if and only if } (\epsilon, q) \text{ is one of the cases recorded in the second column of the table.}

\textbf{Proof.} This is entirely straightforward. For example, suppose that \( N = (q^5 - 1)/(6, q - 1). \text{ Let } d = (6, q - 1) \text{ and suppose that } N = r^e \text{ for some prime number } r \text{ and positive integer } e. \text{ Then } r = \ell_S(q) \text{ and }

\[(q - 1)(q^4 + q^3 + q^2 + q + 1) = dr^e.
\]

Since }r\text{ does not divide } q - 1, \text{ we must have } q - 1 = d \text{ and thus } q - 1 \in \{1, 2, 3, 6\}. \text{ If } q = 4 \text{ then } N = 341 = 11 \cdot 31 \text{ is not a prime power, but one checks that } N \text{ is a prime power if } q \in \{2, 3, 7\}. \text{ The other cases are very similar.} \quad \square

We will also need the following result, which follows from a theorem of Nagell [44].
Lemma 2.9. Let $q = p^f$ be a prime power and let $r$ be a prime.

(i) If $e$ is a positive integer such that $q^2 + q + 1 = r^e$, then $q \not\equiv 1 \pmod{3}$ and $e = 1$.
(ii) If $e$ is a positive integer such that $q^2 + q + 1 = 3r^e$, then $q \equiv 1 \pmod{3}$ and $e \in \{1, 2\}$.
(iii) If $q^2 + q + 1 = (3, q-1)r^e$ for some positive integer $e$, then either $(q, r, e) = (4, 7, 1)$, or $f = 3^a$ for some integer $a \geq 0$.

Proof. Parts (i) and (ii) follow from [44]. For (iii), let $d = (3, q-1)$ and write $f = 3^a m$ with $(3, m) = 1$ and $a \geq 0$. We may assume that $q \neq 4$. Seeking a contradiction, suppose that $m > 1$. Notice that $r^e = \frac{p^{3a+1}m - 1}{d(p^{3m}m - 1)}$.

Since $q \neq 4$, the ppd $\ell_{3f}(p)$ exists and divides $q^2 + q + 1$, so $r = \ell_{3f}(p)$.

Let $s = \ell_{3a+1}(p)$. Since $f = 3^a m$ is indivisible by $3^{a+1}$, it follows that $(s, q-1) = 1$, so $s$ does not divide $d(q-1)$ and thus $s$ divides $r^e$, so $r = s$. But $m > 1$, so $3^f > 3^{a+1}$ and thus $r \neq s$. This is a contradiction and the result follows.

Remark 2.10. By a theorem of van der Waall [50], the Diophantine equation $x^2 + x + 1 = 3y^2$ has infinitely many integer solutions; the smallest nontrivial solution is $(x, y) = (313, 181)$. Here $x$ and $y$ are both primes, and another solution in the primes is $(x, y) = (2288805793, 1321442641)$.

3. A reduction theorem

The following theorem reduces the study of primitive permutation groups with property $(\ast)$ to almost simple and affine groups.

Theorem 3.1. Let $G \leq \text{Sym}(\Omega)$ be a primitive permutation group with point stabilizer $H$. If $(\ast)$ holds, then either

(i) $G$ is almost simple; or
(ii) $G = HN$ is an affine group with socle $N \cong (\mathbb{Z}_r)^k$ for some integer $k \geq 1$.

Moreover, if (ii) holds and $|H|$ is indivisible by $r$, then $G$ is a Frobenius group with kernel $N$ and complement $H$.

Proof. Let $N$ be a minimal normal subgroup of $G$, so $N \cong S_1 \times S_2 \times \cdots \times S_k$, where $S_i \cong S$ for some simple group $S$ and integer $k \geq 1$. Then $G = HN$ and $N$ is transitive on $\Omega$. Let us assume that $(\ast)$ holds.

First assume that $H \cap N = 1$, so $N$ is regular and every nontrivial element in $N$ is a derangement. If $N$ is abelian, then we are in case (ii). Moreover, if $|H|$ is indivisible by $r$, then $N$ is a Sylow $r$-subgroup of $G$ and thus $\Delta(G) \subseteq N$. In this situation, [12, Lemma 4.1] implies that $G$ is a Frobenius group with kernel $N$ and complement $H$. Now, if $N$ is nonabelian then $S$ is a nonabelian simple group and
thus \( |S| \) is divisible by at least three distinct primes, whence \( S \) (and thus \( N \)) contains derangements of distinct prime orders, which is incompatible with property \((\ast)\).

For the remainder, we may assume that \( H \cap N \) is nontrivial. It follows that \( N \cong S^k \), where \( S \) is a nonabelian simple group and \( k \geq 1 \). If \( k = 1 \), then \( G \) is almost simple and \((i)\) holds. Therefore, we may assume that \( k \geq 2 \).

Let \( T \leq N \) be a maximal subgroup of \( N \) containing \( H \cap N \). By Lemma 2.2, we have \( \Delta_T(N) \subseteq \Delta_H(G) \). Since \( k \geq 2 \), there exist integers \( i \) and \( j \) such that \( 1 \leq i < j \leq k \) and \( L := S_i \times S_j \not\subseteq T \). By relabelling the \( S_\ell \), if necessary, we may assume that \( L = S_1 \times S_2 \). Now \( L \leq N \), so \( N = TL \) and thus

\[
\Delta_K(L) \subseteq \Delta_T(N) \subseteq \Delta_H(G) = \Delta(G),
\]

where \( K \) is a maximal subgroup of \( L \) containing \( L \cap T \). Therefore, every derangement of \( L = S_1 \times S_2 \) on the right cosets \( L/K \) is an \( r \)-element.

By [49, Lemma 1.3], there are essentially two possibilities for \( K \); either \( K \) is a diagonal subgroup of the form \( \{(s, \phi(s)) : s \in S_1\} \) for some isomorphism \( \phi : S_1 \to S_2 \), or \( K \) is a standard maximal subgroup, i.e., \( K = S_1 \times K_2 \) or \( K_1 \times S_2 \), where \( K_1 < S_1 \) is maximal. In the diagonal case, every element in \( L \) of the form \( (s, 1) \) with \( 1 \neq s \in S_1 \) is a derangement on \( L/K \). Clearly, this situation cannot arise. Now assume \( K \) is a standard maximal subgroup. Without loss of generality, we may assume that \( K = K_1 \times S_2 \), where \( K_1 \) is maximal in \( S_1 \). Let \( s \in S_1 \) be a derangement on \( S_1/K_1 \) of prime power order, say \( p^e \) for some prime \( p \) and integer \( e \geq 1 \) (such an element exists by the main theorem of [18]). Since \( |\pi(S)| \geq 3 \), choose \( t \in S_2 \) of prime order different from \( p \). Then \( (s, t) \in L \) is a derangement on \( L/K \) of non-prime power order, so once again we have reached a contradiction.

This completes the proof of Theorem 1.

4. Almost simple groups

In this section we prove Theorem 2. We fix the following notation. Let \( r \) be a prime and let \( G \leq \text{Sym}(\Omega) \) be an almost simple primitive permutation group with socle \( G_0 \) and point stabilizer \( H \). Set \( H_0 = H \cap G_0 \) and let \( M \) be a maximal subgroup of \( G_0 \) containing \( H_0 \). As before, let \( \Delta(G) \) be the set of derangements in \( G \), and let \( E(G) \) be the set of orders of elements in \( \Delta(G) \). By Lemma 2.2, we have

\[
\Delta_M(G_0) \subseteq \Delta_{H_0}(G_0) \subseteq \Delta_H(G) = \Delta(G).
\]

Recall that if \( X \) is a finite set, then \( \pi(X) \) denotes the set of prime divisors of \( |X| \).

Let us assume that \((\ast)\) holds, so every derangement in \( G \) is an \( r \)-element, for some fixed prime \( r \). Clearly, every derangement of \( G_0 \) on \( \Omega \) is also an \( r \)-element. Now, if \( s \in \pi(G_0) \setminus \pi(M) \) then every nontrivial \( s \)-element in \( G_0 \) is a derangement, so \( \pi(G_0) = \pi(M) \) or \( \pi(M) \cup \{r\} \). In particular, if we set \( \pi_0 := \pi(G_0) \setminus \pi(M) \), then \( |\pi_0| \leq 1 \).
4.1. Sporadic groups

**Proposition 4.1.** Theorem 2 holds if $G_0$ is a sporadic group or the Tits group.

**Proof.** First assume that $G_0$ is not the Monster. The maximal subgroups of $G_0$ are available in GAP [25], and it is easy to identify the cases $(G_0, M)$ with $|\pi_0| \leq 1$. For the reader’s convenience, the cases that arise are listed in Table 3. We now consider each of these cases in turn. With the aid of GAP [25], we can compute the permutation character $\chi = 1_{G_0}^M$, noting that

$$\Delta_M(G_0) = \{ x \in G_0 : \chi(x) = 0 \}.$$  

In this way, we deduce that property (⋆) holds if and only if $(G_0, M) = (M_{11}, L_2(11))$. Here $\pi(M) = \pi(G_0)$, $G = M_{11}$, $H = L_2(11)$ and $E(G) = \{4, 8\}$. This case is recorded in Table 1.

Now assume $G = \mathbb{M}$ is the Monster. As noted in [6,45], there are 44 conjugacy classes of known maximal subgroups of $\mathbb{M}$ (these subgroups are conveniently listed in [6, Table 1], together with $L_2(41)$). Moreover, it is known that any additional maximal subgroup of $\mathbb{M}$ is almost simple with socle $L_2(13)$, $U_3(4)$, $U_3(8)$ or $2B_2(8)$. It is routine to check that $|\pi_0| \geq 2$ in each of these cases. □

4.2. Alternating groups

**Proposition 4.2.** Theorem 2 holds if $G_0 = A_n$ is an alternating group.

**Proof.** If $n < 12$ then the result can be checked directly using GAP [25]; the only cases $(G, H)$ with property (⋆) are the following:

$$(A_6, 3^2 : 4), (A_5, D_{10}), (A_5, A_4), (A_5, S_3),$$

which are recorded in Table 1 as

$$(L_2(9), P_1), (L_2(4), D_{10}), (L_2(4), P_1), (L_2(4), D_6)$$

respectively (see Remark 3). For the remainder, we may assume that $n \geq 12$. Seeking a contradiction, let us assume that there is a fixed prime $r$ such that every derangement in $G$ is an $r$-element.

Let $s$ be a prime such that $n/2 < s < n - 2$ and let $x \in G_0$ be an $s$-cycle (such a prime exists by Bertrand’s postulate). Since $C_G(x)$ is not an $r$-group, Lemma 2.1(ii) implies that $x$ has fixed points and thus $H$ contains $s$-cycles. By applying a well known theorem of Jordan (see [52, Theorem 13.9]), we deduce that $H$ is either intransitive or imprimitive, and we can rule out the latter possibility since $s$ divides $|H|$. Therefore, $H$ is the stabilizer of a $k$-set for some $k$ with $1 < k < n/2$.

Suppose $n$ is even and let $x_i \in G_0$ be an element with cycles of length $i$ and $n - i$ for $i \in \{3, 5, 7\}$. Then at least two of the $x_i$ are derangements, so we have reached a contradiction. Now assume $n$ is odd. An $n$-cycle does not fix a $k$-set, so $n$ must be an $r$-power. Therefore, any element with cycles of length $(n - 1)/2$, $(n - 1)/2$ and 1 must fix a $k$-set (since its order is not an $r$-power), so $k = 1$ or $(n - 1)/2$. It follows that any element with cycles of length 2, 3 and $n - 5$ is a derangement, and this final contradiction completes the proof of the proposition. □
Table 3. Maximal subgroups of sporadic simple groups, $|\pi_0| \leq 1$

<table>
<thead>
<tr>
<th>$G_0$</th>
<th>$M$</th>
<th>$\pi_0$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_{11}$</td>
<td>$A_6,2_3,S_5$</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>$L_2(11)$</td>
<td>-</td>
</tr>
<tr>
<td>$M_{12}$</td>
<td>$M_{11},L_2(11)$</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>$A_6,2^2,2 \times S_5$</td>
<td>11</td>
</tr>
<tr>
<td>$M_{22}$</td>
<td>$A_7,L_3(4)$</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>$L_2(11)$</td>
<td>7</td>
</tr>
<tr>
<td>$M_{23}$</td>
<td>$M_{22}$</td>
<td>23</td>
</tr>
<tr>
<td>$M_{24}$</td>
<td>$M_{23}$</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>$M_{22}.2$, $L_3(2).2$, $U_3(3)$</td>
<td>5</td>
</tr>
<tr>
<td>$J_2$</td>
<td>$3.A_6.2_2,2^{1+4}:A_5$, $A_4 \times A_5$, $A_5 \times D_{10}$, $5^2:D_{12}$, $A_5$</td>
<td>7</td>
</tr>
<tr>
<td>$J_3$</td>
<td>$L_2(16).2$</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>$L_2(19)$</td>
<td>17</td>
</tr>
<tr>
<td>$Co_1$</td>
<td>$3.Suz.2$, $Co_2$, $Co_3$, $2^{11}:M_{24}$</td>
<td>13</td>
</tr>
<tr>
<td>$Co_2$</td>
<td>$M_{23}$</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>$Mcl,HS.2,U_6(2).2,2^{10}:M_{22}.2$</td>
<td>23</td>
</tr>
<tr>
<td>$Co_3$</td>
<td>$M_{23}$</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>$Mcl.2,HS$</td>
<td>23</td>
</tr>
<tr>
<td>$Fi_{22}$</td>
<td>$2.U_6(2),2^{10}:M_{22}$</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>$\Omega_7(3)$</td>
<td>11</td>
</tr>
<tr>
<td>$Fi_{24}'$</td>
<td>$Fi_{23}$</td>
<td>29</td>
</tr>
<tr>
<td>$HS$</td>
<td>$M_{22}$</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>$U_3(5).2$, $L_3(4).2_1$, $S_8$</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>$M_{11}$</td>
<td>7</td>
</tr>
<tr>
<td>$Mcl$</td>
<td>$M_{22}$</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>$U_4(3)$, $U_3(5)$, $L_3(4).2_2$, $2.A_8$, $2^4:A_7$</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>$M_{11}$</td>
<td>7</td>
</tr>
<tr>
<td>$Suz$</td>
<td>$G_2(4)$</td>
<td>11</td>
</tr>
<tr>
<td>$He$</td>
<td>$Sp_4(4).2$</td>
<td>7</td>
</tr>
<tr>
<td>$HN$</td>
<td>$2.HS.2$, $A_{12}$</td>
<td>19</td>
</tr>
<tr>
<td>$O'N$</td>
<td>$J_1$</td>
<td>31</td>
</tr>
<tr>
<td>$Ru$</td>
<td>$(2^2 \times 2.B_2(8)):3$</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>$L_2(29)$</td>
<td>13</td>
</tr>
<tr>
<td>$^2F_4(2)'$</td>
<td>$L_2(25)$</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>$L_3(3).2$</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>$A_6,2^2,5^2:4A_4$</td>
<td>13</td>
</tr>
</tbody>
</table>

4.3. Exceptional groups

Now let us assume that $G_0$ is a simple exceptional group of Lie type over $\mathbb{F}_q$, where $q = p^f$ and $p$ is a prime. For $x \in G_0$, let $\mathcal{M}(x)$ be the set of maximal subgroups of $G_0$ containing $x$. We will write $\Phi_i$ for the $i$th cyclotomic polynomial evaluated at $q$, so $q^n - 1 = \prod_{d|n} \Phi_d$. Recall that if $e \geq 2$ and $q^e - 1$ has a primitive prime divisor, then we use the notation $\ell_e(q)$ to denote the largest such divisor of $q^e - 1$. 
Proposition 4.3. Theorem 2 holds if $G_0$ is a simple exceptional group of Lie type.

Proof. Recall the notational set-up introduced at the beginning of Sect. 4: $H$ is a point stabilizer in $G$, and $H_0 = H \cap G_0$. In view of (3), in order to show that (●) does not hold we may assume that $G = G_0$. Seeking a contradiction, suppose that every derangement in $G$ is an $r$-element, for some fixed prime $r$. We will consider each possibility for $G$ in turn.

Case 1 $G = 2B_2(q)$, with $q = 2^{2m+1}$ and $m \geq 1$.

Let $\Phi'_4 = q + \sqrt{2q} + 1$ and $\Phi'_4 = q - \sqrt{2q} + 1$ (note that $\Phi'_4 \Phi''_4 = q^2 + 1$).

By inspecting [2, Table II], [29, Table 6] and [30, Table 1], we see that $G$ has two cyclic maximal tori $T_i = \langle x_i \rangle$, $i = 1, 2$, of order $\Phi'_4$ and $\Phi''_4$, respectively, such that $|N_G(T_i)/T_i| = 4$, $(|x_1|, |x_2|) = 1$ and $M(x_i) = \{N_G(T_i)\}$. Since no maximal subgroup of $G$ can contain conjugates of both $x_1$ and $x_2$, it follows that $x_i^G \cap H$ is empty for some $i = 1, 2$. Therefore, $x_i \in \Delta(G)$ and thus $|x_i|$ is a power of $r$. Let $j = 3 - i$. Then $|x_j|$ is indivisible by $r$, so $H$ contains a conjugate of $x_j$ and thus $H = N_G(T_j)$ is the only possibility (up to conjugacy). Now $G$ has a cyclic maximal torus of order $q - 1$, so let $x \in G$ be an element of order $q - 1 \geq 7$. Since $|H|$ is indivisible by $q - 1$, it follows that $x \in \Delta(G)$. But $r$ does not divide $q - 1$, so we have reached a contradiction.

Case 2 $G = 2G_2(q)$, with $q = 3^{2m+1}$ and $m \geq 1$.

This is very similar to the previous case. Here we take two cyclic maximal tori $T_i = \langle x_i \rangle$, $i = 1, 2$, of order $\Phi'_6 = q + \sqrt{3q} + 1$ and $\Phi'_6 = q - \sqrt{3q} + 1$, respectively, such that $|N_G(T_i)/T_i| = 6$, $(|x_1|, |x_2|) = 1$ and $M(x_i) = \{N_G(T_i)\}$. Note that $\Phi'_6 \Phi''_6 = q^2 - q + 1$. By arguing as in Case 1, we deduce that $|x_i|$ is a power of $r$ and $H = N_G(T_j)$ for some distinct $i$, $j$. Let $x \in G$ be an element of order 9 (see part (2) in the main theorem of [51], for example). Since $|H|$ is indivisible by 9, it follows that $x$ is a derangement, but this is a contradiction since $r \neq 3$.

Case 3 $G = 2F_4(q)$, with $q = 2^{2m+1}$ and $m \geq 1$.

Again, we proceed as in Case 1. Here $G$ has two cyclic maximal tori $T_i = \langle x_i \rangle$, $i = 1, 2$, where

$$|T_1| = \Phi'_{12} = q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1$$

$$|T_2| = \Phi''_{12} = q^2 - \sqrt{2q^3} + q - \sqrt{2q} + 1$$

and $|N_G(T_i)/T_i| = 12$, $(|x_1|, |x_2|) = 1$ and $M(x_i) = \{N_G(T_i)\}$. Note that $\Phi'_{12} \Phi''_{12} = q^4 - q^2 + 1$. As in Case 1, we see that $|x_i|$ is a power of $r$ and $H = N_G(T_j)$ for some distinct $i$, $j$. Let $x \in G$ be an element of order $\ell_4(q)$. Since $|H|$ is indivisible by $\ell_4(q)$, it follows that $x \in \Delta(G)$, but this is a contradiction since $r \neq \ell_4(q)$.

Case 4 $G = E_8(q)$.

Again, we can proceed as in the previous cases, working with cyclic maximal tori $T_1, T_2$ and an element $x \in G$ of order $\ell_{24}(q)$, where

$$|T_1| = \Phi_{15} = q^8 - q^7 + q^5 - q^4 + q^3 - q + 1$$

$$|T_2| = \Phi_{30} = q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$$
and $|N_G(T_i)/T_i| = 30$, $i = 1, 2$. We omit the details (note that $\ell_{24}(q) \in \pi(G) \setminus \pi(N_G(T_i)))$.

**Case 5** $G = 3D_4(q)$.

As indicated in [29, Table 6], $G$ has a maximal torus $T = \langle x \rangle$ of order $\Phi_2 = q^4 - q^2 + 1$ such that $|N_G(T)/T| = 4$ and $\mathcal{M}(x) = \{N_G(T)\}$.

Suppose that $x \not\in \Delta(G)$. Then $G \cap H$ is non-empty, and without loss of generality we may assume that $x \in H$ and thus $H = N_G(T)$. If $q = 2$ then $|H| = 52$ and $|\pi(G)/\pi(H)| = 2$, so we must have $q > 2$. Let $y_i \in G$ ($i = 1, 2$) be elements of order $\ell_i := \ell_{m_i}(q) \geq 5$, where $m_1 = 3$ and $m_2 = 6$. Since $|H|$ is indivisible by $\ell_1$ and $\ell_2$, it follows that $y_1, y_2 \in \Delta(G)$. But this is a contradiction since $\ell_1, \ell_2$ are distinct primes.

Now assume that $x \in \Delta(G)$, so $|x| = \Phi_2$ is a power of $r$. If $q = 2$ then $r = 13$ and $H$ must contain elements of order 7, 8, 9, 14, 19, 21, and 28, but no maximal subgroup of $G$ has this property (see [15], for example). Therefore, $q > 2$. Following [30, p. 698], let $y \in G$ be an element of order $\Phi_3$ such that $|C_G(y)|$ divides $\Phi_3^2$ and

$$\mathcal{M}(y) = \{G_2(q), PGL_3(q), (\Phi_6 \circ SL_3(q)).2d, \Phi_3^2 SL_2(3)\},$$

where $d = (3, \Phi_3)$. Now $(\Phi_2, \Phi_3) = 1$, so $y \not\in \Delta(G)$ and thus we may assume that $H \in \mathcal{M}(y)$. Let $z \in G$ be an element of order $\Phi_1 \Phi_2 \Phi_6 = (q^2 - 1)(q^2 - q + 1)$. Then $|H|$ is indivisible by $|z|$, so $z \in \Delta(G)$. But this is a contradiction since $(\Phi_2, \Phi_1 \Phi_2 \Phi_6) = 1$.

**Case 6** $G = 2E_6(q)$.

Let $d = (3, q + 1)$. As indicated in [29, Table 6] and [30, Table 1], $G$ has two cyclic maximal tori $T_i = \langle x_i \rangle$, $i = 1, 2$, of order $\Phi_3/d$ and $\Phi_6 \Phi_2/d$, respectively. Then $(|x_1|, |x_2|) = 1$ and

$$\mathcal{M}(x_1) = \{SU_3(q^3).3\}, \quad \mathcal{M}(x_2) = \begin{cases} \{\Phi_6.3D_4(q).3/d\} & \text{if } q > 2 \\ \{\Phi_6.3D_4(2), F_4(2), Fi_{22}\} & \text{if } q = 2. \end{cases}$$

No maximal subgroup of $G$ contains both $x_1$ and $x_2$ (see [40, Table 10.5]), so $x_i \in \Delta(G)$ for some $i$, and thus $|x_i|$ is a power of $r$.

First assume that $q = 2$, so $|x_1| = 19$, $|x_2| = 13$ and thus $r \in \{13, 19\}$. If $r = 13$, then $H$ contains a conjugate of $x_1$, so $H = SU_3(8).3$ is the only option, but this is not possible since $|\pi(G) \setminus \pi(H)| = 4$. Similarly, if $r = 19$ then $H \in \mathcal{M}(x_2)$ must contain elements of order 11, 13 and 17, but it is easy to check that this is not the case.

Now assume that $q > 2$. Let $x \in G$ be an element of order $\ell_{10}(q)$. Both $|SU_3(q^3).3|$ and $|\Phi_6.3D_4(q).3/d|$ are indivisible by $\ell_{10}(q)$, so $x \in \Delta(G)$. However, this is not possible since $\ell_{10}(q)$ and $|x_1|$ are coprime.

**Case 7** $G = G_2(q)$, $q \geq 3$.

We can use GAP [25] to rule out the cases $q \leq 5$, so we may assume that $q \geq 7$.

First assume that $q = 7$. By inspecting [29, Table 6] and [30, Table 1], we see that $G$ has two cyclic maximal tori $T_i = \langle x_i \rangle$, $i = 1, 2$, of order $\Phi_6 = 43$ and $\Phi_3 = 57$, respectively, with $\mathcal{M}(x_1) = \{SU_3(7).2\}$ and $\mathcal{M}(x_2) = \{SL_3(7).2\}$. From [40, Table 10.5], it follows that $x_i \in \Delta(G)$ for some $i$, so $H$ contains a conjugate
of \(x_j\), where \(j = 3 - i\). Therefore, \(H = \text{SL}_3^\epsilon(7)\) for some \(\epsilon = \pm\). As noted in [37, Table A.7], \(G\) contains elements of order \(7^2 + 7 = 56\) and \(7^2 + 7 + 1 = 57\). Now \(\text{SU}_3(7)\) contains no element of order 57, and \(\text{SL}_3(7)\) has no element of order 56. Therefore, \(G\) always contains a derangement of non-prime power order, which is a contradiction.

For the remainder, we may assume that \(q > 7\). We use the set-up in [17, Section 5.7]. Choose a 4-tuple \((k_1, k_2, k_3, k_6)\) such that \((k_1, k_2) = 1\), \(k_i\) divides \(\Phi_i\) for \(i \in \{1, 2\}\), \(k_3 = \Phi_3/(3, \Phi_3)\) and \(k_6 = \Phi_6/(3, \Phi_6)\). Note that the numbers \(k_1, k_2, k_3\) and \(k_6\) are pairwise coprime. Let \(y_1 \in G\) be an element of order \(k_6\), and fix a regular semisimple element \(y_2 \in G\) of order \(k_1\). Similarly, fix \(z_i \in G\), \(i = 1, 2\), where \(|z_1| = k_3\) and \(z_2\) is a regular semisimple element of order \(k_2\).

From [40, Table 10.5], it follows that either \(y_1\) or \(z_1\) is a derangement. Suppose that \(y_1 \in \Delta(G)\). Then \(H\) contains a conjugate of \(z_1\), so [17, Lemma 5.27] implies that \(H = \text{SL}_3(q)\) is the only possibility. If \(H\) also contains a conjugate of \(z_2\), then \(H = G\) by [17, Corollary 5.28], a contradiction. Therefore \(z_2 \in \Delta(G)\), but once again we reach a contradiction since \((k_2, k_6) = 1\). An entirely similar argument applies if \(z_1 \in \Delta(G)\).

**Case 8** \(G \in \{\text{E}_6(q), \text{E}_7(q)\}\).

First assume that \(G = \text{E}_7(q)\). Let \(d = (2, q - 1)\). As in [17, Section 5.2], let \(y_1, y_2 \in G\) be elements of order \(\Phi_{18}\) and \(\Phi_2\Phi_{14}/d = (q^7 + 1)/d\), respectively, and let \(z_1, z_2 \in G\) be elements of order \(\Phi_9\) and \(\Phi_1\Phi_7/d = (q^7 - 1)/d\), respectively. From [17, Corollary 5.6], we deduce that \(y_i, z_j \in \Delta(G)\) for some \(i, j \in \{1, 2\}\). However, it is easy to check that \(|y_i|, |z_j|) = 1\) for all \(i, j\), so this is a contradiction.

The case \(G = \text{E}_6(q)\) is entirely similar, using [17, Corollary 5.11] and elements \(y_i, z_i \in G\) with \(|y_1| = \Phi_9/d\), \(|y_2| = \Phi_4\), \(|z_1| = \Phi_3\Phi_{12}\) and \(|z_2| = \Phi_5\) (where \(d = (3, q - 1)\)).

**Case 9** \(G = \text{F}_4(q)\).

For \(q > 2\), we can proceed as in Case 8, using the information in [17, Section 5.5]. The reader can check the details.

Now assume that \(q = 2\). By inspecting [29, Table 6] and [30, Table 1], we see that \(G\) has two cyclic maximal tori \(T_i = \langle x_i \rangle\), \(i = 1, 2\), of order \(\Phi_{12} = 13\) and \(\Phi_8 = 17\), respectively, such that \(\mathcal{M}(x_1) = \langle 3D_4(2).3, 2F_4(2), L_4(3).2_2 \rangle\) and \(\mathcal{M}(x_2) = \langle \text{Sp}_8(2) \rangle\). Therefore, \(r \in \{13, 17\}\). If \(r = 13\), then \(H\) contains a conjugate of \(x_2\), so \(H = \text{Sp}_8(2)\). However, [15] indicates that \(G\) has an element of order 28, but \(\text{Sp}_8(2)\) does not, so this case is ruled out. Therefore, \(r = 17\) and \(H\) contains a conjugate of \(x_1\), so \(H \in \mathcal{M}(x_1)\). However, in each case one can check that \(H\) does not contain an element of order 30, but \(G\) does. This final contradiction eliminates the case \(G = \text{F}_4(q)\).

This completes the proof of Proposition 4.3. \(\square\)

### 4.4. Classical groups

In order to complete the proof of Theorem 2, we may assume that \(G_0\) is a classical group over \(\mathbb{F}_q\). Due to the existence of certain exceptional isomorphisms involving low-dimensional classical groups (see [38, Proposition 2.9.1], for example), and in
view of our earlier work in Sects. 4.1, 4.2 and 4.3, we may assume that $G_0$ is one of
the groups listed in Table 4.

We will focus initially on the low-dimensional classical groups with socle $L_2(q)$
and $L_3^\xi(q)$, which require special attention. As before, if a primitive prime divisor of
$q^e - 1$ exists, then $\ell_e(q)$ denotes the largest such prime divisor (as noted in Sect. 2,
if $e \geq 2$, then $\ell_e(q)$ exists unless $(q, e) = (2, 6)$, or $e = 2$ and $q$ is a Mersenne
prime).

**Lemma 4.4.** Theorem 2 holds if $G = L_2(q)$ and $q$ is even.

**Proof.** Write $q = 2^f$, where $f \geq 3$ (since $L_2(4) \cong A_5$, we may assume that
$f \geq 3$). The maximal subgroups of $G$ were originally classified by Dickson [16]
(also see [5, Tables 8.1 and 8.2]); the possibilities for $H$ are as follows:

(a) $H = (\mathbb{Z}_2)^f: \mathbb{Z}_{q-1} = P_1$ is a maximal parabolic subgroup of $G$;
(b) $H = D_{2(q+1)}$;
(c) $H = L_2(q_0)$ with $q = q_0^6$, where $q$ is a prime and $q_0 \neq 2$.

The case $f = 3$ can be handled using GAP [25], and we find that (●) holds if and
only if $(H, r, \mathcal{E}(G))$ is one of the following (recall that $\mathcal{E}(G)$ denotes the set of
orders of derangements in $G$):

$$(P_1, 3, \{3, 9\}), \ (D_{18}, 7, \{7\}), \ (D_{14}, 3, \{3, 9\}).$$

For the remainder, we may assume that $f \geq 4$.

Note that a Sylow 2-subgroup of $G$ is self-centralizing and elementary abelian.
In particular, if $x \in G$ then either $|x| = 2$, or $|x|$ divides $q + 1$. Also note that $G$
contains elements of order $q \pm 1$, and it has a unique class of involutions.

**Case 1** $H = P_1$.

We claim that (●) holds if and only if $r = q + 1$ is a Fermat prime. To see this,
first observe that $|G : H| = q + 1$ and $|H| = q(q - 1)$ are relatively prime, so
any element $x \in G$ of order $q + 1$ is a derangement. Therefore, if (●) holds then
$q + 1 = r^e$ for some $e \geq 1$, and thus Lemma 2.6 implies that $f$ is a 2-power and
$e = 1$ (so $r = q + 1$ is a Fermat prime).

For the converse, suppose that $q + 1$ is a Fermat prime. We need to show that
every derangement in $G$ has order $r = q + 1$. Let $y \in \Delta(G)$, so $|y|$ divides 2 or
$q \pm 1$. But $q + 1 = r$ is a prime, so either $|y| \in \{2, r\}$ or $|y|$ divides $q - 1$. Every
involution has fixed points since $G$ has a unique class of involutions, so $|y| > 2$.
If $|y|$ divides $q - 1$, then $y$ belongs to a maximal torus that is $G$-conjugate to the
subgroup $\mathbb{Z}_{q-1} < H$. Again, this implies that $y$ has fixed points. Therefore, $|y| = r$
is the only possibility and the result follows.

<table>
<thead>
<tr>
<th>$G_0$</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L_n(q)$</td>
<td>$n \geq 2, (n, q) \neq (2, 2), (2, 3), (2, 4), (2, 5), (2, 9), (3, 2), (4, 2)$</td>
</tr>
<tr>
<td>$U_n(q)$</td>
<td>$n \geq 3, (n, q) \neq (3, 2)$</td>
</tr>
<tr>
<td>$PS_{2n}(q)$</td>
<td>$n \geq 4$ even, $(n, q) \neq (4, 2), (4, 3)$</td>
</tr>
<tr>
<td>$P\Omega_n^\pm(q)$</td>
<td>$n \geq 7$</td>
</tr>
</tbody>
</table>
Case 2 $H = D_{2(q \pm 1)}$.

The case $H = D_{2(q - 1)}$ is identical to the previous one, and the same conclusion holds. A very similar argument also applies if $H = D_{2(q + 1)}$. Here any element of order $q - 1$ is a derangement and by applying Lemma 2.6 we deduce that $(\star)$ holds if and only if $r = q - 1$ is a Mersenne prime.

Case 3 $H = L_2(q_0)$, where $q = q_0^e$, $e$ prime, $q_0 \neq 2$.

Finally, observe that subfield subgroups are easily eliminated since elements of order $q \pm 1$ are derangements.

Lemma 4.5. Theorem 2 holds if $G_0 = L_2(q)$ and $q$ is even.

Proof. As before, write $q = 2^f$, where $f \geq 3$. In view of Lemma 4.4, we may assume that

$$G = G_0.\langle \phi \rangle \leq \Gamma L_2(q) = \text{Aut}(G_0),$$

where $\phi$ is a nontrivial field automorphism of $G_0$, so the order of $\phi$ divides $f$. The case $f = 3$ can be handled directly, using [25] for example. Here $G = \Gamma L_2(8)$ and we find that $(\star)$ holds if and only if $(H, r, E(G))$ is one of the following:

$$(N_G(P_1), 3, [3, 9]), (N_G(D_{18}), 7, [7]), (N_G(D_{14}), 3, [3, 9]).$$

For the remainder, we may assume that $f \geq 4$.

Since $G_0 \not\leq H$, we have $G = G_0H$. Set $H_0 = H \cap G_0$ and note that $H_0$ is a maximal subgroup of $G_0$ (see [5, Table 8.1]). As in (3), we have $\Delta_{H_0}(G_0) \subseteq \Delta_H(G)$, whence Lemma 4.4 implies that $(\star)$ holds only if one of the following holds:

(a) $H_0 = P_1$, $r = q + 1$ is a Fermat prime;
(b) $H_0 = D_{2(q + 1)}$, $r = q - 1$ is a Mersenne prime;
(c) $H_0 = D_{2(q + 1)}$, $r = q + 1$ is a Fermat prime.

We consider each of these cases in turn.

Case 1 $H_0 = D_{2(q + 1)}$, $r = q - 1$ is a Mersenne prime.

Here $f \geq 5$ is a prime, so $G = \Gamma L_2(q) = G_0.\langle \phi \rangle$ and $H = H_0.\langle \phi \rangle$ is the only possibility, where $\phi$ has order $f$. Note that

$$C_G(\phi) = L_2(2) \times \langle \phi \rangle \cong S_3 \times \mathbb{Z}_f,$$

so if $x \in G$ then either $|x| \in \{2, r, f, 2f, 3f\}$, or $|x|$ divides $q + 1$. We claim that $E(G) = \{r\}$. Note that $\langle \phi \rangle$ is a Sylow $f$-subgroup of $G$.

Let $y \in G$ be a nontrivial element. If $|y| \in \{2, f\}$, or if $|y|$ divides $q + 1$, then $y$ is conjugate to an element of $H$ and thus $y$ has fixed points. Next suppose that $|y| = kf$ and $k \in \{2, 3\}$. Then $|y^k| = f$ and thus $y^k$ is $G$-conjugate to $\phi^j$ for some $1 \leq i < f$. Without loss of generality, we may assume that $y^k = \phi$, so $y \in C_G(\phi)$. Since $|H| = 2(q + 1)f$, $H$ has a Sylow $2$-group $R = \langle u \rangle \cong \mathbb{Z}_2$ and a normal $2$-complement $V \langle \phi \rangle$ of order $(q + 1)f$, where $V \cong \mathbb{Z}_{q+1}$. Since $\phi$ normalizes $H_0 = VR$, we deduce that $\phi$ centralizes $R$. Now $q + 1$ is divisible by $3$, so $V$ has a unique subgroup of order $3$, say $\langle x \rangle$. Then the involution $u$ inverts $x$, and $\phi$ centralizes $x$ since $|\phi| = f \geq 5$ is odd. Thus $S_3 \cong \langle u, x \rangle \leq C_{G_0}(\phi)$,
which implies that $C_G(\phi) = \langle u, x \rangle \times \langle \phi \rangle \leq H$. Therefore, $y \in H$. We conclude that every derangement in $G$ has order $r$, as required.

In the two remaining cases, $r = q + 1$ is a Fermat prime and $f = 2^m$ for some integer $m \geq 2$. In both cases, we claim that ($\ast$) does not hold. In order to see this, we may assume that the index of $G_0$ in $G$ is a prime number, which in this case implies that $[G : G_0] = 2$, so $G = G_0.\langle \phi \rangle$ and $\phi$ is an involutory field automorphism of $G_0$. Indeed, if $G_0 \trianglelefteq G$ then $G = HG_1$ and Lemma 2.2 implies that $\Delta_L(G_1) \leq \Delta(G)$ for any subgroup $L$ of $G_1$ containing $G_1 \cap H$.

**Case 2** $H_0 = D_{2(q-1)}, r = q + 1$ is a Fermat prime.

By the above comments, we may assume that $G = G_0.\langle \phi \rangle$ and $H = D_{2(q-1)}.\langle \phi \rangle$, where $\phi$ has order 2. Note that $C_G(\phi) = L_2(2^{f/2}) \times \langle \phi \rangle$. Since $C_G(\phi)$ does not contain a Sylow 2-subgroup of $G$, we deduce that the Sylow 2-subgroups of $G$ are nonabelian. Therefore $G$ contains an element $x$ of order 4. However, the Sylow 2-subgroups of $H$ are isomorphic to $C_2 \times C_2$, so $x \in \Delta(G)$. We conclude that $G$ contains derangements of order $r$ and 4, so ($\ast$) does not hold.

**Case 3** $H_0 = P_1, r = q + 1$ is a Fermat prime.

Finally, let us assume that $H = N_G(P_1) = P_1.\langle \phi \rangle = H_0.\langle \phi \rangle$, where $|\phi| = 2$. As above, we have $C_G(\phi) = L_2(2^{f/2}) \times \langle \phi \rangle$, so $C_G(\phi)$ contains an element of order 2. We claim that $H$ does not contain such an element.

Seeking a contradiction, suppose $x \in H$ has order $2(q_0 + 1)$. Since $H = H_0 \cup H_0.\phi$ and $H_0 = P_1$ has no element of order $2(q_0 + 1)$, we deduce that $x \in H_0.\phi$ and we may write $x = u.\phi$ with $u \in H_0$. In terms of matrices (and a suitable basis for the natural $L_2(q)$-module), we have

$$u = \begin{pmatrix} \lambda & a \\ 0 & \lambda^{-1} \end{pmatrix}$$

where $\lambda, a \in \mathbb{F}_q$ and $\lambda \neq 0$. Then $x^2 = (u.\phi)(u.\phi) = uu.\phi$ has order $q_0 + 1$. We may assume that $\phi$ is the standard field automorphism of order 2 with respect to this basis, so

$$x^2 = uu.\phi = \begin{pmatrix} \lambda & a \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} \lambda^{q_0} & a^{q_0} \\ 0 & \lambda^{-q_0} \end{pmatrix} = \begin{pmatrix} \lambda^{1+q_0} & b \\ 0 & \lambda^{-1-q_0} \end{pmatrix}$$

with $b = \lambda^{q_0} + a\lambda^{-q_0}$. Since $x^2$ has order $q_0 + 1$ we deduce that $\lambda^{2(q_0+1)} = 1$, which implies that $\lambda^{q_0+1} = 1$ since $\mathbb{F}_q$ has characteristic 2. Therefore

$$x^2 = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

has order $q_0 + 1$, which is absurd. This justifies the claim, and we deduce that $\Delta(G)$ contains elements of order $2(q_0 + 1)$. In particular, ($\ast$) does not hold.

**Lemma 4.6.** Theorem 2 holds if $G_0 = L_2(q)$ and $q$ is odd.

**Proof.** Write $q = p^f$, where $p$ is an odd prime. In view of the isomorphisms $L_2(5) \cong A_5$ and $L_2(9) \cong A_6$, we may assume that $q \geq 7$ and $q \neq 9$. The case
$q = 7$ can be checked directly using GAP, and we find that $(\star)$ holds if and only if $(G, H, r, \mathcal{E}(G))$ is one of the following:

$$(L_2(7), P_1, 2, \{2, 4\}), \ (L_2(7), S_4, 7, \{7\}), \ (PGL_2(7), N_G(P_1), 2, \{2, 4, 8\}).$$

For the remainder, we may assume that $q \geq 11$.

**Case 1** $G = G_0$.

First assume that $G = L_2(q)$. The maximal subgroups of $G$ are well known (see [5, Tables 8.1 and 8.2]); the possibilities for $H$ are as follows:

(a) $H = (\mathbb{Z}_p)^f : \mathbb{Z}_{(q-1)/2} = P_1$ is a maximal parabolic subgroup of $G$;
(b) $H = D_{q-\epsilon}$, where $q \geq 13$ if $\epsilon = 1$;
(c) $H = L_2(q_0)$, where $q = q_0^\epsilon$ for some odd prime $\epsilon$;
(d) $H = PGL_2(q_0)$, where $q = q_0^2$;
(e) $H = A_5$, where $q \equiv \pm 1 \pmod{10}$ and either $q = p$, or $q = p^2$ and $p \equiv \pm 3 \pmod{10}$;
(f) $H = A_4$, where $q = p \equiv \pm 3 \pmod{8}$ and $q \neq \pm 1 \pmod{10}$;
(g) $H = S_4$, where $q = p \equiv \pm 1 \pmod{8}$.

Note that $G$ contains elements of order $(q \pm 1)/2$, and a unique conjugacy class of involutions.

If $H$ is a subfield subgroup (as in (c) or (d) above), then it is clear that any element of order $(q \pm 1)/2$ is a derangement, so property $(\star)$ does not hold in this situation. Similarly, it is straightforward to handle the cases $H \in \{A_5, A_4, S_4\}$. For example, suppose $H = A_5$, so $q \equiv \pm 1 \pmod{10}$ and either $q = p$, or $q = p^2$ and $p \equiv \pm 3 \pmod{10}$. Note that every nontrivial element of $H$ has order 2, 3 or 5. If $q \geq 19$ then any element of order $(q \pm 1)/2$ is a derangement; if $q = 11$, then elements of order 6 are derangements. The cases $H = A_4$ and $S_4$ are just as easy.

If $H = D_{q-1}$ then any element in $G$ of order $p$ or $(q + 1)/2$ is a derangement, and the dihedral groups of order $q + 1$ can be eliminated in a similar fashion.

Finally, let us assume that $H = P_1 = (\mathbb{Z}_p)^f : \mathbb{Z}_{(q-1)/2}$, so $|H| = q(q-1)/2$ and $|G : H| = q + 1$. We claim that $(\star)$ holds if and only if $q = 2r^\epsilon - 1$ for some positive integer $\epsilon$.

First observe that any element of order $(q + 1)/2$ is a derangement, so if $(\star)$ holds then $q = 2r^\epsilon - 1$ for some $\epsilon \in \mathbb{N}$. For the converse, suppose that $q = 2r^\epsilon - 1$. We claim that

$$\mathcal{E}(G) = \{r^i : 1 \leq i \leq \epsilon\}.$$  

Since $|H|$ is indivisible by $r$, the inclusion $\{r^i : 1 \leq i \leq \epsilon\} \subseteq \mathcal{E}(G)$ is clear. To see that equality holds, let $y \in G$ be a nontrivial element, and suppose that $|y|$ is divisible by a prime $s \neq r$. Since a Sylow $p$-subgroup of $G$ is self-centralizing, it follows that either $|y| = p$, or $|y| = 2$ and $r$ is odd, or $|y|$ is a divisor of $(q-1)/2$. In the first two cases, it is clear that $y$ has fixed points, so let us assume that $|y|$ divides $(q-1)/2$. Then $y$ is conjugate to an element of the maximal torus $\mathbb{Z}_{(q-1)/2} < H$, so once again $y$ has fixed points. This justifies the claim.

**Case 2** $G \neq G_0$.

To complete the proof of the lemma, we may assume that $G \neq G_0$, $q \geq 11$ and $H_0 = H \cap G_0 = P_1$, in which case $(\star)$ holds only if $q = 2r^\epsilon - 1$ for some
positive integer $e$ (note that $H \cap G_0$ is a maximal subgroup of $G_0$). There are several possibilities for $G$.

First assume that $G = \text{PGL}_2(q)$, so $H = (\mathbb{Z}_p)^f : \mathbb{Z}_q - 1$. We claim that ($\bullet$) holds if and only if $r = 2$ and $q = 2^{e+1} - 1$ is a Mersenne prime. As above, any element of order $(q + 1)/2$ is a derangement. Now $G$ also contains elements of order $q + 1$, and they are also derangements. Therefore, if ($\bullet$) holds then $r = 2$ is the only possibility, so $p^f + 1 = 2^{e+1}$ and Lemma 2.6 implies that $q = p = 2^{e+1} - 1$ is a Mersenne prime.

For the converse, suppose that $q = p = 2^{e+1} - 1$ is a Mersenne prime. We claim that

$$E(G) = \{2^i : 1 \leq i \leq e + 1\}.$$  

As above, any involution in $G_0$ is a derangement, and so is any element in $G$ of order $2^i$ with $1 < i \leq e + 1$ since $|H|_2 = 2$, hence $\{2^i : 1 \leq i \leq e + 1\} \subseteq E(G)$. To see that equality holds, suppose that $y \in G$ has order divisible by an odd prime. Then either $|y| = p$, or $y$ is conjugate to an element of the maximal torus $\mathbb{Z}_q - 1 < H$; in both cases, $y$ has fixed points. The result follows.

To complete the proof of the lemma, we may assume that $G = G_0, (\phi)$ or $G_0, (\delta \phi)$, where $\phi$ is a nontrivial field automorphism of $G_0$ of order $e$ (so $e$ divides $f$) and $\delta = \text{diag}(\omega_1, \omega_2) \in \text{PGL}_2(q)$ (modulo scalars) is a diagonal automorphism of $G_0$. Recall that $(q + 1)/2 = r^e$ for some prime $r$ and positive integer $e$. Our goal is to show that ($\bullet$) does not hold.

First observe that $r$ is odd. Indeed, if $r = 2$ then $p^f + 1 = 2^{e+1}$ and thus Lemma 2.6 implies that $f = 1$, which is false. Next we claim that $f$ is a 2-power. To see this, first assume that $f$ is odd and $p = 2^t - 1$ is a Mersenne prime. Then $r^e = (p^f + 1)/2$ is divisible by $(p + 1)/2 = 2^{r-1}$, but $r$ is odd so this is not possible. For the general case, suppose that $f = 2^m a$ where $a \geq 0$ and $m > 1$ is odd (and we may assume that $a > 0$ if $p$ is a Mersenne prime). We now proceed as in the proof of Lemma 2.9(iii). We have

$$r^e = \frac{q^2 - 1}{2(q - 1)} = \frac{p^{2^{a+1}m} - 1}{2(p^{2^m} - 1)}$$

and thus $r = \ell_{2f}(p)$. Set $s = \ell_{2a+1}(p)$ (note that $s$ exists since $a > 0$ if $p$ is a Mersenne prime). Now $f = 2^a m$ is indivisible by $2^{a+1}$, so $(s, q - 1) = 1$ and thus $s$ does not divide $2(q - 1)$. Therefore, $r = s$ is the only possibility, but this is a contradiction since $2f = 2^{a+1}m > 2^{a+1}$. This justifies the claim.

Therefore, in order to show that ($\bullet$) does not hold, we may assume that $|G : G_0| = 2$. Write $G = G_0 \cup G_0^\gamma$.

If we identify $\Omega$ with the set of 1-dimensional subspaces of the natural $L_2(q)$-module, then $\phi$ and $\delta \phi$ fix the 1-spaces $\langle (1, 0) \rangle$ and $\langle (0, 1) \rangle$. Therefore, Lemma 2.4 implies that the coset $G_0^\gamma$ contains derangements. But every element in this coset has even order, which is incompatible with property ($\bullet$). 

To summarize, we have now established the following result. (Note that the case appearing in the final row of Table 5 is recorded as $(G, H) = (L_3(2), P_1)$ in Table 1).
We may assume that $H$ is a maximal parabolic subgroup. Without loss of generality, we will assume that $q + 1$ is a prime number for all $q$. We may assume that $H = \Gamma L_2(q)$, where $q$ is a prime number greater than 3. It is easy to check that $H$ is a maximal parabolic subgroup, or $H = \Gamma L_2(q)$ (with $q$ odd).

Suppose that $H$ is a maximal parabolic subgroup. Without loss of generality, we may assume that $H = \Gamma L_2(q)$. The cases for $H$ are given in [5, Tables 8.3 and 8.4]. We can immediately eliminate any subgroup $H$ that does not contain an element of order $(q^2 + q + 1)/d$, so this implies that $H$ is either a maximal parabolic subgroup, or $H = SO_3(q)$ (with $q$ odd).

Theorem 2 holds if $G_0 = \Gamma L_2(q)$.}

Lemma 4.8. Theorem 2 holds if $G_0 = \Gamma L_2(q)$.}

Proof. Set $d = (3, q - 1)$ and note that $G_0$ contains elements of order $(q^2 + q + 1)/d$ and $(q^2 - 1)/d$. We may assume that $q \geq 3$ since $L_3(2) \cong L_2(7)$. If $3 \leq q \leq 7$, then we can use GAP to verify the desired result; we find that (⋆) holds if and only if $G = \Gamma L_2(q)$, $H \in \{P_1, P_2\}$ and $r = (q^2 + q + 1)/d$, in which case $\mathcal{E}(G) = \{r\}$ (note that $(q^2 + q + 1)/d$ is a prime number for all $q \in \{3, 4, 5, 7\}$). For the remainder, we will assume that $q \geq 8$. In particular, note that $(q^2 - 1)/d$ is a prime power if and only if $q = 3$ or 7.

Case 1 $G = G_0$.

First assume that $G = \Gamma L_2(q)$. The possibilities for $H$ are given in [5, Tables 8.3 and 8.4]. We can immediately eliminate any subgroup $H$ that does not contain an element of order $(q^2 - 1)/d$, so this implies that $H$ is either a maximal parabolic subgroup, or $H = SO_3(q)$ (with $q$ odd).

Suppose that $H$ is a maximal parabolic subgroup. Without loss of generality, we may assume that $H = \Gamma L_2(q)$ (the actions of $G$ on 1-spaces and 2-spaces are permutation isomorphic), so $|H| = q^3(q - 1)(q^2 - 1)/d$. We claim that $G$ has property (⋆) if and only if one of the following holds:

\begin{align}
(a) & \quad d = 1 \text{ and } q^2 + q + 1 = r; \quad \text{or} \\
(b) & \quad d = 3 \text{ and } q^2 + q + 1 \in \{3r, 3r^2\}. \quad (4)
\end{align}

To see this, first notice that any element $x \in G$ of order $(q^2 + q + 1)/d$ is a derangement. Therefore, if (⋆) holds then $(q^2 + q + 1)/d = r^e$ for some positive integer $e$, and by applying Lemma 2.9 we deduce that (a) or (b) holds. Conversely, suppose that (a) or (b) holds. We claim that

\[ \mathcal{E}(G) = \begin{cases} 
\{r, r^2\} & \text{if } d = 3 \text{ and } q^2 + q + 1 = 3r^2 \\
\{r\} & \text{otherwise.}
\end{cases} \]

Table 5. The cases $(G, H, r)$ in Proposition 4.7

<table>
<thead>
<tr>
<th>$G$</th>
<th>$H$</th>
<th>$r$</th>
<th>$\mathcal{E}(G)$</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Gamma L_2(q)$</td>
<td>$N_G(D_{2(q+1)})$</td>
<td>$r$</td>
<td>$r$</td>
<td>$r = q - 1$ Mersenne prime</td>
</tr>
<tr>
<td>$\Gamma L_2(8)$</td>
<td>$N_G(P_1), N_G(D_{14})$</td>
<td>3, 3, 9</td>
<td>$r$</td>
<td>$q = 2^{e+1} - 1$ Mersenne prime</td>
</tr>
<tr>
<td>$PGL_2(q)$</td>
<td>$N_G(P_1)$</td>
<td>2</td>
<td>$2^i, 1 \leq i \leq e + 1$</td>
<td>$q = 2^e - 1$</td>
</tr>
<tr>
<td>$L_2(q)$</td>
<td>$P_1, D_{2(q-1)}$</td>
<td>$r$</td>
<td>$r^i, 1 \leq i \leq e$</td>
<td>$q = q + 1$ Fermat prime</td>
</tr>
<tr>
<td>$L_2(9)$</td>
<td>$P_1$</td>
<td>5</td>
<td>$r$</td>
<td>$q = q - 1$ Mersenne prime</td>
</tr>
<tr>
<td>$L_2(8)$</td>
<td>$P_1, D_{14}$</td>
<td>3, 9</td>
<td>$r$</td>
<td></td>
</tr>
<tr>
<td>$L_2(7)$</td>
<td>$S_4$</td>
<td>7</td>
<td>$r$</td>
<td></td>
</tr>
</tbody>
</table>
To see this, we use the fact that the action of $G$ on 1-spaces is doubly transitive, so the corresponding permutation character has the form $1^G_H = 1 + \chi$ for some irreducible character $\chi \in \text{Irr}(G)$ of degree $q(q + 1)$. By inspecting the character table of $G$ (see [20, Table 2], for example), we see that $\chi(x) = -1$ if and only if $x$ has order $r$ (or $r^2$ if $d = 3$ and $q^2 + q + 1 = 3r^2$). This justifies the claim.

Now assume that $H = \text{SO}_3(q)$, so $q$ is odd. Here elements of order $(q^2 + q + 1)/d$ are derangements, and so is any unipotent element with Jordan form $[J_2, J_1]$ (where $J_i$ denotes a standard unipotent Jordan block of size $i$). Therefore, $(\star)$ does not hold in this situation.

**Case 2** $G \neq G_0$.

To complete the proof of the lemma, we may assume that $G \neq G_0$ and $q \geq 8$. Let $M$ be a maximal subgroup of $G_0$ containing $H_0 := H \cap G_0$. From the analysis in Case 1, we may assume that $M = P_1$, in which case $H_0$ is either equal to $P_1$, or it is a non-maximal subgroup of type $P_{1.2}$ (a Borel subgroup of $G_0$) or $\text{GL}_2(q) \times \text{GL}_1(q)$. We can quickly eliminate the latter two possibilities. For instance, if $H_0$ is a Borel subgroup then $\Delta_{H_0}(G_0)$ contains all elements of order $(q^2 - 1)/d$, so $(\star)$ does not hold (see (3)). Similarly, if $H_0$ is of type $\text{GL}_2(q) \times \text{GL}_1(q)$ then $\Delta_{H_0}(G_0)$ contains elements of order $(q^2 + q + 1)/d$, and also unipotent elements with Jordan form $[J_3]$.

Therefore, we may assume that $H_0 = P_1$, with $q \geq 8$. To show that $(\star)$ does not hold, we may as well assume that we are in one of the two cases (a) and (b) in (4) above (otherwise the conclusion is clear). Note that the condition $H_0 = P_1$ implies that $G \leq \Gamma \text{L}_3(q)$ (that is, $G$ does not contain a graph or graph-field automorphism). Also note that we may identify $\Omega$ with the set of 1-dimensional subspaces of the natural $L_3(q)$-module. Note that $r > 3$.

First assume that $G = \text{PGL}_3(q)$, so $d = 3$ since we are assuming that $G \neq G_0$. Here $G$ has a cyclic maximal torus $\langle x \rangle$ of order $q^2 + q + 1$. Then $x$ is a derangement and thus $(\star)$ does not hold since $q^2 + q + 1$ is not a prime power (note that $(q^2 + q + 1)_3 = 3$).

For the remainder, we may assume that $q = p^f$ and $f \geq 2$ (also recall that $q \geq 8$). In view of (4), Lemma 2.9(iii) implies that $f$ is a 3-power. To deduce that $(\star)$ does not hold, we may assume that $|G : G_0|$ is a prime number. Since $G \leq \Gamma \text{L}_3(q)$ and $f$ is a 3-power, we may assume that $|G : G_0| = 3$ and thus $G = G_0 \langle \phi \rangle$ or $G_0 \langle \delta \phi \rangle$, where $\phi$ is a field automorphism of order 3 and $\delta$ is an appropriate diagonal automorphism $\text{diag}(\omega_1, \omega_2, \omega_3) \in \text{PGL}_3(q)$ (modulo scalars). In both cases, the result follows by applying Lemma 2.4. For example, $\delta \phi$ has more than one fixed point on $\Omega$, so Lemma 2.4 implies that the coset $G_0 \delta \phi$ contains derangements, none of which has $r$-power order. In view of this final contradiction, we conclude that $(\star)$ does not hold if $G \neq G_0$. \hfill \Box

**Lemma 4.9.** Theorem 2 holds if $G_0 = \text{U}_3(q)$.

**Proof.** Set $d = (3, q + 1)$ and observe that $G_0$ contains elements of order $(q^2 - q + 1)/d$ and $(q^2 - 1)/d$. Note that $(q^2 - 1)/d$ is a prime power if and only if $q \in \{3, 5\}$. In order to show that $(\star)$ does not hold, we may assume that $G = G_0$.

The cases $q \in \{3, 4, 5\}$ can be handled directly, using GAP, so for the remainder we will assume that $q \geq 7$. Let $V$ be the natural $G_0$-module, and let $P_1$ (respectively
N₁) be the G₀-stabilizer of a 1-dimensional totally isotropic (respectively, non-
degenerate) subspace of V. Note that N₁ is a subgroup of type GU₁(q) × GU₂(q).

We can immediately rule out any subgroup H that does not contain elements of
order (q² − 1)/d, which means that we may assume H is of type P₁, N₁ or O₃(q)
(q odd). In all three cases, elements of order (q² − q + 1)/d are derangements. In
addition, if H = N₁ (respectively, SO₃(q)) then unipotent elements with Jordan
form [J₃] (respectively, [J₂, J₁]) are derangements. Finally, suppose that H = P₁.
Let ω ∈ F_q² be an element of order q + 1 and set x = diag(1, ω, ω⁻¹) ∈ G
(modulo scalars) with respect to an orthonormal basis for V. Then x does not fix a
totally isotropic 1-space, whence x is a derangement of order q + 1.

Having handled the low-dimensional groups, we are now in a position to com-
plete the proof of Theorem 2 for linear and unitary groups.

Lemma 4.10. Theorem 2 holds if G₀ = Lₙ^±(q).

Proof. We may assume that n ≥ 4. Set d = (n, q − ε) and e = (q − ε)d. Let
V be the natural G₀-module. Let Pᵢ be the G₀-stabilizer of a totally isotropic i-
dimensional subspace of V (so Pᵢ is a maximal parabolic subgroup of G₀, and
we can take any i-space if ε = +). Similarly, if ε = − then let Nᵢ denote the
G₀-stabilizer of an i-dimensional non-degenerate subspace of V (so Nᵢ is of type
GUᵢ(q) × GUₙ₋ᵢ(q)). In order to show that (⋆) does not hold, we may assume that
G = G₀. There are several cases to consider.

Case 1 n = 2m and m ≥ 4 − ε is odd.

First assume that m ≥ 5. As in the proof of [12, Proposition 3.11], let x ∈ G be
an element of order (qᵐ⁺² − ε)(qᵐ⁻² − ε)/e. Then |x| is not a prime power (see
Lemma 2.7), and [28, Table II] indicates that x is a derangement unless one of the
following holds:

(a) ε = + and H = Pₘ₋₂ (or Pₘ₊₂);
(b) ε = − and H = Nₘ₋₂.

In (a), any element of order ℓⁿ(q) or ℓₙ⁻¹(q) is a derangement, and elements of
order ℓₙ(q) and ℓ₂(ₙ⁻¹)(q) are derangements in case (b).

Now assume m = 3, so (ε, n) = (+, 6). Let x ∈ G be an element of order
(q⁶ − 1)/e, which is not a prime power by Lemma 2.8. Here x is a Singer element,
and the main theorem of [3] implies that x is a derangement, unless H is a field
extension subgroup, so we have reduced to the case where H is of type GL₃(q²)
or GL₂(q³). In this situation, elements of order ℓ₅(q) are derangements, and so are
unipotent elements with Jordan form [J₂, J₁].

Case 2 n = 2m and m ≥ 3 − ε is even.

First assume that m ≥ 4. Let x ∈ G be an element of order (qᵐ⁺¹ − ε)(qᵐ⁻¹ −
ε)/e. Then Lemma 2.7 implies that |x| is not a prime power, and from [28, Table
II] we deduce that x is a derangement unless one of the following holds:

(a)’ ε = + and H = Pₘ₋₁ (or Pₘ₊₁);
(b)’ ε = − and H = Nₘ₋₁.
To deal with these cases, we can repeat the argument in Case 1.

Now assume $m = 2$, so $(e, n) = (+, 4)$. By applying the main theorem of [3], we deduce that elements of order $(q^4 - 1)/e$ are derangements unless $H$ is a field extension subgroup of type $GL_2(q^2)$. Moreover, since $(q^4 - 1)/e$ is not a prime power (see Lemma 2.8), we can assume that $H$ is of type $GL_2(q^2)$. Here elements of order $\ell_3(q)$ and unipotent elements with Jordan form $[J_2, J_1^2]$ are derangements.

**Case 3** $\epsilon = +, n = 2m + 1$ and $m \geq 2$.

If $G = L_{11}(2)$, then any element of order $2^{11} - 1 = 23 \cdot 89$ is a derangement, unless $H$ is a field extension subgroup of type $GL_1(2^{11})$, in which case elements of order $2^{10} - 1$ are derangements. For the remainder, we may assume that $(n, q) \neq (11, 2)$.

Let $x \in G$ be an element of order $(q^{m+1} - 1)(q^m - 1)/e$. By Lemmas 2.7 and 2.8, $|x|$ is not a prime power, so we may assume that $H = P_m$ (see [28, Table II]). If $m \geq 3$, then elements of order $\ell_n(q)$ or $\ell_{n-2}(q)$ are derangements. Similarly, if $m = 2$ then we can take elements of order $\ell_5(q)$ or $\ell_4(q)$.

**Case 4** $\epsilon = -, n = 2m + 1$ and $m \geq 4$.

Fix $x \in G$, where

$$|x| = \begin{cases} (q^{m+1} + 1)(q^m - 1)/e & m \text{ even} \\ (q^{m+2} + 1)(q^{m-1} - 1)/e & m \text{ odd} \end{cases}$$

By Lemma 2.7, $|x|$ is not a prime power, and [28, Table II] indicates that $x$ has fixed points only if $H$ stabilizes a subspace $U$ of $V$ with $\dim U \geq 2$. Therefore, we may assume that $H$ has this property, in which case any element of order $\ell_{2n}(q)$ or $\ell_{n-1}(q)$ is a derangement.

**Case 5** $\epsilon = -$ and $n \in \{4, 5, 6, 7\}$.

First assume that $n = 7$. Let $x \in G$ be an element of order $(q^6 - 1)/d$. Since $|x|$ is not a prime power, by inspecting the list of maximal subgroups of $G$ (see [5, Tables 8.37 and 8.38]) it follows that we can assume that $H \in \{P_3, N_1, SO_7(q)\}$. In all three cases, any element of order $\ell_{14}(q)$ is a derangement. Similarly, elements of order $\ell_{10}(q)$ are derangements, unless $H = N_1$, in which case any unipotent element with Jordan form $[J_7]$ is a derangement. The case $n = 5$ is entirely similar.

Next assume that $n = 6$. For now, let us assume that $q \not\in \{2, 5\}$. Let $x \in G$ be an element of order $(q^5 + 1)/d$. Then $|x|$ is not a prime power (see Lemma 2.8) and $H = N_1$ is the only maximal subgroup of $G$ containing such an element (see [28, p. 767]). Now, if $H = N_1$ then any element of order $(q^6 - 1)/e$ is a derangement of non-prime order power.

Suppose that $n = 6$ and $q \in \{2, 5\}$. The case $q = 2$ can be checked directly, using GAP for example, so let us assume that $q = 5$. Let $x \in G$ be an element of order $(5^6 - 1)/e = 434$. By inspecting the list of maximal subgroups of $G$ (see [5, Tables 8.26 and 8.27]), we deduce that $x$ is a derangement unless $H$ is of type $P_3$, $GL_3(5^2)$ or $GU_2(5^3)$, so we may assume that $H$ is one of these subgroups, in which case any element of order $\ell_{10}(5) = 521$ is a derangement. Suppose that $H = P_3$. Fix an orthonormal basis for $V$ and let $y = \text{diag}(1, 1, \omega, \omega^{-1}, \omega^2, \omega^{-2})$ (modulo scalars), where $\omega \in \mathbb{F}_{25}$ is an element of order 6. Then $y$ is a derangement. Similarly, if $H$ is of type $GL_3(5^2)$ or $GU_2(5^3)$, then any unipotent element with Jordan form $[J_2, J_1^4]$ is a derangement. This eliminates the case $G = U_6(5)$. 


A very similar argument applies if \( n = 4 \). Here the cases \( q \in \{2, 3\} \) can be checked directly, so let us assume that \( q \geq 4 \). Let \( x \in G \) be an element of order \((q^3 + 1)/d\). Then \(|x|\) is not a prime power (see Lemma 2.8) and again we reduce to the case \( H = N_1 \) (see [28, p. 767]). We can now take any element of order \((q^4 - 1)/e\), which will be a derangement of non-prime power order. \( \square \)

Next, we turn our attention to symplectic groups. Let \( G_0 = \text{PSp}_n(q) \) be a symplectic group with natural module \( V \). As before, we will write \( P_i \) (respectively, \( N_i \)) for the \( G_0 \)-stabilizer of an \( i \)-dimensional totally isotropic (respectively, non-degenerate) subspace of \( V \). We will also use \( n = m \perp (n - m) \) to denote an orthogonal decomposition of \( V \) of the form \( V = V_1 \perp V_2 \), where \( V_1 \) is a non-degenerate \( m \)-space. Further, we will say that a semisimple element \( x \in G_0 \) is of type \( m \perp (n - m) \) if it fixes such an orthogonal decomposition of \( V \), acting irreducibly on \( V_1 \) and \( V_2 \). Similar notation is used in [7, 12, 28].

To begin with, we will assume that \( n \geq 6 \); the special case \( G_0 = \text{PSp}_4(q) \) will be handled separately in Lemma 4.12.

**Lemma 4.11.** Theorem 2 holds if \( G_0 = \text{PSp}_n(q) \) and \( n \geq 6 \).

**Proof.** Set \( d = (2, q - 1) \) and write \( n = 2m \) with \( m \geq 3 \). As before, we may assume that \( G = G_0 \).

**Case 1** \( m \) odd.

The case \((n, q) = (6, 2)\) can be handled directly (using GAP, for example), so let us assume that \((n, q) \neq (6, 2)\). Let \( x \in G \) be an element of order \((q^m + 1)/d\). If \( q \) is even, then Lemma 2.6 implies that \(|x|\) is not a prime power, and it is easy to see that the same conclusion also holds if \( q \) is odd. By the main theorem of [3], \( x \) is a derangement unless one of the following holds:

(a) \( H \) is a field extension subgroup of type \( \text{Sp}_{n/k}(q^k) \) for some prime divisor \( k \) of \( n \);
(b) \( q \) is even and \( H = O_{n}^{-}(q) \).

In (a), elements of order \( \ell_{n-2}(q) \) are derangements, and so are unipotent elements with Jordan form \([J_2, J_1^{n-2}]\). Similarly, if (b) holds then elements of order \( \ell_m(q) \) are derangements, and so are semisimple elements of type \((n - 2) \perp 2 \) and order \((q^{m-1} + 1)(q + 1)\).

**Case 2** \( m \geq 6 \) even.

First assume that \( q \) is odd. Let \( x \in G \) be a semisimple element of type \((n - 4) \perp 4 \), so

\[
|x| = \begin{cases} 
q^{m-2} + 1 & \text{if } m \equiv 0 \pmod{4} \\
(q^{m-2} + 1)(q^2 + 1)/2 & \text{if } m \equiv 2 \pmod{4}.
\end{cases}
\]

Clearly, if \( m \equiv 2 \pmod{4} \) then \(|x|\) is divisible by \( \ell_4(q) \) and \( \ell_{n-4}(q) \), so \(|x|\) is not a prime power. The same conclusion also holds if \( m \equiv 0 \pmod{4} \) (see Lemma 2.6). By [7, Proposition 5.10], we may assume that \( H \) is of type \( N_4 \) or \( \text{Sp}_{n/2}(q^2) \).

In both cases, elements of order \( \ell_{n-2}(q) \) are derangements. In addition, unipotent elements with Jordan form \([J_2] \) (respectively, \([J_2, J_1^{n-2}] \)) are derangements if \( H \) is of type \( N_4 \) (respectively, \( \text{Sp}_{n/2}(q^2) \)).
Now assume that $q$ is even. Let $x \in G$ be a semisimple element of type $(n - 2) \perp 2$ and order $q^{m-1} + 1$. Now Lemma 2.6 implies that $|x|$ is not a prime power, and by applying the main theorem of [32] we deduce that $x$ is a derangement unless $H \in \{N_2, O_n^+(q)\}$. In both cases, elements of order $\ell_n(q)$ are derangements. Also, unipotent elements with Jordan form $[J_n]$ are derangements if $H = N_2$. Now, if $H = O_n^{++}(q)$ then let $y \in G$ be a block-diagonal element of the form $y = [y_1, y_2]$ (with respect to an orthogonal decomposition $n = (n - 2) \perp 2$), where $y_1 \in \text{Sp}_{n-2}(q)$ has order $\ell_m - 1(q)$ and $y_2 \in \text{Sp}_2(q)$ has order $q + 1$. Then $y$ is a derangement and the result follows.

**Case 3** $m = 4$.

The case $q = 2$ can be checked directly, so we may assume that $q \geq 3$. If $q$ is even, then we can repeat the relevant argument in Case 2. Now assume $q$ is odd. Let $x \in G$ be a semisimple element of type $6 \perp 2$ and order $q^3 + 1$. By Lemma 2.6, $|x|$ is not a prime power. The maximal subgroups of $G$ are listed in [5, Tables 8.48 and 8.49], and we deduce that $x$ is a derangement unless $H$ is of type $N_2$, $\text{GU}_4(q)$ or $L_2(q^3)$ (in the terminology of [5,38], the latter possibility is an almost simple irreducibly embedded subgroup in the collection $\mathcal{S}$). In each of these exceptional cases, any element of order $(q^4 + 1)/2$ is a derangement. In addition, if $H = N_2$ then unipotent elements with Jordan form $[J_8]$ are derangements. Similarly, if $H$ is of type $\text{GU}_4(q)$ or $L_2(q^3)$ then elements with Jordan form $[J_2, J_1^4]$ are derangements.

**Lemma 4.12.** Theorem 2 holds if $G_0 = \text{PSp}_n(q)$.

**Proof.** We may assume that $n = 4$. The result can be checked directly if $q \leq 7$, so let us assume that $q \geq 8$.

First assume that $q$ is odd. In terms of an orthogonal decomposition $4 = 2 \perp 2$, let $x = [x_1, x_2] \in G$ (modulo scalars) be an element of order $p(q + 1)$, where $x_1 \in \text{Sp}_2(q)$ is a unipotent element of order $p$, and $x_2 \in \text{Sp}_2(q)$ is irreducible of order $q + 1$. By inspecting the list of maximal subgroups of $G$ (see [5, Tables 8.12 and 8.13]), we deduce that $x$ is a derangement unless $H$ is of type $P_1$ or $\text{Sp}_2(q) : S_2$. In both of these cases, any element of order $\ell_4(q)$ is a derangement. Similarly, unipotent elements with Jordan form $[J_4]$ are derangements if $H$ is of type $\text{Sp}_2(q) : S_2$. Finally, suppose that $H = P_1$. Now $\text{Sp}_2(q)$ has precisely $\varphi(q+1)/2 \geq 2$ distinct classes of elements of order $q + 1$ (where $\varphi$ is the Euler totient function); if $y_1, y_2 \in \text{Sp}_2(q)$ represent distinct classes, then $y = [y_1, y_2] \in G$ (modulo scalars) is a derangement since it does not fix a totally isotropic 1-space.

Now assume $q$ is even. As above, let $x \in G$ be an element of order $2(q + 1)$. The maximal subgroups of $G$ are listed in [5, Table 8.14], and we see that $x$ is a derangement unless $H$ is of type $P_1$, $\text{Sp}_2(q) : S_2 \cong O_4^+(q)$ or $O_4^-(q)$. For $H = P_1$, we can repeat the argument in the $q$ odd case, so let us assume that $H = O_4^+(q)$. If $\epsilon = +$ then any element of order $\ell_4(q)$ is a derangement, and we can also find derangements of order 4 (with Jordan form $[J_4]$), since there are two conjugacy classes of such elements in $G$, but only one in $H$. Finally, if $\epsilon = -$ then we can find derangements of order 2 (with Jordan form $[J_2^2]$); these are $a_2$-type involutions in the sense of Aschbacher and Seitz [1]), and also derangements of order $q + 1$ of the form $[y_1, y_2]$ as above. \qed
To complete the proof of Theorem 2, we may assume that $G_0 = \Omega^\epsilon_n(q)$ is an orthogonal group, where $n \geq 7$. The low-dimensional groups with $n \in \{7, 8\}$ require special attention. We extend our earlier notation for orthogonal decompositions by writing $m^\pm$ to denote a non-degenerate $m$-space of type $\pm$ (when $m$ is even). Similarly, we write $N^\pm_m$ for the $G_0$-stabilizer of such a subspace of the natural $G_0$-module $V$. If $q$ is even, we will also adopt the standard Aschbacher–Seitz notation for involutions (see [1]).

**Lemma 4.13.** Theorem 2 holds if $G_0 = \Omega_7(q)$.

**Proof.** We may assume that $G = G_0$. The case $q = 3$ can be checked directly, so we may assume that $q \geq 5$ (recall that $q$ is odd). Let $x \in G$ be an element of order $(q^3 + 1)/2$, which is not a prime power. By [7, Proposition 5.20], $x$ is a derangement unless $H = N^-_6$, in which case any element of order $\ell_3(q)$ is a derangement, and so are unipotent elements with Jordan form $[J_7]$. $\square$

**Lemma 4.14.** Theorem 2 holds if $G_0 = \Omega^\pm_8(q)$.

**Proof.** As usual, we may assume that $G = G_0$. Let $V$ be the natural module for $G_0$. The case $q = 2$ can be checked directly, using GAP. Next suppose that $q = 3$. Let $x \in G$ be an element of order 20, fixing a decomposition of $V$ of the form $8 = 4^- \perp 4^-$. As indicated in [7, Table 3], $x$ is a derangement unless the type of $H$ is one of the following:

$$P_4, O_7(3), O^-_4(3) \rtimes S_2, GU_4(3), Sp_4(3) \otimes Sp_2(3)$$

where $O_7(3)$ is irreducible and $P_4$ is the stabilizer in $G$ of a maximal totally singular subspace of $V$.

By considering elements of order 14, we can immediately eliminate the cases $P_4, O^-_4(3) \rtimes S_2$ and $Sp_4(3) \otimes Sp_2(3)$. Similarly, $G$ contains derangements of order 15 if $H$ is of type $GU_4(3)$. Finally, suppose that $H$ is an irreducible subgroup of type $O_7(3)$. To see that $(\star)$ does not hold, we may replace $H$ by a conjugate $H^\tau$, where $\tau \in \text{Aut}(G)$ is an appropriate triality graph automorphism such that $H^\tau$ is the stabilizer in $G$ of a non-degenerate 1-space. For this reducible subgroup, elements with Jordan form $[J_2^J]$ are derangements, and so are elements $y \in G$ of order 5 of the form $y = \hat{y}Z$, where $Z = Z(\Omega^\pm_8(3))$ and $CV(\hat{y})$ is trivial (the eigenvalues of $\hat{y}$ (in $\mathbb{F}_{34}$) are the nontrivial fifth roots of unity, each occurring with multiplicity 2).

For the remainder, we may assume that $q \geq 4$. Let $x \in G$ be an element of order $(q^3 + 1)/(2, q - 1)$, fixing an orthogonal decomposition $8 = 6^- \perp 2^-$. Then $|x|$ is not a prime power, and $x$ is a derangement unless $H$ is of type $N^-_5$ or $GU_4(q)$ (see [28, p. 767]). In both of these cases, elements of order $\ell_3(q)$ are derangements. Similarly, if $q$ is odd then unipotent elements with Jordan form $[J_7^J, J_1^J]$ are also derangements. Finally, if $q$ is even and $H$ is of type $N^-_5$ (respectively, $GU_4(q)$) then unipotent elements with Jordan form $[J_7^J]$ (respectively, $[J_2^J, J_1^J]$; $c_2$-involutions in the terminology of [1]) are derangements. The result follows. $\square$

**Lemma 4.15.** Theorem 2 holds if $G_0 = \Omega^-_8(q)$. 

Proof. Again, we may assume that $G = G_0$. If $q \leqslant 3$ then we can use GAP to verify the result, so let us assume that $q \geqslant 4$. The maximal subgroups of $G$ are listed in [5, Tables 8.52 and 8.53]. By considering elements of order $\ell_8(q)$ and $\ell_6(q)$, we can eliminate subfield subgroups, together with the reducible subgroups of type $P_2$, $P_3$, $N_2^-$, $N_3$ and $N_4^+$. Similarly, elements of order $\ell_8(q)$ and $\ell_4(q)$ are derangements if $H$ is a non-geometric subgroup of type $L_3^-(q)$. Therefore, to complete the proof, we may assume that $H$ is either a field extension subgroup of type $O_4^-(q^2)$, or a reducible subgroup of type $P_1$, $N_2^+$, $O_7(q)$ ($q$ odd) or $Sp_6(q)$ ($q$ even).

If $H$ is of type $O_4^-(q^2)$, then elements of order $\ell_6(q)$ are derangements, as well as unipotent elements with Jordan form $[J_2, J_1]$ if $q$ is odd, and unipotent elements with Jordan form $[J_2^2, J_1^4]$ ($a_2$-type involutions) if $q$ is even. Similarly, if $H = P_1$ or $N_2^+$ then elements of order $\ell_8(q)$ and $\ell_3(q)$ are derangements (note that an element of order $\ell_3(q)$ fixes a $2^-$-space, but not a $2^+$-space). Finally, suppose $H$ is of type $O_7(q)$ ($q$ odd) or $Sp_6(q)$ ($q$ even). In both cases, elements of order $\ell_8(q)$ are derangements. In addition, there are derangements with Jordan form $[J_5, J_3]$ ($q$ odd) and $[J_2^2]$ ($q$ even).

\[ \square \]

Lemma 4.16. Theorem 2 holds if $G_0 = P\Omega_n^+(q)$.

Proof. We may assume that $G = G_0$ and $n \geqslant 9$. We have three cases to consider.

Case 1 $G_0 = P\Omega_n^+(q)$ and $n \geqslant 10$.

Write $n = 2m$ and first assume that $m$ is odd. Let $x \in G$ be an element of order $(q^{(m-1)/2} + 1)/(q^{(m+1)/2} + 1)/(4, q - 1)$, fixing an orthogonal decomposition of the form $(m + 1)^- \perp (m - 1)^-$. Then Lemma 2.7 implies that $|x|$ is not a prime power, so by [7, Proposition 5.13] we may assume that $H = N^I_{m-1}$. In this situation, elements of order $\ell_{n-2}(q)$ are derangements, and so are unipotent elements with Jordan form $[J_{n-1}, J_1]$ ($q$ odd) or $[J_{n-2}, J_2]$ ($q$ even).

A similar argument applies if $m$ is even. Here we take an element $x \in G$ of order $(q^{(m-2)/2} + 1)/(q^{(m+2)/2} + 1)/(4, q - 1)$, fixing a decomposition $(m + 2)^- \perp (m - 2)^-$. Then $|x|$ is not a prime power, and [7, Proposition 5.14] implies that $x$ is a derangement unless $H$ is of type $N^-_{m-2}$ or $O_{n/2}^+(q^2)$. In the former case, we complete the argument as above, so let us assume that $H$ is of type $O_{n/2}^+(q^2)$. Any element of order $\ell_{n-2}(q)$ is a derangement, and so are unipotent elements with Jordan form $[J_{n-1}, J_1]$ if $q$ is odd. Finally, if $q$ is even then $a_2$-type involutions are derangements.

Case 2 $G_0 = P\Omega_n^-(q)$ and $n \geqslant 10$.

Again, write $n = 2m$. First assume that $m \geqslant 11$. Let $x \in G$ be an element of order

$$\text{lcm}(q^{m-5} + 1, q^3 + 1, q^2 + 1)/(2, q - 1)$$

fixing a decomposition $(n - 10)^- \perp 6^- \perp 4^-$. Then $|x|$ is not a prime power, and [7, Proposition 5.16] implies that $x$ is a derangement unless $H$ is of type $N_5^+$, $N_6^-$ or $N_{10}^+$. In each of these cases, it is clear that elements of order $\ell_n(q)$ and $\ell_{n-2}(q)$ are derangements.

Next suppose that $m \in \{5, 6, 7, 9, 10\}$. Let $x \in G$ be an irreducible element of order $(q^m + 1)/(2, q - 1)$. We claim that $|x|$ is not a prime power (here we
Derangements of prime power order

require \( m \neq 8 \). If \( q \) is even, this follows immediately from Lemma 2.6, so let us assume that \( q \) is odd. Suppose \( m = 5 \) and \( q^5 + 1 = 2r^e \) for some prime \( r \) and positive integer \( e \). Then \((q + 1)(q^4 - q^3 + q^2 - q + 1) = 2r^e \) and \( r = \ell_{10}(q) \). Therefore, \( q + 1 = 2 \) is the only possibility, which is absurd. Similarly, if \( m = 6 \) and \( q^6 + 1 = (q^2 + 1)(q^4 - q^2 + 1) = 2r^e \), then \( r = \ell_{12}(q) \) and \( q^2 + 1 = 2 \), which is not possible. The other cases are entirely similar. Now, by the main theorem of [3], \( x \) is a derangement unless \( H \) is a field extension subgroup of type \( O_{n/k}(q^k) \) (\( k \) a prime divisor of \( n \), \( n/k \geq 4 \) even) or \( \text{GU}_{n/2}(q) \) (\( n/2 \) odd). In both cases, elements of order \( \ell_{n-2}(q) \) are derangements. In addition, there are unipotent derangements; take \([J_{n-1}, J_1]\) if \( q \) is odd, an \( a_2 \)-involution if \( q \) is even and \( H \) is of type \( O_{n/k}(q^k) \), and a \( c_2 \)-involution if \( q \) is even and \( H \) is of type \( \text{GU}_{n/2}(q) \).

Finally, let us assume that \( m = 8 \). As in [28, Table II], let \( x \in G \) be an element of order \( \text{lcm}(q^5 + 1, q^2 + 1, q + 1)/(2, q - 1) \), fixing an orthogonal decomposition of the form \( 10^- \perp 4^- \perp 2^- \). Note that \(|x|\) is divisible by \( \ell_{10}(q) \) and \( \ell_4(q) \), so it is not a prime power. As indicated in [28, Table II], \( x \) is a derangement unless \( H \) is of type \( N_7^\pm, N_4^\pm \) or \( N_6^0 \). In each of these cases, elements of order \( \ell_{16}(q) \) and \( \ell_{14}(q) \) are derangements.

**Case 3** \( G_0 = \text{S}_n(q) \) and \( n \geq 9 \) is odd.

Write \( n = 2m + 1 \) and note that \( q \) is odd. First assume \( m \) is odd. Let \( x \in G \) be an element of order

\[
\text{lcm}(q^{(m+1)/2} + 1, q^{(m-1)/2} + 1)/2 = (q^{(m+1)/2} + 1)(q^{(m-1)/2} + 1)/4,
\]

fixing an orthogonal decomposition \((m + 1)^- \perp (m - 1)^- \perp 1\). Note that \(|x|\) is divisible by \( \ell_{m+1}(q) \) and \( \ell_{m-1}(q) \), so \(|x|\) is not a prime power. Let \( H \) be a maximal subgroup of \( G \) containing \( x \). By carefully applying the main theorem of [32], we deduce that \( H \in \{N_{m+1}^-, N_{m-1}^-, N_{2m}^+\} \). For example, the order of \( x \) rules out subfield subgroups and imprimitive subgroups of type \( O_1(q) \rtimes S_n \) (see [7, Remark 5.1(i)]), and the dimensions of the irreducible constituents of \( x \) are incompatible with field extension subgroups of type \( O_{n/k}(q^k) \). Now, if \( H \) is one of these reducible subgroups, then elements of order \( \ell_{n-1}(q) \) and \( \ell_{n-3}(q) \) are derangements. The result follows.

A similar argument applies if \( m \) is even. Here we take \( x \in G \) to be an element of order

\[
\text{lcm}(q^{(m+2)/2} + 1, q^{(m-2)/2} + 1)/2 = (q^{(m+2)/2} + 1)(q^{(m-2)/2} + 1)/4,
\]

fixing a decomposition \((m + 2)^- \perp (m - 2)^- \perp 1\). We claim that \(|x|\) is not a prime power. This is clear if \( m \geq 6 \), or if \( m = 4 \) and \( q \) is not a Mersenne prime, since \(|x|\) is divisible by \( \ell_{m \pm 2}(q) \). Suppose that \( m = 4 \) and \( q \) is a Mersenne prime. If \( q = 3 \) then \(|x| = 28 \) and the claim holds, and if \( q > 3 \) then \(|x|\) is divisible by \( 2 \) and \( \ell_6(q) \). This justifies the claim. Using [32] one can check that the only maximal subgroups of \( G \) containing \( x \) are of type \( N_{m+2}^-, N_{m-2}^- \) or \( N_{2m}^+ \), so we may assume that \( H \) is one of these subgroups. Here we observe that elements of order \( \ell_{n-1}(q) \) are derangements, and so are unipotent elements with Jordan form \([J_n]\).

\[\Box\]

This completes the proof of Theorem 2.
5. Affine groups

Let $G$ be a finite primitive permutation group. By Theorem 1, if $(\ast)$ holds then $G$ is either almost simple or affine. In the previous section, we determined all the almost simple examples, and we now turn our attention to the affine groups with property $(\ast)$. Our main aim is to prove Theorem 4.

Let $G = HV \leq AGL(V)$ be a finite affine primitive permutation group with point stabilizer $H = G_0$ and socle $V = (\mathbb{Z}_p)^k$. As an abstract group, $G$ is a semidirect product of $V$ by $H$. Therefore, we will begin our analysis by studying the structure of a general semidirect product $G = H \rtimes N$ with property $(\ast)$, so $G$ is a finite group, $H$ is a proper subgroup and $N$ is a normal subgroup of $G$ such that $G = HN$ and $H \cap N = 1$.

We will need some additional notation. If $K$ is a subgroup of $G$ and $g \in G$, then we set

$$[K, g] = \{[k, g] = k^{-1}g^{-1}kg : k \in K\}.$$ 

We also write $K^*$ for the set of all nontrivial elements of $K$.

**Lemma 5.1.** Let $G = H \rtimes N$. The following hold:

(i) $C_G(x) = C_H(x)C_N(x)$ for all $x \in H$.
(ii) If $K \leq H$, then $K \cap K^n = C_K(n)$ for all $n \in N^*$.
(iii) If $N$ is abelian, then $\Delta_H(G) = \{tv : t \in H, v \in N \setminus [N, t]\}$.
(iv) If property $(\ast)$ holds, then $N$ is an $r$-group.

**Proof.** First consider part (i). The result is clear if $x = 1$, so assume that $x \in H^*$. The inclusion $C_H(x)C_N(x) \subseteq C_G(x)$ is clear. Conversely, suppose that $g = hn \in C_G(x)$ where $h \in H$, $n \in N$. Then $hnx = xhn$. Multiplying both sides by $(xh)^{-1} = h^{-1}x^{-1}$, we obtain

$$hnxh^{-1}x^{-1} = (xh)n(xh)^{-1}$$

which implies that

$$(hn^{-1})(xhx^{-1}) = (xh)n(xh)^{-1}.$$ 

Since $n \in N \trianglelefteq G$ and $h, x \in H$, we deduce that

$$hnxh^{-1}x^{-1} = (hn^{-1}h^{-1})(xh)n(xh)^{-1} \in H \cap N = 1$$

so $h \in C_H(x)$. Since $hnx = xhn = hxn$, we deduce that $nx = xn$ and thus $n \in C_N(x)$. Therefore, $g = hn \in C_H(x)C_N(x)$ and part (i) follows.

For part (ii), let $K \leq H$ and let $n \in N^*$. Assume that $y \in K \cap K^n$. Then $y = kn$ for some $k \in K$, so

$$k^{-1}y = k^{-1}n^{-1}kn = (k^{-1}n^{-1}k)n \in K \cap N = 1,$$

which implies that $kn = nk$ and $y = k$, or equivalently $y \in C_K(n)$. Therefore, $K \cap K^n \subseteq C_K(n)$. Conversely, if $y \in C_K(n)$ then $y \in K$ and $y = n^{-1}yn \in K^n$, so $y \in K \cap K^n$ and thus $C_K(n) \subseteq K \cap K^n$. The result follows.
Now consider part (iii). Assume that $N$ is abelian. Set
\[ \Gamma := \{ t v : t \in H, v \in N \setminus \{ N, t \} \}. \]

First we claim that $\Gamma \subseteq \Delta_H(G)$. Let $g \in \Gamma$, say $g = hn$ with $h \in H$ and $n \in N \setminus \{ N, h \}$. Seeking a contradiction, suppose that $g \notin \Delta_H(G)$. Then $g \in H^t$ for some $t \in G$. Since $t \in G = HN$, we may write $t = h_1m_1$ with $h_1 \in H$ and $m_1 \in N$. It follows that $g \in H^t = H^{m_1}$, so $m_1g^{-1}m_1 \in H$. Let $m := m_1^{-1} \in N$. Then $m^{-1}gm = m^{-1}hnm = hnm \in H$ (note that $nm = mn$ since $N$ is abelian) and thus $h^{-1}hnm = [h, m]n \in H$. We also have $[h, m]n = (h^{-1}m^{-1}h)mn \in N$, so $[h, m]n \in H \cap N = 1$ and we deduce that $n = [m, h] \in [N, h]$, contradicting our choice of $n$. We have now shown that $\Gamma \subseteq \Delta_H(G)$. Conversely, suppose that $g = hn \in \Delta_H(G)$ with $h \in H$, $n \in N$. We claim that $n \in N \setminus \{ N, h \}$. Seeking a contradiction, suppose that $n \in [N, h]$, say $n = [m, h]$ for some $m \in N$. Then $m^{-1}(hn)m = h$, or equivalently $g^m \in H$, which is a contradiction.

Finally, let us turn to part (iv). If $x \in N^*$ then $x^G \subseteq N$, so $x^G \cap H \subseteq N \cap H = 1$ and thus $x^G \cap H = \emptyset$ since $x \neq 1$. Therefore $N^* \subseteq \Delta_H(G)$. In particular, if every element of $\Delta_H(G)$ is an $r$-element (for some fixed prime $r$), then every element of $N$ is also an $r$-element and thus $N$ is an $r$-group. \hfill $\square$

**Lemma 5.2.** Let $G = H \ltimes N$, where $N$ is an $r$-group for some prime $r$. Then the following are equivalent:

(i) Property $(\star)$ holds.

(ii) $C_H(n) = H \cap H^n$ is an $r$-group for all $n \in N^*$.

(iii) $C_N(x) = 1$ for every nontrivial $r'$-element $x \in H$. In other words, every nontrivial $r'$-element of $H$ induces a fixed-point-free automorphism of $N$ via conjugation.

**Proof.** First we will show that (i) implies (ii). Suppose that $(\star)$ holds. Let $n \in N^*$. We claim that $C_H(n) = H \cap H^n$ by Lemma 5.1(ii). Seeking a contradiction, suppose that $|C_H(n)|$ is divisible by a prime $s \neq r$. Choose $y \in C_H(n)$ with $|y| = s$ and let $g := ny = yn \in G$. We claim that $g \in \Delta_H(G)$, which would be a contradiction since $|g| = |n|s$ is not a power of $r$. Assume that $g \notin \Delta_H(G)$, so $g \in H^t$ for some $t \in G$. Since $G = HN$, we may assume that $t \in N$. Then
\[ g^s = (ny)^t = n^s y^s = n^s \in H^t \]
and $n^s \in N \trianglelefteq G$, so $t(n^s)t^{-1} \in H \cap N = 1$ and thus $n^s = 1$, which is not possible since $n$ is a nontrivial $r$-element. Therefore, $g = ny \in \Delta_H(G)$ as required.

Next we will show that (ii) implies (i). Suppose that $C_H(n)$ is an $r$-group for all $n \in N^*$. Let $g \in \Delta_H(G)$, say $g = hn$ with $h \in H$ and $n \in N^*$. We claim that $g$ is an $r$-element. Seeking a contradiction, suppose that $m := |g|$ is divisible by a prime $s \neq r$. Set $x := g^{m/s} \in G$ and let $S$ be a Sylow $s$-subgroup of $H$. Then $|x| = s$ and $S$ is also a Sylow $s$-subgroup of $G$ since $|G : H| = |N|$ is coprime to $s$. By Sylow’s theorem, $x^t \in S \leq H$ for some $t \in G$. Since $g^G \subseteq \Delta_H(G)$, replacing $g$ by $g^t$ we may assume that $x \in H$. Then $g \in C_G(x) = C_H(x)C_N(x)$ by Lemma 5.1(i).
Suppose that $C_N(x) \neq 1$, say $1 \neq n \in C_N(x)$. Then $x \in C_H(n)$, but this is a contradiction since $|x| = s$ and we are assuming that $C_H(n)$ is an $r$-group. Therefore, $C_N(x) = 1$ and thus $C_G(x) = C_H(x)$. Hence $g \in C_H(x) \leq H$, which contradicts the fact that $g \in \Delta_H(G)$. This final contradiction shows that $g$ is an $r$-element, so $(\ast)$ holds.

Now let us show that (ii) implies (iii). Suppose that $C_H(n)$ is an $r$-group for all $n \in N^*$. Let $x \in H^*$ be an $r'$-element. We claim that $C_V(x) = 1$. Seeking a contradiction, suppose that $1 \neq n \in C_N(x)$. Then $x \in C_H(n)$, so $|C_H(n)|$ is divisible by $|x|$, which is not an $r$-power. This contradicts the assumption that $C_H(n)$ is an $r$-group.

To complete the proof, it remains to show that (iii) implies (ii). Suppose that $C_N(x) = 1$ for every nontrivial $r'$-element $x \in H$. Let $n \in N^*$. If $C_H(n)$ is not an $r$-group, then there exists an element $x \in C_H(n)$ with $|x| = s$, where $s \neq r$ is a prime. Therefore, $1 \neq n \in C_N(x)$, which is not possible since $C_N(x) = 1$. \hfill $\square$

We are now in a position to prove Theorem 4.

**Proof of Theorem 4.** Let $G = HV \leq AGL(V)$ be a finite affine primitive permutation group with point stabilizer $H = G_0$ and socle $V = (\mathbb{Z}_p)^k$, where $p$ is a prime and $k \geq 1$. If property $(\ast)$ holds, then $r = p$ and Lemma 5.2 implies that no nontrivial $r'$-element of $H$ has fixed points on $V \setminus \{0\}$. Therefore, the pair $(H, V)$ is $r'$-semiregular in the sense of [19]. Conversely, if $r = p$ and $(H, V)$ is $r'$-semiregular, then $C_V(x) = 0$ for every nontrivial $r'$-element $x \in H$, so Lemma 5.2 implies that $G$ has property $(\ast)$. \hfill $\square$

**Remark 5.3.** Note that the equivalence of (i) and (ii) in Lemma 5.2 implies that an affine group $G = HV \leq AGL(V)$ has property $(\ast)$ if and only if every two-point stabilizer in $G$ is an $r$-group.

If $G = HV \leq AGL(V)$ is an affine group (with $V = (\mathbb{Z}_r)^k$ and $r \not\in \pi(H)$, then $G$ is a Frobenius group and property $(\ast)$ clearly holds. Therefore, we may focus on the case where $r \in \pi(H)$. As noted in the Introduction, detailed information on $r'$-semiregular pairs $(H, V)$ was initially obtained by Guralnick and Wiegand in [33, Section 4], where this notion arises naturally in their study of the multiplicative structure of field extensions. Similar results were established in later work by Fleischmann et al. [19]. In both papers, the main aim is to determine the structure of $H$. For solvable affine groups, we have the following result (in the statement, $O_r(Y)$ denotes the largest normal $r'$-subgroup of $Y$):

**Proposition 5.4.** Let $G = HV \leq AGL(V)$ be a finite affine primitive permutation group with point stabilizer $H = G_0$ and socle $V = (\mathbb{Z}_r)^k$. Assume that $H$ is solvable and $r \in \pi(H)$. Then $G$ has property $(\ast)$ only if $H \cong X \times Y$ or $(X \times Y):2$, where $X \in \{1, SL_2(3)\}$, $Y = O_r(Y)R$ and $R$ is a Sylow $r'$-subgroup of $Y$.

**Proof.** This follows from [19, Theorem 2.1]. \hfill $\square$

The main result for a perfect group $H$ is Proposition 5.5 below (see [19, Theorem 4.1]; also see [33, Theorem 4.2]). In part (iv), $S = \{5, 13, 37, 73, \ldots\}$ is the set of all primes $s$ satisfying the following conditions:
Derangements of prime power order

(a) \( s = 2^a 3^b + 1 \), where \( a \geq 2 \) and \( b \geq 0 \);
(b) \( (s+1)/2 \) is a prime.

It is not known whether or not \( S \) is finite.

**Proposition 5.5.** Let \( G = HV \leq AGL(V) \) be a finite affine primitive permutation group with point stabilizer \( H = G_0 \) and socle \( V = (\mathbb{Z}_r)^k \). Assume that \( H \) is perfect and \( r \in \pi(H) \). Then \( G \) has property (\( \star \)) only if one of the following holds:

(i) \( H \cong SL_2(r^a) \), where \( a \geq 1 \) and \( r^a > 3 \);
(ii) \( H \cong 2B_2(2^{2a+1}) \), \( r = 2 \) and \( a \geq 1 \);
(iii) \( H \cong 2B_2(2^{2a+1}) \times SL_2(2^{2b+1}) \), \( r = 2 \) and \( a, b \geq 1 \) such that \( (2a+1, 2b+1) = 1 \);
(iv) \( H \cong SL_2(s) \), \( r = 3 \) and \( s \in S \cup \{7, 17\} \).

For instance, \( H = SL_2(7) \) has a 12-dimensional faithful, irreducible module \( V \) over \( \mathbb{F}_3 \), and the corresponding affine group \( G = HV \) has property (\( \star \)) (with \( E(G) = \{3, 9\} \)). In the general case, we refer the reader to [19, Theorem 6.1] for a detailed description of the structure of \( H \).

Finally, let us suppose that \( G = HV \leq AGL(V) \) is a finite affine primitive permutation group with property (\( \star \)). Set

\[
E(G) = E_H(G) = \{ |x| : x \in \Delta_H(G) \}.
\]

Can we determine when \( E(G) = \{r\} \)? In order to address this question, let \( P \) be a Sylow \( r \)-subgroup of \( G \). Then \( V \leq P \) since \( V \) is a normal \( r \)-subgroup of \( G \), and we have \( P = (H \cap P)V = KV \) with \( K := H \cap P \). Note that \( P = KV \) is a semidirect product.

**Proposition 5.6.** Let \( G = HV \leq AGL(V) \) be a finite affine primitive permutation group with point stabilizer \( H = G_0 \) and socle \( V = (\mathbb{Z}_r)^k \). Assume that property (\( \star \)) holds. Let \( P \) be a Sylow \( r \)-subgroup of \( G \) and set \( K = H \cap P \). Then the following hold:

(i) \( P = KV \) is a transitive permutation group on \( P/K \).
(ii) \( \Delta(G) = \bigcup_{g \in G} \Delta_K(P)^g \) and \( E(G) = E_K(P) \).

**Proof.** As above, \( P = KV \) is a semidirect product. For part (i), it suffices to show that the core \( L \) of \( K \) in \( P \) is trivial. We have \( L \leq K \leq H \) and \( L \leq P \), so \( [L, V] \leq L \cap V \leq K \cap V = 1 \) and thus \( L \leq C_K(V) \leq C_H(V) = 1 \) (here we are using the fact that \( V \) is a faithful irreducible \( H \)-module). This proves (i).

Now consider part (ii). Clearly, it suffices to show that the first equality holds. By applying Lemma 5.1(iii) we have

\[
\Delta_K(P) = \{tv : t \in K, v \in V \setminus [V, t] \}.
\]

Since \( K \leq H \), a further application of Lemma 5.1(iii) (this time for \( G = HV \)) shows that \( \Delta_K(P) \subseteq \Delta(G) \). As \( \Delta(G) \) is a normal subset of \( G \), it follows that

\[
\bigcup_{g \in G} \Delta_K(P)^g \subseteq \Delta(G).
\]
Since property (⋆) holds, every $g \in \Delta(G)$ is an $r$-element, so some $G$-conjugate of $g$ is in $P$. Without loss of generality, we may assume that $g \in P = KV$. By Lemma 5.1(iii) we have $g = hn$, with $h \in H$ and $n \in V \setminus \{V, h\}$. Moreover, since $V \leq P$ and $g \in P$, we have $h = gn^{-1} \in H \cap P = K$. Therefore, by applying Lemma 5.1(iii) once again, we conclude that $g = hn \in \Delta_K(P)$, so $\Delta(G) = \bigcup_{g \in G} \Delta_K(P)^g$ and the proof is complete.

Now, if we assume that $G = HV$ has property (⋆), then part (ii) of Proposition 5.6 implies that $\mathcal{E}(G) = \{r\}$ if and only if $\mathcal{E}_K(P) = \{r\}$. Clearly, if $P$ has exponent $r$, then $\mathcal{E}_K(P) = \{r\}$. Conversely, if $\mathcal{E}_K(P) = \{r\}$ with $r = 2$ or $3$, then a theorem of Mann and Praeger [43, Proposition 2] implies that $P$ has exponent $r$. In fact, for this specific transitive group $P$ we can show that the same conclusion holds for any prime $r$ (we thank an anonymous referee for pointing this out).

**Theorem 5.7.** Let $G = HV \leq AGL(V)$ be a finite affine primitive permutation group with point stabilizer $H = G_0$ and socle $V = (\mathbb{Z}_p)^k$, where $p$ is a prime and $k \geq 1$. Then every derangement in $G$ has order $r$, for some fixed prime $r$, if and only if $r = p$ and the following two conditions hold:

(i) Every two-point stabilizer in $G$ is an $r$-group;
(ii) A Sylow $r$-subgroup of $G$ has exponent $r$.

**Proof.** Let $P$ be a Sylow $r$-subgroup of $G$. First assume that $r = p$ and (i) and (ii) hold. By (i), the pair $(H, V)$ is $r'$-semiregular so Theorem 4 implies that property (⋆) holds. Therefore, $\mathcal{E}(G) = \mathcal{E}_K(P)$ by Proposition 5.6(ii) (with $K = H \cap P$) and thus condition (ii) implies that $\mathcal{E}(G) = \{r\}$ as required.

Conversely, let us assume that $\mathcal{E}(G) = \{r\}$, so $r = p$ and property (⋆) holds. By Theorem 4, every two-point stabilizer in $G$ is an $r$-group and so it remains to show that $P$ has exponent $r$. Seeking a contradiction, suppose that $\exp(P) \geq r^2$. Note that $r$ divides $|H|$. Let $Q$ be a Sylow $r$-subgroup of $H$. Let $x \in P$ be an element of order $r^2$ and observe that $x$ belongs to a conjugate of $H$ (since $\mathcal{E}(G) = \{r\}$), so $\exp(Q) \geq r^2$. We may assume $x \in H$ and we choose an element $v \in V \setminus \{V, x\}$. Then $xv \in G$ is a derangement by Lemma 5.1(iii), but $|xv| \geq r^2$ so we have reached a contradiction. 

**Acknowledgements.** This work was done while the second author held a position at the CRC 701 within the project C13 ‘The geometry and combinatorics of groups’, and he thanks B. Baumeister and G. Stroth for their assistance. Part of the paper was written during the second author’s visit to the School of Mathematics at the University of Bristol and he thanks the University of Bristol for its hospitality. Burness thanks R. Guralnick for helpful comments. Both authors thank an anonymous referee for suggesting several improvements to the paper, including a simplified proof of Proposition 4.2 and a proof of Theorem 5.7.

**Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.
References

[37] Kantor, W.M., Seress, Á.: Large element orders and the characteristic of Lie-type simple groups. J. Algebra 322, 802–832 (2009)
[44] Nagell, T.: Des équations indéterminées $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$. Norsk. Mat. Forenings Skr. (I) 2, 12–14 (1920)
Derangements of prime power order

[50] van der Waall, R.W.: On the Diophantine equations $x^2 + x + 1 = 3v^2$, $x^3 - 1 = 2y^2$, $x^3 + 1 = 2y^2$. Simon Stevin 46, 39–51 (1972)