ALMOST ELUSIVE PERMUTATION GROUPS

TIMOTHY C. BURNESS AND EMILY V. HALL

Abstract. Let G be a nontrivial transitive permutation group on a finite set Ω. An element of G is said to be a derangement if it has no fixed points on Ω. From the orbit counting lemma, it follows that G contains a derangement, and in fact G contains a derangement of prime power order by a theorem of Fein, Kantor and Schacher. However, there are groups with no derangements of prime order; these are the so-called elusive groups and they have been widely studied in recent years. Extending this notion, we say that G is almost elusive if it contains a unique conjugacy class of derangements of prime order. In this paper we first prove that every quasiprimitive almost elusive group is either almost simple or 2-transitive of affine type. We then classify all the almost elusive groups that are almost simple and primitive with socle an alternating group, a sporadic group, or a rank one group of Lie type.

1. Introduction

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group on a finite set Ω with $|\Omega| \geqslant 2$ and point stabiliser H. By a classical theorem of Jordan [30], which is an easy consequence of the orbit counting lemma, G contains elements that act fixed point freely on Ω. Such an element is called a *derangement* and we note that $x \in G$ has this property if and only if $x^G \cap H$ is empty, where x^G denotes the conjugacy class of x. In particular, the set of derangements is closed under conjugation. Derangements arise naturally in a wide range of contexts and Jordan's theorem turns out to have interesting applications in several different areas (see Serre's article [39], for example).

The existence of derangements leads to a number of natural problems that have been extensively studied by various authors. For example, there is a substantial literature on the proportion of derangements in finite transitive permutation groups. Here one of the main highlights is the sequence of papers [16, 17, 18, 19] by Fulman and Guralnick, which shows that the proportion of derangements in a transitive simple group is bounded from below by an absolute constant (this settles a conjecture of Boston and Shalev from the 1990s).

In this paper, we focus on the existence of derangements with prescribed properties, noting that problems of this flavour have also attracted significant interest in recent years. A landmark result in this direction is established by Fein, Kantor and Schacher in [15]. By applying the Classification of Finite Simple Groups, they prove that every nontrivial finite transitive group contains a derangement of prime power order. Moreover, they also observe that the conclusion does not extend to prime order derangements, in general. For example, the 3-transitive action of the smallest Mathieu group M_{11} on 12 points has no derangements of prime order (but it does contain derangements of order 4 and 8). Indeed, M_{11} has unique conjugacy classes of elements of order 2 and 3, and both primes divide the order of a point stabiliser $\mathrm{L}_2(11)$.

Following [11], we say that a transitive group is *elusive* if it contains no derangements of prime order. These groups have been the subject of several papers in recent years (see [11, 20, 21, 22, 23, 44] for example), but a complete classification remains out of reach. One of the main results towards a classification is a theorem of Giudici [21], which states that if G is an elusive group with a transitive minimal normal subgroup, then there exists

Date: December 7, 2021.

a positive integer k such that $G = \mathrm{M}_{11} \wr A$ in its product action on Δ^k, where $|\Delta| = 12$ and $A \leqslant S_k$ is transitive. In particular, every elusive group with this property is primitive.

Further interest in elusive groups stems from an open problem in algebraic graph theory from the early 1980s. In [35], Marušič conjectures that if Γ is a finite vertex-transitive digraph, then $\mathrm{Aut}(\Gamma)$ contains a derangement of prime order (with respect to the action on vertices). This was later extended by Klin (see [10, Problem 282 (BCC15.12)]), who conjectures that the same conclusion holds for every nontrivial finite transitive 2-closed permutation group (it is easy to see that $\mathrm{Aut}(\Gamma)$ as above is 2-closed, so this is a natural generalisation). This is known as the *Polycirculant Conjecture* and although there has been progress towards a positive solution, both problems remain open (see [6, Section 1.3.4] for further details and references). In particular, none of the known elusive groups are 2-closed.

In this paper, we introduce and study a new family of permutation groups.

Definition. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group. Then G is *almost elusive* if it contains a unique conjugacy class of derangements of prime order.

For example, if $n = p^a$ is a prime power then it is easy to see that the natural action of the symmetric group S_n on n points is almost elusive (every derangement of prime order is a product of n/p disjoint p-cycles, which form a single conjugacy class). In particular, there are infinitely many almost simple primitive groups with this property, which is in stark contrast to the situation for elusive groups, where Giudici's theorem [21] implies that the action of M_{11} on 12 points is the only example. We can also find affine type examples. For instance, if $q = 2^f$ with $f \geqslant 1$ then the natural 2-transitive action of $\mathrm{AGL}_2(q)$ on q^2 points is almost elusive.

Remark 1. As noted above, Jordan's theorem implies that every nontrivial finite transitive group contains at least one conjugacy class of derangements. It turns out that there are groups with a unique conjugacy class of derangements. Indeed, the main theorem of [8] states that a primitive group $G \leqslant \mathrm{Sym}(\Omega)$ with point stabiliser H has a unique class of derangements if and only if G is sharply 2-transitive (that is, any pair of distinct elements in Ω can be mapped to any other such pair by a unique element in G) or $(G, H) = (A_5, D_{10})$ or $(\mathrm{L}_2(8){:}3, D_{18}{:}3)$. Further work by Guralnick [25] shows that the same conclusion holds for all transitive groups. Note that all of these groups are almost elusive.

Remark 2. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a nontrivial finite transitive permutation group with point stabiliser H and let r be a prime divisor of $|\Omega|$. Following [7], we say that G is *r-elusive* if G does not contain a derangement of order r, whence G is elusive if and only if G is r-elusive for every prime divisor r of $|\Omega|$. Similarly, G is almost elusive only if the same conclusion holds for all but one prime r. In particular, note that G is almost elusive only if $|\pi(G) \setminus \pi(H)| \leqslant 1$, where $\pi(X)$ denotes the set of prime divisors of $|X|$. We refer the reader to [5, 6, 7] for results on r-elusive primitive groups.

Recall that a finite permutation group is *quasiprimitive* if every nontrivial normal subgroup is transitive. In [37], Praeger establishes a version of the O'Nan-Scott theorem for quasiprimitive groups, which describes the structure and action of such a group in terms of its socle (recall that the *socle* of a group is the product of its minimal normal subgroups). By applying this important theorem, we can prove the following result.

Theorem 1. *Let G be a finite quasiprimitive almost elusive permutation group. Then either G is almost simple, or G is a 2-transitive affine group.*

Remark 3. It is worth noting that there exist almost elusive quasiprimitive groups that are not primitive (once again, this differs from the situation for elusive groups). For instance, suppose $G = \mathrm{L}_2(q)$ and $q = 2^m - 1$ is a Mersenne prime such that $2^{m-1} - 1$ is divisible by 9. For example, we can take

$$m \in \{7, 13, 19, 31, 61, 127, 607, 1279, 2203, 2281, 3217, 4423, \ldots\}.$$

G_0	G	H	Conditions	x
A_n	S_n	S_{n-1}	$n = r^a$	$[r^{n/r}]$
		$S_{n-2} \times S_2$	$n = 2^m = r + 1$	$[r, 1]$
			$n = 2^m + 1 = r$	$[r]$
	A_n	A_{n-1}	$n = r^a$, $a \geqslant 2$	$[r^{n/r}]$
			$n = 2r^a$, $r \geqslant 3$	$[r^{n/r}]$
A_{10}	A_{10}	$(S_7 \times S_3) \cap G$		$[5^2]$
A_9	S_9, A_9	$(S_7 \times S_2) \cap G$		$[3^3]$
		$(S_6 \times S_3) \cap G$		$[7, 1^2]$
A_6	S_6	$S_3 \wr S_2$		$[5, 1]$
	A_6	$\mathrm{L}_2(5)$		$[3, 1^3]$
	$\mathrm{PGL}_2(9)$	D_{20}		3
	M_{10}	5:4		3
		$3^2{:}Q_8$		5
A_5	A_5	D_{10}		$[3, 1^2]$

TABLE 1. The primitive almost elusive groups with socle A_n, $n \geqslant 5$

Let $H = C_q{:}C_{(q-1)/2}$ be a Borel subgroup of G and set $\Omega = G/K$, where $K = C_q{:}C_{(q-1)/6}$ is a subgroup of H. Then G is quasiprimitive (but not primitive) on Ω and we note that $|\Omega| = 3.2^m$. Moreover, G has unique conjugacy classes of elements of order 2 and 3, and our choice of q implies that $|K|$ is divisible by 3. Therefore, G is almost elusive on Ω. We do not know if there are infinitely many almost elusive quasiprimitive groups that are not primitive.

With the reduction theorem in hand, our ultimate aim is to classify all the almost elusive quasiprimitive groups. In this paper, we take a first step in this direction by establishing Theorem 2 below on almost simple primitive groups (recall that G is *almost simple* if the socle G_0 of G is a nonabelian finite simple group, in which case $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$). In order to state this result, set

$$\mathcal{G} = \mathcal{A} \cup \mathcal{B},$$

where $\mathcal{A}$ is the set of all alternating groups A_n with $n \geqslant 5$, and $\mathcal{B}$ is the set of all sporadic simple groups (including the Tits group ${}^2F_4(2)'$), together with all simple groups of Lie type of the form $\mathrm{L}_2(q)$ (with $q \geqslant 7$ and $q \neq 9$), $\mathrm{U}_3(q)$ (with $q \geqslant 3$), ${}^2G_2(q)$ (with $q \geqslant 27$) and ${}^2B_2(q)$ (with $q \geqslant 8$). Note that $\mathcal{G}$ contains every simple group of Lie type with (twisted) Lie rank equal to 1.

Theorem 2. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite almost simple primitive permutation group with socle $G_0 \in \mathcal{G}$ and point stabiliser H. Then G is almost elusive if and only if (G, H) is one of the cases recorded in Table 1 or 2.*

Remark 4. Some comments on the statement of Theorem 2 are in order.

(a) If G_0 is one of the 26 sporadic simple groups then by combining Theorem 2 with the main result of [21] we deduce that either $(G, H) = (\mathrm{M}_{11}, \mathrm{L}_2(11))$ and G is elusive, or G contains at least two conjugacy classes of derangements of prime order. In particular, G is not almost elusive. Similarly, there are no primitive almost elusive groups with socle ${}^2G_2(q)$ (with $q \geqslant 27$) or ${}^2B_2(q)$.

(b) In the fourth column of Table 1, r denotes a prime number and a is a positive integer. For example, in the second row $r = 2^m - 1$ is a Mersenne prime and thus m is a prime. Similarly, in the next row $r = 2^m + 1$ is a Fermat prime, which implies that m is a 2-power.

G_0	Type of H	G	Conditions	x
$\mathrm{L}_2(q)$	P_1	$\mathrm{PGL}_2(q)$, G_0	$q = p = 2^m - 1$	2
		G_0	$q = p$, $p + 1 = 2.3^a$, $a \geqslant 2$	3
		$G_0.f$	See Remark 4(f)	r
		$G_0.3$, G_0	$q = 8$	3
	$\mathrm{GL}_1(q) \wr S_2$	$\mathrm{PGL}_2(q)$	$q = p = 2^m - 1$	p
		$G_0.3$, G_0	$q = 8$	3
	$\mathrm{GL}_1(q^2)$	$\mathrm{PGL}_2(q)$	$q = p = 2^m + 1$	p
		$G_0.3$	$q = 8$	7
$\mathrm{U}_3(q)$	P_1	$G_0.2$	$q = 3$	7
	$\mathrm{GU}_2(q) \times \mathrm{GU}_1(q)$	$G_0.4$	$q = 4$	13
		$G_0.6$	$q = 8$	19
	$\mathrm{GU}_1(q) \wr S_3$	$G_0.4$	$q = 4$	13
	$\mathrm{L}_2(7)$	$G_0.2$, G_0	$q = 3$	$[J_2, J_1]$
${}^2F_4(2)'$	$\mathrm{L}_2(25)$	$G_0.2$, G_0		2A
	$5^2{:}4A_4$	$G_0.2$		13

TABLE 2. The primitive almost elusive groups with socle $G_0 \in \mathcal{B}$

(c) In the final column of Table 1 we record a representative x of the unique conjugacy class in G of derangements of prime order; in the cases where $G = S_n$ or A_n, we give the cycle-shape of x in the form $[r^d, 1^{n-dr}]$, which means that x is a product of d disjoint r-cycles in its natural action on $\{1, \ldots, n\}$. For the cases with $G = \mathrm{PGL}_2(9)$, we use 3 to denote a representative in the unique conjugacy class of elements of order 3 in G. Similarly, we write 5 for the unique class of elements of order 5 in M_{10}.

(d) In Table 2 we list all the primitive almost elusive groups with socle $G_0 \in \mathcal{B}$. Note that the conditions on q in the definition of $\mathcal{B}$ are justified in view of the isomorphisms

$$\mathrm{L}_2(4) \cong \mathrm{L}_2(5) \cong A_5, \ \ \mathrm{L}_2(9) \cong A_6, \ \ {}^2G_2(3)' \cong \mathrm{L}_2(8),$$

together with the fact that the groups $\mathrm{L}_2(2)$, $\mathrm{L}_2(3)$, $\mathrm{U}_3(2)$ and ${}^2B_2(2)$ are soluble.

(e) In the second column of Table 2 we record the *type* of H. If G_0 is a classical group with natural module V, then this gives an approximate description of the structure of $H \cap \mathrm{PGL}(V)$ (our usage is consistent with [32, p.58]). Note that P_1 denotes a parabolic subgroup, which is the stabiliser in G of a 1-dimensional totally isotropic subspace of V. For the cases with $G_0 = {}^2F_4(2)'$, the type of H coincides with the structure of $H \cap G_0$.

(f) Consider the case recorded in the third row of Table 2. First note that there are two groups of the form $G_0.f$, namely $G_0.\langle\phi\rangle$ and $G_0.\langle\delta\phi\rangle$, where ϕ is a field automorphism of order f and δ is a diagonal automorphism. In addition we require $q = 2r^a - 1$, where $r = 2^m + 1$ is a Fermat prime, $m \geqslant 2$ is a 2-power, a is a positive integer and $f = 2^{m-1}$. See Remark 4.6 for further comments on the number-theoretic conditions arising in the second and third rows of Table 2.

(g) In the final column of Table 2 we describe the unique conjugacy class of derangements of prime order in G. If $G_0 = \mathrm{U}_3(3)$ with H of type $\mathrm{L}_2(7)$, then G_0 contains two G-classes of elements of order 3; as indicated in the table, the derangements have Jordan form $[J_2, J_1]$ on V, where J_i denotes a standard unipotent Jordan block of size i. Similarly, if $G_0 = {}^2F_4(2)'$ and H is of type $\mathrm{L}_2(25)$, then G_0 has two G-classes of involutions, labelled 2A and 2B with $|\mathtt{2A}| = 1755$ and $|\mathtt{2B}| = 11700$; the derangements are in 2A. In each of the remaining cases, we use a prime ℓ to

describe the unique class of derangements of prime order; in every case, this is the unique G-class of elements of order ℓ in G_0. In the first row, for instance, $\mathrm{PGL}_2(q)$ has two classes of involutions, with representatives labelled t_1 and t_1' in [24, Table 4.5.1]; since $q \equiv 3 \pmod 4$, the involutions of type t_1' are contained in G_0 and they are the only derangements of prime order in G.

The analysis of the primitive almost elusive permutation groups initiated in this paper has recently been extended in [27], where the almost simple classical groups are handled. A classification of the almost elusive primitive groups will be presented in [28], which will play a key role in completing the full classification in the more general quasiprimitive setting.

Notation. The notation we adopt in this paper is all fairly standard. Let A and B be groups and let n be a positive integer. We write C_n, or just n, for a cyclic group of order n and A^n is the direct product of n copies of A. An unspecified extension of A by B will be denoted by $A.B$ and we use $A{:}B$ if the extension splits. We adopt the standard notation for simple groups from [32]. For positive integers a and b, we write (a, b) for the greatest common divisor of a and b.

Acknowledgments. Both authors thank Tim Dokchitser and Michael Giudici for helpful conversations concerning the content of this paper. EVH also acknowledges the financial support of the Heilbronn Institute for Mathematical Research.

2. A reduction theorem

In this section we prove Theorem 1. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite quasiprimitive almost elusive group with point stabiliser H and socle N. By [37, Theorem 1] we have $N = T_1 \times \cdots \times T_k$, where $k \geqslant 1$ and each T_i is isomorphic to a fixed simple group T. Note that $G = NH$ since N is transitive. Let $\pi_i : N \to T_i$, $i = 1, \ldots, k$, be the natural projection maps.

First assume N is abelian, so $N = (C_p)^k$ for some prime p. Here N is regular and [37, Theorem 1] implies that G is an affine group. Moreover, each nontrivial element in N is a derangement, so the almost elusivity of G implies that H acts transitively on these elements and thus G is 2-transitive.

For the remainder, we may assume N is non-abelian. If $k = 1$ then G is almost simple, so we may assume $k \geqslant 2$. Let J be a minimal normal subgroup of G and note that $N = J \times C_G(J)$ (see the proof of [37, Theorem 1]). If $C_G(J) \neq 1$ then both J and $C_G(J)$ are regular on Ω and thus every nontrivial element in J is a derangement. But $|T|$ is divisible by at least three distinct primes, which implies that G contains at least three conjugacy classes of derangements of prime order. This is a contradiction. Therefore, $C_G(J) = 1$ and $N = J$ is a minimal normal subgroup. In particular, H acts transitively on the set $\{T_1, \ldots, T_k\}$ and it follows that there exists a subgroup $R \leqslant T$ such that $\pi_i(H \cap N) \cong R$ for all i. We now consider two separate cases.

First assume $R = T$. Here $H \cap N = D_1 \times \cdots \times D_l \cong T^l$, where each

$$D_i = \{(x, x^{\varphi_{i,1}}, \ldots, x^{\varphi_{i,m-1}}) : x \in T\} \cong T$$

is a full diagonal subgroup of $\prod_{j \in I_i} T_j$ and the I_i partition $\{1, \ldots, k\}$ (here each $\varphi_{i,j}$ is an automorphism of T). Note that $k = lm$ and $m \geqslant 2$. Clearly, we have $T_1 \cap H = 1$, so each nontrivial element in T_1 is a derangement on Ω and as above we deduce that G contains at least three conjugacy classes of derangements of prime order. Once again, this is a contradiction.

Finally, let us assume $R < T$. Here we are in Case 2(b) in the proof of [37, Theorem 1] and it follows that $G \leqslant L \wr S_k$ in its natural product action on $\Delta = \Gamma^k$, where $L \leqslant \mathrm{Sym}(\Gamma)$ is a quasiprimitive almost simple group with socle T and point stabiliser U (note that

T acts transitively on Γ since L is quasiprimitive). In particular, G is a group of type III(b)(i) in the notation of [37, Section 2], which means that the following hold:

(a) $N = T^k$ is the unique minimal normal subgroup of G.

(b) Δ is a G-invariant partition of Ω.

(c) Fix $\gamma \in \Gamma$ and $\delta = (\gamma, \ldots, \gamma) \in \Delta$. If $\alpha \in \Omega$ is contained in the part $\delta \in \Delta$, then $N_\delta = (T_\gamma)^k$ and N_α is a subdirect product of S^k for some nontrivial normal subgroup S of T_γ.

In particular, there exist $\alpha \in \Omega$ and $\gamma \in \Gamma$ such that

$$N_\alpha \leqslant (T_\gamma)^k < T^k = N.$$

If $z \in T$ is a derangement of prime order with respect to the action of T on Γ, then the elements $(z, 1, \ldots, 1)$ and $(z, z, 1, \ldots, 1)$ in N are derangements of prime order on Ω. Moreover, these elements are not G-conjugate and thus G is not almost elusive.

Therefore, to complete the proof, we may assume that T is elusive on Γ. By applying [21, Theorem 1.4] we see that $L = T = \mathrm{M}_{11}$ and $U = \mathrm{L}_2(11)$. Since U is simple, property (c) above implies that N_α is a subdirect product of U^k. If $N_\alpha = U^k$ then N is elusive and by arguing as in the proof of [21, Theorem 1.1] we deduce that $G = \mathrm{M}_{11} \wr A$ for some transitive subgroup $A \leqslant S_k$. But then G is elusive and we have reached a contradiction. Finally, suppose $N_\alpha < U^k = U_1 \times \cdots \times U_k$ and write $N_\alpha = F_1 \times \cdots \times F_c$, where each $F_i \cong U$ is a full diagonal subgroup of $\prod_{j \in I_i} U_j$ and the I_i partition $\{1, \ldots, k\}$. Then by arguing as above (the case $R = T$) we deduce that G contains at least three classes of derangements of prime order. This final contradiction completes the proof of Theorem 1.

3. Symmetric and alternating groups

In this section, we begin the proof of Theorem 2 by considering the almost simple groups with socle an alternating group. Our main result is the following.

Theorem 3.1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be an almost simple primitive permutation group with socle $G_0 = A_n$ and point stabiliser H. Then G is almost elusive if and only if (G, H) is one of the cases recorded in Table 1.*

It is straightforward to handle the cases with $n \leqslant 10$.

Proposition 3.2. *The conclusion to Theorem 3.1 holds if $n \leqslant 10$.*

Proof. This is an entirely straightforward Magma [2] calculation. In each case, we use the functions `MaximalSubgroups` and `CosetAction` to construct G as a permutation group on the set of cosets of H. Then by taking a set of conjugacy class representatives in G, we can read off the derangements of prime order and verify the result. □

For the remainder, we may assume $G = S_n$ or A_n with $n \geqslant 11$. We will divide the rest of the proof into three parts, according to the action of H on $\{1, \ldots, n\}$. We denote the cycle-shape of an element $g \in S_n$ of prime order r by writing $[r^d, 1^{n-dr}]$, where d is the number of r-cycles in the cycle decomposition of g.

3.1. **Intransitive subgroups.** We start by assuming H acts intransitively on $\{1, \ldots, n\}$. Therefore $H = (S_k \times S_{n-k}) \cap G$ and we may identify Ω with the set of k-element subsets (k-sets for short) of $\{1, \ldots, n\}$ for some k in the range $1 \leqslant k < n/2$.

We will need some number-theoretic preliminaries on the prime factors of $|\Omega| = \binom{n}{k}$.

Lemma 3.3. *If $|\Omega|$ is divisible by a prime power p^a, then $p^a \leqslant n$.*

Proof. See [13, Lemma, p.1084]. □

Lemma 3.4. *Write $|\Omega| = UV$, where $U = p_1^{a_1} \cdots p_l^{a_l}$, $V = q_1^{b_1} \cdots q_m^{b_m}$ and p_i, q_j are distinct primes such that $p_i < k$ and $q_i \geqslant k$ for all i. Then either*

(i) $U \leqslant V$; *or*

(ii) $(n,k) = (8,3),(9,4),(10,5),(12,5),(21,7),(21,8),(30,7),(33,13),(33,14),(36,13),(36,17)$ *or* $(56,13)$.

Proof. This is [14, Theorem, p.258]. □

Lemma 3.5. *Suppose $n \geqslant 12$ and k is a prime such that $5 \leqslant k < \frac{n}{2}$. Then $\binom{n}{k} > n^4$ if $k \geqslant 11$, or if $k = 7$ and $n \geqslant 24$, or $k = 5$ and $n \geqslant 130$.*

Proof. This is an easy exercise and we omit the details. □

A classical theorem of Sylvester and Schur (see [14, p.258]) states that $|\Omega|$ is divisible by a prime $r > k$. For $k \geqslant 4$, we can now establish the following extension.

Proposition 3.6. *For $k \geqslant 4$, either $|\Omega|$ is divisible by distinct primes $r, s > k$, or $(n,k) = (12,5),(9,4)$.*

Proof. Write $|\Omega| = UV$ as in the statement of Lemma 3.4. Our aim is to show that V has at least two distinct prime divisors q_1 and q_2 that are not equal to k. This is clear if $m \geqslant 3$. Let us also note that the cases arising in part (ii) of the lemma can be checked using Magma; the only exceptions are $\binom{12}{5}$ and $\binom{9}{4}$. For the remainder, we may assume $U \leqslant V$ and $m \leqslant 2$.

First assume $m = 1$, so $V = q_1^{b_1}$. By Lemma 3.3 we have $V \leqslant n$ and thus $|\Omega| = UV \leqslant V^2 \leqslant n^2$. But this is a contradiction since $|\Omega| > n^2$ for $n \geqslant 9$.

Now assume $m = 2$, so $V = q_1^{b_1} q_2^{b_2}$. Clearly, if k is composite then $q_1, q_2 \neq k$ and the result follows. Similarly, if k is a prime and k does not divide $|\Omega|$, then $q_1, q_2 \neq k$ and we are done. Finally, suppose k is a prime divisor of $|\Omega|$. Set $q_1 = k$, so $V = k^{b_1} q_2^{b_2}$ and $q_2 > k$. By Lemma 3.3 we have $k^{b_1}, q_2^{b_2} \leqslant n$ and so $V \leqslant n^2$. Since $U \leqslant V$ we have $|\Omega| \leqslant n^4$ and thus Lemma 3.5 implies that either $k = 7$ and $15 \leqslant n \leqslant 23$, or $k = 5$ and $11 \leqslant n \leqslant 129$. This finite list of cases can be checked using Magma and we conclude that $(n,k) = (12,5)$ is the only exception to the main statement of the proposition. □

We will also need the following number-theoretic result, which is [9, Lemma 2.6]. This lemma will also be useful in Section 4.

Lemma 3.7. *Let r and s be primes and let m and 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) $(r,n) = (2,1)$ *and* $s = 2^m + 1$ *is a Fermat prime.*

(iii) $(s,m) = (2,1)$ *and* $r = 2^n - 1$ *is a Mersenne prime.*

We are now ready to begin the proof of Theorem 3.1 in the case where $G = S_n$ or A_n and Ω is the set of k-element subsets of $\{1,\ldots,n\}$ with $1 \leqslant k < n/2$.

Lemma 3.8. *If $k \geqslant 4$ then G is not almost elusive.*

Proof. Suppose $k \geqslant 4$. The cases $(n,k) = (12,5)$ and $(9,4)$ can be handled directly. For example, if $(n,k) = (9,4)$ then it is easy to see that G contains derangements of order 3 and 7. In each of the remaining cases, Proposition 3.6 implies that $|\Omega|$ is divisible by at least two distinct primes r and s with $r, s > k$.

Since $r > k$, it follows that r divides $n - t$ for some $t \in \{0,1,\ldots,k-1\}$ and we can consider an element $g \in G$ with cycle-shape $[r^{(n-t)/r}, 1^t]$. Since $t < k$, it follows that g is a derangement. Therefore, in the remaining cases we see that G contains derangements of order r and s, whence G is not almost elusive. □

Lemma 3.9. *If $k = 1$ then G is almost elusive if and only if one of the following holds:*

(i) $n = r^a$, *r prime, with $a \geqslant 2$ if $G = A_n$.*

(ii) $G = A_n$, $n = 2r^a$, $r \geqslant 3$ *prime.*

Proof. If n is divisible by two distinct odd primes, say r and s, then G contains derangements with cycle-shape $[r^{n/r}]$ and $[s^{n/s}]$, so G is not almost elusive. Therefore, for the remainder we may assume $n = 2^m r^a$, where r is an odd prime and $m, a \geqslant 0$.

Suppose $m, a > 0$. If $G = S_n$, or $G = A_n$ with $m \geqslant 2$, then elements of the form $[2^{n/2}]$ and $[r^{n/r}]$ are derangements. However, if $G = A_n$ and $m = 1$, then $n \equiv 2 \pmod 4$ and G does not contain elements of the form $[2^{n/2}]$, so in this case G is almost elusive. If $a = 0$ then $n = 2^m$ and G is almost elusive since both S_n and A_n have a unique conjugacy class of elements with cycle-shape $[2^{n/2}]$. Finally, if $m = 0$ then $n = r^a$ and G is almost elusive unless $G = A_n$ and $a = 1$, in which case G has two classes of r-cycles. □

Lemma 3.10. *If $k = 2$ then G is almost elusive if and only if $n = 9$, or $G = S_n$ and either n is a Fermat prime, or $n - 1$ is a Mersenne prime.*

Proof. Let $g \in G$ be an element of order r, with cycle-shape $[r^d, 1^{n-dr}]$. Clearly, if $r = 2$ or $n - dr \geqslant 2$, then g fixes a 2-set. Now assume r is odd and $n - dr \leqslant 1$.

First assume $n = 2^m l$ is even, where $m \geqslant 1$ and l is odd. If r is a prime divisor of $n - 1$ then every element with cycle-shape $[r^{(n-1)/r}, 1]$ is a derangement, so we may assume $n - 1 = r^a$ for some $a \geqslant 1$. Similarly, if r is a prime divisor of l, then there exist derangements with cycle-shape $[r^{n/r}]$, so we may also assume $n = 2^m$. By Lemma 3.7 we deduce that $a = 1$, so $r = 2^m - 1$ is a Mersenne prime and $|\Omega| = 2^{m-1}r$. In particular, every prime order derangement in G is an r-cycle and thus G is almost elusive if $G = S_n$, but not if $G = A_n$ (since there are two A_n-classes of r-cycles).

Now assume $n = 2^m l + 1$ is odd, where $m \geqslant 1$ and l is odd. If r is a prime divisor of n, then elements of the form $[r^{n/r}]$ are derangements, so we may assume $n = r^a$ is a prime power. Similarly, if l is divisible by an odd prime s, then we get derangements of the form $[s^{(n-1)/s}, 1]$, so we can assume $l = 1$ and thus $r^a = 2^m + 1$. By Lemma 3.7, it follows that either $n = 9$, or $n = r = 2^m + 1$ is a Fermat prime.

If $n = 9$ then it is easy to see that every derangement of prime order has cycle-shape $[3^3]$, so G is almost elusive. Now assume $n = r = 2^m + 1$ is a Fermat prime, so $|\Omega| = 2^m r$ and the only prime order derangements are r-cycles. We conclude that $G = S_n$ is almost elusive, but $G = A_n$ has two conjugacy classes of prime order derangements. □

Proposition 3.11. *The conclusion to Theorem 3.1 holds if H is intransitive.*

Proof. We may assume $k = 3$ and our aim is to show that G is almost elusive if and only if $n = 9$ or $G = A_{10}$. Let $g \in G$ be an element of prime order r with cycle-shape $[r^d, 1^{n-dr}]$. Visibly, g is a derangement if and only if $r = 2$ and $n = 2d$, or $r \geqslant 5$ and $n - dr \leqslant 2$. We divide the proof into two parts, according to the parity of n. Note that the condition $k < n/2$ implies that $n \geqslant 7$.

Case 1. n even

First assume n is even, say $n = 2^m l$ with $m \geqslant 1$ and $l \geqslant 1$ odd. For now, let us also assume that $m \geqslant 2$ if $G = A_n$. Then G contains derangements of shape $[2^{n/2}]$ and the observation above implies that G is almost elusive only if $n = 2^m 3^b$ and $n - 1 = 3^c$ with $b, c \geqslant 0$. Therefore $n - 1 = 2^m 3^b - 1 = 3^c$, so $b = 0$ and $n - 1 = 2^m - 1 = 3^c$. But now Lemma 3.7 implies that $n = 4$, so this situation does not arise and we conclude that G is not almost elusive.

Next assume $G = A_n$ and $n = 2l$, where $l \geqslant 5$ is odd. If l is divisible by two distinct primes $r, s \geqslant 5$, then G is not almost elusive since there are derangements of shape $[r^{n/r}]$ and $[s^{n/s}]$. So we may assume that $l = 3^a r^b$, where $r \geqslant 5$ is a prime and $a, b \geqslant 0$.

Suppose $b = 0$, so $l = 3^a$, $a \geqslant 2$ and we have

$$|\Omega| = \binom{n}{3} = 3^{a-1}(n-1)(n-2).$$

Note that $n-1$ is odd and indivisible by 3, so it is divisible by a prime $s \geqslant 5$ and thus elements in G of shape $[s^{(n-1)/s}, 1]$ are derangements. If $n-2 = 2^c$, then $3^a - 1 = 2^{c-1}$ and Lemma 3.7 implies that $a = 2$ and $c = 4$, so $n = 18$. But here G has two classes of 17-cycles, so G is not almost elusive. Therefore, we have reduced to the case where $n-2$ is divisible by a prime $t \geqslant 5$; since s and t are distinct, we conclude that G is not almost elusive.

Now assume $b \geqslant 1$, so G contains derangements of shape $[r^{n/r}]$. If $a \geqslant 1$, then $n-1$ is divisible by a prime $s \geqslant 5$ with $s \neq r$, which implies that G contains derangements of shape $[s^{(n-1)/s}, 1]$ and thus G is not almost elusive. Now assume $a = 0$. Suppose G is almost elusive. Then neither $n-1$ nor $n-2$ can be divisible by a prime $s \geqslant 5$, so we have $n-1 = 3^c$ and $n-2 = 2^d 3^e$ for integers c, d and e. But $n-1$ and $n-2$ are not both divisible by 3, so $e = 0$ and we have $3^c = 2^d + 1$. By Lemma 3.7 we deduce that $c = 2$ and $d = 3$ is the only solution, so $G = A_{10}$ and this is an almost elusive group (the only derangements have cycle-shape $[5^2]$).

Case 2. n odd

Now assume n is odd, say $n = 2^m l + 1$ with $m \geqslant 1$ and l odd. First assume n is divisible by 3 and G is almost elusive. Since $n-2$ is odd and indivisible by 3, it must be divisible by a prime $r \geqslant 5$ and thus G contains derangements of shape $[r^{(n-2)/r}, 1^2]$. Therefore, we must have $n-2 = r^a$. In addition, if n is divisible by a prime $s \geqslant 5$, then $s \neq r$ and G contains derangements of the form $[s^{n/s}]$, whence $n = 3^b$. Similarly, $n-1 = 2^c$ and thus $3^b = 2^c + 1$, which has the unique solution $(b, c) = (2, 3)$ by Lemma 3.7. Therefore, $n = 9$ and every prime order derangement is a 7-cycle, so both S_9 and A_9 are almost elusive.

Next assume $n \equiv 1 \pmod 3$, so both n and $n-2$ are odd and indivisible by 3. Therefore, there exist distinct primes $r, s \geqslant 5$ such that r divides n and s divides $n-2$, whence G contains derangements of the form $[r^{n/r}]$ and $[s^{(n-2)/s}, 1^2]$. In particular, G is not almost elusive.

Finally, suppose $n \equiv 2 \pmod 3$ and G is almost elusive. Let $r \geqslant 5$ be a prime divisor of n. Then G contains derangements of shape $[r^{n/r}]$, so $n = r^a$. Similarly, if $n-2$ is divisible by a prime $s \geqslant 5$, then G contains derangements of the form $[s^{(n-2)/s}, 1^2]$, so this forces $n-2 = 3^b$. Similarly, $n-1 = 2^c$ for some integer c and thus $2^c = 3^b + 1$. By Lemma 3.7 it follows that $(b, c) = (1, 2)$ and thus $n = 5$, which is a contradiction since $n \geqslant 7$. □

3.2. **Imprimitive subgroups.** Next we assume H acts transitively and imprimitively on $\{1, \ldots, n\}$, so $n = ab$ with $a, b \geqslant 2$ and $H = (S_a \wr S_b) \cap G$. In addition, we may identify Ω with the set Ω_a^b of partitions of $\{1, \ldots, n\}$ into b parts of size a. In view of Proposition 3.2, we will assume $n \geqslant 11$.

Lemma 3.12. *Consider the action of $G = S_n$ on $\Omega = \Omega_a^b$, where $n \geqslant 5$. If $r > a$ is a prime divisor of $|\Omega|$, then every r-cycle in G is a derangement.*

Proof. Let $H = S_a \wr S_b$ be a point stabiliser. If $r > b$ then r does not divide $|H|$ and thus every element in G of order r is a derangement.

Now assume $r \leqslant b$ and let $x \in G$ be an r-cycle. Seeking a contradiction, suppose x fixes a partition $\alpha = \{X_1, \ldots, X_b\}$ in Ω; let π be the permutation of $\{1, \ldots, b\}$ induced from the action of x on the parts in α. Note that $\pi \neq 1$ since $r > a$. In fact, since x has order r it follows that π also has order r and thus $|\mathrm{supp}(x)| \geqslant ra$ with respect to the action of x on $\{1, \ldots, n\}$. But this is a contradiction since x is an r-cycle and $a \geqslant 2$. We conclude that x is a derangement. □

Recall *Bertrand's postulate*: for every integer $n \geqslant 4$, there exists a prime number in the interval $(n/2, n)$. We will need the following extension, which is a special case of a result due to Ramanujan [38].

Lemma 3.13. *If $n \geqslant 12$, then there are at least two primes in the interval $(n/2, n)$.*

Proposition 3.14. *The conclusion to Theorem 3.1 holds if H is imprimitive.*

Proof. As above, write $n = ab$, where $a, b \geqslant 2$, and identify Ω with the set of partitions of $\{1, \ldots, n\}$ into b subsets of size a. By Proposition 3.2, we may assume $n \geqslant 12$. Applying Lemma 3.13, fix primes r, s such that $n/2 < r < s < n$. Then r and s both divide $|\Omega|$ and both primes are strictly larger than a, so Lemma 3.12 implies that every r-cycle and every s-cycle in G is a derangement. Therefore, G is not almost elusive. □

3.3. **Primitive subgroups.** To complete the proof of Theorem 3.1, it remains to handle the groups where H acts primitively on $\{1, \ldots, n\}$.

Lemma 3.15. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a primitive permutation group with socle $G_0 = A_n$ and point stabiliser H. Assume $n \geqslant 7$ and H acts primitively on $\{1, \ldots, n\}$.*

(i) *If r is a prime divisor of $|\Omega|$, then G contains a derangement of order r.*

(ii) *$|\Omega|$ is divisible by at least two distinct primes.*

Proof. Part (i) is [7, Proposition 3.5], which follows by combining classical results of Jordan [29] and Manning [34]. Now consider (ii). Seeking a contradiction, suppose $|\Omega| = r^a$ for some prime r.

First assume $G = A_n$. By [26, Theorem 1] we have $n = r^a$ and $H \cong A_{n-1}$, so [42, Lemma 2.2] implies that H is the stabiliser of a point in the natural action of $\{1, \ldots, n\}$. This is incompatible with the fact that H acts primitively on $\{1, \ldots, n\}$.

Now assume $G = S_n$ and set $L = A_n$. Since H is maximal we have $H \not\leqslant L$ and thus $G = LH$. Therefore, $|L : H \cap L| = r^a$ and so the result for alternating groups implies that $n = r^a$ and $H \cap L = A_{n-1}$ is a point stabiliser with respect to the natural action of L on $\{1, \ldots, n\}$. Write $H \cap L = L_k \leqslant G_k$ for some $k \in \{1, \ldots, n\}$. Since $|H : H \cap L| = 2$ we have $|H : L_k| = 2$ and thus L_k is normal in H. In particular, $L_k = L_{k^h}$ for all $h \in H$, so $k = k^h$ for all $h \in H$ and thus H acts intransitively on $\{1, \ldots, n\}$. So once again we have reached a contradiction. □

Proposition 3.16. *The conclusion to Theorem 3.1 holds if H is primitive.*

Proof. By Proposition 3.2, we may assume $n \geqslant 11$. Then Lemma 3.15 implies that G is not almost elusive. □

This completes the proof of Theorem 2 for symmetric and alternating groups.

4. Rank one groups of Lie type

As in Section 1, let $\mathcal{B}$ be the set of sporadic simple groups, together with the simple groups of Lie type of the form $\mathrm{L}_2(q)$ (with $q \geqslant 7$ and $q \neq 9$), $\mathrm{U}_3(q)$ (with $q \geqslant 3$), ${}^2G_2(q)$ (with $q \geqslant 27$) and ${}^2B_2(q)$ (with $q \geqslant 8$); see Remark 4(d) for an explanation of the conditions on q in each case. In this section we will prove the following result, which establishes Theorem 2 in the cases where $G_0 \in \mathcal{B}$ is a group of Lie type (the sporadic groups will be handled in Section 5).

Theorem 4.1. *Let G be an almost simple primitive permutation group with socle $G_0 \in \mathcal{B}$ and point stabiliser H, where G_0 is a group of Lie type. Then G is almost elusive if and only if (G, H) is one of the cases recorded in Table 2.*

For the classical groups with socle $G_0 = \mathrm{L}_2(q)$ or $\mathrm{U}_3(q)$, we follow [32] in referring to the *type* of a maximal subgroup of G. Recall that this provides an approximate description of the structure of $H \cap \mathrm{PGL}(V)$, where V is the natural module for G_0. Throughout this section, we set $q = p^f$ with p a prime and we write $H_0 = H \cap G_0$.

Recall that if $n \geqslant 2$ is an integer, then a prime divisor r of $q^n - 1$ is a *primitive prime divisor* if $q^i - 1$ is indivisible by r for all $1 \leqslant i < n$. By a well known theorem of Zsigmondy [45], primitive prime divisors exist unless $(n, q) = (6, 2)$, or if $n = 2$ and q is a Mersenne

prime. Note that if r is such a prime and m is a positive integer, then r divides $q^m - 1$ if and only if n divides m. Also note that Fermat's Little Theorem implies that $r \equiv 1 \pmod{n}$. In addition, it will be useful to observe that every primitive prime divisor of $p^{fn} - 1$ is also a primitive prime divisor of $q^n - 1$.

Throughout this section, it will be helpful to recall that G is not almost elusive if $|\pi(G) \setminus \pi(H)| \geqslant 2$, where $\pi(X)$ denotes the set of prime divisors of $|X|$ (see Remark 2).

4.1. **Two-dimensional linear groups.** In this section we prove Theorem 4.1 for the groups with socle $G_0 = \mathrm{L}_2(q)$. Write $q = p^f$ with p a prime and set $d = (2, q-1)$. Fix a basis $\{e_1, e_2\}$ for the natural module V and recall that $|G_0| = \frac{1}{d}q(q^2-1)$. As in [32], for $g \in \mathrm{Aut}(G_0)$ we write $\ddot{g}$ for the coset $G_0 g \in \mathrm{Out}(G_0) = \mathrm{Aut}(G_0)/G_0$. By [32, Proposition 2.2.3] we have

$$\mathrm{Out}(G_0) = \begin{cases} \langle \ddot{\delta} \rangle \times \langle \ddot{\phi} \rangle = C_2 \times C_f & \text{if } p > 2 \\ \langle \ddot{\phi} \rangle = C_f & \text{if } p = 2. \end{cases}$$

With respect to the basis $\{e_1, e_2\}$, we may assume δ is the diagonal automorphism induced by conjugation by $\left(\begin{smallmatrix} \mu & 0 \\ 0 & 1 \end{smallmatrix}\right)$, where $\mathbb{F}_q^\times = \langle \mu \rangle$, and ϕ is the field automorphism of order f corresponding to the Frobenius map $(a_{ij}) \mapsto (a_{ij}^p)$ on matrices. In particular, we may assume ϕ acts on V by sending $ae_1 + be_2$ to $a^p e_1 + b^p e_2$.

The maximal subgroups of G_0 were originally determined by Dickson (see Dickson's book [12], first published in 1901) and the complete list of (core-free) maximal subgroups of G (up to conjugacy) is conveniently reproduced in [3, Tables 8.1 and 8.2].

Proposition 4.2. *Let G be an almost simple group with socle $G_0 = \mathrm{L}_2(q)$ and let H be a core-free maximal subgroup of G. Then the type of H is one of the following:*

$$P_1,\ \mathrm{GL}_1(q) \wr S_2,\ \mathrm{GL}_1(q^2),\ \mathrm{GL}_2(q_0)\ (q = q_0^k,\ k \text{ prime}),$$
$$2_-^{1+2}.O_2^-(2)\ (q = p \geqslant 3),\ A_5\ (q = p \text{ or } p^2).$$

Proof. See Tables 8.1 and 8.2 in [3], which record the precise structure of H_0, together with the exact conditions needed for maximality. For example, we see that

$$(G, H) = \begin{cases} (G_0, S_4) & q = p \equiv \pm 1 \pmod 8 \\ (G_0, A_4) & q = p \equiv \pm 3, 5, \pm 13 \pmod{40} \\ (\mathrm{PGL}_2(q), S_4) & q = p \equiv \pm 11, \pm 19 \pmod{40} \end{cases}$$

if H is of type $2_-^{1+2}.O_2^-(2)$. □

Remark 4.3. Note that if H is of type $\mathrm{GL}_1(q) \wr S_2$ or $\mathrm{GL}_1(q^2)$, then $H_0 = D_{2(q-1)/d}$ or $D_{2(q+1)/d}$, respectively.

Write $\mathrm{PGL}_2(q) = \mathrm{GL}_2(q)/Z$, where $Z = Z(\mathrm{GL}_2(q))$ is the centre of $\mathrm{GL}_2(q)$. We will need to recall some basic properties of certain conjugacy classes of prime order elements in $\mathrm{PGL}_2(q)$. For a general reference, we refer the reader to [6, Section 3.2]. Let $x \in \mathrm{PGL}_2(q)$ be an element of prime order r and recall that x is *semisimple* if $r \neq p$ and *unipotent* if $r = p$. Write $x = Z\hat{x}$ with $\hat{x} \in \mathrm{GL}_2(q)$.

(a) First assume x is semisimple, so r divides $q^2 - 1$ and $x^{G_0} = x^{\mathrm{PGL}_2(q)}$. Suppose r is odd, which means that we may assume $\hat{x}$ also has order r. If r divides $q-1$ then $\hat{x}$ is $\mathrm{GL}_2(q)$-conjugate to a diagonal matrix. On the other hand, if r divides $q+1$ then the eigenvalues of $\hat{x}$ are contained in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and thus $\hat{x}$ acts irreducibly on V. In both cases, it will be useful to note that G contains $(r-1)/2$ distinct G_0-classes of semisimple elements of order r, so there are at least $\lceil (r-1)/2f \rceil$ conjugacy classes in G of such elements.

(b) Next assume x is a semisimple involution, so q is odd. Here x is G_0-conjugate to either t_1 or t_1' in the notation of [6, Section 3.2], which is consistent with [24, Table 4.5.1]. These elements are distinguished by the fact that t_1 lifts to an involution in $\mathrm{GL}_2(q)$, while t_1' lifts to an irreducible element of order 4. It is worth noting that

G_0 has a unique class of semisimple involutions, with $t_1 \in G_0$ if and only if $q \equiv 1 \pmod 4$. In addition, let us record that t_1 and t_1' are non-conjugate in $\mathrm{Aut}(G_0)$.

(c) Finally, suppose x is unipotent. Here we may assume $\hat{x}$ has order p and Jordan form $[J_2]$ on V. If $p = 2$ then $G_0 = \mathrm{PGL}_2(q)$ has a unique conjugacy class of involutions. On the other hand, if p is odd then there are two classes of such elements in G_0, which are fused in $\mathrm{PGL}_2(q)$.

We are now ready to begin the proof of Theorem 4.1 for $G_0 = \mathrm{L}_2(q)$. We start by handling the groups where the underlying field is small.

Proposition 4.4. *The conclusion to Theorem 4.1 holds if $G_0 = \mathrm{L}_2(q)$ and $q \leqslant 11$.*

Proof. This is an entirely straightforward Magma [2] calculation, using the standard commands `ConjugacyClasses`, `MaximalSubgroups` and `CosetAction`. □

For the remainder, we may assume $q \geqslant 13$. The possibilities for the point stabiliser H are recorded in Proposition 4.2 and we consider each one in turn.

Proposition 4.5. *The conclusion to Theorem 4.1 holds if $G_0 = \mathrm{L}_2(q)$ and H is of type P_1.*

Proof. Here $H_0 = (C_p)^f{:}C_{(q-1)/d}$ is a Borel subgroup of G_0 and we have $|\Omega| = q+1$. We may identify Ω with the set of 1-dimensional subspaces of the natural module V. Notice that if r is an odd prime divisor of $q+1$, then $|H_0|$ is indivisible by r and thus every element in G_0 of order r is a derangement. In particular, if $q+1$ is divisible by two distinct odd primes, then G is not almost elusive. So for the remainder, we may assume $q+1 = 2^a r^b$ if q is odd and $q+1 = r^b$ if q is even, where r is an odd prime.

First assume q is even and $q+1 = r^b$. By Lemma 3.7, either $q = 8$, or $b = 1$ and r is a Fermat prime (in which case, $q = 2^f$ and $f \geqslant 4$ is a 2-power). The case $q = 8$ was handled in Proposition 4.4, so let us assume $q+1 = r \geqslant 17$ is a Fermat prime. As noted above, G_0 has $(r-1)/2 = q/2$ distinct conjugacy classes of elements of order r and thus G contains at least $q/2f \geqslant 2$ such classes. Since each of these elements is a derangement, we conclude that G is not almost elusive.

Now assume q is odd and $q+1 = 2^a r^b$, where $a \geqslant 1$ and $b \geqslant 0$. If $b = 0$ then Lemma 3.7 implies that $q = 2^a - 1$ is a Mersenne prime, so $|\Omega| = 2^a$ and $G = G_0$ or $\mathrm{PGL}_2(q)$. In terms of the notation introduced above, each involution in G_0 is of type t_1' (since $q \equiv 3 \pmod 4$) and these elements are derangements since they act irreducibly on V (alternatively, note that $|H_0|$ is odd). On the other hand, every t_1-type involution in $\mathrm{PGL}_2(q) \setminus G_0$ visibly fixes a 1-space and we conclude that G is almost elusive.

Finally, let us assume $b \geqslant 1$. As noted above, G contains derangements of order r. In addition, if $a \geqslant 2$ then $q \equiv 3 \pmod 4$ and we note that the involutions in G_0 (which are of type t_1') are derangements. Similarly, if $a = 1$ and $\mathrm{PGL}_2(q) \leqslant G$ then G contains involutions of type t_1' and these elements are derangements. So to complete the proof, we may assume that $a = 1$ and $G \cap \mathrm{PGL}_2(q) = G_0$. Now if $x \in G \setminus G_0$ has prime order, then x is $\mathrm{PGL}_2(q)$-conjugate to a standard field automorphism of the form ϕ^i (see [24, Proposition 4.9.1(d)], for example), where ϕ acts on V by sending $ae_1 + be_2$ to $a^p e_1 + b^p e_2$. In particular, ϕ fixes the 1-space $\langle e_1 \rangle$ and thus x has fixed points on Ω. As a consequence, it follows that an element $x \in G$ is a derangement of prime order if and only if $x \in G_0$ has order r.

By the theorem of Zsigmondy mentioned at the beginning of Section 4, there exists a primitive prime divisor s of $p^{2f} - 1$. Since we are assuming r is the unique odd prime divisor of $q+1$, it follows that $r = s$ and thus $r \equiv 1 \pmod{2f}$, so $r \geqslant 2f+1$. If $r > 2f+1$ then G has at least $\lceil (r-1)/2f \rceil \geqslant 2$ distinct conjugacy classes of such elements, so G is not almost elusive. Now assume $r = 2f+1$. By arguing as in the proof of [9, Lemma 4.6] we deduce that $f = 2^m$ is a 2-power, so $r = 2^{m+1} + 1$ is a Fermat prime and thus $m+1 = 2^l$ for some $l \geqslant 0$.

If $l = 0$, then $f = 1$, $r = 3$ and $G = \mathrm{L}_2(p)$ is almost elusive since it contains a unique class of elements of order 3.

Now assume $l \geqslant 1$ and write $G = G_0.J$ with

$$J \leqslant \mathrm{Out}(G_0) = \langle \ddot{\delta} \rangle \times \langle \ddot{\phi} \rangle = C_2 \times C_f.$$

Recall that G_0 contains $(r-1)/2 = f$ distinct conjugacy classes of elements of order r. If J does not project onto $\langle \ddot{\phi} \rangle$, then G has at least two conjugacy classes of elements of order r and thus G is not almost elusive. On the other hand, if this projection is surjective then the condition $G \cap \mathrm{PGL}_2(q) = G_0$ implies that $J = \langle \ddot{\phi} \rangle$ or $\langle \ddot{\delta}\ddot{\phi} \rangle$ and we see that G has a unique class of elements of order r. We conclude that G is almost elusive if and only if $G = G_0.f$. □

Remark 4.6. Consider the case $G_0 = \mathrm{L}_2(q)$ in the proof of Proposition 4.5, where $q+1 = 2r^a$, $r = 2^{2^l} + 1$ is a Fermat prime and $q = p^f$ with $f = 2^{2^l-1}$. If $l = 0$ then $f = 1$, $r = 3$ and there exist primes p with $p + 1 = 2.3^a$ for some $a \geqslant 1$. For example, the primes $p < 10^6$ of this form are 5, 17, 53, 4373 and 13121. For $l = 1$ we have $f = 2$, $r = 5$ and one checks that 3 and 7 are the only primes $p < 10^6$ with $p^2 + 1 = 2.5^a$. For $l \geqslant 2$, we are not aware of any solutions to the equation $q + 1 = 2r^a$ with f and r as above.

Proposition 4.7. *The conclusion to Theorem 4.1 holds if $G_0 = \mathrm{L}_2(q)$ and H is of type $\mathrm{GL}_1(q) \wr S_2$.*

Proof. Here $H_0 = D_{2(q-1)/d}$ and $|\Omega| = \frac{1}{2}q(q+1)$. If r is an odd prime divisor of $q+1$ then every element in G_0 of order r is a derangement. Therefore, we may assume $q + 1 = 2^a r^b$, where r is an odd prime and $a, b \geqslant 0$.

Suppose $q = 2^f$ is even, so $2^f + 1 = r^b$ and Lemma 3.7 implies that either $q = 8$, or $b = 1$, f is a 2-power and $q + 1$ is a Fermat prime. In view of Proposition 4.4, we can assume we are in the latter situation with $f = 2^m$ and $m \geqslant 2$. Here G has at least $q/2f \geqslant 2$ conjugacy classes of elements of order r, whence G is not almost elusive.

Now assume q is odd and $q+1 = 2^a r^b$, where $a \geqslant 1$ and $b \geqslant 0$. Here every element in G_0 of order p is a derangement, so we may assume $b = 0$ and thus $p^f + 1 = 2^a$. By applying Lemma 3.7, we deduce that $q = 2^a - 1$ is a Mersenne prime and thus $|\Omega| = 2^{a-1}q$. If $G = G_0$, then G contains two conjugacy classes of elements of order q, so G is not almost elusive. On the other hand, if $G = \mathrm{PGL}_2(q)$ then there is a unique class of elements of order q and we observe that both classes of involutions in G have fixed points. Indeed, since $q \equiv 3 \pmod 4$ it follows that the involutions in $H_0 = D_{q-1}$ are of type t_1', while the involution in the centre of $H = D_{2(q-1)}$ is of type t_1. It follows that $\mathrm{PGL}_2(q)$ is almost elusive. □

Proposition 4.8. *The conclusion to Theorem 4.1 holds if $G_0 = \mathrm{L}_2(q)$ and H is of type $\mathrm{GL}_1(q^2)$.*

Proof. In this case we have $H_0 = D_{2(q+1)/d}$ and $|\Omega| = \frac{1}{2}q(q-1)$. By arguing as in the proof of the previous proposition, we may assume that $q - 1 = 2^a r^b$, where r is an odd prime and $a, b \geqslant 0$.

Suppose $q = 2^f$ is even, so $2^f - 1 = r^b$ and Lemma 3.7 implies that $b = 1$, so $r = 2^f - 1$ is a Mersenne prime and $f \geqslant 5$ is a prime (the case $f = 3$ was handled in Proposition 4.4). Since G contains at least $\lceil (r-1)/2f \rceil \geqslant 2$ distinct classes of such elements, we conclude that G is not almost elusive.

Now assume q is odd and $q - 1 = 2^a r^b$ with $a \geqslant 1$. Note that every element in G_0 of order p is a derangement. If $b \geqslant 1$ then G also contains derangements of order r, so we may assume $p^f = 2^a + 1$. Since the case $q = 9$ is excluded (recall that $\mathrm{L}_2(9) \cong A_6$), Lemma 3.7 implies that $q = 2^a + 1 \geqslant 17$ is a Fermat prime. If $G = G_0$ then G has two classes of elements of order q, so G is not almost elusive. Now assume $G = \mathrm{PGL}_2(q)$ and note that G has a unique class of derangements of order q. The involutions in $H_0 = D_{q+1}$

are of type t_1 (note that $q \equiv 1 \,(\mathrm{mod}\, 4)$), while the central involution in $H = D_{2(q+1)}$ is of type t_1'. Therefore, every involution in G has fixed points and we conclude that G is almost elusive. □

Proposition 4.9. *The conclusion to Theorem 4.1 holds if $G_0 = \mathrm{L}_2(q)$ and H is of type $\mathrm{GL}_2(q_0)$, where $q = q_0^k$ with k a prime.*

Proof. First assume k is odd, so $H_0 = \mathrm{L}_2(q_0)$ and

$$|\Omega| = q_0^{k-1}\left(\frac{q_0^{2k}-1}{q_0^2-1}\right) = q_0^{k-1}\left(\frac{q_0^k-1}{q_0-1}\right)\left(\frac{q_0^k+1}{q_0+1}\right).$$

As noted in [3, Table 8.1], the maximality of H requires $q_0 \neq 2$, so Zsigmondy's theorem [45] implies that there exist primitive prime divisors r and s of $q_0^{2k}-1$ and q_0^k-1, respectively. Then $r \neq s$ and both r and s divide $|\Omega|$, but neither divide q_0^2-1. Therefore, every element in G of order r or s is a derangement and we conclude that G is not almost elusive.

Now assume $k = 2$, so $H_0 = \mathrm{PGL}_2(q_0)$ and $|\Omega| = \frac{1}{d}q_0(q+1)$. Suppose q is odd, so $q \equiv 1 \,(\mathrm{mod}\, 4)$ since $q = q_0^2$. Here $q+1$ is divisible by an odd prime r and we see that every element in G_0 of order r is a derangement. Let us also observe that the maximality of H implies that $G \leqslant G_0.\langle\phi\rangle$, where ϕ is a field automorphism of order f (see [3, Table 8.1]), so G has two conjugacy classes of unipotent elements of order p, whereas H has just one. Therefore, G contains derangements of order p and we deduce that G is not almost elusive.

Finally, let us assume $k = 2$ and $q = 2^f$ is even. If r is a prime divisor of $q+1$ then every element in G_0 of order r is a derangement and so we may assume that $2^f + 1 = r^a$. Since f is even, Lemma 3.7 implies that $r = 2^f + 1$ is a Fermat prime with $f \geqslant 4$ a 2-power. Finally, since G contains at least $(r-1)/2f \geqslant 2$ distinct conjugacy classes of elements of order r, we see that G is not almost elusive. □

Proposition 4.10. *The conclusion to Theorem 4.1 holds if $G_0 = \mathrm{L}_2(q)$ and H is of type $2_-^{1+2}.O_2^-(2)$.*

Proof. Here we may assume $q = p \geqslant 11$ and by inspecting [32, Proposition 4.6.7] we see that $H_0 = S_4$ if $q \equiv \pm 1 \,(\mathrm{mod}\, 8)$, otherwise $H_0 = A_4$. Every element in G of order p is a derangement and there are two classes of such elements if $G = G_0$, so for the remainder we may assume $G = \mathrm{PGL}_2(q)$ and thus the maximality of H implies that $q \equiv \pm 3 \,(\mathrm{mod}\, 8)$. In particular, q is neither a Mersenne nor a Fermat prime, whence q^2-1 is divisible by a prime $r \geqslant 5$ and we deduce that G contains derangements of order r. In particular, G is not almost elusive. □

Proposition 4.11. *The conclusion to Theorem 4.1 holds if $G_0 = \mathrm{L}_2(q)$ and H is of type A_5.*

Proof. Here $H_0 = A_5$, $p \geqslant 7$ and the maximality of H in G implies that either $G = G_0$, or $q = p^2$ and $G = G_0.\langle\phi\rangle$, where ϕ is an involutory field automorphism (see [3, Table 8.2]). In both cases, G has two conjugacy classes of elements of order p and we deduce that G is not almost elusive. □

4.2. **Three-dimensional unitary groups.** Next we turn to the groups with socle $G_0 = \mathrm{U}_3(q)$, where $q = p^f \geqslant 3$. Set $d = (3, q+1)$.

The cases with $q \leqslant 19$ can be handled using Magma; as in the proof of Proposition 4.4, this is a straightforward computation (here it is helpful to recall that G is almost elusive only if $|\pi(G) \setminus \pi(H)| \leqslant 1$, where $\pi(X)$ is the set of prime divisors of $|X|$).

Proposition 4.12. *The conclusion to Theorem 4.1 holds if $G_0 = \mathrm{U}_3(q)$ and $q \leqslant 19$.*

In view of the proposition, for the remainder we may assume $q \geqslant 23$ and our goal is to prove that G is not almost elusive. The maximal subgroups of G are recorded in [3, Tables 8.5 and 8.6] and by inspection we obtain the following result (see the tables in [3] for additional conditions on G and q that are needed for the maximality of H).

Proposition 4.13. *Let G be an almost simple group with socle $G_0 = \mathrm{U}_3(q)$ and let H be a core-free maximal subgroup of G. If $q \geqslant 23$, then the type of H is one of the following:*

$$P_1,\ \mathrm{GU}_2(q) \times \mathrm{GU}_1(q),\ \mathrm{GU}_1(q) \wr S_3,\ \mathrm{GU}_1(q^3),\ \mathrm{GU}_3(q_0)\ (q = q_0^k,\ k \geqslant 3 \text{ prime}),$$

$$\mathrm{SO}_3(q)\ (q \text{ odd}),\ 3^{1+2}.\mathrm{Sp}_2(3)\ (q = p \equiv 2 \pmod 3),\ \mathrm{L}_2(7)\ (q = p),\ A_6\ (q = p).$$

The following number-theoretic lemma will be useful.

Lemma 4.14. *Let $q = p^f$ be a prime power with $q \geqslant 3$ and let $\mathcal{P}$ be the set of primitive prime divisors of $q^6 - 1$. If $\mathcal{P} = \{r\}$ then either $r \geqslant 12f + 1$, or $q \in \{3, 4, 5, 8, 19\}$ and $r = 6f + 1$.*

Proof. Suppose $\mathcal{P} = \{r\}$. Since $\mathcal{P}$ contains every primitive prime divisor of $p^{6f} - 1$, it follows that $r = 6mf + 1$ for some $m \geqslant 1$ and so we may assume $r = 6f + 1$. Note that r divides $q^2 - q + 1$. If $s \geqslant 5$ is a prime divisor of $q^2 - q + 1$ then it is easy to check that s does not divide $q^2 - 1$ nor $q^3 - 1$, so s is a primitive prime divisor of $q^6 - 1$ and thus $s = r$. Since $q^2 - q + 1$ is odd and indivisible by 9, it follows that either $q^2 - q + 1 = r^e$, or $q \equiv 2 \pmod 3$ and $q^2 - q + 1 = 3r^e$ for some positive integer e.

Suppose $q \equiv 2 \pmod 3$ and $q^2 - q + 1 = 3r^e$. If we set $x = -q$ and $y = r$, then we have an integer solution (x, y) to the Diophantine equation $x^2 + x + 1 = 3y^e$. By a theorem of Nagell [36], if $e \geqslant 3$ then the only integer solutions are $(x, y) = (1, 1)$ and $(-2, 1)$, neither of which are compatible since $x = -q \leqslant -3$. Therefore, $e = 1$ or 2 and thus

$$p^{2f} - p^f + 1 = 3(6f + 1) \text{ or } p^{2f} - p^f + 1 = 3(6f + 1)^2.$$

It is straightforward to check that $q = 5, 8$ are the only possibilities. Note that if $q = 5$ then $r = 7$ and $q^2 - q + 1 = 3r$. Similarly, if $q = 8$ then $r = 19$ and $q^2 - q + 1 = 3r$.

Finally, suppose $q \not\equiv 2 \pmod 3$ and $q^2 - q + 1 = r^e$. Setting $x = -q$ and $y = r$, we get an integer solution to the equation $x^2 + x + 1 = y^e$. If $e \geqslant 2$, then by applying [1, Proposition 1] we deduce that $(x, y, e) = (-19, 7, 3)$ is the only solution. Here $q = 19$, $r = 7$ and $q^2 - q + 1 = r^3$. On the other hand, if $e = 1$ then $p^{2f} - p^f + 1 = 6f + 1$ and we find that $q = 3$ or 4. Indeed, if $q = 3$ then $r = 7$ and $q^2 - q + 1 = r$. Similarly, if $q = 4$ then $r = 13$ and $q^2 - q + 1 = r$. The result follows. □

Proposition 4.15. *The conclusion to Theorem 4.1 holds if $G_0 = \mathrm{U}_3(q)$ and H is of type P_1, $\mathrm{GU}_2(q) \times \mathrm{GU}_1(q)$, $\mathrm{GU}_1(q) \wr S_3$ or $\mathrm{SO}_3(q)$.*

Proof. In view of Proposition 4.12,we may assume $q \geqslant 23$. Let r be a primitive prime divisor of $q^6 - 1$. In each case, we observe that $|H_0|$ is indivisible by r and thus every element in G_0 of order r is a derangement. Therefore, we may assume r is the unique primitive prime divisor of $q^6 - 1$. By applying Lemma 4.14 we get $r \geqslant 12f + 1$, where $q = p^f$ as above, and we note that G_0 contains $(r - 1)/3 \geqslant 4f$ distinct $\mathrm{PGU}_3(q)$-classes of such elements (see [6, Section 3.3.1]). Since $|\mathrm{Aut}(G_0) : \mathrm{PGU}_3(q)| = 2f$ it follows that there at least $(r - 1)/6f \geqslant 2$ such classes in G and we conclude that G is not almost elusive. □

Proposition 4.16. *The conclusion to Theorem 4.1 holds if $G_0 = \mathrm{U}_3(q)$ and H is of type $\mathrm{GU}_1(q^3)$.*

Proof. Here $H_0 = C_m{:}C_3$ with $m = \frac{1}{d}(q^2 - q + 1)$, so $|\Omega| = \frac{1}{3}q^3(q^2 - 1)(q + 1)$. Since $|H_0|$ is odd, it follows that every involution in G_0 is a derangement. Similarly, if $p \geqslant 5$ then every nontrivial unipotent element in G_0 is a derangement. For $p = 3$, the unipotent elements with Jordan form $[J_2, J_1]$ are derangements (the elements of order 3 in H_0 have Jordan

form $[J_3]$ on the natural module for G_0). Finally, suppose $p = 2$. In view of Proposition 4.12 we may assume $q \geqslant 32$, which implies that there exists a prime divisor r of $q-1$ with $r \geqslant 7$. Since $|H_0|$ is indivisible by r, we conclude that every element in G_0 of order r is a derangement and the proof of the proposition is complete. □

Proposition 4.17. *The conclusion to Theorem 4.1 holds if $G_0 = \mathrm{U}_3(q)$ and H is of type $\mathrm{GU}_3(q_0)$, where $q = q_0^k$ and $k \geqslant 3$ is a prime.*

Proof. By [32, Proposition 4.5.3] we have $H_0 = \mathrm{U}_3(q_0).e$, where $e = 3$ if $k = 3$ and $q \equiv -1 \pmod 9$, otherwise $e = 1$. Let r and s be primitive prime divisors of $q_0^{6k} - 1$ and $q_0^k - 1$, respectively. Then $|H_0|$ is indivisible by both r and s, so every element in G_0 of order r or s is a derangement and thus G is not almost elusive. □

Proposition 4.18. *The conclusion to Theorem 4.1 holds if $G_0 = \mathrm{U}_3(q)$ and H is of type $3^{1+2}.\mathrm{Sp}_2(3)$, $\mathrm{L}_2(7)$ or A_6.*

Proof. In each of these cases we have $q = p$ and so in view of Proposition 4.12 we may assume that $p \geqslant 23$. Then $|H_0|$ is indivisible by p and thus every element in G_0 of order p is a derangement. In particular, G is not almost elusive since it contains at least two conjugacy classes of elements of order p. □

4.3. **Ree groups.**

Proposition 4.19. *If $G_0 = {}^2G_2(q)$ with $q \geqslant 27$, then G is not almost elusive.*

Proof. Here $q = 3^{2m+1}$ with $m \geqslant 1$ and we have $|G_0| = q^3(q^3+1)(q-1)$. The maximal subgroups of G are recorded in [3, Table 8.43], which is reproduced from [31].

First assume H is a Borel subgroup, so $|H_0| = q^3(q-1)$ and $|\Omega| = q^3+1$. If r is an odd prime divisor of q^3+1 then every element in G_0 of order r is a derangement (note that $(q^3+1, q-1) = 2$). Now q^3+1 is divisible by 7, and it is also divisible by a primitive prime divisor r of $3^{12m+6}-1$. Since $r \geqslant 12m+7 \geqslant 19$, we deduce that q^3+1 is divisible by at least two distinct odd primes and thus G is not almost elusive.

Next suppose $H_0 = 2 \times \mathrm{L}_2(q)$, so $|\Omega| = q^2(q^2-q+1)$ and $H_0 = C_{G_0}(x)$ for an involution $x \in G_0$. If r is a prime divisor of q^2-q+1 then every element in G_0 of order r is a derangement. In addition, we observe that there exists an element $y \in G_0$ of order 3 with $|C_{G_0}(y)| = q^3$ (see [33, Table 22.2.7], for example); since $|C_{G_0}(y)|$ is odd, it follows that y is a derangement and we conclude that G is not almost elusive.

Next assume $H_0 = (2^2 \times D_{(q+1)/2})$:3. Let r and s be primitive prime divisors of $3^{12m+6}-1$ and $3^{2m+1}-1$, respectively. Then $r, s \geqslant 5$ and $|H_0|$ is indivisible by r and s, whence G is not almost elusive. Similarly, if $H_0 = (q \pm \sqrt{3q}+1)$:6 and we take r to be any prime divisor $q \mp \sqrt{3q}+1$, then every element in G_0 of order r or s is a derangement (with s a primitive prime divisor of $3^{2m+1}-1$ as above).

Finally, let us assume $H_0 = {}^2G_2(q_0)$, where $q = q_0^k$ and k is an odd prime. Let r and s be primitive prime divisors of $q_0^{6k}-1$ and q_0^k-1, respectively. Then $|H_0|$ is indivisible by r and s, whence G is not almost elusive. □

4.4. **Suzuki groups.**

Proposition 4.20. *If $G_0 = {}^2B_2(q)$ then G is not almost elusive.*

Proof. This is similar to the proof of the previous proposition. We have $q = 2^{2m+1}$ and $|G_0| = q^2(q^2+1)(q-1)$ with $m \geqslant 1$. The maximal subgroups of G are conveniently listed in [3, Table 8.16] (the original reference is [40]). It will be useful to observe that

$$q^2+1 = (q+\sqrt{2q}+1)(q-\sqrt{2q}+1),$$

where both factors are odd and coprime. In particular, q^2+1 is divisible by at least two distinct odd primes.

First assume $H_0 = q^{1+1}{:}(q-1)$ is a Borel subgroup, so $|\Omega| = q^2+1$. If r, s are distinct prime divisors of q^2+1, then neither prime divides $|H_0|$ and thus G is not almost elusive. The same argument applies if $H_0 = D_{2(q-1)}$. Next assume $H_0 = (q \pm \sqrt{2q}+1){:}4$. Here we take r and s to be prime divisors of $q \mp \sqrt{2q}+1$ and $q-1$, respectively, and we observe that $|H_0|$ is indivisible by both primes. Finally, suppose $H_0 = {}^2B_2(q_0)$, where $q = q_0^k$, $q_0 \neq 2$ and $k \geqslant 3$ is a prime, and let r and s be primitive prime divisors of $q_0^{4k}-1$ and $q_0^k - 1$, respectively. Then $r \neq s$ and neither prime divides $|H_0|$, whence all elements in G_0 of order r or s are derangements. □

This completes the proof of Theorem 4.1.

5. Sporadic groups

In this final section we complete the proof of Theorem 2 by handling the almost simple groups with socle a sporadic group. As noted in Section 1, we also include the almost simple groups with socle ${}^2F_4(2)'$.

Proposition 5.1. *The conclusion to Theorem 2 holds if $G_0 = {}^2F_4(2)'$.*

Proof. This is a routine Magma computation, using a permutation representation of G of degree 1755 from the Web-Atlas [43]. □

Theorem 5.2. *Let G be an almost simple primitive permutation group with socle a sporadic group. Then G is not almost elusive.*

Proof. Let H be a point stabiliser and first assume $G \neq \mathbb{B}, \mathbb{M}$, where $\mathbb{B}$ is the Baby Monster and $\mathbb{M}$ is the Monster. In each of these cases we can use the GAP Character Table Library [4] to show that G is not almost elusive. Indeed, the character tables of both G and H are available in [4] (to access the character table of H, we use the `Maxes` function), together with the fusion map from H-classes to G-classes. It is now a routine exercise to check that H has at least two conjugacy classes of prime order derangements, with the single exception of the elusive group $G = \mathrm{M}_{11}$ with $H = \mathrm{L}_2(11)$.

Next assume $G = \mathbb{B}$ and let $\pi(G)$ be the set of prime divisors of $|G|$. Define $\pi(H)$ in the same way. The complete list of maximal subgroups of G (up to conjugacy) is conveniently presented in the Web-Atlas [43] and it is easy to check that $|\pi(G) \setminus \pi(H)| \geqslant 2$ in every case. Therefore, we can find distinct primes that divide $|G|$ but not $|H|$, so G contains at least two conjugacy classes of derangements of prime order.

Finally, let us assume $G = \mathbb{M}$. There are 44 known conjugacy classes of maximal subgroups of G and it has been shown that any additional maximal subgroup has to be almost simple, with socle $\mathrm{L}_2(8)$, $\mathrm{L}_2(13)$, $\mathrm{L}_2(16)$ or $\mathrm{U}_3(4)$ (see [41]). In every case, including the list of candidate maximal subgroups, one checks that $|\pi(G) \setminus \pi(H)| \geqslant 2$ and the result follows as before. □

References

[1] M.A. Bennett and A. Levin, *The Nagell-Ljunggren equation via Runge's method*, Monatsh. Math. **177** (2015), 15–31.

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

[3] J.N. Bray, D.F. Holt and C.M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, LMS Lecture Note Series, vol. 407, Cambridge University Press, Cambridge, 2013.

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

[5] T.C. Burness and M. Giudici, *Locally elusive classical groups*, Israel J. Math. **225** (2018), 343–402.

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

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

[8] T.C. Burness and H.P. Tong-Viet, *Derangements in primitive permutation groups, with an application to character theory*, Quart. J. Math. **66** (2015), 63–96.

[9] T.C. Burness and H.P. Tong-Viet, *Primitive permutation groups and derangements of prime power order*, Manuscripta Math. **105** (2016), 255–291.
[10] P.J. Cameron (ed.), *Research problems from the Fifteenth British Combinatorial Conference (Stirling, 1995)*, Discrete Math. **167/168** (1997), 605–615.
[11] P.J. Cameron, M. Giudici, G.A. Jones, W.M. Kantor, M.H. Klin, D. Marušič and L.A. Nowitz, *Transitive permutation groups without semiregular subgroups*, J. London Math. Soc. **66** (2002), 325–333.
[12] L.E. Dickson, *Linear groups, with an exposition of the Galois field theory*, Teubner, Leipzig, 1901 (Dover reprint 1958).
[13] E.F. Ecklund and R.B. Eggleton, *Prime factors of consecutive integers*, Amer. Math. Monthly **79** (1972), 1082–1089.
[14] E.F. Ecklund, R.B. Eggleton, P. Erdős and J.L. Selfridge, *On the prime factorization of binomial coefficients*, J. Aust. Math. Soc. **26** (1978), 257–269.
[15] B. Fein, W.M. Kantor and M. Schacher, *Relative Brauer groups II*, J. Reine Agnew. Math. **328** (1981), 39–57.
[16] J. Fulman and R.M. Guralnick, *Derangements in finite classical groups for actions related to extension field and imprimitive subgroups and the solution of the Boston-Shalev conjecture*, Trans. Amer. Math. Soc. **370** (2018), 4601–4622.
[17] J. Fulman and R.M. Guralnick, *Derangements in subspace actions of finite classical groups*, Trans. Amer. Math. Soc. **369** (2017), 2521–2572.
[18] J. Fulman and R.M. Guralnick, *Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements*, Trans. Amer. Math. Soc. **364** (2012), 3023–3070.
[19] J. Fulman and R.M. Guralnick, *Derangements in simple and primitive groups*, in Groups, combinatorics & geometry (Durham, 2001), 99–121, World Sci. Publ., River Edge, NJ, 2003.
[20] M. Giudici, *New constructions of groups without semiregular subgroups*, Comm. Algebra **35** (2007), 2719–2730.
[21] M. Giudici, *Quasiprimitive groups with no fixed point free elements of prime order*, J. Lond. Math. Soc. **67** (2003), 73–84.
[22] M. Giudici and S. Kelly, *Characterizing a family of elusive permutation groups*, J. Group Theory **12** (2009), 95–105.
[23] M. Giudici, L. Morgan, P. Potočnik and G. Verret, *Elusive groups of automorphisms of digraphs of small valency*, European J. Combin. **46** (2015), 1–9.
[24] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups, Number 3*, Mathematical Surveys and Monographs, vol. 40, Amer. Math. Soc., 1998.
[25] R.M. Guralnick, *Conjugacy classes of derangements in finite transitive groups*, Proc. Steklov Inst. Math. **292** (2016), 112–117.
[26] R.M. Guralnick, *Subgroups of prime power index in a simple group*, J. Algebra **81** (1983), 304–311.
[27] E.V. Hall, *Almost elusive classical groups*, submitted (arXiv:2108.10190), 2021.
[28] E.V. Hall, *The classification of the almost elusive primitive groups*, in preparation.
[29] C. Jordan, *Sur la limite de transitivité des groupes non alternés*, Bull. Soc. Math. France **1** (1872/1873), 40–71.
[30] C. Jordan, *Recherches sur les substitutions*, J. Math. Pures Appl. (Liouville) **17** (1872), 351–367.
[31] P.B. Kleidman, *The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups*, J. Algebra **117** (1988), 30–71.
[32] P.B. Kleidman and M.W. Liebeck, *The subgroup structure of the finite classical groups*, LMS Lecture Note Series, vol. 129, Cambridge University Press, 1990.
[33] M.W. Liebeck and G.M. Seitz, *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, Mathematical Surveys and Monographs, vol. 180, Amer. Math. Soc., 2012.
[34] W.A. Manning, *The primitive groups of class $2p$ which contain a substitution of order p and degree $2p$*, Trans. Amer. Math. Soc. **4** (1903), 351–357.
[35] D. Marušič, *On vertex symmetric digraphs*, Discrete Math. **36** (1981), 69–81.
[36] T. Nagell, *Des équations indéterminées $x^2+x+1=y^n$ et $x^2+x+1=3y^n$*, Nordsk. Mat. Forenings Skr. **2** (1920), 12–14.
[37] C.E. Praeger, *An O'Nan-Scott theorem for finite quasiprimitive permutation groups and an application to 2-arc transitive graphs*, J. London Math. Soc. **47** (1993), 227–239.
[38] S. Ramanujan, *A proof of Bertrand's postulate*, J. Indian Math. Soc. **XI** (1919), 181–182.
[39] J.-P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. **40** (2003), 429–440.
[40] M. Suzuki, *On a class of doubly transitive groups*, Annals of Math. **75** (1962), 105–145.
[41] R.A. Wilson, *Maximal subgroups of sporadic groups*, in Finite simple groups: thirty years of the Atlas and beyond, 57–72, Contemp. Math. vol. 694, Amer. Math. Soc., Providence, RI, 2017.
[42] R.A. Wilson, *The finite simple groups*, Graduate Texts in Math. vol. 251. Springer-Verlag London, 2009.

[43] R.A. Wilson et al., *A World-Wide-Web Atlas of finite group representations*, `http://brauer.maths.qmul.ac.uk/Atlas/v3/`.
[44] J. Xu, *On elusive permutation groups of square-free degree*, Comm. Algebra **37** (2009), 3200–3206.
[45] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), 265–284.

T.C. Burness, School of Mathematics, University of Bristol, Bristol BS8 1UG, UK
Email address: `t.burness@bristol.ac.uk`

E.V. Hall, School of Mathematics, University of Bristol, Bristol BS8 1UG, UK
Email address: `ky19128@bristol.ac.uk`